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

Radiografía del sector industrial aragonés ante el reto de la ciberseguridad

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 transformación digital está redefiniendo la manera en que las empresas industriales diseñan, fabrican y comercializan sus productos. La conexión de máquinas, procesos y datos abre nuevas oportunidades de eficiencia y competitividad, pero también introduce riesgos crecientes asociados a la ciberseguridad. En un entorno donde la producción, la logística y la gestión dependen cada vez más de sistemas digitales interconectados, proteger la información y los activos industriales se ha convertido en una condición imprescindible para garantizar la continuidad operativa y la confianza en la industria.

En Aragón, dos clústeres empresariales desempeñan un papel clave en el impulso de la innovación y la digitalización industrial: **ANMOPYC** y **CAMPAG**.

ANMOPYC (Asociación Española de Fabricantes Exportadores de Maquinaria para Construcción, Obras Públicas y Minería) agrupa a más de un centenar de empresas fabricantes y distribuidoras de maquinaria y medios auxiliares, representando uno de los sectores industriales más dinámicos y exportadores de la comunidad. Desde su sede en Zaragoza, ANMOPYC actúa como motor de modernización tecnológica y como punto de encuentro para la cooperación, la internacionalización y la adopción de soluciones innovadoras que aumenten la competitividad del sector.

CAMPAG (Clúster Aragonés de los Medios de Producción Agrícolas y Ganaderos) integra a empresas industriales, centros tecnológicos, instituciones académicas y entidades de apoyo a la innovación con el objetivo de fomentar la excelencia tecnológica y la colaboración empresarial en torno a los medios de producción. Su labor se centra en la mejora de procesos, la digitalización industrial y la incorporación de tecnologías avanzadas —como la automatización, la sensórica o la inteligencia artificial— en el tejido productivo aragonés.

Ambos clústeres comparten una visión estratégica de la ciberseguridad industrial como factor esencial para consolidar la transformación digital del sector. Con esta motivación impulsaron conjuntamente el proyecto **securizAR**, financiado por el **Instituto Aragonés de Fomento** en el marco de la convocatoria de ayudas de apoyo a Agrupaciones Empresariales Innovadoras (AEI) para la realización de proyectos colaborativos, con el fin de fortalecer la ciberseguridad en la industria aragonesa, especialmente en los sectores vinculados a la maquinaria y los bienes de equipo.

El presente informe se enmarca en dicho proyecto y constituye un paso relevante para comprender la situación actual del tejido industrial aragonés ante los retos de la ciberseguridad, ofreciendo una visión global que sirva de referencia para el diseño de futuras actuaciones.

1.2. Objetivos del informe

El objetivo principal de este informe es diagnosticar el **nivel de preparación del tejido industrial aragonés frente a los desafíos de la ciberseguridad**, poniendo el foco en las empresas vinculadas a ANMOPYC y CAMPAG como sectores representativos de la industria manufacturera regional.

A través de este diagnóstico se pretende:

- Evaluar la madurez digital y de ciberseguridad de las empresas analizadas.
- Identificar brechas, necesidades y retos comunes que condicionan la adopción de soluciones de protección digital.
- Visibilizar el ecosistema aragonés de ciberseguridad industrial, incluyendo sus actores clave y capacidades disponibles.
- Analizar las oportunidades de financiación y apoyo existentes para el desarrollo de proyectos en esta materia.
- Y, en definitiva, proporcionar una base sólida para la toma de decisiones estratégicas orientadas a mejorar la seguridad, la resiliencia y la competitividad del tejido industrial aragonés.

1.3. Metodología empleada

Para elaborar este informe se ha seguido un enfoque integral que combina información cuantitativa y cualitativa, con el objetivo de ofrecer una visión completa del estado de la ciberseguridad industrial en Aragón. La metodología se estructuró en varias fases complementarias, que permitieron obtener datos fiables y contextualizados sobre las capacidades del tejido industrial y las oportunidades de mejora.

En primer lugar, se diseñó un **cuestionario sectorial** específico, dirigido a las empresas asociadas o vinculadas a los clústeres ANMOPYC y CAMPAG. Esta herramienta permitió recabar información sobre distintos ámbitos clave, como las políticas internas de seguridad, las medidas de protección adoptadas, la formación y competencias del personal, la inversión tecnológica y la percepción de riesgos. La encuesta se estructuró en siete bloques temáticos que cubren desde los datos generales de la empresa hasta la seguridad en la cadena de suministro y la concienciación del personal.

A continuación, se procedió a la recopilación de información directa, con la cumplimentación del cuestionario por parte de las empresas participantes. Esto permitió disponer de una visión representativa del tejido productivo aragonés y conocer de primera mano el nivel de preparación frente a los retos de la digitalización segura.

Posteriormente, se realizó un análisis de los resultados, clasificando a las empresas según su **nivel de madurez digital y de ciberseguridad**, identificando patrones, carencias y buenas prácticas. Esta fase sirvió como base para elaborar recomendaciones adaptadas a cada perfil empresarial y orientar acciones futuras de mejora.

La metodología también incluyó la identificación de **oportunidades de financiación y apoyo**, mediante la revisión de programas y convocatorias activas en los ámbitos regional, nacional y europeo que pueden facilitar la adopción de soluciones de ciberseguridad industrial.

Finalmente, se llevó a cabo un mapeo del **ecosistema aragonés de ciberseguridad**, recopilando información sobre agentes relevantes —como proveedores tecnológicos, centros de investigación, universidades, asociaciones y administraciones públicas— con capacidad para colaborar en proyectos de innovación y transferencia tecnológica.

Gracias a este enfoque integral, el informe ofrece una radiografía realista y contrastada del estado actual de la ciberseguridad industrial en Aragón, identificando fortalezas, brechas y áreas prioritarias de actuación y cooperación.

1.4. Herramienta de recogida de información: cuestionario sectorial

Para obtener una comprensión profunda de la situación de la ciberseguridad en el sector industrial aragonés y poder orientar futuras actuaciones, se diseñó un cuestionario exhaustivo que recoge información detallada sobre distintos aspectos de las empresas y su preparación en materia de ciberseguridad. La encuesta consta de 84 preguntas distribuidas en siete secciones, cada una enfocada en un ámbito específico de interés.

La primera sección se centra en los **datos generales de la empresa**, incluyendo información sobre tamaño, sector de actividad y ubicación. Estos datos permiten contextualizar los resultados y entender cómo las características organizativas pueden influir en el enfoque y las capacidades de ciberseguridad.

La segunda sección aborda aspectos generales de **seguridad informática**, explorando las políticas y prácticas implementadas, la frecuencia de evaluaciones de riesgo y la percepción de la importancia de la ciberseguridad dentro de la organización. Esta parte del cuestionario ayuda a identificar tendencias comunes y áreas que requieren atención prioritaria.

En la tercera sección, el foco se pone en el **personal dedicado a la ciberseguridad**. Se recaba información sobre la estructura del equipo, el número de profesionales involucrados, su formación y certificaciones, así como la existencia de roles específicos. Esta información permite evaluar la capacidad humana de respuesta ante incidentes y la preparación general de la organización.

La cuarta sección analiza la **gestión de la información digital de los procesos industriales**, incluyendo métodos de protección de datos, copias de seguridad y prácticas de recuperación ante incidentes. Esto ofrece una visión sobre la resiliencia y la seguridad de la información crítica para la operación industrial.

La quinta sección se centra en la **evaluación y gestión de incidentes de ciberseguridad**, recopilando información sobre su frecuencia, tipo de incidentes experimentados y eficacia de las medidas de mitigación adoptadas. Este bloque permite entender mejor las amenazas a las que se enfrenta cada empresa y su capacidad de reacción.

La sexta sección explora la **seguridad en la cadena de suministro**, un aspecto fundamental en un entorno industrial interconectado. Se analizan las prácticas de seguridad adoptadas, la evaluación de proveedores y la gestión de riesgos asociados, lo que permite garantizar la integridad del ecosistema industrial completo.

Finalmente, la séptima sección aborda la **formación y concienciación en ciberseguridad industrial**. Se recogen datos sobre programas de capacitación, frecuencia de las acciones formativas y percepción de su efectividad, aportando información sobre la cultura de seguridad y la preparación del personal.

La información obtenida a través de este cuestionario permite construir un panorama detallado y completo del estado de la ciberseguridad en el tejido industrial aragonés, identificando buenas prácticas, brechas y áreas de mejora. Los resultados de la encuesta han servido como base para elaborar el diagnóstico de madurez y capacidades en ciberseguridad presentado en este informe. El cuestionario completo, con todas sus preguntas y posibles respuestas, se encuentra disponible en el Apéndice A.

2. Caracterización del tejido industrial aragonés vinculado al sectro de maquinaria

El sector de la maquinaria en Aragón constituye un pilar fundamental de la economía regional, combinando tradición industrial, innovación tecnológica y dinamismo empresarial. Las empresas participantes en este análisis, vinculadas a las agrupaciones ANMOPYC y CAMPAG, representan distintos segmentos de la cadena de valor industrial, desde la fabricación de equipos completos hasta el suministro de componentes, servicios de integración y soluciones tecnológicas avanzadas.

2.1. Descripción general de las empresas participantes

Las organizaciones analizadas abarcan un amplio espectro de actividades industriales, incluyendo fabricantes de maquinaria de construcción, maquinaria agrícola y equipos auxiliares para distintos sectores productivos. **ANMOPYC** aglutina empresas orientadas principalmente a la **maquinaria de construcción, minería, reciclaje y servicios**, mientras que **CAMPAG** concentra su representatividad en el ámbito de la **maquinaria agrícola**. Esta diversidad de áreas de especialización refleja la capacidad del sector aragonés para atender a múltiples nichos de mercado, tanto nacionales como internacionales.

El conjunto de empresas participantes combina actores históricos con décadas de trayectoria en el sector y compañías emergentes orientadas a la innovación tecnológica. Esta mezcla favorece la transferencia de conocimiento, la adopción de buenas prácticas y el desarrollo de soluciones adaptadas a los retos actuales de digitalización y seguridad industrial.

2.2. Perfil tecnológico y digital de las organizaciones analizadas

El nivel de digitalización y la integración tecnológica en estas empresas varía significativamente según el tamaño, la actividad y la estrategia de innovación de cada compañía. Entre las organizaciones de mayor tamaño se observa un elevado grado de adopción de herramientas digitales: sistemas de control industrial, software de planificación de recursos empresariales (ERP), monitorización en tiempo real de procesos productivos y tecnologías de automatización avanzada. Estas empresas suelen disponer de departamentos dedicados a la innovación, la mejora continua y la gestión de riesgos digitales.

Por su parte, muchas pymes presentan una digitalización incipiente o focalizada en áreas concretas, como la gestión administrativa, la logística o la monitorización básica de maquinaria. Sin embargo, existe un interés creciente por soluciones que permitan

conectar los procesos productivos, obtener datos en tiempo real y mejorar la eficiencia mediante tecnologías digitales, lo que indica un potencial de crecimiento en este ámbito.

En términos de ciberseguridad, el análisis muestra que, si bien la mayoría de las empresas reconoce la importancia de proteger la información y los sistemas industriales, las prácticas y políticas implementadas no siempre son homogéneas ni sistemáticas. Muchas compañías están en fases iniciales de adopción de medidas de seguridad industrial, mientras que otras han avanzado hacia enfoques más estructurados, incluyendo auditorías periódicas, políticas de acceso y monitorización de sistemas OT/ICS.

2.3. Principales ámbitos de actividad y tamaño empresarial

El sector aragonés de la maquinaria se caracteriza por la coexistencia de empresas de distintos tamaños y perfiles de actividad. Las grandes empresas y fabricantes de maquinaria completa suelen liderar la incorporación de nuevas tecnologías y establecer estándares de calidad y seguridad en el sector. Estas compañías cuentan con capacidad para invertir en investigación, formación y sistemas de ciberprotección, lo que les permite anticiparse a riesgos emergentes y adoptar soluciones innovadoras.

Las pymes, que constituyen la mayoría del tejido industrial, destacan por su flexibilidad, especialización en nichos concretos y agilidad en la adopción de mejoras operativas. Si bien sus recursos para inversión tecnológica pueden ser más limitados, muchas buscan asociarse con centros tecnológicos, universidades y proveedores especializados para acceder a conocimientos y herramientas avanzadas, generando sinergias que fortalecen el ecosistema regional.

En cuanto a los ámbitos de actividad, las empresas participan en la fabricación de maquinaria agrícola, equipos para construcción y minería, componentes para sistemas industriales, soluciones de automatización y servicios de mantenimiento. Esta diversidad permite que el sector aragonés sea resiliente, con capacidad de adaptación ante cambios en la demanda y frente a los desafíos de la digitalización y la ciberseguridad industrial.

