GUÍA DE BOLSILLO

CIBERSEGURIDAD EN LA PIRÁMIDE DE AUTOMATIZACIÓN INDUSTRIAL

Las tecnologías empleadas en la **automatización y gestión de procesos productivos** quedan representadas en la llamada **"Pirámide de Automatización"**, la cual recoge los **cinco niveles tecnológicos** que se pueden encontrar en un entorno industrial.

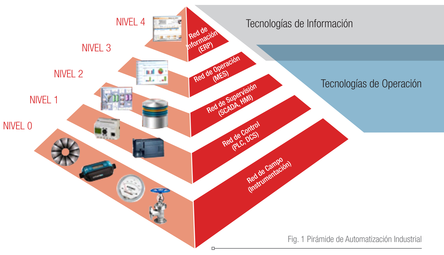

Fig. 1 Pirámide de Automatización Industrial

NIVEL 0

Nivel de adquisición de datos de campo o instrumentos, es decir, sensores y actuadores que se encuentran repartidos por el proceso y que permiten el control de las máquinas y equipos de producción.

Este documento se centra en los **sensores inalámbricos.**

NIVEL 1

Nivel que agrupa a todos **controladores locales** tales como: ordenadores, PLCs, etc.

Los equipos de este nivel utilizarán **datos del proceso** proporcionados por los instrumentos del NIVEL 0 y darán **consignas a los actuadores.**

NIVEL 2

Nivel de supervisión con equipos destinados a **controlar la secuencia de fabricación y/o producción** como: SCADA, estaciones de operaciones o servidores de ingeniería.

NIVEL 3

Nivel de operaciones de fabricación donde se **gestionan los flujos de trabajo** para producir u optimizar los productos finales.

NIVEL 4

Nivel de **gestión** donde se desarrolla todas las actividades relacionadas con el negocio necesarias en una **organización** industrial, **comunicando** distintas plantas y manteniendo **relaciones** con proveedores y clientes.

	Niveles de la pirámide de Automatización Industrial				
Principales vulnerabilidades que pueden existir*	0	1	2	3	4
Falta de medidas de seguridad física	•	•	•	•	•
Arquitectura de red insegura	•	•	•	•	•
Posibilidad de Interceptar y alterar comportamiento de sensor	•				
Debilidad en los protocolos de comunicación	•	•	•	•	•
Instalación configuración incorrecta o servicios innecesarios habilitados	•	•	•	•	
Falta de actualización de software		•	•	•	•
Fallos 0-day	•	•	•	•	•
Almacenamiento sin protección		•	•	•	•
Debilidad frente a Desbordamiento de buffer		•	•	•	•
Debilidad en identificación y autenticación (contraseñas)		•	•	•	
Asignación incorrecta de privilegios		•	•	•	•
Debilidad frente a Fuzzing (técnicas para proporcionar datos invalidos e inesperados)		•	•	•	
Debilidad frente a ataques de Cross-Site Scripting			•	•	•
Debilidad frente a ejecución de código remoto			•	•	•
Personal de planta no capacitado en tecnologías de operación y/o información	•	•	•	•	
Personal de TI no capacitado en tecnologías de operación	•		•	•	•
Acuerdos de nivel de servicio insuficientes	•	•	•	•	•
Falta de control de cambios	•	•	•	•	•
Falta de planes de continuidad	•	•	•	•	•
Falta de procedimientos adecuados en el uso de las tecnologías de operación		•	•	•	
Personal contratado inadecuado o sin concienciación o formación en ciberseguridad	•	•	•	•	•
Falta de mecanismos de monitorización	•	•	•	•	•
Conexiones públicas desprotegidas	•	•	•	•	•
Uso de herramientas de red no permitidas	•	•	•	•	•
Existencia de servidores dual home		•	•	•	•
Interfaz de acceso inadecuados			•	•	•
Documentación escasa	•	•	•	•	•
No realización de copias de seguridad (Perdida de datos, Ransomware,...)		•	•	•	•
Carencia de software anti-malware		•	•	•	•
Utilización de usuarios genéricos		•	•	•	•

* Lista de Vulnerabilidades incluidas en el documento "Guía Práctica para la Construcción de un Sistema de Gestión de la Ciberseguridad Industrial" https://www.CCI-es.org/informes-y-analisis-estategicos

