Ricardo Díaz Sánchez, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 12, Issue 11, November 2022, pp. 221-226

RESEARCH ARTICLE OPEN ACCESS

Minimum Cybersecurity Framework for Industry 4.0/SMEs

Ricardo Díaz Sánchez*, Gerardo Rodríguez Barba**
**Posgrados CIATEQ/Tecnológico Nacional de México/Instituto Tecnológico de Querétaro, Av. Tecnológico S/N Esquina Mariano Escobedo, Col. Centro, Querétaro, Qro. 76000. México.*
***(CIATEQ, Nodo Servidor Público 165 Col. Anexo Club de Golf. Las Lomas. Zapopan, Jal. C.P. 45136. México.*

ABSTRACT
The NIST CSF v1.1 cybersecurity framework is a fairly robust framework, well developed and accepted by many companies from different sectors around the world. However, for an SME company, its use and implementation become very complicated. For this reason, this article proposes the creation of a minimum cybersecurity framework based on the NIST CSF v1.1, suitable for an SME company, which has few human and material resources for its implementation.
Keywords – Industry 4.0, Security, Cybersecurity, Cybersecurity Program.

Date of Submission: 15-11-2022 Date of Acceptance: 30-11-2022

I. Introduction

The 4th Industrial Revolution has brought many benefits and challenges that companies have to face in relation to cybersecurity. Among the domains currently accepted in the 4th Industrial Revolution are automation, digitization, and information [1]. Regarding digitization, we can find the areas of economy, society, industry, services, and education. The response to digitization in the industrial domain is known as Industry 4.0, considered as a special case of digitization. Therefore, Industry 4.0 faces great cybersecurity challenges from technical, governance, social, legal, and regulatory perspectives.

The work to be developed focuses on the challenges, in particular how to face them from the technical perspective of Mexico. This can be the starting point to develop projects that satisfy the requirements in the mentioned areas. According to CANIETI [2] "it has been shown that organizations that implement risk-managed cybersecurity programs have lower costs associated with cyber incidents."

Most companies in México do not have a cybersecurity program, with high costs associated with cybersecurity incidents. In México, in particular, since 2017 through the National Cybersecurity Strategy (ENCS) [3], proposed by the government of the Mexican Republic, the integration of a front to combat cybersecurity problems began, and established this document as strategic in terms of cybersecurity. This proposal did not mature. However, it was not until October 2021, when the document "National Homologated Protocol for Cyber Incident Management" was published through the National Guard under the Ministry of Security and Citizen Protection [4]. The National Guard is the coordinating body for cybersecurity, currently in Mexico. There is still no collaboration between the different sectors in the social, economic and political spheres, and the risks, threats, attacks, vulnerabilities that industry 4.0 faces are not dimensioned, there is not enough trained personnel for cybersecurity requirements, and lack of cybersecurity culture.

Among the problems faced by those who work in cybersecurity in Industry 4.0 are: the lack of integration and cooperation between the stakeholders [5] of the organizations, for not having a common language, as there are many disciplines with different types of experts, and multiplicity of technologies, in addition to attacks, security risks and vulnerabilities. The convergence of Information

Technologies (IT) and Operational Technologies (OT), have come to increase the problem of integration in the development of projects in Industry 4.0.

The lack of a regulatory framework in the area of cybersecurity has been observed in Industry 4.0/SMEs organizations. In order for Industry 4.0 to reach its full potential, traditional cybersecurity problems must be overcome along with the problems of Industry 4.0 [5].

It is necessary to have a minimum integrated framework that helps to define the scope and functions in the companies, so that these functions and responsibilities do not remain untraceable in the event of an incident related to unauthorized access to data, and its traceability cannot be recognized within organizations.

II. State of the Art

The landscape in Mexico in terms of cybersecurity has been analyzed by the government (ENCS), national organizations (IFT, CANIETI [2]), international organizations (OAS, IDB), and they have agreed that the development of a national cybersecurity strategy based on analysis of risks is the most advisable to elaborate.