3. Diagnóstico de madurez y capacidades en ciberseguridad industrial

3.1. Resultados de la encuesta sectorial

La encuesta realizada a 27 empresas asociadas a ANMOPYC y CAMPAG ofrece una visión amplia y representativa del sector de maquinaria de construcción, minería y agrícola en Aragón. El conjunto de entidades participantes refleja un equilibrio entre compañías consolidadas con una larga trayectoria y otras de creación más reciente que aportan innovación y dinamismo al ecosistema industrial.

La mayoría de las empresas cuenta con más de dos décadas de experiencia, lo que pone de manifiesto la solidez y madurez del tejido industrial aragonés en este ámbito. Junto a ellas conviven organizaciones jóvenes, con menos de cinco años de actividad, que contribuyen a la modernización del sector mediante nuevos enfoques tecnológicos y modelos de negocio más flexibles.

En cuanto a su tamaño, predominan las pequeñas y medianas empresas, aunque el estudio también incorpora varias compañías de gran dimensión. Esta combinación permite disponer de un entorno equilibrado en el que las pymes aportan agilidad y especialización, mientras que las grandes firmas proporcionan capacidad de inversión, producción y acceso a mercados internacionales.

Si bien la mayoría de las organizaciones centra su actividad en el diseño y fabricación de maquinaria de construcción, minería o agrícola, es frecuente que complementen esta labor con servicios asociados, como la distribución, el alquiler, el montaje o el mantenimiento de equipos. Esta diversificación de actividades contribuye a aumentar la resiliencia del sector y su capacidad de adaptación a las demandas del mercado.

El grado de internacionalización es elevado: buena parte de las empresas desarrolla su actividad en mercados exteriores, lo que refleja un sector competitivo, exportador y con presencia consolidada en distintas regiones del mundo. No obstante, también existen compañías con un enfoque eminentemente nacional o regional, que desempeñan un papel clave en la cadena de valor local y en el soporte técnico especializado.

Desde el punto de vista de la estructura empresarial, coexisten modelos de gestión familiar y no familiar en proporciones similares. Esta dualidad permite combinar la continuidad y el arraigo propios de las empresas familiares con la profesionalización y los procesos más estructurados característicos de las corporaciones de mayor tamaño.

En términos económicos, la mayoría de las empresas se sitúa en rangos de facturación de entre 1 y 50 millones de euros anuales, aunque también se incluyen compañías de gran volumen que superan los 100 millones. Esta diversidad refleja la coexistencia de

diferentes escalas operativas dentro del mismo sector, capaces de cubrir desde nichos especializados hasta grandes proyectos internacionales.

Desde una perspectiva operativa, casi todas las empresas cuentan con personal propio para el mantenimiento de sus equipos y sistemas industriales, recurriendo a proveedores externos únicamente cuando se requieren intervenciones especializadas. Asimismo, la práctica totalidad permite el acceso remoto de proveedores autorizados para la resolución de incidencias, lo que favorece una respuesta rápida y eficiente ante posibles problemas técnicos.

Por último, la gestión de la información industrial se realiza mayoritariamente con recursos propios y en infraestructuras internas, una práctica que refleja la preocupación por mantener el control directo sobre los datos críticos del negocio. Algunas organizaciones, sin embargo, comienzan a adoptar soluciones híbridas que combinan almacenamiento interno con servicios en la nube, buscando un equilibrio entre seguridad, flexibilidad y continuidad operativa.

Información general sobre ciberseguridad

Las empresas del sector coinciden en que varios factores son clave para fortalecer la ciberseguridad en sus procesos industriales. Entre ellos, destacan la experiencia práctica de los proveedores en la aplicación de estándares de seguridad industrial, la disponibilidad de personal altamente cualificado en ciberseguridad, y el acceso a tecnologías específicas orientadas a proteger sistemas industriales. También se valora la posibilidad de realizar pruebas en entornos controlados conforme a requisitos estandarizados y contar con proveedores especializados en ciberseguridad industrial. Por el contrario, las certificaciones formales parecen tener un peso menor, lo que indica que la experiencia demostrable y las competencias prácticas son más valoradas que los títulos o acreditaciones académicas.

En cuanto a los impulsores para reforzar la ciberseguridad, la digitalización de los procesos industriales aparece como el principal motivo. Le siguen el cumplimiento normativo y la experiencia directa con incidentes de seguridad significativos, que actúa como un recordatorio de la importancia de contar con medidas de protección robustas.

Respecto a la inversión, muchas empresas del sector destinan porcentajes modestos de su facturación a ciberseguridad, generalmente centrados en cumplir con los requisitos legales y asegurar la continuidad de la operación, más que como una inversión estratégica de crecimiento.

En relación con los activos críticos, se subraya la protección de datos de clientes, propiedad intelectual, información de producción y datos financieros. Un número importante de empresas ha adoptado o planea implementar marcos normativos como

ISO 27001 o IEC 62443, mientras que otras todavía no aplican estándares formales de manera sistemática.

Finalmente, en cuanto a la evaluación de la eficacia de las medidas de seguridad, solo algunas empresas realizan auditorías internas periódicas, y varias aún no llevan a cabo ningún tipo de evaluación formal. Esto pone de manifiesto que, aunque existe conciencia sobre la importancia de la ciberseguridad, todavía hay margen de mejora en la monitorización y el control sistemático de los riesgos dentro del sector.

Información sobre el personal de ciberseguridad

En el sector de la maquinaria de construcción, minería y agrícola, la incorporación de la ciberseguridad en la estructura organizativa de las empresas se encuentra todavía en una fase incipiente. Solo un número reducido de compañías ha integrado esta función dentro del equipo directivo, generalmente vinculándola a perfiles tecnológicos existentes como el responsable de sistemas o el director técnico. En la mayoría de los casos, la seguridad digital se gestiona de forma transversal desde los departamentos de informática o de producción, o bien se confía a consultoras externas que prestan apoyo en aspectos concretos.

La falta de figuras directivas dedicadas en exclusiva a la ciberseguridad tiene su reflejo en la composición de los equipos. Predominan las estructuras reducidas, donde uno o dos técnicos compaginan funciones de soporte tecnológico con tareas relacionadas con la protección de sistemas y redes industriales. Solo unas pocas organizaciones disponen de personal especializado a tiempo completo, mientras que muchas dependen del asesoramiento de terceros para cubrir necesidades puntuales.

En cuanto a los perfiles profesionales, las empresas que buscan reforzar sus capacidades en ciberseguridad industrial valoran sobre todo la experiencia práctica en análisis de riesgos, la capacidad de respuesta ante incidentes y el conocimiento de los entornos de control industrial. Más que la certificación formal, se aprecia la capacidad para comprender la operativa de las plantas y adaptar las medidas de protección a equipos y procesos específicos del sector.

La formación del personal es otro de los ámbitos donde persiste margen de mejora. Una parte de las empresas facilita el acceso a cursos o jornadas especializadas, aunque la mayoría continúa sin disponer de un programa estructurado de capacitación. En general, las acciones formativas se realizan de manera puntual, vinculadas a proyectos concretos o a la incorporación de nuevas tecnologías, sin una planificación sistemática.

Tampoco es habitual que existan planes de sucesión o mecanismos formales para garantizar la transferencia de conocimiento en ciberseguridad. Ante la falta de estructuras consolidadas, muchas compañías recurren a la documentación interna de

procedimientos o a la formación cruzada entre personal de distintas áreas como forma de mitigar los riesgos derivados de la dependencia de personas clave.

Finalmente, la colaboración entre los equipos de ciberseguridad y el resto de departamentos aún es limitada. En la mayoría de los casos, la seguridad se percibe como una tarea técnica y no como una responsabilidad compartida, lo que dificulta su integración en la gestión global de la empresa. Las organizaciones más avanzadas comienzan a promover una cooperación más estrecha entre las áreas de producción, mantenimiento y sistemas, sentando así las bases para una cultura de seguridad industrial más madura y transversal.

Información sobre la gestión y almacenamiento de información digital de los procesos industriales

Las empresas del sector manufacturero de maquinaria gestionan la información de sus procesos industriales mediante una combinación de sistemas desarrollados internamente y soluciones comerciales específicas para la industria. Muchas organizaciones utilizan sus propias plataformas para adaptar la gestión de datos a sus necesidades, mientras que otras confían en software especializado disponible en el mercado.

En términos de cumplimiento normativo, varias compañías aplican estándares reconocidos del sector o regulaciones gubernamentales, mientras que un número menor todavía no sigue ninguna norma formal sobre gestión y almacenamiento de datos industriales. La información se almacena predominantemente en servidores locales, aunque cada vez más empresas combinan estas infraestructuras con servicios en la nube o soluciones híbridas para mayor flexibilidad y resiliencia.

Para proteger la información, las organizaciones implementan medidas diversas, incluyendo cifrado de datos, control de acceso basado en roles, auditorías periódicas y monitorización continua. La mayoría también aplica políticas de actualización y parches de seguridad, así como controles físicos de acceso a las instalaciones donde se almacenan los datos.

En cuanto a la retención de la información, algunas empresas cuentan con políticas documentadas, otras aplican directrices más informales y otras no poseen políticas específicas. Los periodos de almacenamiento dependen de la criticidad de los datos y del tipo de producto o proceso. El acceso a la información se gestiona mediante controles de autenticación multifactor y supervisión del uso de datos, garantizando que solo el personal autorizado pueda acceder a la información sensible.

Todas las organizaciones realizan copias de seguridad de sus datos, mayoritariamente de forma periódica, y las almacenan en servidores internos, en la nube de proveedores

confiables, en dispositivos externos o en sistemas de almacenamiento en red, incluidos sistemas distribuidos o replicados. La integridad de estos respaldos se asegura mediante técnicas de cifrado, controles de acceso y pruebas periódicas de recuperación, mientras que la disponibilidad se refuerza mediante almacenamiento en ubicaciones geográficamente dispersas y registro detallado de cada copia.

La integración de los sistemas de gestión de datos con otros sistemas empresariales es todavía parcial en muchas empresas, y algunas no cuentan con integración alguna. La actualización y mantenimiento de estos sistemas sigue un enfoque combinado: programas regulares de actualizaciones, pruebas en entornos de desarrollo y evaluación de impactos antes de aplicar cambios. Un pequeño número de empresas externaliza esta labor o no gestiona las actualizaciones de manera formal.

Para el control de cambios sobre la información, algunas organizaciones utilizan registros automáticos, otras mantienen un seguimiento manual, y varias realizan auditorías periódicas para asegurar trazabilidad y coherencia en los datos. En lo que respecta a la transferencia de información entre sistemas y ubicaciones, se aplican protocolos cifrados, redes privadas virtuales y validación de destinatarios autorizados para proteger la información sensible.

Finalmente, respecto a la preparación del personal, varias empresas ofrecen formación ocasional o sesiones regulares sobre prácticas seguras de gestión de la información industrial, mientras que otras limitan la capacitación únicamente al proceso de incorporación o no cuentan con programas formales de formación continua. Esto refleja una necesidad latente de fortalecer la concienciación y las competencias internas en ciberseguridad de la información industrial.

Información sobre la evaluación y gestión de incidentes de ciberseguridad

En las empresas del sector, la gestión de riesgos de ciberseguridad en procesos industriales automatizados recae principalmente en personal interno, con soporte puntual de especialistas externos. Algunas compañías confían completamente en integradores de automatización, mientras que otras cuentan con proveedores especializados en ciberseguridad. No obstante, todavía existe un grupo de empresas que no gestiona de manera formal los riesgos de ciberseguridad en sus procesos automatizados.

En cuanto a la evaluación de la postura de seguridad, muchas organizaciones combinan auditorías internas y externas, mientras que otras dependen únicamente de servicios externos. Existe también un número significativo que no realiza evaluaciones formales de manera regular. Para valorar la eficacia de las medidas implementadas, se utilizan auditorías internas, revisión de incidentes previos, simulacros de respuesta y métricas

de rendimiento. Sin embargo, varias empresas admiten que actualmente no evalúan de forma sistemática la eficacia de sus controles de seguridad.

La frecuencia de estas evaluaciones varía: algunas organizaciones realizan revisiones anuales, otras de manera trimestral o semestral, y algunas llevan a cabo evaluaciones mensuales. Sin embargo, un número importante todavía no realiza evaluaciones periódicas de sus sistemas industriales.

Entre las medidas de protección adoptadas para los sistemas de control industrial destacan los firewalls industriales, el control de acceso estricto, la segmentación de redes, detección de intrusiones y monitorización continua. Un pequeño grupo aún no ha implementado medidas específicas de protección.

Respecto a incidentes de ciberseguridad, varias empresas han experimentado eventos que, aunque en muchos casos han sido de baja repercusión, han permitido mejorar la seguridad de los sistemas. Las respuestas más comunes incluyen mitigación inmediata, implementación de mejoras en seguridad, notificación a autoridades y realización de investigaciones forenses cuando se considera necesario.

