Aire Networks is a wholesale telecommunications services operator with a national operator's licence granted by the National Competition Market Commission in Spain that offers connectivity, voice, audiovisual, hosting and security services to operators, companies and public bodies.

For the correct performance of the business functions and to be able to have the information available when necessary, that this information is complete and that its confidentiality is preserved, it was decided to implement an Information Security Management System based on the current **ISO 27001, ISO 27017, and ISO 27018 standards**. Incorporate into Aire Networks' systems the security measures established therein, which guarantee the dimensions of; **integrity, confidentiality and availability** of information systems. In addition, the ISO 27018 implemented provides the capacity to guarantee better protection of the personal data processed in the products and services offered as a Cloud provider.

For this purpose, it is based on and assisted by the processing of different types of data and information, supported by systems, programmes, communications infrastructures, files, databases, archives, etc., which constitute one of Aire Networks' main assets, in such a way that their damage or loss affects the performance of its services and may jeopardise the continuity of the organisation.

In particular, for the provision of services of the commercial product OASIX (Co-location and IaaS) and the cross-cutting service GECO, Aire Networks is linked through electronic means, inter alia, with citizens, employees, customers and suppliers and with other telecommunications service providers. These services must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that may affect the **availability, integrity or confidentiality** of the information processed or the services provided, with the aim of guaranteeing the quality of the information and the continuous provision of services, acting preventively, supervising daily activity and reacting promptly to any security incidents that may occur.

With the advance of new technologies in recent years, such as cloud storage, which provides organisations with multiple benefits related to the speed and ease of access to information from anywhere. This management model provided by Aire Networks comes at the cost of data protection and data privacy concerns regarding personally identifiable information (PII). In order to have processes in place to cover cloud services, Aire Networks has implemented the **ISO 27018 Personal Information Protection in the Cloud standard**.

Thus, the Aire Networks systems required for the provision of these services must be protected against rapidly evolving threats with the potential to impact the **confidentiality, integrity, and availability**, intended use and value of information and services, and be prepared to prevent, detect, react and recover from incidents. To defend against these threats, a strategy is required to adapt to changing environmental conditions to ensure the continued provision of services. This implies that, without prejudice to the measures already taken, both Aire Networks and its staff must implement the minimum security measures required by the 270xx family ISO standards, as well as continuously monitor service delivery levels, track and analyse reported vulnerabilities, and prepare an effective response to incidents that occur in order to ensure the continuity of the services provided.

For this reason, the different areas and departments of Aire Networks must be aware that security in information systems is an integral part of each stage of the life cycle of each of the Information Systems existing in Aire Networks, from their conception to their decommissioning, passing through the development or acquisition phases and the operating activities. It will also be taken into account that security requirements and the funding needs of these should be identified and included in the planning and tendering process. Establishing the following principles in its management:

- Ensure that the necessary resources are available to make the Management System available.
- **Observe and complywith** with all **legal requirements and other requirements** to which Aire Networks subscribes relating to **information security**, **data protection** and regulation applicable to the

telecommunications sector. Aire Networks has internal procedures in which the legal and regulatory framework in which the activities will be carried out is analysed.

- **Protect**, through controls/measures, **assets** against threats that could lead to security incidents. For these purposes, security is understood as an integral process made up of all the technical, human, material and organisational elements related to the System.
- **Mitigating** the effects of security **incidents** . For this purpose, Aire Networks bases its incident procedure on prevention, reaction and recovery.
- **Establish** an **information** and data **classification** systemto protect critical information assets. It also defines guidelines for the structuring of the system's documentation, its management and access.
- **Define responsibilities** for information security by creating the corresponding organisational structure.
- **Develop** a set of **rules, standards and procedures** applicable to management bodies, employees, partners, external service providers, etc.
- **Specify** the effects of **non-compliance** with this Policy and other information security policies in the workplace.
- **To assess the risks** affecting the assets in order to take appropriate security measures/controls, risk management being one of the basic principles of the integrated management system. Also, to have a protection strategy consisting of multiple layers of security. The lines of defence must consist of measures of an organisational, physical and logical nature.
- **Verify** the functioning of **security measures/controls** through internal security audits by independent auditors. Security measures shall be periodically **reassessed and updated** to adapt their effectiveness to constantly evolving risks and protection systems, including, if necessary, a security review.
- **Train users in security management** and information and communication technologies.
- **Control information and data traffic** through communication infrastructures or by sending optical, magnetic, paper, etc. data carriers.
- **Protect the organisation's intellectual capital** from unlawful disclosure and use.
- **Reduce** the chances of **unavailability** through the proper use of the organisation's assets.
- **Defend assets** against internal or external attacks so that they do not become security incidents.
- **Monitor the functioning of security measures** by ascertaining the number of incidents, their nature and effects
- **Reduce the risks of authorised insider information.**
- **Ensure isolation of customers from multi-tenancy and cloud services (including virtualisation).**
- **Ensure the protection and confidentiality of client assets.**

Raúl Aledo Coy

CEO

Elche, 23 September 2024