Culture of data protection, service and quality is cybersecurity in SMEs

Cultura de protección de datos, servicio y calidad es ciberseguridad en MyPyMES

PEÑA-MONTES DE OCA, Adriana Isela†* & MONDRAGÓN-GUTIÉRREZ, Einar

Universidad Tecnológica de Jalisco, Cuerpo Académico: Responsabilidad Social, Sustentabilidad y Desarrollo Integral para Pymes

ID 1st Author: *Adriana Isela, Peña-Montes De Oca* / **ORC ID**: 0001-8220-3108, **CVU CONAHCYT ID**: 70757

ID 1st Co-author: *Einar, Mondragón-Gutiérrez*

DOI: 10.35429/EJRC.2023.17.9.22.28 Received July 27, 2023; Accepted October 20, 2023

Abstract

The purpose of this paper is to develop a strategic model to establish the best cybersecurity mechanisms and standards, mediating the protection and care of product and service information, emphasizing the importance of creating a culture of data care in order to deal with the challenges of global competition. A methodology was develop integrating tools such as PMI, SDLC, Kaizen and NIST framework, in order to establish responsibilities scope, times and resources, acquiring or adapting existing resources. The proposed model makes efficient use of Internet tools and new technologies to guarantee sustainability, cybersecurity, speed, flexibility, privacy of the information processed and energy backup, in order to promote change in favor of the development of competitive advantages in SMEs. The results allowed, through a collegiate work between the members of the interdisciplinary team, the construction of a Cybersecurity Model that supports SMEs, better safeguarding the data, although with a residual risk associated with routines due to updates and/or needs changing.

Industrial Evolution, Technologial Adaptation, Industrial Project

Resumen

El propósito del presente trabajo es desarrollar un modelo estratégico para establecer los mejores mecanismos y normas de ciberseguridad, mediando el resguardo y cuidado de la información de productos y servicios, enfatizando la importancia crear una cultura de cuidado de datos con la finalidad de hacer frente a los desafíos de la competencia globalizada. Se desarrolló una metodología integrando herramientas como PMI, SDLC, Kanban, ITIL, Kaizen, y marco NIST, a fin de establecer responsabilidades, alcances, tiempos y recursos, adquiriendo o adaptando los recursos existentes. El modelo propuesto, hace uso eficiente de nuevas tecnologías e internet, para garantizar, sustentabilidad, ciberseguridad, velocidad, flexibilidad, privacidad de la información procesada y respaldo de energía, a fin de impulsar el cambio en favor del desarrollo de ventajas competitivas en MyPyMES. Los resultados permitieron, a través de un trabajo colegiado entre los miembros del equipo interdisciplinario, la construcción de un Modelo de ciberseguridad que apoye a las MyPyMES, salvaguardando mejor los datos, aunque con un riesgo residual asociado en las rutinas por actualizaciones y/o necesidades cambiantes.

Ciberseguridad, Vulnerabilidad, Evolución tecnológica-industrial

Citation: PEÑA-MONTES DE OCA, Adriana Isela & MONDRAGÓN-GUTIÉRREZ, Einar. Culture of data protection, service and quality is cybersecurity in SMEs. ECORFAN Journal-Republic of Cameroon. 2023. 9-17: 22-28

* Correspondence to author (e-mail: adriana-isela@utj.edu.mx)

† Researcher contributing first Author.

Introduction

In recent decades, the technological revolution, new forms of communication, globalization, have made information the most important and valuable asset of organizations, thus increasing the need for control, in order to prevent, cyber attacks, its important to create a contingency plans to face threat to information systems.

Cybersecurity according to the International Telecommunication Union is defined as "a set of policy tools, security concepts, guidelines, risk management methods, actions, training, best practices, insurance and technologies that can be used to protect the assets of the organization and users in the cyber environment.

ISACA (2015) defines cybersecurity as: "protection of digital information assets, through the tratment of threats that put at risk the information that is processed, stored and transported by information systems that are interconnected".

