S2 GRUPO
Anticipando un mundo **ciberseguro**

CASO DE ÉXITO

Plan Director
de Ciberseguridad Integral

01

Introducción

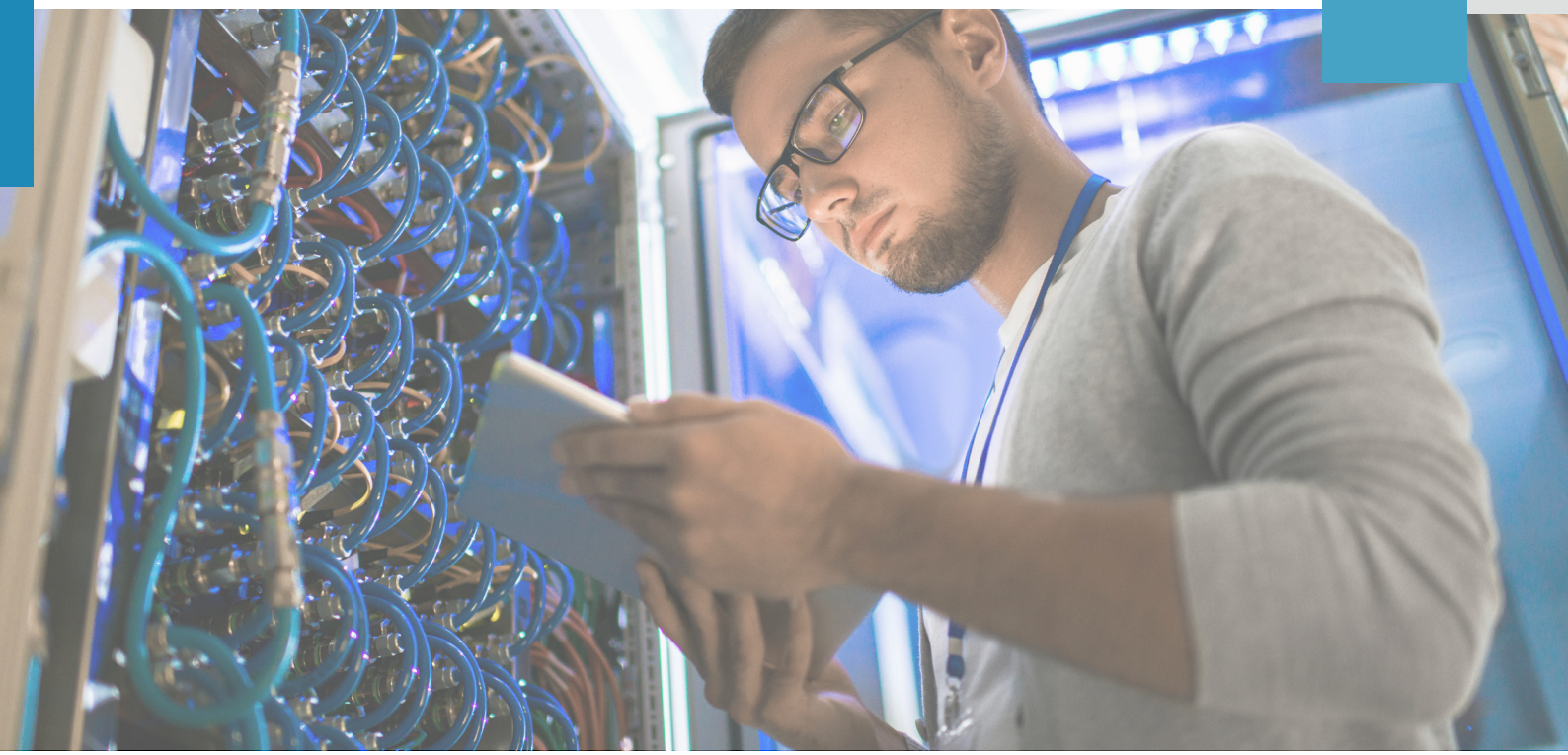
Nuestro cliente es un gran **grupo empresarial operador de servicios esenciales y de una importante infraestructura crítica.**

Emprendió su andadura en materia de ciberseguridad en 2019, año en el que nos solicitó ayuda para realizar un análisis diagnóstico tras el cual emitimos un informe de recomendaciones que sentaría las bases de lo que tendría que venir después.

