International Interdisciplinary Congress on Renewable Energies, Industrial Maintenance, Mechatronics and Informatics

Booklets

RENIECYT
Registro Nacional de Instituciones y Empresas Científicas y Tecnológicas
1702902 CONAHCYT

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - Google Scholar DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID - V|LEX

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

Authors: PEÑA-MONTES DE OCA, Adriana Isela and OROZCO-MAGALLANES, Rubén Ulises

Editorial label RINOE: 607-8695
VCIERMMI Control Number: 2023-02
VCIERMMI Classification (2023): 261023-0002

Pages: 15
RNA: 03-2010-032610115700-14

RINOE - Mexico
Park Pedregal Business. 3580-
Adolfo Ruiz Cortines Boulevard –
CP.01900. San Jerónimo Aculco-
Álvaro Obregón, Mexico City
Skype: RINOE-México S.C.
Phone: +52 1 55 1260 0355
E-mail: contact@rinoe.org
Facebook: RINOE-México S. C.
Twitter: @Rinoe_México

www.rinoe.org

Holdings

Mexico	Peru
Bolivia	Taiwan
Cameroon	Western
Spain	Sahara

Introducción

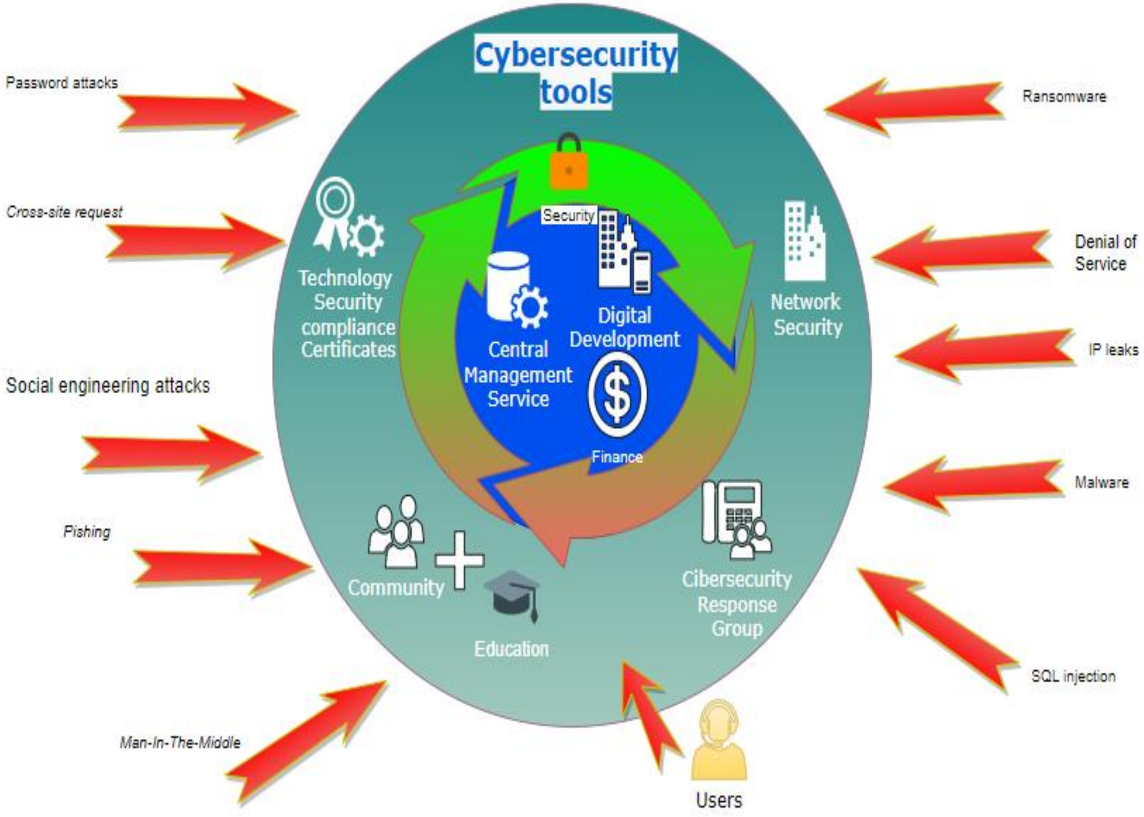
Cybersecurity according to the International Telecommunication Union is defined as “a set of policy tools, security concepts, guidelines, risk management methods, actions, training, best practices, insurance and technologies that can be used to protect the assets of the organization and users in the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

Introduction

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).