The costs of global cybercrime are set to reach $10.5 trillion pesos annually by 2025. On average, US companies lose 27.4 million dollars due to cyber attacks, 90 percent related to human errors such as security breaches, as demostrated by Accenture (2019) and IBM (2018).

Vulnerabilities are failures in IT systems, which allow risk situations in the security of your data and information; among the best known we can mention: Ransomware, open port scanning, phishing, cookies theft, denial of service, SQL injection, Man in the middle, cross-site request, wireless networks, among others.

Currently in Mexico, the formulation of an engineering project, as well as its own direction and development, focuses on the factor of solutions and data protection, such as encryption, to achieve the desired objective. Last year Sophos© mentioned that of 200 companies surveys carry out, 57% received an attack on their data encryption, of which 79% had backup implemented. However, 44% had to pay the ransom for their data. The payment amounts of 68% ranged from half a million USD (Verizon, 2018)

Below is the percentage of operational impact and business losses both in the country and globally, as well as the percentage of companies that contracted cyber insurance.

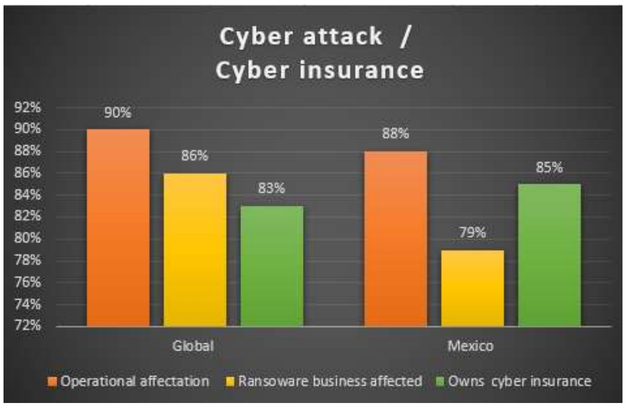

Figure 1 Percentage of losses due to ransomware

The ISO organization in February 2018, presented the ISO/IEC TR 27103:2018 Information technology –Security techniques, in response through a guide that facilitates the implementation of cyber security aligned with existing good practices, since it promotes the same concepts of NIST Cybersecurity Framework (CSF).

The core functions are identify, protect, detect, respond and recover, these five core functions represent the pillars for a successful and holistic cybersecurity program.

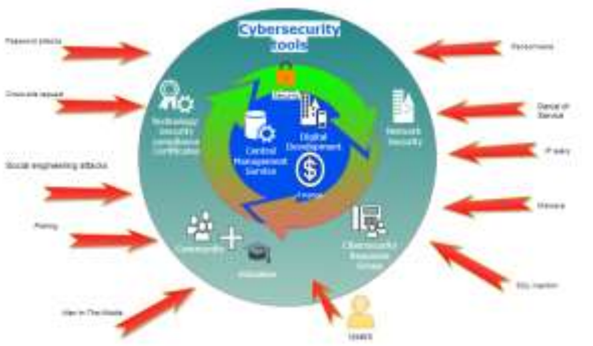

Figure 2 Data Protection Model

Thus, an improvement in the organization's results is explained through the company's ability to constantly renew itself, by being able to identify and exploit new opportunities, in response to customer demands and continuous improvement.

According to the literature, responding to cybersecurity incidents should include:

- Polices and response plans
- Procedures for registration and handling of incidents.
- Communication between internal and external parties.
- Determine which services provide the answers.

The objective of this paper is to develop a strategic model to establish the best cybersecutity mechanisms and standards, mediating the protection and care of product and service information, emphasizing the importance of creating a culture of data care.

The importance of this research is based on the fact that there are no instruments in Spanish, according to the author's knowledge, that evaluate the traits and interactions, arousing concern through the literature and due to its importance in the economic development of the country; in order to achieve the correct fit between the environment and the capabilities that organizations must adopt to promote efficient data care practices, which allow for the establishment of an intelligence capable of significantly reducing incidents caused by the human factor, in such a way that promote business innovation, causing the generation of competitive advantages in MyPyMES.

