International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:13, No:7, 2019

Information Security Risk Management in IT-Based Process Virtualization: A Methodological Design Based on Action Research

Jefferson Camacho Mejía, Jenny Paola Forero Pachón, Luis Carlos Gómez Flórez

***Abstract*—**Action research is a qualitative research methodology, which leads the researcher to delve into the problems of a community in order to understand its needs in depth and finally, to propose actions that lead to a change of social paradigm. Although this methodology had its beginnings in the human sciences, it has attracted increasing interest and acceptance in the field of information systems research since the 1990s. The countless possibilities offered nowadays by the use of Information Technologies (IT) in the development of different socio-economic activities have meant a change of social paradigm and the emergence of the so-called information and knowledge society. According to this, governments, large corporations, small entrepreneurs and in general, organizations of all kinds are using IT to virtualize their processes, taking them from the physical environment to the digital environment. However, there is a potential risk for organizations related with exposing valuable information without an appropriate framework for protecting it. This paper shows progress in the development of a methodological design to manage the information security risks associated with the IT-based processes virtualization, by applying the principles of the action research methodology and it is the result of a systematic review of the scientific literature. This design consists of seven fundamental stages. These are distributed in the three stages described in the action research methodology: 1) Observe, 2) Analyze and 3) Take actions. Finally, this paper aims to offer an alternative tool to traditional information security management methodologies with a view to being applied specifically in the planning stage of IT-based process virtualization in order to foresee risks and to establish security controls before formulating IT solutions in any type of organization.

***Keywords*—**Action research, information security, information technology, methodological design, process virtualization, risk management.

I. Introduction

RESEARCH, understood as a set of systematic, critical and empirical processes that are applied to the study of a phenomenon or problem [1], can be classified according to the method used: quantitative methods originating in the natural sciences to study natural phenomena and qualitative methods originating in the social sciences enabling Qualitative research methods are designed to help researchers understand the people and the social and cultural contexts in which they live [2]. In these studies, the hypothesis takes on a different role from that of quantitative research, as they are rarely established before entering the environment and beginning data collection [1]. For several decades, qualitative research has been ignored and minimized by the scientific community, but today it has gained prestige and recognition in the academic world [3]. This paper shows progress in the development of a methodological design based on the principles of action research for the management of information security risks in the virtualization of IT-based processes.

C. M. Jefferson and F. P. Jenny P., master students, systems and informatics department, Universidad Industrial de Santander, Bucaramanga, SA 680002 Colombia (e-mail: jefferson.camacho@correo.uis.edu.co, jenny2178186@correo.uis.edu.co).

G. F. Luis C., titular professor, systems and informatics department, Universidad Industrial de Santander, Bucaramanga, SA 680002 Colombia (phone: +573164650312; e-mail: lcgomezf@uis.edu.co).

II. Virtualization of Processes Based on IT

Generally speaking, according to the terminology presented by the IEEE, a process is a set of interrelated activities of steps that are followed to achieve an objective [4]. Unlike a physical process, in which physical interaction between people and/or between people and objects occurs, in a virtual process, physical interaction is eliminated, that is, the objective pursued by the process is achieved without interaction between people and/or between people and objects [5].

There are some characteristics of IT that can influence the development of processes and in this way can achieve the virtualization of them. Thus, Overby proposes a conceptual model with dependent variables (process characteristics) and independent variables (IT characteristics) to achieve process virtualizability [5] by defining four constructs that affect the virtualizability of a process:

1. Sensory requirements
2. Relationship requirements
3. Synchronization requirements
4. Identification and control requirements

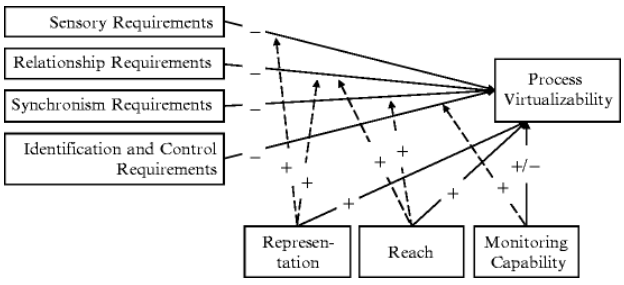

Fig. 1 Constructs and relationships proposed in the Theory of Process Virtualization

These constructs affect whether the process is subject to being performed virtually or whether it resists this. Also, there are characteristics of IT that influence the constructs mentioned above, such as the representation, scope, and monitoring capacity. These characteristics positively moderate the four main constructs. Fig. 1 shows graphically how these variables are related and their impact on the virtualizability of the process presented in [17].

