International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6337
***Article Received**: 29 December 2022 **Revised**: 30 January 2023 **Accepted**: 12 February 2023*

Experimental Study based on the Implementation of a Regulatory Framework for the Improvement of Cyber Resilience in SMEs

Liset S. Rodriguez-Baca[1], Shridhar Allagi [2], Rosa Larrea-Serquen[1], Carlos F. Cruzado[1], Mitchell Alarcon Diaz[3], Sandra Garcia-Hernández[4], Julio Daza Monteiro[1]
[1] Universidad Autónoma del Perú, Lima, Peru
[2]KLE Institute of Technology, Hubballi, India
[3] Universidad Nacional Mayor de San Marcos, Lima, Peru
[4]Tecnológico de Monterrey, Morelia, Mexico
Liset.rodriguez@autonoma.pe

Abstract— Currently, applying regulations oriented to cybersecurity, cyber resilience is relevant to face the high rates of cyberattacks, which have caused an interruption in the operational processes of organizations, generating an economic loss, and affecting the continuity of their business processes on the web. In this scenario, small and medium-sized enterprises (SMEs) are the most affected due to their weak technological infrastructure. Given this, this experimental study was developed to implement a regulatory framework for the improvement of cyber resilience; the criteria anticipate, resist, recover and evolve presented significant statistical values of improvement after the application of the experiment. This research contributes to counteract the refusal to use information technologies for business development; Improvement actions were carried out to face threats and computer vulnerabilities to which organizations are exposed when carrying out operations in cyberspace.

Keywords- Cyber resilience, cybersecurity, business continuity

I. INTRODUCTION

In recent years, even more so with the consequences of the health emergency that has occurred, the volume of cybersecurity incidents has increased, causing an interruption in business processes; this is due to the dependence on technology of different sectors of society. This situation has been affecting all organizations that carry out their operations in cyberspace; however, the most affected are the SMEs since they have the weak technological infrastructure, but they constantly fight to be current in the market and respond to the requirements of the current consumer. According to the report by [1], it can be stated that 51% of organizations had a significant interruption of their business in recent years due to cybersecurity incidents. This report also states that cyber resilience is essential to minimize disruption to business processes in the face of cyberattacks. Likewise, the European Union Agency for Cybersecurity and the computer emergency response team for European institutions [2] argue that it is urgent to promote cyber resilience in organizations since there is evidence of an increase in the threat level of cyberattacks. globally. In the same sense, [3]maintains that the rise in cyber threats was evidenced more frequently in 2021. These critical incidents were managed by the CCN-CERT. [3] specify that the sophistication of attacks through the supply chain increased. This involves the reliability of communications between service providers and users. Considering the results of the last survey carried out by [4] regarding cyber resilience during a crisis, it was obtained as a result that more than a third of the respondents affirmed that the SMEs they lead are prepared for growth in sales since they have a plan strategic, business plan for new products; however, they do not have an effective cybersecurity plan. It should be noted that it is no longer enough to implement cybersecurity mechanisms or policies, but organizations must be capable of preventing attacks, resisting them, and recovering from them; likewise, evolve in the strategy to avoid being affected repeatedly. Therefore, it was essential to develop the research that allowed the implementation of a regulatory framework related to cyber resilience and guaranteed the continuity of services in SMEs.

II. BACKGROUND AND RELATED WORKS

After an exhaustive review, the following antecedents can be mentioned:

[5] maintains that the cybernetic resilience of a company depends on the IT infrastructure and the cybersecurity mechanisms it adopts. However, it specifies that employees

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6337
***Article Received**: 29 December 2022 **Revised**: 30 January 2023 **Accepted**: 12 February 2023*

constitute a relevant factor in improving resilience. In their research, these authors presented a framework for measuring the cyber resilience behavior of employees at a banking center in India.

