Information Security Policy: The regulatory basis for the protection of information systems

Chapter · July 2014

DOI: 10.4018/978-1-4666-6320-6.ch006

Edison Luiz Gonçalves Fontes
Faculdade de Informática e Administração Paulista

Antonio José Balloni
Centro de Tecnologia da Informação Renato Archer

Draft version- 1.3 – Final Version published by Hershey, PA: IGI Global:
1.2 – In 2015, this chapter was published in the book " Laboratory Management Information Systems: Current Requirements and Future Perspectives, 2015, **SCOPUS INDEXED**, " < https://www.igi-global.com/chapter/information-security-policy/115609 , DOI: 10.4018/978-1-4666-6320-6.ch006> e, republicado -pelo Editor-,
2.2 – In 2016 the chapter was republished in the book “Web Design and Development: Concepts, Methodologies, Tools, and Applications, 2016, **SCOPUS INDEXED**,” < https://www.igi-global.com/chapter/information-security-policy/137340 , DOI: 10.4018/978-1-4666-8619-9.ch003 >

- Fontes, E., & Balloni, A. J. (2015). Information Security Policy: The Regulatory Basis for the Protection of Information Systems. In A. Moumtzoglou, A. Kastania, & S. Archondakis (Eds.), *Laboratory Management Information Systems: Current Requirements and Future Perspectives* (pp. 95-117). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-6320-6.ch006
- Fontes, E., & Balloni, A. J. (2016). Information Security Policy: The Regulatory Basis for the Protection of Information Systems. In I. Management Association (Ed.), *Web Design and Development: Concepts, Methodologies, Tools, and Applications* (pp. 38-59). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8619-9.ch003

Information Security Policy: The regulatory basis for the protection of information systems

by
Edison Fontes - *FIAP - Brazil*

Antonio José Balloni - *CTI Renato Archer, Brasil*

ABSTRACT

In paper, the reader will find a structured definition to develop, implement and keep the needed regulatory – rules or principles – for an Information System Security (ISS). Also, the reader will find how to ensure the right use of this ISS, as well as regarding the authorization and protection against disaster situations such as an effective system protection when accessing, storing, using and retrieving the information in normal or contingency situations. This compound is the structure of information security policy which is based on a set of controls as described in NBR ISO/IEC 27002 (ABNT, 2005). The definition of this structure for the information security policy is important because the Norm ABNT (2005) does not indicate nor define - or explain - how should be the structure of this policy, i.e., which are their fundamental elements and functions, which are the standards of rules for the controls and other practical issues so that the policy could be effective for the organization. The structure showed in this chapter represents a practical and useful architecture regarding the elements of the information security policy of the organization.

INTRODUCTION

This chapter describes a structure for the information security policy with the objective of facilitating the elaboration of a set of regulations of the organization which comprises this policy. So, this information security policy structure aims to facilitate the development of this set of regulation.

The NBR ISO/IEC 27002 (ABNT, 2005) (Information Technology - Security Techniques - Practice Code for Information Security Management) requires the need of information security policy, but the Norm does not indicate how the regulation or regulations, which make up this policy, should be structured.

It is desirable that the directions of the organization establishes a clear political guidance aligned with the business goals, and demonstrate support and commitment with the information security through the publication and maintenance of an information security policy for the entire organization. (ABNT, 2005)

To prepare an information security policy is a difficult task for the organizations. A tangible example was recorded in organizations that deal with health data, and which do not yet have their policies for information security in spite of their executives understanding of the importance of regulations for information security. Albertin and Pinochet (2010) in their research "Cycle of continuous monitoring for the development of information security policy in hospital organizations", described the survey in five hospitals in the State of San Paolo, Brazil, where in all of them, in a direct or indirect way, the managers declare the importance of information security, but none of them had an appropriate information security policy. Declarations from managers of such hospitals demonstrate the difficulty that these organizations have to generate an information security policy:

The hospital has a serious lack in developing information security policy. (Albertin and Pinochet, 2010).
The managers, in their majority, consider there is a lack of knowledge regarding how to map the needs to develop a formal information security policy. (Albertin and Pinochet, 2010).
The hospital has clear shortcomings in developing information security policy due to lack of guidance from the Secretary (of State) and the board of health. (Albertin and Pinochet, 2010).

According to Picovsky (2012), it is, therefore, necessary the proper and suitable use of information systems, aiming to improve the quality and safety of health care at lower cost. Yet, according to Morales (2007), all of the information that a physician may need should be available in the charts of the patient and, therefore, it is necessary to guarantee security in obtaining this information. This shows clearly the issue and need of a security system -information security policy-.

A survey conducted by Consultancy PriceWaterhouseCoopers (2011), CIO Magazine and CSO Magazine shows policies for information security is an ongoing concern. This study represents a unified data analysis regarding the information provided by more than 12,800 executives, among CEOs, CFOs, CIOs, CSO, and vice presidents, directors of IT and information security officers from medium, large and giant enterprises from 135 countries and all sectors. About 500 of these executives were from Brazil.
In spite of the world crises regarding information security -as described in the survey-, the PriceWaterhouseCoopers (2011) document also presents a compliance with the organization internal policies for information security and the resources with information security process as one of the five most important factors. The other factors were identified as: economic conditions, business continuity/disaster recovery, company reputation and regulatory compliance.
The authors believe the investment in information security is dragged/pulled by five items above mentioned: the information security policy requires the organization to implement actions in such a way that the organization is in compliance with the security rules. In this way, the compliance with the policy and other organizational internal rules becomes a driver/(give directions) towards the spending of resources in information security.

In the year 2013, the PricewaterhouseCoopers (2013) carried out a new research. This time there were 575 executives from Brazil and 9,300 executives from others countries. The survey showed 68% of respondents understand the major challenge of an organization is the establishment of a Security Corporative Strategy. This research indicates that executives need structures which guide them how to implement an information security process; i.e. the executives need guidance on how to distribute, how to prioritize and how to make the controls which will materialize (make real) the information security process.

In a specific situation, Terra and Bax (2003) observes "The analysis of the current situation of Portugal clinical information systems shows that the policies and mechanisms for the security throughout Portugal National Health System -SNS- are not adequate". This indicates the difficulty for establishing policies and norms of information security.

With the objective of facilitating the development of organizational policies and norms for information security, the Court of Accounts of the Union -TCU Brazil- has developed a Document of Best Practices in Information Security -PSI- and guides in relation to the documents elaboration. However this document does not explain the hierarchical structure from this set of documents which will comprise the Information Security Policy:

> *In addition, when the organization finds it is convenient and necessary that its PSI be more comprehensive and detailed; it is suggested the creation of other documents which specify practices and procedures that describe in more detail the rules of use of information technology. These documents are usually available on more specific rules, which detail the users, managers and auditors responsibilities and, typically, are updated with greater frequency. The PSI is the first of many documents with increasingly detailed information about procedures;practices and standards to be applied in certain circumstances, systems or resources. (TCU, 2007)*

However, the lack of guidance on how these documents should be prepared and how should be its structure becomes evident, when in the year 2010 the TCU published the book "Summary Executive Book - Survey of IT Governance-" a survey carried out in three hundred and fifteen (315) government agencies from the Federal Public Administration. This survey indicated only 37% of these agencies had a Security Policy. It should be noted that in this survey was not evaluated the quality of the documents that make up these policies of these 37% agencies. (TCU, 2010).

The necessity of existence of guidance on how it should be the set of regulations that will comprise the Information Security Policy is evident.

At first, in this chapter the information security dimensions based on NBR ISO/IEC 27002 (ABNT, 2005) (Information Technology - Security Techniques - Practice Code for Information Security Management) are presented. In this chapter, the information security policy is presented as one of these dimensions. Next it is presented, according to the norm ISO/IEC 27001 (ABNT, 2006), as the political dimension of security is addressed by Information Security Management Systems. Then practical situations for elaboration of information security policies and presented some normative instructions given by the Brazilian government are presented.

