S2 GRUPO
Anticipanting a
**cyber secure** world

CASE STUDY

# Comprehensive Cybersecurity **Master Plan**

01

# Introduction

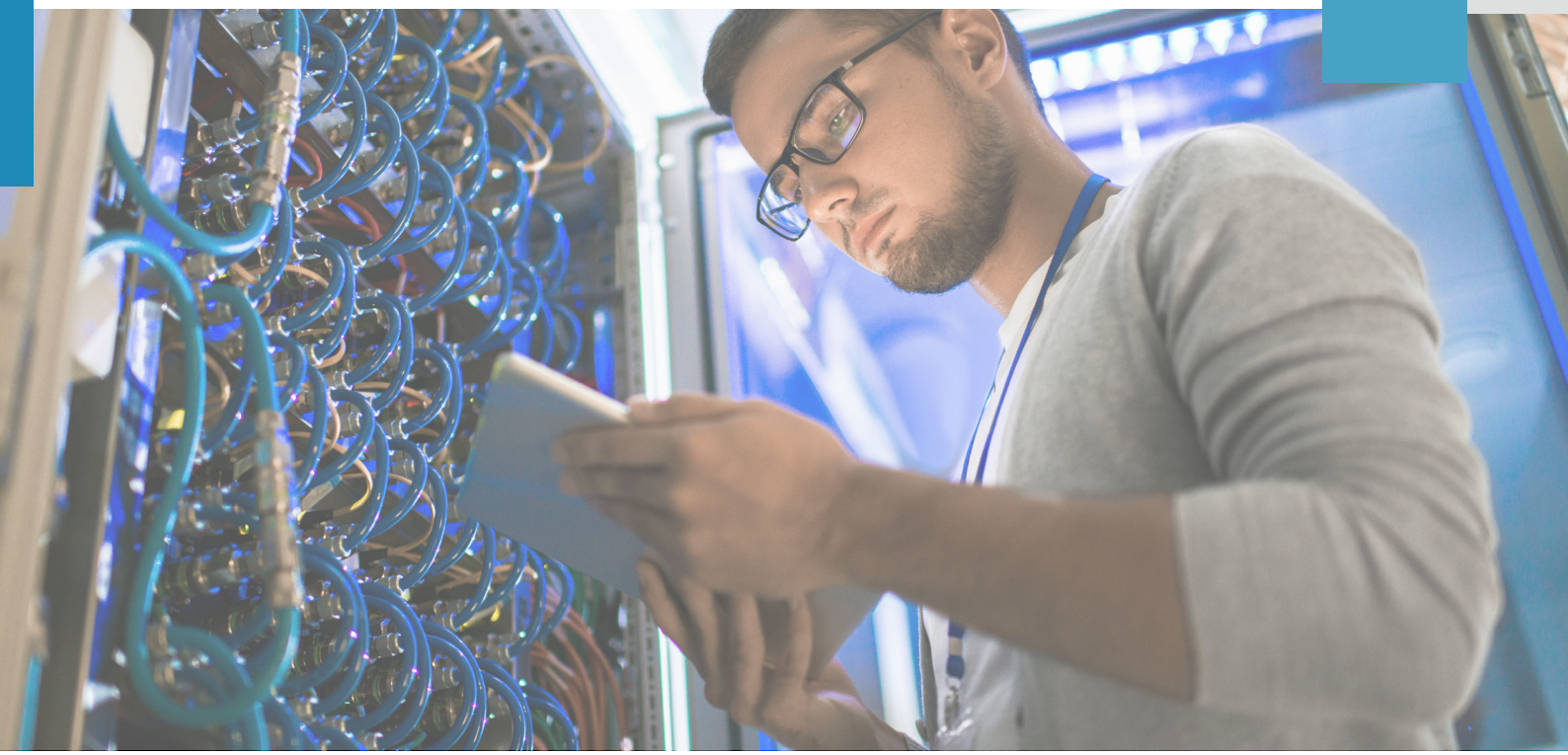
Our client is a large **business group operating essential services and an important critical infrastructure.**

It embarked on its cybersecurity journey in 2019, the year in which it asked us to help it conduct a diagnostic analysis after which we issued a report of recommendations that would lay the groundwork for what would have to come next.

