© International Journal of Combinatorial Optimization Problems and Informatics, Vol. 5, No. 1, Jan-April 2014, pp. 2-14. ISSN: 2007-1558.

Soft Systems Methodology for the Strategic Planning of the Enterprise Computer Security

Ocotlán Díaz-Parra[1], Jorge A. Ruiz-Vanoye[2], Ricardo A. Barrera-Cámara[1], Alejandro Fuentes-Penna, Natalia Sandoval[1]
[1] Universidad Autónoma del Carmen
ocotlan@diazparra.net

Abstract. Soft Systems Methodology (SSM) is a problem-solving methodology employing systems thinking. SSM has been applied to the management, planning, health and medical systems, information systems planning, human resource management, analysis of the logistics systems, knowledge management, project management, construction management and engineering, and development of expert systems. This paper proposes using SSM for strategic planning of Enterprise Computer Security.

Keywords. Soft Systems Methodology, CATWOE, Computer Security, Strategic Planning.

Introduction

There are several categories of complexity of problems in the world, as well as methods and methodologies to solve them. Problems vary between two extremes [1]:

- Hard Problems. These are those situations where the "¿what?" (This is the problem) and the ¿how? (As they solve the problem) are clearly defined. Some examples of problems can be hard, maximize corporate profits, minimize the cost of production of the company, change the tire on my car, prepare a chocolate cake, and construct a building, among others. Some methodologies related to hard problems are systems theory, operations research, decision theory and systems analysis, among others.
- Soft Problems. These are those situations where the "¿what?" (This is the problem) it is very difficult to define and the "¿how?" (As they solve the problem) is difficult to solve. Some examples of problems can be soft, to define the business mission, to solve the problem of poverty in a country, implement a quality program in a company to develop an information system for decision making, implementing a strategic change in the company, among others. A methodology related problems is Soft Systems Methodology (SSM).

The Soft Systems Methodology was created by Peter Checkland and colleagues at the University of Lancaster in the 1970s [1]. SSM was designed to deal with a situation where the people in a problematic situation perceive and interpret the world in their own way and make judgments about what they use standards and values that cannot be shared by others or where solutions need practices such as organizational management and policy where stakeholders dealing with the confusion of the context of the situation and analysis of the focus is on ensuring that the process of inquiry into real-world complexity is itself a system for learning [2]. It is applicable to various domains such as administration, planning of medical and health systems, planning of information systems, human resources management, analysis of logistics systems, knowledge management, project management, construction and engineering management, development of expert system.

SSM is a methodology that allows support and structure the thinking and intervention on the complex organizational problems [1]. The advantages of the methodology of Checkland are that makes easier to structure problem situations of complex organizations and forces the user to not act rigidly and just technically, it is a mandatory tool to be used if they are very complex problems, and it allows to use specific techniques for solving problems.

Received Nov 20, 2013 / Accepted Dec 19, 2013

SSM consists of seven stages, the order may vary in accordance with the characteristics of what we want to study [5]:

1. Unstructured problematic situation.
2. To express the problem situation.
3. Definitions significant of the root system (containing the methodology or tool called CATWOE).
4. Conceptual models.
5. Comparison of the conceptual model with the expression of the problem situation.
6. Identification of feasible and desirable changes.
7. Actions to improve the system.

This paper proposes to use Soft Systems Methodology for strategic planning of Enterprise Computer Security, specifically the methodology called CATWOE. Section 2 is the related works, section 3 describes the CATWOE methodology for Strategic Planning of the Enterprise Computer Security, in section 4 the CATWOE methodology is applied to a Mexican company, and finally is shown the conclusions of the research.

Related Works

The use of SSM and CATWOE tool (Customers, Actors, Transformation, Weltanschauung: German expression for the views of the world, Owner, Environment Constraints in where system activity is performed), addresses problematic of life through a systemic approach. Some work are associated with public Healthcare, transformation processes of the organizations, quality, software development, social responsibility, education, public safety, and proposals for new situations.