A. Dependent Variables: The dependent variables represent the characteristics of the processes; these are sensory requirements, relationship requirements, synchronization requirements and identification and control requirements. Each of these proposed ideas aims to maintain a negative effect on the virtualizability of the process. In other words, as each requirement increases, the process becomes less suitable for virtualization [6].

a. Sensory requirements: Refers to the need for process participants to be able to enjoy a complete sensory experience of the process, other participants and the objects, for example, excited, vulnerable, etc.

b. Relationship requirements: Refers to the need for participants in the process to interact with others in a social or professional context. Interactions can lead to the acquisition of knowledge, trust, development of friendship.

c. Synchronization requirements: Refers to the degree to which the activities that make up the process need to occur quickly with minimal delay. Processes should be carefully analyzed to ensure that they are carried out synchronously or asynchronously, or both in some cases.

d. Identification and Control Requirements: Refers to the degree to which process participants require: (a) the identification of other participants in the process, and (b) the ability to exercise control over the behavior of those participants.

B. Independent variables: The independent variables that represent the characteristics of the virtualization mechanisms are Representation, Scope and Monitoring Capability. These variables are characteristics of IT that influence the characteristics of the process. The representation and scope are intended to maintain a positive effect on the virtualizability of the process, while the effect of the monitoring capability is ambiguous and depends on the process under investigation. In addition to the main effects, each of these ideas has a moderating effect on the relationship between the characteristic variables of the process and the virtualizability process [6].

a. Representation: Refers to the ability of IT to present information relevant to the process, including simulations of actors and objects in the physical world, their properties and characteristics, and how we interact with them. For example, representations can satisfy many sensory requirements such as sight and sound (and to a lesser extent, touch, taste and smell) when replicated with IT-based virtual processes [7].

b. Scope: Is the ability of IT to allow participation in the process in space and time [8]. The scope allows for flexible participation in processes around the world.

c. Monitoring Capability: Is the ability of IT to authenticate process participants and track activity [9]. Authentication systems such as ID/password combinations, digital certificates, and biometric devices capture who is participating in a process, and associated database entries capture what these participants do and when they do it.

III. Information Security Risk Management

According to international standard ISO/IEC 17999:2005 information is an asset that, like other important assets, is essential to an organization's business and therefore needs to be properly protected [10], so concern for information security has grown year after year and aims to protect information contained in information systems and, in this way prevent any unauthorized access, use, disclosure, interruption or destruction of information [11], by implementing a set of controls defined through a risk management process and, based on the preservation of three fundamental dimensions, confidentiality, availability and integrity of information [12]. Before studying the risk management process, it is advisable to define risk as the measure of the damage that could be caused by the occurrence of a dangerous event. Additionally, a risk could be defined as a function of two variables, threat, and vulnerability. The first is related with weakness in technology or information-related processes and the second one with events that, if they do occur, could directly affect the information or the systems that process it and disturb the normal development of activities in an organization. As risk is directly proportional to these two factors, it can be considered a dependent or dynamic variable, since it increases or decreases as both factors or one of them varies [13].

According to [14], the risk management process comprises two main steps, the analysis, and treatment of risks.

A. Risk analysis: It is a process of understanding the nature of risk and determining the level of risk, which provides the fundamental basis for making decisions regarding the treatment of risk [12]. Likewise, [14] defines it as a methodical approach to determining risk by following a set number of steps:

a. Determine the relevant assets for the Organization, their interrelationship and their value, in the sense of what damage (cost) their degradation would entail.

b. Determine what threats those assets are exposed to.

c. Determine what safeguards are in place and how effective they are against risk.

d. Estimate the impact, defined as the damage to the asset resulting from the materialization of the threat.

e. Estimate the risk, defined as the impact weighted with the rate of occurrence (or expectation of materialization) of the hazard.

B. Risk treatment: Once the risk analysis is completed, it must be clear what is to be protected and from which it is to be protected, that is to say, which are the information assets to be protected and which are the threats from which it is to be protected, in this way, a series of

decisions are made which are conditioned by various factors such as [14]:

a. The severity of the impact and/or risk.
b. The obligations to which the Organization is subject by law.
c. The obligations to which the Organization is subject by sectoral regulations.
d. The obligations to which the Organization is subject by contract.