In the second section of the work, the conceptual framework is presented, as well as a review of the literature and empirical studies related to technological and procedural assurance for cybersecurity management, focused on the protection of value creation and innovation. The third section describes the methodology used, while the analysis and results are presented in the fourth section, to finally present and discuss the conclusions, limitations, and implications for future research

Theorical framework

There are many antecedents that are identified in the literatura as ideas and determining factors to include analysis technologies and improvements in cybersecurity processes, although with poor analytical processing for the intelligent use of information.

In Mexico as in Latin America, people lack awareness for the care and safeguarding of information, considering that in recent decades the technological revolution, with new forms of communication (internet) and new globalization processes, have created a niche of importance in terms of security in cyberspace.

Thus, the International Telecommunication Union approved Resolution 181mentions that cybersecurity is: “a set of political tools, security concepts, guidelines, risk management methods,
actions, training, best practices, insurance and technologies that can use to protect the assest of the organization and users in the cyber environment”

A computer attack that wants to affect an individual or organization can manifest itself in various ways, in relation to infrastructure vulnerabilities or personal or internal behavior patterns of the organization, among the known vulnerabilities are: Ransomware, Open port scanning, phishing, cookies theft, DoS, SQL, injection, Man-In-The Middle, Cross-site request, Hacking by social engineering, Wireless networks.

In Mexico, the secretary of the public function suffered a security incident that exposed the patrimonial declarations of 830,000 public officials, among others, the extortion of the National Insurance and Bonds Commission, mediating a Lockbit ransomware, with which the attackers hijacked the institution's equipment.

International standards for managing processes and achieving information security in order to build trust include:

ISO 27032 Standard –Allows the development of guidelines to safeguard the information assets that are in cyberspace.

ISO/IEC 27032 Standard-Garantees security in data or information exchanges on the network, when facing cybercrime with reliable and secure cooperation.

ISO/IEC 27032:2012 Standar – Strengthens the state of cyber security throug technical and strategic parameters relevant to this activity related to Interner, information and application and network security.

Mexico is attractive for investment by companies from North America, Asia and Europe, due to its workforce, its geographical location and its telecommunications infrastructure, land, air and maritime communication routes, as well as an operational and trained human resource with training of technological capabilities from foreign trade and the entry of foreign capital (Solleiro-Rebolledo and Castañon-Ibarra, 2014); Currently, it has a favorable perspective in terms of innovation according to the Global Competitiveness Index 2018, of the World Economic Forum, occupying the 50th place out of 140 countries in terms of innovative capacity to generate new goods and services.

There is still much to be done, in terms of linking technology companies in projects with universities, consultancies suppliers and other specialist bodies for the development or integration of industrial solutions for technological application.

Metodology

The research refers to the development of a model base on Project Management Institute (PMI), Systems development life cycle (SDLC), Kanban, Information Technology Infrastructure Library (ITIL) and Kaizen methodologies in order to establish responsibilities, scope, times and resources, acquiring or adapting existing resources.

Stage 1: Diagnosis and requirements, for the construction of the cybersecurity strategy plan.

Stage 2: Development; analysis and organization of processes through PMI technology, for the creation of a map of operation processes and standards oriented to cybersecurity.

Stage 3: Pilot tests to validate functionality and efficiency, by carrying out both internal and external attacks within a laboratory and WarRoom.

To improve the performance of cybersecurity and take care of innovation in MyPYMES, the design used is experimental, quantitative, cross-sectional and correlational (Hernández, Fernández and Baptista, 2010),

The scope of the research is exploratory, since it approaches the problema of relatively unknows studies and, in turn, verifiable statements are suggested in order to generate knowledge that allows contributing to research on the subject.

Fort he first stage, a questionnaire was carried out for the dignosis of social engineering attacks in the Guadalajara metropolitan área (ZMG) through the surveyMonkey.com tool, sharing the link with the interest groups. Given the consideration that the social engineering cycle of an attack by cybercriminals begins with an investigation, followed by the fabrication of a deception through a story to gain trust and take control of the situation, executing a plan to manipulate the victim, for after the objective is achieved, the cybercriminal disappears, cuts off contact with the victim. (INCIBE, 2019)

Fort he second stage, the creation of a map of operation processes andstandards oriented to cybersecurity, base don analysis and organization of processes through PMI technology.

