ANMOPYC

ASOCIACIÓN ESPAÑOLA DE FABRICANTES DE MAQUINARIA DE CONSTRUCCIÓN, OBRAS PÚBLICAS Y MINERÍA

CAMPAG

Cluster Aragonés de los Medios de Producción Agrícolas y Ganaderos

**Documento divulgativo**

# Informe sobre ciberseguridad industrial en el sector maquinaria

22 de Octubre de 2025

Actividad financiada parcialmente por el Instituto Aragonés de Fomento a través de la convocatoria de ayudas de 2025 a Agrupaciones Empresariales Innovadoras para la realización de proyectos colaborativos (Nº expediente 25/036-013).

IAF Instituto Aragonés de Fomento

GOBIERNO DE ARAGON

# Índice

# 1. Introducción

## 1.1. Contexto del proyecto securizAR y papel de ANMOPYC y CAMPAG

La ciberseguridad industrial se ha consolidado en los últimos años como un factor crítico para la competitividad y sostenibilidad del tejido manufacturero. La creciente digitalización de los procesos productivos y la integración de tecnologías avanzadas —como la robótica, el internet industrial de las cosas (IIoT) o la analítica de datos— han ampliado exponencialmente la superficie de exposición a riesgos cibernéticos en las plantas industriales. En este contexto, el proyecto *securizAR – Impulsar la ciberseguridad industrial en Aragón* se concibe como una iniciativa estratégica orientada a fortalecer la protección digital de la industria aragonesa, con especial atención al sector de la maquinaria de construcción, minería y agrícola.

El proyecto se desarrolla bajo el liderazgo de **ANMOPYC** (Asociación Española de Fabricantes Exportadores de Maquinaria para Construcción, Obras Públicas y Minería) y **CAMPAG** (Clúster Aragonés de los Medios de Producción Agrícolas y Ganaderos), entidades que representan un tejido empresarial diverso, con una fuerte orientación a la exportación y un alto nivel de tecnificación industrial. Ambas organizaciones actúan como agentes vertebradores entre las empresas, los centros tecnológicos y las administraciones públicas, promoviendo la cooperación en torno a la innovación, la digitalización y la seguridad industrial.

A través de ***securizAR***, ANMOPYC y CAMPAG han impulsado un trabajo conjunto de diagnóstico, formación y transferencia de conocimiento, con el propósito de elevar el nivel de madurez en ciberseguridad de las empresas del sector, generar sinergias con el ecosistema tecnológico regional y posicionar a Aragón como un referente en materia de ciberseguridad industrial.

## 1.2. Ciberseguridad industrial como pilar estratégico de la industria conectada

La ciberseguridad en la industria manufacturera ya no es una opción, sino un requisito imprescindible para sostener la transformación digital. La creciente digitalización, la interconexión de sistemas IT y OT, el uso de IoT industrial, inteligencia artificial y plataformas en la nube, genera ventajas operativas significativas, pero también amplía la superficie de ataque. La protección de los sistemas industriales debe centrarse en tres dimensiones fundamentales:

- **Disponibilidad:** garantizar que las líneas de producción, sistemas de control y maquinaria crítica permanezcan operativos, evitando paradas imprevistas que puedan interrumpir la fabricación o la cadena de suministro.
- **Integridad:** asegurar que los datos de producción, parámetros de máquinas y sensores no sean manipulados, evitando errores que puedan afectar la calidad, la seguridad del personal o el correcto funcionamiento de los procesos.
- **Confidencialidad:** proteger información sensible sobre productos, procesos, clientes o propiedad intelectual frente al espionaje industrial o el robo de datos.

Proteger estas dimensiones no depende únicamente de soluciones tecnológicas. Es fundamental implementar medidas organizativas y formativas: concienciar a los operarios, establecer protocolos rigurosos con proveedores y colaboradores, y diseñar la infraestructura y las aplicaciones con seguridad desde el inicio, siguiendo el principio de **security by design**. En este sentido, la ciberseguridad se convierte en un pilar estratégico de la transformación digital, ya que sin ella, los beneficios de la automatización, la conectividad y la analítica avanzada no pueden aprovecharse de manera segura ni sostenible.

El proyecto *securizAR* se enmarca precisamente en este contexto: fomentar la concienciación, la capacitación y la adopción de medidas de seguridad digital adaptadas a la realidad del sector de maquinaria, contribuyendo al desarrollo de una cultura de prevención y resiliencia cibernética en la industria aragonesa.

## 1.3. Objetivos del informe

Este informe surge con el propósito de proporcionar una visión completa y accesible sobre las **amenazas actuales y emergentes en entornos industriales**, así como sobre las **tendencias de digitalización** y las **buenas prácticas** para su gestión. Busca, por un lado, ayudar a las empresas manufactureras y a los fabricantes de maquinaria a entender los riesgos asociados a la convergencia IT/OT, al uso de IoT industrial, a la inteligencia artificial y a la computación en la nube. Por otro lado, pretende ofrecer una guía práctica y realista de **medidas de protección**, alineadas con las directrices europeas, como NIS2 y CRA, y con recomendaciones de organismos nacionales de referencia en ciberseguridad, como INCIBE y CCN-CERT.

De manera más amplia, este documento persigue fomentar una **cultura de ciberseguridad sólida y consciente**, donde la protección de sistemas, datos y procesos críticos esté integrada en la estrategia empresarial. Solo así será posible que la transformación digital cumpla su promesa de eficiencia, resiliencia y sostenibilidad, reduciendo la exposición a incidentes y fortaleciendo la confianza en la operación de la industria manufacturera.

El informe adopta un enfoque técnico y divulgativo, buscando servir tanto a empresas con un nivel de madurez avanzado como a aquellas que se encuentran en etapas iniciales de su transformación digital, promoviendo una visión integral de la ciberseguridad como elemento habilitador de la innovación y la competitividad industrial.

# 2. Principales amenazas en entornos de fabricación

La revolución digital que ha transformado la industria manufacturera en las últimas décadas ha traído consigo una eficiencia sin precedentes y un nivel de automatización que antes era impensable. Sensores conectados, maquinaria inteligente, sistemas de control industrial y plataformas en la nube permiten supervisar en tiempo real las operaciones, optimizar la producción y mejorar la trazabilidad de los productos. Sin embargo, esta interconexión masiva también ha creado un nuevo ecosistema de riesgos. Cada dispositivo conectado, cada actualización remota de software, cada acceso a la nube o a un sistema de control industrial (OT) es un punto potencial de entrada para un atacante. Los ciberdelincuentes, los grupos organizados e incluso actores estatales han identificado estas vulnerabilidades y, con creciente sofisticación, buscan comprometer procesos, robar información o interrumpir la producción de manera deliberada.

Las amenazas en entornos de fabricación no son homogéneas: abarcan desde ataques técnicos sofisticados hasta errores humanos que permiten el acceso no autorizado. Entre las más críticas se encuentran el ransomware, los ataques a la cadena de suministro, las vulnerabilidades de sistemas OT, la dependencia de tecnología obsoleta y los ataques de ingeniería social, como el phishing y el robo de credenciales. Estas amenazas están evolucionando rápidamente, y su complejidad aumenta con cada nueva capa de conectividad e inteligencia artificial que se integra en la planta industrial.

## 2.1. Tipologías de atacantes y motivaciones

La ciberseguridad en entornos de fabricación no se enfrenta a amenazas genéricas, sino a actores con perfiles, capacidades y motivaciones muy diferenciadas. Comprender quién está detrás de un ataque y qué objetivos persigue es fundamental para priorizar medidas de protección y anticiparse a posibles incidentes. Los atacantes en la industria manufacturera se pueden clasificar en cuatro grandes grupos:

1. **Ciberdelincuentes organizados**: motivados principalmente por el lucro económico, buscan interrumpir la producción para exigir rescates mediante ransomware, realizar espionaje industrial o vender información confidencial. Estos grupos actúan con sofisticación comparable a empresas legítimas, planificando ataques “estacionales” que coinciden con momentos de máxima actividad industrial para maximizar su impacto financiero.
2. **Actores internos o “insiders”**: empleados, contratistas o colaboradores con acceso a sistemas críticos pueden provocar incidentes, de forma intencional o por error. La falta de formación específica, la rotación de personal y el acceso sin restricciones a redes OT incrementan significativamente este riesgo, mostrando

que la seguridad no depende únicamente de la tecnología, sino también de la gestión del factor humano.