Then, as a result of one of the recommendations, **we proceeded to design and develop an ISMS based on the ISO 27001 standard** and its implementation and subsequent certification in all Group companies. We also deployed a Managed Security service from S2 Grupo CERT, S2 Grupo's SOC. These two initiatives resulted in a significant improvement in the organization's overall cybersecurity in just two years.

02

# Problem/challenge



Due to the importance of its mission, our client subsequently informed us of its need and intention to continue investing in improving its level of cyber protection. It also had an IT strategy to be deployed in the following years, which contemplated important changes in its technological architecture.

Evidently, the deployment of the IT strategy, the changes in the architecture and the management of cybersecurity had to go hand in hand.

In addition, **the need to broaden the scope of the project** to cover, of course, **an extensive (and dispersed) OT infrastructure was brought to our attention.**

A standard Security Master Plan is developed from the results of an in-depth gap analysis against a cybersecurity framework (usually ISO 27002). This type of service is frequently requested by organizations with an incipient and clearly improvable level of cyber protection (sometimes practically non-existent) and that need guidance to take their first steps in cybersecurity.

However, our client already had a more than reasonable level of cybersecurity after the implementation of ISO 27001 and the deployment of the managed security service. But it needed a major plus, aligned with the deployment of its IT strategy for the future and also with a view to extending the scope to its industrial infrastructures.

03

# Upgrade performed

Based on the scenario described above, we proposed to our client the **development of an Integral Cybersecurity Master Plan**. We would take into account their current and future infrastructures, IT and OT areas, in all their plants, and we also had to guarantee the security of the deployment process of their three-year technological strategy.

With these premises, it was not possible to perform a gap analysis against any cybersecurity standard, since the level of maturity was already high, in addition to having an ISO 27001 certification. The approach had to be different and, with the **aim of providing comprehensive protection**, what we did was to perform a **360º analysis against a catalog of comprehensive cybersecurity services** to determine (or rule out) the convenience and necessity of each of the services in the catalog from the point of view of the benefit/cost ratio.

To do so, we held a series of in-depth analysis interviews with senior experts from our staff in all possible cybersecurity disciplines (identity management, communications, systems, industrial cybersecurity, training/awareness, cloud, compliance, software development...) who met with the corresponding interlocutors identified by our client.

**For each service in the catalog** (for example: the possible deployment of a DLP / IRM solution) **we analyzed with the customer its context and circumstances**: critical business information, file servers, IDSs, permissions management policy, network security, USB port management, internal and external NDAs...) to determine the possible need and/or appropriateness of the measure or, alternatively, validate the approach and discard the initiative.

**If the initiative is appropriate:**

**We describe the initiative.**

**We analyze possible dependencies and relationships with other initiatives.**

**We assign an order of priority.**

**We propose an implementation plan.**

**We estimate the effort of its take-off in economic terms or in man-hours.**

04

# Benefits obtained

With the realization of this project the client obtained:

- **A Comprehensive Cybersecurity Master Plan**, i.e. a perfectly mapped roadmap.
- **A tailor-made guide** for the **organization for the next three years in terms of cybersecurity.**
- A **tailor-made guide** rationalizing and prioritizing **investment in IT and OT technology** while ensuring its security at all times.
- Although it is impossible to guarantee 100% cyber protection of any infrastructure or organization, it is possible to expect, after the deployment of a Comprehensive Cybersecurity Master Plan, **an exposure surface over time with a value close to zero.**

S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
LISBOA
RÓTERDAM

Follow us: • @s2grupo • s2grupo.es