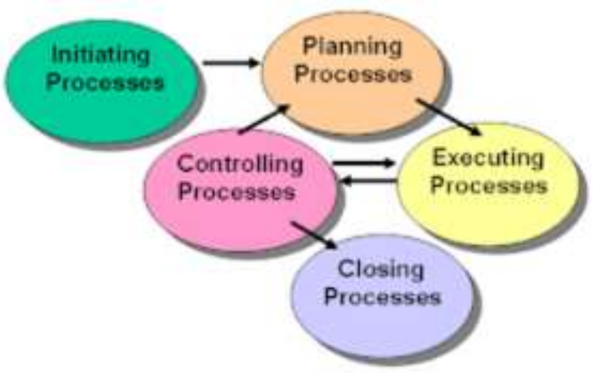

Figure 3 Project Management Processes
Fuente: PMI

The starting point of the project methodologies is to define the basic parameters of the process, or indicators of the classic control system: awareness, training and evaluation, in order to determine the arrangement and sizing of equipment and ideal modes, design and specify the systems in the case of hardware and software, in order to establish the performance specification in a ideal industrial environment.

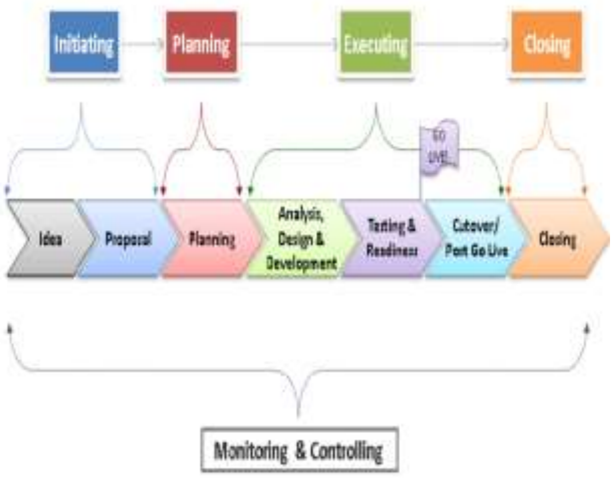

Figure 4 Details of Project Management Processes
Fuente: PMI

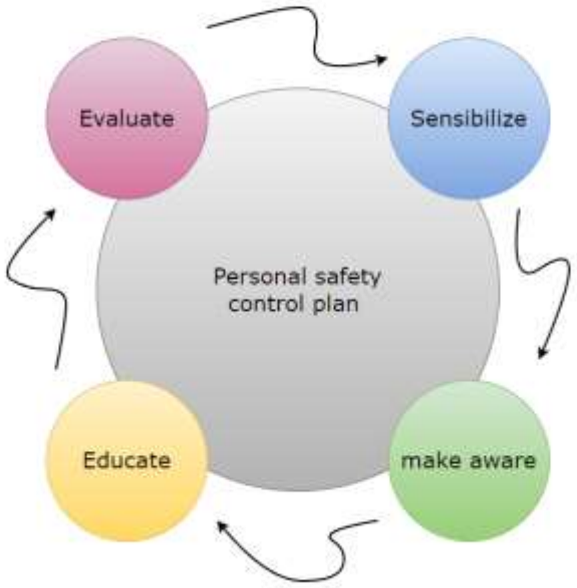

Figure 5 Model of Data Protection Culture

Technological integrations of IT solutions for Smart grids, through next-generation servers connected to the IT cloud, once unified and developed through SDLC, require four phases: planning, risk assessment, development and evaluation, in iterations until finalization, obtaining the product, which of course comply with the quality of its variables, supported by the wider context of customer experiences, value streams, and digital trasformation across the enterprise ITIL/Kanban and kaizen philosophy.

It is proposed, for stage 3, to apply a level of normalization of operation and value generation, through the integration of devices and software programs, which consider cybersecurity protocols vertical and horizontal integration communication, information processing in big data, the Internet of things as well as simulation, whose functions and interfaces are already duly installed in the devices or platforms currently marketed as conventional line products.

Results

In the case of MyPyMES, due to their specific characteristics, it is considered appropriate to consider interdisciplinary work groups, favoring cooperation and diversity, to address the planning process, as well as visualize the information necessary for execution; elements such as problems, execution time, budgets, áreas involved, risks, products obtained, etc., focused on creating value (Aguilar, 2020).

As a result of the phising password recocery simulation at the first stage, it was obtained that 85% of the users failed and clic to the pishing link, in the survey made by Sophos to companies. It was obtained that 97% of the companies consider making important changes in their cyber defenses, 64% will implemented new technologies for internal protections and periphery of the infrastructure, 53% considered that awareness and Training of your staff, as well as improvements to your processes, is important to close gaps vulnerable to identity theft and infections of business IT systems.

By identifying the possible risks or uncertainties for PyMES, strategies can be defined, thus the support of Ishikawa diagram, help to better face the challenges.

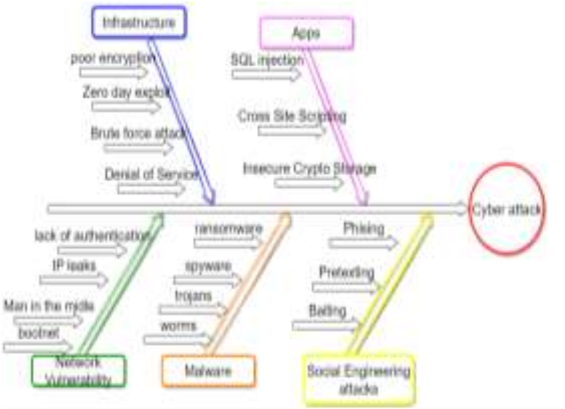

Figure 6 Risk Plan

ITIL/Kaban provides us with a best practices approach for the administration and support in incident control, likewise it will be related and combined.

The mdel generated a solid base to frame the scopeof an integration with a mediatic expectation of high impact, which also represents a considerable economic cost when attending to a high number of technological media integrated with each other.

Through modular visualization, Technology Management takes a highly representative place by contemplating determining factors from technological planning, implementation, assimilation processes, acquisition and development of technology, considering process automation, as a vallue proposition, and key differentiator in a Company that develops comprehensive technical solutions.

It is important that the information serves to control processes in real time, making efficient use of new technoligies and the internet of things, which does not require a specific space and can guarantee sustainability, cybersecurity, speed, flexibility, privacy of the information processed and backup of energy.

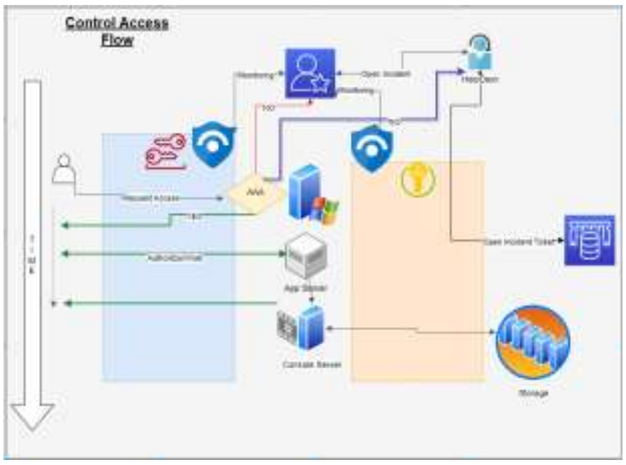

Figure 7 Network proposal Model for Cybersecurity

Faced with the challenge of developing a coherent and efficient cybersecurity protocol, engineering principles are fundamental in efficient diagnosis and relevant to the design of the solution, from the digitized design, the support of the human, economic and legal dimensions, through work collegiate among the members of the interdisciplinary team.

