



GRUPO
Anticipating a
cyber secure world



CASE STUDY

Automotive Sector



Cybersecurity to meet present and future challenges.

Brief presentation of the company



Our customer is a leading supplier of components for various **automobile manufacturers**.



It manufactures elements that are part of the **car body and interior**.



It is a clear example of a company that is part of the **supply chain**. Of several important companies in the automotive sector.



It has several production plants where the different accessories it supplier are manufactured and from where the planned deliveries to its different customers are made.




02


Description of the problem/challenge

The organization **has no experience** in the field of industrial cybersecurity. It is aware of the risks it faces but does not know what it needs to do to improve its situation or how to address them.






It has an IT department that is responsible for keeping the corporate IT network up to date, from where ERP, financial, accounting and HR management operations are carried out. **But it does not have personnel with knowledge or experience in operational cybersecurity.**



It wants to know how to improve its situation. It has a rough idea of the risks it runs and the possible consequences of an incident.



Its customers are beginning to **demand cybersecurity measures** in the supply contracts it has with them. In order to participate in the successive agreements for which it is eligible, its customers demand that it implement specific cybersecurity measures. It has neither the knowledge nor the resources to do so.

Description of the work performed

As a first approach, an **assessment of the organization's current state of cybersecurity is proposed** in order to subsequently propose an **improvement Plan**.




1

A visit is made to one of the main plants with the collection of all available information: inventory of IT and OT equipment and devices, network architectures, existing procedures.

2

Interviews are conducted with the main managers of the production process, such as the plant manager, the maintenance manager and the IT department, in order to learn about the operation of the plant, its processes and the degree of segmentation of the IT and OT networks.

3

It is verified that the organization **does not have cybersecurity procedures in the operational part**: updated maintenance of assets inventory and network architectures, user management, access management, relationship with third parties (suppliers, maintainers and clients).



4

Given the difficulties of performing a technical intrusion test in a production process, **a series of visibility tests are performed**, with a limited and previously agreed test plan, in order to identify if there is access to the OT network from the corporate network and the degree of protection of the different Wi-Fi networks: corporate, public, etc.

5

Risk analysis. The main points of the process, the factors that affect them and the impact of a possible incident to these parts of the business are identified.