The delimitation of territories and aspects related are analyzed using conceptual approaches of soft systems and complex adaptive systems, allowing describe relations of the territories and organizations [3].

Macías-Chapula [4] design a model for the transfer of research results in the public health care system in Honduras. He models six definitions of the problem: Research and Development System in Honduras; system that organizes and manages the knowledge generated; system that helps public health professionals to access sources of scientific information and use of the knowledge; translation system of scientific knowledge to non-technical health workers; system that helps people without access to information and knowledge about the results of research to acquire them; systems for the population to participate in the identification of health problems and promote solutions. Identifies four actors: researchers, information professionals and documentation, health professionals and the public.

Arriola-Arciniega and Aceves [6] developed software for visually impaired people to pretend to study mathematics in engineering careers, apply the CATWOE model for the agents involved in the implementation.

Martínez and Rios [7] developed a management information system for the oriente University of Venezuela, the system is based on Soft System and UML to enhance the activities of the subcommittee.

Carrillo et al. [8] present a system for the training of personnel for operation of transmission substations of electrical energy. They assume the improvement as from learning and from which proposes the conceptualization of the situation of interest, the conceptual modeling of the system and the functional specification of support technology.

Córdoba and Campbell [9] considered that the social responsibility of enterprise must meet the needs of society, for it combines systems thinking, soft systems methodologies and critical systems heuristics.

Osorio Fonseca and Huacuja [10] propose the implementation of information systems in the management of quality by soft systems methodology, forcing the user to find comprehensive solutions and not only techniques that cover all organizational aspects.

Coelho et al. [11] mentioned that the use of CATWOE allowed formulating the preliminary vision and a set of indicators to assess, guide and monitor a postgraduate program in management.

Watson [12] presents situations that have not been addressed by the SSM, such as simulation, virtual reality, ubiquitous computing, the design of cities, service management and information architectures in enterprises and territorial boundaries.

Rodriguez-Ulloa and others [13] used the combination of system dynamics and soft systems methodology, to form the soft systems dynamics methodology to problems public insecurity of the province of Argentina.

Al-Zhrani [14] mentions that the Soft Systems Methodology has attracted much attention in industry and academia. The focus of the research is to demonstrate the application of SSM to problems and obstacles faced by Saudi government institutions using Information Technology. This was the first attempt to use SSM to address IT issues in Saudi Arabia.

Diaz-Parra et al. [15] applied the methodology of SSM in combination with deployment of the quality function for the analysis of an NP-complete problem.

Martínez-Rangel et al. [16] present a method for the identification of critical processes and variables involved in the problem of scheduling of resources for machining parts used in the assembly of reciprocating compressors in a manufacturing company, they used the methodologies of Checkland and IDEFO for a combinatorial optimization problem.

Ruiz-Vanoye et al. [17] propose the use of the strategic management techniques to provide computer security for financial institutions and government companies.

Barros de Deus e Mello et al. [18] propose a way of administration of the Occupational Safety and Health (OSH) for the electric sector of a company, the presentation of relevant information that can be used by any organization for the development and implementation of an Occupational Health and Safety Management System (OHSMS) using soft systems methodology. The implementation of the OHSMS model provides significant improvements in the working environment of the company.

Mehregan et al. [19] propose to use SSM to solve the University TimeTable Scheduling Problem, as well as generate the list of courses of the Faculty of Management at the University of Tehran.

Small and Wainwright [20] propose to use Soft Operations Research (soft OR) to iteratively develop a framework that encompasses structuring problem through technology choice and adoption based on the combination of SSM for structuring and operation of problem, learning theories and methods for problem diagnosis and management of technology to select between alternatives and implement the solution.

This paper proposes to apply the SSM and CATWOE tool (Customers, Actors, Transformation, Weltanschauung: German expression for the views of the world, Owner, Environment Constraints in where system activity is performed) for strategic planning of Enterprise Computer Security.