Mexico, like other countries, has developed a National Cybersecurity Strategy (ENCS) [3], helped by the OAS at the end of 2017. The Federal Institute of Telecommunications (IFT), joins the ENCS in 2018 to achieve the objectives of the strategy. However, says Patricio Garza [6], "this strategy failed to become a binding document, much less a true State policy". Although this strategy did not prosper, Garza continues, "it was the first step to position the issue on the government's agenda."

It was until October 2021, when the Presidency of the Republic published the document, Homologated National Protocol for Cyber Incident Management. After analyzing various frameworks [4], it decides to use the NIST CSF v1.1, NIST 800-61, the ENISA (European Network and Information Security Agency) Best Practices Guide for Incident Management as the basis for its development.

A study by the Inter-American Development Bank (IDB) [7], and the Organization of American States (OAS) in 2020, cites "this study shows that the Latin American and Caribbean region is not yet sufficiently prepared to face the attacks that occur in cyberspace", and recommends that Mexico should focus on improving the deployment of cybersecurity standards and technical controls.

Another data of interest is published by the International Communications Union (ITU), the Global Cybersecurity Index [8], this aims to help countries identify areas for improvement in the field of cybersecurity and encourage them to take action in these areas, in its 2020 report, it places Mexico in 56th place out of 182 countries. Resulting in areas of opportunity for improvement in the cybersecurity area for Mexico.

Finally, in Mexico with the entry of the Free Trade Agreement between Mexico, the United States and Canada (T-MEC) from July 1, 2020 [9], it includes provisions on cybersecurity, in its article 19.15: Cybersecurity, that it has to comply with and it is necessary to consolidate in order to comply with this requirement.

III. Methodology

This section explains how to make use of the NIST CSF v1.1 framework [10] and the steps used to generate a Minimum Cybersecurity Framework for an Industry 4.0/SME enterprise. In the first place, a bibliographic review of the topics related to the work to be developed was carried out. The results of the search were used for the development of this work, in the same way the references were used for its elaboration and the citations are included, where appropriate, and added to the references.

To carry out the proposal, an Industry 4.0 company from the auto parts industry was selected, located in Apaseo el Grande in the State of Guanajuato in an industrial park. In particular, the self-assessment applies to the business network. Company-specific data is not provided for reasons of confidentiality.

Fig.1 shows the process in a general way:

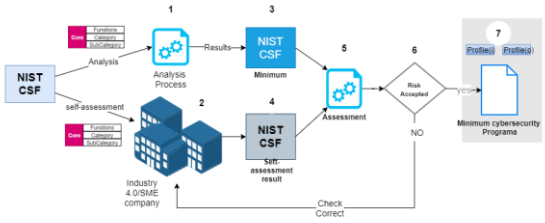

Figure. 1. Methodology used to generate the minimum cybersecurity framework.

The steps carried out to prepare the proposal for the minimum cybersecurity framework are shown below:

1. The core component of NIST CSF v1.1 is used as the entry point to the analysis process. In this process of analysis, the current regulations of the industry under study, the bibliography analyzed, and personal experience will be used as selection criteria for the subcategories.
2. In the part of the company that is being analyzed, the core component will be assigned so that a self-assessment of the corresponding subcategories is carried out according to the personnel in charge of the cybersecurity area.
3. This analysis process will generate a minimum framework as a result. Fig. 1 shows the entire process.
4. The result of this self-assessment was contrasted with the minimum framework of point 3.
5. The evaluation was carried out for the analysis of the results obtained.
6. Together with the case study company, they analyzed whether these results were acceptable to the organization. If they were not acceptable, it was iterated to review and reassess, returning to step 2.
7. At the end of the iterations, the minimum cybersecurity framework was generated for the company in the case study. An initial profile (i) and an objective profile (o/Proposal) were obtained, the difference between Profile (o) minus Profile (i) resulted in the subcategories that should be included in the cybersecurity program of the company of the case study.

IV. Results

To start the process, a spreadsheet provided by the NIST CSF v1.1 framework is used as an initial reference, where all the components of the core part of the framework are included, Fig 2: functions (5), categories (23), and subcategories (108).