After these considerations, a structure for the standards and policies for information security is presented. It is important to mention that has been taken into account that there are a few guidelines published on the matter and so, the intrinsic difficulty for the preparation of a structure for the information security policy.

Finally, considerations regarding futures work, taking as guideline the content of this chapter, are presented.

AN ARCHITECTURE MODEL FOR AN INFORMATION SYSTEM SECURITY -ISS-.

The previous model of the information architecture of the organization (Balloni, 2004, 2006; Balloni, Azevedo & Silveira, 2012, Oliveira, Balloni, Oliveira & Toda, 2012) has been modified to take into consideration Information System Security (ISS), (Figure 1). This proposed model "*Architecture Model of an Information System Security (AMISS)*" complies (see figure 1) with:

a) - the processes and the organizational levels (strategic, management, knowledge and operational) that allow the definition of the use of the information by the organization, and

b) - the information systems (Supply Chain Management -SCM-, Customer Relationship Management -CRM- and Knowledge Management -KM-), which support the organizational processes assuring the organization uses the information to meet the business objectives.

c) - The IT infrastructure which represents the platform on which the organizations can construct specific IS (the hardware, software and the connections between the systems).

d) - The Information System Security -ISS-, which stands for information security activity monitoring for all managerial levels of the enterprise. It is important to make clear that, in the original figure, (Balloni, 2004, 2006; Balloni, Azevedo & Silveira, 2012, Oliveira, Balloni, Oliveira & Toda, 2012), the BAM (business activity monitoring) has been replaced by the ISS with a similar function, standing for an information system activity monitoring for all managerial levels of the enterprise.

e) - The strategic level in the figure 1 is concerned with the "Information Security Main Policy", as will be presented in figure 3. Yet, the Management Level of figure 1 is also concerned with the "Logical Access, Email message & Internet, Development and Systems Acquisition, Physical Access, Continuity Plan, Information Backup & Retrieval and Information Classification", as also presented in figure 3.

f) – Finally, according to Balloni (2006), the Corporative Portal represented in figure 1, allows the enterprise to have access and to modify the corporation information. It provides the user with a single gateway to get information for decision making. The access and interactivity with the corporation data and information through this Corporative Portal occur in a safe and protected form, for example, through the public keys cryptography system, employed to authenticate the user.

Therefore, for a correct operationalization of all the above systems -the organizational levels & the information systems- towards the security concerns, the model proposed by Figure 1 complies with a transversal Information System Security -ISS-, regarding all other systems previously mentioned. So, the definition is necessary on how this ISS interacts with all the business processes (Process in Figure 1), which uses the information towards the business goals (business partners, suppliers and clients in figure 1).

So, regarding the Information System Security -ISS- the existence of policies and norms are mandatory. They must define how the accuracy of the information controls may meet and deliver a trustful requirement of the needs of the organization, such as:

- Authorized users
- Accountability for the users' authorization
- Continuity of the use of the information
- Compliance to: the legal and corporation requirements

Therefore, in light of the above explanation, the Information System Security -ISS-, figure 1, exists as a third element that makes the inter-relationship among the information of the organization (their businesses processes) and the information technology systems (SCM, CRM, KM).

POLICY FOR THE INFORMATION SECURITY AND THE ORGANIZATION

For an effective, efficient and continued information protection, there are policies to be followed -among other controls- as presented below:

The information security is got from the implementation of a set of appropriate controls, including policies, processes, procedures, organizational structures and software & hardware functions (ABNT, 2005).

These controls, whenever needed, must be established, implemented, monitored, critically analyzed and improved, to ensure the objectives of the organizational business and security issues are met. (ABNT, 2006).

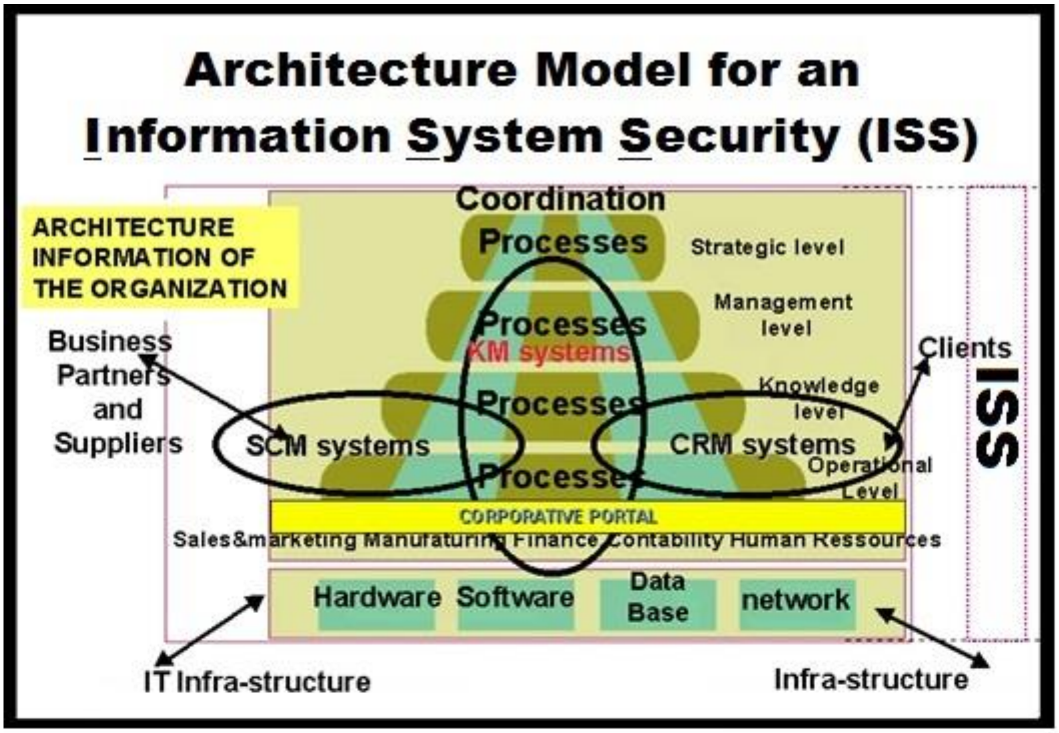

Figure 1: Architecture Model of an Information System Security (AMISS). The AMISS deals with the particular project of a security ecosystem towards a chain or specific information security concerns. The.AMISS comprise both, the Information Technology -IT-hardware and the Information System -IS- in the organizational structure. Details from this figure has been explained in the beginning of the section "Architecture Model for an Information System Security" -ISS-, itens a - f. This figure has been adapted from Balloni et al (Balloni, 2004, figure 1; Balloni, 2006, figure 1; Balloni and Azevedo, 2012, figure 6; Balloni and Barbará, 2012, figure 4), by inserting the concept of ***ISS****.*

Figure 1: *The Architecture Model of an Information System Security (AMISS)" deals with the particular project of a security ecosystem towards a chain or specific information security concerns. The AMISS comprise both, the Information Technology -IT- hardware and the Information System -IS-in the organizational structure. Details from this figure have been explained in the beginning of the section "The Architecture Model of an Information System Security" -ISS-, items a – f. This figure has been adapted (Balloni, 2004, 2006; Balloni, Azevedo & Silveira, 2012, Oliveira, Balloni, Oliveira & Toda, 2012), by inserting the concepts of* ***ISS****.*

For a better understanding, Fontes (2008) organized these controls in functions of dimensions as presented in the figure 2, the security policy and their dimensions.

