Checklist de Cumplimiento

Reglamento (UE) 2023/1230 — Ciberseguridad y Seguridad de Maquinaria

Objetivo: Identificar activos críticos en riesgo de inmovilización por incumplimiento de ciberseguridad y seguridad física integrada. Fecha límite de adaptación completa: 14 de enero de 2027.

Empresa: _____ **Responsable:** _____ **Fecha:** _____

1 Inventario de Activos Conectados

Identifica qué maquinaria es susceptible de ser auditada

- ☐ **1.1** Tenemos un listado de toda la maquinaria que usa software, sensores, cámaras o está conectada a la red.
  Incluye: AMR, AGV, carretillas inteligentes, sistemas de picking, muelles automáticos, básculas conectadas.
- ☐ **1.2** Sabemos qué equipos fueron adquiridos o modernizados después de enero de 2023.
  Los equipos nuevos deben cumplir obligatoriamente el nuevo estándar. Los anteriores siguen bajo la Directiva 2006/42/CE.
- ☐ **1.3** Ningún equipo ha sido importado directamente de fuera de la UE por nuestra cuenta sin verificar certificación.
  Si importas directamente, tú eres el responsable legal de la certificación — no el fabricante extranjero.

2 Documentación Legal

El 'pasaporte' de la máquina — sin esto el activo es vulnerable

- ☐ **2.1** Tenemos la Declaración de Conformidad UE actualizada para cada equipo.
  Debe mencionar específicamente el Reglamento (UE) 2023/1230. Si solo cita la Directiva 2006/42/CE, está desactualizada.
- ☐ **2.2** Disponemos del Expediente Técnico Digital del fabricante, incluyendo el informe de evaluación de riesgos de ciberseguridad.
  Este informe debe describir las vulnerabilidades evaluadas y las medidas adoptadas. Si no existe, es un vacío legal inmediato.
- ☐ **2.3** Todos los equipos tienen el marcado CE visible y legible.
  Sin marcado CE la inmovilización es automática ante cualquier inspección de vigilancia de mercado.

3 Ciberseguridad Operativa

La capa invisible — la seguridad física ya no existe sin ciberseguridad

- ☐ **3.1** Las actualizaciones de firmware de nuestras máquinas provienen siempre del fabricante o fuente verificada.
  Firmware no oficial puede invalidar la certificación de seguridad y generar responsabilidad legal directa.
- ☐ **3.2** Los robots y carretillas inteligentes operan en una red aislada, sin acceso abierto a internet.
  La conexión directa a internet expone los sistemas a ataques remotos que el reglamento considera fallos de seguridad física.
- ☐ **3.3** Existe un registro de qué personal tiene acceso para modificar los parámetros de seguridad o lógica de las máquinas.
  El control de accesos es un requisito explícito del reglamento para sistemas con IA o automatización avanzada.

4 Auditoría de Proveedores

Delegar la compra no es delegar la responsabilidad

- ☐ **4.1** En los contratos de compra o leasing existe una cláusula donde el proveedor garantiza el cumplimiento del Reglamento (UE) 2023/1230.
  Sin esta cláusula, ante una vulnerabilidad de ciberseguridad, la responsabilidad recae enteramente sobre el operador.
- ☐ **4.2** El fabricante ofrece soporte técnico activo para la seguridad del software durante toda la vida útil del equipo.
  Un fabricante que no ofrece actualizaciones de seguridad convierte el equipo en un pasivo legal con el tiempo.

Veredicto de Riesgo — Cómo interpretar tus respuestas

Respuestas NO	Nivel de riesgo	Acción inmediata
Menos de 2	■ BAJO	Mantener registro actualizado y revisión anual.
3 a 5	■ MEDIO	Solicitar auditoría técnica al proveedor antes de 30 días.
Más de 5	■ CRÍTICO	Paralizar nuevas adquisiciones y contactar con asesoría legal/técnica urgentemente.

Cómo usar este checklist: Reúne las fichas técnicas de tus principales máquinas. Si al revisar la documentación no se hace mención a 'Ciberseguridad' o al 'Reglamento 2023/1230', tienes un vacío legal que cubrir con el proveedor antes de la próxima auditoría de mercado.

Modelo de requerimiento al proveedor

Utiliza esta plantilla para solicitar la documentación de cumplimiento a tus proveedores de maquinaria. Personaliza los campos entre corchetes.

ASUNTO: Requerimiento urgente — Certificación Reglamento (UE) 2023/1230

A la atención del Departamento Técnico / Dirección Comercial de [Nombre del Proveedor]:

En el marco de nuestra política interna de auditoría de cumplimiento normativo, y de conformidad con el Reglamento (UE) 2023/1230 relativo a las máquinas, les solicitamos la siguiente documentación actualizada para los equipos suministrados a nuestras instalaciones (ref.: [ID del equipo / nº de serie]):

1. **Declaración de Conformidad UE actualizada** — con mención expresa del cumplimiento del Reglamento (UE) 2023/1230.
2. **Informe de Evaluación de Riesgos de Ciberseguridad** — certificando que el firmware no presenta vulnerabilidades que comprometan la seguridad física o la integridad de nuestra red operativa.
3. **Expediente Técnico del Fabricante** — disponible según lo exigido para la comercialización de equipos en la Unión Europea.

Les recordamos que cualquier incumplimiento en la certificación nos obliga a adoptar medidas preventivas, pudiendo derivar en la inmovilización de los activos afectados. Solicitamos respuesta en un plazo máximo de **[10 días hábiles]**.

Atentamente,

[Tu nombre y firma] · Dirección de Operaciones · [Empresa]