S2 GRUPO
Anticipando un mundo ciberseguro

CASO DE ÉXITO

Sector Automoción

Ciberseguridad para hacer frente a los **desafíos** presentes y futuros.

01

Breve presentación de la empresa

Nuestro cliente es un destacado proveedor de componentes para diferentes **fabricantes de automóviles**.

Fabrica elementos que forman parte de la **carrocería y el interior del automóvil**.

Es un claro exponente de una empresa que forma parte de la **cadena de suministro** de varias empresas importantes del sector de la automoción.

Dispone de **varias plantas de producción** dónde se fabrican los diferentes accesorios que suministra y desde dónde se realizan las entregas previstas a sus diferentes clientes.

02

Descripción de la problemática/reto

La organización **no tiene experiencia** en el ambito de la ciberseguridad industrial. Es consciente de los riesgos que corre pero no sabe qué tiene que hacer para mejorar su situación ni cómo abordarlo.

Dispone de un departamento de informática que se encarga de mantener al día la red informática corporativa desde dónde se realizan las operaciones de ERP, financiera, contabilidad, gestión de RRHH. **Pero no cuenta con personal con conocimientos ni experiencia en ciberseguridad operacional.**

Quiere saber cómo mejorar su situación. Tiene una idea aproximada de los riesgos que corre y las posibles consecuencias de un incidente.

Sus clientes le empiezan a **exigir medidas de ciberseguridad** en los contratos de suministro que tiene con ellos. Para poder participar en los sucesivos acuerdos a los que opta le exigen que implemente medidas concretas de ciberseguridad. No dispone de conocimientos ni de recursos para hacerlo.

03

Descripción de la actuación realizada

Como primera aproximación se le propone una **evaluación del estado actual de ciberseguridad de la organización** para posteriormente proponerle un **Plan de mejora**.

1

Se realiza una **visita a una de las plantas principales** con recopilación de la toda la información disponible: inventario de equipos y dispositivos IT y OT, arquitecturas de red, procedimientos existentes.

2

Se realizan **entrevistas con los principales responsables del proceso de producción** como el Jefe de planta, de mantenimiento y del departamento de informática, con la intención de conocer el funcionamiento de la planta, sus procesos y el grado de segmentación de las redes IT y OT.

3

Se comprueba que la organización **no dispone de procedimientos de ciberseguridad en la parte operacional**: mantenimiento actualizado de inventario de activos y arquitecturas de red, gestión de usuarios, gestión de accesos, relación con terceros (proveedores, mantenedores y clientes).

4

Dadas las dificultades de realizar un test técnico de intrusión en un proceso en producción **se realizan una serie de pruebas de visibilidad**, con un plan de pruebas limitado y previamente acordado, para identificar si de dispone de acceso a la red OT desde la red corporativa y el grado de protección de las diferentes redes wifi: corporativa, pública, etc.

5

Análisis de riesgos. Se identifican los puntos principales del proceso, los factores que les afectan y el impacto de un posible incidente a estas partes del negocio.