	Etapas del Ciclo de Vida de un Proyecto de Automatización Industrial				
Principales Medidas de Protección por Niveles**	Diseño	Provisión	Ejecución	Operación y mantenimiento	Desmantelamiento
Modelado de amenazas (identificación de activos y vectores de ataque)	0 1 2 3 4	N/A	N/A	0 1 2 3 4	0 1 2 3 4
Análisis de riesgos	0 1 2 3 4	N/A	N/A	0 1 2 3 4	0 1 2 3 4
Medidas de protección físicas	0 1 2 3 4	N/A	N/A	0 1 2 3 4	0 1 2 3 4
Diseño seguro de red	0 1 2 3 4	N/A	N/A	N/A	N/A
Definición o aplicación de modelo de defensa en profundidad	0 1 2 3 4	N/A	0 1 2 3 4	0 1 2 3 4	N/A
Diseño o gestión de acceso (autenticación y autorización)	1 2 3 4	N/A	1 2 3 4	1 2 3 4	N/A
Definición o aplicación de Segmentación y filtrado de red	1 2 3 4	N/A	1 2 3 4	1 2 3 4	N/A
Definición o protección mediante antivirus y Listas blancas	2 3 4	N/A	2 3 4	2 3 4	N/A
Definición o implantación de Cifrado	2 3 4	N/A	2 3 4	2 3 4	N/A
Definición o adecuación de configuración de red, sistemas y aplicaciones	1 2 3 4	N/A	1 2 3 4	1 2 3 4	N/A
Diagnóstico de debilidades	0 1 2 3 4	N/A	0 1 2 3 4	0 1 2 3 4	N/A
Análisis exhaustivo de la cadena de suministro y sus proveedores	N/A	0 1 2 3 4	N/A	N/A	N/A
Acuerdos de Nivel de servicio con requisitos adecuados de ciberseguridad	N/A	0 1 2 3 4	0 1 2 3 4	0 1 2 3 4	N/A
Validación de las funcionalidades de ciberseguridad de los componentes	N/A	0 1 2 3 4	0 1 2 3 4	N/A	N/A
Verificación de la adopción de prestaciones de ciberseguridad de los sistemas	N/A	0 1 2 3 4	0 1 2 3 4	N/A	N/A
Garantizar las versiones de software contratadas - Gestión de parches	N/A	1 2 3 4	1 2 3 4	1 2 3 4	N/A
Comprobar documentación sobre características físicas y de ciberseguridad	N/A	0 1 2 3 4	0 1 2 3 4	N/A	N/A
Verificación de cumplimiento de requisitos de ciberseguridad	N/A	N/A	0 1 2 3 4	N/A	N/A
Test de intrusión (como parte de las Pruebas FAT y SAT)	N/A	N/A	0 1 2 3 4	N/A	N/A
Plan de pruebas integral y multidimensional	N/A	N/A	0 1 2 3 4	N/A	N/A
Supervisión y gestión de incidentes en la operación y mantenimiento	N/A	N/A	N/A	0 1 2 3 4	N/A
Protección de las consolas de operación y supervisión	N/A	N/A	N/A	2 3 4	N/A
Gestión de la seguridad de red	N/A	N/A	N/A	0 1 2 3 4	N/A
Formación y concienciación	N/A	N/A	N/A	0 1 2 3 4	N/A
Comprobación de antecedentes	N/A	0 1 2 3 4	0 1 2 3 4	0 1 2 3 4	N/A
Gestión de cambios derivados de incidentes de ciberseguridad	N/A	N/A	N/A	0 1 2 3 4	N/A
Segregación de funciones	N/A	N/A	N/A	2 3 4	N/A
Proceso continuo de gestión de la ciberseguridad	N/A	N/A	N/A	0 1 2 3 4	N/A
Destrucción de datos	N/A	N/A	N/A	N/A	1 2 3 4
Conservación y recuperación de datos	N/A	N/A	N/A	N/A	1 2 3 4

** Lista de Medidas incluidas en el documento "Ciberseguridad en el Ciclo de Vida en un Proyecto de Automatización Industrial" https://www.CCI-es.org/informes-y-analisis-estategicos