

FOLLETO

LA APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA PREVENCIÓN DE RIESGOS LABORALES

Oportunidades y riesgos.



CON LA FINANCIACIÓN DE:

AI2024-0012



GOBIERNO
DE ESPAÑA

MINISTERIO
DE TRABAJO
Y ECONOMÍA SOCIAL



FUNDACIÓN
ESTATAL PARA
LA PREVENCIÓN
DE RIESGOS
LABORALES, F.S.P.



FOLLETO

LA APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA PREVENCIÓN DE RIESGOS LABORALES

Oportunidades y riesgos.

Edita y publica: Fundación Cultural 1º de Mayo -CCOO

Materiales elaborados por: Alicia Martínez Poza y Esther Madroñal Cano

Dirección y coordinación: Vicente López Martínez y Valeria Uberti-Bona

Difusión: Lourdes Larripa Ferriz

Gestión y apoyo administrativo: Sergio Alvira Fernández, Lara Criado Bonilla y Lola García Moreno

Agradecimientos:

Queremos agradecer la colaboración de las secretarías confederales de Salud Laboral y Medio Ambiente y de Acción Sindical y Transiciones Estratégicas de CCOO, así como de las Federaciones de Industria, Servicios, Servicios a la Ciudadanía y del Habitat de CCOO. Agradecer igualmente las contribuciones de los delegados y delegadas que participaron en los workshops y a todas las personas que han nutrido, con su conocimiento experto y sus experiencias, las distintas fases del proyecto.

Diseño gráfico y maquetación: Pilixip

Edición: Valencia, marzo 2026

Este folleto se realiza en la convocatoria ordinaria intersectorial de la Fundación Estatal para la Prevención de Riesgos Laborales (proyecto AI2024-0012), 2024-2026.

ÍNDICE

1. LA DIGITALIZACIÓN AVANZADA: LA GESTIÓN ALGORÍTMICA Y LA IA COMO PALANCAS DE TRANSFORMACIÓN DEL MUNDO LABORAL	9
1.1. Definiciones y conceptos clave	11
1.2. El ecosistema tecnológico de la digitalización	13
1.3. La implantación de la gestión algorítmica y la inteligencia artificial	14
2. LA INTELIGENCIA ARTIFICIAL Y LOS SISTEMAS DIGITALES INTELIGENTES APLICADOS A LA PREVENCIÓN DE RIESGOS LABORALES	17
2.1. Usos de la inteligencia artificial y los sistemas digitales inteligentes para la prevención de riesgos laborales	18
2.2. Una tipología de usos de sistemas digitales inteligentes para la PRL	19
3. EL IMPACTO DE LA ADOPCIÓN DE IA Y SISTEMAS DIGITALES INTELIGENTES PARA LA PREVENCIÓN	24
3.1. Factores de riesgo tecnológicos	25
3.1.1. Interacción humano-máquina	25
3.1.2. Uso de pantallas de visualización de datos y tecnologías inmersivas	26
3.1.3. Automatización cognitiva y supervisión tecnológica	27
3.2. Factores de riesgo organizativos	29
3.2.1. Intensificación derivada de la monitorización preventiva inteligente	29
3.2.2. Reducción de autonomía del trabajador y mayor control algorítmico	30
3.2.3. Vigilancia digital continua	30
3.3. Factores de riesgo preventivos	33
3.3.1. Digitalización de la vigilancia preventiva	33
3.3.2. Individualización de la prevención	33
3.3.4. Desigualdad sectorial y precariedad	33
3.3.5. Desigualdades y sesgos en la prevención digital	34
3.3.6. Brecha de formación y capacitación preventiva digital	34
4. LA INCORPORACIÓN DE SISTEMAS INTELIGENTES PARA LA PRL	37
4.1. Gestión de la seguridad y salud en el trabajo: criterios a tener en cuenta	37
4.2. El papel estratégico de la RLPT de prevención ante la IA	43
5. REFERENCIAS	47



