PUBLIC SUBMISSION

As of: 4/25/22 12:54 PM
Received: April 24, 2022
Status: Pending_Post
Tracking No. l2d-r5vr-l330
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0037
Comment on FR Doc # N/A

Submitter Information

Name: María Eugenia Corti
Ad [redacted]

Email: [redacted]

General Comment

See attached file(s)

Attachments

NISTFrameworkComments2022

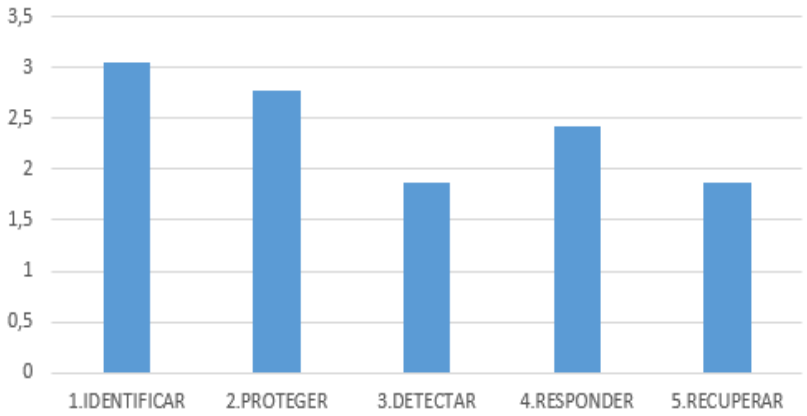
The comments made below to the NIST Cybersecurity Framework are based on the experience generated by supporting the development of the first version of a Uruguayan National Cybersecurity Framework, firmly based on the "Framework for Improving Critical Infrastructure Cybersecurity" from NIST and the analysis of the last published framework version.

Use of the Framework

NIST framework is beneficial for organizations to analyze the current state of Cybersecurity, establish future objectives and plan actions. Having a good reference guide to establish the level of maturity of the organization in terms of information security represents a good starting point for those organizations that have carried out isolated activities about Cybersecurity and want to deepen or improve them with a general framework that allows them to have a complete look. It is also suitable for organizations that have already certified, for example, against an ISO 27001 standard and still want to have a complementary vision; and provide organizations with continuous improvement in security by repeatedly applying the implementation steps of the Framework.

The established division of Functions allows an organization to clearly identify its weaknesses and address them specifically. The functions selected in the framework contemplate the most important actions when thinking about Cybersecurity processes and allow a high-level perspective beyond specific activities facilitating the communication of strengths and weaknesses to senior management of the organization. In this sense, the categories and subcategories allow a higher level of granularity. The Informative References allow us to delve deeper into the implementation details, which is very useful when putting together plans of concrete actions that will raise the level of Cybersecurity maturity. Additionally, the fact that the informative references are from various sources allows the organization, if it wishes, to align itself more closely with one or the other, or take ideas and complement several of them.

For the organizations in which I participated in the security analysis against our National Framework, the compliance percentage was established in a spreadsheet for each function's subcategory. This made it easy to visualize later the state of maturity of the organization concerning the framework for each function and category. Figure 1 shows an example of how the results were displayed. In this way, the organization's executive level could have a greater appreciation of the weak points in which more effort and resources had to be put. Similar graphs were used to represent the gaps for the different Categories.



Defining the Implementation Tiers can be complex or challenging for an organization to determine, especially if it is the first time the framework is applied or in organizations where the level of process maturity is very low. This is the case for most organizations I have worked with, which end up ignoring this step, which generates more confusion during the implementation.

On the other hand, defining the Target Profile is another point that can be cumbersome for organizations, presenting a difficulty when selecting the actions they must add to be in a higher profile, allowing them to cover the indicated requirements. This method leaves the definition of the target profile and therefore the actions to be implemented too flexible and broad. This amplitude level may not apply to all types of organizations, especially those that, as we indicated above, do not have an organizational maturity and a security vision that allows them to evaluate and define the new objectives on their own. These organizations need stricter and more defined indications that enable a more precise orientation to avoid getting lost in the implementation and frustrating the attempt.

Organizations that set a very high bar for their target profile may fall into the need for very high resource requirements that end up leading to failure in implementation; on the contrary, if they set a very weak target profile, they may generate a false idea of improvement, when in reality the optimization could be higher.

Considering the two previous points, the implementation levels could be mapped to the subcategories, selecting which of these and under what conditions they allow to be placed in the different levels. This would allow less mature organizations to have a staggered, stricter implementation that clearly defines the actions to follow to reach each level, from the most basic to the toughest. The objective level will depend on the objectives set by the organization and may remain at an intermediate level if it is so determined. Something similar to this proposal was made in the adaptation for the National Framework[1].

The following table shows what the before-mentioned integration could look like.

1https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Marco+de+Ciberseguridad

Function	IDENTIFY (ID)			
Category	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.			
Subcategory	**Level 1**	**Level 2**	**Level 3**	**Level 4**
ID.AM-1: Physical devices and systems within the organization are inventoried	Physical devices and systems within the organization are not inventoried.	Physical devices and systems within the organization tare inventoried, but there are no processes to support them.	Physical devices and systems within the organization are inventoried. There are processes and policies that support it. The process is automated.	Physical devices and systems within the organization are inventoried. There are processes and policies that support it. The process is automated. There are regular activities to validate compliance with the policies and the lessons learned and improvements detected are incorporated.

Relationship with other risk management resources

Some of the companies I participated in the evaluation against our National Framework were ISO 27001 certified. This generated a difference in the level of maturity in Cybersecurity compared to other companies that did not have this certification. Still, in any case, it was not sufficient to cover the aspects considered in the Framework. Implementing the Framework in companies with certifications showed that despite having implemented controls and control objectives and a clear vision of what information security means, the associated risks, and their management, there were specific and general deficiencies in actions and procedures. The Framework represents a valuable complement to Cybersecurity management for these organizations and covers existing gaps and unresolved risks.

Considering which other concepts or frameworks could the NIST Framework benefits from, it could be interesting to explore the integration with the zero trust architecture concept at the level of Categories, Subcategories, or the Informative References. This integration could be helpful for enterprises wanting to implement the Framework and enterprises that are thinking of implementing ZTA.