

■ CASE STUDY

Cybersecurity Awareness Office

01

Introduction

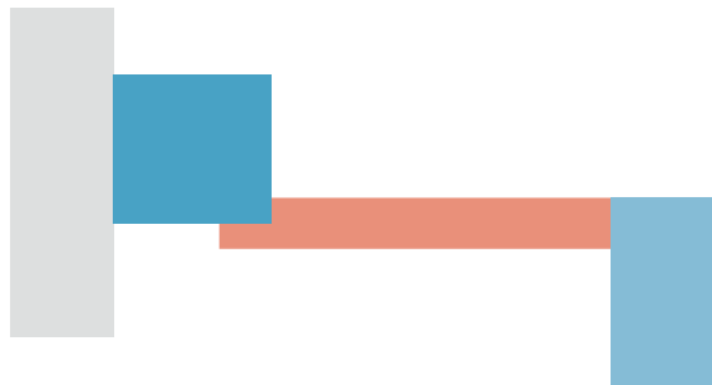
It is one of the leading companies in the **Spanish energy market**, supplying electricity and gas in this and other European energy markets, as well as value-added products in the energy sector.





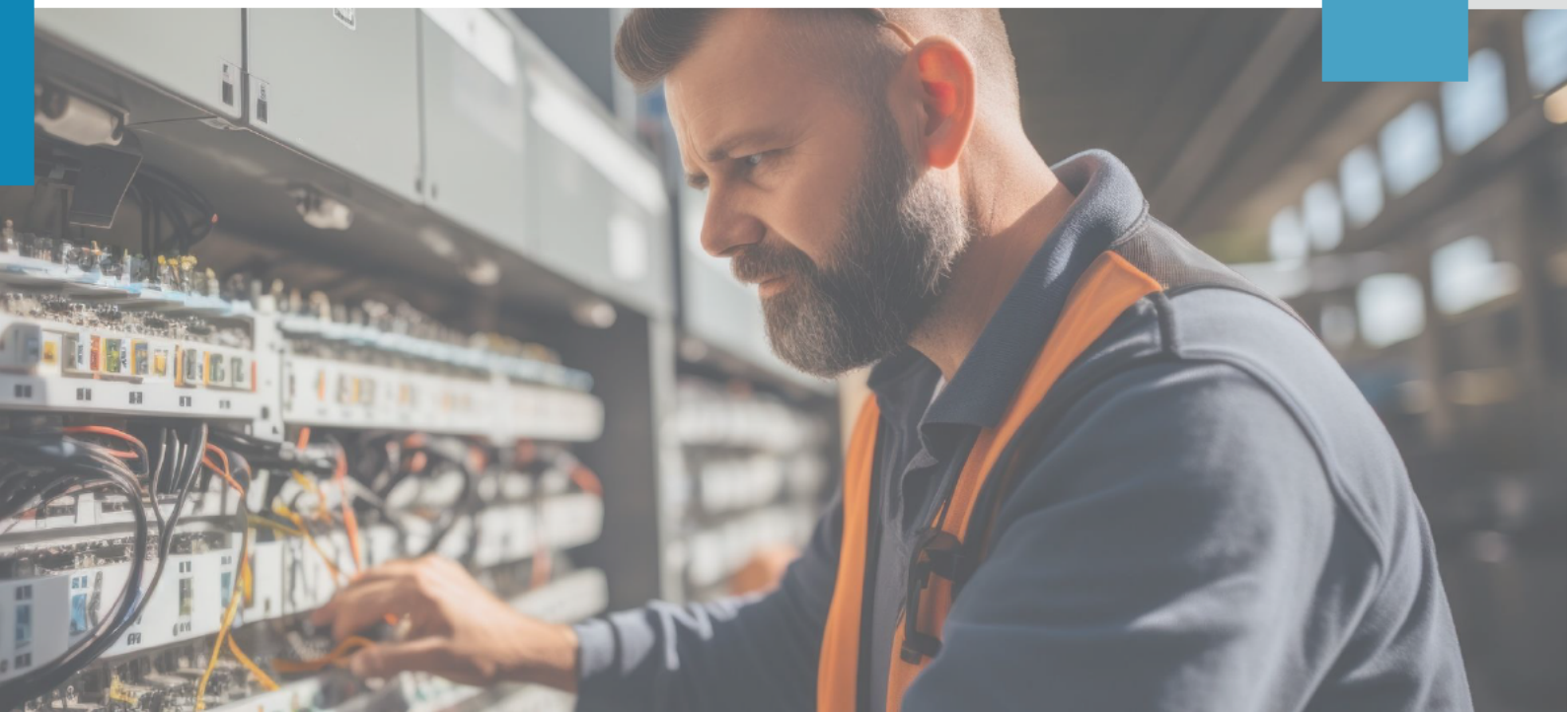
The company employs close to 10,000 people and serves more than 10 million customers on a continuous basis.

In addition to the infrastructure for managing the proper functioning of the organization, it has an **extensive industrial structure dedicated to the generation, logistics and control of constant energy.**



02

Problem/challenge



The company has personnel specialized in ensuring IT and OT security conditions related to internal cybersecurity.

However, **it does not have an effective security culture plan** to help increase the company's overall security level and reduce the risk of incidents directly related to one of the key components in this area: people.

There is a **need to raise awareness, educate and train people** working in the organization on an ongoing basis about which situations or circumstances may compromise security, and also to train them in prevention and protection models associated with specific risks.

03

Upgrade performed

A team of S2 Grupo's cybersecurity awareness experts has been managing the client's Information Security Office for more than 10 years, addressing risks associated with people in the IT and OT fields. This is an ongoing service aimed at **improving people's behavior towards cybersecurity** through actions of:

- **AWARENESS:**

To involve people in the protection of the technologies and information they manage. People are shown **the threats they face and their possible impact**, making them understand why they should carry out adequate security management.

