Febraban

General

Observing the news about the increase in remote work and, consequently, the actions of cybercriminals, we are more attentive to learn from scenarios that are emerging indicating updates to procedures for responding to incidents based on new scenarios. We follow national regulatory standards that can follow international standards. We recommend the use of international frameworks from institutions such as NIST, CIS, FSSCC and FS-ISAC. For severe incidents, communication with financial authorities must be easily accessible and support essential investigations.

Preparation

It is interesting for the company to have solutions to centralize monitoring view on the environment, as well as detection and response to incidents for, for example SIEM and or SOAR (Security Orchestration, Automation, and Response). Incident response processes and procedures defined through previously mapped scenarios, by experience in the environment, company, business or segment. The improvement of the incident response plan should be frequent, an example to be used are cyber exercises carried out in order to feed new scenarios and incident handling. For a better view on the risks linked to third parties, a program to know your supplier must be developed and applied based on the best market practices and periodic controls must be carried out.