Data Protection Model



Objetive

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.

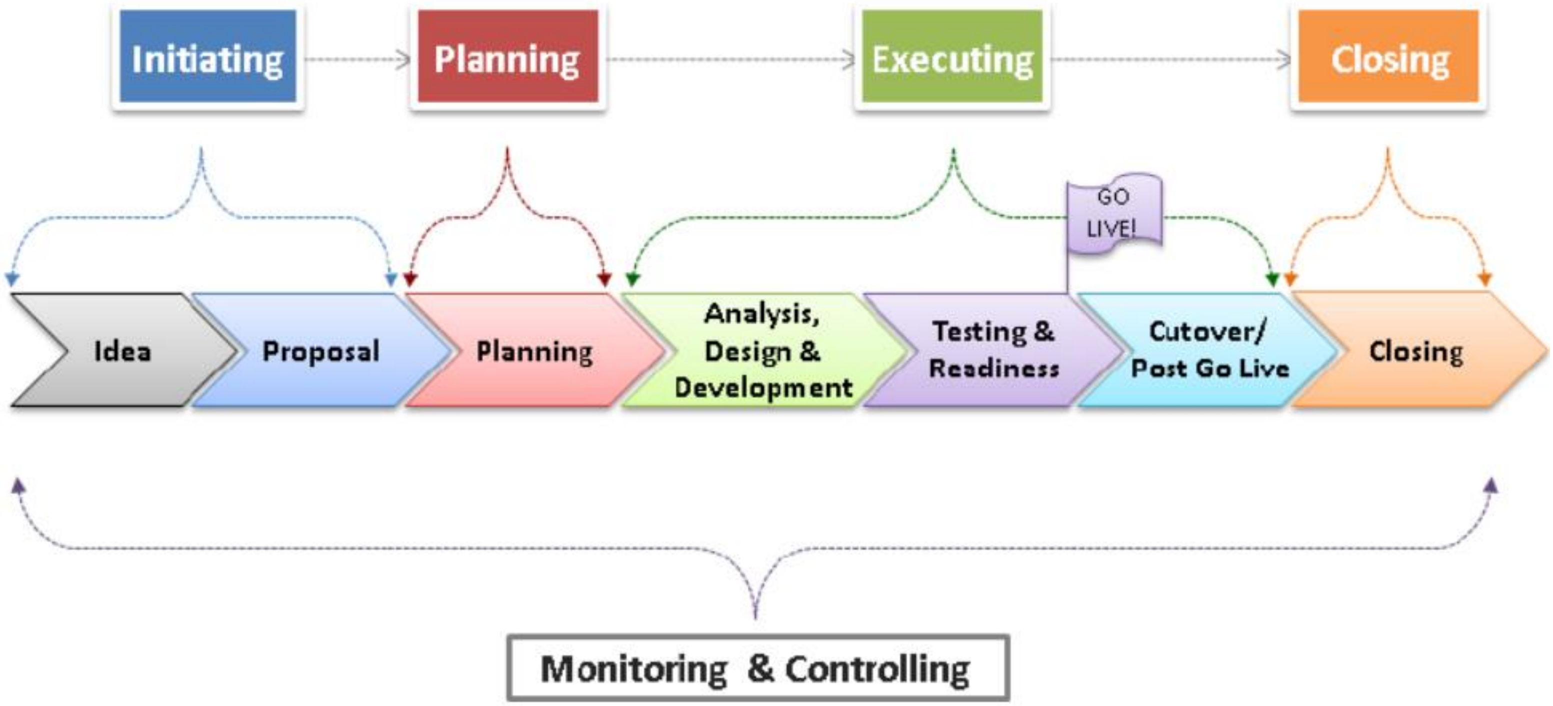
Metodology

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.

