S2 GRUPO

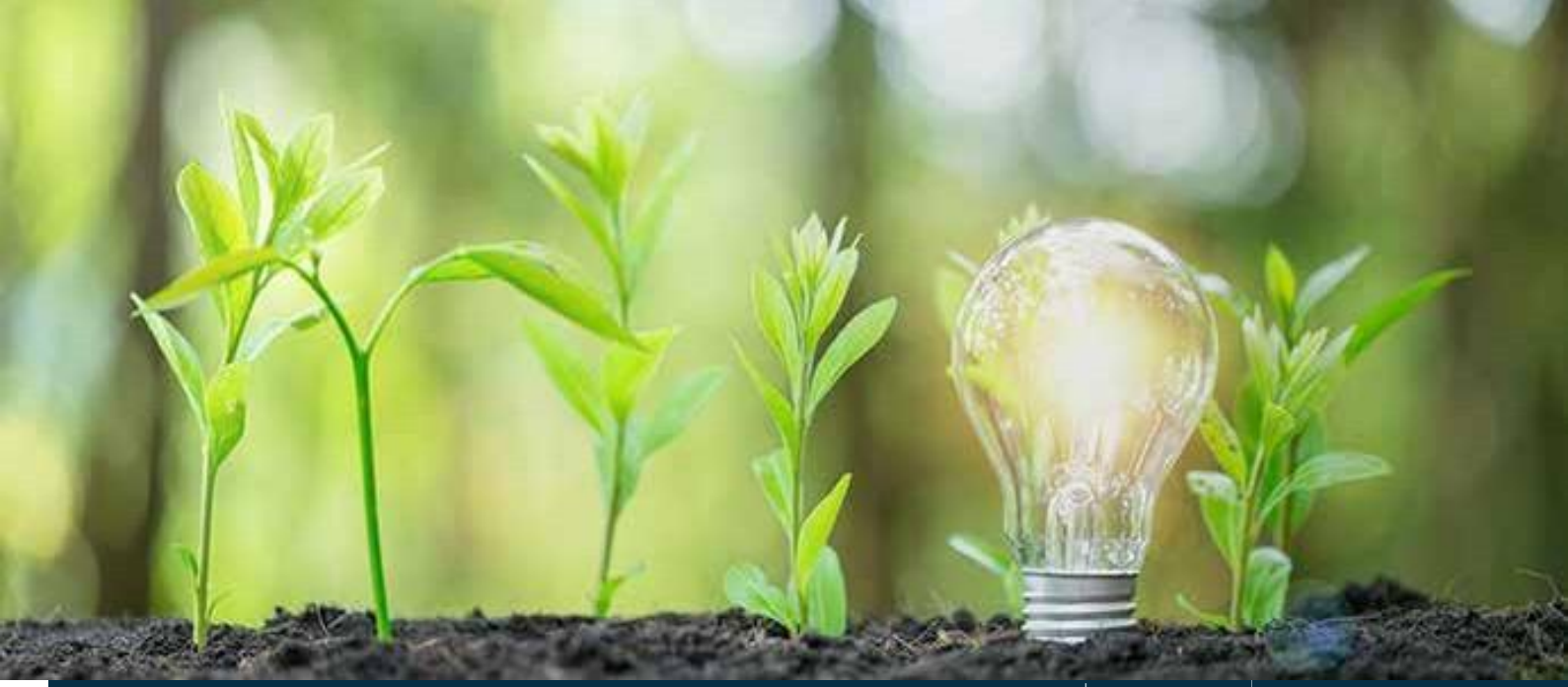
Case study

Renewable Energy Sector

01

Brief presentation of the company:

Our client is a **national industrial group** diversified in different business lines: renewable energy, mining, chemicals and logistic infrastructures... With mines, production plants and infrastructures in different cities of Spain and the headquarters.



Each division has autonomy in its operation. But the head office sets the general strategy of the organization. With an annual turnover of around 1,000 million euros and more than 3,000 employees.

They have a single general systems department for the entire company in charge of managing corporate networks, but do not have a cybersecurity department per se or an **OT industrial cybersecurity** department.

Case study: Renewable Energy Sector

03

Problem/challenge

They have heard about incidents in other similar companies and know that they have to improve the company's cybersecurity. Being an industrial company they want to review especially the cybersecurity of the operational part. But they do not have a clear idea of how to do it.

They have personnel in charge of the corporate network but **lack knowledge and experience in industrial cybersecurity**.

Some time ago we conducted an assessment of the state of one of their renewable energy facilities and many opportunities for improvement became evident. The results revealed weaknesses in the organization's OT cybersecurity.

Specifically, the evaluated installation had not foreseen minimum security conditions in the levels of user identification, access passwords, network segmentation, etc., etc. On many occasions, this type of infrastructure is installed far from urban centers and the supervision is done remotely, where the blocking or shutdown of the installation can cause **serious economic damages**.

04

Action performed

For several months, a specialized team of **industrial cybersecurity** consultants conducted a general diagnosis of the cybersecurity status of the entire organization.

The currently available work procedures were analyzed by reviewing the security-related part and taking as a reference a general industrial cybersecurity framework such as **IEC 62443**.

To get an overview of the whole picture, a series of interviews were conducted with maintenance and plant control personnel from different parts of the company. To understand their way of working, the complexity of their processes and to understand their business priorities.

From the analysis of the information gathered and as a result of the interviews carried out, a picture of the current state of the organization's industrial cybersecurity was obtained, the risk scenarios to which they are exposed and the weaknesses to be corrected in order to improve their degree of maturity were identified.

As a result, a general status report was prepared describing the work carried out, the results obtained and, as a consequence, an **Action Plan** with the different lines of work proposed for the improvement of the industrial group's cybersecurity.

Benefits obtained

With the realization of this project, the client:

1. Has a detailed analysis of the general state of industrial cybersecurity in your organization, its shortcomings and weaknesses. And a list of proposals for the improvement of the different weaknesses observed with an estimate of the effort required.

2. Can prioritize those initiatives that improve the deficiencies detected according to their degree of importance and the resources needed to do so.

3. It has a general industrial cybersecurity plan for the organization as a continuous improvement process that will become part of the general work procedures of the entire company.

S2 GRUPO

Anticipando un mundo
ciberseguro

MADRID
BARCELONA
VALENCIA
CERTVALENCIA
HQ
SEVILLA

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
BRUSELAS
LISBOA
RÓTERDAM

Síguenos • **@s2grup** • **s2grupo.e**