En lo que se refiere al acceso remoto a los sistemas industriales, la práctica habitual es restringirlo solo al personal autorizado, implementando autenticación de múltiples factores y supervisión continua. Algunas empresas no permiten acceso remoto, mientras que otras mantienen políticas más abiertas por necesidades operativas.

La gestión de actualizaciones y parches sigue diferentes enfoques: algunas organizaciones mantienen programas regulares de actualización, otras automatizan procesos o realizan pruebas en entornos de desarrollo antes de aplicarlas a producción, y algunas no gestionan formalmente esta tarea.

En cuanto a planes de respuesta a ciberincidentes, unas pocas empresas disponen de planes establecidos y probados, otras están en proceso de desarrollo, y varias no cuentan con ningún plan formal. De manera similar, la implementación de sistemas de gestión de incidentes que involucren a personal de distintas áreas aún es limitada, aunque algunas compañías están trabajando en ello.

La colaboración externa con organismos o comunidades de intercambio de información sobre amenazas cibernéticas es todavía incipiente. Solo algunas organizaciones participan activamente o están considerando hacerlo, mencionando como ejemplos entidades como INCIBE y asociaciones sectoriales.

Entre los principales desafíos identificados para la ciberseguridad industrial se encuentran la falta de concienciación del personal, la dificultad de equilibrar operatividad y seguridad, la escasez de profesionales especializados, la complejidad de integrar nuevas soluciones y la coexistencia de múltiples fabricantes. Algunos

participantes también destacan limitaciones presupuestarias como un factor que dificulta el desarrollo de planes de gestión de ciberincidentes.

Por último, solo una parte de las empresas cuenta con planes específicos de Continuidad del Negocio y Recuperación ante Desastres orientados a ciberincidentes, mientras que otras se encuentran en fase de desarrollo. La revisión de estos planes se realiza con distinta frecuencia: principalmente anual, aunque algunas compañías revisan sus planes de manera semestral o continúan ajustándolos a medida que evolucionan sus procesos y riesgos.

Información sobre seguridad en la cadena de suministro

En el ámbito del sector manufacturero de maquinaria, pocos cambios recientes en la cadena de suministro han tenido un impacto directo en la ciberseguridad de las empresas. La mayoría de las organizaciones no ha detectado alteraciones significativas que requieran ajustes específicos en sus políticas de seguridad.

La evaluación de la seguridad de la cadena de suministro frente a amenazas cibernéticas se realiza de manera desigual. Algunas empresas colaboran con terceros para auditorías especializadas, mientras que otras realizan evaluaciones internas de forma ocasional. Sin embargo, existe un número considerable que aún no ha implementado ningún tipo de evaluación sistemática.

Entre las prácticas más habituales para revisar la ciberseguridad de los proveedores destacan cuestionarios de seguridad y análisis de riesgos, mientras que las auditorías presenciales y el monitoreo continuo son menos frecuentes. Aun así, un buen número de organizaciones no evalúa actualmente la seguridad de sus proveedores.

En relación con la integración de proveedores en los planes de contingencia y continuidad del negocio, algunas compañías incluyen explícitamente a sus socios clave en ambos planes, aunque la mayoría no contempla esta integración de manera formal.

Para proteger la información sensible durante su transferencia a lo largo de la cadena de suministro, las medidas más utilizadas son el cifrado de datos y políticas de acceso restringido. Otras acciones, como la protección frente a ataques de intermediarios, son menos comunes, y un grupo de empresas reconoce no tener ninguna protección específica en este ámbito.

Respecto a la resiliencia de la cadena de suministro frente a ciberincidentes, las estrategias más habituales incluyen la implementación de planes de continuidad del negocio, colaboración con proveedores en análisis de riesgos y establecimiento de estrategias de recuperación rápida. Sin embargo, muchas organizaciones aún no han adoptado medidas concretas o no disponen de información clara sobre este aspecto.

En materia de formación, la gran mayoría de las empresas no proporciona capacitación en ciberseguridad a sus proveedores, y solo unas pocas lo hacen de manera puntual. De manera similar, la evaluación de riesgos potenciales en cada etapa de la cadena de suministro se centra principalmente en análisis de riesgos periódicos y colaboración con expertos, aunque muchas compañías todavía no realizan ningún tipo de revisión sistemática.

Las medidas de protección frente a ciberataques dirigidos a proveedores son limitadas. Solo algunas empresas establecen acuerdos contractuales sobre seguridad o colaboran en estrategias de respuesta a incidentes, mientras que la mayoría no aplica acciones específicas en este sentido. En cuanto a las políticas de notificación de incidentes por parte de los proveedores, solo un pequeño grupo cuenta con procedimientos formales de comunicación inmediata o colaboración en investigaciones, y la mayoría carece de políticas claras.

Por último, en lo que respecta a la innovación segura en el desarrollo de nuevos productos y tecnologías, varias organizaciones implementan evaluaciones de riesgos durante las fases de desarrollo, colaboran con proveedores en I+D y aplican estándares de seguridad en el diseño. Sin embargo, un porcentaje relevante de empresas todavía no promueve de manera activa la innovación segura.

La participación en iniciativas de colaboración con otras empresas del sector para mejorar la ciberseguridad de la cadena de suministro es todavía limitada. Algunas compañías colaboran en el desarrollo de estándares de seguridad o en el intercambio de información, mientras que la mayoría no participa en este tipo de actividades ni tiene planes inmediatos de hacerlo.

Información sobre la capacitación y concienciación en ciberseguridad industrial

En las empresas del sector, la alta dirección suele mostrar un grado elevado de conciencia sobre los riesgos asociados a la ciberseguridad industrial. La mayoría de las organizaciones considera que la dirección está bien informada y preocupada por estas amenazas, aunque todavía existen algunas empresas donde el nivel de conocimiento es moderado o bajo.

La identificación de las necesidades de capacitación se realiza principalmente mediante el análisis de riesgos de seguridad, la revisión de incidentes anteriores y la evaluación de las competencias actuales del personal. Sin embargo, varias organizaciones reconocen que aún no cuentan con un sistema activo para detectar y priorizar estas necesidades.

En cuanto a los programas de formación, muchas compañías ofrecen cursos de manera ocasional o únicamente durante la incorporación de nuevo personal, mientras que otras aún carecen de formación formal. Entre los contenidos más comunes destacan las

buenas prácticas de seguridad, la prevención de phishing y el uso seguro de dispositivos y redes, así como la concienciación sobre amenazas actuales. No obstante, un número significativo de empresas todavía no dispone de ningún programa de capacitación específico.

Para reforzar la conciencia y colaboración del personal, se emplean distintas estrategias, como sesiones de formación periódicas, comunicaciones sobre amenazas, pruebas internas de phishing y políticas de seguridad claramente definidas. A pesar de ello, muchas organizaciones aún no implementan medidas sistemáticas para involucrar activamente a su personal en estos programas.

La evaluación de la efectividad de los programas de capacitación es limitada. Solo algunas empresas realizan análisis posteriores a la formación, simulaciones de phishing o seguimiento de comportamientos seguros, mientras que la mayoría no realiza ningún tipo de evaluación.

La formación continua del personal en nuevas amenazas y tecnologías sigue siendo insuficiente en muchas organizaciones. Solo un grupo de empresas proporciona actualizaciones de forma regular o en ocasiones específicas, y la participación activa de los empleados en estos programas es generalmente baja.

La adaptación de los contenidos de capacitación según roles y responsabilidades específicas también es limitada. Algunas empresas ofrecen programas generales para todo el personal, y pocas cuentan con formación personalizada para cada departamento o función.

Tras la capacitación inicial, pocas organizaciones implementan medidas de refuerzo, como simulacros de incidentes, sesiones de repaso o evaluaciones recurrentes de conocimientos. Asimismo, la disponibilidad de recursos de autocapacitación, como módulos en línea, es escasa y todavía no está generalizada en el sector.

Por último, la colaboración con expertos externos o instituciones educativas para formación especializada es aún limitada. La mayoría de las empresas confía únicamente en personal interno y no ofrece formación externa especializada, lo que refleja un área de mejora importante para aumentar la resiliencia frente a riesgos cibernéticos en el sector industrial.

3.2. Nivel de madurez digital y de ciberseguridad

El análisis de los resultados obtenidos permite establecer una visión clara sobre el nivel de madurez digital y de ciberseguridad de las empresas del sector de maquinaria en Aragón. En términos generales, puede afirmarse que el sector se encuentra en una **fase intermedia de madurez**, caracterizada por una **amplia conciencia sobre la importancia**

de la ciberseguridad, pero con un **grado de implantación desigual** de medidas, políticas y estructuras formales de protección.

La digitalización industrial está avanzando de manera significativa, impulsada por la automatización de procesos, la monitorización remota de equipos y la incorporación progresiva de soluciones digitales de gestión y control. No obstante, este desarrollo tecnológico no siempre se ha acompañado de una estrategia integral de ciberseguridad. En muchos casos, las medidas implementadas responden a **necesidades operativas inmediatas o requisitos normativos**, más que a una planificación preventiva y estratégica de la seguridad digital.

En función de los resultados del cuestionario y de la interpretación de los indicadores recogidos, puede establecerse una clasificación orientativa de las empresas en tres niveles de madurez:

- **Nivel inicial (alrededor del 40 % de las empresas):** organizaciones que han comenzado a digitalizar sus procesos, pero carecen de políticas formales de seguridad o procedimientos documentados. La gestión de la ciberseguridad se aborda de manera reactiva, generalmente a través de personal de sistemas o proveedores externos, sin estructuras específicas ni planes de continuidad del negocio claramente definidos.
- **Nivel intermedio (aproximadamente el 45 %):** empresas con cierta consolidación en materia de digitalización y con medidas básicas de ciberprotección implantadas, como control de accesos, copias de seguridad y segmentación de redes. Estas organizaciones han adoptado una postura más proactiva, realizan auditorías o evaluaciones de riesgos de forma puntual y muestran interés en avanzar hacia la certificación en normas reconocidas como ISO 27001 o IEC 62443.
- **Nivel avanzado (alrededor del 15 %):** compañías que han integrado la ciberseguridad dentro de su estrategia empresarial y disponen de personal cualificado, políticas formales, planes de respuesta a incidentes y programas de formación continua. Este grupo corresponde principalmente a empresas de mayor tamaño o con fuerte orientación internacional, que consideran la ciberseguridad un elemento clave para su competitividad y reputación.

En conjunto, la madurez digital del sector puede considerarse **moderada**, con una sólida base de digitalización en procesos productivos, pero con **carencias en la gestión integral del riesgo cibernético**. La mayoría de las empresas no dispone todavía de un **sistema de gestión de ciberseguridad industrial estructurado**, ni de mecanismos sistemáticos de evaluación y mejora continua.

Otro aspecto relevante es la **escasa integración entre las áreas IT y OT**, lo que genera brechas en la supervisión conjunta de sistemas y dificulta la aplicación de medidas de seguridad transversales. Las empresas más avanzadas están comenzando a implantar arquitecturas segmentadas y herramientas de monitorización que permiten una detección temprana de incidentes, pero se trata todavía de un número limitado de casos.

En materia de **concienciación y formación**, el grado de madurez también es heterogéneo. Si bien existe una creciente sensibilización entre la dirección y el personal técnico, las acciones formativas suelen ser esporádicas y no siempre se adaptan a los distintos niveles de responsabilidad. Este factor, unido a la falta de especialistas internos en ciberseguridad industrial, limita la capacidad de respuesta ante incidentes y la consolidación de una cultura organizativa orientada a la seguridad.

Por último, aunque la adopción de estándares y certificaciones todavía es incipiente, se observa una **tendencia positiva hacia la profesionalización** de la ciberseguridad industrial, especialmente en las empresas que participan en proyectos de innovación o colaboran con centros tecnológicos y proveedores especializados. Esta evolución, unida a la creciente digitalización de los procesos industriales, sugiere que el sector está preparado para **avanzar hacia niveles superiores de madurez** si cuenta con apoyo técnico, formación específica y mecanismos de colaboración adecuados.

3.3. Barreras, necesidades y retos comunes

El análisis de los resultados obtenidos a través del cuestionario sectorial y de la información complementaria recopilada permite identificar un conjunto de barreras, necesidades y retos comunes que condicionan la adopción de medidas de ciberseguridad industrial en las empresas aragonesas. Estos elementos reflejan tanto limitaciones estructurales y operativas como oportunidades para fortalecer la resiliencia y competitividad del sector.

Barreras para la adopción de ciberseguridad industrial

Entre las principales barreras identificadas destacan:

- **Recursos financieros limitados:** La mayoría de las pymes dispone de presupuestos reducidos para inversión en ciberseguridad, orientados principalmente a cumplir requisitos normativos y asegurar la continuidad operativa. Esto dificulta la adquisición de soluciones avanzadas y la contratación de personal especializado.
- **Falta de personal cualificado:** Existe escasez de profesionales con experiencia específica en ciberseguridad industrial, especialmente en la integración de sistemas IT/OT y en la protección de entornos de control industrial. Muchas

empresas dependen de consultoras externas o personal técnico multitarea, lo que limita la capacidad de respuesta ante incidentes complejos.

- **Baja integración entre IT y OT:** La separación de sistemas de tecnologías de la información y sistemas de control industrial genera brechas de seguridad, dificultando la aplicación de políticas y controles coherentes en toda la organización.
- **Desconocimiento de riesgos específicos:** A pesar de la concienciación general sobre la importancia de la ciberseguridad, muchas empresas carecen de procedimientos formales de análisis de riesgos, evaluación de proveedores o pruebas de resiliencia ante ciberincidentes.
- **Complejidad tecnológica y diversidad de fabricantes:** La coexistencia de múltiples sistemas, equipos y proveedores dificulta la implementación de soluciones homogéneas de protección, especialmente en cadenas de suministro interconectadas.

Necesidades del sector

A partir de las barreras identificadas, se observan necesidades comunes que deberían ser abordadas para fortalecer la ciberseguridad industrial:

- **Formación y concienciación:** Es imprescindible incrementar la capacitación del personal en todos los niveles, desde la alta dirección hasta operarios de planta, incluyendo conocimientos prácticos sobre riesgos, buenas prácticas y protocolos de actuación ante incidentes.
- **Herramientas y soluciones tecnológicas adaptadas:** Las empresas requieren tecnologías específicas para la monitorización de sistemas OT, detección de intrusiones, segmentación de redes y gestión de incidentes, así como soluciones integradas que faciliten la cooperación entre áreas IT y OT.
- **Certificaciones y estándares sectoriales:** La adopción de marcos normativos como ISO 27001, IEC 62443 o estándares internos de buenas prácticas ayudaría a estructurar la gestión de riesgos y reforzar la confianza de clientes y socios.
- **Colaboración y apoyo externo:** Se destaca la necesidad de acceso a expertos, centros tecnológicos y programas de apoyo público o privado que faciliten la implantación de medidas de seguridad avanzadas, así como el intercambio de información sobre amenazas y buenas prácticas entre empresas del sector.

Retos estratégicos y operativos

Además de las barreras y necesidades, las empresas se enfrentan a retos estratégicos y operativos que condicionan su evolución en materia de ciberseguridad:

- **Resiliencia y continuidad de negocio:** Garantizar la operación frente a incidentes cibernéticos es un reto crítico, especialmente para aquellas organizaciones con dependencia de sistemas interconectados o con actividad internacional.
- **Gestión de la cadena de suministro:** La seguridad de proveedores y socios constituye un desafío creciente, dado el nivel de interdependencia tecnológica y la falta de evaluación sistemática de riesgos en muchos casos.
- **Digitalización segura:** La transformación digital industrial debe acompañarse de estrategias de ciberseguridad integradas desde el diseño de procesos, evitando que la adopción de nuevas tecnologías genere vulnerabilidades.
- **Cultura organizativa:** Promover la concienciación y la responsabilidad compartida sobre ciberseguridad entre todas las áreas de la empresa constituye un reto continuo, que requiere liderazgo de la dirección y estructuras internas consolidadas.
- **Evolución normativa y tecnológica:** Las empresas deben adaptarse a un entorno normativo en constante cambio y a la rápida evolución de amenazas y tecnologías, manteniendo capacidad de aprendizaje y actualización permanente.

A continuación, en la Tabla 1 se presenta una **síntesis de los niveles de madurez digital y de ciberseguridad** identificados en el sector de maquinaria en Aragón, junto con las principales **barreras, necesidades y retos comunes** detectados. Esta tabla permite visualizar de forma estructurada las diferencias entre los tres perfiles de madurez —inicial, intermedio y avanzado—, facilitando la interpretación de los resultados del diagnóstico y la priorización de acciones de mejora.

La información recogida refleja que la mayoría de las empresas se sitúan en niveles **inicial e intermedio**, caracterizados por un grado de digitalización progresivo pero todavía con importantes carencias en la gestión integral de la ciberseguridad. En estos segmentos predominan las medidas reactivas, la ausencia de responsables específicos y la dependencia de proveedores externos. Por el contrario, el grupo reducido de empresas con un nivel **avanzado** demuestra una integración más estratégica de la ciberseguridad, con estructuras internas definidas, personal especializado y políticas consolidadas.

Tabla 1. Niveles de madurez digital y de ciberseguridad en el sector industrial aragonés y principales barreras, necesidades y retos asociados

Nivel de madurez	Porcentaje de empresas	Características principales	Barreras más relevantes	Necesidades prioritarias	Retos estratégicos
Inicial	40 %	• Digitalización incipiente de procesos. • Ausencia de políticas o responsables de ciberseguridad. • Medidas reactivas y dispersas. • Dependencia de proveedores externos sin estrategia interna.	• Falta de presupuesto. • Escasez de personal cualificado. • Baja integración IT/OT. • Limitada concienciación del personal.	• Formación básica y concienciación. • Asesoramiento externo. • Procedimientos y controles iniciales. • Evaluación de activos críticos.	• Establecer cultura de seguridad. • Implementar medidas mínimas de protección. • Preparar continuidad operativa.
Intemedio	45 %	• Procesos parcialmente digitalizados. • Controles básicos implantados (copias de seguridad, antivirus, contraseñas, segmentación de redes). • Evaluaciones de riesgo puntuales. • Interés en certificaciones y buenas prácticas.	• Recursos limitados para certificaciones avanzadas. • Conocimiento insuficiente de riesgos globales. • Coordinación interdepartamental incompleta.	• Formación avanzada adaptada a roles. • Herramientas de monitorización OT. • Adopción de estándares y certificaciones. • Gestión segura de la cadena de suministro.	• Mejorar resiliencia. • Coordinar IT y OT. • Consolidar gestión de riesgos.
Avanzado	15 %	• Ciberseguridad integrada en estrategia empresarial. • Personal especializado. • Planes de respuesta a incidentes y formación continua. • Innovación segura en procesos y productos.	• Complejidad tecnológica. • Adaptación a normativas y evolución de amenazas.	• Actualización continua de estrategia. • Innovación segura y pruebas de vulnerabilidad. • Formación especializada y retención de talento. • Participación en ecosistemas de colaboración.	• Mantener liderazgo en seguridad. • Adaptación a nuevas amenazas. • Digitalización segura y resiliente.

En conjunto, el análisis evidencia que **el avance hacia niveles superiores de madurez requiere superar barreras estructurales** —como la falta de recursos, la escasez de talento y la baja integración IT/OT—, al tiempo que se refuerzan las capacidades organizativas y tecnológicas. Este diagnóstico constituye la base para las **recomendaciones por nivel de madurez** que se presentan en el siguiente apartado.

3.4. Recomendaciones por nivel de madurez

A partir del diagnóstico realizado, se plantean recomendaciones específicas para cada nivel de madurez identificado, con el objetivo de orientar a las empresas en la mejora progresiva de su ciberseguridad industrial. Estas recomendaciones combinan acciones estratégicas, operativas y de formación, adaptadas a los recursos y capacidades de cada perfil empresarial.

Nivel Inicial (40 % de las empresas)

- **Implantación de políticas y procedimientos básicos de ciberseguridad:** Establecer normas internas de acceso a sistemas, gestión de contraseñas, control de dispositivos y actualización de software
- **Formación y concienciación del personal:** Realizar cursos básicos y talleres prácticos sobre riesgos cibernéticos y buenas prácticas, dirigidos a todos los niveles organizativos.
- **Evaluación inicial de riesgos y activos críticos:** Identificar los sistemas y datos más relevantes para la operación industrial y definir medidas mínimas de protección.
- **Colaboración con proveedores y asesores externos:** Incorporar apoyo de consultoras o integradores especializados para cubrir carencias de personal y experiencia interna.
- **Desarrollo de planes de continuidad del negocio básicos:** Establecer procedimientos de recuperación ante incidentes y respaldo de información crítica.

Nivel Intermedio (45 % de las empresas)

- **Consolidación de medidas de ciberprotección:** Implementar segmentación de redes, monitorización de sistemas industriales, control de accesos avanzados y auditorías periódicas de seguridad.

- **Adopción de estándares y certificaciones:** Comenzar la alineación con normas reconocidas (ISO 27001, IEC 62443) para estructurar la gestión de riesgos y mejorar la confianza de clientes y socios.
- **Fortalecimiento de la formación y concienciación:** Desarrollar programas regulares de capacitación avanzada, adaptados a roles específicos y a la operativa de los sistemas industriales.
- **Integración IT/OT y coordinación interdepartamental:** Establecer protocolos y estructuras que permitan una gestión unificada de los riesgos cibernéticos en toda la organización.
- **Gestión segura de la cadena de suministro:** Evaluar proveedores, establecer requisitos contractuales de seguridad y promover la colaboración en iniciativas de innovación segura.

Nivel Avanzado (15 % de las empresas)

- **Optimización y actualización continua de la estrategia de ciberseguridad:** Revisar y mejorar periódicamente políticas, procedimientos y sistemas de protección ante la evolución de amenazas.
- **Innovación segura en procesos y productos:** Incorporar criterios de ciberseguridad desde el diseño de nuevos productos y tecnologías, incluyendo pruebas de vulnerabilidad y análisis de riesgos.
- **Formación especializada y desarrollo de talento interno:** Mantener programas avanzados de capacitación, fomentar la especialización y retención de profesionales cualificados en ciberseguridad industrial.
- **Participación en ecosistemas de colaboración:** Interactuar con centros tecnológicos, asociaciones sectoriales y comunidades de intercambio de información sobre amenazas para anticiparse a riesgos emergentes.
- **Fortalecimiento de la resiliencia y continuidad de negocio:** Mejorar planes de recuperación ante incidentes y pruebas de estrés periódicas, asegurando la capacidad de respuesta ante escenarios críticos de ciberataques o fallos tecnológicos.

Con el objetivo de orientar a las empresas industriales en la mejora progresiva de su ciberseguridad, la siguiente tabla presenta un conjunto de **recomendaciones específicas según el nivel de madurez digital y de ciberseguridad** identificado en el diagnóstico sectorial. Estas orientaciones permiten adaptar las estrategias de actuación a las capacidades, recursos y situación tecnológica de cada organización, fomentando una

evolución gradual y sostenible hacia modelos de gestión de la ciberseguridad más avanzados.

Tabla 2. Recomendaciones por nivel de madurez digital y de ciberseguridad en el sector industrial aragonés

Nivel de madurez	Porcentaje de empresas	Características principales
Inicial	40 %	• Implantar políticas y procedimientos básicos de ciberseguridad. • Formar y concienciar al personal en riesgos y buenas prácticas. • Evaluar activos críticos y establecer medidas mínimas de protección. • Colaborar con proveedores y asesores externos. • Desarrollar planes básicos de continuidad del negocio y backups.
Intemedio	45 %	• Consolidar medidas de protección (segmentación de redes, monitorización, control de accesos). • Adoptar estándares y certificaciones reconocidas (ISO 27001, IEC 62443). • Fortalecer programas de formación adaptados a roles específicos. • Integrar IT/OT y fomentar coordinación interdepartamental. • Gestionar la cadena de suministro de forma segura y colaborativa.
Avanzado	15 %	• Optimizar y actualizar continuamente la estrategia de ciberseguridad. • Incorporar innovación segura en procesos y productos. • Mantener formación especializada y retención de talento interno. • Participar en ecosistemas de colaboración sectorial y tecnológico. • Fortalecer la resiliencia y los planes de continuidad ante incidentes críticos.

La aplicación de estas recomendaciones permitirá a las empresas **fortalecer su resiliencia frente a ciberamenazas**, consolidar una cultura de seguridad transversal y avanzar hacia una **transformación digital segura y competitiva**. Asimismo, la diferenciación por niveles de madurez facilita el diseño de **itinerarios personalizados de mejora**, contribuyendo al objetivo global del proyecto *securizAR* de impulsar la ciberseguridad industrial en Aragón mediante acciones adaptadas a la realidad del tejido productivo.

4. Ecosistema aragonés de ciberseguridad industrial

El ecosistema de ciberseguridad industrial en Aragón se caracteriza por la **coexistencia de múltiples actores** que aportan capacidades complementarias en formación, desarrollo tecnológico, soluciones empresariales y colaboración sectorial. Estos agentes facilitan la protección de sistemas industriales, la adopción de buenas prácticas y la promoción de la innovación digital, constituyendo un soporte clave para que las empresas del sector de la maquinaria mejoren su resiliencia frente a riesgos cibernéticos.

4.1. Ámbito empresarial

Aragón cuenta con un conjunto diverso de empresas que ofrecen soluciones de ciberseguridad industrial, consultoría tecnológica y servicios especializados para la protección de sistemas OT/ICS. Entre las más representativas destacan:

- **Alfa 5.** Proveedor local de soluciones de seguridad informática y servicios de monitorización para entornos industriales. Ofrece soporte en continuidad operativa, gestión de parches y detección temprana de incidentes.
- **Asistec Bajo Aragón.** Empresa de servicios tecnológicos y mantenimiento industrial que presta servicios a pymes manufactureras de la provincia de Teruel y zonas limítrofes; realiza auditorías preventivas y soporte en gestión de incidentes operativos y de seguridad.
- **Continuum Security (IriusRisk).** Empresa creadora de IriusRisk, herramienta de threat-modelling y análisis automatizado de riesgos en arquitecturas software y sistemas conectados. Su producto es usado para securizar diseño de aplicaciones y procesos digitales industriales.
- **Cibergob.** Consultoría orientada a la seguridad de la información y cumplimiento normativo (ISO 27001, RGPD) para organizaciones públicas y privadas, con experiencia en adaptar controles a entornos industriales y corporativos.
- **Ciberseguridad Aragón.** Empresa regional dedicada a la formación, auditoría y servicios de ciberseguridad aplicados a la industria: phishing tests, pentesting en entornos OT/ICS y programas de concienciación para operarios.
- **Ciberseguros.** Especialista en soluciones de aseguramiento cibernético: evaluación de exposición, diseño de coberturas y gestión de siniestros relacionados con incidentes digitales para empresas industriales.

- **Dasit.** Integrador de sistemas de control industrial (OT/ICS) que incorpora medidas de protección, segmentación y monitorización para maquinaria conectada y líneas de producción.
- **Digital Hand Made.** Empresa de desarrollo de soluciones digitales con foco en seguridad de software embebido y plataformas industriales: cifrado de datos, hardening de dispositivos y gestión de firmware seguro.
- **Esi Soluciones.** Consultora tecnológica que presta servicios de ciberseguridad (SIEM, IDS/IPS, auditorías, respuesta a incidentes) para clientes medianos y grandes, con experiencia en entornos productivos.
- **GFT.** Consultora internacional con presencia en Zaragoza que ofrece servicios de modernización IT y ciberseguridad (aplicaciones seguras, cloud y compliance) y puede prestar soporte a la industria local.
- **Global Technology.** Firma orientada a infraestructuras IT/OT; ayuda a las empresas a segmentar redes industriales, cifrar comunicaciones entre planta y nube, y desplegar soluciones de protección perimetral y comunicaciones seguras.
- **Guara Servicios Informáticos.** Proveedor local de soporte TI para pymes y entidades del Alto Aragón; ofrece administración de redes, firewalls gestionados y servicios básicos de ciberseguridad.
- **Hiberus Tecnología.** Gran consultora tecnológica con base en Aragón que presta servicios de transformación digital, integración de sistemas y ciberseguridad (SOC, detección, respuesta y servicios gestionados). Atiende a clientes industriales con soluciones 360º.
- **Inycom.** Consultora e integrador aragonés con amplia presencia sectorial; ofrece servicios de ciberseguridad avanzada para empresas industriales, soluciones de red, control de accesos y asesoramiento en continuidad de negocio.
- **Integra Tecnología.** Empresa tecnológica aragonesa especializada en ciberseguridad, IA y consultoría; realiza auditorías OT/ICS, servicios gestionados de seguridad y está ampliando plantilla y capacidades en Aragón (proyectos e inversiones recientes).
- **ITCY Proyectos Tecnológicos.** Empresa focalizada en desarrollo de software seguro y consultoría tecnológica para sectores industriales; trabaja en asegurar cadenas de suministro de software/firmware y en proyectos de integración segura.

- **JEVA Systems & Compliance.** Firma que ofrece servicios de cumplimiento normativo (RGPD, ISO) y seguridad de la información, con actividades de implantación de controles, auditorías y gestión de identidades.
- **DXC Technology.** Multinacional con centro en Zaragoza que presta servicios de cloud, modernización de aplicaciones, IA y seguridad gestionada. Su presencia en Aragón aporta capacidades de integración, seguridad a gran escala y servicios gestionados (relevante para empresas industriales que requieren SOC y modernización IT/OT).
- **SafetyBits.** Plataforma especializada en OT Security Posture Management (OT-SPM) para la ciberseguridad industrial (detección de activos OT, control de configuraciones y cumplimiento NIS2), con operaciones o representación en Zaragoza.
- **Sincronet Security & Networking.** Especialista local en monitorización de redes y seguridad industrial, con enfoque en detección de intrusiones y respuesta en entornos de manufactura y maquinaria conectada.

4.2. Asociaciones y clústeres

El ecosistema se ve reforzado por asociaciones y clústeres sectoriales, que facilitan la colaboración, la difusión de buenas prácticas y la estandarización de procesos de ciberseguridad. Entre los más representativos se encuentran:

- **Tecnara Cluster TIC de Aragón**: clúster que agrupa empresas del sector TIC, promoviendo innovación, transferencia de conocimiento y proyectos colaborativos relacionados con ciberseguridad.
- **IDiA** (Investigación, Desarrollo e Innovación en Aragón): clúster que fomenta la I+D+i y apoya proyectos de seguridad industrial, promoviendo sinergias entre empresas y centros tecnológicos.
- **Asociación Aragonesa de Delegados de Protección de Datos**: orientada a la formación y concienciación sobre protección de datos, normativa y seguridad de la información.
- **Asociación de Ingenieros de Telecomunicación de Aragón**: ofrece programas de formación, eventos y soporte técnico especializado, incluyendo ciberseguridad en redes y sistemas de comunicación.

Estos organismos contribuyen mediante programas de formación, eventos de networking, proyectos colaborativos y difusión de información sobre ciberamenazas, generando sinergias con las empresas del sector de maquinaria para impulsar la adopción de estándares de seguridad y mejorar la resiliencia del tejido productivo.

4.3. Hubs y centros tecnológicos

Los hubs y centros tecnológicos proporcionan capacidades de investigación, desarrollo de soluciones y entornos de prueba controlados para la industria. Entre los principales destacan:

- **Aragón Digital Innovation Hub (DIH)**: promueve la digitalización industrial, incluyendo proyectos de ciberseguridad, conectividad y mejora de procesos productivos.
- **Grupo DisCo – Universidad de Zaragoza**: Grupo de I+D en Computación Distribuida que desarrolla soluciones de ciberseguridad aplicadas a entornos industriales.
- **Grupo CeNIT – Universidad de Zaragoza**: especializado en redes de comunicación, tecnologías de la información y ciberseguridad, proporcionando investigación aplicada y colaboración con empresas.
- **Cátedra Telefónica-Universidad de Zaragoza y Grupo RME**: Escuela de retos de ciberseguridad, destinada a detectar talento y mejorar las capacidades de estudiantes universitarios mediante proyectos prácticos y formación especializada.
- **Instituto Tecnológico de Aragón (ITA)**: Centro tecnológico público aragonés fundado en 1984, dotado de más de 280 profesionales y especializado en I+D+i para apoyar la competitividad de las empresas. Sus actividades abarcan proyectos de innovación, ensayos y servicios tecnológicos en ámbitos como lo digital-industrial, mecatrónica, materiales o data/IA, y es considerado un actor estratégico para la digitalización del tejido productivo aragonés.

Estos centros permiten al sector de maquinaria acceder a tecnologías emergentes, prototipos seguros y talento cualificado, facilitando la adopción de soluciones de ciberseguridad adaptadas a los procesos industriales.

4.4. Ámbito universitario y educativo

El ecosistema universitario y educativo en Aragón ofrece formación especializada y desarrollo de talento en ciberseguridad industrial. Entre las ofertas más destacadas se encuentran:

- Grado en Ingeniería de la Ciberseguridad (Universidad San Jorge)
- Programas y Másteres en Ciberseguridad (Universidad de Zaragoza)
- Programa Ejecutivo en Ciberseguridad (CEEIARAGON-EOI)

- Formación Profesional en Ciberseguridad aplicada a TI (Aragón)
- Experto en Ciberseguridad (Universidad Autónoma de Madrid e Ibercaja)
- Máster en Ciberseguridad (CESTE)

Estos programas contribuyen a preparar personal especializado para las empresas del sector, a cubrir la escasez de perfiles cualificados y a fomentar la incorporación de talento joven mediante prácticas y colaboraciones académicas.

4.5. Sinergias con el sector de la maquinaria

La interacción entre los distintos actores del ecosistema y el sector de la maquinaria permite generar sinergias estratégicas que fortalecen la ciberseguridad industrial:

- **Colaboración con centros tecnológicos** para desarrollar soluciones adaptadas a maquinaria específica y sistemas industriales críticos.
- **Participación en clústeres y asociaciones** para intercambiar experiencias, estandarizar procedimientos y compartir información sobre amenazas emergentes.
- **Aprovechamiento de programas de formación** para capacitar personal interno y cubrir vacantes de especialistas.
- **Integración con proveedores y consultoras** para implementar medidas preventivas y mejorar la resiliencia operativa de los procesos industriales.

En conjunto, Aragón dispone de un **ecosistema diversificado y complementario**, que combina talento, innovación tecnológica, proveedores especializados y estructuras de colaboración sectorial. La adecuada interacción entre estos actores y el sector de la maquinaria constituye un factor clave para impulsar la digitalización segura, la protección de activos críticos y la competitividad del tejido industrial regional.

5. Oportunidades de financiación y apoyo a la ciberseguridad industrial

La ciberseguridad se ha consolidado como una prioridad estratégica tanto en las políticas europeas de digitalización como en las agendas nacionales y autonómicas de innovación. Las empresas industriales aragonesas disponen actualmente de un conjunto de programas y convocatorias que facilitan la incorporación de medidas de protección digital, el desarrollo de soluciones tecnológicas seguras y la mejora de las competencias en este ámbito.

Estas oportunidades de apoyo económico y técnico constituyen un elemento clave para acelerar la madurez digital del sector, reducir las brechas de seguridad existentes y fomentar la colaboración entre industria, centros tecnológicos y administraciones públicas.

5.1. Principales programas y líneas de ayuda disponibles

Las principales fuentes de financiación para actuaciones en ciberseguridad industrial se articulan a través de programas de ámbito **europeo**, **nacional** y **autonómico**, que combinan subvenciones, préstamos blandos, asesoramiento técnico y servicios de innovación.

5.1.1. Programas europeos

Horizon Europe – Cluster 3 "Civil Security for Society"

Dentro del programa marco Horizon Europe, el Cluster 3 dedica una *destination* específica a la ciberseguridad, con el propósito de reforzar la soberanía digital, la autonomía estratégica y la resiliencia tecnológica de la Unión Europea.

El programa impulsa la investigación aplicada y la innovación orientada a proteger infraestructuras críticas, fortalecer las capacidades de prevención y respuesta ante ciberataques, y consolidar la comunidad europea de competencias en ciberseguridad en coordinación con el European Cybersecurity Competence Centre (ECCC).

El **Programa de Trabajo 2025–2027**, vigente en la fecha de redacción del presente informe, presta especial atención a las **pymes industriales**, fomentando la seguridad y la privacidad desde el diseño en tecnologías emergentes y sistemas conectados.

Para 2025, el presupuesto total asciende a 90,55 millones de euros, con seis convocatorias abiertas hasta el 12 de noviembre de 2025:

- HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications (RIA, 40 millones de euros)
- HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity (IA, 13,55 millones de euros)
- HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies (RIA, 11 millones de euros)
- HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives (RIA, 4 millones de euros)
- HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms (RIA, 6 millones de euros)
- HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols (RIA, 6 millones de euros)

Estas convocatorias ofrecen una oportunidad directa para empresas industriales aragonesas que deseen participar en consorcios europeos junto con centros tecnológicos, universidades y proveedores tecnológicos especializados.

Programa Digital Europe (DIGITAL)

El programa Digital Europe, actualmente en ejecución, apoya la transformación digital del tejido económico europeo y refuerza la capacidad de respuesta frente a ciberincidentes.

Hasta 2027, destina 45,6 millones de euros a actuaciones centradas en:

- La creación de una reserva de ciberseguridad de la UE, para dar soporte operativo ante incidentes de gran escala.
- El desarrollo de una plataforma única de notificación de vulnerabilidades bajo el Cyber Resilience Act, gestionada por ENISA.
- El funcionamiento del Centro Europeo de Situación y Análisis en Ciberseguridad, encargado de coordinar la respuesta y el análisis ante amenazas.

El lanzamiento de las nuevas acciones se realizó durante el segundo trimestre de 2025, con cierre en el cuarto trimestre de 2025, ofreciendo oportunidades para consorcios industriales, hubs de innovación y centros tecnológicos con actividad en digitalización segura.

European Defence Fund (EDF)

El Fondo Europeo de Defensa (EDF) financia proyectos orientados al desarrollo de capacidades tecnológicas en defensa, incluyendo la ciberseguridad aplicada a sistemas y operaciones críticas.

En 2025 cuenta con un presupuesto de 54 millones de euros, distribuido en dos convocatorias actualmente abiertas (hasta el 16 de octubre de 2025):

- EDF-2025-LS-RA-SI-CYBER-3RAV-STEP: Risk, robustness and resilience for autonomous vehicles in military operations. Generating knowledge, integrating knowledge, studies, and design (20 millones de euros).
- EDF-2025-DA-CYBER-CDOC-STEP: Improved cyber defence operations capabilities. Integrating knowledge, studies, design, and system prototyping, not excluding upstream and downstream activities eligible for development actions (34 millones de euros).

5.1.2. Programas nacionales

Ministerio de Industria y Turismo – Ayudas IDI y ACTIVA Financiación

Las Ayudas IDI (Investigación, Desarrollo e Innovación) y ACTIVA Financiación se enmarcan dentro del Plan de Recuperación, Transformación y Resiliencia, y están diseñadas para apoyar la digitalización y la innovación tecnológica en la industria manufacturera. Ambas líneas de financiación buscan impulsar la transición hacia la Industria 4.0, facilitando la adopción de nuevas tecnologías y la mejora de procesos industriales. Es importante destacar que el Ministerio de Industria y Turismo está trabajando en la nueva Orden de Bases que unificará estas dos líneas de ayuda. La unificación responde a la necesidad de simplificar el acceso a la financiación pública para proyectos industriales, reduciendo las barreras administrativas y potenciando el impacto de las inversiones en la transformación tecnológica de la industria manufacturera.

Ministerio de Industria y Turismo – Programa Activa Ciberseguridad

Programa del Ministerio de Industria y Turismo, en colaboración con INCIBE, que ofrece a las pymes industriales un diagnóstico gratuito de ciberseguridad y un plan de mejora personalizado elaborado por consultoras acreditadas. Su objetivo es evaluar el nivel de madurez digital y de seguridad de las empresas, identificar vulnerabilidades y proponer medidas concretas para reforzar la protección de sistemas IT y OT.

CDTI (Centro para el Desarrollo Tecnológico y la Innovación)

Ofrece financiación para proyectos de I+D en tecnologías de seguridad digital a través de líneas como Proyectos de I+D+i, NEOTEC o Proyectos de Cooperación Tecnológica Internacional (Eureka, Eurostars).

INCIBE (Instituto Nacional de Ciberseguridad)

Canaliza programas específicos para empresas y pymes industriales, como los Bonos de Ciberseguridad, los programas INCIBE Emprende (apoyo a startups del sector) y las Ayudas para la certificación en ENS o ISO 27001.

Red.es – Programa Kit Digital

El Programa Kit Digital, impulsado por el Gobierno de España a través de Red.es, tiene como objetivo subvencionar la adopción de soluciones de digitalización por parte de pymes, microempresas y autónomos, mediante los bonos digitales gestionados a través de los Agentes Digitalizadores. El programa facilita el avance en áreas clave como la presencia en internet, comercio electrónico, gestión de clientes y proveedores, automatización de procesos, oficina virtual y ciberseguridad, contribuyendo al incremento de la madurez digital de las empresas beneficiarias.

Red.es – Programa Kit Consulting

El Kit Consulting es un programa de ayudas del Gobierno de España para pymes de entre 10 y 250 empleados que busca facilitarles el asesoramiento especializado en transformación digital. Su objetivo es ayudar a las empresas a desarrollar una hoja de ruta para la digitalización, abarcando áreas como la inteligencia artificial, ciberseguridad o análisis de datos. La cantidad de la ayuda varía según el tamaño de la empresa, con bonos de 12.000 €, 18.000 € o 24.000 €.

ENISA – Línea Crecimiento

Esta línea forma parte del conjunto de instrumentos financieros del Ministerio de Industria y Turismo para fortalecer el tejido innovador y mejorar la competitividad empresarial. La Línea ENISA Crecimiento ofrece préstamos participativos a pymes y empresas medianas innovadoras que buscan consolidar su proyecto o acometer una expansión empresarial basada en la innovación tecnológica o digital. Financia inversiones destinadas a incrementar la capacidad productiva, diversificar la oferta, digitalizar procesos o impulsar la internacionalización, con importes de entre 25.000 y 1,5 millones de euros.

5.1.3. Programas autonómicos y regionales

Línea TDI-FEDER 2026 – Programa PAIP

La Línea TDI-FEDER (Transformación Digital e Innovación) forma parte del Programa PAIP (Programa de Ayudas a la Industria y la PYME de Aragón), gestionado por el Gobierno de Aragón a través del Departamento de Industria, Competitividad y Desarrollo Empresarial. Esta línea, actualmente en vigor, apoya proyectos de transformación digital, innovación tecnológica y sostenibilidad industrial en empresas aragonesas, priorizando aquellas que integren tecnologías habilitadoras digitales, soluciones de ciberseguridad o automatización de procesos. La financiación se articula mediante subvenciones cofinanciadas con fondos FEDER, orientadas a impulsar la modernización de las pymes industriales y su adaptación al marco de la Industria 4.0.

Instituto Aragonés de Fomento (IAF) - Ayudas a la digitalización de pymes aragonesas

El IAF tiene prevista para 2026 una nueva convocatoria de ayudas dirigidas a pequeñas y medianas empresas que impulsen actuaciones de digitalización, automatización y adopción de tecnologías avanzadas. Estas ayudas buscan reforzar la competitividad del tejido empresarial aragonés mediante la incorporación de soluciones de inteligencia artificial, análisis de datos, sensorización, conectividad segura y ciberseguridad industrial. El programa se enmarca en la estrategia regional de Transformación Digital de Aragón, complementando las líneas PAIP y los fondos europeos del Mecanismo de Recuperación y Resiliencia.

Línea de ayudas del Fondo de Transición Justa (FTJ) – Provincia de Teruel

El Fondo de Transición Justa (FTJ) tiene como objetivo mitigar los impactos socioeconómicos derivados del cierre de actividades intensivas en carbono, promoviendo la diversificación económica y la creación de empleo sostenible en las zonas afectadas. En Aragón, está prevista para el primer trimestre de 2026 una nueva convocatoria de ayudas dirigidas a pymes radicadas en la provincia de Teruel, centradas en proyectos de innovación, digitalización y eficiencia energética. Estas ayudas permitirán financiar inversiones productivas, incorporación de tecnologías digitales y proyectos de modernización industrial, con especial atención a iniciativas de ciberseguridad y resiliencia tecnológica.

5.2. Recomendaciones para su aprovechamiento por parte de las empresas

A pesar de la disponibilidad creciente de programas de apoyo, muchas pymes industriales no logran acceder de forma eficaz a las oportunidades de financiación

existentes, debido a la complejidad administrativa o la falta de recursos internos. Para mejorar su aprovechamiento, se plantean las siguientes recomendaciones:

1. Integrar la ciberseguridad en la estrategia de innovación empresarial, de modo que las inversiones en seguridad digital sean parte del plan global de transformación tecnológica.
2. Monitorizar activamente las convocatorias de organismos como INCIBE, CDTI, Red.es, Gobierno de Aragón y DIH Aragón, manteniendo contacto con entidades colaboradoras (clústeres, cámaras, centros tecnológicos).
3. Aprovechar los servicios de acompañamiento y diagnóstico ofrecidos por programas como *Activa Ciberseguridad* o *Acelera Pyme*, que facilitan el acceso a ayudas posteriores más avanzadas.
4. Participar en proyectos colaborativos junto con centros tecnológicos y universidades, lo que aumenta la puntuación y el impacto en convocatorias competitivas.
5. Priorizar la certificación en normas y estándares reconocidos (ISO 27001, ENS, IEC 62443), que mejoran la ciberresiliencia y son valoradas positivamente en programas de financiación pública.
6. Destinar recursos a la formación del personal técnico y directivo en materia de ciberseguridad industrial, utilizando las ayudas formativas disponibles en Aragón (EOI, USJ, Universidad de Zaragoza, INAEM).
7. Explorar líneas complementarias de apoyo financiero, como los préstamos de ENISA o los incentivos fiscales a la I+D+i, para cubrir costes no subvencionables directamente por convocatorias de ayudas.

En conjunto, estas medidas permitirán a las empresas industriales aragonesas aprovechar de manera más eficaz los fondos públicos, incrementar su nivel de madurez digital y fortalecer su competitividad y resiliencia frente a ciberamenazas.

6. Conclusiones

6.1. Grado de preparación del tejido industrial aragonés

El tejido industrial aragonés presenta un **nivel de madurez digital medio-avanzado**, fruto de un proceso progresivo de modernización impulsado por la adopción de tecnologías de automatización, sensórica y gestión de procesos. Sin embargo, la **ciberseguridad aún se encuentra en una fase de desarrollo desigual** entre las empresas, especialmente entre las pymes, que representan la mayoría del sector.

Las empresas más consolidadas han iniciado estrategias de protección de sus sistemas productivos, pero en muchos casos estas medidas se centran en el ámbito corporativo (IT) y no abarcan plenamente los entornos industriales (OT). Esta brecha evidencia la necesidad de **reforzar la cultura de la ciberseguridad industrial**, incorporando la protección digital como parte esencial de la gestión de riesgos empresariales.

Aun así, la elevada conciencia sobre la importancia del tema y la creciente disponibilidad de programas de apoyo —tanto públicos como privados— indican un **entorno favorable para avanzar hacia una mayor resiliencia digital**.

6.2. Potencial de colaboración y crecimiento en el ámbito de la ciberseguridad

Aragón dispone de **capacidades científicas, tecnológicas y empresariales consolidadas** que pueden potenciar su papel como referente en ciberseguridad industrial. Centros tecnológicos, universidades y empresas especializadas ya ofrecen servicios avanzados en diagnóstico, auditoría y desarrollo de soluciones de seguridad, lo que sienta las bases para un **ecosistema de innovación colaborativo**.

La interrelación entre el sector de la maquinaria —representado por asociaciones como ANMOPYC y CAMPAG— y las entidades tecnológicas de la región puede generar **sinergias estratégicas**, orientadas a la transferencia de conocimiento, el desarrollo de productos seguros desde el diseño (“security by design”) y la creación de cadenas de suministro más robustas.

Asimismo, los programas europeos (Horizon Europe, Digital Europe, EDF), nacionales (IDI, Activa Financiación, Activa Ciberseguridad, ENISA) y regionales (TDI-FEDER, PAIP, IAF) configuran un **marco de apoyo sólido para el crecimiento de la ciberseguridad aplicada al entorno industrial**, facilitando la inversión en innovación, capacitación y digitalización avanzada.

6.3. Próximos pasos y continuidad de iniciativas

El proyecto *securizAR* ha contribuido a **visibilizar el estado de la ciberseguridad industrial en Aragón** y a establecer una base de conocimiento sobre la que construir futuras actuaciones. A partir de los resultados obtenidos, se identifican varias líneas de acción prioritarias:

- **Consolidar un observatorio regional de ciberseguridad industrial**, que permita mantener actualizado el diagnóstico del sector y detectar tendencias emergentes.
- **Impulsar programas de capacitación y sensibilización** adaptados a las pymes, orientados tanto a personal técnico como a perfiles directivos.
- **Fomentar proyectos piloto y demostradores tecnológicos**, en colaboración con centros tecnológicos y proveedores locales, que muestren el impacto real de las soluciones de ciberseguridad en entornos industriales.
- **Aprovechar las sinergias con programas públicos de financiación**, para facilitar la ejecución de proyectos de innovación y digitalización segura.
- **Promover la cooperación intersectorial y la transferencia de conocimiento**, consolidando la relación entre los sectores industriales tradicionales y el ecosistema TIC aragonés.

Estas líneas de trabajo permitirán dar continuidad al esfuerzo iniciado con *securizAR*, consolidando una **estrategia regional de ciberseguridad industrial** que refuerce la competitividad, sostenibilidad y resiliencia del tejido productivo aragonés frente a los desafíos digitales actuales y futuros.

7. Cuestionario

A.1. Preguntas de carácter demográfico sobre la empresa

Datos generales de la empresa y contacto del encuestado

- Nombre de la empresa: *Campo libre*
- Nombre y apellidos del encuestado (opcional): *Campo libre*
- Cargo o función desempeñada en la empresa (opcional): C*ampo libre*

Preguntas sobre la trayectoria y estructura de la empresa

1. ¿Cuánto tiempo lleva su empresa operando en el sector industrial?
   - Menos de 5 años
   - Entre 5 y 10 años
   - Entre 10 y 20 años
   - Más de 20 años
2. Aproximadamente, ¿cuál es el tamaño de su empresa en número de empleados?
   - Micropyme (menos de 10 empleados)
   - Pequeña empresa (10 a 50 empleados)
   - Mediana empresa (50 a 250 empleados)
   - Gran empresa (más de 250 empleados)
3. ¿Cuál es el sector industrial principal en el que opera su empresa?
   - Fabricación de maquinaria para las industrias extractivas y de la construcción.
   - Fabricación de maquinaria agraria y forestal.
   - Otro (especificar)
4. ¿Cuál es el código de actividad económica principal de su empresa (CNAE-2009)? Campo libre
5. ¿Qué alcance geográfico tienen sus operaciones?
   - Local (una única ubicación)
   - Regional (varias ubicaciones dentro de la misma región)
   - Nacional

- Internacional

6. ¿Cuál es la forma de propiedad de su empresa?
    - Privada
    - Pública
    - Familiar
    - Mixta (pública y privada)
    - Otro (especificar)
7. Indique el rango aproximado de facturación anual de su empresa:
    - Menos de 1 millón de €
    - 1 a 10 millones de €
    - 10 a 50 millones de €
    - 50 a 100 millones de €
    - Más de 100 millones de €

Preguntas sobre capacidad de mantenimiento y gestión de información

8. ¿Cuenta su empresa con personal capacitado para mantener los equipos y máquinas industriales?
    - Sí, disponemos de personal propio y, cuando es necesario, asistencia puntual (remota o presencial).
    - No, el mantenimiento lo realiza directamente el fabricante (remota o presencial).
    - No, usamos personal externo de integradores especialistas en automatización (remota o presencial).
    - No, contamos con fabricantes o integradores especialistas, pero solo con asistencia presencial.
9. ¿Permite su empresa que proveedores o prestadores de servicios accedan de forma remota a sus sistemas para asistencia o resolución de incidencias?
    - Sí
    - No
    - No lo sé

10. En relación con la gestión de la información de su empresa, ¿dónde se almacena principalmente?
    - Toda la información se gestiona en nuestros propios equipos.
    - Parte de la información se gestiona internamente y otra parte en equipos de proveedores.
    - Toda la información se gestiona en equipos de proveedores.

A.2. Preguntas generales sobre ciberseguridad

11. Desde su experiencia profesional, ¿cuáles cree que serían los factores que podrían mejorar la ciberseguridad de los procesos industriales? (selección múltiple)
    - Acceso a entornos o proyectos con requisitos de ciberseguridad basados en estándares reconocidos.
    - Disponibilidad de tecnología de ciberseguridad específica para la industria.
    - Acceso a proveedores especializados en ciberseguridad industrial.
    - Que los proveedores cuenten con personal altamente cualificado en ciberseguridad.
    - Que los profesionales de ciberseguridad de los proveedores estén certificados en el área.
    - Experiencia de los proveedores en el cumplimiento de normas y estándares de seguridad.
    - Otro (especificar).
12. ¿Cuál considera que es la razón principal por la que la ciberseguridad es relevante en su empresa?
    - Cumplimiento de regulaciones y normativas de seguridad.
    - Haber sufrido previamente algún incidente con impacto notable.
    - Necesidad de proteger la digitalización de los procesos productivos.
    - No considera que la ciberseguridad sea relevante.
13. Aproximadamente, ¿qué porcentaje de su facturación anual se destina a actividades relacionadas con la ciberseguridad?
    - Menos del 1 %
    - Entre 1 % y 3 %

- Entre 3 % y 5 %
- Entre 5 % y 10 %
- Más del 10 %

14. ¿Qué tipo de información crítica maneja su empresa y qué medidas de protección aplica frente a posibles ciberamenazas? (selección múltiple)
    - Propiedad intelectual
    - Datos de clientes
    - Información financiera
    - Datos de producción
    - Otros (especificar)
15. ¿Qué estándares de ciberseguridad aplicables a entornos industriales ha implementado o considerado implementar en su empresa? (selección múltiple)
    - NIST SP 800-82
    - ISO 27001 / IEC 62443
    - ISA/IEC 62443
    - ANSI/ISA-99
    - Ninguno
    - Otros (especificar)
16. ¿Cómo evalúa su empresa el impacto y la eficacia de la implementación de estándares de seguridad en sus sistemas industriales? (selección múltiple)
    - Mediante auditorías internas periódicas
    - Con métricas de seguridad específicas
    - Basándose en evaluaciones externas o certificaciones
    - Monitoreando incidentes y la respuesta ante ellos
    - No se realiza ninguna evaluación formal
    - Otros (especificar)

A.3. Preguntas sobre personal de ciberseguridad

17. ¿Cómo se integra la ciberseguridad en la estructura organizativa de su empresa?

- Existe un CISO o posición equivalente dentro de la alta dirección.
- La responsabilidad se combina con otro rol ejecutivo (por ejemplo, CIO o CTO).
- Se gestiona a nivel departamental, sin un rol específico de ciberseguridad en la dirección.
- Se externaliza a un consultor o servicio especializado.
- No hay una posición dedicada exclusivamente a ciberseguridad.
- Se encuentra en proceso de incorporar un rol directivo de ciberseguridad.
- Otro (especificar).

18. ¿Cuenta su empresa con personal dedicado específicamente a la ciberseguridad industrial?
    - Sí, disponemos de un equipo a tiempo completo.
    - Sí, pero con dedicación parcial (asignación de roles adicionales).
    - Sí, pero el servicio está externalizado mediante un proveedor externo.
    - No, pero estamos considerando contratar personal dedicado próximamente.
    - No, actualmente no disponemos de personal especializado.
19. En caso afirmativo, ¿cuántos profesionales de ciberseguridad conforman su equipo? (opcional)
    - 1 a 3 profesionales
    - 4 a 6 profesionales
    - 7 a 10 profesionales
    - Más de 10 profesionales
20. Al contratar personal para ciberseguridad industrial, ¿qué competencias o certificaciones busca su empresa? (selección múltiple)
    - Experiencia en sistemas de control industrial (SCI).
    - Conocimientos en análisis de riesgos.
    - Experiencia en respuesta a incidentes cibernéticos.
    - Otras (especificar).
21. ¿Se proporciona formación continua al personal de ciberseguridad para mantenerse al día con nuevas amenazas y tecnologías? (selección múltiple)

- Programas de formación regulares.
- Participación en conferencias y eventos especializados.
- Acceso a cursos en línea y certificaciones actualizadas.
- Sesiones de actualización sobre amenazas emergentes.
- Colaboración con expertos externos para formación práctica.
- No se ofrece formación continua actualmente.

22. ¿Cómo gestiona la empresa la rotación de personal en el área de ciberseguridad para garantizar la continuidad del conocimiento? (selección múltiple)
    - Planes de sucesión definidos.
    - Documentación detallada de procedimientos y procesos críticos.
    - Capacitación cruzada entre los miembros del equipo.
    - Otros (especificar).
23. ¿Existe una colaboración estrecha entre el equipo de ciberseguridad y otros departamentos de la empresa?
    - Sí
    - No
    - No lo sé

A.4. Preguntas sobre gestión y almacenamiento de la información de los procesos industriales

24. ¿Cómo gestiona su empresa la información generada por sus procesos industriales?
    - Sistemas de gestión de datos específicos para la industria.
    - Sistemas desarrollados internamente por la empresa.
    - Otros (especificar).
25. ¿Cumple su empresa con normativas o estándares específicos relacionados con la gestión y almacenamiento de la información de procesos industriales?
    - Sí, cumplimos con normativas sectoriales específicas.
    - Sí, cumplimos con regulaciones gubernamentales.
    - Sí, implementamos estándares reconocidos de seguridad.
    - No seguimos ninguna normativa específica.

- Otro (especificar).

26. ¿Dónde almacena la información generada por los procesos industriales?
    - Servidores locales dentro de la empresa.
    - Servicios de almacenamiento en la nube.
    - Otros (especificar).
27. ¿Qué medidas de seguridad implementa para proteger la información almacenada? (selección múltiple)
    - Cifrado de datos.
    - Control de acceso basado en roles.
    - Auditorías de acceso.
    - Monitoreo continuo de la integridad de los datos.
    - No se aplican medidas actualmente.
    - Otros (especificar).
28. ¿Dispone su empresa de políticas de retención de datos de los procesos industriales?
    - Sí, políticas claras y documentadas.
    - Políticas informales.
    - No existen políticas de retención.
29. En caso afirmativo, ¿cuál es la duración típica de retención de los datos? (opcional)
    - Campo libre.
30. ¿Cómo se controla el acceso a la información de los procesos industriales dentro de la organización?
    - Acceso basado en necesidad.
    - Autenticación multifactor.
    - Supervisión en tiempo real de los accesos.
31. ¿Qué medidas aplica para prevenir accesos no autorizados? (selección múltiple)
    - Autenticación multifactor.
    - Políticas estrictas de acceso basadas en roles.

- Cifrado robusto, tanto en reposo como en tránsito.
- Monitoreo continuo.
- Actualización y parches de seguridad constantes.
- Restricción física y vigilancia de las áreas críticas.
- Auditorías periódicas de seguridad.
- Otros (especificar).

32. ¿Realiza copias de seguridad periódicas de la información de sus procesos industriales?
    - Sí, de manera regular.
    - Ocasionalmente.
    - No se realizan copias de seguridad.
33. En caso afirmativo, ¿dónde se almacenan estas copias de seguridad? (selección múltiple; opcional)
    - Servidores internos dedicados.
    - Servicios en la nube de proveedores confiables.
    - Combinación de discos y cintas magnéticas.
    - Dispositivos externos guardados fuera de la ubicación principal.
    - Sistemas de almacenamiento en red (NAS).
    - Copias distribuidas en varios medios (disco, cinta, nube).
    - Proveedores externos gestionando las copias de seguridad.
    - Sala de servidores segura con control físico.
    - Sistemas de almacenamiento replicado (RAID).
    - Centros de datos externos o gestionados por terceros.
    - Otros (especificar).
34. En caso afirmativo, ¿cómo garantiza la integridad de las copias de seguridad? (selección múltiple; opcional)
    - Uso de mecanismos matemáticos como hashes criptográficos.
    - Controles de acceso estrictos.

- Cifrado robusto de la información.
- Pruebas periódicas de recuperación para verificar consistencia.
- Otros (especificar).

35. En caso afirmativo, ¿cómo asegura la disponibilidad de la información respaldada? (selección múltiple; opcional)
    - Almacenamiento en ubicaciones geográficas distintas.
    - Pruebas periódicas de recuperación de datos.
    - Registro detallado de copias realizadas (contenido, fecha, ubicación).
    - Políticas de retención claras y cumplimiento de requerimientos legales y empresariales.
    - Otros (especificar).
36. ¿Están integrados los sistemas de gestión de datos de los procesos industriales con otros sistemas empresariales?
    - Sí, completamente integrados.
    - Parcialmente integrados.
    - No están integrados.
37. ¿Cómo se gestionan actualizaciones y mantenimiento de los sistemas para garantizar su seguridad y eficacia? (selección múltiple)
    - Programa regular de actualizaciones.
    - Evaluación de impacto antes de aplicar cambios.
    - Pruebas exhaustivas en entornos de desarrollo.
    - No se gestionan actualizaciones ni mantenimiento.
    - Otros (especificar).
38. ¿Cómo se registra y documenta el historial de cambios en la información de los procesos industriales? (selección múltiple)
    - Registro automatizado de cambios.
    - Seguimiento manual de modificaciones.
    - Auditorías periódicas de cambios.
    - No se documentan los cambios.

- Otros (especificar).

39. ¿Qué medidas se aplican para asegurar la transferencia segura de datos entre sistemas y ubicaciones? (selección múltiple)
    - Protocolos de cifrado.
    - Uso de redes privadas virtuales (VPN).
    - Validación de destinatarios autorizados.
    - No se aplican medidas actualmente.
    - Otros (especificar).
40. ¿Se implementan medidas para prevenir pérdida o corrupción de datos? (selección múltiple)
    - Sistemas de respaldo redundantes.
    - Monitoreo continuo de integridad.
    - Políticas de prevención de pérdida de datos (DLP).
    - No se implementan medidas actualmente.
    - Otros (especificar).
41. ¿Se ofrece formación regular al personal sobre gestión y almacenamiento seguro de datos de procesos industriales?
    - Sí, de manera regular.
    - Ocasionalmente.
    - Solo durante la incorporación.
    - Actualmente no se proporciona formación.