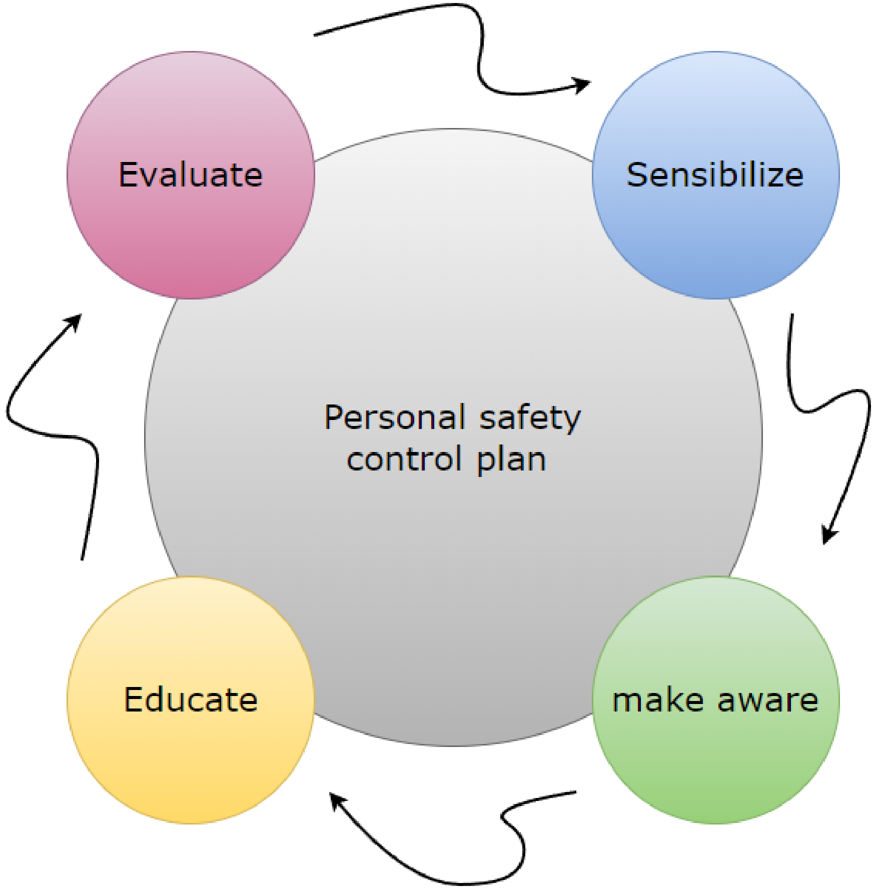
Stage 1: Diagnosis and requirements, for the construction of the cybersecurity strategy plan.

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.

