Case study

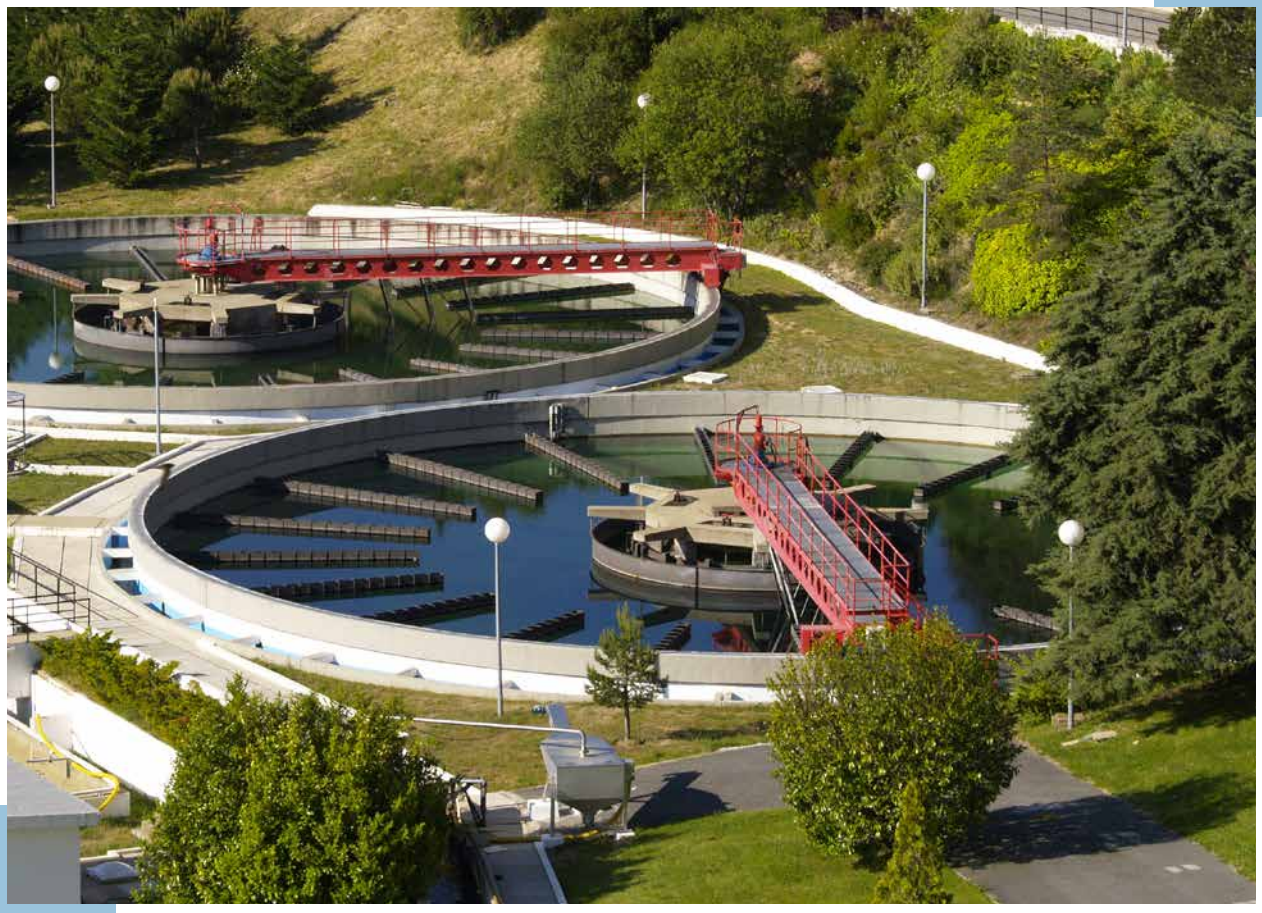
Water sector.

Cybersecurity of the integral water cycle

01

Introduction

Water is a fundamental resource for our society. The facilities in charge of the purification, treatment and distribution phases up to the purification and discharge stages are **critical infrastructures** that require special attention.



The facilities in charge of the different stages of the **Integral Water Cycle** are managed by specialized service provision companies. Our client is a multinational company in charge of managing a large number of desalination, treatment and water treatment plants throughout the country.

It must comply with **national and international regulations on the security of critical infrastructures** and essential services. It is aware of the security risks of the current environment with the introduction of digitization and connectivity in all industrial processes.

Case study: Water sector

03

Problem/challenge

The water treatment infrastructures have **industrial control facilities** with SCADAs, automation and supervision elements, and remote management.

The managers of the facilities need to have **real-time information** on demands, flows, pressures, water quality... They need to permanently monitor the continuity and quality of the service. In no case can there be **an interruption of the supply**. An unforeseen discharge of wastewater could lead to an **environmental incident**.

As it is an essential service with the possibility of permanent access, and given the current context, with a continuous increase in incidents of all kinds, it is necessary to submit their facilities to periodic procedures for evaluating cybersecurity **conditions**.

04

Action performed

Facilities of different types were selected: a wastewater treatment plant, a drinking water treatment plant and a desalination plant. A team made up of experts in industrial cybersecurity from S2 Grupo traveled to the different locations.

The facilities were toured, identifying the elements that were part of the critical processes and the current access conditions, architecture and segmentation of the communications networks, updated inventory of assets, user access, encryption, supplier access, backup copies, change management etc.

A series of interviews were held with the technical staff in charge of infrastructure management and maintenance to find out their level of awareness, the availability of work procedures, levels of access, assignment of responsibilities, availability of a risk analysis and/or incident response plan.

A series of **technical visibility tests** were carried out to verify the degree of segmentation of the corporate and operational networks.

As a result of the analysis of the evaluated plants, a **detailed report** was prepared with a description of the actions carried out, the results obtained and the procedural, technical and operational deficiencies found. It was accompanyed by a list of recommended measures and improvement proposals that would improve the cybersecurity conditions of the facilities.

Benefits obtained

With the assessment process carried out:

1. Those responsible for managing the plants have a **detailed and objective diagnosis** carried out by experts from an external company, carried out on a representative sample of the different types of infrastructures they manage.

2. They have a **global vision of the cybersecurity status of the facilities evaluated** and the deficiencies identified with the proposal of a series of action plans.

3. They can plan the next actions to be incorporated into their improvement plans. It allows them to justify compliance with the different applicable standards and regulations and propose the development of a **Cybersecurity Management System** in the organization as a process of continuous improvement.

S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLE
SAN SEBASTIAN

SANTIAGO DE CHILE
C.D. MEXICO
BOGOTA
BRUSSELS
LISBON
ROTTERDAM

Follow us: @s2grupo • s2grupo.es