According to [6], resilience is a feature that is gaining more and more attention in computing and engineering. However, the definition of resilience in the cyber landscape is still unclear. For this reason, these authors analyzed definitions provided by various authors in different years and areas of application in computing. They concluded with a holistic definition using attributes for cyber resilience. They indicate that cyber resilience is facing cyber vulnerabilities and ensuring business continuity.

For his part, [7] states that digital twins significantly impact industry and research. The authors maintain that it is a technology that adds value to society since it allows virtualizing any physical system and observing the fundamental dynamics of its state, processes, and functions through data obtained from the physical counterpart. In his research, he explores the literature to improve cyber resilience from the perspective of cybersecurity and digital twins.

[8] argue that security in mobile applications is a relevant factor when safeguarding the data stored in an organization. In their study, they carry out an analysis of the mechanisms of different frameworks used in the market and prioritize and select the most important security aspects, proposing a new framework for the development of secure mobile applications and maintaining that cyber resilience must be included in the development process to support data management.

[9]state that cybernetic resilience is highly relevant as a prevention and security mechanism in any organization. Thus, they propose a redundancy cybernetic resilience technique based on fast redirection under security metrics with basic schemes to protect a network, node, link, and bandwidth elements. Their proposed model is configured to calculate primary and backup roads. Their results demonstrated the efficiency and adequacy of the model in practical applications.

According to [10] in his article, he argues that contemporary companies often encompass or aspire to the automated and networked production of industrial goods through international supply chains with many digitized interfaces. This allows very competitive operations in time, cost, and quality; however, it also involves cyber threats with significant risks. Therefore, to adequately manage these risks in the digital world, it is necessary to raise awareness and establish and maintain cyber security measures to guarantee an adequate level of protection throughout the entire value and supply chain.

[11] present a new shared design scheme for the sustained digital thread in video transmission to address the problem of IP theft and tampering. The authors maintain that their proposal has the potential to improve cyber resilience, for which they carry out an exhaustive analysis of digital supply chains.

[12] in their study, they develop a multi-level theoretical framework to explore blockchain integration strategies. They perform custom tests regarding the resilience of business models in detecting false data injection attacks. The integration of blockchain with different business scenarios can be appreciated in cyber-physical systems where resilience is critical for the stability of the system's operation.

[13] states that software-defined networking (SDN) technology is an approach to cloud computing that facilitates network management and efficient network programming and configuration, thereby enabling performance optimization and monitoring of the network. It is important to note that SDN is highly resistant to cyber-attacks using controllers that help specialists manage the network remotely. The authors examined the effects of security attacks using the SDN penetration tool, the reflector driver. They found that the driver is vulnerable to address resolution protocol, man-in-the-middle, and spoofing attacks. Distributed denial of service attacks. These attacks affect normal network operations by reducing performance and increasing packet delivery time.

[14]maintain that cybernetic resilience is a growing concern for the autonomous navigation of marine vessels. Their study analyzes three relevant aspects: fusion of information from multiple sensors, diagnosis of abnormal behaviors, and change detection. This background shows how it is possible to detect deviations from nominal behavior when the navigation sensor is under attack or defects occur.

According to [15], They maintain that cybersecurity is crucial in the health sector and that the levels of cybernetic resilience are optimal. They say it's conceivable that a cybersecurity incident would render anesthesia systems useless, comparing it to a ransomware attack that locks out end users. Only in healthcare would the consequences be ominous. For this reason, they maintain that perioperative services must have reasonable devices and a power failure mitigation measure; they also propose that training on cyberattacks for medical personnel is very relevant, how to mitigate them and apply good cybersecurity practices to protect patients in anesthesia systems.

