



GRUPO  
Anticipating a  
cyber secure world



CASE STUDY

# Food Sector



Cybersecurity to meet present and future challenges.

# Brief presentation of the company



Our client is a multinational company in the **food** sector.



It has different plants in a number of countries around the **world**.



It has recently suffered an **incident** that has affected its food processing and preservation processes with **repercussions** on the development of its business.



As a large and complex organization, it requires a global approach to adopt a general **OT cybersecurity framework** adapted to the different stages of maturity of the company's various facilities: different locations, cultures, issues, etc.



02

## Description of the problem/challenge

It is a **complex organization** with many departments, plants, processes and suppliers. It has global service providers who are managing its communications networks. It has no experience in **OT cybersecurity** and its IT suppliers have no knowledge or experience in this field.





This is a **high-risk sector**.

Food production and processing is an essential sector. It is a supplier to the distribution sector.



You are aware that you do not have an **OT cybersecurity** procedural framework in place and the **risk** this poses to your business. You have already experienced the negative effects of a **cyber incident**.



It requires an expert analysis that can provide you with a **general solution** to be implemented throughout the organization in a progressive manner and that **improves** your **cybersecurity** conditions.

## Description of the work performed

The organization is approaching this **problem** in phases: first it will conduct an **analysis** of one of its main **production plants**. The first step will be to **identify** the **devices, networks** and **components** in this plant as a representative sample of the rest of the organization.



  
**1**

A **multidisciplinary team** made up of personnel with experience in the industrial sector and technical personnel with knowledge of networks and security will travel to the plant.

**2**

A network traffic analysis probe is installed with the intention of carrying out a **detailed inventory of the plant's devices**. Only in one of the first areas to be inventoried, more than **1,000** different devices were detected, with the consequent complexity of an inventory of assets with this procedure. In agreement with the client, it was decided to carry out an inventory by groups of assets according to the different zones and stages of production.

**3**

**Interviews are carried out both with key production process managers and service providers.**

## Description of the work carried out

In a second step, a risk **analysis** of the plant under study and a general **industrial cybersecurity framework** for the entire organization will be developed.



NISTIR 8183  
Revision 1

### Cybersecurity Framework Version 1.1 Manufacturing Profile

Keith Stouffer  
Timothy Zimmerman  
Chee Yee Tang  
Joshua Lubell  
Jeffrey Cichonski  
Michael Pease  
Jhon McCarthy

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8183r1>

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce



**4**

It is found that the organization **does not have OT cybersecurity procedures**. A **general training and awareness plan** for the entire organization is needed.

**5**

**A series of visibility tests are performed.**

With a limited and previously agreed test plan. The presence of a number of vulnerabilities is tested.

**6**

A **risk analysis** of the factory is prepared.




**7**

Taking the **NIST.IR.8183** standard as a reference document, a cybersecurity framework is prepared for its extension to all the company's plants.



## Benefits obtained

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

-  To evaluate the actual current state of one of its **main factories**. As a representative sample of the real state of the rest of the organization.
-  To have a **Risk Analysis** of this plant. Since it is one of the main production centers of the company, it is a sample of the state of the rest of the company. With an evaluation of the impact of an incident and the corrective measures proposed according to the degree of urgency.
-  To have a general framework based on the **NIST.IR.8183** reference standard and its application to the plant that is the object of the first analysis with the diagnosis of the state according to the different domains of the document and that can serve as a template for application to the rest of the company's plants.

Function Unique Identifier	Function	Category Unique Identifier	Category
<b>ID</b>	<b>Identify</b>	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
<b>PR</b>	<b>Protect</b>	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
<b>DE</b>	<b>Detect</b>	PR.PT	Protective Technology
		DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
		RS.RP	Response Planning
<b>RS</b>	<b>Respond</b>	RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
		RC.RP	Recovery Planning
<b>RC</b>	<b>Recovery</b>	RC.M	Improvements
		RC.CO	Communications



**MADRID**  
Avda de Manoteras 46  
BIS 6°C  
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**  
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 Gilisagasti  
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