	Functions	Categories	Subcategories
1 Identify-ID	1	6	29
2 Proted-PR	1	6	39
3 Detect-DE	1	3	18
4 Response-RS	1	5	16
5 Recover-RC	1	3	6
	5	23	108

Figure 2. NIST Core Component summary.

As part of the development, this sheet is divided into different tabs so that the generated information can be properly managed. Fig. 3 shows the tabs that correspond to each function along with their categories and subcategories.

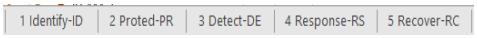

Figure 3. Tabs corresponding of the NIST CSF framework v1.1

For example: in Fig. 4, the content of the Identify (ID) function is shown, its category Asset Management (ID.AM), and its corresponding subcategories, each subcategory corresponds to a cybersecurity activity that has to be evaluated.

				Implementation Level (0,1,2,3,4)		1st Iteration
Function	Category	Subcategory	Target Profile Proposal	Initial Profile Current Profile	GAP	Enterprise Target
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1	4	3	1	4
		ID.AM-2	4	0	4	2
		ID.AM-3	4	0	4	2
		ID.AM-4	4	4	0	4
		ID.AM-5	4	3	1	4
		ID.AM-6	3	3	0	4

Figure. 4. Function description Identify-category Management Assets-Subcategories Framework NIST CSF v1.1.

Next, the content of each of the columns that contains each of the functions is defined.

4.1 Proposal (Target profile)

This value indicates the level that is proposed for the implementation of each of the subcategories. The value is proposed according to

the informative references proposed by the NIST CSF v1.1 reference framework. This value is obtained by reviewing the standards proposed for each subcategory, and only those that apply to this case study are selected.

4.2 Current Profile (Initial Profile)

This value was obtained from the self-assessment carried out by the staff of the company in the case study. The staff in charge selects the value for each subcategory. It was supported in the determination of concepts mentioned in each category, the level of implementation was determined by the person in charge of the area.

4.3 Gap

To determine the GAP, the following formula is used:

Proposal – Current Profile ……. (1)

For the GAP results, the following is proposed in Table 1:

Table 1: GAP, results.

Result	Description	Observations
Zero (0)	The proposal value and the current profile value were the same.	It is not required to implement security controls.
Positive number (1~4)	The proposal value is greater than the self-assessment value.	You have to assess if you want to stay at that level of implementation, or if you want to implement a security control to mitigate the risk. If you do not want to take the suggested level, you must document your justification and put it as an accepted risk, for the benefit of the company.
Negative number (-1) ~ (-4)	The proposal value was less than the self-assessment value.	Indicates that the level of implementation of the subcategory is above the proposal. No need to modify any controls.

4.4 Target

This value is the result of the first iteration and can take a value between 1-4 according to the description in Table 2. This value was determined by the company as a value that it wants to achieve for the improvement of its cybersecurity posture. This value can be improved in relation to the GAP found. If the company does not want to improve the GAP, it must be written that the improvement is not convenient for the company due to the cost benefit of the investment in the implementation and that level of risk found is accepted.

Table 2: Target, results.

Target	Description
Positive number (1~4)	The current profile must be increased. The company must assess to what level it wishes to increase it according to the recommendations of each subcategory. If you don't want to take it to the suggested level, you should document your justification and put it as an accepted risk, because that's in the company's interest.

4.6 charts

You can visually appreciate each of the categories and subcategories, and which of them is farthest from the target profile value (target). This difference is used by the company to determine if it wants to invest in the implementation of cybersecurity controls, or accept the risk of not implementing anything because the resulting investment is more expensive than the value of the loss in the event of a cybersecurity incident.

4.6.1 Bars

It shows the values of the Proposal, the Current profile, the GAP, and the Target profile. Graphically, it can be seen when the value of the Proposal is higher than the value of the current Profile for each of the functions, and their categories together with their subcategories. In the same way you can see the value of the Target profile and the current difference with the current profile.

4.6.2 Radar

Graph the value of the Proposal, the Current Profile. This graph helps to perceive clearly when the value of the Proposal is higher than the value of the Current Profile.

