Cybersecurity diagnosis project in a software services SME and the organizational change management.

Daniel Ballén [1], Andrés Mauricio Paredes [2], Ruth Karina Duque Zúñiga [3], Ana María Orozco Vargas [4]

1. *Corporación Universitaria Minuto de Dios; jballenbric@uniminuto.edu.co; ORCID*
2. *Universidad del Valle; andres.paredes@correounivalle.edu.co; ORCID*
3. *Corporación Universitaria Minuto de Dios; ruth.duque@uniminuto.edu.co; ORCID*
4. *Corporación Universitaria Minuto de Dios; ana.orozco@uniminuto.edu.co; ORCID*

Abstract: Cybersecurity is a fundamental process for the continuity of operations in 21st century organizations. In the case of Latin American SME, cybersecurity is occasionally neglected and are priories the activities of product development and sales. This paper study a cybersecurity diagnosis project for a Colombian SME of software services. In the initial phase, the identification of information assets is carried out. Subsequently, the risks in information management, as well as the effectiveness of control measures, will be evaluated. For the success of this project, in addition to the cybersecurity disciplinary component, a methodological tool is required to manage this organizational paradigm shift. This will be proposed through the PMI's Practical Guide for Change in Organizations. With this study case, it is intended to understand how this SME valued its cybersecurity challenges and based on this diagnosis, to propose an actionable plan in accordance with international standards, the company's context and practical tool for this organizational change.

Keywords: project management; change management; cybersecurity; ISO-27000; SME.

Proyecto del diagnóstico en ciberseguridad de una PYME de servicios de software y la gestión del cambio organizacional.

Resumen: La ciberseguridad es fundamental para la continuidad de las operaciones en las organizaciones del siglo XXI. En el caso particular de las PYMES latinoamericanas, ocasionalmente la ciberseguridad es descuidada y se priorizan las actividades de desarrollo de productos y las ventas. En este trabajo se estudia un proyecto de diagnóstico en ciberseguridad para una PYME colombiana de servicios de software. En la fase inicial se realiza la identificación de los activos de información, posteriormente se evaluarán los riesgos en la gestión de la información, así como la efectividad de las medidas de control. Para el éxito de este proyecto, además del componente disciplinar en ciberseguridad es requerida una herramienta metodológica para gestionar este cambio de paradigma organizacional, y esto se propondrá a través de la Guía Práctica para el cambio en las organizaciones del PMI. Con este estudio de caso se pretende entender como esta PYME valoraba sus desafíos en ciberseguridad y a partir de este diagnóstico proponer un plan realizable de acuerdo con los estándares internacionales, el contexto de la empresa y una herramienta practica para el cambio organizacional.

Palabras clave: gestión de proyectos; gestión del cambio; ciberseguridad; ISO-27000; PYME

Introduction

Cybersecurity challenges for SME in Latin America

For Latin America, SME represent 90% of the business population and 55% of the GDP of its economy. [1] With this in context, it can be said that if the cybersecurity of SME is affected then the economy of Latin America will be significantly impacted. Currently, SME have a very large attack surface [2]. So, the implementation of cybersecurity controls helps as countermeasures to detect, prevent, reduce or counteract risks. However, many SME do not have sufficient resources to implement cybersecurity due to lack of leadership support or lack of technical skills. [3]

SME are using digital technologies to change a model company's business in a way that provides new revenue and value creation options, while digital business models also enable scalability and rapid cross-border expansion. Likewise, there must be a cybersecurity practice that allows the company to avoid accidents and provide security in aspects such as: email encryption, security patches, authentication solutions and have measures to mitigate gaps in cybersecurity [4]

The SME companies that establish a security capabilities and security standardization saves the company money and time, thus allowing it to identify areas for improvement and increase compliance with international standards. [5]

A special case of cybersecurity challenge is where different layers of technologies are combined, such as the Industrial Internet of Things, the control of physical systems and the modeling of the interaction between humans and cyber physical systems, where Industry 4.0 must prepare for the digitalization of processes, smart manufacturing, and connectivity between companies, which will allow organizations to satisfy customer requirements and create value opportunities. At the same time, increase resource productivity and provide flexibility in business processes. The research found that the successful adaptation of Site technologies is highly dependent on cyber resources. This specifically affects SME, as they do not have the same supply chain resources as large companies. [6]

the interaction of the internet in developing countries, considering that SME are seen as the vehicle for employment and job creation, but also because cybersecurity in this is limited. This study is a contribution to addressing this gap. They are constant cyber-attacks, as they are found. Since many of the most SME companies will not spend money on independent security tests because they are too expensive and they do not have that amount, the intention is to use open-source software. [7]