For their part,[16] argue that the cyber connectivity of vehicles between vehicles and infrastructure will drastically reshape future scenarios. They affirm that the cybernetic components used in the vehicles give rise to cyber-attacks on the transportation system, for this reason, they investigated the possible operating scenarios of the cybernetic components and autonomous mobility systems (AMS) before identifying potential cyber-attacks. To AMS at both the vehicle and system levels. They concluded that it is necessary to improve cybersecurity and implement strategies to improve cyber resilience. They also recommended maintaining an autonomous road network and deploying different sub-autonomous mobility systems.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6337
***Article Received**: 29 December 2022 **Revised**: 30 January 2023 **Accepted**: 12 February 2023*

[17] state that it is necessary to know the situational status of business cybersecurity in SMEs to identify improvement opportunities that allow the continuity of their services and therefore remain current in the market.

According to [18], the use of technology in manufacturing and other sections of the supply chain makes it more susceptible to cyber threats. The authors state that AM supply chains pose higher degrees of threat than other supply chains due to their heavy reliance on technology and information sharing. Therefore, assessing the cyber resilience of an AM supply chain is a crucial task to ensure competitive business advantages. They proposed an integrated and complete approach based on the Dempster-Shafer (DS) theory as a methodology to develop a framework to assess a supply chain's cyber resilience. They executed it in a company in said field, validating its effectiveness. They also recommend that the model be applied to different organizations regarding their state of cyber resilience.

[19]states that the term cyber resilience by design (RBD) is gaining more importance in recent years due to its influence on the continuity of organizations operations.

[20] affirm that the world is experiencing an accelerated growth of smart cities, including the Internet of Things (IoT) and enhanced by the application of emerging innovative technologies that increasingly create highly complex cyber-physical-natural ecosystems, and this is susceptible to threats. cybernetic They argue that cyber resilience is a recent paradigm, and most studies focus on a subset of incident responses in phases of detection and analysis, but not prevention.

III. METHODOLOGY

The research work was developed through a pre-experimental design in which all those processes that are part of implementing a regulatory framework for improving cyber resilience were considered. The proposed hypothesis is that, after the experimentation, there were significant statistical differences between the pretest and the posttest of all those processes. Another relevant methodological aspect is that the dimensions were considered for the cyber resilience variable: attract, resist, recover, and evolve. The observation was used as an analysis technique. The instrument used was the checklist which consisted of 46 items that allowed us to identify if the control objectives related to cyber resilience were being met.

In the statistical analysis, Shapiro-Wilk was used to determine the normality of the data and considering that the data did not present normality, the Wilcoxon test was used.

IV. EXPERIMENTS, RESULTS AND DISCUSSIONS

A. Results

Regarding descriptive results, we have:

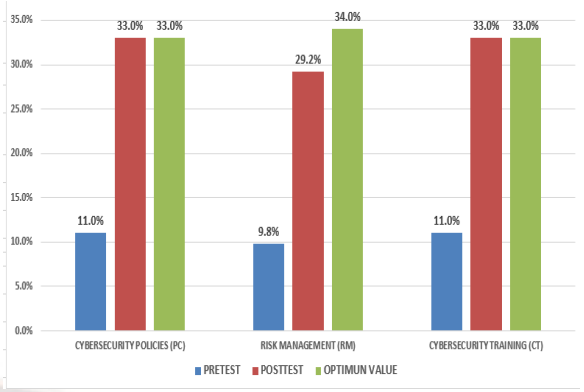

Figure1. Comparison of the results of the pretest and posttest gap of the "anticipate" dimension applied in the company

In relation to dimension 1: Anticipate; It can be seen in Figure1 that a gap of 22% was obtained in the pretest, compared to the 0% that was achieved in the posttest in the Cybersecurity Policies (PC) domain due to the implementation of cyber resilience requirements for the main service, defining the impact and the probability that it would cause if any interruption occurred, as well as the approach of strategies to face cyberattacks.

Likewise, it is observed that in the Risk Management (RM) domain, in the pretest, a gap of 24% was identified compared to the 5% that was obtained in the posttest, since relevant procedures were developed and implemented to manage risks associated with the main service, which allowed mitigating cyber risks to the main processes of the company. An inventory of assets directly supporting the main service was also prepared and documented, and a schedule for the corresponding maintenance was established. It was validated that backup copies are made on time; the information is classified according to criticality. In the same way, in the Cybersecurity Training (FO) domain, a gap of 22% was found in the pre-test, compared to the 0% achieved in the post-test due to the definition and implementation of a cyber training plan. Resilience oriented to the collaborators involved with the main service of the company. Defining and executing an awareness plan aimed at all collaborators was also possible.

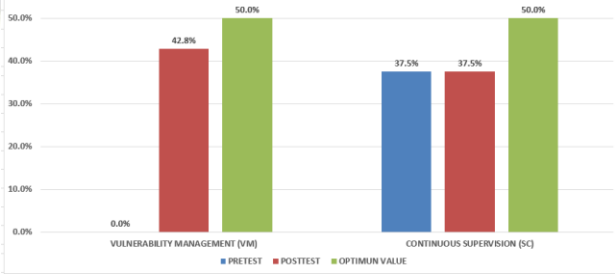

Figure2. Comparison of the results of the pretest and posttest gap of the "Resist" dimension applied in the company

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6337
***Article Received**: 29 December 2022 **Revised**: 30 January 2023 **Accepted**: 12 February 2023*

In dimension 2: Resist; It can be seen in Figure 2 that a gap of 50% was obtained in the pretest, compared to the 0% that was achieved in the posttest in the Vulnerability Management (VM) domain due to the development and implementation of specialized management procedures. of vulnerabilities in the company, modern tools have been used, and strategies have been applied to identify asset vulnerabilities. It was possible to categorize and prioritize the vulnerabilities that directly impact the main service so that they can be managed on time. A repository of the main vulnerabilities that affect the main service was established, which must be permanently updated. Regarding vulnerabilities that could not be fully resolved, their status is monitored, and they are subjected to an exhaustive analysis process to identify their origins. Likewise, it is observed that in the domain of Continuous Supervision (SC) in the pretest a gap of 13% was identified. It was not possible to improve in the posttest since there was no timely response from external providers regarding the proposed procedure to be followed. report potential cybersecurity events that affect the main service since they stated that due to an aspect of confidentiality of the information, they could not socialize it and would carry out the treatment internally.

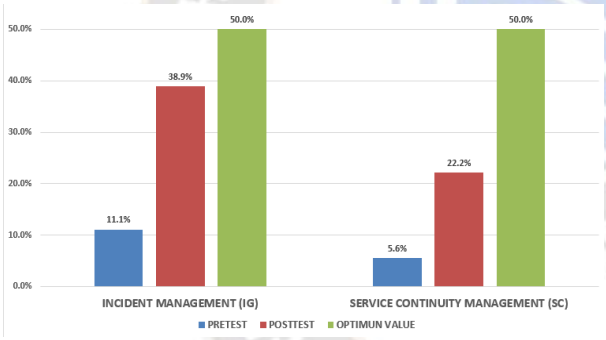

Figure3. Comparison of the results of the pretest and posttest gap of the "Recover" dimension applied in the company

Regarding dimension 3: Recover; It can be seen in figure 3 that a gap of 39% was obtained in the pretest, compared to the 11% that was achieved in the posttest in the Incident Management (IG) domain due to the implementation of procedures that allowed the identification and recognition cyber incidents that, after applying prioritized criteria, were classified and valued according to the classification of the regulations. After its analysis, the most appropriate response was determined in the shortest possible time. A registry of cyber incidents was implemented until its resolution, and the causes that originated it are investigated. In this same sense, it is observed that in the Service Continuity Management (SC) domain, in the pre-test, a gap of 44% was identified compared to the 28% obtained in the post-test due to the establishment of a continuity plan to guarantee the validity of the main service of the company, as well as the response of the SME was evaluated from the interruption of the main service until it was possible to recover to a minimum required level and then until its complete recovery.

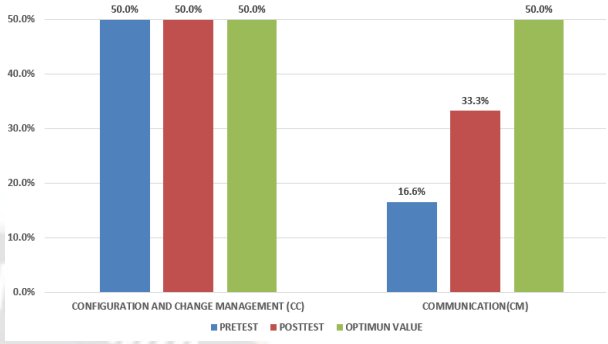

Figure 4. Comparison of the results of the pretest and posttest gap of the "Evolve" dimension applied in the company

Regarding dimension 4: Evolve; It can be seen in Figure 4 that no gap was identified in the pretest in the Configuration and Change Management (CC) domain because the SME uses a configuration management procedure for equipment that is linked to the service system Principal. In the Communication (CM) domain, a gap of 33% was found in the pre-test, compared to the 17% achieved in the post-test due to the definition and establishment of effective communication mechanisms with suppliers, clients, and referring users to cyber resilience issues.

TABLE I. GENERAL RESULTS OF THE POST TEST-PRETEST

	Post test- Pre test
FROM	-3,192[b]
One. asymptomatic (bilateral)	,001

a. Wilcoxon signed rank test
b. It is based on negative ranks.

The statistical results show that if there is a significant difference between the pre and post-test, in this sense, it can be affirmed that the implementation of a regulatory framework improves cyber resilience in an MYPE.

TABLE II. RESULTS OF THE POST TEST -PREPEST:ANTICIPATE DIMENSION

	Posttest Anticipar – Pretest Anticipar
FROM	-2,585[b]
One. asymptomatic (bilateral)	,010

a. Wilcoxon signed rank test
b. It is based on negative ranks.

The statistical results show that if there is a significant difference between the pre and the post-test, in this sense, it can

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6337
***Article Received**: 29 December 2022 **Revised**: 30 January 2023 **Accepted**: 12 February 2023*

be affirmed that the implementation of a regulatory framework improves the dimension to anticipate in an MYPE.

TABLE III. RESULTS OF THE POST TEST -PREPEST:RESIST DIMENSION

	Resist Posttest – Resist Pretest
FROM	-2,449[b]
One. asymptomatic (bilateral)	,014

a. Wilcoxon signed rank test
b. It is based on negative ranks.

The statistical results show that if there is a significant difference between the pre and post-test, in this sense it can be affirmed that the implementation of a regulatory framework improves the dimension of resistance in a MYPE.

TABLE IV. RESULTS OF THE POST TEST -PREPEST:RECOVER DIMENSION

	Resist Posttest – Resist Pretest
FROM	-2,828[b]
One. asymptomatic (bilateral)	,005

a. Wilcoxon signed rank test
b. It is based on negative ranks.

The statistical results show that if there is a significant difference between the pre and post-test, in this sense it can be affirmed that the implementation of a regulatory framework improves the dimension of resistance in a MYPE.

TABLE V. RESULTS OF THE POST TEST -PREPEST:EVOLVE DIMENSION

	Posttest Evolve - Pretest Evolve
FROM	-2,121[b]
One. asymptomatic (bilateral)	,034

a. Wilcoxon signed rank test
b. It is based on negative ranks.

The statistical results show that if there is a significant difference between the pre and post-test, in this sense it can be affirmed that the implementation of a regulatory framework improves the dimension of evolving in a MYPE.

B. Discussions

In relation to the results obtained, relevant aspects were found in applying a regulatory framework to improve cyber resilience in the SME studied. These relevant aspects refer to the importance of cybersecurity training (FO) corresponding to dimension 1: Anticipate. That it should be promoted in all collaborators who are directly involved with the company's business processes to prevent social engineering attacks, for this reason, it was possible to define and implement a training plan and a cyber resilience awareness plan aimed at employees. collaborators that will be carried out permanently in the organization. Studies such as [5] maintain that a company's cyber resilience depends on its technological infrastructure; however, he affirms that employees are the main factor in improving cyber resilience.

Likewise, [15] maintain that training regarding cyber resilience, mitigation of cyber attacks, and application of good practices to their organization's personnel to protect information systems is essential. In this sense, it is shown that the study carried out has a theoretical and methodological value since, in the fieldwork, it was verified that the implementation of a regulatory framework allows permanent training in cybersecurity for all employees of an organization since it is everyone's responsibility to protect the most critical asset: information. In the same way, [21]argues that it is necessary to promote the knowledge and development of cyberculture to maintain operational cyber resilience, and this allows for preventing cyberattacks.

Concerning dimension 2: Resist, in the Vulnerability Management (VM) domain, it can be stated that implementing procedures using modern tools and applying strategies to identify asset vulnerabilities makes it possible to reduce the existing gap and improve cyber resilience. of the organization. Research such as the one developed by [11]shows that it is relevant to implement mechanisms that help manage vulnerabilities such as IP theft and manipulation. They also state that a thorough analysis of its origins should be done. Likewise, [12] indicates that adopting security mechanisms in digital environments generates a competitive advantage for the protection of assets and proposes exploring integration strategies with blockchain in different business scenarios. This is also indicated by [16] in his research, where he states that improving cybersecurity and implementing strategies to optimize cybernetic resilience is necessary.

Regarding dimension 3: Recover, positive results were obtained in the Incident Management (IM) domain according to the implementation of procedures to identify cyber incidents classified according to regulations. After its analysis, the most appropriate response was determined in the shortest possible time. A registry of cyber incidents was implemented until its resolution, and the causes that originated it are investigated. In the same sense, in the Service Continuity Management (SC) domain, establishing a continuity plan to guarantee the validity of the company's main service was crucial, as well as the response of the SME since the interruption of the service. main service until recovery to a minimum required level was achieved

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6337
***Article Received**: 29 December 2022 **Revised**: 30 January 2023 **Accepted**: 12 February 2023*

and then until full recovery. Research such as [18] argues that cyber resilience in an organization is a crucial activity to ensure competitive business advantages. Likewise, [19] states that cyber resilience has gained high importance due to its influence on the continuity of operations in the business sector. In the same sense, [20] indicates that cyber resilience focuses on a subset of responses to incidents in the detection and analysis phases.

On the other hand, in dimension 4: Evolve. It can be mentioned that no gap was found in the Configuration and Change Management (CC) domain because the SME adequately uses a configuration management procedure for equipment that is linked to the main service system. In the same sense, positive results were obtained in the communication domain (CM) as a response to the definition and establishment of effective mechanisms with the suppliers, clients, and users of the organization, making them participants in the training to create awareness of applying regulations and therefore good practices related to cybersecurity to prevent cyberattacks. This finding coincides with [10], who argue that it is necessary to create awareness, and establish cyber security measures that guarantee adequate levels of protection throughout the entire value chain. Likewise, [9] affirms that cybernetic resilience is relevant as a prevention and security mechanism throughout the organization.

Finally, regarding the importance of applying a regulatory framework to improve cyber resilience, it responds to the application of good practices in the business processes of organizations regardless of their size. This makes it possible to protect assets, mitigate risks, and prevent cyberattacks that affect the normal development of SME operations. This finding coincides with what was mentioned by [8]; who maintains that cyber resilience is a relevant factor when protecting the data stored in an organization. It also states that cyber resilience must support management. Likewise, [14] says that cyber resilience is a growing concern that all members of an organization must address.

V. CONCLUSIONS AND FUTURE RESEARCH

Regarding the results, it can be mentioned that:

Regarding the implementation of a regulatory framework to anticipate cyber resilience in an SME, it is relevant to consider the control objectives of the functional domains: Cybersecurity Policies (PC), Risk Management (GR), Cybersecurity Training (FO) so that with the implementation of pertinent procedures, risks associated with the main service are managed in a timely manner, as well as having an updated asset inventory and constant monitoring, knowing the impact and probability that it would cause if any interruption occurred, as well as the approach of strategies to face cyberattacks. The implementation of a cyber resilience training plan aimed at employees involved with the main service of the company is crucial to avoid social engineering attacks.

Regarding the implementation of a regulatory framework to resist cyber resilience in an SME, it is extremely important to apply procedures for vulnerability management (VM) using specialized tools and applying effective strategies that allow the identification of vulnerabilities in assets, so that they can be Prioritize those that have a direct impact on the main service and are managed in a timely manner. Likewise, in the Continuous Supervision (SC) domain, it is necessary to involve external providers in order to report potential cybersecurity events that affect the service.

In relation to the implementation of a regulatory framework to recover cyber resilience in an SME, the Incident Management (IG) domain should be considered since when implementing cyber incident identification procedures so that they can be classified and typified according to the regulations; based on this, provide an appropriate response in the shortest possible time. In the Service Continuity Management (SC) domain, it is necessary to establish a continuity plan to guarantee the validity of the company's main service.

Regarding implementing a regulatory framework to evolve cyber resilience in an SME, consider Configuration and Change Management (CC) using a relevant configuration management procedure for assets linked to the main service system. In the Communication (CM) domain, defining and establishing effective communication mechanisms with suppliers, customers, and users regarding cyber resilience issues is necessary.

The inferential results show that there are significant differences between the post and pre test, which allows us to affirm that the implementation of a regulatory framework improves cyber resilience, as well as the dimensions of anticipating, resisting, recovering and evolving.

The implementation of a regulatory framework for cyber resilience in SMEs is recommended in order to provide business continuity, for this it is relevant to carry out a situational study that allows identifying the current situation of the control objectives and after an analysis, the actions are prioritized. improvement in functional domains to mitigate risks of cyberattacks.

As future research, other study scenarios can be considered, for example, organizations from different fields and number of collaborators. In such a way that different areas can be studied and thus obtain a greater diversity of results.

ACKNOWLEDGMENT

We would like to thank the Universidad Autónoma del Perú, Universidad Nacional Mayor de San Mayor,Tecnológico de Monterrey – campus Morelia, KLE Institute Technology for their support of our work. Also, to COLTRANSA Company for allowing us to apply our research in this organization.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6337
***Article Received**: 29 December 2022 **Revised**: 30 January 2023 **Accepted**: 12 February 2023*

REFERENCES

[1] IBM Security, "Cyber Resilient Organization Report," Ibm, 2020.

[2] Joint Publication ENISA and CERT-EU, "Boosting your Organisation's Cyber Resilience," vol. 22–01, pp. 1–5, 2022.

[3] Centro Criptológico Nacional, "CCN-CERT IA-24-22 - Ciberamenazas y tendencias," Https://Medium.Com/, 2022, [Online]. Available: https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf

[4] Kaspersky, "Cyber-resilience during a crisis: How are Small and Medium businesses staying security-prepared in an unpredictable market?," 2022. [Online]. Available: https://www.kaspersky.com/blog/smb-cyber-resilience-report-2022/

[5] T. Godbole, S. Gochhait, and D. Ghosh, "Developing a framework to measure cyber resilience behaviour of indian bank employees," pp. 299–309, 2022, doi: 10.1007/978-981-16-4177-0_31.

[6] R. Faleiro, L. Pan, Pokhrel, S. R., and R. Doss, "Digital twin for Cybersecurity: Towards enhancing cyber resilience," pp. 57–76, 2022, doi: 10.1007/978-3-030-93479-8_4.

[7] E. Vogel, Z. Dyka, D. Klann, and P. Langendörfer, "Resilience in the Cyberworld: Definitions, Features and Models," Futur. Internet, vol. 13, no. 11, p. 293, 2021, doi: 10.3390/fi13110293.

[8] D. Jaramillo, K. Romero, and C. Ramos, "Security framework for mobile application development and its contribution to cyberresilience," RISTI - Rev. Iber. Sist. e Tecnol. Inf., vol. 2021, no. E42, pp. 442–458, 2021.

[9] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, and D. Ageyev, "Redundancy cyber resiliency technique based on fast ReRouting under security metric," 2021, doi: 10.1109/PICST51311.2020.9468072.

[10] Gajek S., L. M., and J. C., "IIoT and cyber-resilience: Could blockchain have thwarted the Stuxnet attack?," AI Soc., vol. 36, no. 3, pp. 725–73, 2021, doi: 10.1007/s00146-020-01023-w.

[11] A. Tiwari, R. A. L. Narasimha, and S. Bukkapatnam, "Cybersecurity assurance in the emerging manufacturing-as-a-service (MaaS) paradigm: A lesson from the video streaming industry," Smart Sustain. Manuf. Syst., vol. 4, no. 3, 2020, doi: 10.1520/SSMS20200066.

[12] X. Liang, C. Konstantinou, S. Shetty, E. Bandara, and R. Sol, "Decentralizing Cyber Physical Systems for Resilience: An Innovative Case Study from A Cybersecurity Perspective," Informática y Segur., vol. 124, 2023, doi: 10.1016/j.cose.2022.102953.

[13] M. T. Ralekgokgo, M. Velempini, and S. S. Mapunya, "Malicious Packet Injection on Software-Defined Networking as a Strategy to Improve Security," in 7th International Congress on Information and Communication Technology, ICICT 2022, 2023, pp. v–vi. doi: 10.1007/978-981-19-2397-5_1.

[14] D. Dagdilelis, M. Blanke, R. H. Andersen, and R. Galeazzi, "Cyber-resilience for marine navigation by information fusion and change detection," Ocean Eng., vol. 266, 2022, doi: 10.1016/j.oceaneng.2022.112605.

[15] Goldstein J.C. and Goldstein H.V., "Intraoperative cyberattacks: cyberthreat awareness and cyber-resilience strategies in anesthesia," Can. J. Anesth., vol. 68, no. 12, pp. 1838–1839, 2021, doi: 10.1007/s12630-021-02102-2.

[16] J. Groenendaal and I. Helsloot, "Cyber resilience during the COVID-19 pandemic crisis: A case study," J. Contingencies Cris. Manag., vol. 29, no. 4, pp. 439–444, 2021, doi: 10.1111/1468-5973.12360.

[17] L. S. . Rodriguez-Baca, R. L. . Larrea-Serquen, C. F. Cruzado, M. ;Alarcon-Diaz, S. E. ;Garcia- Hernandez, and J. ;Pebe-Espinoza, "Business Cybersecurity. Case study in Peruvian and Mexican SMEs," 2022. doi: 10.1109/INCET54531.2022.9824900.

[18] S. Rahman, N. U. I. Hossain, K. Govindan, F. Nur, and M. Bappy, "Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain," CIRP J. Manuf. Sci. Technol., vol. 35, pp. 911–928, 2021, doi: 10.1016/j.cirpj.2021.09.008.

[19] A. Kott, M. S. Golan, B. D. Trump, and I. Linkov, "Cyber Resilience: By Design or by Intervention?," Computer (Long. Beach. Calif)., vol. 54, no. 8, pp. 112–117, 2021, doi: 10.1109/MC.2021.3082836.

[20] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and C. Maple, "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review," Smart Cities, vol. 3, no. 3, pp. 894–927, 2020, doi: 10.3390/smartcities3030046.

[21] INCIBE, "Indicadores para Mejora de la Ciberresiliencia (IMC)," no. Imc, pp. 1–17, 2020, [Online]. Available: https://www.incibe-cert.es/guias-y-estudios/guias/imc-indicadores-mejora-ciberresiliencia