A continuación, como consecuencia de una de las recomendaciones, **procedimos a diseñar y desarrollar un SGSI basado en la norma ISO 27001** y a su implantación y posterior certificación en todas las empresas del Grupo. Además les desplegamos un servicio de Seguridad Gestionada desde S2 Grupo CERT, el SOC de S2 Grupo. Estas dos iniciativas se tradujeron en una mejora notable de la organización en materia de ciberseguridad en general en apenas dos años.

02

Problemática/reto



Debido a la importancia de su misión, nuestro cliente nos trasladó posteriormente su necesidad e intención de seguir invirtiendo en la mejora de su nivel de ciberprotección. Contaba, además, con una estrategia TI a desplegar en los siguientes años la cual contemplaba cambios importantes en su arquitectura tecnológica.

Evidentemente el despliegue de la estrategia TI, los cambios en la arquitectura y la gestión de la ciberseguridad tenían que ir de la mano.

Además, nos trasladó la **necesidad de ampliar el scope del proyecto para abarcar**, como no puede ser de otra manera, **una extensa (y dispersa) infraestructura OT.**

Un Plan Director de Seguridad estándar se desarrolla a partir de los resultados arrojados por un análisis gap realizado en profundidad contra un framework de ciberseguridad (normalmente la norma ISO 27002). Este tipo de servicios es frecuentemente solicitado por organizaciones con un nivel de ciberprotección incipiente y manifiestamente mejorable (en ocasiones prácticamente inexistente) y que necesitan orientación para dar sus primeros pasos en materia de ciberseguridad.

Sin embargo, nuestro cliente disponía ya de un nivel de ciberseguridad más que razonable tras la implantación de la norma ISO 27001 y el despliegue del servicio de seguridad gestionada. Pero necesitaba un plus importante, alineado con el despliegue de su estrategia de IT a futuro y pensando también en la ampliación del scope a sus infraestructuras industriales.

03

Actuación realizada

Partiendo del escenario descrito planteamos a nuestro cliente el **desarrollo de un Plan Director de Ciberseguridad Integral.** Tendríamos en cuenta sus infraestructuras actuales y futuras, ámbitos IT y OT, en todas sus plantas, y teníamos que garantizar, además, la seguridad del propio proceso de despliegue de su estrategia tecnológica a tres años.

Con estas premisas no cabía realizar un análisis gap contra ningún estándar de ciberseguridad puesto que el nivel de madurez ya era elevado, además de disponer de una certificación ISO 27001. El enfoque debía ser distinto y, con el **objetivo de brindar una protección integral**, lo que hicimos fue hacer un **análisis 360º contra un catálogo de servicios integrales de ciberseguridad** para determinar (o descartar) conveniencia y necesidad de cada uno de los servicios del catálogo desde el punto de vista del ratio beneficio / coste.

Para ello, mantuvimos una serie de entrevistas de análisis a fondo con expertos senior de nuestra plantilla en todas las posibles disciplinas de ciberseguridad (gestión de identidades, comunicaciones, sistemas, ciberseguridad industrial, formación / concienciación, cloud, compliance, desarrollo de software…) quienes se reunieron con los interlocutores correspondientes identificados por nuestro cliente.

Para cada servicio del catálogo (por ejemplo: el posible despliegue de una solución DLP / IRM) **analizamos junto con el cliente su contexto y circunstancias**: información de negocio crítica, file servers, IDSs, política de gestión de permisos, seguridad de las redes, gestión de puertos USBs, NDAs internos y externos…) para determinar la posible necesidad y/o conveniencia de la medida o, alternativamente, validar el planteamiento y descartar la iniciativa.

En caso de resultar la iniciativa procedente:

Describimos la iniciativa.

Analizamos posibles dependencias y relaciones con otras iniciativas.

Le asignamos un orden de prioridad.

Proponemos un plan de implantación.

Estimamos el esfuerzo de su despegue en términos económicos o en horas-hombre.

04

Beneficios obtenidos

Con la realización de este proyecto el cliente obtuvo:

- Un **Plan Director de Ciberseguridad Integral**, es decir, una hoja de ruta trazada perfectamente.
- Una **guía a medida** para la organización para **los próximos tres años en materia de ciberseguridad.**
- Una **guía a medida** racionalizando y priorizando la **inversión en tecnología IT y OT** garantizando en todo momento su seguridad.
- Si bien es imposible garantizar al 100% la ciberprotección de ninguna infraestructura u organización sí cabe esperar, tras el despliegue de un Plan Director de Ciberseguridad Integral, **una superficie de exposición en el tiempo con un valor cercano a cero.**

S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
LISBOA
RÓTERDAM

Síguenos en: @s2grupo • s2grupo.es