3. **Hacktivistas y grupos ideológicos**: impulsados por causas políticas, sociales o medioambientales, buscan visibilidad y notoriedad. Sus ataques suelen ser menos sofisticados que los de ciberdelincuentes organizados, pero pueden generar interrupciones relevantes, especialmente si apuntan a sistemas de producción críticos o a infraestructuras estratégicas dentro de la planta.

4. **Estados-nación**: actores estatales con capacidades avanzadas y objetivos estratégicos que pueden abarcar desde el espionaje industrial hasta el sabotaje de instalaciones críticas. Ejemplos históricos incluyen el malware Stuxnet, que manipuló centrifugadoras nucleares, y los ataques a centros de control eléctrico en Ucrania en 2015. En la industria, estos ataques se dirigen a plantas de energía, fabricantes de componentes estratégicos y líneas de ensamblaje de alta tecnología, donde un fallo intencionado puede tener consecuencias geopolíticas y económicas de gran alcance.

En conjunto, estas tipologías de atacantes muestran que las amenazas no son solo técnicas, sino también estratégicas, humanas y organizativas. Cada grupo exige un enfoque distinto de mitigación y defensa: mientras los ciberdelincuentes demandan soluciones tecnológicas y resiliencia operativa, los insiders requieren controles de acceso, concienciación y protocolos internos. La identificación de estas motivaciones permite a las empresas anticiparse a los posibles vectores de ataque, alineando estrategias de ciberseguridad con la naturaleza real y actual de las amenazas en la industria manufacturera.

## 2.2. Vulnerabilidades y tecnología obsoleta

Muchas plantas dependen de equipos y sistemas antiguos que no fueron diseñados pensando en la ciberseguridad. La falta de actualizaciones, la dependencia de configuraciones por defecto y la incompatibilidad con protocolos modernos de seguridad aumentan significativamente la superficie de ataque.

Dispositivos IoT e IIoT conectados a la red industrial, como sensores, actuadores o controladores, suelen presentar puertos abiertos, servicios innecesarios habilitados y contraseñas predeterminadas. Estos factores facilitan que un atacante obtenga acceso no autorizado. La obsolescencia tecnológica y la falta de mantenimiento adecuado generan un círculo vicioso: los dispositivos antiguos permanecen vulnerables, los parches tardan en aplicarse y la infraestructura global se expone a ataques que podrían haberse prevenido.

## 2.3. Ransomware: paralizando la producción

El ransomware se ha convertido en la amenaza más devastadora para las plantas de fabricación. A diferencia de los ataques informáticos convencionales, en los que la pérdida de datos afecta principalmente al entorno administrativo, el ransomware industrial puede paralizar líneas de producción enteras, comprometer la seguridad física de los trabajadores o interrumpir el suministro de bienes esenciales. Este tipo de ataque cifra los archivos de los sistemas afectados y exige un rescate —en ocasiones de millones de euros— para restablecer el acceso.

En los últimos años se ha observado la aparición de variantes específicas dirigidas a entornos OT, que aprovechan la conexión entre las redes de control industrial y las redes corporativas. Algunos grupos criminales, como LockBit o BlackCat, han desarrollado versiones del malware adaptadas a los sistemas SCADA y PLC empleados en fábricas y plantas químicas. Estas versiones pueden bloquear la comunicación entre los controladores y los equipos de producción, generando paradas que, en determinados procesos continuos, resultan extremadamente costosas y peligrosas.

Un ejemplo paradigmático fue el **ataque a Norsk Hydro en 2019**, cuando el ransomware LockerGoga obligó a la multinacional noruega del aluminio a detener temporalmente la producción en varias de sus plantas. El impacto económico superó los 70 millones de euros, pero el efecto más preocupante fue la alteración del proceso industrial: hornos apagados abruptamente, flujos de materiales interrumpidos y necesidad de volver a calibrar maquinaria crítica. Casos similares han afectado a fabricantes automovilísticos, farmacéuticos y de componentes electrónicos, evidenciando cómo los ciberataques pueden causar daños físicos en activos de alto valor.

La tendencia actual apunta a una **especialización "sectorial" del ransomware**, con ataques cuidadosamente planificados en función del calendario productivo, una práctica que algunos expertos denominan *ransomware estacional*. Los atacantes eligen los momentos de máxima actividad —por ejemplo, campañas de producción o cierres de trimestre—, cuando el coste de una interrupción es inasumible, y así incrementan la presión para pagar el rescate.

## 2.4. Ataques a la cadena de suministro

La digitalización ha conectado estrechamente a fabricantes, proveedores y clientes, creando cadenas de suministro altamente eficientes pero también extremadamente vulnerables. Los ataques a la cadena de suministro aprovechan esta interdependencia. Un atacante que compromete un proveedor de software, firmware o componentes críticos puede insertar vulnerabilidades en productos que serán distribuidos a múltiples clientes, propagando el riesgo de forma masiva.

El sector manufacturero depende de terceros como proveedores de software, firmware, componentes críticos y servicios en la nube, lo que lo expone a ataques indirectos. Un adversario que comprometa a un proveedor puede distribuir actualizaciones maliciosas que infecten múltiples clientes, aumentando la probabilidad de incidentes generalizados. La Directiva NIS2 y el marco de ciberresiliencia de la UE refuerzan las obligaciones de gestión de riesgos de terceros y de notificación de vulnerabilidades. Un ejemplo paradigmático de este tipo de ataque fue el incidente a la empresa de software SolarWinds, cuyos efectos se extendieron a centenares de organizaciones.

En entornos industriales, estas vulnerabilidades pueden alterar parámetros de maquinaria conectada, introducir fallos en sistemas OT o manipular algoritmos de control de producción. Las consecuencias se traducen en interrupciones simultáneas de operaciones, pérdida de confianza en proveedores críticos y riesgos para la continuidad y seguridad de la fabricación. La dependencia creciente de servicios en la nube y software de terceros intensifica este riesgo. Las actualizaciones automáticas, si no están correctamente aseguradas, pueden convertirse en vectores de ataque, provocando sabotajes inadvertidos o comprometiendo la trazabilidad y la calidad de los productos.

El caso de **SolarWinds** es paradigmático, aunque se produjo en entornos IT: una actualización maliciosa comprometió cientos de organizaciones, evidenciando cómo un punto débil en la cadena puede derivar en un riesgo global. En el sector manufacturero, estas vulnerabilidades pueden alterar parámetros de maquinaria conectada, introducir fallos en sistemas OT o manipular algoritmos de control de producción. La consecuencia es una interrupción simultánea de operaciones, pérdida de confianza y riesgo para la trazabilidad de los productos.

## 2.5. Ataques a entornos OT

Los sistemas de tecnología operacional (OT) son el núcleo de las plantas de fabricación: controlan procesos físicos, supervisan maquinaria crítica y aseguran la continuidad de la producción. Tradicionalmente, estos sistemas se diseñaban con un enfoque centrado en la disponibilidad y la fiabilidad, y operaban en entornos aislados, lo que los protegía de intrusiones externas. Sin embargo, la convergencia con redes corporativas (IT), la incorporación de tecnologías conectadas como IoT industrial, plataformas en la nube y el telemantenimiento han eliminado gran parte de este aislamiento. Hoy, cualquier acceso remoto representa un vector crítico que puede ser explotado por atacantes sofisticados.

El telemantenimiento y las plataformas de gestión remota, esenciales para supervisar líneas de producción, procesos de ensamblaje o flotas de robots colaborativos, pueden convertirse en puertas de entrada si no se implementan medidas de seguridad adecuadas. Los incidentes más comunes se originan en credenciales débiles,

contraseñas por defecto o la ausencia de autenticación multifactor. Los accesos remotos son uno de los vectores más peligrosos para redes de control industrial, ya que permiten a los atacantes moverse lateralmente desde la red corporativa (IT) hasta la red de operaciones (OT), comprometiendo sistemas críticos.

Además de accesos remotos inseguros, los sistemas OT son vulnerables por su dependencia de controladores antiguos, PLCs con firmware desactualizado y plataformas que operan sin capacidad de actualización segura. Estas plataformas suelen emplear configuraciones por defecto, carecen de autenticación robusta y no cifran la comunicación, facilitando la intrusión de actores maliciosos. Los ataques a OT pueden ser extremadamente costosos y peligrosos, ya que comprometen tanto la disponibilidad de la producción como la integridad de los procesos físicos e incluso pueden generar consecuencias de seguridad para los trabajadores.

