Dear Amy and colleagues

The Uruguayan government has adopted, in 2016, the NIST Cybersecurity Framework, although it was adapted to the context, the core remains the same. With this we carry out periodic audits and from them have arisen needs and comments that we detail below.
Recommendations and comments for the NIST CSF update or use:

- **Cloud**: The use of the cloud and the specific risks that its use implies are not explicitly addressed. Although they can be considered in existing subcategories, it could be a topic to be dealt with specifically. For example, making use of the new ISO/IEC 27002 standard and/or the NIST standards for the use the cloud.
- **Self-assessment**: In the experience of using the framework, one of the questions that arises most frequently is "where do I start?". For this we have generated various strategies; One of them is the use of the cybersecurity assessment tool developed by IDB (https://www.iadb-tools.org/ [gcc02.safelinks.protection.outlook.com]). We are currently coordinating efforts with the bank to adapt the tool to various sectors. This tool allows, based on high-level questions, to determine a cybersecurity maturity and initial recommendations, allowing the user to develop an action plan. Perhaps NIST can contribute to it.

I hope our comments are useful to you.

Best regards

--

Ing. Fabiana Santellán
Gerente de gestión y auditoría
Seguridad de la Información, AGESIC

Torre Ejecutiva Sur
Liniers 1324 - Piso 3
(11.000) Montevideo – URUGUAY