



CASO DE ÉXITO

Sector Alimentación



Breve presentación de la empresa



Nuestro cliente es una multinacional del sector de la **alimentación**.



Dispone de diferentes plantas en una serie de países de todo el **mundo**.



Ha sufrido recientemente algún **incidente** que ha afectado a sus procesos de elaboración y conservación de alimentos con **repercusiones** en el desarrollo de su negocio.



Al tratarse de una organización grande y compleja requiere de un planteamiento global que permita adoptar un marco general de **ciberseguridad OT** adaptado a diferentes estados de madurez de las diferentes instalaciones de la compañía: distintos emplazamientos, culturas, problemáticas, etc.

Descripción de la problemática/reto

Se trata de una **organización compleja** con muchos departamentos, plantas, procesos y proveedores. Dispone de proveedores globales de servicios que están gestionando sus redes de comunicaciones. No tiene experiencia en **ciberseguridad OT** y sus proveedores **IT** no disponen de conocimientos ni experiencia en este campo.





Se trata de un sector de **alto riesgo**. La producción y elaboración de alimentos es un sector esencial. Es proveedor del sector de la distribución.



Es consciente de que no dispone de un marco procedimental de **ciberseguridad OT** y del **riesgo** que eso supone para su negocio. Ya ha tenido ocasión de comprobar los efectos negativos de un **ciberincidente**.



Requiere de un análisis experto que pueda ofrecerle una **solución general** para implantar en toda la organización de forma progresiva y que **mejore** sus condiciones de **ciberseguridad**.

Descripción de la actuación realizada

La organización aborda este **problema** por fases: primero realizará un **análisis** de una de sus principales **plantas de producción**. El primer paso será una **identificación** de los **dispositivos, redes y componentes** de esta planta como muestra representativa del resto de la organización.



1

Se desplazan a la planta un **equipo multidisciplinar** formado por personal con experiencia en el sector industrial y personal técnico con conocimiento de redes y seguridad.

2

Se instala una sonda de análisis del tráfico de red con la intención de realizar un **inventario detallado de la relación de dispositivos** de la planta. Sólo en una de las primeras zonas que se someten a inventariado se detectan mas de **1.000** dispositivos diferentes con la consiguiente complejidad de abordar un inventario de activos con este procedimiento. De acuerdo con el cliente se decide realizar un inventario por grupos de activos según las diferentes zonas y etapas de producción.

3

Se llevan a cabo **entrevistas** tanto con los principales **responsables del proceso de producción** como con los **proveedores de servicios**.

Descripción de la actuación realizada

En un segundo paso se elaborará un **análisis** de riesgos de la planta en **estudio** y un **framework** general de **ciberseguridad industrial** para toda la organización.



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

Se comprueba que la organización **no dispone de procedimientos de ciberseguridad OT**. Es necesario un **plan general de formación y concienciación** de toda la organización.

5

Se realizan una serie de pruebas de visibilidad. Con un plan de pruebas limitado y previamente acordado. Se comprueba la presencia de un a número de vulnerabilidades.

6




Se elabora un **Análisis de riesgos** de la factoría.

7

Tomando como documento de referencia la norma **NIST.IR.8183** se elabora un framework de ciberseguridad para su extensión a todas las plantas de la compañía.

Beneficios obtenidos

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

-  Evaluar el estado real actual de una **de sus principales factorías**. Como muestra representativa del estado real del resto de la organización.
-  Disponer de un **Análisis de Riesgos** de esta planta. Al tratarse de uno de los principales centros de producción de la empresa es una muestra del estado del resto de la compañía. Con una evaluación del impacto de un incidente y las medidas correctoras propuestas según el grado de urgencia.
-  Contar con un framework general basado en la normativa de referencia **NIST.IR.8183** y su aplicación a la planta objeto del primer análisis con el diagnóstico del estado según los diferentes dominios del documento y que puede servir de plantilla de aplicación al resto de plantas de la empresa.

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



GRUPO

Anticipando un mundo
ciberseguro

MADRID

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

BARCELONA

Lluís, 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

CIC ROTTERDAM

Stationsplein 45, 4th floor
3013 AK Rotterdam
The Netherlands
T (34) 963 110 300
F (34) 963 106 086

Síguenos en:



@s2grupo



s2grupo.es