Details of Project Management Processes



Model of Data Protection Culture



Evaluate

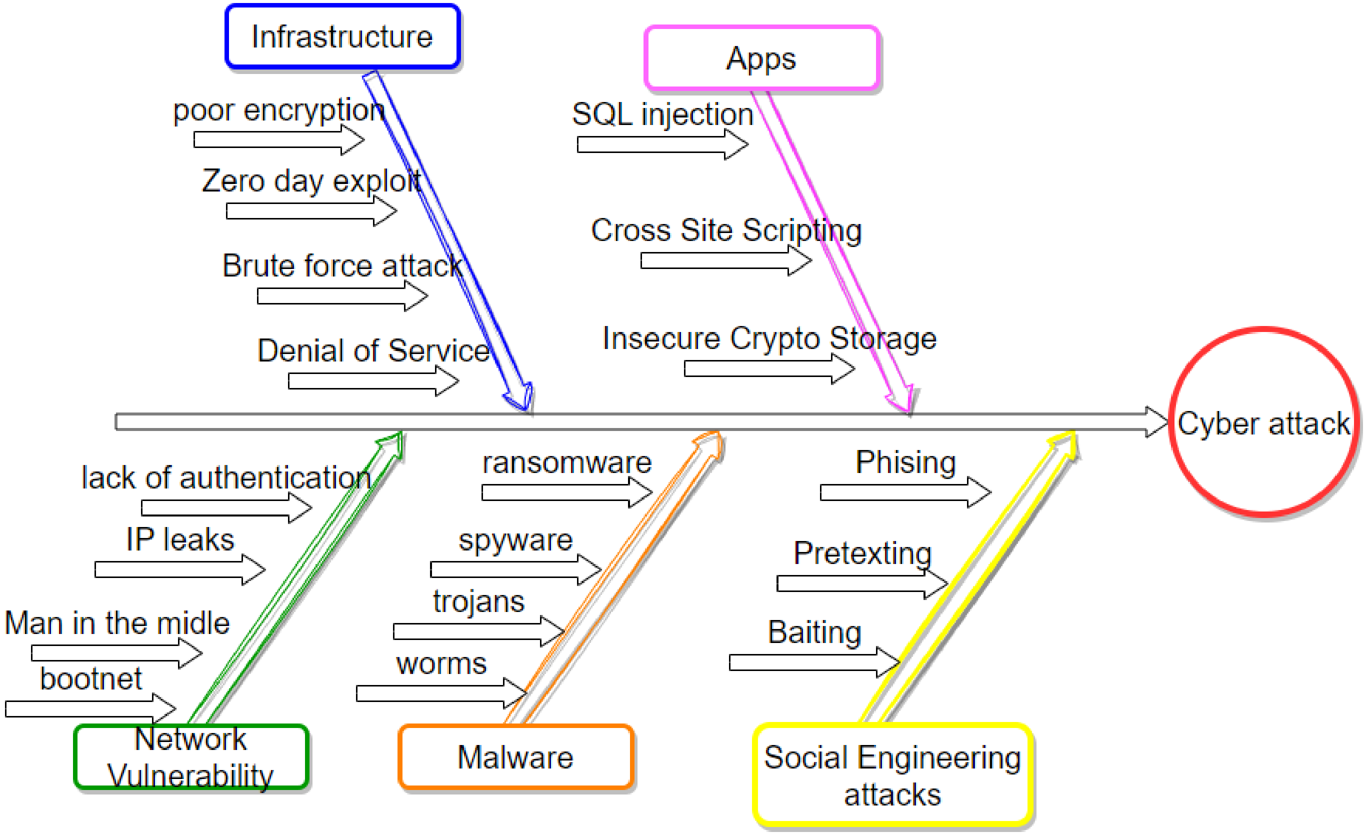
Sensibilize

Personal safety control plan

make aware

Educate

Risk Plan


Infrastructure
poor encryption
Zero day exploit
Brute force attack
Denial of Service
Apps
SQL injection
Cross Site Scripting
Insecure Crypto Storage
Cyber attack
lack of authentication
IP leaks
Man in the midle
bootnet
Network Vulnerability
ransomware
spyware
trojans
worms
Malware
Phising
Pretexting
Baiting
Social Engineering attacks