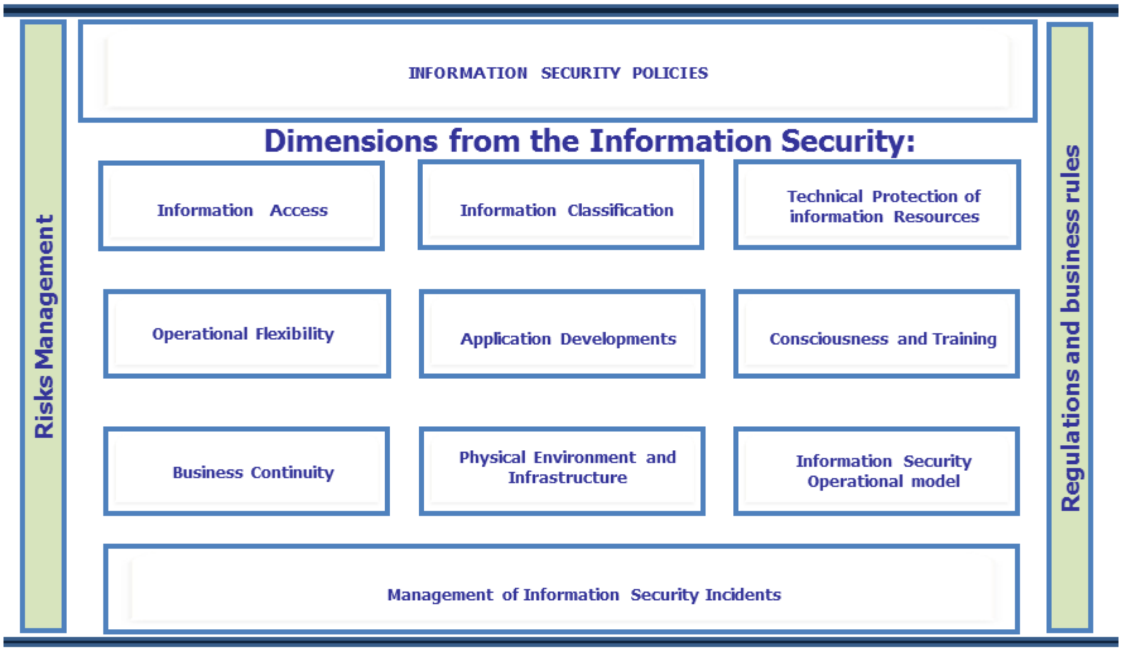
INFORMATION SECURITY POLICIES
Dimensions from the Information Security:
Information Access
Information Classification
Technical Protection of information Resources
Operational Flexibility
Application Developments
Consciousness and Training
Business Continuity
Physical Environment and Infrastructure
Information Security Operational model
Management of Information Security Incidents
Risks Management
Regulations and business rules

Figure 2: This figure presents the ten Dimensions from the Information Security.
This structure has been based on International Standard ISO/IEC 27002:2005 - Source: Fontes, 2008.

Figure 2: *This figure presents the ten Dimensions form the Information Security. This structure has been based on International Standard NBR ISO/IEC 27002 (ABNT, 2005) – Source: Fontes (2008).*

However, this NBR ISO/IEC 27002 (ABNT, 2005) Norm mentioned in figure 2 do not present how the controls should be structured. It only defines the purpose of the policy - such as information access, information classification, technical protection of information resources etc - and suggests the organization must support these actions. This is also presented by the item 5.1 in the Brazilian Norm NBR ISO/IEC 27002 (ABNT, 2005), as is presented below:

> *5.1 - Information Security Policy*
> *Objective: Providing the managers a guidance and support regarding the information security in compliance with the business requirements, the laws and the relevant regulations.*
> *The managers should establish a clear policy aligned with the business goals as well, to demonstrate their support and commitment regarding the security of the information by publishing and maintaining information security policy for the entire organization.*

Regarding the Brazilian Norm NBR ISO/IEC 27002 (ABNT, 2005) above described, we could affirm the business goals mentioned in its second paragraph could be part of the business processes -and the respective managerial levels- presented in Figure 1. The Information System Security -ISS- stands for the information security activity monitoring all managerial levels of the enterprise (Strategic, Management, Knowledge and Operational)
However, the importance of an information security policy and an effective information security program has been highlighted by Peltier (2004, 2005) as:

> *The policy is a directive from the executive management who aims to create an information security program, to establish the goals and to define accountabilities. With the policy implementation process, the organization takes control of its destiny. (Peltier 2004). The first and most important aspect of information security is the security policy issues. If the security of the information were a human being, so the security policy would be its nervous system. Politics is the basis of the information security, since it provides the structure and defines the goals of all other aspects of information security. (Peltier 2005).*

The statement above (Peltier, 2005) is in agreement with the model proposed in the figure 1: the ISS stands for the information security activity monitoring all managerial levels of the enterprise (Strategic, Management, Knowledge and Operational) -so secure policies are indeed the core for the proposed Architecture Model of an Information System Security (AMISS)- figure1.

The norm ISO/IEC 27001 (ABNT, 2006) is another regulatory element. According to this norm the security policy should take into consideration the PDCA model (Plan, Do, Check, Act) regarding the Management of System and Information Security (MSIS) -this management should be carried out through the Information Security System- ISS, Figure 1.

According to Dartmouth (Dartmouth, 2008) the PDCA cycle is a methodology which may be applied aiming the improvement of any process or system. Balloni and Holtz (Balloni & Holtz, 2008) proposed the use of the PDCA cycle -associated with other methodologies-, as a way to make feasible the Business Process Reengineering (BPR) towards the IT Sociotechnical Concerns & Human Relationship & Synergy.

As previously mentioned the ISS, figure 1, stands for the information security activity monitoring all managerial levels of the enterprise. Regarding the PDCA, Table 1 presents its description towards the security management which is clearly concerned with sociotechnical aspects of the enterprise (figure 1), its synergism and the ISS continuous improvement.

*Table 1 – PLAN, DO, CHECK, ACT (PDCA) towards the **M**anagement of **S**ystems and **I**nformation **S**ecurities -**MSIS**-.Source: NBR ISO/IEC 27001(ABNT, 2006) and* 02/IN01/DSIC/GSIPR (DSCI, 2008)

PLAN: establishment of the MSIS	To establish a policy, goals, process and procedures for the Management of System and Information Security. These are relevant for the risk management and the improvement of the information security. It aims to generate results according to the policies and global objectives of the organization. These policies are established by the Strategic level, figure 1.
DO: implementing and functioning the MSIS	To implement and accomplish the policies, controls, processes and procedures for the Management of System and Information Security -MSIS-. These policies are implemented by the Managerial level of figure 1.
CHECK: monitoring and critical analysis from the MSIS	To assess and when possible, to measure the performance of the process regarding the policy, objectives and practical experience of the Management of System and Information Security -MSIS-. To present the results for the managerial critical analysis -which should be carried out by the Knowledge level in compliance with the Managerial and Strategic levels, figure 1-.
ACT: to keep and generate improvement in MSIS	To prevent and improve actions based on the Management of System and Information Security -MSIS- internal auditing and a managerial critical analysis –or any other pertinent information–, aiming for continuous improvement in the MSIS. This internal auditing and critical analysis should be carried out in compliance with the Knowledge level, figure1.

Therefore, this security PDCA cycle process -Table 1- should be applied constantly from top to bottom through all managerial levels, figure 1, establishing the politics for information security of the organization.

For the reasons above, the organization must have a policy regarding its security of information to ensure the process of information security can be developed, implemented and maintained according to the security *PLAN, DO, CHECK, ACT* -PDCA cycle- as presented in Table 1. This policy will define the guidelines, the limits and directions regarding the controls that will be implemented for the protection of the information from the organization. (ABNT, 2005; Vianez, Segobia and Camargo, 2008)

By virtue of the legislation -Sarbanes-Oxley Law-, the financial segment of organizations and also large corporations from the United States, which have shares in Stock Exchanges, have already been forced to draw up their policies for information security. Other organizations have decided to follow this structured Corporative Governance, including Brazil, and so they are also constrained to develop and implement policies for information security. So, since a few years ago, many organizations have already their security policies and have also made revisions and practical adjustments to these security policy regulations.

However, other organizations are not -yet- qualified regarding their information protection through a more formal and structured manner. This lack of capability from these organizations happens because they provide services for larger organizations and the larger organizations are required to have their own structure of information security. Nowadays these organizations have understood their suppliers (small organizations as being part of their business supply chain) must have the same degree and security infrastructure of information as have larger organizations. This was in harmony with the proposed Architecture Model of an Information System Security -AMISS-, figure 1, which has presented an integrated vision of all business supply chains: the Information System Security -ISS- standing for an information security activity monitoring all enterprises in the chain.