En conjunto, la convergencia IT/OT y la expansión de la conectividad han aumentado la superficie de ataque en las fábricas modernas, exponiendo sistemas antes aislados a amenazas complejas y sofisticadas. Por ello, la protección de los entornos OT requiere no solo medidas tecnológicas como segmentación de redes, gestión de accesos y auditorías continuas, sino también un enfoque organizativo que integre cultura de ciberseguridad, formación de operarios y protocolos de seguridad desde el diseño. Solo así se puede garantizar que la digitalización y la automatización se traduzcan en beneficios sostenibles y seguros para la industria.

El histórico ataque de Stuxnet en 2010 evidenció el potencial destructivo de los ciberataques dirigidos a infraestructuras industriales. A través de un malware altamente sofisticado, se demostraba cómo la manipulación imperceptible de parámetros de control podía provocar fallos físicos en maquinaria crítica. Posteriormente, incidentes como el de una acería alemana en 2014, donde un ataque informático impidió el apagado seguro de un horno de fundición, demostraron que estas tácticas también podían afectar a la industria civil, poniendo en riesgo tanto la producción como la seguridad de los trabajadores.

## 2.6. Phishing, robo de credenciales e ingeniería social

Aunque los ataques técnicos, como ransomware o intrusiones en sistemas OT, suelen captar más atención, la ingeniería social sigue siendo un vector crítico y muy eficaz en entornos de fabricación. Los ciberdelincuentes aprovechan las vulnerabilidades humanas para obtener acceso a sistemas críticos sin necesidad de vulnerar directamente el hardware o el software. Entre las técnicas más comunes se encuentran el phishing, el fraude del CEO, la manipulación de correos electrónicos y otros engaños diseñados para robar credenciales o inducir a los empleados a ejecutar acciones inseguras.

Los errores humanos son una de las principales causas de incidentes en entornos OT. Prácticas como el uso de contraseñas por defecto, la conexión de dispositivos externos no verificados o la utilización de redes Wi-Fi inseguras amplifican significativamente los riesgos. La rotación frecuente de personal, la falta de formación específica en ciberseguridad y la ausencia de políticas claras de acceso a sistemas críticos crean un entorno propicio para que los atacantes exploten estas debilidades.

En las fábricas, el impacto de estos incidentes puede ser considerable: desde la modificación inadvertida de parámetros de producción, la introducción de malware en sistemas industriales, hasta la interrupción de procesos críticos de manera directa o indirecta. Los atacantes combinan estas técnicas con otros vectores técnicos, como accesos remotos inseguros o vulnerabilidades en la red OT/IT, aumentando la probabilidad de éxito y la gravedad del ataque.

## 2.7. Inteligencia Artificial como vector de ataque emergente

La incorporación de la inteligencia artificial (IA) en entornos industriales representa un cambio profundo en la manera en que se diseñan, operan y supervisan los procesos de fabricación. La IA permite optimizar la producción, detectar anomalías en tiempo real, anticipar fallos y mejorar la eficiencia energética. Sin embargo, esta misma capacidad de automatización e inteligencia ofrece nuevas oportunidades a los atacantes, quienes pueden emplearla para generar intrusiones más sofisticadas, automatizar ataques y manipular sistemas de decisión de manera más efectiva que nunca.

Uno de los riesgos emergentes más críticos es la **manipulación de los datos que alimentan los modelos de IA**. Sensores, registros de máquinas y métricas de producción constituyen la información que determina el comportamiento de los sistemas inteligentes. Si un atacante corrompe o altera estos datos, puede inducir decisiones erróneas del sistema, degradando la calidad del producto, provocando fallos en la línea de producción o incluso comprometiendo la seguridad de los trabajadores. Esta vulnerabilidad ilustra cómo la integridad de los datos se convierte en un pilar fundamental para garantizar la seguridad industrial en la era de la IA.

Los ataques de IA ofensiva ya se están materializando en diversos escenarios. Modelos generativos permiten crear campañas de phishing altamente personalizadas, redactar mensajes que imitan estilos humanos o incluso generar código malicioso sin intervención manual. En el contexto industrial, esta tecnología puede ser utilizada para manipular sistemas de control que emplean aprendizaje automático, por ejemplo alterando los parámetros que regulan la temperatura de hornos, la dosificación de materiales o la calibración de robots colaborativos. Estos fallos pueden ser sutiles, acumulativos y difíciles de detectar hasta que su impacto sea crítico, afectando tanto la producción como la seguridad operativa.

Los sistemas de visión artificial utilizados en inspección de calidad y guiado de robots presentan riesgos adicionales. Mediante técnicas de *adversarial machine learning*, un atacante puede introducir perturbaciones mínimas en las imágenes capturadas por cámaras o sensores, provocando errores en la clasificación de piezas o en el posicionamiento de los robots. Estos ataques, aunque todavía minoritarios, ilustran cómo incluso pequeñas modificaciones pueden comprometer procesos altamente automatizados, especialmente en fábricas con un alto grado de autonomía.

A medio plazo, la convergencia de IA generativa, análisis predictivo y manipulación de datos abrirá la puerta a una nueva generación de ciberataques autónomos. Estos ataques serán capaces de adaptarse dinámicamente a las defensas implementadas en la fábrica, modificando su comportamiento en tiempo real para maximizar el impacto y dificultar su detección. Frente a este escenario, la industria deberá apostar por estrategias de defensa que incluyan la supervisión humana, la trazabilidad verificable y la integración de IA defensiva que permita monitorizar y reaccionar ante patrones de ataque avanzados.

En definitiva, la irrupción de la IA en entornos industriales plantea un doble desafío: aprovechar sus ventajas operativas para mejorar la eficiencia y la calidad, a la vez que se protegen los sistemas frente a amenazas inéditas que combinan sofisticación técnica, automatización y adaptación dinámica. La seguridad ya no puede considerarse un añadido: debe integrarse desde el diseño de los sistemas y mantenerse a lo largo de todo su ciclo de vida, garantizando que los beneficios de la transformación digital se obtengan de manera segura y sostenible.

## 2.8. Amenazas futuras: computación cuántica, bots y ataques híbridos

Mirando hacia el futuro, la evolución tecnológica plantea desafíos aún mayores. La **computación cuántica**, cuando alcance su madurez, podría romper en minutos los algoritmos de cifrado que hoy protegen la mayoría de las comunicaciones industriales. Aunque las primeras soluciones de criptografía poscuántica ya están en desarrollo, su implementación en entornos con recursos limitados —como sensores o PLCs— sigue siendo compleja.

Por otra parte, las **botnets industriales** se están volviendo más sofisticadas. El malware Mirai demostró en 2016 cómo miles de dispositivos IoT inseguros podían unirse para lanzar ataques DDoS masivos. En el futuro, variantes de este tipo podrían dirigirse a redes de control industrial, saturando las comunicaciones entre plantas o bloqueando servicios de mantenimiento remoto.

También es probable que aumenten los **ataques híbridos** combinados, donde un ciberataque se acompaña de sabotaje físico, manipulación mediática o desinformación. Los incidentes registrados en Ucrania (2015) y posteriormente en Europa del Este han

mostrado cómo las campañas patrocinadas por actores estatales pueden afectar tanto a infraestructuras energéticas como a plantas de fabricación, con fines estratégicos o geopolíticos.

# 3. Marco normativo sobre ciberseguridad industrial

Frente a un panorama de amenazas cada vez más complejo y dinámico, la industria europea se enfrenta al desafío de proteger no solo sus procesos y productos, sino también la información y la seguridad de sus trabajadores. Es en este contexto que surge la necesidad de un **marco normativo sólido y coherente**, capaz de establecer obligaciones claras, fomentar buenas prácticas y guiar a las empresas en la implementación de medidas de ciberseguridad industrial. La normativa no solo persigue la prevención de incidentes, sino también la resiliencia frente a ataques, la transparencia en la seguridad de productos y servicios y la protección de la cadena de suministro frente a vulnerabilidades externas.

Este marco normativo se articula en dos niveles principales: **la legislación de alcance general**, que establece obligaciones para toda la industria y sectores críticos, y **las normas y certificaciones sectoriales**, que especifican requisitos técnicos y organizativos adaptados a las características de cada tipo de producto o proceso industrial. Mientras que las primeras definen el "qué" debe lograrse en términos de seguridad, las segundas detallan el "cómo" implementarlo de manera práctica, desde el diseño y desarrollo del producto hasta su operación y eventual retirada.