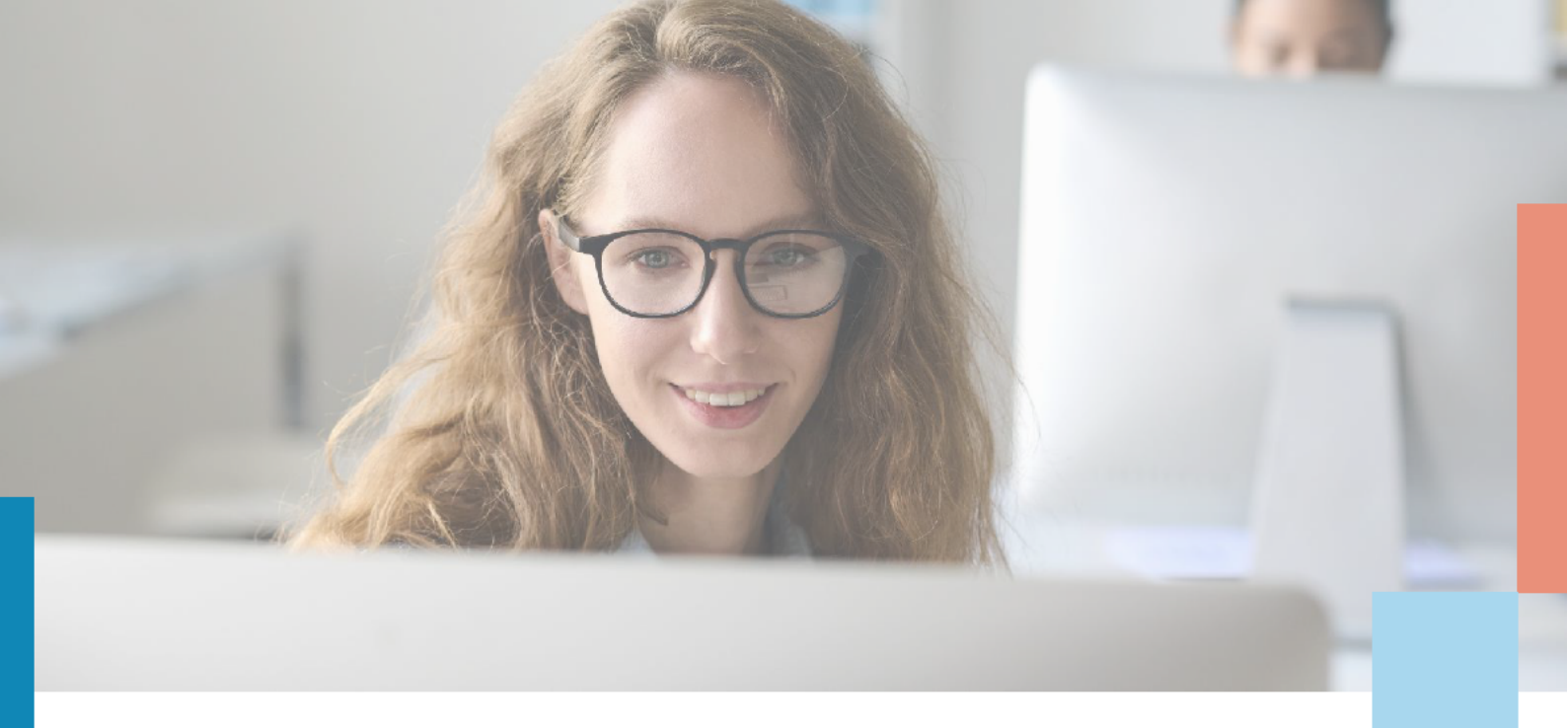
- **TRAINING:**

Through training, the necessary knowledge is transferred **to implement proper safety management**. They are trained on how to do it.

- **SIMULATION:**

Through the implementation of training actions, people are helped **to keep their knowledge up to date** in order to effectively manage risk.





Entre The main tasks carried out by the security office include the following:

1. **Elaboration of annual awareness plans** taking into account the specific risks to which the organization's employees are exposed and the analysis of the impact of the actions previously carried out.

2. These plans include actions with the capacity **to impact the greatest number of people** by means of original contents that are close to personal situations and avoid the use

of technical terms. To this end, **we combine the emotional with the rational**, making people aware of the risks and the need to avoid them.

3. **Management of channels** such as the website, traffic and impact analysis, content publication and daily email support for doubts and incidents received in the office mailbox.

4. **Generation of reports** to assist in decision making on which risks to treat and which groups to target.

Some of the **relevant data**:

-  42 employee sessions and 8 children's sessions.
-  Average rating per session: 4.8/5.
-  More than 5,000 awareness-raising hits in sessions.
-  Number of security site subscribers: +1500 security site subscribers.
-  More than 1100 queries solved.
-  More than 1000 linked news items.

04

Benefits obtained

With the completion of this project the client has:



An **information security awareness office** that continuously supports the security team and helps to make decisions on the risks to be dealt with in the IT and OT areas.



An **effective communication strategy** to optimize the content developed, making it attractive and simple to reach employees, and to promote safety messages and best practices.



A **specialized communication channel** as a reference within the organization on information security culture and **to increase the degree of reporting of possible threats** in its support CAU.



People with **safe behavioral practices** in cybersecurity by addressing the need to manage risks in their closest environment, the personal and family environment, and then transfer the same risks to the corporate environment.



A **higher level of security** by improving the cybersecurity culture.



MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLE
SAN SEBASTIAN

SANTIAGO DE CHILE
C.D. MEXICO
BOGOTA
LISBON
ROTTERDAM

Follow us:



@s2grupo



s2grupo.es