In other situations, such as aiming at the business sustainability, there are the entrepreneur awareness and/or the mature attitude from the shareholders. These required the organization to make use of the best security practices by having the appropriate organizational controls for information security.

Many health organizations do not have -yet- their policies for information security aiming the protection of their data, even though their executives have understood the importance of safety regulations of information. Albertin and Pinochet (2010) have presented in the paper "Cycle of continuous monitoring for the development of information security policy in hospital organizations" that in all the five hospitals from their survey (in the State of San Paolo, Brazil), the hospitals' managers have declared that, in spite of their understanding regarding the importance of information security, none of the hospitals has an appropriate policy for information security. Occasionally, they have some rules for supervising the access to the computing environment. Based on statements by the hospital managers, it becomes clear that the difficulty of these organizations relates to the generation of an information security policy:

> *The hospitals have shortcomings in developing information security policy and most of their manager's state there is a lack of knowledge regarding how to map out, develop and implement a hospital information security policy; there is a lack of guidance from Board of Health and State Secretary. (Albertin & Pinochet, 2010).*

When the hospital organization seeks to develop an information security policy, it will be faced with a large amount of requirements described in the Brazilian Norm ISO/IEC 27002 (ABNT, 2005). In this NBR norm, these requirements are addressed in an egalitarian way, pointing out that a possible policy should contain all those requirements. Besides, the NBR norm does not provide information how this set of regulation or requirements should be structured. In the section, "Structure for the Information Security Policy", this set of regulations is presented in its figure 3.

In a pilot research carried out in 118 hospitals distributed around 7 countries (Management of System and Information Technology in Hospitals –GESITI-), (GESITI, 2013) it has been found that several controls for Information System Security (ISS) have not been implemented such as, to highlight the research, the following essential control: Identification and Access Management Software. Table 2 presents the results from this pilot research regarding the ISS of countries and hospitals surveyed:

Table 2: GESIT Health Pilot Project and some Security Information System VS. Countries and Number of Hospitals Surveyed. Source: GESITI (2013).

COUNTRIES and Amount of Hospitals: **Information System Security (ISS):**	SLOVAKIA **20**	CZECH REPUBLIC **3**	BRAZIL **76**	PERU **5**	PORTUGAL **7**	BULGARIA **4**	MÉXICO **4**
Security System Management Software	2	2	18	-	5	1	-
Firewall	17	2	49	3	7	3	4
Net Security Software	10	1	36	1	4	2	4
Intrusion Detection System	6	-	23	-	6	1	-
Identification and Access Management Software	**7**	**2**	**26**	**-**	**4**	**1**	**4**
Antivirus	20	3	64	5	7	4	4
SSO (Single Sign-On)	-	-	38	-	5	1	-

The non-existence of an information system security -such as Identification and Access Management Software - may signify there is not any security policy, or if it exists, its application is not happening as it should. Whatever the option, it indicates that the existence and implementation of an information security policy are not an easy task.

According to Fontes and Balloni (2007) "The security in information systems must contemplate not only the technical aspects. The social aspects related to the organization environment and the people also have importance and must be considered". The information security policy interacts directly with people since it is the instrument by which the organization shows the organization information security. This policy needs to be well thought out, very well structured and easy for communication to meet the social aspect of the information security process from the organization. Fontes and Balloni (2007) explain this characteristic as follows:

> *4. SOCIAL ASPECTS*
>
> *4.1 – Regulations - The regulations (politics, norms and procedures) provide the definitions and make explicit what must be considered as a standard behavior. The people must follow these regulations; otherwise they will be breaking the organization coexistence rules. The existence of these explicit rules is very important for the social environment*. (Edison & Balloni, 2007).

As we have showed, through this chapter, the characteristic, above mentioned, was in harmony with the concepts presented in the Figure 1 (Architecture Model of an Information System Security -AMISS-), where all managerial levels are responsible for the rules of the organizational coexistence -also presented in Table 1, PDCA security cycle- regarding the business process reengineering (BPR), as previously discussed.

STRUCTURE FOR THE INFORMATION SECURITY POLICY

For the development of regulations (policies, standards and procedures) that will comprise the information security policy it is necessary to structure a set of regulations to facilitate the understanding. Figure 3 presents the Architecture of the Information Security Policy with a Set of Regulations.

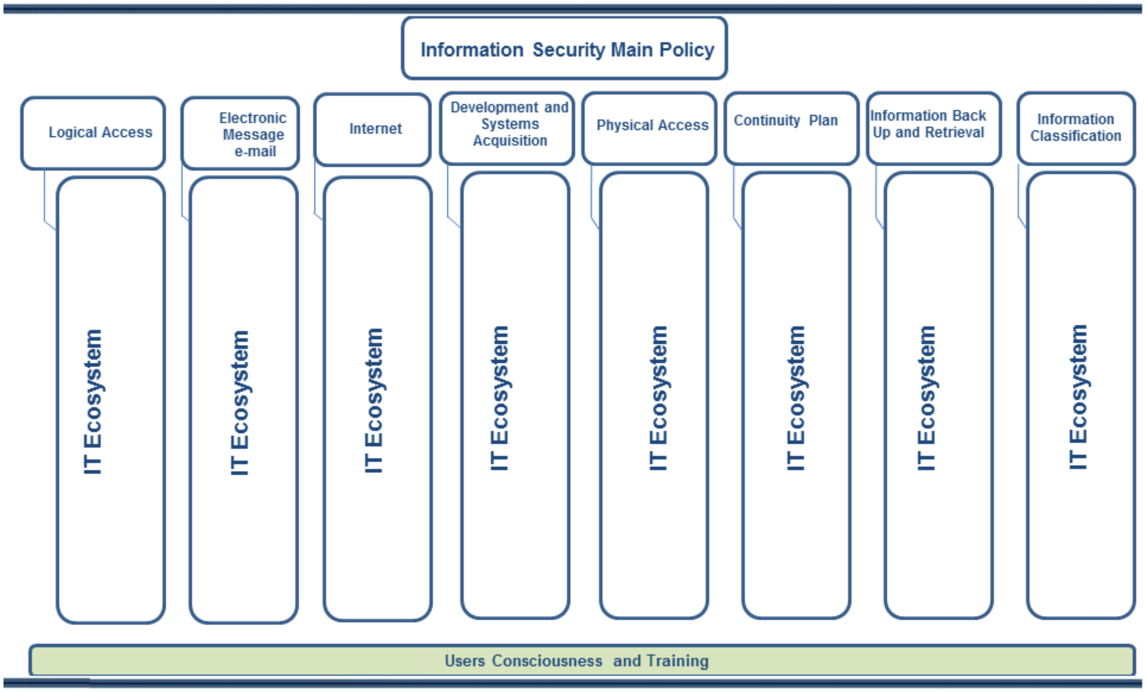
Information Security Main Policy
Logical Access
Electronic Message e-mail
Internet
Development and Systems Acquisition
Physical Access
Continuity Plan
Information Back Up and Retrieval
Information Classification
IT Ecosystem
IT Ecosystem
IT Ecosystem
IT Ecosystem
IT Ecosystem
IT Ecosystem
IT Ecosystem
IT Ecosystem
Users Consciousness and Training

Figure 3: Architecture of the Information Security Policy presenting a Set of Regulations (such as: Logical Acess, electronic Message e-mail etc), wich should comprise the rules of an information security system. The IT Ecosystem deals with the particular project of an ecosystem towards a chain or specific niche of market [Balloni and Azevedo, 2008]. To maximize the benefits of the IT ecosystem is necessary to plan the AMISS Architecture (figure 1) of this IT Ecosystem and, this is the great managerial challenge, i.e., to create a uniform sociotechnical system uniform in which everyone is using similar processes and information: integration of key business processes of this IT ecosystem and improvement of the ISS coordination, efficiency and decision making in all managerial levels of figure 1. This figure has been adapeted from Fontes (Fontes, 2012, figure 10), by inserting the concept of IT Ecosystem

Figure 3: *Architecture of the Information Security Policy presenting a Set of Regulations (such as: Logical Access, electronic Message e-mail etc.), which should comprise the rules of an information security system. According to Balloni, Azevedo and Silveira (2012), the IT Ecosystem deals with the particular project of an ecosystem towards a chain or specific niche of market. To maximize the benefits of the IT Ecosystem is necessary to plan the AMISS Architecture (figure 1) of this IT Ecosystem and, this is the great managerial challenge, i.e., to create a uniform sociotechnical system in which everyone is using similar processes and information: integration of key business processes of this IT Ecosystem and improvement of the ISS coordination, efficiency and decision making in all managerial levels of figure 1. The figure 3 has been adapted from Fontes (2012), by inserting the concept of IT Ecosystem.*

Peltier (2004) considers the Policy as the highest level of statement an organization believes and wants. These levels of statement from all organizations are known as functional areas of business organization. Figure 1 presents the main and more important functional areas from an organization (Human resources, Finance etc).

So, the policy is a directive from the executive board (or strategic level from figure 1) to create a program of information security, establish goals and define all responsibilities which must be drilled up (detailed) to all functional areas. This executive board must be aware of the description of PDCA -Table 1- regarding the management of systems and information securities and which is clearly concerned with sociotechnical aspects of the enterprise (figure 1), its synergism and the ISS continuous improvement. The PDCA cycle process should be applied constantly from top to bottom through all managerial levels for establishing the politics for the information security of the organization.

Policy and Security Policy definitions: *A policy is a general guide for the action. It delineates an action and not a moment for that action. It is a definition of purpose from a company, and it establishes guidelines and limits for the individual actions which are responsible for its implementation. The policies are principles that establish rules for action and contribute the successful achievement of objectives. (Chiavenato, 2010).*

Regarding the above Chiavenato statement, the rules for the actions mentioned are aligned with the PDCA security cycle process -Table 1-, which should be applied constantly from top to bottom through all managerial levels, figure 1, establishing the politics for information security of the organization.

Security Policy is a general guideline set intended to manage the protection that will be given to information assets. (Caruso & Steffen, 1999) -Security Policy is a set of rules and standards regarding what must be done to ensure the information could receive a convenient protection guarantying its confidentiality, integrity and availability. (Barman, 2002).The policies are guidelines that indicate the limits or restrictions regarding what you want to achieve. (Albertin and Pinochet, 2010)

The Court of Accounts of the Union - Brazil - presents its definition of Security Policy:

The Information security Policy is a set of principles that govern the management of information security, which must be followed by the technical and managerial staff and internal and external users. The established policy guidelines must be followed by the institution in order to be assured their computing resources and information - guaranteed protection by the policy guideline-. (TCU, 2012).

Again, the definition from the Court of Accounts of the Union - Brazil can be delineated from the PDCA security cycle process -Table 1. The Document 03/IN01/DSIC/GSIPR of 30 June 2009 (DSIC, 2009) - Guidelines for the preparation of the Information Security Policy and Communications in Government Agency and Entities from the Federal Public Administration-, from the Department of Communication and Security Information, Office of Institutional Security of the Brazilian Republic Presidency- states: “the commitment from the high level directions of the organization with views to provide strategic guidelines, responsibilities, skills and support to implement the communication and information security management in the Government Agency or Entities from direct and indirect Federal Public Administration."

However, the NBR ISO/IEC 27002 (ABNT, 2005) Norm (Information Technology - Security Techniques - Practice Code for Information Security Management), and no other norm from the ISO/IEC 27000 Family, defines the set of documents that constitute the Information Security Policy, as well as, in which way these documents will be divided.

The Information Security Best Practices Manual, from the Court of Accounts of the Union (TCU, 2012) cites some topics that should be considered in the Information Security Policy. However, this TCU/Manual does not define the composition of these topics. This Manual presents the following:

The Information Security Policy (ISP) may be composed of several inter-related policies, such as the policy of passwords, backup, recruitment and installation of equipment and software. Furthermore, when the institution finds that it is convenient and necessary the ISP should be more comprehensive and detailed, so it suggested the creation of other documents which specify practices and procedures describing in more detail the rules of using information technology. (TCU, 2012)

This TCU (2012) Best Practices Manual mentioned above is in agreement with the survey presented in Table 2: Security Information System VS. Countries and Number of Hospitals Surveyed. It can be seen from this table, regarding the Security Information System that, in all 76 Brazilians Hospitals surveyed, we have only 64 with antivirus protections, only 49/firewall, 38/SSO etc). This observation has generated a new research proposal outlined in the section "future research direction".

In relation to the elements that compose the Information Security Policy, the Document 03/IN01/DSIC/GSIPR of 30 June 2009 (DSIC, 2009) -Guidelines for the preparation of an Information Security Policy and Communications in Government Agency and Entities from the Federal Public Administration-, from the Department of Communication and Security Information, Office of Institutional Security of the Brazilian Republic Presidency- points out that at least the followings topics should be considered:

a) Handling of Information;
b) Handling of Network Incidents;
c) Risk Management;
d) Management of Continuity;
e) Auditing and Compliance;
f) Access Controls;
g) Using e-mail; and
h) Internet Access

Therefore, for the elaboration of a set of regulations -presented in figure 3- which comprises the information security policy, the existence of architecture is required, which must settle how linked are these set of regulations. This architecture enables the Organization to understand and plan (before having the set of regulations), the set of documents which comprises the rules of information security that should be complied by all. Figure 2- Dimensions from the Information Security presents how linked are these set of regulations. Figure 3 and figure 1 as well the PDCA Security cycle -Table 1- are intertwined regarding the "Structure for the Information Security Policy".

Taking into consideration the norm NBR ISO/IEC 27002 (ABNT, 2005), Fontes (2012) recommends that the structure of the regulations -rules to be applied in the organization-, must be divided into at least three levels of specifications. Fontes (2012) has identified the following levels of details -rules to be applied in the organization- as described below.

a) Level 1 - Guideline Document or Main Policy

This document - Guideline or Main Policy- contains the basic controls for the information security of the organization. It does not detail how these controls will be implemented and, nor it presents how or in which time and restrictions will these controls happen. In short, this document describes the philosophy of the organization in connection to information security. It presents the principles which should be followed by all users (employees, trainees, service providers, visitors and etc) of the organization. This organization philosophy must be the basis for the documents which will contain the detailed rules for each dimension of the information security. Table I should be extensively considered in the generation of the main policy document.

This Guideline or Main Policy of Information Security must be devised as a strategic planning document which does not need to be changed in the next five to ten years. As this strategic document contains the Basic Principles (the controls the organization wants -their guidelines-), and which explicitly states the organization philosophy, so very hardly the defined controls from this document will be changed over time. A specific technology should never be presented in the guideline document since this technology will be obsolete in a couple of years -rather this guideline document should mention the IT ecosystem as in figure 3-. This guideline document must also be generated by the security process coordination -the strategic level of the organizations, as presented in figure 1-.

This Guideline or Main Policy -which must be aligned with the organization's guidelines-, must also be signed by the president of the organization or must be approved by the Board of Directors of the Organization, with the final decision making formally registered in the Board´s minutes meeting.
This main policy should present what is requested from the information security, i.e., what are the macro controls the organization must implement to protect its information. However, this policy does not describe how the macro controls will be implemented. This will be described in detail in the documents of levels 2 and 3.

The approval by the Board of Directors becomes indispensable if the Counselors make use of an information system and receive an identification and authentication code for the information access. In general, for the information architecture of the organization, as proposed in the figure 1, the organization has its Corporative Portal, which provides the infrastructure means for such transaction -in whatever place it could be located by the Board of Director members-.

Example of control described in the Guideline or Main Policy Document
=> The identification of each user is nontransferable -which guarantees the information veracity-.

b) Level 2 – Document Norm or Policy Dimension

The documents that will compose Level 2 from the Structure of the Information Security Policy of the Organization shall define the basic rules (basic controls) for each Information Security Dimension.

The basic controls of the documents for Level-2 must be consistent with the structural controls (organization philosophy) as explained in the second paragraph of “a) – Level 1”, and begin to detail how the controls should be implemented.

The controls defined in these Level 2 Norms should be detailed in such a way as to present how they should be developed and implemented. For the specific situation of existing distinct environments which requires different controls for its implementation, Level-2 controls should not go in detail and must clarify the basic rules for the specific Information Security Dimension. For this specific situation, the details must be left to Level-3” Action Procedure or Technical Guidance Document.

At least there should be a quantity of Level-2 documents which are identical to the quantity of Information Security Dimensions (ten) and are considered in the Process of Information Security of the Organization. Figure 2 presents the ten Dimensions from the Information Security.

Example of control described in the Norm or Policy Dimension.
=> When the authentication is performed by using a password; it must be kept secret and within the exclusive knowledge of the owner. Not even the headship should request the password of another user.

c) Level 3 - Action Procedure or Technical Guidance Document

This document sets out in detail the actions that must be performed, or the content that must exist in the documentation or the technical detail which must be followed to ensure that the controls (as defined in Dimension Norm or Policy Dimension or the Main Policy Guideline), can be developed and implemented in the organization.

The documents prepared for this level and levels below, are of great detail. These documents complement and will allow the organization has the settings for the operationalisation of its controls and, in this way develop, implement and keep the success from its Information Security Policy, which is the basis for its Information Security Organizational Process.

d) The Next Levels

For a formal effect of architecture, the definition will be up to Level 3 -Action Procedure or Technical Guidance Document-. In short: the three levels already presented allow the understanding of the structure, so whenever this is necessary more detailed level of definitions -level higher than 3- regarding the organization information security regulation may be carried out.

Example of controls described in the Procedure for Action Document or Technical Specification Document. = When forgetting the password in the computational environment the user must ask his manager to send an email to the security support in order to give him a new password.

Structure: Visualization of the Information Security Policy Architecture

According to Fontes (2012), figure 3 presents the structuring of the Information Security Policy Architecture. This figure presents three levels, respectively:
1. The first level (Information Security Main Policy) must be a Guideline or Main Policy document.
2. The second level presents the eight structuring Dimensions of Norm (Logical Access, Electronic Message, Email, Internet, etc). For each of these structuring Dimensions of the Norm there are the corresponding ten dimensions as has been described in figure 2 (Information Access, Information Classification, Technical Protection etc).
3. Finally, in the third level of figure 3 (IT Ecosystem), documents with a detailed description of the actions must exist, presenting technical standards or documentation registration (IT ecosystem) regarding the concerned Dimensions of the Norm (level 2).

ELEMENTS OF THE ARCHITECTURE/STRUCTURE FROM THE INFORMATION SECURITY POLICY

According to Fontes (2008) the Political Dimension of Information Security (Figure 2) deals with controls from other dimensions of the process of information security. Therefore, the elements that make up the Structure of the Information Security Policy correspond to the Dimensions of Information Security. This Structure of Information Security Policy is formed by the following levels of controls:

Main Guideline or Policy - Level 1

This document sets out the basic rules and the foundations for the information security process of the organization. Everything that has been written in this document should be described with more detail in documents of Levels 2 and/or 3 and, by showing how it should be done.

Each one of the information security dimensions -figure 2- must be considered in this document so that the organization directions explain the basic rules and guiding questions for each dimension and must exist only as one Guideline Document or an Information Security Main Policy document. This document must be signed by the President of the Organization or must be approved by the Board of Directors of the Organization or approved by another body-person who has hierarchical power to ensure that all the people who will read the document will understand that these rules are serious, are for all users and are mandatory -Table 1-

The Dimension Norm or Dimension Policy - Level 2

a) Logical Access

This document details the basic principles of information security defined in the Main Policy in relation to logical access of information. It should be detailed controls and rules that are common to all the technology environments. The detail of each technology environment must be defined in a document of logical access for each environment, standard Level-3 in the Architecture of Information Security Policy -Figure 3-.

You must set user id, user authentication, access logging, access authorization, access limitations (time, scheduling, dates), information manager, manager of the user, inclusion/change/deletion of user identification.

b) Physical Access

This document details the basic principles of information security defined in the Main Policy in relation to the physical access that contains information resources. It should be detailed controls and rules that are common to all physical environments. The specific controls for each physical environment must be defined in a document of physical access of each environment, standard Level-3 in the Architecture of Information Security Policy.

You must set user id, user authentication, access logging, access authorization, access limitations (time, scheduling, dates), information manager, manager of the user, inclusion/change/deletion of user identification.

c) Electronic Mail

This document details the basic principles of information security policy defined in the Main Document in relation to the use of electronic mail by users. It should be detailed controls and rules that are common to all types of electronic mail used by users of the Organization. Specific controls of information security for each type of electronic mail should be defined in an e-mail document -a specific tool, standard Level-3 in the Architecture of Information Security Policy-.

You must set: electronic address identification, types of users that will have access to electronic mail, authorizer for user access electronic mail, responsibility for the user inclusion and exclusion in electronic mail, rules for professional use of corporate mail, rules use of personal mailbox.

d) Internet

This document details the basic principles of information security defined in the Main Policy in relation to the use of the general environment of the Internet. It should be detailed controls and rules that are common to the general environment of the Internet used by users of the Organization.

For the construction of the information security controls of this regulation, the organization should identify what activities are and are not allowed by the user when using the Internet. The laws of the country where the organization is, the contracts with customers and the business rules should be considered in the definition of these controls. The necessity of the use of the Internet for conducting the business of the organization should be considered as priority -business goals-. The controls must be explicitly defined, without leaving doubts in its interpretation.

e) Social Networks

This document details the basic principles set out in the information security in the Main Policy in relation to the use of tools of social network by users. This issue can be included in the Internet Dimension, but possessing specific characteristics. A separate document for this subject, thus facilitating its maintenance is recommended. See Table 1 and discussion earlier -above- to that table-.

It should be detailed controls and rules that are common to all types of social networking tools used by users of the Organization. Specific controls of information security for each type of social networking tools should be defined in a document of social network -specific tool, standard Level-3 in the Architecture of Information Security Policy-.

The use of social networks by using the organization's resources should consider two situations. The first is the use of these social networks for the official presence of the organization in the corporate world of the digital environment. In reality, the rules of the organization's exposure must exist for this digital environment as for the conventional environment. The organization must be present in social networks to communicate with their customers, with the market and also for the corporate positioning in this digital world. The second situation is the presence of the user as an individual, as a person in this social network. For the two situations described -corporative or individual presence-, the organization must define information security controls for using the social networks. Consideration of legislation, contractual and which affect the organizational climate should be considered when defining the information security controls of this regulation. The controls must be explicitly defined, without leaving doubts in its interpretation.

f) Information Technology Equipment

This document details the basic principles of information security defined in Main Policy in relation to the use of information technology equipment by users.

It should be detailed controls and rules that are common to all types of information technology equipment used by the users of the Organization. Specific Controls for information security for each type of information technology should be defined in a specific document of technology equipment, standard Level-3 in the Architecture of Information Security Policy -figure 3-.

The performance of each user with the digital world happens with the use of equipment. Currently there is a great diversity of types of equipment, as well as a diversity of operating systems which control equipment. Another issue is in relation to the equipment when the users have their own equipment with better quality and more modern than those supplied by the organization. In such cases, users want to use their personal equipment in the digital environment of the organization (BYOD - Bring Your Own Device). In the light of this huge variety of options for use of equipment, the organization needs to define what information security controls are required to follow. This regulation must set the rules how the information technology equipment will be allowed and used by users.

For the controls, the definition and positioning of the area of information technology are fundamental. Why? Because the maturity of the organization, the technical possibilities available and the capacity of the technical area to control and to protect the digital environments, will determine the rigidity of controls to be defined and implemented. According to the continuous and rapid updating of equipment, this regulation will be one which will be more frequently updated. The controls must be explicitly defined, without leaving doubts in its interpretation.

g) Classification of the pattern of information secrecy

This document details the basic principles of information security defined by the Main Policy in relation to the pattern of secrecy of information, that is, classification of information.

It should be detailed controls and rules that are common to the information standard secrecy used by the users of the Organization. This means that this document should contain what procedures define the pattern of secrecy of information and must also contain the controls that should be implemented in relation to information, after the same is classified in relation to their pattern of secrecy.

Before elaborating this regulation of information classification, the organizations must analyze and assess their needs in relation to the information confidentiality. Once the organization needs are identified, the levels of information confidentiality are identified, that is, where each level has rules for the use of classified information. This requires new responsibilities for the managers of the organization specifically for the information managers, because the managers have an obligation to carry out the information confidentiality classification. With the existence of this regulation, presenting the levels of information confidentiality, the information of the organization must be classified based on this classification, and the procedures for maintaining the confidentiality of information may be defined and implemented. The controls must be explicitly defined, without leaving doubts in the interpretation.

h) Development, implementation and maintenance of applications systems

This document details the basic principles of information security defined in the Main Policy in relation to the development, implementation and maintenance of application systems.

It should be detailed controls and rules that are common to all types of applications developed and implemented for the organization. Specific controls of information security for each type of application must be defined in a document for the development, implementation and maintenance - System application, standard Level-3 in the Architecture of Information Security Policy-, figure3.
The implementation of information security controls in the process of development and maintenance of application systems of information technology is dependent on the existence of a methodology for systems development that consider the participation of the information security area. It is necessary the security controls described in this regulation be considered in the beginning of the development or maintenance process of applications. The organization must be determined to require the security controls definitions on each of the applications. For the implementation of the regulation of each control of information security, it is a must have the participation of business areas, while also considering the information and user managers. It is important to note that typically the business areas do not participate in these definitions of information protection. This regulation will help to change the organization culture in relation to the responsibilities concerned with information security. The controls must be explicitly defined, without leaving doubts in the interpretation.

i) Continuity Business Plan

This document details the basic principles of information security, as defined in Main Policy in relation to the use of information resources required for the business continuity, unavailability of information resources.

It should be detailed controls and rules that are common to all types of business continuity plans used by the organization. Specific controls of information security for each type of business continuity plan should be defined in a continuity plan - specific situation, standard Level-3 in the Architecture of Information Security Policy.
Business continuity is the responsibility of all areas of the organization. With the existence of the digital environment, this responsibility has migrated to the technology area; which is an ongoing mistake. The technology area will implement solutions to meet the needs of business and/or administrative areas. Therefore, it is a must be very well defined and explicit to the business and/or administrative areas their responsibility to define the requirements for recovery, such as time and limit of financial impact, operational and image, when the occurrence of a situation of unavailability. There is another important issue which, in spite of being valid for all other regulations of information security, it is critical to this regulation: the control definitions must be endlessly tested at a frequency consistent with the size of the organization and business type. This regulation deals with the business existence after adverse situations and so; it must be explicitly approved by the organization executive manager: the rigidity of this regulation controls will generate financial costs and impact on people's time. The controls must be explicitly defined, without leaving doubts in the interpretation.

j) Security Copies – Backup copy

This document details the basic principles of information security defined in the Main Policy in relation to the use of security copies of the organization.

It should be detailed controls and rules that are common to all types of security copies used by the business areas of the organization. Specific controls of information security for each type of security should be defined in a document of backup -specific system, standard Level-3 in the Architecture of Information Security Policy-, figure 3.
For the elaboration of this regulation, it is a must the involvement from the business and administrative areas. Backup copies exist to meet the legal, information technology, historical and care for audit needs. Except for the information technology, other needs must be defined by business and administrative areas: this is a situation where these areas are not commonly used to be involved i.e., in practice, because all the information is in a digital environment; the responsibility has been left for the information technology area. The information technology area should develop actions to meet the backup needs from the business and administrative areas. This regulation will allow the existence of a business continuity plan since it will make possible the existence of the information backup in alternate locations, even if the original information has been destroyed. This regulation affects the organization culture in relation to the responsibilities concerned with information security processing. The controls must be explicitly defined, without leaving doubts in the interpretation.

k) Risk Management

This document details the basic principles of information security defined in the Main Policy in relation to the Risk Management. It should be detailed controls and rules that are common to all types of risk management used by the organization. Specific controls of information security for each type of risk management should be defined in a document of risk management -specific situation, standard Level-3 in the Architecture of Information Security Policy-, figure 3.
The information security risk management implementation is the responsibility of the area of information security which should involve other organizational areas concerned with each aspect of information security. The controls defined in this regulation shall indicate the manager responsible for the risk management. The business and administrative areas must be involved (this does not occur in most of the organizations). Therefore, it is necessary the responsibilities be well defined and the security control of this regulation ensures its implementation. For organizations which already have implemented some risk management, the development and implementation of this control should be much easier. For organizations in which this theme is not common, there will be greater difficulty in the development and especially in the implementation of risk management in information security. In this latter case, the true participation of the executive direction of the organization will be crucial. The risk management interacts with all aspects of information security and indicates the effectiveness of the controls of other regulations. In short: the more effective the risk management, more effective will be the information security of the organization.

FUTURE RESEARCH DIRECTIONS

The following future studies on policies and standards for information security are recommended:

1. To apply the structure presented in this chapter in organizations of various sizes and, also to conduct a survey evaluating the difficulty of implementation and easiness of maintenance of elements of security policy.

2. To make a research in a large number of organizations, questioning the elements presented in this chapter, regarding the structure of information security policy, need for other elements?

3. Search for the comparison of the effectiveness between organizations that have implemented this structure -presented in this chapter- to the information security policy and organizations of size and type of business equivalent that do not have implemented this structure, or other equivalent structure.

4. Take into consideration other information security structures, other than those presented by the norms of the family ISO/IEC 27000 family.

5. Regarding the results presented in Table 2 (*GESIT Health Pilot Project and some Security Information System VS. Countries and Number of Hospitals Surveyed, GESITI (2013)*), a future research could be the investigation of correlations between the low implementation of information security controls and the existence of the Information Security Policy in the 118 organizations (hospitals surveyed). Another research could be the investigation of the organizations pointed out by the TCU as organizations which do not comply -do not have- an Information Security Policy. The investigation question could involve the following: after the security policy has been enforced by organizations mentioned by the TCU would they implement the policies? We understand the implementation of an Information Security Policy as well its respective operational controls, are a vast research field, which could indicate how the organizations behave regarding their security and policies issues.

CONCLUSION

The development of the information security policy for the organization has too much to be researched when it comes to contemplate the controls of the process of information security.
The Family norms ISO/IEC 27000 are dedicated to the topic of information security controls and present this very well. The difficulty occurs when the information security professional intends to transform the concept of information security policy for the organization. How to divide the elements? How to separate the granularity of the guidelines? What issues should be considered in each regulations block?
To these questions there is not a single truth. The structure presented here is a solution to facilitate the development and implementation of the Political Dimension of Information Security -figure 2-.

The approach of "how to do" is little explored, and consequently little publicized. But, it is believed that the more this topic is explained, the more experiences are gathered. All this with the aim of ensuring the organization has an effective security policy; i.e.; effective, efficient and over time.

REFERENCES

ABNT, (2006). ABNT-*NBR ISO/IEC 27001 Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de segurança da informação – Requisitos.* Rio de Janeiro: Associação Brasileira de Normas Técnicas.
______, (2005). *NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação.* Rio de Janeiro: Associação Brasileira de Normas Técnicas.

Albertin, A. L.; Pinochet, L.H.C. (2010). *Política de Segurança de Informações, página 275*. Rio de Janeiro: Elsevier Editora.