To define the treatment to be given to risks, they are classified into four categories according to their impact [12].

a. **Critical** in that it requires urgent attention.
b. **Serious** in the sense that it requires attention.
c. **Appreciable** in the sense that it can be studied for treatment.
d. **Assumable** in the sense that no action will be taken to tackle it.

Fig. 2 shows the stages that are commonly part of a risk management process presented in [14].

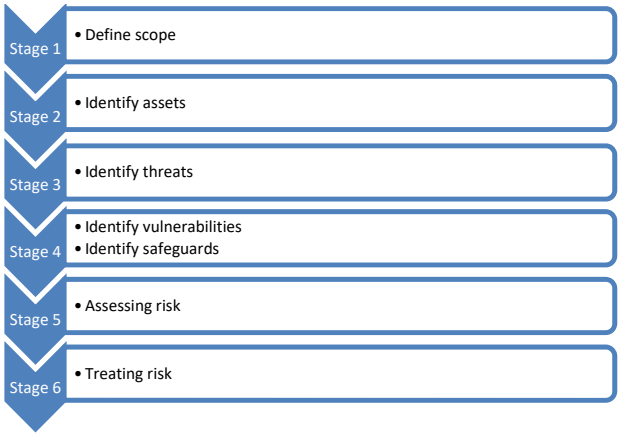

Fig. 2 Risk management process

IV. Action Research

Action research is concerned with finding solutions to everyday problems and improving specific practices. Its main purpose is to provide information to guide decision-making for programs, processes and structural reforms [15], permanently involving the actors of the context under study.

Although action research has been accepted as a valid research method in different areas of knowledge in information systems, it has long been ignored. However, in recent years, this research design has attracted interest and acceptance in the field of information systems research [2]. According to [16], action research consists of three fundamental stages: Observe, analyze and act. Reference [1] defines these three stages as follows:

Stage 1. The technical-scientific vision (observe): This first stage focuses on getting to know the nature of the problem situation in depth and carrying out an immersion in the context or environment, to understand what events occur and how they happen, to achieve clarity about the specific problem and the people who are linked to it. Once the conceptual clarity of the research problem and the problem to be addressed through the immersion is achieved, data are collected on it, where it is suggested to interview key actors, observing sites in the environment, events, and activities related to the problem. The data collected are then analyzed, for which there are various support tools such as concept maps, cause-effect diagrams, among others. After the data have been analyzed, a report is prepared with the diagnosis of the problem, which is presented to the participants to aggregate data, validate information and confirm findings.

Stage 2. The deliberative vision (analyze): In this stage, the development of the plan to implement solutions or introduce change or innovation is carried out. During the development of the plan, the researcher remains open to collect more data and information that can be associated with the problem statement and its resolution. The plan should incorporate practical solutions for this or generate change and establish how to assess success in its implementation.

Stage 3. The emancipatory vision (act): In this stage, the plan is implemented; however, this depends on the specific circumstances of each study and problem. Throughout its implementation, the researcher's task is extremely proactive, informing participants about the activities carried out by others, motivating people so that the plan is executed as expected and each person expresses their best efforts and assists them when they have difficulties. During this stage, the researcher continuously collects data to evaluate each task performed and the development of the implementation.

V. Information Security Management Applying Research Principles Action

Generally, the information security management process is conceived as an engineering task within an organization, guided by rigid standards and/or methodologies pre-designed for this purpose, however, when the organization is not clearly defined since it is composed of actors of different nature and their roles are not formally defined, it is difficult to predict the risks that may arise when virtualizing an IT-based process. The methodological design proposed in this paper (Fig. 3) is based on the risk management process presented in Fig. 2 and consists of nine stages organized in each of the three stages of action research: observe, analyze and act.

In this design, the literature review stage is added to the information security management process presented by Magerit v3.0. At this stage, the researcher deepens his or her knowledge of the context to be studied and the particularities of the processes and roles of its actors. The rest of the information security management process obeys the one proposed in Magerit v3.0, however, the position of the executor obeys that of a researcher, who must propose to become part of the problem situation, making an immersion in the studied community and identifying its needs, fears and resistance to change, in order to carry out the information security management process in an open and participative way, according to what was proposed in the action research.

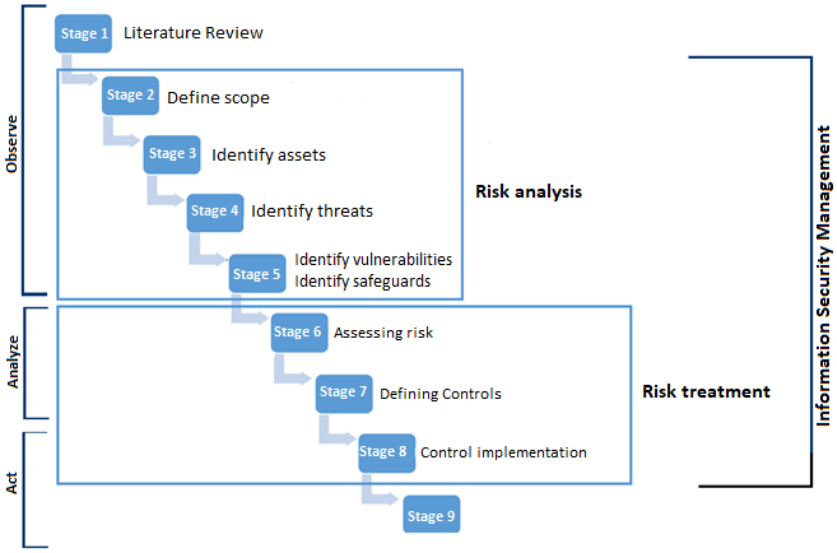

Fig. 3 Proposed methodological design (Adapting Magerit's IT security management process to action research)

REFERENCES

[1] Hernández, R., Fernández, C., Baptista, M. (6Ed.). (2014). Metodología de la investigación. México DF, México: McGraw-Hill
[2] Myers, M. D. "Qualitative Research in Information Systems," MIS Quarterly (21:2), June 1997, pp. 241-242. MISQ Discovery, archival version, June 1997, http://www.misq.org/supplements/ Association for Information Systems (AISWorld) Section on Qualitative Research in Information Systems, updated version, last modified: September 15, 2017, www.qual.auckland.ac.nz.
[3] A.C. Salgado, "Quality investigation, designs, evaluation of the methodological strictness and challenges", *Liberabit,* vol. 13, no. 14
[4] ISO/IEC/IEEE 24765, (2010). "Systems and software engineering — Vocabulary".
[5] Overby, E. (2008). Process Virtualization Theory and the Impact of Information.
[6] Dwivedi, Y., Wade, M. and Schneberger, S. (2012). Information Systems Theory. New York, NY: Springer New York, pp.107-124
[7] J Steuer, J. (1992). Defining virtual reality: Dimensions determining telepresence. The Journal of Communication, 42(4), 73–93.
[8] Broadbent, M., Weill, P., Clair, D. S., & Kearney, A. T. (1999). The implications of information technology infrastructure for business process redesign. Management Information Systems Quarterly, 23(2), 159–182
[9] Zuboff, S. (1988). In the age of the smart machine: The future of work and power. New York: Basic Books.
[10] ISO. (2005). ISO/IEC 17799:2005 (E) Information technology - Security techniques - Code of practice for information security management. International Organization for Standardization and International Electrotechnical Commission.
[11] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Manual para la Estrategia de Gobierno en Línea. (En Línea). Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf
[12] ISO. (2016). ISO/IEC 27000:2016 (E) Information technology - Security techniques - Information security management systems - Overview and vocabulary. International Organization for Standardization and International Electrotechnical Commission.
[13] Organización de las Naciones Unidas. (2011). Manual de gestión de riesgos de desastre para comunicadores sociales. (En Línea). Disponible en: http://unesdoc.unesco.org/images/0021/002191/219184s.pdf
[14] Ministerio de hacienda y administraciones públicas de España. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. (En Línea). Disponible en: https://www.ccncert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.htm
[15] Salgado Lévano, Ana Cecilia. (2007). Investigación cualitativa: diseños, evaluación del rigor metodológico y retos. Liberabit, 13(13), 71-78.
[16] Stringer, E. T. (1999). Action Research (2nd ed.). Thousand Oaks, CA: Sage
[17] Dwivedi, Y., Wade, M. and schneberger, S. (2012). "Information System Theory"