The adoption of Industry 4.0 can bring many benefits to SME, such as greater efficiency, better responsiveness to market demand, reduced production costs, better quality of products and service, as well as greater competitiveness, but also represents a great change in thinking about production due to the interconnection of devices, machines and systems through the Internet of Things and the cloud, which is why the article highlights the most important technologies and elements of Industry 4.0, such as artificial intelligence, process automation, robotics collaborative, virtual and augmented reality, cybersecurity and systems interoperability.[8] At the same time, the main challenges that arise in the Industry 4.0 environment, such as the adaptation of workers to new technologies and the need to implement cybersecurity strategies to protect data and network systems. [9]

Improvement cybersecurity in SME

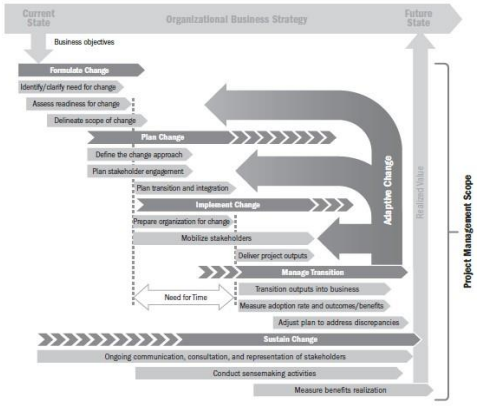
The recommended start of a cybersecurity improvement project is to train the employees in cybersecurity, create disaster recovery plans, periodically update the systems and software, and seek advice from cybersecurity experts. [10] also the use of cybersecurity assessment tools provides practical recommendations for each potential gap and also provide a cost/benefit score, additionally, it will not only help identify strengths and weaknesses, but also make best practice recommendations on how to plug security gaps effectively. Finally, it is noted that cybersecurity preparation is key to organizational survival and growth. [11]

The improvement of cybersecurity can also be developed with a national approach, such is the case of Taiwan where the creation of a central authority responsible for the development of cybersecurity policies and strategies, as well as the development of standards and guidelines for implementation of cybersecurity measures in all organizations and companies in the country. In addition, the central authority could conduct periodic cybersecurity audits and assessments to ensure compliance with established standards and at the same time this strategy is expected to strengthen the country's cybersecurity and protect national interests from increasingly sophisticated cyber threats. [12]

PMI Change management: a practice guide

The proposed framework for the change management is the methodological tool for support the cybersecurity improvement project, the first step is clarifying the reason because the organization need this change and delineate the scope of the change. It's necessary define the change approach and the plan to engage the stakeholders. For implement the change in this case a better cybersecurity model for a SME is necessary mobilize the stakeholders and prepare the organization for change with a clear set of Delivery project outputs. All organization change process is adaptive in accordance with the real execution, for this reason the transition will be managed in outputs for the business, the necessary measurement of the adoption and benefits and finally, the changes and adjust the plan to address discrepancies. [13]

Figure 1. PMI Framework for organizational change



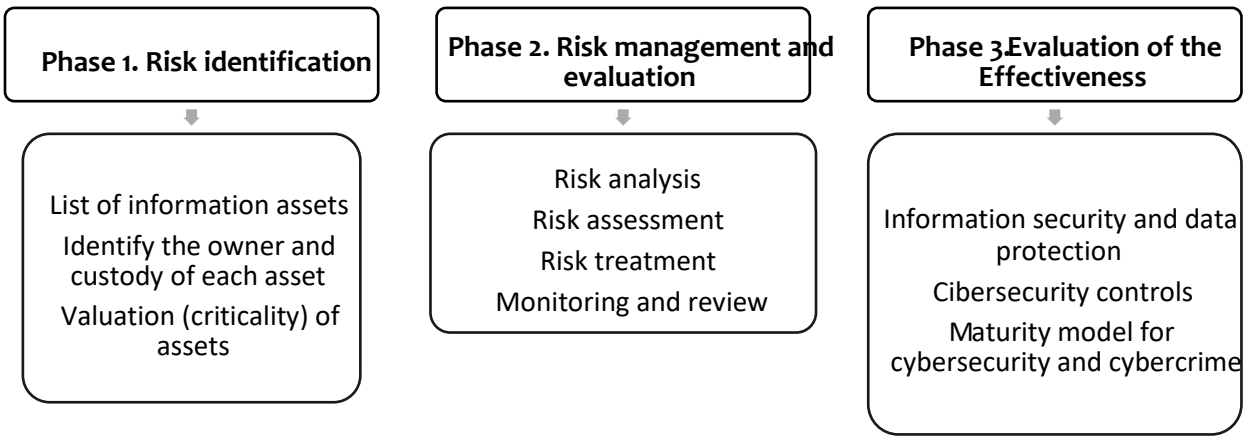
Source: Managing Change in Organizations: A Practice Guide. Project Management Institute. [13]