INTRODUCCIÓN

La detección de peligros mediante sistemas de visión artificial, los sensores capaces de anticipar fallos en la maquinaria o el uso de dispositivos inteligentes —como relojes o cascos que recopilan datos posturales o fisiológicos— son algunos ejemplos de la aplicación de la inteligencia artificial (*en adelante* IA) en la prevención de riesgos laborales (*en adelante* PRL). Estas tecnologías abren nuevas posibilidades para mejorar la seguridad y la salud en el trabajo. El uso de estas tecnologías en nuestra vida cotidiana implica inevitablemente reflexionar sobre su impacto medioambiental, dado su alto consumo de recursos energéticos, hídricos y minerales; pero también plantean interrogantes relevantes sobre su solidez técnica, su utilidad preventiva real y los posibles efectos secundarios sobre la salud y los derechos de las personas trabajadoras.

La introducción de sistemas de IA en los entornos laborales obliga a formular preguntas clave: ¿Hasta qué punto pueden asumir algunas funciones propias de los servicios de prevención? ¿Qué implicaciones tiene la recopilación masiva de datos personales, incluidos los de carácter sensible? ¿Qué límites éticos deben establecerse? ¿Y qué papel corresponde a la representación legal de las personas trabajadoras en su diseño, implantación y control?

La digitalización de las empresas comenzó a implantarse a partir de las décadas de 1970 y 1980, con la introducción de los primeros sistemas informáticos destinados a tareas administrativas y contables. En las décadas posteriores, la generalización del ordenador personal, el correo electrónico e Internet transformó los procesos productivos, impulsó la globalización y contribuyó a la reorganización del trabajo, modificando de manera profunda los perfiles profesionales y las competencias requeridas.

Desde hace algo más de una década se inicia una nueva fase de transformación caracterizada por el uso masivo de datos, la computación en la nube y los algoritmos en la toma de decisiones empresariales. En este contexto se consolidan modelos de negocio basados en plataformas digitales y se extienden los sistemas de gestión algorítmica, cuyos efectos comienzan a hacerse visibles en el control del desempeño, la transparencia de los procesos, los derechos laborales y la protección de datos personales.

En los últimos años, la incorporación de sistemas de decisión automatizada impulsados por la inteligencia artificial generativa, el aprendizaje automático y la automatización avanzada ha ampliado este proceso.

Las tecnologías digitales y la inteligencia artificial ofrecen oportunidades relevantes para mejorar la seguridad y salud en el trabajo. La *Organización Internacional del Trabajo* (*en adelante* OIT) señala que estas herramientas pueden contribuir a la detección temprana de peligros, al control de las condiciones ambientales, a la anticipación de fallos en equipos y a la automatización de tareas peligrosas, reduciendo así la exposición de las personas trabajadoras a situaciones de riesgo (OIT, 2025).

No obstante, la digitalización también introduce nuevos riesgos para la seguridad y la salud laboral. Entre ellos se encuentran los derivados de la interacción entre personas y sistemas automatizados, las sobrecargas físicas asociadas al uso de dispositivos, los riesgos visuales, la intensificación del trabajo, el tecnoestrés, las prácticas de vigilancia intrusiva o las vulneraciones de la privacidad y de la protección de datos personales. Tal y como advierte la *Agencia Europea para la Seguridad y la Salud en el Trabajo* (*en adelante* EU-OSHA), el impacto de estas tecnologías depende en gran medida de los equipos utilizados y, sobre todo, de la forma en que el trabajo se organiza y se gestiona: su éxito y seguridad dependen de

que se priorice el factor humano y se gestione bajo los principios de prevención y jerarquía de control (EU-OSHA, 2026).

Los impactos de la digitalización y de la inteligencia artificial no están predeterminados. Su alcance y su intensidad dependen de factores económicos, sociales e institucionales, pero también, de manera decisiva, de las estrategias, capacidades y poder de los actores sociales implicados. El grado de control humano, regulación y orientación de estas tecnologías es un elemento clave para maximizar sus beneficios y limitar sus riesgos.

