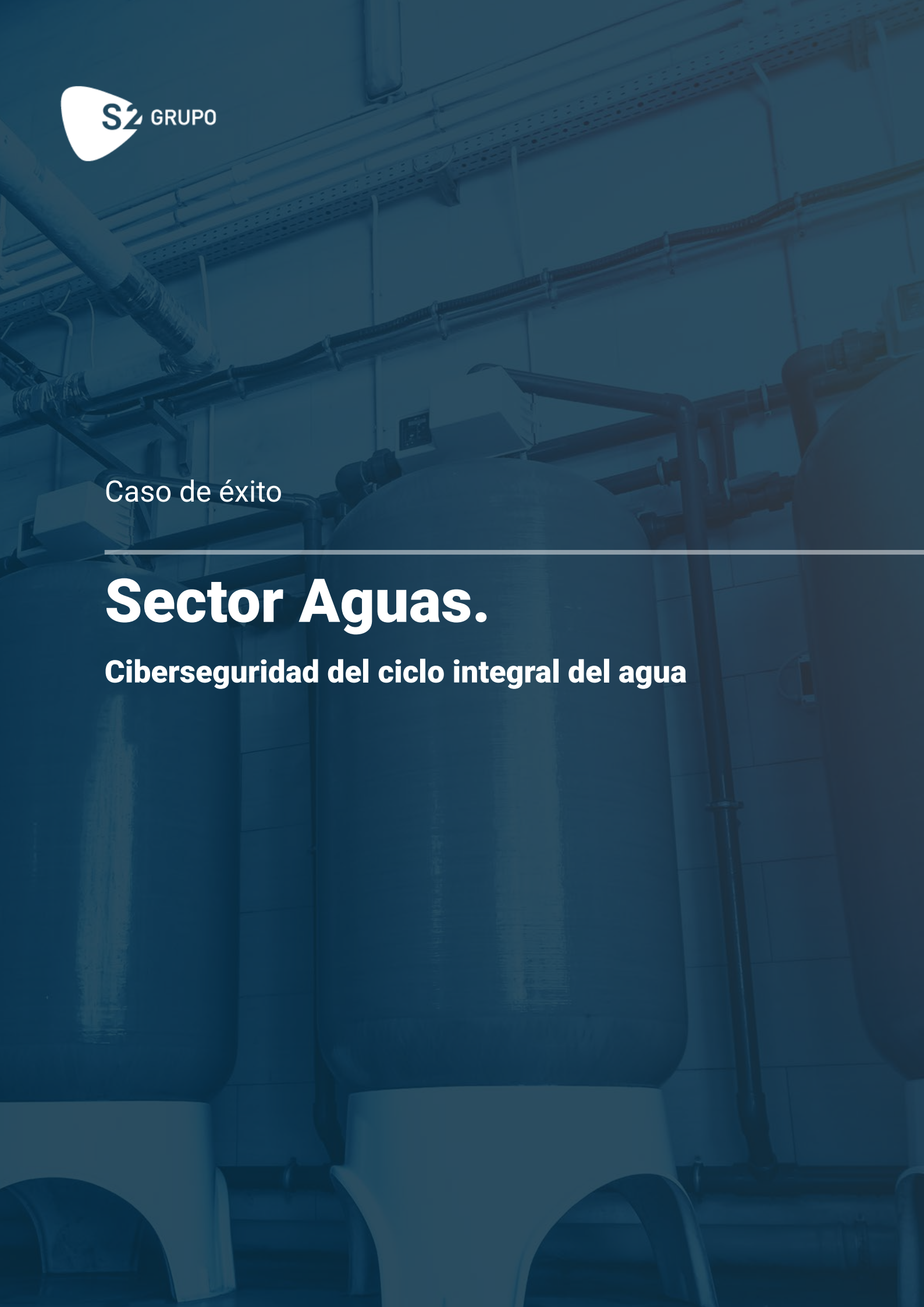


Caso de éxito