1. Methodology

The methodology used in the research is coherent with ISO 27005 Risk Management of Information Security Framework and is comprehensive to address the objective of identifying the information assets of the SME [14], and its valuation. Below, it's necessary the analysis, assessment and control of threats and risk. Finally, it is necessary to propose cybersecurity controls and determine its cybersecurity organizational maturity model. Figure 1 presents the methodological phases proposed for the research. This project is part of the initiative *Hackers Wanted* of the **Universidad EAN** applied to its SME started with the entrepreneurship program *EAN Impacta*, for this case, this cybersecurity improvement project is applied to *Ancla Support SAS* (www.anclasupport.com) an SME for software services placed in Guadalajara de Buga (Colombia southwest) with the propose to sell industrial software for industrial knowledge management.

The technical standard ISO 27005 defines general principles and guidelines for information security risk management. The standard consists of six main parts, including introduction, scope, terms and definitions, risk management principles, framework and risk management process. The risk management principles section defines the basic principles of risk management, such as accountability, transparency, and continuous improvement. The framework, on the other hand, presents an approach to information security risk management based on risk identification, analysis, evaluation and treatment [14]. Finally, the risk management process defines the specific steps that must be followed to implement the risk management framework. These steps include communication and consultation, context, risk identification, risk analysis, risk assessment, risk management, risk acceptance, and continuous monitoring and review of the risk management process [15].

Figure 1. Methodological process of the research



Phase 1. Risk identification

This stage begins with data collection, for which the list of information assets of the SME and identify the owner and custody of each information asset, in addition to value that assets. This valuation is applied to an only SME called Ancla Support SAS and its principal product: KM2S a registered software of Industrial knowledge management.

Phase 2. Risk management and evaluation.

At this phase, a risk analysis, assessment, and proposal for treatment together a monitoring and review protocol, given that cyber threats are updated very frequently.

Phase 3. Evaluation of the Effectiveness.

In this final phase, protocols for information and data security are stablish as well as cybersecurity controls through projects that can be implemented soon of the organization [16].

2. Results

Phase 1. Risk identification

Firstly, an assessment of the existing information assets and controls was carried out, where initially an identification of the risk, the description of the control, the person responsible, periodicity of execution and the purpose of the control were carried out, see table 1.

Table 1. Risk identification and valuation.

ITEM	Associated risk	Proccess	Owner	Causes
1	Loss of integrity and availability of software installed and configured in the provider's technological infrastructure	Infraestructure	Infraestruture Leader	Platform attacks
				Changes without control
				Conectivity failures
				Failures in the perimeter security infrastructure provided by Cloud
				Coding alteration
2	Loss of confidentiality, integrity and availability of information processed in technological systems and services (Email, information systems, applications,	Development and Infraestructure	Development Leader	Platform attacks
				Insufficient capacity of technological resources (memory, processing, storage and connectivity).
				Failure to comply with specific information security policies.
				Inadequate management of technical vulnerabilities.

	cloud provider servers).			Technological systems and services without redundancy or high availability.
				disabled antivirus.
				Weaknesses in the appropriation of the information security culture.
				Leave the computer session unlocked when leaving the workplace.
3	Unavailability on the part of collaborators who perform critical tasks	Development	Development Leader	Absence of collaborators due to any administrative situation (Disability, vacations, licenses). Critical staff without backup. Absence of information transfer.
4	Unauthorized access or hijacking of information stored and/or transmitted through electronic messaging	Development and Infraestructure	Development Leader	Inadequate email control access
				Social engineering attacks via email by the entity's officials/contractors

Phase 2. Risk management and evaluation.

This phase consists of risk analysis, which is carried out by identifying Threats it is the potential cause of an unwanted incident, identifying vulnerability that represents the weakness of an asset and finally identifying Consequences these are the economic effects or reputations resulting from the materialization of the risk that impact the processes. finally, a risk management matrix was created, considering

the probability, impact, evaluation and level of inherent risks, analysis and evaluation of residual risk, acceptance criteria [17]. See table 2.

This part focuses on the evaluation of risks through different analyses: Probability: It is the frequency carried out by the process. Impact: It is the set of consequences that causes the materialization of a risk. On the other hand, an evaluation of inherent and residual risks is made. At this stage, the acceptable risk level defined for the information security risks and the area of residual risk, at the same time monitoring and review is carried out, which refers to the information security risk management process.