Soft Systems Methodology for the Strategic Planning of Enterprise Computer Security

The use of strategic planning in computer security issues is an excellent mechanism to manage security issues in any organization. One way to strengthen the strategic planning for enterprise computer security is by applying CATWOE contained in the Soft Systems Methodology of Checkland.

The process CATWOE (Customers, Actors, Transformation, Weltanschauung: German expression for the views of the world, Owner, Environment Constraints in where system activity is performed) for strategic planning of corporate computer security consists of the following steps:

Step 1. Identification of the beneficiaries or customers (internal or external) affected by the lack of enterprise computer security. If errors in computer security involve costs for the company and therefore layoffs then be regarded as customers.

Step 2. Identify the actors that perform activities related to enterprise security.

Step 3. Perform the task of transformation, which is described by the type of work related to enterprise computer security. It is necessary to collect information on the functioning of the enterprise by pointed questions of security aspects of enterprise.

Step 4. Identify input and output of the processes of enterprise information security.

Step 5. Identify points of interest and reframe the questions to get more specific information, tips of the users and staff working in the enterprise for the issue of enterprise computer security.

Step 6. Determine its owner or proprietor can make important decisions on computer security.

Step 7. Conduct interviews with staff concerning computer security needs and availability of time as well as suggestions for improving the aspects of computer security.

Step 8. Perform CATWOE scheme for enterprise computer security. The scheme should contain actors, customers, transformation, worldview, owner and environment. And it must be supported by the IEEE 17799 standard.

Results and Discussion

In this section apply the CATWOE methodology for computer security of a Mexican publishing company applies. The Mexican Publisher (pseudonym of the original name of the company) is engaged in peer review of original research, editing journals, books, conference proceedings and theses in English and Spanish. Mexican Publisher is a service provider for all people who need:

1.-Editing journals and other periodical publications integrated printing.

2.-Print books, newspapers and journals under contract.

3.-Publishing of books integrated printing.

4.-Other scientific and technical consulting.

5.-Translation and interpretation of articles and books.

6.-Scientific and technological research activities enrolled in the Mexican National Register of Scientific and Technological Institutions and Enterprises.

The Mexican publisher rent services in the cloud (cloud Computing) of a company in the United States. The technology services supplier of the cloud services provides initial server configuration (operating systems, reception systems journal articles, etc.), monitoring systems, server, network, and any service that is in the server including databases, web servers, monitoring pings, HTTP monitoring, site update, Backup and Recovery hourly, monthly security scanning, corrective actions to security problems, install patches and updates all Wednesday at 11:00 pm. The company servers of the cloud include Linux CentOS 64-Bit, Intel ® Core ™ i7 - 4 cores, 16 GB RAM, 2 x 2 TB Storage HDD, 20 TB each month of bandwidth.

The results of applying CATWOE for the strategic planning of enterprise computer security to the Mexican publisher are:

Step 1. Identification of the beneficiaries or customers (internal or external) affected by the lack of enterprise computer security. If errors in computer security involve costs for the company and therefore layoffs then be regarded as customers. Customers of the company in question are: Researchers, Professors, undergraduate and postgraduate students.

Step 2. Identify the actors that perform activities related to enterprise security. Actors of the company are: Data Center Manager and the technical support group.

Step 3. Perform the task of transformation, which is described by the type of work related to enterprise computer security. It is necessary to collect information on the functioning of the enterprise by pointed questions of security aspects of enterprise. Some questions used are:

1. ¿Have the computers data stored of the company on the hard drive? Yes, no, do not know

2. ¿Do you realize backups of company data? Yes, no, do not know

3. ¿How often you perform a backup? Daily, Weekly, Other.

4. ¿Do you have a backup device (CD / DVD / consolidated storage, cloud, other) out of the company? Yes, no, do not know

5. ¿Is performed maintenance to the company backups? Yes, no, do not know.

Various topics related to computer security business were used:

a) Firewalls: determine which data packets are allowed on a network, and restricting access to specific resources.

b) Intrusion Detection: An intrusion detection system (IDS) detects security breaches by searching for anomalies in normal activities, looking for patterns of activity that are associated with intrusions or misuse of privileged information, or both.

c) Audit: Install and configure mechanisms to record activities occurring through networking, including application processes and user activities.

d) Identification and Authentication: Identification and authentication is used to prevent unauthorized personnel from entering an IT system.

e) logical access controls: logical access controls are mechanisms used to designate the users who have access to system resources and the types of transactions and functions that are allowed to perform.

f) Virus detection. The data and information moving from one IT system to another must be analyzed with your antivirus software to detect and eliminate malicious code such as viruses, worms and Trojan horses.

g) Encryption: Encryption is used to ensure that the data cannot be reading or modified by unauthorized users.

h) Physical and environmental security: physical security addresses the physical protection of hardware and software.

i) Denial of Service (DoS). An attack that prevents or impairs the authorized networks, systems, or applications by exhausting resources.

j) The malicious code. Viruses, worms, Trojan horses or other malicious entity based infects a host code successfully.

k) The unauthorized access. A person obtains physical or logical access without permission to a network, system, application, data, or other IT resources.

l) Incorrect use. One who breaks the acceptable use of any network or security policies.

m) multiple components. A single incident that encompasses two or more incidents, for example, a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts access.

Step 4. Identify input and output of the processes of enterprise information security.

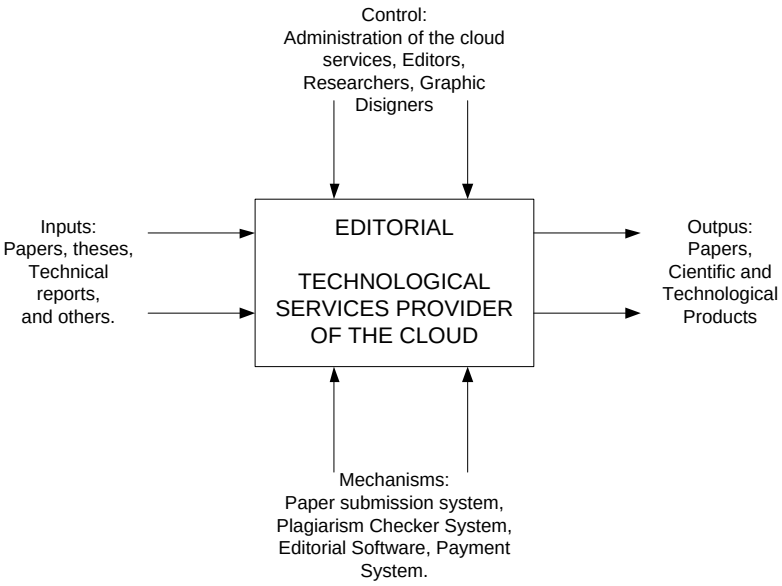

Fig. 1. IDEF0 of Inputs and Output

Step 5. Identify points of interest and reframe the questions to get more specific information, tips of the users and staff working in the enterprise for the issue of enterprise computer security. To obtain more information on the staff working in the company was necessary to address the issues of:

a) Access Control (policies and procedures, account management, access to the application, information about the application flow, separation of duties, least privilege, failed login attempts, use notification system, start notification of previous session, concurrent session control, session locking session termination, supervision and review of access control, allowed actions without identification or authentication, automatic dialing, automatic labeling, remote access, wireless access restrictions, access control for laptops and mobile devices, the use of external information systems).

b) Security awareness and training (Awareness security, political training and safety procedures, safety training records, contacts with security groups and associations).

c) Audit and accountability (policy and procedures of the audit and accountability, auditable events, the content of audit records, audit storage capacity, response to audit processing failures, monitoring, audit generation, analysis and reporting, reduced report audit, the time stamps, auditing the security information, non-repudiation, recordkeeping audit).

d) Certification, accreditation and safety assessment (certification, accreditation of the security, policies and procedures assessment, safety assessments, connections, certification of the information system security, action plan goals, security accreditation, continuous control).

e) Configuration Management (policy and procedures of the configuration management, the base configuration, configuration control, monitor configuration of the changes, change access, restrictions for changes, configuration settings, inventory of the information system component).

f) Contingency planning (policy and procedures of the contingency planning, contingency plan, contingency training, contingency plans, tests and exercises, updating the contingency plan, storage, alternate processing site, telecommunications, information in alternate system, backup, recovery and reconstitution system information).

g) Identification and authentication (policy and procedures of the identification and authentication, identification and authentication of users, devices, identification and authentication, authenticator identifier management, management, feedback authenticator, the authentication cryptographic module).

h) Incident Response (policy and procedures of the incident response, incident response training, testing and exercises, incident management, incident tracking, incident reporting, incident response assistance).

i) Maintenance (policy and procedures of the system maintenance, controlled maintenance, maintenance tools, remote maintenance, Maintenance Staff, timely maintenance).

j) Protection (protection policy to the media and procedures, access to media, media labeling, media storage, transportation, disposal and disinfectants).

k) Physical and environmental protection (policy and procedures of the physical environmental protection, physical access authorization, access control, access control to physical transmission medium, the medium access control of the display, monitor physical access, visitor management, records access, power supply wiring and equipment, emergency shutdown, emergency power, emergency lighting, fire protection, temperature and humidity controls, water damage protection, delivery and pickup, alternative workplace, location of components of the information system, information leakage).

l) Planning (policy planning and safety procedures, system for security plan, update of the security system plan, performance standards, privacy impact assessment, safety related planning activities).

m) Security staff (security staff of the policies and procedures, categorization position, recruitment, termination of staff, transfer of personnel, access agreements, third party security personnel, the personal sanctions).

n) Risk assessment (policy and procedures of the risk assessment, security categorization, risk assessment, update the risk assessment, vulnerability analysis).

o) System and services of acquisition (policy and procedures, resource allocation, life cycle support, procurement, information system documentation, software usage restrictions, user-installed software, Safety Engineering principles, external services information systems, configuration management developer, developer security) tests.

p) System and communications protection (policy and procedures, the partitioned application, security function isolation, denial of service protection, priority of resources protection limit, the transmission integrity, confidentiality, transmission, network disconnection, establishment of cryptographic keys and the management, the use of cryptography, protection of public access, collaborative computing, transmission security settings, PKI certificates, mobile code, voice over Internet protocol, secure name resolution service

address, the strong name, address resolution service, recursive or caching resolution, architecture and provisioning for name, address resolution service, authenticity session).

q) The integrity of the system and the information. (Policy, trouble-shooting, protection against malicious code, information system tools and techniques for monitoring, security alerts and warnings, verifying the functionality, integrity of software and information spam protection, restrictions on entry information, accuracy of information, completeness, validity and authenticity, error control, manipulation and output of information retention).

Some of the reformulated questions: Is the company site on a cluster of multiple servers with load balancing in real time, if the server is damaged, does the site will continue to run? Do you must pay for more bandwidth?, Is the site is protected URL Spoofing?, Has the site has Secure Socket Layer and a fixed IP address?, Is the company website can be scanned for malware vulnerabilities?, Is the site is protected against DoS (denial of service) attacks and other malicious?, What level of intrusion has the site of the company? Has Network and Server-level intrusion prevention?

Step 6. Determine its owner can make important decisions on computer security. The owners are a group of researchers from the cities and / or states of Morelos, Chihuahua, Sinaloa, Morelia, State of Mexico, Los Angeles, Malaysia, Spain and DF they are the ones who can make decisions on enterprise computer security.

Step 7. Conduct interviews with staff concerning computer security needs and availability of time as well as some of the questions are:

1. ¿Do you have antivirus installed on Computers of the company? Yes, no, do not know.

2. Having antivirus installed (if applicable). Are you updated with the latest definitions? Yes, no, do not know.

3. ¿Does the company carry maintenance a computerized daily about computers? Yes, no, do not.