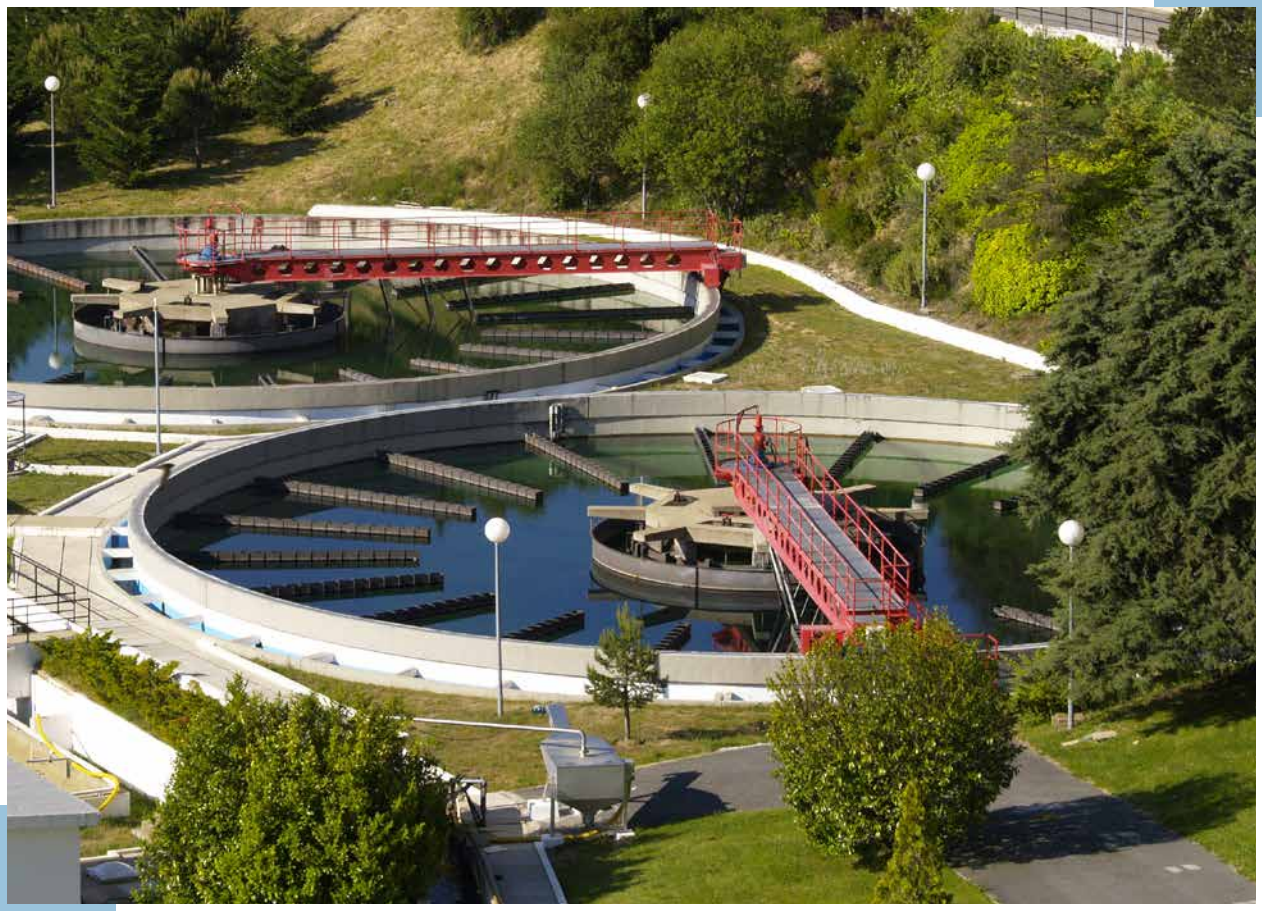
Sector Aguas.

Ciberseguridad del ciclo integral del agua

01

Introducción

El agua es un recurso fundamental para nuestra sociedad. Las instalaciones encargadas de las fases de potabilización, tratamiento y distribución hasta las etapas de depuración y vertido son **infraestructuras críticas** que requieren una atención especial.



Las instalaciones encargadas de las diferentes etapas del **Ciclo Integral del Agua** son gestionadas por empresas especializadas de prestación de servicios. Nuestro cliente es una compañía multinacional encargada de la gestión de un gran número de plantas desaladoras, depuradoras y potabilizadoras de todo el país.

Debe cumplir con la **normativa nacional e internacional de seguridad de infraestructuras críticas** y servicios esenciales. Es consciente de los riesgos de seguridad del entorno actual con la introducción de la digitalización y la conectividad en todos los procesos industriales.

Caso de éxito: Sector aguas

03

Problemática/reto

Las infraestructuras de tratamiento de agua disponen de **instalaciones de control industrial** con SCADAs, elementos de automatización y supervisión y telegestión en remoto.

Los gestores de las instalaciones necesitan disponer de **información en tiempo real** sobre demandas, caudales, presiones, calidad del agua... Necesitan supervisar de forma permanente la continuidad y calidad del servicio. En ningún caso se puede producir **una interrupción del suministro**. Un vertido imprevisto de aguas residuales podría llegar a suponer un **incidente medioambiental**.

Al tratarse de un servicio esencial con posibilidad de acceso permanente, y dado el contexto actual, con un contínuo incremento de incidentes de todo tipo, es necesario someter sus instalaciones a **procedimientos periódicos de evaluación de las condiciones de ciberseguridad**.

04

Actuación realizada

Se seleccionaron **varias instalaciones de distintas tipologías**: una depuradora de aguas residuales, una planta potabilizadora de agua potable y una planta desaladora. Un equipo formado por expertos en ciberseguridad industrial de S2 Grupo se desplazó a las diferentes localizaciones.

Se recorrieron las instalaciones, identificando los elementos que formaban parte de los procesos críticos y las condiciones actuales de acceso, arquitectura y segmentación de las redes de comunicaciones, inventario de activos actualizado, acceso de usuarios, cifrado, acceso de proveedores, copias de seguridad, gestión de cambios, etc.

Se mantuvieron una serie de entrevistas con el personal técnico encargado de la gestión y mantenimiento de las infraestructuras para conocer su nivel de concienciación, la disponibilidad de procedimientos de trabajo, niveles de acceso, asignación de responsabilidades, disponibilidad de un análisis de riesgos y/o plan de respuesta ante incidentes.

Se realizaron una serie de **test técnicos de visibilidad** para comprobar el grado de segmentación de las redes corporativa y de operación.

Como resultado del análisis de las plantas evaluadas se preparó **un informe detallado** con la descripción de las actuaciones realizadas, los resultados obtenidos y las deficiencias encontradas tanto procedimentales como técnicas y operativas. Acompañándolo de una relación de medidas recomendadas y propuestas de mejora que mejorarían las condiciones de ciberseguridad de las instalaciones.

Beneficios obtenidos

Con el proceso de assessment realizado:

1. Los responsables de la gestión de las plantas cuentan con un **diagnóstico detallado y objetivo** realizado por expertos de una empresa externa. Realizado sobre una muestra representativa de los diferentes tipos de infraestructuras que gestionan.

2. Disponen de una **visión global del estado de ciberseguridad de las instalaciones evaluadas** y de las deficiencias identificadas con la propuesta de una serie de planes de acción.

3. Pueden planificar las próximas actuaciones a incorporar en sus planes de mejora, les permite justificar el cumplimiento de las diferentes normativas y reglamentos de aplicación y plantear la elaboración de un **Sistema de Gestión de la ciberseguridad** en la organización como un proceso de mejora continua.

S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

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

Síguenos en: @s2grupo • s2grupo.es