Table 2. Risk valuation

ITEM	**Associated RISK**	**Risk Valuation**	**Risk Level**	**Final**
1	Loss of integrity and availability of software installed and configured in the provider's technological infrastructure.	4	Medium	Not acceptable
2	Loss of confidentiality, integrity and availability of information processed in technological systems and services (Email, information systems, applications, cloud provider servers).	6	High	Not acceptable
3	Unavailability on the part of collaborators who perform critical tasks	1	Low	Acceptable
4	Unauthorized access or hijacking of information stored and/or transmitted through electronic messaging	4	Medium	Not acceptable

Phase 3. Evaluation of the Effectiveness.

In this phase it analyzes the information collected and has different conditions: requirement id, position, requirement, sheet, element, qualification obtained, level 1 (initial), initial level compliance, level 2 (managed) compliance level of managed, level 3 (defined), compliance level defined, level 4 (quantitatively managed), compliance level managed quantitatively, level 5 (optimized), compliance level optimized.

To finish this part of the information, a general table is established where the plan to follow and the organization to achieve it are established. Therefore, the following factors are taken into account: name of the recommended project, approximate duration of the project (established in months) and recommended order of implementation. This in order to be able to specify within the established deadlines whether what was proposed was fulfilled, to improve security in the study company. See table 3.

Mainly, the objective of the project presented by the initiative *Hackers Wanted*, which sets out the following: Provide cybersecurity support for businesses in this case *Ancla Support SAS*, which aims to suggest to the business the activities that allow it to comply with current regulations in terms of protection of personal data and the security of the technological platform that supports it. Finally, regarding the evaluation of the Effectiveness of Cybersecurity Controls, it is stated that the *Ancla Support SAS* is currently in the initial stage of each of the phases of the cybersecurity model based on the NIST standard.

Table 3. Gap identification and prioritized solution projects

Recommended Order of Implementation	**Projects description**	**Timelapse**
1	ISO - 9001 Implementation	6 months
2	Implementation of standards regarding the Protection of personal data (Based on the Law 1581:2012 standard)	6 months
3	Implementation of Information Security standards or models such as (MSPI and ISO 27000)	4 months
4	Definition and Implementation of life cycle guides framed in PDCA processes (comes from the acronym Plan, Do, Check and Act), based on standards (ISO 27003:2017)	3 Month
5	Implementation of good practices in Information Security based on standards such as (ISO 27001:2013 and ISO 27002:2013)	6 months

6	Implement good practices in software development according to what is recommended in the standards (Agile methodologies such as ITIL and SCRUM, OWASP, ISO 27034)	3 Months
7	Execution of internal audits, in order to carry out periodic reviews of the projects and controls implemented within the enterprise.	1 Mounth
8	Implementation of mechanisms to guarantee the security of remote work teams	2 Mounths
9	Execution of activities corresponding to managing technical vulnerabilities based on the risks that may arise in the core applications of the enterprise.	3 Mounths
10	Implementation of the Approximate Cybersecurity and Cybercrime Model	6 Mounths

3. Discussion

Regarding cybersecurity improvement strategies, it highlights the importance of innovation and research in the field of cybersecurity in the development of more efficient and effective information security solutions, at the same time highlighting the need to invest more in cybersecurity training and awareness, especially SME. In other words, industrial cybersecurity policy as a key tool to protect critical infrastructure and the economy against cyber threats, emphasizing the need to continue improving and updating as cyber threats and technology evolve. [18]

The data source of a SME shall be analyzed because any source information can vary depending on server or network activity, and command logs and application logs are common sources of analytical information. To avoid data that requires analysis, most identification systems store data for a period. For later reference. The results show that in general SMEs are adopting cloud computing solutions and open-source software, and the pressure to emulate is widely accepted. [19]

Without regulatory pressures, small businesses may operate without the institutional legitimacy necessary to access a wide variety of resources within the environment [20].

Organizational legitimacy is achieved when you meet and address organizational pressures that can shape your behavior, such as how cybersecurity is adopted and implemented. [21]

4. Conclusions

For the case of *Ancla Support SAS, this SME* is currently in the initial stage of each of the phases of the cybersecurity model based on the NIST standard. However, the proposed project has allowed the company to identify its cybersecurity risks. Likewise, the improvement cybersecurity project has allowed the assessment of risk with the purpose of prioritizing decisions and resources to make its cybersecurity maturity.