Balloni, A.J. (2006); Por que GESITI? - Por que gestão em Sistemas e Tecnologias de Informação -. São Paulo: Editora Komedi, - page 23. Retrieved October 15, 2013, from < https://www.cti.gov.br/pt-br/dtsd/gesiti/livros-gesiti >

Balloni, A.J. (2004). Why Management in System and Information Technology? In Virtual Enterprises and Collaborative Networks, IFIP/ V.149 (pp. 291-300). Springer Publisher. Retrieved October 15, 2013, from < https://goo.gl/S4ZNMn >

Balloni, A. J., Azevedo, A. M. M., & Silveira, M. A. (2012). Socio-technical management model for governance of an ecosystem. *International Journal of Managing Information Technology (IJMIT)*. Retrieved October 15, 2013, from < http://airccse.org/journal/ijmit/papers/4312ijmit01.pdf >

Balloni, A. J., Holtz, S.V..(2008). Aspectos sociotécnicos das TI & Relacionamento Humano & Sinergia . Revista Iérica de Sistemas e Tecnologias de Informação (RISTI) - Retrieved October 15, 2013, from < https://goo.gl/Mt5Yuy >

Barman, S. (2002). *Writing Information Security Polices, page 4*. Indianapolis: New Riders.

DSIC. (2009). *Diretrizes para elaboração de política de segurança da informação e comunicações nos órgão e entidades da administração pública federal. 03/IN01/DSIC/GSIPR*. Brasília: Gabinete de Segurança Institucional da Presidência da República. Retrieved June 6, 2014, from <http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf>

_____. (2008). *Metodologia de gestão de segurança da informação e comunicações. 02/IN01/DSIC/GSIPR.* Brasília: Gabinete de Segurança Institucional da Presidência da República. Retrieved June 6, 2014, from <http://dsic.planalto.gov.br/documentos/nc_2_metodologia.pdf>

Caruso, C.; Steffen, F. D. (1999). *Segurança em Informática e de Informações, página 49*. São Paulo: Editora SENAC.

Chiavenatto, I. (2010). *Administração – Teoria, Processo e Prática, página 173*. Rio de Janeiro: Elsevier Editora.

Dartmouth (2008). The PDCA Cycle. *Dartmouth Medical School - Office of Community-Based Education and Research - The Clinician's Black Bag of Quality Improvement Tools.* Retrieved October 15, 2013, from <http://www.aha.org/advocacy-issues/workforce/nww/nww-res-s5c.pdf>

Fontes, E. (2008). *Praticando a segurança da informação*. Rio de Janeiro, Editora Brasport.

Fontes, E. (2012). *Políticas e normas para a segurança da informação*. Rio de Janeiro, Editora Brasport,

Fontes, E.L.G & Balloni, A.J. (2007). Security In Information Systems: Sociotechnical Aspects. In Innovations and Advanced Techniques in Computer and Information Sciences and Engineering (pp. 163-166). Springer Publisher. Retrieved October 15, 2013, from < https://goo.gl/rHDs4p >

GESITI (2013). Management of System and Information Technology in Hospitals (GESITI). CTI Renato Acher – Campinas/SP – Brasil
a) - Balloni, Antonio José; Levy, Sylvain Nahum; Nemer, Gleide Isaac Costa Tanios;
Freire, Júlio Márcio Barreto; Júnior, José C. Leão; Pereira, Delton Assis & Monteiro, Bruno Luis Freitas. (2014). *Por que GESITI?: Gestão de Sistemas e Tecnologias da Informação em Hospitais: panorama, tendências e perspectivas em saúde.* Location: Brasília, Brasil. Publisher: Ministério da Saúde, Brasil. Retrieved June 06, 2014,from <bvsms.saude.gov.br/bvs/publicacoes/por_que_gesiti_gestao_sistemas.pdf > or < https://www.cti.gov.br/pt-br/dtsd/gesiti/livros-gesiti >

a) - Technical Scientific Reports from GESITI Health Project available at:
< https://www.cti.gov.br/pt-br/dtsd/gesiti-hospitalar/relatorios-tecnicos-cientificos >
Last access: March 2014.

MORAES, Ilara Hämmerli Sozzi de; GOMEZ, Maria Nélida (2007). de. Informação e informática em saúde: caleidoscópio contemporâneo da saúde. *Ciênc. saúde coletiva*. *12*(3), 553-565.

PELTIER, Thomas (2005). Information Security Fundamentals. USA: Auerbach, pag 17.

_______________ (2004). Information Security Policies and Procedures. USA: Auerbach, pag. 47.

PICOVSKY, José. Análise de Gestão de Riscos e Impactos da Tecnologia da Informação nos Negócios Hospitalares. XIII – Congresso de Informática na Saúde, São Paulo (2012: 12-63).

PRICEWATERHOUSECOOPERS. Pesquisa Global de Segurança da Informação 2011. São Paulo: PricewaterhouseCoopers, 2011.

PRICEWATERHOUSECOOPERS. Pesquisa Global de Segurança da Informação 2013. São Paulo: PricewaterhouseCoopers, 2011.

Saulo Barbará de Oliveira, Antonio José Balloni, Felipe Nogueira Barbará de Oliveira, Favio Akiyoshi Toda (2012). Information and Service-Oriented Architecture & Web Services: Enabling Integration and Organizational Agility. *Procedia Technology, 5,* 141–151. Retrieved October 15, 2013, from <www.sciencedirect.com/science/article/pii/S2212017312004471/pdf?md5=b48d7661a085ad66831c483e5e6c629c&pid=1-s2.0-S2212017312004471-main.pdf>

Vianez, M. S.; Segobia, R.H.; Camargo, V. (2008). Segurança de Informação: Aderência à Norma ABNT NBR ISO/IEC N. 17.799:2005. *Revista de Informática Aplicada (Journal of Applied Computing), Vol. IV - Nº 01 - Jan/Jun, São Caetano do Sul: USCS.*

TERRA, J. C.; BAX, M. P. (2003). Portais corporativos: instrumento de gestão de informação e de conhecimento. In: Isis Paim. (Org.). A Gestão da Informação e do Conhecimento. 1 ed. Belo Horizonte, p. 33-53.

TCU. (2007). Tribunal de Contas da União, Manual de Boas Práticas em Segurança da Informação, Brasília, p.27-28.

TCU. (2010). Tribunal de Contas da União, Levantamento de Governança de TI, 2010, Brasília, p.17-18.

TCU. (2012). Tribunal de Contas da União. *Boas práticas em segurança da informação.* Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação.

KEY TERMS & DEFINITIONS

User: it is the person who uses the information both in the digital environment as in conventional environment.
Manager´s User: it is a person, usually the headmaster, which has the responsibility to indicate that the user, which performs tasks in the organization, is a real person.
Information Confidentiality Level: indicates the kind of handling which must be given to the information regarding the possibility of accessing it. We may have a more rigid or less rigid handling of information in relation to the possibility of its access. For example, information classified as public does not need be destroyed after its use. Otherwise, confidential information must be handled carefully and, sometimes must be destroyed in such a way that may not be recovered.
Information Manager: it is the person who authorizes or denies the information access. This authorization or denial is an assessment function that the manager makes regarding the need of accessing that information.
Information Resource: they are elements that store, process, transmit or deal with the information. These elements could be technological discs, tapes and equipment or could even include the environment such as: conventional paper or our minds.
Information Security Process: it is the organizational process which aims to allow and enable organizations reach their objectives regarding the correct use of information and information resources.
Digital Environment: it is the environment that uses technology to represent the information in digital format. The information is stored in an Information Resource and is available for retrieval through information technology hardware and software.
Contingency Situations: are situations that make an information (or other resource) unavailable. Such situations may be concerned with the nature (rain, lightning, and earthquake) or by human action (theft, outrage, error).
Conventional Environment: it is the physical environment. The information in this conventional environment is available in several situations such as: in a piece of paper, written in table, and chalkboard or in other physical media

Backup Copy: it is a copy of information (audio, video and data) which can be used for restoring the original information when it has been lost or destroyed.

BAM -Business Activity Monitoring: it is a tool that provides real time access to the critical indicators of business performance, improving the business operations in a more efficient and effective way.
Depending on the business and from the BAM applications, these events can vary from
sweeping a bar code, up to an Information Security System threat (ISS -Figure 1 and item d, page 4-), and then correlating these events with relevant data inside a context or organizational environment.