Con esta perspectiva, la normativa se convierte en una herramienta esencial para mitigar los riesgos descritos en el apartado anterior, asegurando que los fabricantes y operadores de plantas de producción puedan enfrentar los desafíos de ciberseguridad con un enfoque integral y sistemático.

## 3.1. Legislación de alcance general

### 3.1.1. Directiva NIS2

La **Directiva 2022/2555/UE (NIS2)** representa la evolución de la Directiva NIS1 y establece un marco obligatorio para garantizar la ciberseguridad en sectores estratégicos de la economía europea. Su enfoque es amplio y estratégico, abarcando entidades esenciales y importantes según su criticidad, tamaño y tipo de servicio. Entre sus principales aportaciones destacan:

- **Refuerzo de requisitos de seguridad**: obliga a las empresas a implementar políticas de gestión de riesgos, controles de acceso, monitorización de incidentes y medidas de resiliencia operativa.
- **Notificación obligatoria de incidentes**: establece plazos y procedimientos para informar sobre ciberincidentes que puedan afectar servicios esenciales, garantizando una respuesta coordinada.

- **Seguridad en la cadena de suministro**: requiere que las empresas evalúen y gestionen riesgos de proveedores, incluyendo actualizaciones de software y firmware, y relaciones con integradores externos.
- **Intercambio de información y divulgación de vulnerabilidades**: fomenta la cooperación entre organizaciones, autoridades nacionales y la red europea de soporte de crisis (EU-CYCLONe), mejorando la respuesta ante ataques sofisticados.

La NIS2 proporciona un marco normativo integral que conecta directamente con los riesgos descritos en el apartado 2, como ransomware dirigido a entornos OT, ataques a la cadena de suministro y vulnerabilidades en sistemas obsoletos. Su enfoque obligatorio obliga a las empresas a adoptar un nivel mínimo de seguridad, independientemente de su tamaño, contribuyendo a una ciberresiliencia industrial más homogénea en Europa.

### 3.1.2. Reglamento de ciberresiliencia (CRA)

El Reglamento europeo de Ciberresiliencia, conocido como **Cyber Resilience Act (CRA)**, se centra en los productos con elementos digitales, aquellos que permiten la conectividad o la digitalización de funcionalidades industriales. Su objetivo es garantizar que tanto hardware como software sean seguros desde su concepción hasta su retirada del mercado. La CRA establece cuatro pilares fundamentales:

1. **Seguridad desde el diseño**: los fabricantes deben incorporar medidas de protección desde las fases iniciales de desarrollo, incluyendo análisis de riesgos, identificación de vulnerabilidades y controles de seguridad integrados.
2. **Marco coherente de ciberseguridad**: la normativa proporciona un conjunto de directrices comunes que facilitan la implementación consistente de medidas de seguridad en todos los productos digitales.
3. **Transparencia en propiedades de seguridad**: los productos deben ofrecer información clara sobre sus mecanismos de protección, permitiendo a empresas y consumidores evaluar su seguridad antes de su uso.
4. **Uso seguro de los productos**: los productos digitales deben diseñarse para que los usuarios puedan operarlos sin comprometer la seguridad, incluso en entornos industriales complejos.

La CRA es especialmente relevante para mitigar los riesgos de ataques a dispositivos IoT/IIoT, accesos remotos inseguros y actualizaciones de software comprometidas, todos ellos descritos en el apartado de amenazas. Al exigir medidas de seguridad a lo largo de todo el ciclo de vida, se busca reducir la probabilidad de incidentes críticos que puedan afectar la continuidad de la producción o la integridad física de los trabajadores.

### 3.1.3. Reglamento (UE) 2023/1230 de máquinas

El **Reglamento de Máquinas (UE) 2023/1230**, que entró en vigor el 19 de julio de 2023, sustituye a la Directiva de Máquinas 2006/42/CE tras 17 años de vigencia, con un período de transición de 42 meses para su plena implementación. Aunque no introduce un cambio de paradigma radical, el reglamento incorpora **consideraciones clave de ciberseguridad**, reflejando los riesgos derivados de la creciente digitalización y del uso de tecnologías avanzadas, como la inteligencia artificial, en productos mecánicos y sistemas de control industrial.

Una de las novedades más relevantes es que los fabricantes de máquinas **deben garantizar la protección de los sistemas de control**, asegurando que no puedan ser manipulados por terceros. Esto implica que la ciberseguridad se integra dentro de la evaluación global de riesgos de la máquina, considerando su funcionamiento dentro de sistemas más amplios, y no como una medida aislada. Aunque el reglamento no especifica procedimientos concretos de implementación, se desprende la obligación de:

- Realizar **evaluaciones de riesgos anticipadas**, identificando amenazas y vulnerabilidades potenciales.
- Implementar medidas de ciberseguridad adecuadas al contexto operativo de la máquina.
- Mantener una **documentación exhaustiva** que respalde la conformidad con los requisitos de seguridad y ciberseguridad.

### 3.1.4. Directiva 2014/53/UE de equipos radioeléctricos

La **Directiva RED 2014/53/UE** regula la comercialización de equipos radioelécricos en Europa, asegurando que dispositivos conectados, incluidos sistemas IoT y de comunicación industrial, cumplan criterios de seguridad, compatibilidad y eficiencia espectral.

Con la **reforma de 2024**, la Directiva refuerza significativamente las responsabilidades de los fabricantes, especialmente en ciberseguridad y protección de datos. Los principales cambios son:

- **Ciberseguridad reforzada:** los dispositivos deben protegerse frente a accesos no autorizados y ataques, integrando medidas de seguridad desde el diseño.
- **Evaluaciones de conformidad más estrictas:** pruebas adicionales para garantizar seguridad digital, interoperabilidad y robustez frente a ataques.
- **Protección de datos de usuarios:** requisitos claros sobre recopilación, procesamiento y seguridad de los datos, alineados con GDPR.

En conjunto, la actualización convierte la seguridad digital en un requisito obligatorio para comercializar equipos de radio en Europa, armonizando la RED con otros marcos regulatorios como el **Reglamento de Máquinas** y la **Ley de Ciberresiliencia Europea**, elevando la ciberseguridad de productos industriales y de consumo.

## 3.2. Certificaciones y normas sectoriales

Mientras que CRA y NIS2 establecen **qué** se debe lograr en términos de seguridad, las normas y certificaciones sectoriales definen **cómo implementarlo** de manera práctica y técnica, adaptándose a las características de cada producto y proceso industrial.

### 3.2.1. Norma IEC 62443

La norma **IEC 62443** es la referencia global para la seguridad de los sistemas de automatización y control industrial. Proporciona un enfoque por niveles y roles, que cubre desde la gestión de riesgos hasta la protección de dispositivos y redes OT. Su aplicación permite estructurar la seguridad en capas, mitigando riesgos como ataques a PLCs, SCADA o redes industriales. La norma incluye requisitos para:

- Evaluación y gestión de riesgos de sistemas OT.
- Diseño seguro de dispositivos industriales.
- Segmentación de redes y controles de acceso.
- Monitorización continua y gestión de incidentes.

### 3.2.2. Norma ISO/IEC 27001

Aunque no es específica del sector industrial, la Norma **ISO/IEC 27001** establece un marco robusto para la gestión de la seguridad de la información (SGSI). Su objetivo principal es ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de sus datos mediante la gestión de riesgos de seguridad de la información a través de un enfoque de mejora continua.

### 3.2.3. Norma ISO 21434 y Reglamento UNECE R155/R156

En sectores como el de la movilidad, la Norma **ISO 21434** regula la gestión de riesgos de ciberseguridad para sistemas eléctricos y electrónicos en vehículos, incluyendo diseño, desarrollo, producción y mantenimiento. Complementariamente, el **Reglamento UNECE R155/R156** establece los requisitos de homologación de vehículos respecto a ciberseguridad y actualizaciones de software, obligando a los fabricantes a demostrar la gestión segura del ciclo de vida del producto.

### 3.2.4. Proyecto de norma pEN 50742

La **pEN 50742** es una norma europea emergente que aborda la ciberseguridad en entornos industriales complejos, poniendo énfasis en la protección de sistemas críticos y el aseguramiento del ciclo de vida de dispositivos conectados. Complementa a la Norma IEC 62443 en aspectos de gestión de vulnerabilidades y actualización segura de software, siendo especialmente relevante para plantas con maquinaria conectada y sistemas OT interdependientes.