En este sentido, el papel de la representación legal de las personas trabajadoras resulta fundamental. La OIT subraya que, para maximizar los beneficios de la transformación digital y mitigar sus riesgos, es esencial adoptar un enfoque proactivo, participativo y basado en la evidencia, apoyado en un diálogo social efectivo (OIT, 2025). La negociación colectiva se configura como una herramienta central para establecer garantías, asegurar la transparencia, reforzar el control humano y proteger los derechos fundamentales en el uso de sistemas de IA en las empresas.

En este contexto, el presente folleto tiene como objetivo analizar el uso de la inteligencia artificial en la PRL, prestando especial atención al papel de la negociación colectiva y de la representación legal de las personas trabajadoras. En particular, se examinan las implicaciones del uso de la IA en las estructuras organizativas de la prevención, el grado de participación sindical y los elementos clave para reforzar una acción preventiva eficaz en la empresa.

Desde el punto de vista metodológico, el folleto se ha elaborado a partir de un análisis bibliográfico y de la realización de tres talleres participativos, con la participación de entre 12 y 15 personas trabajadoras. Cada uno de los talleres agrupa a delegados y delegadas de un sector diferente: industria, servicios (banca) y construcción, con diferentes niveles de conocimiento de aplicación de herramientas y sistemas de digitalización avanzada en sus centros de trabajo.



1. LA DIGITALIZACIÓN AVANZADA: LA GESTIÓN ALGORÍTMICA Y LA IA COMO PALANCAS DE TRANSFORMACIÓN DEL MUNDO LABORAL

Para comprender el papel actual de la inteligencia artificial en la prevención de riesgos laborales resulta necesario situarla en el contexto más amplio de la digitalización y de la expansión de la gestión algorítmica. Los mismos sistemas digitales que hoy se utilizan para organizar, asignar y supervisar el trabajo —basados en datos, algoritmos y plataformas digitales— están comenzando a aplicarse también a la identificación de riesgos, la monitorización de las condiciones laborales y el apoyo a la toma de decisiones preventivas. Por ello, este apartado analiza la digitalización como el marco necesario para comprender su aplicación en la prevención de riesgos y analizar los efectos que en la salud laboral conlleva este mismo proceso de digitalización.

La gestión algorítmica se ha convertido en un elemento central en la organización del trabajo, especialmente en el ámbito de las plataformas digitales y en las grandes corporaciones. A través de sistemas algorítmicos, se asignan tareas, se evalúa el desempeño y se toman decisiones que anteriormente dependían explícitamente y casi exclusivamente de supervisores humanos. La inteligencia artificial, por su parte, siguiendo el diseño e instrucciones empresariales, actúa como un agente transformador adicional al asumir funciones cognitivas complejas, como el análisis predictivo, la toma de decisiones o la interacción automatizada con clientes.

La incorporación de sistemas algorítmicos automatizados y de inteligencia artificial en la dirección y gestión empresarial está modificando de manera sustancial el escenario laboral. Como ocurrió en anteriores revoluciones industriales, estas tecnologías permiten aumentar la productividad y el propio beneficio empresarial. Esto ha reactivado el debate sobre una posible destrucción masiva de empleo o hasta qué punto estas tecnologías aumentan los niveles de desigualdad en el reparto del ingreso. En este contexto, se han generado expectativas de enorme calado, tanto en el mundo laboral como en la sociedad en general, vaticinando la desaparición o precarización de numerosos puestos de trabajo o una sociedad con mayor concentración de riqueza.

La aplicación de sistemas de inteligencia artificial amplifica el alcance de la digitalización al automatizar procesos de decisión tradicionalmente humanos, desde la selección y evaluación de personal hasta la gestión del rendimiento o la asignación de tareas. Con frecuencia, estas tecnologías se presentan como herramientas capaces de tomar decisiones basadas exclusivamente en grandes volúmenes de datos objetivos, lo que, en teoría, permitiría superar errores y sesgos humanos. Sin embargo, esta supuesta neutralidad técnica resulta discutible y requiere un análisis crítico.