A.5. Preguntas sobre evaluación y gestión de incidentes de ciberseguridad

42. ¿Quién se encarga de gestionar los riesgos de ciberseguridad en los procesos industriales automatizados de su organización?
    - Personal propio con asistencia puntual de especialistas externos en ciberseguridad.
    - Integradores responsables de la automatización de procesos industriales.
    - Fabricantes de tecnología de automatización industrial.
    - Proveedor especializado en ciberseguridad.

- Actualmente no se gestionan los riesgos de ciberseguridad en los procesos automatizados.
- Otro (especificar).

43. ¿Realiza su empresa auditorías de ciberseguridad internas o contrata servicios externos para evaluar su postura de seguridad?
    - Auditorías internas regulares.
    - Servicios externos especializados.
    - Ambas, auditorías internas y externas.
    - Actualmente no se realizan auditorías.
44. ¿Cómo se evalúa la eficacia de las medidas de seguridad implementadas por el equipo de ciberseguridad? (selección múltiple)
    - Auditorías internas periódicas.
    - Simulacros de incidentes y pruebas de respuesta.
    - Métricas de rendimiento y cumplimiento establecidas.
    - Encuestas de percepción y satisfacción del personal.
    - Evaluación de incidentes previos y medidas correctivas aplicadas.
    - No se realiza ninguna evaluación formal.
    - Otros (especificar).
45. ¿Con qué frecuencia se llevan a cabo evaluaciones de ciberseguridad en su infraestructura industrial?
    - Anualmente.
    - Semestralmente.
    - Trimestralmente.
    - Mensualmente.
    - Nunca.
46. ¿Qué medidas de seguridad se implementan para proteger los sistemas de control industrial? (selección múltiple)
    - Firewalls industriales.
    - Sistemas de detección de intrusiones.

- Segmentación de redes.
- Control de acceso estricto.
- Monitorización continua.
- No se implementa ninguna medida actualmente.
- Otros (especificar).

47. ¿Ha sufrido su empresa incidentes de ciberseguridad?
    - Sí.
    - No.
    - No lo sé.
48. En caso afirmativo, ¿cómo se gestionaron estos incidentes? (selección múltiple; opcional)
    - Respuesta inmediata y mitigación.
    - Investigación forense.
    - Notificación a autoridades competentes.
    - Implementación de mejoras en las medidas de seguridad.
49. Comentarios adicionales sobre la gestión de incidentes anteriores (opcional)
    - Campo libre.
50. ¿Cuál es la política de acceso a sistemas industriales desde redes externas? (selección múltiple)
    - Acceso restringido.
    - Autenticación de dos factores.
    - Monitorización continua.
    - Acceso únicamente a personal autorizado.
    - Acceso abierto (sin restricciones implementadas).
    - Los sistemas industriales no son accesibles desde redes externas.
    - Otros (especificar).
51. ¿Cómo gestiona su empresa las actualizaciones de seguridad y parches en sistemas industriales? *(selección múltiple)*

- Programa regular de actualizaciones.
- Evaluación de impacto antes de aplicar cambios.
- Automatización de actualizaciones.
- Pruebas en entornos de desarrollo antes de implementarlas en producción.
- Actualmente no se gestionan actualizaciones ni parches.
- Otros (especificar).

52. ¿Existe un plan de respuesta a ciberincidentes? ¿Se ha probado?
    - Sí, establecido y probado.
    - Sí, establecido pero no probado.
    - En proceso de establecimiento.
    - No existe un plan.
53. ¿Cuenta con un sistema de gestión de incidentes que involucre a diferentes áreas de la empresa en caso de ciberamenaza?
    - Sí, sistema interdepartamental implementado.
    - No, actualmente no existe.
    - En proceso de implementación.
54. ¿Participa su empresa en colaboración con organismos externos o comunidades de intercambio de información sobre ciberamenazas?
    - Sí, colaboración activa.
    - Participación en comunidades de ciberseguridad.
    - No actualmente, pero se está considerando.
    - No participa.
55. En caso afirmativo, ¿con qué organismos o comunidades colabora? (opcional)
    - Campo libre.
56. ¿Cuáles considera que son los principales desafíos en ciberseguridad industrial? *(selección múltiple)*
    - Falta de concienciación del personal.
    - Escasez de habilidades en ciberseguridad.

- Dificultad para equilibrar operatividad y seguridad.
- Complejidad de la infraestructura.
- Otros (especificar).

57. Comentarios adicionales sobre ciberseguridad industrial no contemplados en preguntas anteriores (opcional)
    - Campo libre.
58. ¿Dispone su empresa de un plan de Continuidad del Negocio y Recuperación ante Desastres específico para ciberincidentes?
    - Sí.
    - En desarrollo.
    - No.
59. En caso afirmativo, ¿con qué frecuencia se actualiza y revisa dicho plan?
    - Anualmente.
    - Semestralmente.
    - Trimestralmente.
    - Mensualmente.
    - Continuamente en tiempo real.
    - No aplicable / en desarrollo.
    - No existe plan.

A.6. Preguntas sobre ciberseguridad en la cadena de suministro

60. ¿Ha habido cambios recientes en la cadena de suministro de sus procesos industriales que hayan afectado la ciberseguridad de su empresa?
    - Sí
    - No
    - No estoy seguro
61. ¿Cómo evalúa su empresa la seguridad de la cadena de suministro frente a posibles amenazas cibernéticas?
    - Realizamos evaluaciones de forma periódica.
    - Colaboramos con terceros para realizar auditorías de seguridad.

- Actualmente no realizamos evaluaciones.

62. ¿Qué prácticas utiliza para verificar la ciberseguridad de sus proveedores dentro de la cadena de suministro? *(selección múltiple)*
    - Cuestionarios de seguridad.
    - Auditorías presenciales.
    - Evaluaciones de riesgos de ciberseguridad.
    - Monitoreo continuo de las actividades del proveedor.
    - No evaluamos la ciberseguridad de nuestros proveedores.
    - Otro (especificar).
63. ¿Incluye a proveedores clave de la cadena de suministro en su plan de contingencias?
    - Sí
    - No
    - No estoy seguro
64. ¿Incorpora a estos proveedores clave en su plan de Continuidad del Negocio y Recuperación ante Desastres?
    - Sí
    - No
    - No estoy seguro
65. ¿Cómo protege la información sensible durante su transferencia a lo largo de la cadena de suministro? *(selección múltiple)*
    - Cifrado de datos.
    - Políticas de acceso restringido.
    - Protección frente a ataques de intermediarios.
    - Actualmente no se implementan medidas de protección durante la transferencia.
    - Otro (especificar).
66. ¿Qué medidas adopta para garantizar la resiliencia de la cadena de suministro ante interrupciones derivadas de ciberincidentes? *(selección múltiple)*

- Planes de continuidad del negocio.
- Estrategias de recuperación rápida.
- Colaboración estrecha con proveedores para recuperación conjunta.
- No se aplican medidas actualmente.
- Otro (especificar).

67. ¿Proporciona formación en ciberseguridad a sus proveedores como parte de buenas prácticas en la cadena de suministro?
    - Sí, de forma regular.
    - Solo en ocasiones específicas.
    - Actualmente no proporcionamos formación.
68. ¿Cómo evalúa los riesgos de ciberseguridad en cada etapa de su cadena de suministro? *(selección múltiple)*
    - Análisis de riesgos periódicos.
    - Evaluación de vulnerabilidades.
    - Colaboración con expertos en seguridad.
    - No se evalúan riesgos en ninguna etapa.
    - Otro (especificar).
69. ¿Qué acciones implementa para protegerse frente a ciberataques dirigidos a sus proveedores que puedan afectar la cadena de suministro? *(selección múltiple)*
    - Acuerdos contractuales específicos sobre seguridad.
    - Evaluación de la postura de seguridad de los proveedores.
    - Colaboración en estrategias de respuesta a incidentes.
    - No se aplican medidas de protección contra ciberataques a proveedores.
    - Otro (especificar).
70. ¿Qué políticas tiene en vigor para que sus proveedores notifiquen incidentes de seguridad? *(selección múltiple)*
    - Procedimientos de notificación inmediata.
    - Colaboración en investigaciones de incidentes.
    - Sanciones por falta de notificación.

- Actualmente no existe ninguna política.
- Otro (especificar).

71. ¿Cómo fomenta la innovación segura en la cadena de suministro, especialmente durante el desarrollo de nuevos productos y tecnologías? *(selección múltiple)*
    - Evaluación de riesgos en las etapas de desarrollo.
    - Colaboración con proveedores para investigación segura.
    - Implementación de estándares de seguridad en el diseño.
    - Actualmente no se fomenta la innovación segura.
    - Otro (especificar).
72. ¿Participa en iniciativas conjuntas con otras empresas de la industria para mejorar la seguridad en la cadena de suministro? *(selección múltiple)*
    - Colaboración en estándares de seguridad.
    - Intercambio de información sobre amenazas.
    - Participación en grupos de trabajo de ciberseguridad.
    - No se participa en ninguna iniciativa de colaboración.
    - Otro (especificar).

A.7. Preguntas sobre capacitación y concienciación en ciberseguridad industrial

73. ¿Cómo calificaría el nivel de conciencia y preocupación de la alta dirección respecto a los riesgos de ciberseguridad industrial en su empresa?
    - Muy alto
    - Alto
    - Moderado
    - Bajo
    - Muy bajo
74. ¿De qué manera identifica su empresa las necesidades de capacitación del personal en ciberseguridad industrial? *(selección múltiple)*
    - Encuestas periódicas.
    - Evaluación de las habilidades actuales.
    - Análisis de incidentes de seguridad previos.

- Evaluación de riesgos de seguridad.
- Actualmente no identificamos necesidades de capacitación.
- Otro (especificar).

75. ¿Su empresa ofrece programas formales de capacitación en ciberseguridad industrial para su personal?
    - Sí, de forma regular.
    - Ocasionalmente.
    - Solo durante la incorporación.
    - No, nunca.
76. ¿Qué contenidos específicos incluye su programa de capacitación en ciberseguridad industrial? *(selección múltiple)*
    - Concienciación sobre amenazas actuales.
    - Buenas prácticas de seguridad.
    - Prevención de phishing.
    - Uso seguro de dispositivos y redes.
    - Ninguno, no existe programa de capacitación.
    - Otro (especificar).
77. ¿Qué acciones toma para garantizar que todo el personal sea consciente y participe activamente en ciberseguridad industrial? *(selección múltiple)*
    - Sesiones regulares de formación y concienciación.
    - Pruebas internas de phishing.
    - Comunicaciones periódicas sobre amenazas cibernéticas.
    - Programas de incentivos por reportes de seguridad.
    - Implementación de políticas claras de seguridad.
    - Actualmente no se toman medidas.
    - Otro (especificar).
78. ¿Cómo evalúa su empresa la efectividad de los programas de capacitación en ciberseguridad industrial? *(selección múltiple)*
    - Evaluaciones al finalizar la capacitación.

- Pruebas de simulación de phishing.
- Análisis comparativo de incidentes antes y después de la capacitación.
- Seguimiento de comportamientos seguros del personal.
- Actualmente no se evalúa la efectividad.
- Otro (especificar).

79. ¿Proporciona formación continua a su personal de ciberseguridad industrial para mantenerse actualizado frente a nuevas amenazas y tecnologías?
    - Sí, de forma regular.
    - En ocasiones específicas.
    - Actualmente no proporcionamos formación continua.
80. ¿Qué medidas adopta para fomentar la participación activa del personal en los programas de capacitación? *(selección múltiple)*
    - Reconocimientos y premios.
    - Competencias y desafíos internos.
    - Incentivos económicos.
    - Actualmente no se fomenta la participación activa.
    - Otro (especificar).
81. ¿La capacitación se adapta a los roles y responsabilidades de cada empleado?
    - Sí, personalizada según departamento o función.
    - Se proporciona una capacitación general para todos.
    - No se adapta la capacitación según roles.
    - No se realiza ninguna capacitación.
    - No estoy seguro.
    - Otro (especificar).
82. ¿Su empresa implementa medidas posteriores a la capacitación para reforzar los conceptos aprendidos? *(selección múltiple)*
    - Sesiones de repaso periódicas.
    - Evaluaciones de conocimientos recurrentes.

- Simulacros de incidentes.
- Actualmente no se aplican medidas posteriores.
- Otro (especificar).

83. ¿Ofrece su empresa recursos de autocapacitación en línea u otros materiales para que los empleados aprendan de manera autónoma?
    - Sí, una amplia variedad de recursos.
    - Sí, algunos recursos disponibles.
    - No se ofrecen recursos de autocapacitación.
84. ¿Colabora su empresa con expertos externos o instituciones educativas para ofrecer capacitación especializada en ciberseguridad industrial?
    - Sí, colaboración activa.
    - En ocasiones específicas.
    - No se colabora con expertos externos.
    - No se proporciona capacitación especializada.