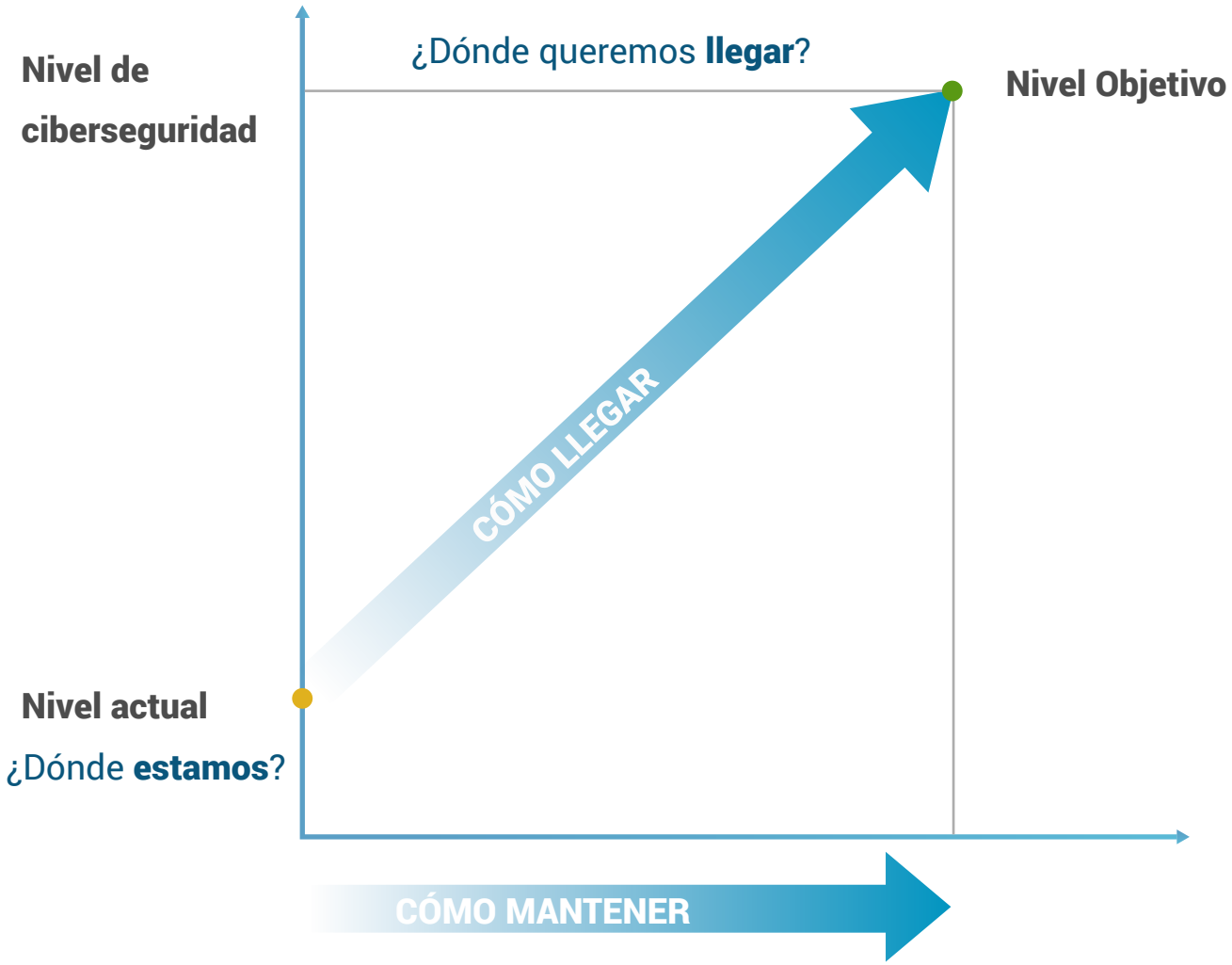
6

Con toda la información recopilada se elabora un **Plan de mejora**, con diferentes grados de implantación. Desde los aspectos más básicos y más rápidos de adoptar hasta las medidas más ambiciosas con un periodo de implementación más largo y costoso.

04

Beneficios Obtenidos

Como resultado de la serie de acciones realizadas el cliente **obtiene una serie de beneficios**:



Disponer de un diagnóstico de su **estado real actual**. Un primer análisis de sus debilidades y una estimación de los esfuerzos necesarios para mejorar la ciberseguridad de su organización.

Le permite **planificar las medidas que es necesario adoptar** y el grado de urgencia al conocer la repercusión de un posible incidente en las diferentes partes de su negocio.

Puede demostrar a sus clientes que dispone de una estrategia para mejorar el nivel de ciberseguridad de sus procesos mejorando su imagen como un **proveedor más seguro y fiable**.

S2 GRUPO

Anticipando un mundo
ciberseguro

MADRID
Avda de Manoteras 46
BIS 6ºC
28050 Madrid
T (34) 902 882 992

BARCELONA
Llull, 321
08019 Barcelona
T (34) 933 030 060

VALENCIA CERT
Ramiro de Maeztu, 7
46022 Valencia
T (34) 963 110 300
F (34) 963 106 086

VALENCIA HQ
Doctor Juan Regla, 6
46010 Valencia
T (34) 960 010 105

SEVILLA
C/Gonzalo Jiménez de
Quesada 2, Planta 18
41092 Sevilla
T (34) 902 882 992

SAN SEBASTIAN
Juan Fermín Gilisagasti
nº 2 (Zuatzu)
Edificio Pi@ Oficina 121
Donostia 20018
T (34) 902 882 992

SANTIAGO DE CHILE
Calle Padre Mariano N° 82
of. 1102, Providencia,
T (56) 9 9440 4365

MÉXICO D.F.
Monte Athos 420
CDMX 11000
T (52) 55 5035 7868

BOGOTÁ
Carrera 14, nº 98-51,
Oficina 701
T (571) 745 74 39

BRUSELAS
Rue belliard,20.
1040
T (32) (0) 474 532 974

LISBOA
Avda do Brasil, nº1,
1749-008 Lisboa
T (351) 217 923 729

Síguenos en: • @s2grupo • s2grupo.es