La evidencia disponible sugiere que la IA no ha provocado una sustitución generalizada de ocupaciones íntegras; más bien, un impacto desigual debido a limitaciones de viabilidad técnica o a que la automatización de determinadas tareas aún no alcanza el umbral de rentabilidad económica necesario para desplazar al factor humano. Parece que sí se observa una tendencia clara a la sustitución de funciones de mandos intermedios y de supervisión mediante el uso de algoritmos para dirigir y gestionar el trabajo (Todolí, 2023).

Esta tendencia a la reconfiguración de roles se ha hecho especialmente visible en la coyuntura más reciente. A comienzos de 2026, las empresas tecnológicas están inmersas en procesos de despidos colectivos. La narrativa de que la inteligencia artificial está desplazando masivamente el empleo tecnológico está ganando peso, pero es importante reconocer que la suma de factores que pueden estar detrás requiere un análisis más cauteloso. Las empresas están transformando su estructura de costes, reduciendo plantillas en determinadas áreas para financiar tanto la infraestructura de sistemas inteligentes como la captación de perfiles técnicos muy cualificados tecnológicamente. Por un lado, la tecnología permite a ciertos perfiles absorber una densidad de tareas antes inabarcable, reduciendo las necesidades de determinados puestos, mientras que, por otro, las presiones financieras dictan una transición hacia modelos de negocio más ligeros en personal y más intensivos en software. Por tanto, por el momento las empresas, o al menos el pequeño porcentaje de empresas que a día de hoy están inmersas en procesos de digitalización profunda, podrían estar realizando un trasvase estratégico de recursos cuya huella definitiva en el mercado laboral global todavía no puede determinarse con exactitud.

Tras años de expansión, lo que sí se puede afirmar es que las tecnologías digitales ya han transformado de manera significativa la forma en que trabajamos y seguirán haciéndolo en el futuro. Este proceso constituye un **cambio de paradigma** histórico que trasciende la preocupación tradicional por la cantidad de empleos para incidir directamente en la organización misma del trabajo. Más allá de ser una mera herramienta técnica, la inteligencia artificial actúa como un agente transformador que altera el tejido de nuestras sociedades y redefine las relaciones de poder y subordinación en el entorno laboral, modificando profundamente la manera en que la actividad se planifica, se supervisa y se dirige (Ponce del Castillo, 2024).

En este punto, el impacto más profundo de la revolución digital no reside tanto en la cantidad de empleo o en los tipos de ocupaciones, sino en **la manera en que se organiza el trabajo y en las relaciones entre personas trabajadoras y empleadores** (Fernández-Macías et al., 2025) o en los propios **procesos de reestructuración de las cadenas de valor**. Estos cambios tienen, además, consecuencias relevantes en términos de desigualdad y segmentación del mercado de trabajo (Lahera, 2021). Por este motivo, el interés creciente no se centra únicamente en el empleo, sino en el impacto que el uso de algoritmos —con o sin inteligencia artificial— está teniendo sobre las condiciones de trabajo de las personas sometidas a sistemas de dirección y gestión algorítmica.

Existe una estrecha relación entre la gestión algorítmica y la vigilancia digital. Esto se debe a que los algoritmos necesitan datos para funcionar y a que la información digital se procesa de manera más eficiente mediante algoritmos. Por lo tanto, la gestión algorítmica del trabajo generalmente presupone cierto grado de supervisión digital y, a la inversa, la supervisión digital tiende a fomentar el uso de algoritmos para dirigir, evaluar y disciplinar, así como para coordinar a la fuerza laboral (González, et al, 2025).

La digitalización avanzada no se reduce a la incorporación de nuevas tecnologías en las empresas, sino que constituye un proceso más amplio que combina distintos elementos interrelacionados y que transforma de manera profunda la forma de producir, organizar el trabajo y tomar decisiones. En primer lugar, implica la digitalización de la información, es decir, la conversión de datos, procesos analógicos y objetos físicos en información digital que puede ser recopilada, almacenada, procesada y analizada por sistemas informáticos.