# 4. Retos específicos del sector de maquinaria

El sector manufacturero atraviesa un momento de transformación sin precedentes, en el que la adopción de tecnologías digitales no solo redefine los procesos productivos, sino que también modifica radicalmente el panorama de riesgos. La integración de sistemas de control industrial, sensores conectados, inteligencia artificial y plataformas en la nube ha mejorado la eficiencia y la trazabilidad, pero ha generado un ecosistema donde las operaciones críticas ya no están aisladas y cada dispositivo conectado puede ser un vector de ataque.

Los retos del sector surgen, por tanto, tanto de la **complejidad tecnológica** como de la necesidad de **garantizar la continuidad operativa y la seguridad física** frente a un escenario de amenazas cada vez más sofisticado. La convergencia IT/OT, la dependencia de sistemas heredados, la expansión de la conectividad y las obligaciones normativas crean un entorno donde la resiliencia industrial se convierte en un requisito estratégico para la competitividad.

En este contexto, la industria de fabricación debe enfrentarse a desafíos como la vulnerabilidad de los sistemas legados, la integración de tecnologías emergentes, la gestión de la identidad digital, la trazabilidad de equipos y el cumplimiento normativo, factores que condicionan directamente la seguridad y la sostenibilidad de las operaciones industriales.

## 4.1. Convergencia IT/OT y expansión de la conectividad

Hasta hace pocos años, los sistemas de producción en las plantas industriales funcionaban en gran medida aislados. Las órdenes de trabajo llegaban en papel o mediante procesos cerrados, los equipos de control industrial operaban desconectados de redes corporativas y la información fluía de manera secuencial y controlada. Esta barrera natural, aunque limitada, proporcionaba un nivel de seguridad pasiva: sin conexión a Internet ni integración con sistemas externos, las posibilidades de intrusión remota eran mínimas.

La transformación digital ha alterado radicalmente este escenario. Hoy, los sistemas IT y OT están profundamente interconectados: los ERPs transmiten órdenes en tiempo real a las líneas de producción, mientras que los controladores recopilan información instantánea sobre parámetros de fabricación, calidad y mantenimiento. Esta convergencia permite optimizar procesos, mejorar la eficiencia y garantizar la trazabilidad de cada producto. Sin embargo, la misma conectividad que ofrece ventajas operativas también diluye los perímetros tradicionales de seguridad y expone activos críticos a ciberamenazas.

El mantenimiento remoto, la adopción de tecnologías como IoT industrial, inteligencia artificial y 5G, así como la integración de plataformas en la nube, han convertido la planta en un sistema distribuido, en el que cada nodo conectado representa un posible vector de ataque. Delincuentes organizados, hacktivistas o actores estatales pueden ahora acceder de manera remota a sistemas previamente inaccesibles, interfiriendo en los procesos industriales sin necesidad de presencia física. Como ha señalado la experiencia en múltiples industrias, robar o sabotear a distancia es más sencillo y menos riesgoso para un atacante que hacerlo de forma presencial, lo que aumenta exponencialmente la criticidad de las medidas de ciberseguridad.

Esta convergencia también genera retos de coordinación interna. La velocidad de transmisión de información y la interdependencia entre sistemas IT/OT obligan a revisar continuamente los procesos de control, actualización y supervisión de las máquinas y los sistemas de automatización. Cada modificación en un ERP, cada actualización remota de firmware o software de control, y cada sensor conectado a la red industrial introduce potenciales vulnerabilidades que deben ser identificadas y gestionadas de manera proactiva.

## 4.2. Dependencia de sistemas heredados y obsolescencia tecnológica

Muchas fábricas dependen de equipos y software “legacy” que no fueron diseñados con la ciberseguridad en mente. Estos sistemas obsoletos siguen siendo funcionales para tareas críticas, pero presentan importantes desafíos: tecnología anticuada, falta de soporte, vulnerabilidades de seguridad y dificultades de integración con sistemas modernos. Su sustitución suele ser compleja, costosa o arriesgada, lo que hace que sigan en uso a pesar de los riesgos asociados, especialmente en un entorno industrial cada vez más interconectado y digitalizado.

En las plantas de fabricación, los controladores antiguos, los PLCs con firmware desactualizado y los sistemas OT sin capacidad de actualización segura representan un riesgo crítico. Estas plataformas suelen operar con configuraciones por defecto, carecen de cifrado y no implementan autenticación robusta, lo que facilita que un atacante obtenga acceso no autorizado y comprometa procesos de producción y seguridad operativa.

La coexistencia de sistemas modernos y legacy crea un círculo vicioso: los dispositivos antiguos permanecen vulnerables mientras se introducen nuevas tecnologías conectadas, aumentando la superficie de ataque y dificultando la aplicación de políticas de seguridad homogéneas. En muchos casos, la inversión en actualización de equipos se percibe como un coste, pero su ausencia puede traducirse en incidentes mucho más graves y costosos.

## 4.3. Integración de IoT industrial, IA y tecnologías en la nube

El despliegue de IoT industrial y la incorporación de inteligencia artificial en plantas de fabricación permiten optimizar procesos, realizar mantenimiento predictivo y mejorar la calidad del producto. Sin embargo, estas tecnologías amplían exponencialmente los vectores de ataque. Cada sensor, actuador, robot colaborativo o sistema de visión artificial conectado representa un potencial punto de intrusión.

La IA, aunque útil para detectar anomalías y optimizar decisiones, también puede ser manipulada mediante ataques de datos adversariales, corrupción de modelos predictivos o sabotaje de algoritmos de control. La dependencia de plataformas en la nube para almacenamiento y análisis de datos críticos introduce riesgos adicionales relacionados con accesos remotos inseguros, robo de credenciales y compromisos en la cadena de suministro digital.

## 4.4. Cumplimiento normativo y obligaciones regulatorias

La normativa europea impone nuevas obligaciones a las empresas manufactureras, tanto para productos con componentes digitales como para procesos de fabricación críticos. La Directiva 2006/42/CE y el reciente Reglamento de Máquinas (UE) 2023/1230 incorporan la ciberseguridad como parte integral de la seguridad de las máquinas. Los fabricantes deben garantizar que los sistemas de control de sus equipos no puedan ser manipulados y realizar evaluaciones de riesgos anticipando posibles ataques.

Otras regulaciones, como la Directiva NIS2 y el Reglamento de Ciberresiliencia (CRA), amplían la obligación de implementar medidas de seguridad, gestionar incidentes y supervisar la cadena de suministro. El desafío no es solo técnico, sino también organizativo: se requiere documentación completa, seguimiento de vulnerabilidades y formación del personal para asegurar que las políticas de ciberseguridad se cumplan de manera efectiva.

## 4.5. Identidad digital, trazabilidad y confianza tecnológica

La trazabilidad y la identidad digital de equipos y componentes son cada vez más críticas en la fabricación avanzada. Garantizar que cada máquina, sensor o software está autenticado y opera con integridad es esencial para prevenir manipulación de datos, sabotaje industrial o fraude en la cadena de suministro. Tecnologías como la blockchain ligera, los entornos de ejecución confiables (TEE) y la gestión de identidad de dispositivos ofrecen soluciones, pero requieren inversión y adaptación de procesos para ser eficaces.

## 4.6. Evolución de las amenazas y preparación frente al futuro

El panorama de riesgos evoluciona constantemente. Los ataques ya no son genéricos; el ransomware se ha especializado en entornos industriales, existen actores estatales con capacidad de sabotaje y la IA puede ser utilizada ofensivamente. A futuro, la computación cuántica, las botnets industriales y los ataques híbridos —combinando sabotaje digital, físico y desinformación— representan un desafío adicional para la resiliencia industrial.

En este contexto, la industria de fabricación debe anticiparse a los cambios y desarrollar estrategias de seguridad integrales, que incluyan no solo tecnología, sino también procesos, formación y cultura organizativa. La capacidad de adaptarse a nuevas amenazas y cumplir con un marco normativo cada vez más exigente será determinante para garantizar la continuidad operativa, la seguridad de los trabajadores y la confianza de clientes y socios.

# 5. Ciberdefensa y protección de plantas de fabricación

La seguridad de las plantas de fabricación ha dejado de ser un tema secundario para convertirse en un elemento estratégico de la operación industrial. La convergencia de tecnologías IT y OT, la adopción masiva de IoT industrial, la integración de inteligencia artificial, la conectividad en la nube y la dependencia de proveedores externos han transformado radicalmente el panorama de riesgos. Lo que antes estaba protegido por un aislamiento físico –el llamado "air gap"– ahora está expuesto a ciberamenazas sofisticadas y persistentes, capaces de comprometer tanto la continuidad operativa como la integridad de los procesos críticos.

Proteger estas instalaciones requiere un enfoque integral, estructurado en capas de defensa que se complementan entre sí, combinando tecnología, procesos y cultura organizativa. Cada capa fortalece a la siguiente, creando un ecosistema resiliente frente a ataques de diversa naturaleza.

## 5.1. Visibilidad integral y conocimiento del entorno

El primer paso para proteger cualquier planta es **saber qué activos existen y cómo operan**. Esto implica un inventario dinámico de todos los dispositivos y sistemas conectados: controladores lógicos programables (PLC), variadores, sensores, sistemas SCADA, estaciones de supervisión, maquinaria con buses industriales y, en general, cualquier equipo que participe en el control de procesos. No se trata únicamente de conocer direcciones IP, sino de comprender el tipo de activo, sus vulnerabilidades conocidas, sus patrones normales de comunicación y su contexto operativo dentro de la planta.

Las soluciones modernas incorporan motores de descubrimiento automatizados basados en inteligencia artificial, capaces de identificar dispositivos de forma pasiva, sin interrumpir la operación. La **identificación contextual** permite diferenciar entre equipos IT, OT o IoT, así como reconocer dispositivos que funcionan en redes críticas y determinar si presentan riesgos específicos. La **visualización jerárquica** de los activos, alineada con modelos como el Purdue Model, facilita a los ingenieros de planta entender la topología, priorizar acciones y tomar decisiones informadas de protección.

## 5.2. Segmentación y aislamiento de redes

Asas La protección de los sistemas industriales comienza por limitar el alcance de cualquier posible ataque. Una red plana, donde todos los dispositivos están conectados sin distinciones, es un terreno fértil para que una intrusión inicial se propague rápidamente. Por ello, la **segmentación y aislamiento de redes** constituye la primera línea de defensa estratégica.

En la práctica, esto implica separar la infraestructura corporativa —ofimática, correo electrónico, acceso a Internet— de la red operativa de la planta, donde residen los PLC, SCADA, sensores y maquinaria conectada. Entre ambas redes se sitúa una **zona desmilitarizada industrial (iDMZ)** que actúa como filtro y punto de control, evitando que un ataque en la oficina alcance directamente los sistemas críticos de producción.

Dentro de la propia red operativa, se implementa la **micro-segmentación**, creando subzonas de seguridad alrededor de líneas de producción, celdas de trabajo o procesos críticos. Esto limita la posibilidad de movimientos laterales de un atacante, reduciendo el riesgo de interrupciones generalizadas. Por ejemplo, en una explotación agrícola inteligente, las estaciones de riego, los silos de almacenamiento y los tractores conectados pueden pertenecer a segmentos distintos, con firewalls internos y VLAN que regulen estrictamente la comunicación entre ellos.

La segmentación no solo protege contra ataques externos, sino que también mitiga errores internos y fugas accidentales de información. La implementación adecuada de esta estrategia requiere un inventario preciso de activos, una comprensión de los protocolos industriales específicos (Modbus, OPC UA, ISOBUS) y la aplicación de políticas de control adaptadas a cada zona. Este enfoque estructurado establece la base sobre la que se construyen todas las demás capas de defensa, convirtiéndose en un pilar esencial de la ciberresiliencia industrial.

## 5.3. Gestión de accesos e identidades

Si la segmentación define los límites del territorio, la **gestión de accesos e identidades** decide quién puede moverse dentro de él y con qué privilegios. Cada usuario, técnico externo o dispositivo conectado debe contar con credenciales únicas y roles bien definidos que determinen su nivel de acceso. Esta capa de seguridad es clave, ya que gran parte de los incidentes en entornos OT se originan por accesos indebidos o mal configurados.

Las mejores prácticas incluyen la **autenticación multifactor**, la asignación de privilegios mínimos y la gestión de cuentas privilegiadas mediante soluciones de **Privileged Access Management (PAM)**. Todo acceso debe registrarse y auditarse, permitiendo reconstruir la cadena de eventos ante cualquier anomalía o incidente. En contextos agrícolas distribuidos, donde distintos proveedores intervienen en la misma instalación, esta trazabilidad resulta imprescindible para atribuir responsabilidades y detectar comportamientos fuera de lo normal.

Asimismo, la rotación periódica de contraseñas, la desactivación automática de cuentas inactivas y la revisión de accesos tras cada campaña agrícola forman parte de una política integral de identidad. Combinada con la segmentación de redes, esta gestión asegura

que incluso si un dispositivo o usuario queda comprometido, el alcance del posible daño se mantiene limitado, reforzando la resiliencia de la planta ante amenazas internas y externas.

Una vez identificados los activos, es fundamental **limitar la exposición** mediante segmentación de redes y control de accesos. La macro-segmentación separa estrictamente las redes corporativas (IT) de las redes de planta (OT) a través de zonas desmilitarizadas industriales (iDMZ). Esto evita que un ataque originado en la red administrativa se propague a sistemas de control críticos.

La micro-segmentación añade un segundo nivel de defensa, protegiendo líneas de producción, celdas de trabajo y procesos esenciales frente a movimientos laterales de posibles intrusos. En paralelo, la gestión de identidades y privilegios asegura que cada usuario, técnico o proveedor externo tenga **acceso mínimo necesario**, con autenticación multifactor y trazabilidad completa de cada operación. Políticas de "Zero Trust" sustituyen los modelos permisivos tradicionales, verificando continuamente el contexto de cada conexión, el tipo de dispositivo y la acción solicitada.

## 5.4. Prevención de amenazas y monitorización continua

El control de accesos es necesario, pero insuficiente. La detección temprana de amenazas es **la diferencia entre un incidente menor y una crisis operativa**. Los sistemas de monitorización industrial permiten inspeccionar tráfico, detectar desviaciones de comportamiento y alertar ante anomalías, sin interferir con los procesos productivos.

Se implementan múltiples niveles de prevención: bloqueo de vulnerabilidades en equipos heredados que no pueden actualizarse, uso de firmas de malware específicas para entornos industriales y detección de comportamientos anómalos mediante análisis de inteligencia artificial. Además, el monitoreo de la integridad de procesos permite identificar intentos de manipulación de comandos críticos, como cambios no autorizados en PLCs o variadores, asegurando que las operaciones físicas se mantengan dentro de parámetros seguros.

## 5.5. Inteligencia artificial en análisis forense de ciberataques

Entre las tecnologías emergentes en materia de ciberseguridad, la **inteligencia artificial (IA) aplicada al análisis forense de ciberataques** está ganando relevancia como herramienta de apoyo a los expertos en plantas de fabricación y entornos industriales. Esta aproximación no sustituye al analista, sino que **multiplica su capacidad de detección, análisis y reconstrucción de incidentes**, acelerando procesos que tradicionalmente requerían largas horas de trabajo manual.

Las plataformas en desarrollo combinan técnicas de **machine learning, deep learning y modelos generativos de lenguaje**, capaces de correlacionar grandes volúmenes de datos provenientes de sensores, registros de máquinas, redes OT/ICS e incluso consumo energético. Su objetivo es identificar huellas digitales de ataques sofisticados, generar hipótesis sobre la cadena de eventos y producir borradores de informes forenses que permitan al especialista validar y tomar decisiones rápidas.

Entre las ventajas principales se incluyen:

- **Detección y reconstrucción acelerada:** la IA analiza patrones anómalos en tiempo casi real, facilitando la identificación de la causa raíz de incidentes complejos.
- **Reducción de falsos negativos y aumento de cobertura:** la correlación de múltiples fuentes de datos permite descubrir relaciones sutiles que podrían pasar desapercibidas para un análisis manual.
- **Escalabilidad y eficiencia:** reduce drásticamente el tiempo necesario para evaluar grandes volúmenes de información, optimizando los recursos humanos disponibles.

Estas herramientas, actualmente en fase piloto y desarrollo en centros como el Instituto Tecnológico de Aragón (ITA), representan una **tendencia futura en ciberdefensa industrial**, donde la convergencia de IA y análisis forense permitirá anticipar, mitigar y comprender ataques sin comprometer la operación continua de la planta. Aunque aún no se trata de soluciones comerciales generalizadas, su integración gradual en entornos industriales promete transformar la forma en que se gestionan incidentes de ciberseguridad, reforzando la resiliencia operativa y la capacidad de respuesta ante amenazas sofisticadas.

