Minimum information security requirements for organizations of the National Public Sector

The National Cybersecurity Directorate of the Ministry of Public Innovation created a series of minimum information security requirements for organizations of the National Public Sector, which are the main receivers and producers of information in the country. The measure aims to promote a public policy that frames responsible conduct in matters of information security in state agencies, their agents, and officials.

In order to comply with this measure, organizations must develop an information security policy based on an assessment of the risks that could affect them. Said policy must be approved by the highest authorities of the organization or by the official to whom the function has been delegated. It must also be notified and disseminated to all personnel and to those third parties involved when it is pertinent and in the corresponding aspects. In addition, once approved, it must be reported to the National Cybersecurity Directorate.

Each organization has to adopt the necessary measures to prevent, detect, manage, resolve and report security incidents that may affect its information assets. In this context, they must take a series of actions:

- Identify weaknesses in the organization's information management processes, in order to adopt measures that prevent the occurrence of security incidents.
- Have documented, approved, and adequately communicated security incident management procedures, according to the functional areas deemed necessary.
- Adopt a clear prioritization and escalation strategy, which includes communication to the areas involved, authorities and technical areas.
- Instruct agents for the prevention, detection, and reporting of security incidents, according to the corresponding responsibilities.
- Notify the National Cybersecurity Directorate of the occurrence of security incidents, within a period not exceeding 48 hours of their detection.

Likewise, the regulation indicates that agencies must adopt a systemic perspective to protect their information assets, within which personnel must be considered “a central resource”. It also highlights that "they must establish a policy of respect for the individual rights of employees and protect their privacy." To comply with the indicated, the following will be necessary:
• Carry out and implement awareness plans on the safe and responsible use of information assets, which include periodic training aimed at all agents and officials of the agency, designing them for each type of public and with different themes.
• Establish the obligation to sign minutes or commitments regarding information security for all employees of the organization,
• Clearly establish information security requirements, including levels of access to information for each job profile.
• Require agents and officials, when the agency deems it necessary, according to their powers, to sign a confidentiality agreement.
• Incorporate within the disciplinary processes any violation of the organization's security policies.

On the other hand, the standard explains that the organization's information assets must be managed and protected effectively and classified according to the degree of criticality for the organization from the perspective of its confidentiality, integrity, and availability. This requires classifying information assets in line with the type and importance of the information they manage for the organization. It is also necessary to make an updated inventory in which the necessary data is detailed to know the location, the owner, and the corresponding responsibilities of each asset.

https://www.argentina.gob.ar/jefatura/innovacion-tecnologica