Este proceso va acompañado del **uso creciente de tecnologías y datos digitales interconectados**, que permiten optimizar actividades existentes y, al mismo tiempo, dar lugar a nuevas formas de producción, intercambio y prestación de servicios. La interconexión entre sistemas, organizaciones y personas facilita la automatización de procesos, la coordinación en tiempo real y la integración de distintas fases de la actividad productiva.

En segundo lugar, la digitalización también conlleva una **transformación de los procesos y de la organización del trabajo**. Afecta a la manera en que se planifican las tareas, se coordinan las actividades y se toman decisiones dentro de las organizaciones, modificando los mecanismos de supervisión, control y evaluación del trabajo. Estos cambios no son únicamente tecnológicos, sino también organizativos y sociales.

Para que estas transformaciones sean posibles, resulta imprescindible la adquisición de **nuevas competencias y el desarrollo de una cultura digital** tanto a nivel individual como organizativo. La capacidad de utilizar las tecnologías de forma eficaz y crítica, así como de adaptarse a los cambios que generan, se convierte en un factor clave para las personas trabajadoras y para las propias empresas.

Finalmente, la digitalización plantea la necesidad de una **gobernanza de sus impactos sociales, laborales e institucionales**. El uso de tecnologías digitales tiene efectos sobre el empleo, las condiciones de trabajo, los derechos y las relaciones laborales, por lo que requiere marcos normativos, mecanismos de regulación y formas de participación que permitan orientar estos procesos y gestionar sus consecuencias. Los impactos de la revolución digital en el trabajo y el empleo están fuertemente mediados por las instituciones del mercado de trabajo: las normas laborales, el empleo y las regulaciones laborales, así como las relaciones industriales, desempeñan un papel fundamental en la configuración de los efectos de la digitalización, y las prácticas de gestión habilitadas por tecnologías digitales interactúan con las formas preexistentes de organización y control del trabajo (González, et al, 2025).

La negociación colectiva debe recuperar su función esencial de **límite al poder empresarial**, adentrándose en la regulación de los algoritmos y la IA para evitar que estos procesos se conviertan en una prerrogativa unilateral de la empresa. La gobernanza de la transición digital requiere un enfoque participativo para garantizar transformación más democrática, equilibrada y respetuosa con los derechos fundamentales (Bastante y Rodríguez, 2025)

Diversas organizaciones y autores (OIT, ETUI, EU-OSHA, EUROFUND entre otras) coinciden en la necesidad de promover una transición digital justa, que combine la innovación tecnológica con la protección de la salud, la seguridad y la dignidad de las personas trabajadoras.

1.1. Definiciones y conceptos clave

Para comprender el alcance de estos procesos, resulta necesario detenerse en algunas definiciones básicas. No existen definiciones únicas ni universalmente aceptadas de inteligencia artificial o de gestión algorítmica del trabajo. En el caso de la inteligencia artificial, se ha señalado la existencia de una notable “flexibilidad interpretativa”, ya que el término se utiliza para referirse a fenómenos muy distintos: desde un campo científico que estudia la cognición y los métodos computacionales para crear herramientas, hasta aplicaciones tecnológicas concretas que combinan software y hardware. Además, la inteligencia artificial opera también como un dispositivo retórico en discursos empresariales y políticos, y como un concepto social para reflexionar sobre una sociedad crecientemente organizada por máquinas (Galanos y Stewart, 2024).

En el ámbito laboral, la gestión digital del trabajo mediante algoritmos y sistemas de inteligencia artificial tiene una elevada capacidad de transformación cuando se introduce en las empresas. Se utilizan grandes volúmenes de datos para tomar decisiones sobre las personas trabajadoras; sin embargo, el crecimiento exponencial de la información recopilada ha hecho necesario incorporar algoritmos capaces de procesar automáticamente esos datos, ya sea para apoyar la toma de decisiones humanas o para aplicar directamente decisiones automatizadas (Todolí, 2023).