The cybersecurity identified risks were loss of integrity and availability of the software, loss of confidentiality, unauthorized access, or hijacking. All these risks have been classified as high or medium and are not acceptable for the integrity of the company. The only acceptable risk is the unavailability on the part of collaborators who perform critical. All these risks are associated to the development and infrastructure process.

The route the cybersecurity improvement is made up of the following projects, which are described according to their priority: ISO - 9001 implementation, implementation of standards regarding the protection of personal data (Based on the Law 1581:2012 standard), implementation of Information Security standards or models such as (MSPI and ISO 27000), definition and implementation of life cycle guides framed in PDCA processes, implementation of good practices in Information security based on standards such as (ISO 27001:2013 and ISO 27002:2013), implement good practices in software development according to what is recommended in the standards (agile methodologies such as ITIL and SCRUM), execution of internal audits, in order to carry out periodic reviews of the projects and controls implemented within the enterprise, implementation of mechanisms to guarantee the security of remote work teams, execution of activities corresponding to managing technical vulnerabilities based on the risks that may arise in the core applications of the enterprise and finally the implementation of the Approximate Cybersecurity and Cybercrime Model.

The proposed projects for close the gap are coherent with the maturity of the company and it is expected that results will be obtained within reasonable times and deadlines. Finally, a solid cybersecurity requires that, in addition to the proposed projects, the organizational change management route proposed by the PMI is implemented, that is, clearly define the expected change and outline its scope, define the plan to connect the stakeholders, as well as the transition and integration plan and finally implement and sustain the change.

5. References

[1] Matilde-Espino, L.R. (2022). Análisis bibliométrico de la producción, científica sobre México en temas de ciberseguridad (2015-2020). CIENCIA ergo-sum, Revista Científica, 16.

[2] Alarcón Aldana, A. (2011). Guía para pymes desarrolladoras de software, basada en la norma ISO/IEC 15504. Revista Virtual Universidad Católica del Norte, 30.

[3] Ozkan, M. S. (2022). Adaptable Security Maturity Assessment and Standardization for Digital SME. Journal of Computer Information Systems , 23.

[4] Pawar, S., & Palivela, H. (2022). LCCI: un marco para implementar controles mínimos de ciberseguridad para pequeñas y medianas empresas (PYME). ELSEVIER, 13.

[5] Westerlund, M. (2020). Digitalización, Internacionalización y Escalamiento de pymes online. Technology Innovation Management Review, 10.

[6] Ozkan, M. S. (2019). Modelado de seguridad de la información adaptativa para pymes en un clúster. Revista de Capital Intelectual, 22.

[7] Melnyk, S. (2021). New challenges in supply chain management: cybersecurity across the supply chain. International Journal of Production Research , 21

[8] Mercado, E. B. (2022). Propuesta de adopción de tecnologías Propuesta de adopción de tecnologías mexicanas. CIENCIAS SOCIALES, HUMANIDADES Y ARTES, 28.

[9] Yunzunza Cortés, C. (2017). El Entorno de la Industria 4.0: Implicaciones y Perspectivas Futuras. Conciencia Tecnológica, 19.

[10] Salah Kabanda, M. T. (2018). Exploring SME cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce, 14

[11] Benza, M. (2020). ¿Riesgo calculado? Una herramienta de evaluación de la ciberseguridad para las pymes. ELSEVIER, 10.

[12] Tien-Shen Li, H. H. (2018). A centralised cybersecurity strategy for Taiwan. Journal of Cyber Policy , 18.

[13] PMI. (2013). Managing Change in Organizations: A Practice Guide. Project Management Institute.

[14] Bustamante García, S. (2021). Políticas basadas en la ISO 27001: 2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. ENFOQUE, 12.XXX

[15] Garzás, J. (2009). Una aplicación de ISO/IEC 15504 para la evaluación por niveles de madurez de PYMEs y pequeños equipos de desarrollo. Revista Española de Innovación, calidad e Ingeniería del Software, 12.

[16] Bustamante, S. (2020). Factores que contribuyen en la pérdida de información en las organizaciones . Revista Cubana de Ciencias Informáticas, 20

[17] Carías, J. (2019). Enfoque sistemático para la operacionalización de la resiliencia cibernética en las pymes. IEE Access,
22.

[18] Timmers, P. (2019). The European Union's cybersecurity industrial policy. Journal of Cyber Policy, 21 [19] Roldán Molina, G. (2017). A Comparison of Cybersecurity Risk Analysis Tools. ELSEVIER, 8.

[20] Flores Canto, F. P. (2021). Desafíos del Liderazgo Transformacional en asuntos de Ciberseguridad organizacional. Revista Venezolana en gerencia , 14.

[21] Radanliev, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. Cybersecurity, 21