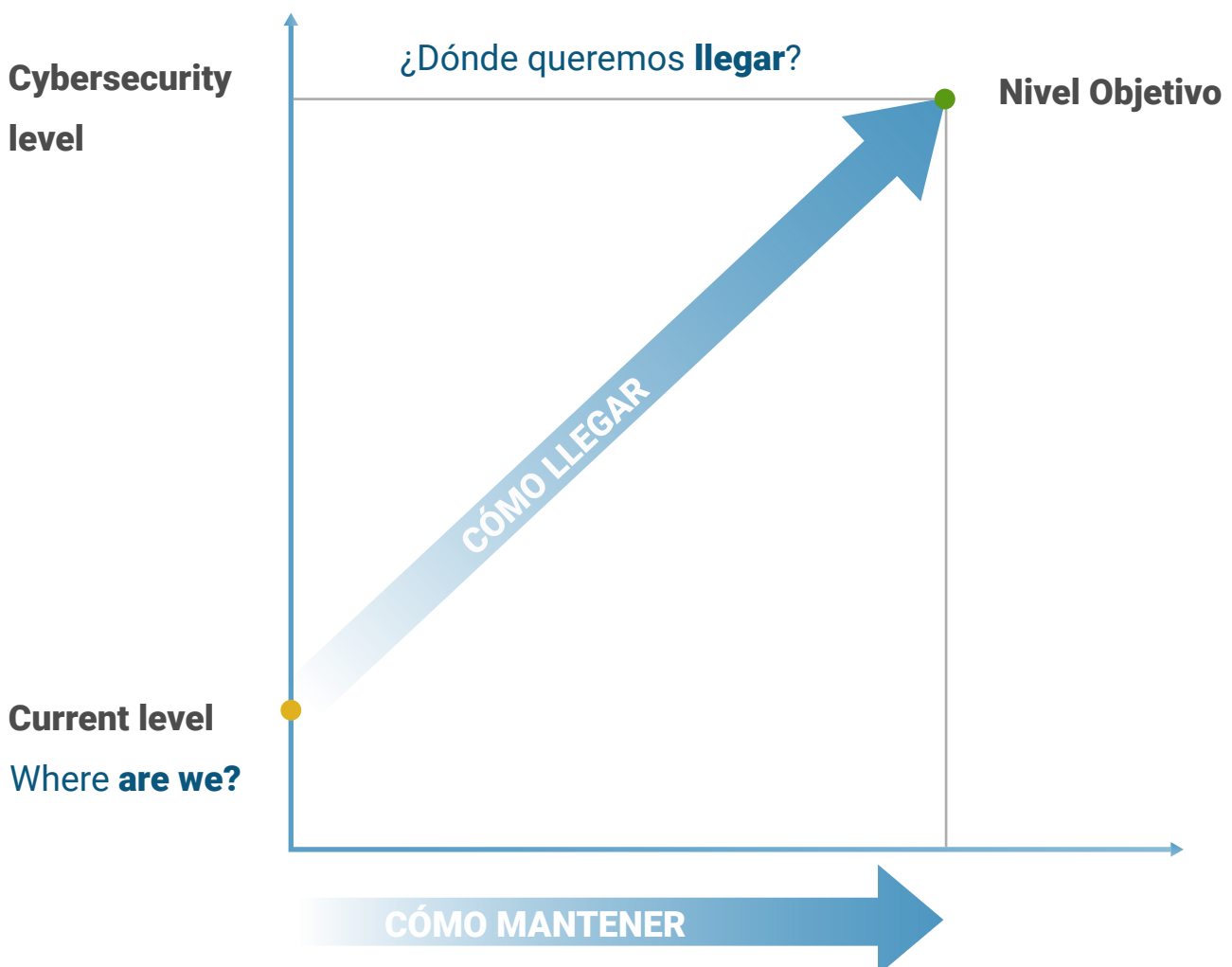
6


An **Improvement Plan** is drawn up with all the information collected, with different degrees of implementation. From the most basic and fastest to adopt aspects to the most ambitious measures with a longer and more costly implementation period.

Benefits Obtained





As a result of the actions carried out, the client obtains a **series of benefits:**







Have a diagnosis of your **current real state**. A first analysis of your weaknesses and an estimate of the efforts needed to improve your organization's cybersecurity.



Allows you to **plan the measures that need to be taken** and the degree of urgency by knowing the impact of a potential incident on different parts of your business.



You can demonstrate to your customers that you have a strategy to improve the cybersecurity level of your processes by enhancing your image as **a more secure and reliable supplier**.



GRUPO
Anticipating a
cyber secure world

MADRID

Avda de Manoteras 46
BIS 6°C
28050 Madrid
T (34) 902 882 992

BARCELONA

Lluïa, 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

Dr Joan Reglà, 6 bajo
46010 Valencia
T (34) 963 110 300
F (34) 963 106 086

SEVILLA

Calle Gonzalo Jiménez
de Quesada 2, Planta 18
Edificio Torre Sevilla
41092 Sevilla
T (34) 902 882 992

SAN SEBASTIÁN

C/ Juan Fermín Gillisagasti
nº 2 (Zuatzu)
Edificio Pi@ - Oficina 121
20018 Donostia
T (34) 902 882 992



SANTIAGO DE CHILE

Calle de Padre Mariano
Nº 82 of. 1102
Comuna de Providencia
T +56 9 9440 4365

C.D. MÉXICO

Monte Athos 420
CDMX 11000
T (+52) 55 5035 7868

BOGOTÁ

Carrera 14, nº 98-51,
Oficina 701
T (57) 601 745 74 3

BRUSELAS

Rue Beillard, 20
1040 Bruselas
T (32) (0) 474 532 974

LISBOA

Av. do Brasil, 1
1749-008 Lisboa
T (351) 21 7923729

ROTTERDAM

Stationsplein 45, 4th floor
3013 AK Rotterdam
T (34) 963 110 300

Síguenos en



@s2grupo



s2grupo.es