

Ciberseguridad de máquinas industriales y sistemas de control

Más valor.
Más confianza.

Protege las funciones de seguridad frente a alteraciones digitales

TÜV SÜD te ayuda a identificar los riesgos, proteger la seguridad de las personas y definir una hoja de ruta aplicable a cada máquina

Las máquinas industriales incorporan PLC, HMI, software, redes, dispositivos conectados, puertos de mantenimiento y accesos remotos. Una modificación accidental o intencionada puede afectar a parámetros, configuraciones o funciones esenciales.

Una máquina no necesita estar conectada permanentemente a internet para presentar riesgos. Un ordenador de ingeniería, una memoria USB, una conexión temporal o un componente comprometido pueden modificar su comportamiento.

Las consecuencias pueden incluir **movimientos inesperados, pérdida de funciones de seguridad, fabricación fuera de especificación, paradas prolongadas o imposibilidad de recuperar una configuración fiable.**

¿Por qué evaluar la ciberseguridad de una máquina?

Una alteración digital puede afectar a:

- paradas de emergencia y enclavamientos;
- barreras, escáneres y resguardos;
- límites de velocidad, fuerza o posición;
- comunicaciones entre PLC, robots y accionamientos;
- software y configuraciones relevantes para la seguridad.

No basta con saber si la máquina está conectada. Debes conocer qué puede modificarse, quién puede hacerlo y qué consecuencias tendría sobre las personas, el equipo y la producción.



Ciberseguridad y Reglamento de Máquinas

El Reglamento (UE) 2023/1230, aplicable con carácter general desde el 20 de enero de 2027, incorpora requisitos de protección frente a la corrupción accidental o intencionada de hardware, software y datos cuando pueda producirse una situación peligrosa.

Este alcance se centra en **evitar que una alteración digital comprometa la seguridad de la máquina**. No sustituye una evaluación global de la infraestructura OT ni un sistema de gestión conforme a ISO/IEC 27001.

¿A quién se dirige?

- **Fabricantes e integradores**: Para incorporar seguridad digital desde el diseño, establecer requisitos para componentes y proveedores y generar evidencias para la conformidad de máquinas nuevas.
- **Empresas usuarias**: Para evaluar equipos instalados con acceso remoto, software modificable, conexiones con la red de planta o componentes actualizados.
- **Compras e ingeniería**: Para incluir **requisitos verificables de ciberseguridad** en las especificaciones técnicas y criterios de aceptación de nuevas máquinas.

¿Cómo realizamos el diagnóstico?

Definimos la máquina y sus límites, identificamos componentes y conexiones, revisamos PLC, HMI, software y accesos, analizamos posibles alteraciones y valoramos sus consecuencias.

Según el alcance, podemos aplicar referencias de la serie IEC 62443. IEC 62443-3-2 estructura la evaluación de riesgos mediante zonas, conductos y niveles de seguridad objetivo, mientras que IEC 62443-4-2 establece requisitos técnicos para componentes de sistemas de control.

¿Qué recibirá tu empresa?

El entregable puede incluir:

- inventario de activos y conexiones relevantes;
- arquitectura revisada;
- escenarios de amenaza y alteración;
- matriz priorizada de riesgos;
- vulnerabilidades y carencias documentales;
- requisitos para proveedores e integradores;
- plan de acciones y análisis del riesgo residual.

El resultado no es un listado genérico de vulnerabilidades, sino una hoja de ruta adaptada a la máquina y a su ciclo de vida.

¿Por qué elegir TÜV SÜD?

Combinamos **ciberseguridad industrial, seguridad de máquinas, evaluación de riesgos, seguridad funcional, conformidad reglamentaria y revisión documental.** Esta visión integrada permite proteger la máquina sin comprometer innecesariamente su disponibilidad o funcionalidad.



Servicios relacionados

- Seguridad de máquinas
- Elevación industrial

TUV SUD IBERIA S.A.U.
tuvsud.com/es-es/ciberseguridad-maquinas

Solicita tu presupuesto

2026 © TÜV SÜD IBERIA S.A.U. | ES-MKG/COG/550/es/ES