4. Do you use programs to download user files (music, movies, software)? Yes, no, do not know

5. How many computers the firm has available? 1-5, 5-10, + 10.

6. Do you have central data server at your company? or Do you rented in the cloud? Yes, no, do not know.

7. On that server, Does performed a regular computer maintenance? Yes, no, do not know.

8. Do you have batteries for each computer to avoid blackouts and surges? Yes, no, do not know.

9. Does battery to the central server or cloud to avoid blackouts and surges? Yes, no, do not know.

Step 8. Perform CATWOE scheme for enterprise computer security. The scheme should contain actors, customers, transformation, worldview, owner and environment. And it must be supported by the IEEE 17799 standard. The scheme should contain actors, customers, transformation, worldview, and business environment. And it must be supported by the IEEE 17799 standard. The CATWOE scheme is shown in Figure 2.

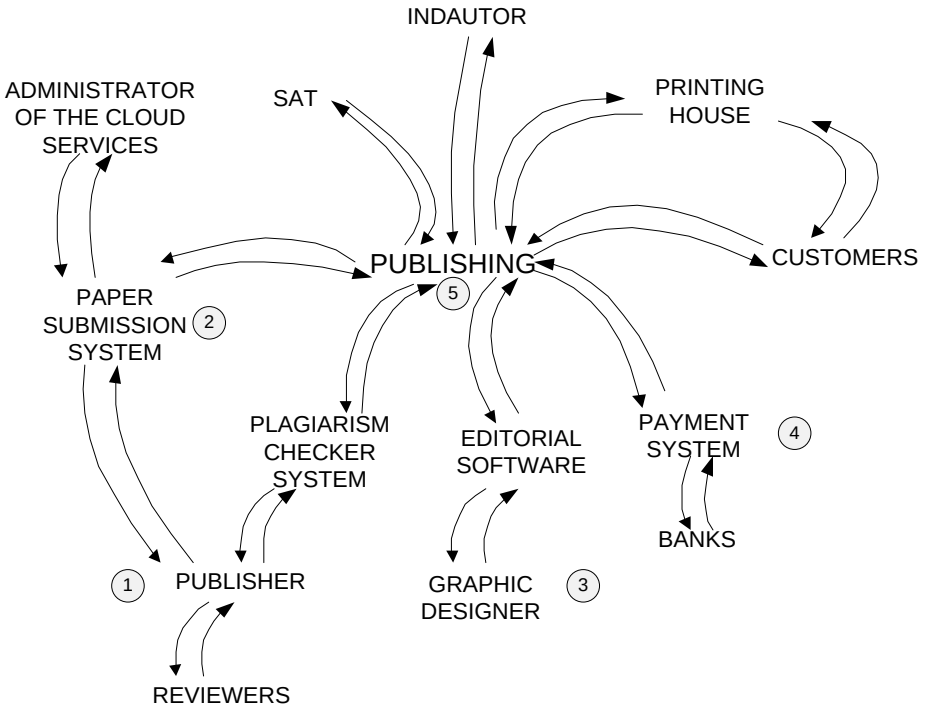

Figure 2. CATWDA for enterprise computer security.

Strategy 1 of Computer Security. The Protection is necessary from malicious code of computer equipment used by chief editors and guests, the derivative spam protection system server submission of articles, to create security alerts and warnings.

Strategy 2 of Computer Security. It was determined that there is unauthorized access to the articles submission system. You need to upgrade the version of Open Journal Systems software. It is also necessary to reconfigure the system audit process of submission of articles, because currently allow send spam from the mail server, the accounting system.

Strategic 3 of Computer Security. It should to create a protection policy to the storage media for the purpose of to avoid virus infection of the editorial repository.

Strategic 4 of Computer Security. It is necessary to continually review the information of the payment system, the solution of failures, malware protection, monitoring techniques events related to the security.

Strategic 5 of Computer Security. It is essential to create protection policy of the environment, physical access to servers, monitor visitor management, access logs, emergency lighting, fire protection, temperature and humidity controls, water damage protection, delivery and retirement, alternative workplace, location of components of the information system, information leakage.