4.7 Current Profile and Target Profile

Next, the results of the graphs of each function of the core are shown together with their categories and their corresponding subcategories. The corresponding explanations are made where it has to be assessed if the company has to verify if the level of risk is accepted. If the level of risk is accepted, the justification in this regard must be left in writing. The resulting values in each function will form the current profile, and the target profile.

4.8 Identify function

Fig.5 shows the summary of the subcategories that make up the Identify function. Here you can see the difference between the target profile (proposal) and the Initial value.

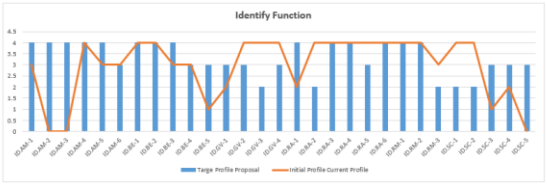

Figure. 5. Function description: Identify. Categories-Subcategories.

Fig. 6 shows the detail of each Asset Management subcategory. Here you can see the differences between the target profile (proposal) and the Initial value. On the radar plot, you can see a colored oval where you see the value of zero for the current profile, against the value of 4 for the proposal.

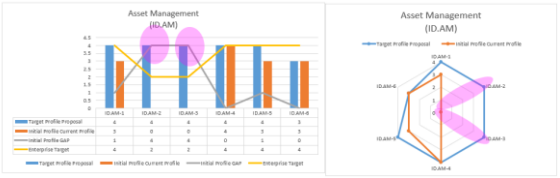

Figure 6. Function description: Identify. Category: Asset Management-Subcategories.

The subcategories ID.AM-2, ID.AM-3 have a current profile lower than the one proposed. The company has to assess whether it accepts that level of risk.

Recommendation: "To determine whether the company accepts this level of risk or not, the references of the standards that apply to this subcategory should be consulted. If you do not want to take them to the suggested level, you must document your justification and put it as an accepted risk, in order to suit the company".

For the remaining graphs, the same recommendation is made for all the subcategories where the current profile is less than the proposal.

V. Conclusion

Through the spreadsheet tool, it is possible to provide detailed visibility to the components of the cybersecurity program. Critical areas that need attention were identified, such as: ID.AM2, ID.AM-3, among others, already explained in the results analysis section. From the subcategories identified, it will be possible to prioritize in which areas it is necessary to implement security controls; to improve cybersecurity posture.

This document can serve as a basis for a Mexican SME to use as a baseline to start with cybersecurity posture.

REFERENCES

[1]. V. R. J. A. V. K. E. Kumar, Digital Transformation in Industry Trends, Management, Strategies (Springer Nature, 2021).

[2]. CANIETI, Evaluación de ciberseguridad en México: brechas y recomendaciones en un mundo hiper-conectado (CANIETI, Ciudad de México, 2017).

[3]. G. de la R. Mexicana, (2021, Aug, 15). Estrategia Nacional de Ciberseguridad, 2017. Retrieve from Gobierno de México: https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf

[4]. G. de la R. Mexicana, (2021, Dec 20). Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, 2021. Retrieve from Gobierno de México: https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

[5]. D. Thames, Lane. Schaefer, Cybersecurity for Industry 4.0. Analysis for Design and Manufacturing (Switzerland, Springer, 2017).

[6]. P. Garza, (2021, Dec 20). La ciberseguridad en México: ¿una necesidad?. Retrieve from KAS Blog: https://www.kas.de/es/web/mexiko/einzeltitel/

-/content/la-ciberseguridad-en-mexico-una-necesidad.

[7]. O, BID P. Garza, (2021, Dec 20). Ciberseguridad Riesgos, avances y el camino a seguir en América Latina y el Caribe. Retrieve from iadb org: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

[8]. Secretary of Foreign Relations, (2019). T-MEC. Retrieve from iadb org: https://dof.gob.mx/2020/SRE/T_MEC_290620.pdf.

[9]. ITU, (2021, Dec 20). Global Cybersecurity Index 2020. Retrieve from ITU org: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[10]. NIST, (2021, Jun 7). Framework for Improving Critical Infrastructure Cybersecurity, 2018. Retrieve from NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf