S2 GRUPO

CASO DE ÉXITO

Sector Medio Ambiente

Ciberseguridad de la economía circular

01

Introducción

No hay futuro para nuestra sociedad sin una economía sostenible, con el uso responsable de los recursos del planeta. La UE es un modelo para el mundo con el **Pacto Verde Europeo** y cómo modelo de economía moderna, eficiente y competitiva que hace de la economía circular uno de sus principios fundamentales.

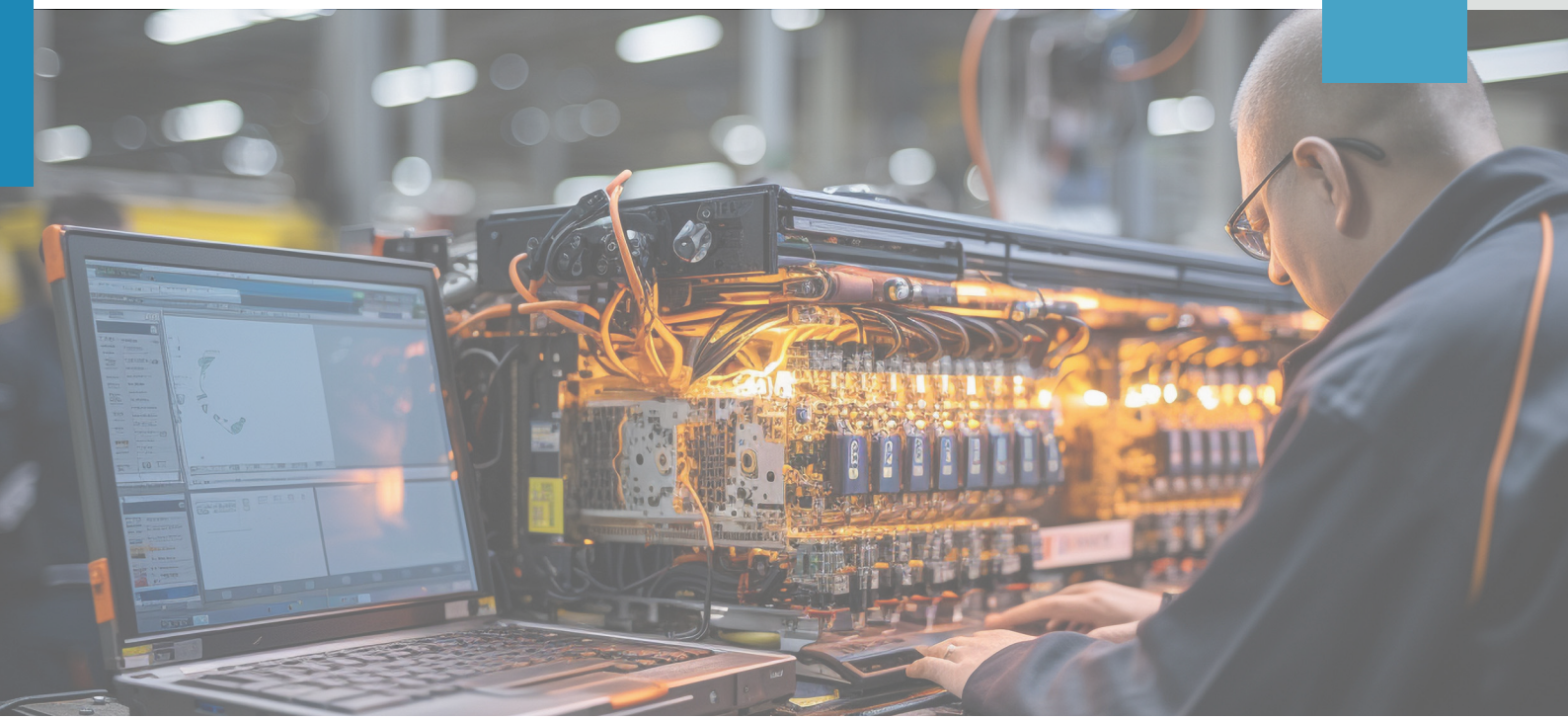
Nuestro cliente es un **grupo multinacional del sector del Medio Ambiente**. Especializado en el reciclaje y la gestión de residuos. Dispone de casi un centenar de plantas de tratamiento en diferentes países del mundo. En algunos casos es propietario de las instalaciones y en otros casos titular de una concesión o contrato de servicios.

Contar con una **red tan extensa de infraestructuras interconectadas en diferentes países** con diferentes culturas hace que su superficie de exposición a cualquier amenaza sea un riesgo considerable.

Se trata de una entidad "importante" en la clasificación que establece la Directiva NIS 2. Su actividad está sujeta a la normativa internacional de ciberseguridad por tratarse de servicios críticos esenciales para la sociedad y la ciberseguridad forma parte de sus líneas estratégicas.

02

Problemática/reto



La organización ya dispone de un departamento de ciberseguridad. Hasta ahora ha venido desarrollando la **estrategia de ciberseguridad de su parte corporativa IT** dónde tiene un alto grado de madurez.

Desde hace algún tiempo está realizando un gran esfuerzo en el desarrollo de la **ciberseguridad de la parte operacional OT**. Ya tiene un Plan de trabajo para el desarrollo de esta parte de su política corporativa. Sin embargo, **las especiales particularidades de este sector requieren un conocimiento experto**. Además, algunas de las medidas a adoptar son urgentes. Y la disponibilidad y limitación de sus recursos le han hecho decidirse por la búsqueda de un proveedor especializado que le acompañe.

03

Actuación realizada

Para el acompañamiento en el desarrollo a medio plazo de un Plan General ha contratado los servicios de una ***Oficina de ciberseguridad industrial***. Desde S2 Grupo se le presta un asesoramiento experto con diferentes especialistas en distintas disciplinas de la seguridad industrial que le permiten contar con el conocimiento necesario en todo el proceso.

Se asignan varios recursos de forma permanente como fuerza de trabajo y conocimiento a disposición del cliente, que coordinará las diferentes líneas de trabajo y los objetivos a conseguir.

Nuestros expertos aportan su experiencia para:

- **El análisis del estado inicial de la organización**, que cuenta con una amplia variedad de plantas con distintos grados de madurez en seguridad. Comprender su entorno de amenazas y determinar el conjunto de vulnerabilidades que podrían comprometerla.

- El **establecimiento de unos objetivos claros** como resultado del proyecto planteado. Nivel de riesgo aceptable.

- La elaboración de un **Análisis de Riesgos** y una serie de procedimientos específicos de ciberseguridad OT que se puedan aplicar a las diferentes plantas de la compañía.

- Aprovechando en el proceso los trabajos que ya ha venido realizando la compañía hasta el momento, con la elaboración de un cuadro de mando de la seguridad de toda la organización.

- Sugiriendo **mejoras alternativas** a los planes inicialmente previstos que contribuyan a la elaboración de un marco documental de ciberseguridad industrial estructurado, sólido y consistente.

04

Beneficios obtenidos

Disponer del acompañamiento de una empresa especializada en ciberseguridad industrial como S2 Grupo ha permitido a nuestro cliente:

- Contar con el **apoyo de una serie de expertos en diferentes disciplinas** que le ofrecen una visión general objetiva de su estado inicial y de las posibles iniciativas a plantear.

- Desarrollar en un tiempo récord, imposible de realizar sin ayuda por sus propios medios, una **estrategia general de ciberseguridad industrial**. Aplicable a toda la organización. Con la variedad de instalaciones con las que cuenta y los diferentes matices culturales en distintos países del mundo.

- Dar continuidad a su **Plan General de ciberseguridad** con la convergencia de la parte IT y de la parte OT y su integración en el Sistema de Gestión de la compañía como proceso de mejora contínua.

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
LISBOA
RÓTERDAM

Síguenos en: • @s2grupo • s2grupo.es