Conclusions

In this paper is presented the implementation of CATWOE methodology for strategic planning for the Enterprise Computer Science Security. The benefits of applying CATWOE allow to make easier the structure of problem situations of complex organizations and obliges the user to do not act just rigid and technical way, it is also a mandatory tool to be used when it is very complex security problems. Finally the 5 strategies of enterprise computer security for a Mexican company obtained applying CATWOE to the enterprise.

As future work we will be made new metrics and methodologies for evaluating computer security of Mexican Companies.

References

1. Checkland P and Scholes J, Soft systems methodology in action, (John Wiley, West Sussex) 1990, 329.

2. Checkland P, Soft Systems Methodology: A Thirty Year Retrospective, Systems Research and Behavioral Science, 17 (2000) s11-s58

3. Montoya I and Montoya A,. Identification and systems methodologies for territorial delimitation, Agronomía Colombiana, 28 (2010) 455-465.

4. Macías-Chapula C, Diseño de un modelo conceptual sobre la transferencia de resultados de investigación en Salud pública en Honduras, Salud Pública de México, 54, (2012) 624-631.

5. Checkland P B, Systems Thinking, Systems Practice, (John Wiley & Sons, Chichester), 1999.

6. Arriola-Arciniega C and Aceves F J, Herramienta auditiva para acceder expresiones matemáticas digitales, Científica, 14 (2010) 137-144.

7. Martínez M A and Rios R F, Estudio de sistemas blandos para el desarrollo de un sistema de información gerencial, mediante una adaptación de la metodología para sistemas blandos de Peter Checkland, Ciencia Ergo Sum, 15 (2008) 45-53.

8. Carrillo G, Gómez L, Galvis E, González M, Olave Y, Propuesta de un sistema para la formación en la operación de subestaciones de transmisión de energía eléctrica, Scientia Et Technica, 13 (2007) 67-72.

9. Córdoba J, Campbell T, Implementing CSR Initiatives - The Contribution of Systemic Thinking, Pensamiento & Gestión, 23 (2007) 112-130.

10. Castillo Fonseca J, Osorio Huacuja C, La Información Documental para la implantación de sistemas de gestión de calidad aplicando la Metodología de Sistemas Blandos, Anales de Documentación, 14 (2011) 1-17.

11. Coelho F, Romero M, Yáber G, Indicadores de desempeño clave para programas académicos de postgrado, Investigación y Postgrado, 20 (2005) 123-153.

12. Watson R, Suggestions for New Application Areas for Soft Systems Methodology in the Information Age, Systemic Practice and Action Research, 25 (2012) 441-456.

13. Rodriguez-Ulloa R, Montbrun A, Martinez-Vicente S, Soft System Dynamics Methodology in Action: A study of the Problem of Citizen Insecurity in an Argentinean Province, Systemic Practice and Action Research, 24 (2011) 275-323.

14. Al-Zhrani S, Desarrollo de un modelo de Sistema Suave para la identificación de la información y los problemas de las comunicaciones y obstáculos en la tecnología de las organizaciones gubernamentales en Arabia Saudita, JATIT & LLS, 2005.

15. Díaz-Parra O, Cruz-Chávez M A, Galván-Montiel D, Técnicas de Modelación de Sistemas Blandos Aplicadas al problema del Transporte Escolar, AGECOMP, 1 (2006) 47-59.

16. Martínez-Rangel M G, Cruz-Chávez M A, Galván-Montiel D, Zavala-Díaz J C, Modelado del problema de calendarización de recursos para la fabricación de compresores, AGECOMP, 1 (2006) 147-159.

17. Ruiz-Vanoye J A, Díaz-Parra O, Ponce-Medellín, I R, Olivares Rojas, J C, Planificación Estratégica para la seguridad informática, Transactions on Computers, 7-5 (2008) 387-396.

18. Barros de Deus e Mello S R, Oenning Soares E, Dumke de Meiros D, Metodología de Checkland aplicada a la implementación de SGSST y nueva NR 10 en una empresa de sector eléctrico nacional, Octubre (2010).