## 5.6. Copias de seguridad y resiliencia operativa

Ninguna defensa es completamente infalible, por lo que la capacidad de r**ecuperación rápida** frente a incidentes constituye un elemento esencial de la ciberdefensa industrial. Para ello, las organizaciones deben garantizar la realización de copias de seguridad periódicas, almacenadas de forma aislada y sometidas a verificaciones regulares mediante pruebas de restauración. Estas prácticas permiten no solo proteger los datos, sino también asegurar que, ante cualquier eventualidad, los sistemas críticos puedan recuperarse con la mayor rapidez posible.

Los planes de contingencia y de respuesta a incidentes deben contemplar de manera detallada cómo aislar los equipos comprometidos, notificar a las partes responsables y restaurar la operativa de los procesos críticos. La resiliencia operativa no solo minimiza el impacto económico de los tiempos de inactividad, sino que también salvaguarda la

reputación de la organización y refuerza la confianza de clientes, socios y autoridades reguladoras. En industrias donde cada minuto de parada se traduce en pérdidas significativas, contar con procedimientos claros, bien documentados y ensayados se convierte en un factor estratégico diferenciador.

En paralelo, mantener actualizado el software de control y automatización de cada máquina es fundamental para reducir la exposición a vulnerabilidades conocidas. Las actualizaciones regulares, la aplicación de parches de seguridad y la gestión centralizada de versiones contribuyen a prevenir "exploits" y garantizar la integridad de los procesos industriales críticos. Integrar estas prácticas dentro de un enfoque global de resiliencia y continuidad operacional fortalece la defensa de la planta, asegurando que tanto los datos como los sistemas de control estén protegidos frente a amenazas emergentes.

## 5.7. Cumplimiento normativo y gobernanza

La defensa de la planta se refuerza mediante la adopción de estándares y normativas internacionales, que proporcionan un marco común para la gestión de riesgos y la auditoría de seguridad. Normativas europeas como NIS2 y el Reglamento de Ciberresiliencia (CRA), junto con normas internacionales como IEC 62443, NIST SP 800-82 e ISO/IEC 27001, permiten implementar buenas prácticas, evaluar proveedores, auditar la seguridad de sistemas y demostrar cumplimiento ante autoridades, aseguradoras y clientes.

En este contexto, conocer el nivel de seguridad de la organización se convierte en un primer paso esencial, alcanzable mediante auditorías periódicas que identifican vulnerabilidades y generan hojas de ruta para la mejora continua. Estos resultados deben integrarse dentro de un plan de gestión de ciberseguridad y gobernanza, que defina responsabilidades, protocolos y procesos de supervisión, asegurando que la seguridad industrial no dependa únicamente de medidas técnicas aisladas.

La estrategia se completa con la contratación de ciberseguros, instrumentos cada vez más imprescindibles para el sector industrial, que no solo cubren daños directos a los sistemas o pérdidas de información, sino también costes derivados de la interrupción de la producción, responsabilidad ante terceros y recuperación de datos. De manera complementaria, los acuerdos de nivel de servicio (SLA) con proveedores críticos permiten garantizar que el soporte técnico, la actualización de software y la protección de servicios esenciales cumplan estándares mínimos de seguridad y disponibilidad, evitando interrupciones inesperadas en la operación de las plantas. La formalización de estas obligaciones contractuales asegura que los terceros que participan en la cadena industrial asuman un compromiso claro con la ciberseguridad, minimizando riesgos asociados a la externalización de servicios y tecnología.

Con esta combinación de normativa, auditorías, planificación estratégica, seguros y acuerdos contractuales, las empresas manufactureras pueden reforzar significativamente su resiliencia frente a incidentes de ciberseguridad, demostrando de manera tangible su capacidad para proteger procesos críticos, datos sensibles y continuidad operativa, al tiempo que cumplen con las exigencias regulatorias y las expectativas de clientes y aseguradoras.

## 5.8. Cultura y formación

Más allá de la tecnología, la defensa efectiva depende de las **personas que operan y supervisan la planta**. La formación continua, la concienciación sobre phishing, el uso seguro de dispositivos y la simulación de incidentes reducen drásticamente los errores humanos, responsables de gran parte de los incidentes OT. La cultura de ciberresiliencia fomenta la colaboración entre equipos IT y OT, elimina silos organizativos y convierte la seguridad en un habilitador de la innovación, en lugar de un coste.

## 5.9. Ciberseguridad como habilitador estratégico

El paradigma ha cambiado: la ciberseguridad ya no protege únicamente contra el robo de información, sino que garantiza la continuidad operativa, la integridad de los procesos y la seguridad física. Adoptar un modelo **Zero Trust** y aplicar capas de defensa complementarias permite enfrentar amenazas avanzadas, desde ransomware dirigido hasta manipulación de sistemas críticos. Las plantas que implementan esta estrategia no solo se defienden de los ataques actuales, sino que construyen una base sólida para evolucionar de manera segura en un entorno industrial cada vez más conectado, digitalizado y automatizado.

# 6. Propuesta de proyectos de ciberseguridad industrial

Considerando que las empresas industriales se han convertido en objetivos preferentes de los ciberdelincuentes, resulta evidente que la resiliencia y pervivencia de estas organizaciones depende de mantener un nivel de seguridad adecuado, proporcional al riesgo que presentan sus actividades. Esto implica la puesta en marcha de proyectos de ciberseguridad que permitan proteger los sistemas críticos, la información sensible y la continuidad de los procesos industriales.

Los proyectos que se presentan a continuación representan iniciativas esenciales que cualquier empresa industrial debería contemplar en algún momento, ya sea de forma reactiva ante amenazas detectadas, de manera planificada para alcanzar un nivel de riesgo asumible o por requisitos contractuales de clientes y proveedores.

La implementación de estos proyectos de ciberseguridad industrial no debe considerarse de manera aislada, sino como parte de una estrategia integral de protección de los activos críticos de la empresa. Planificar y ejecutar estas iniciativas de forma coordinada permite anticiparse a amenazas, reducir riesgos operativos y garantizar la continuidad de los procesos productivos. Además, contribuye a consolidar la confianza de clientes, proveedores y aseguradoras, demostrando un compromiso claro con la seguridad, la resiliencia y la innovación en el entorno industrial. En última instancia, estas acciones posicionan a la organización no solo como tecnológicamente avanzada, sino también como un actor responsable y preparado frente al panorama de ciberamenazas actual.

## 6.1. Evaluación inicial y planificación

**Desarrollo de un plan integral de ciberseguridad industrial**

Este proyecto identifica y cuantifica los riesgos, estableciendo las actividades necesarias para mitigarlos, transferirlos o eliminarlos. El objetivo es disponer de un marco estratégico para gestionar la ciberseguridad de manera estructurada. Los beneficios abarcan la reducción del riesgo global, la priorización de recursos y la mejora de la capacidad de respuesta frente a incidentes.

**Evaluación de la seguridad de la información y de los datos industriales**

Consiste en determinar el nivel de exposición y resiliencia de la información industrial frente a ataques externos e internos. El objetivo es identificar vulnerabilidades, proteger la información crítica y asegurar su disponibilidad. Los beneficios incluyen la prevención de pérdidas de datos, mejora de la toma de decisiones basada en información fiable y refuerzo de la confianza de clientes y socios.

**Análisis y mejora del software industrial en plantas**

Este proyecto analiza las aplicaciones y sistemas de control industriales para evaluar riesgos frente a accesos no autorizados y vulnerabilidades conocidas. Su objetivo es establecer medidas de seguridad, actualizaciones y parches necesarios para proteger la operación industrial. Los beneficios incluyen la reducción de incidentes de seguridad, la mejora de la integridad de los procesos y la minimización de interrupciones en la producción.

## 6.2. Diseño de arquitectura y controles técnicos

**Diseño e implementación de arquitecturas de red industriales seguras**

El objetivo de este proyecto es establecer una arquitectura de red que garantice la separación efectiva de los entornos IT y OT, definiendo zonas, conductos y controles adecuados para cada segmento. Esto reduce el riesgo de propagación de ataques, protege los sistemas críticos y facilita la gestión y supervisión de la red. Los beneficios incluyen mayor resiliencia operativa, disminución de vulnerabilidades y cumplimiento de buenas prácticas internacionales.