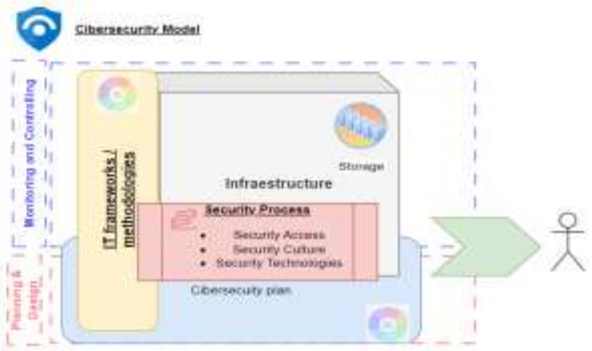

Figure 8 Comprehensive Cybersecurity Model

Pilot test were caried out in compaies of the work group, through cyber attacks on the main assets of the information systems, to calculate the level of risk, after the implementation of the model, it was found that the data safeguard model improved between 7-9 % the control of information, however there is a residual risk associated with routines due to updates and/or changing needs.

Conclusions

The study demostrates the importance in the work of the Project leader, in the initial diagnosis, the plan or design for the construction of instruments that allow the control of all kinds of comercial, social and governmental interactions, since it is a high level of complexity, due to the multiplicity of the variables found, thus, in the dynamics of cybersecurity, organization, technologies, dynamics of the sector and the response of society are interwoven.

It is importan to state that, if a Company wishes to be competitive within the global market, it is necessary to have a cybersecurity plan and educational strategies to have defenses against any cyberattack that intends to affect the operation of services, theft of protected or sensitive information, as well as having the security strengthening culture to reduce any risk that affects the Company or persons

The model introduces an reliable and highly efficient active security system, applied on critical infrastructure networks, the system proposed is base on a multi-dimensional dataset for data safeguarding, which improved information control by 7-9 %, however there is a residual risk associated with routines due to updates and/or changing needs.

The present study is not without its limitations, complete coverage of all articles could not have been achieved, given the chosen search procedure. Therefore, there could have been works that had been directed to migration or technological adaptation where a different language was used. Consequently, the factors derived from the analysis need to be treated with caution.

References

Aguilar, J.M. (2020) Presente y future de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional. Revista Legislativa de Estudios Sociales y de opinión pública. 29, Vol.13.

Center for Internet Security. CIS Configuration Assessment Tool CIS-CAT. 2015. Retrieved from https://learn.cisecurity.org/cis-cat-lite

CIS. Center for Internet Security (CIS). 2000. Retrieved from hhttps://www.cisecurity.org/

Hernández S.R., Fernández, C.c: y Baptista, P. (2010). Metodología de la investigación (5ª. ed.), México: Mc Graw-Hill.

International, Electrotechnical, and Commission. Welcome to the IEC – International Electrotechnical Commission. 1904. Retrieved from https://www.iec.ch/

International Organization for Standardization ISO- International Organization for Standardization. 1947. Retrieved from https://www.iso.org/home.html

ISACA. Information Technology-Information Security _Information Assurance (ISACA).1994 Retrieved from https://www.isaca.org/pages/default.aspx.

ITIL. Information Technology Infrastructure Library (ITIL) Guide 2003. Retrieved from https://www.ibm.com/cloud/learn/it-infrastructure-library

Kaspersky, Eugene. Fobres.com.mx Fobres Mexico. [On line] 01-02-2023. Retrieved form https://www.forbes.com.mx/ciberamenazas-que-retaran-al-sector-empresarial-en-2023/

National Istitute of Standards and Technology-National Institute of Standards and Technology NIST. 2019. Retrieved from https://www.nist.gov/

Solleiro J.L., Gaona C., Castañón R. (2014) Políticas para el desarrollo de Sistemas de Innovación en México. Journal of Technology Management & Innovation Vol. 9 (4)

Sophos [En línea] 11 de Mayo de 2022. https://sophosmx.another.co/66-de-las-empresas-del-mundofueron-victimas-de-ransomware-en-latinoamerica-es-de-hasta-el-74

Verizon (2018). Payment security compliance drops for the first time in six years. https://www.bloomberg.com/releases/2018-09-25/payment-security-compliance-drops-for-the-first-time-in-six-years-states-verizons2018-payment-security-report