Results

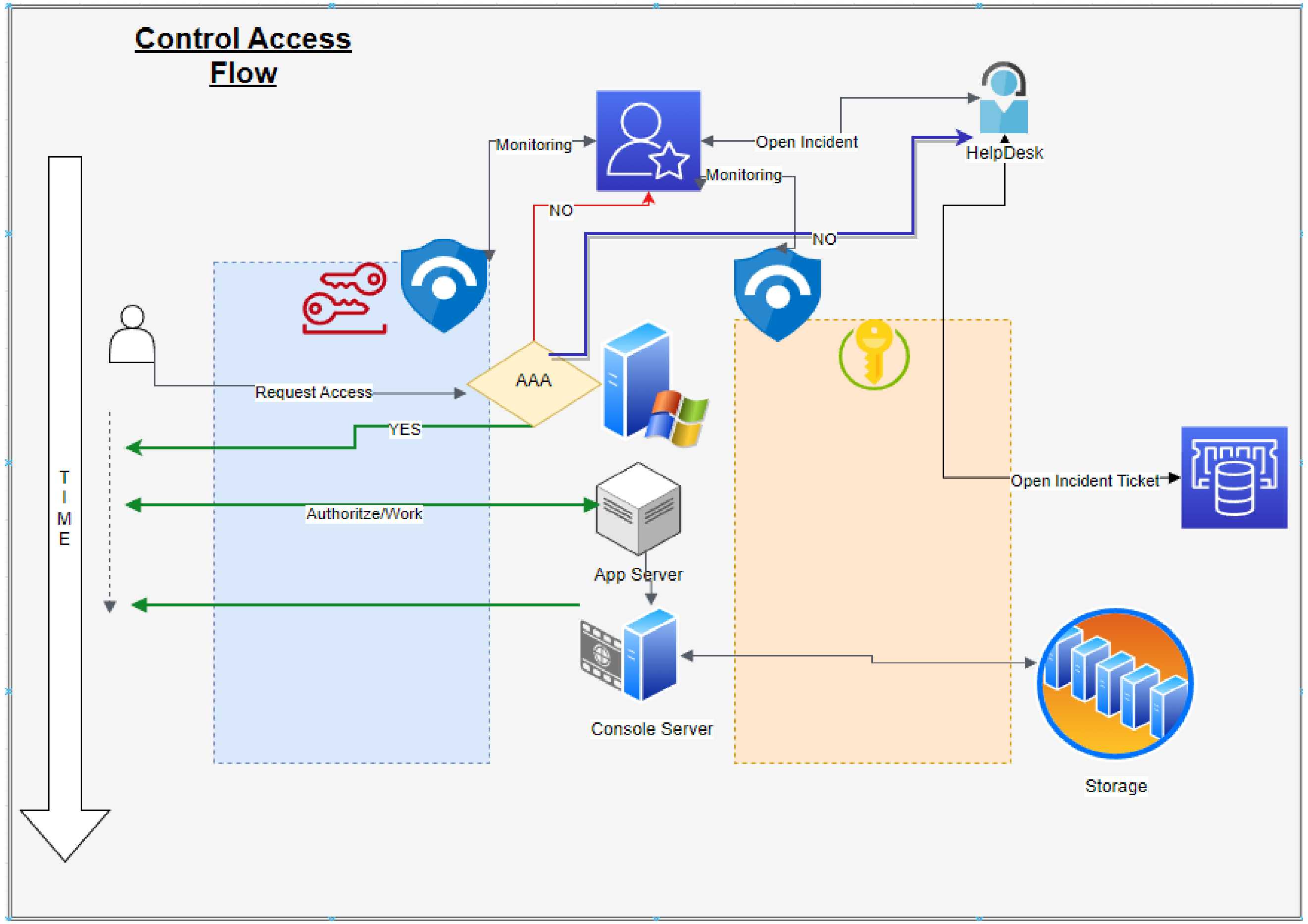
In the case of MyPyMES, due to their specific characteristics, it is considered appropriate to consider interdisciplinary work groups, favoring cooperation and diversity, to address the planning process, as well as visualize the information necessary for execution; elements such as problems, execution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

It is important that the information serves to control processes in real time, making efficient use of new technologies 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.

.

Results

Proposed Cibersecurity Model



Results

Pilot test were caried out in companies 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 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.

As a future lines of research; aims to promote the development of secure software, assess the advantage of inclusion in the era of digital transfomation, and development international regulations or legal actions for security with biometric access.

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

RINOE®