**Seguridad en los accesos remotos a entornos OT**

Este proyecto busca implementar un modelo seguro de accesos remotos que permita la conexión de personal interno y proveedores externos de manera controlada y auditable. Los objetivos son garantizar la visibilidad, la trazabilidad y la autenticidad de las conexiones, evitando accesos no autorizados. Entre los beneficios se encuentra la reducción del riesgo de intrusión, el control sobre operaciones críticas y el cumplimiento de normativas de ciberseguridad.

**Protección avanzada de endpoints y OT**

Este proyecto aborda la implementación de soluciones avanzadas de protección para endpoints y entornos OT, mediante tecnologías EDR, XDR y MDR adaptadas al contexto industrial. Estas herramientas permiten la monitorización en tiempo real de dispositivos críticos y la detección de comportamientos anómalos, contribuyendo a neutralizar amenazas avanzadas, proteger los activos industriales y minimizar los riesgos de interrupción o daño físico.

## 6.3. Gestión continua y resiliencia

**Monitorización de la seguridad industrial**

Se centra en disponer de sistemas que permitan supervisar de manera continua la seguridad de los entornos industriales. El objetivo es mejorar los tiempos de detección y respuesta ante incidentes. Los beneficios incluyen una reducción del impacto de los ataques, mayor capacidad de reacción ante amenazas y mejora continua del sistema de seguridad.

**Gestión de vulnerabilidades y parches**

Este proyecto se centra en la gestión sistemática de vulnerabilidades y la aplicación de parches de seguridad en los sistemas IT y OT, incluyendo el software de operación de maquinaria, controladores y aplicaciones críticas. La adopción de este enfoque reduce la exposición a ataques conocidos, protege la integridad de los procesos industriales y contribuye a mantener la continuidad operativa frente a posibles exploits.Objetivo:

**Respuesta a incidentes y ejercicios de simulación**

Este proyecto aborda la definición de procedimientos claros para la detección, contención, mitigación y recuperación frente a ciberincidentes. Se incorporan además ejercicios de simulación, tanto tipo tabletop como live drills, que permiten al personal experimentar situaciones realistas. La implementación de estas prácticas mejora significativamente la preparación de la organización, reduce los tiempos de respuesta, minimiza los impactos de los incidentes y fortalece la experiencia práctica del equipo ante posibles escenarios de riesgo.

## 6.4. Gobernanza, buenas prácticas y cultura

**Formación y concienciación del personal**

Se centra en dotar a los empleados de conocimientos de ciberseguridad contextualizados a su puesto de trabajo, fomentando una cultura de seguridad. El objetivo es que el personal sea capaz de identificar riesgos y actuar de forma segura. Los beneficios incluyen menor probabilidad de incidentes causados por errores humanos, mayor eficiencia en la respuesta a amenazas y fortalecimiento de la cultura corporativa de seguridad.

**Adopción de estándares y buenas prácticas**

Consiste en integrar normas y estándares internacionales (como IEC 62443, ISO/IEC 27001 o NIST SP 800-82) en los procesos y operaciones de la empresa. El objetivo es establecer una práctica continua y estructurada de ciberseguridad. Los beneficios incluyen mayor coherencia en la gestión de riesgos, facilidad para auditorías y certificaciones, y alineamiento con las expectativas del sector y clientes.

**Gestión de proveedores y seguridad en la cadena de suministro**

Objetivo: Establecer controles de seguridad y revisiones periódicas para proveedores críticos, asegurando que cumplan con estándares de ciberseguridad adecuados. Beneficios: Minimiza riesgos derivados de terceros, evita brechas por proveedores comprometidos y fortalece la resiliencia de la cadena de suministro.

**Protección de información estratégica o sensible**

Este proyecto busca asegurar la confidencialidad de la información crítica frente a accesos no autorizados internos o externos, cumpliendo además con la Ley de Propiedad Industrial. El objetivo es proteger el conocimiento clave de la empresa. Entre los beneficios destacan la preservación de la ventaja competitiva, reducción de riesgos legales y cumplimiento normativo.

# 7. Conclusiones

La transformación digital de la industria manufacturera ha generado oportunidades sin precedentes de eficiencia, trazabilidad y automatización, pero también ha introducido un ecosistema de riesgos inéditos. Las empresas del sector de maquinaria se enfrentan a un entorno altamente interconectado, donde la convergencia de tecnologías IT y OT, la adopción de IoT industrial y la integración de plataformas en la nube redefinen los perímetros tradicionales de seguridad. Garantizar que la digitalización se traduzca en beneficios sostenibles requiere la planificación estratégica y la implementación progresiva de medidas de ciberseguridad, capaces de mitigar riesgos operativos y proteger la continuidad del negocio.

El panorama de amenazas es amplio y en constante evolución. Desde ransomware industrial, ataques a la cadena de suministro y vulnerabilidades de sistemas OT, hasta errores humanos y ataques de ingeniería social, las posibles fuentes de riesgo son múltiples y de distinta naturaleza. Cada tipo de atacante —ciberdelincuentes organizados, insiders, hacktivistas o actores estatales— presenta motivaciones y capacidades diferenciadas, lo que exige enfoques de mitigación específicos. La irrupción de la inteligencia artificial y otras tecnologías emergentes abre nuevas oportunidades para optimizar la producción, pero también introduce vectores de ataque sofisticados, desde la manipulación de datos que alimentan sistemas inteligentes hasta la explotación de modelos de visión artificial, mientras que el horizonte tecnológico, con la computación cuántica y los ataques híbridos, plantea desafíos futuros que requieren vigilancia y preparación constante.

En el contexto regional, el sector industrial aragonés muestra un tejido maduro y diverso en términos de digitalización, pero persisten importantes brechas en ciberseguridad. Si bien algunas empresas cuentan con procedimientos básicos de protección y monitorización, muchas dependen de sistemas heredados o carecen de una estrategia integral. La variabilidad en tamaño, antigüedad de los sistemas y nivel de digitalización condiciona la exposición a amenazas, destacando la necesidad de formación específica, actualización tecnológica y adopción de buenas prácticas. Reconocer esta diversidad es clave para diseñar intervenciones efectivas y escalables, adaptadas a cada perfil de organización.

El cumplimiento normativo se ha convertido en un elemento esencial de la ciberresiliencia industrial. Directivas y regulaciones europeas, junto con normas internacionales como IEC 62443, ISO/IEC 27001 o NIST SP 800-82, establecen obligaciones claras para la protección de entornos industriales, la gestión de incidentes y la supervisión de proveedores. Adoptar estas directrices no solo garantiza conformidad legal, sino que fortalece la capacidad de reacción ante amenazas, protege la información

sensible y refuerza la confianza de clientes, socios y aseguradoras, integrando la ciberseguridad en la estrategia corporativa de manera tangible.

El sector de maquinaria enfrenta retos específicos derivados de la combinación de sistemas obsoletos, integración de tecnologías emergentes y creciente interdependencia con proveedores y plataformas externas. La trazabilidad de equipos, la gestión de identidades digitales y la protección de información estratégica se vuelven críticas para mantener la integridad de los procesos. La expansión de la conectividad multiplica los vectores de ataque, mientras que la resiliencia frente a incidentes requiere un enfoque integral que combine tecnología, procesos y cultura organizativa, anticipando amenazas actuales y emergentes.

La protección de plantas de fabricación requiere una estrategia en capas, que integre visibilidad completa de activos, segmentación de redes, gestión de accesos, monitorización continua, copias de seguridad y formación del personal. La aplicación de inteligencia artificial en análisis forense y detección de anomalías multiplica la capacidad de respuesta ante incidentes complejos, mientras que la adopción de estándares internacionales y auditorías periódicas asegura gobernanza y cumplimiento normativo. Este enfoque integral no solo protege sistemas y datos críticos, sino que garantiza la continuidad operativa, la seguridad de los trabajadores y la confianza de clientes y socios, constituyendo un factor diferenciador en la competitividad industrial.

Finalmente, la implementación de proyectos estructurados permite avanzar desde la evaluación inicial de riesgos hasta la consolidación de una cultura de ciberseguridad. Iniciativas como la actualización y protección de software industrial, la monitorización de seguridad, la gestión de vulnerabilidades, los ejercicios de respuesta a incidentes, la formación de personal y la adopción de buenas prácticas aseguran la resiliencia y reducen la exposición a amenazas. Cuando estas acciones se planifican de forma coordinada, la ciberseguridad deja de ser un coste operativo para convertirse en un habilitador estratégico, posicionando a las empresas como actores responsables, preparados y competitivos en un entorno industrial cada vez más digitalizado y automatizado.