¿Qué es un algoritmo?

Un algoritmo puede definirse como un conjunto ordenado y finito de operaciones o reglas que permiten resolver un problema o realizar una tarea. Un algoritmo puede implementarse mediante programas informáticos, aunque no necesariamente es digital ni implica el uso de inteligencia artificial.

¿Qué es un sistema de decisión automatizada?

Un sistema de decisión automatizada es un proceso mecanizado que utiliza datos y algoritmos para apoyar u optimizar la toma de decisiones. Pueden distinguirse dos grandes modalidades:

- Sistemas programados mediante reglas explícitas, en los que quien programa define de antemano los criterios que el sistema debe aplicar para tomar decisiones.
- Sistemas que aprenden dichas reglas de forma implícita a partir del análisis de datos, identificando patrones estadísticos que permiten generar decisiones automatizadas (MITES, 2022).

¿Qué es la inteligencia artificial?

Los sistemas de decisión automatizada que “aprenden” de forma autónoma, no siguiendo instrucciones fijas, sino entrenándose a partir de datos, ajustando sus parámetros e identificando patrones para tomar decisiones, se denominan sistemas de inteligencia artificial. Los algoritmos son una condición necesaria, pero no suficiente, para la existencia de inteligencia artificial (CCOO, 2025).

Aunque no existe una definición única, el *Reglamento Europeo de Inteligencia Artificial (en adelante RIA)* define la IA como “un sistema basado en una máquina, diseñado para funcionar con distintos niveles de autonomía y que puede mostrar adaptabilidad después del despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de las entradas que recibe, cómo generar resultados que puedan influir en entornos físicos o virtuales” (RIA, 2024).

En esta misma línea, el RIA distingue los sistemas de inteligencia artificial del tratamiento básico de datos, señalando que se trata de sistemas capaces de inferir modelos para generar resultados —como predicciones, contenidos o decisiones— que influyen en entornos físicos o virtuales.

Como disciplina científica, la inteligencia artificial agrupa diversas metodologías, entre las que destacan el “aprendizaje” automático (incluido el llamado *deep learning* y por refuerzo), el “razonamiento” automático orientado a la planificación y optimización del conocimiento, y la robótica, que integra estas técnicas en sistemas ciberfísicos mediante sensores, percepción y control. En la práctica, esto significa que la IA no posee un pensamiento consciente, sino que, utiliza modelos estadísticos masivos para reajustar sus reglas iniciales provistas por un programador, a medida que procesa nueva información.

¿Qué es la gestión algorítmica del trabajo?

La OIT define la gestión algorítmica como el uso de sistemas algorítmicos automatizados que emplean datos de seguimiento y otra información para organizar, asignar, controlar, supervisar y evaluar el trabajo (OIT, 2025).

En términos similares, la OCDE señala que la gestión algorítmica consiste en el uso de herramientas tecnológicas para automatizar total o parcialmente tareas que tradicionalmente realizaban gestores humanos, incluida la recopilación de datos de las personas trabajadoras, con o sin el procesamiento posterior de dichos datos (OCDE, 2025).

1.2. El ecosistema tecnológico de la digitalización

La inteligencia artificial no actúa de forma aislada, sino que forma parte de un **ecosistema tecnológico interdependiente**, en el que distintas tecnologías y procesos se combinan y refuerzan mutuamente. Desde un enfoque formativo y generalista, este ecosistema puede agruparse en los siguientes ámbitos:

- **Inteligencia artificial y análisis de datos.** Incluye la inteligencia artificial, los algoritmos, el *Big Data*, la minería de datos y el análisis predictivo. Su función principal es procesar grandes volúmenes de información, identificar patrones y apoyar o automatizar la toma de decisiones.
- **Automatización y robótica.** Comprende la automatización de procesos mediante software, los chatbots y la robótica colaborativa. Estas tecnologías permiten ejecutar tareas repetitivas o de apoyo y complementar el trabajo humano en distintos entornos.
- **Infraestructuras digitales y computación en la nube.** La computación en la nube proporciona almacenamiento, capacidad de cálculo y aplicaciones que permiten un uso flexible y escalable de los sistemas digitales.
- **Conectividad y sistemas ciberfísicos.** Incluye el Internet de las cosas y las tecnologías de geolocalización, que conectan objetos físicos a redes digitales y permiten la monitorización y el control de procesos en tiempo real.
- **Tecnologías inmersivas.** La realidad virtual y otras tecnologías inmersivas se utilizan en ámbitos como la formación, la simulación de procesos, el diseño o el entretenimiento.
- **Plataformas laborales digitales.** Son infraestructuras que facilitan la interacción entre empresas, personas trabajadoras, clientes e instituciones, y organizan actividades económicas y sociales como el comercio electrónico o el trabajo en plataformas.
- **Tecnologías de registro y seguridad de la información.** Herramientas como el *blockchain* permiten registrar datos y transacciones de forma segura, transparente y descentralizada, contribuyendo a generar confianza en entornos digitales.

¿Cómo funcionan las innovaciones tecnológicas digitales?

Las innovaciones tecnológicas digitales comparten una serie de características que condicionan su funcionamiento y sus efectos sobre el trabajo y la organización productiva:

Una característica central es su **alta conectividad e interdependencia**, ya que los sistemas digitales se basan en la conexión constante entre dispositivos, plataformas y actores, lo que permite integrar procesos y adaptar la actividad en tiempo real.

Otra característica fundamental es su **dependencia de datos y algoritmos**. El funcionamiento de estas tecnologías se apoya en la recopilación y el análisis de grandes volúmenes de datos mediante algoritmos que orientan decisiones y automatizan procesos, influyendo directamente en la organización del trabajo y en las condiciones en las que este se desarrolla.

Estas tecnologías tienen, además, una **elevada capacidad para reorganizar procesos y formas de trabajo**. Permitirían y facilitarían la introducción modalidades de prestación laboral como el teletrabajo, la reorganización de turnos, la fragmentación de tareas o la posibilidad de asignarlas de manera flexible, en función de criterios como la eficiencia, los costes o la disponibilidad de recursos.

Por último, es importante subrayar la **ausencia de neutralidad tecnológica**. Las tecnologías digitales incorporan, como ya hemos señalado, decisiones humanas, criterios técnicos y marcos normativos que influyen en su diseño, implementación y uso. Por esta razón, los efectos de la digitalización no están predeterminados, y van a depender de cómo finalmente se configuren estos sistemas y del contexto social, organizativo y regulatorio en el que se utilicen.

1.3. La implantación de la gestión algorítmica y la inteligencia artificial

La gestión algorítmica y la inteligencia artificial se expandieron inicialmente en las plataformas digitales de empleo —como el reparto, la logística o el transporte con conductor—, pero progresivamente se han extendido a otros sectores como los cuidados, la limpieza o los servicios profesionales. Este fenómeno, como ya hemos indicado, ha sido descrito como *“plataformización del trabajo”*, y refleja que los sistemas algorítmicos ya no son exclusivos de la economía de plataformas, sino que están penetrando en todo tipo de entornos laborales.

Los datos recientes de la OCDE (2025), basados en una encuesta a más de 6.000 directivos, muestran una implantación muy amplia de estas herramientas. En Estados Unidos, el 90 % de las empresas declara utilizar algún tipo de software de gestión algorítmica, mientras que en España el porcentaje se sitúa en torno al 78 %, en línea con otros países europeos. Esto confirma que la digitalización de la gestión del trabajo es ya una realidad estructural en las economías avanzadas.

Estas herramientas se emplean principalmente para tres funciones: la organización y dirección del trabajo (asignación de tareas, planificación de turnos, gestión de cargas), la supervisión y seguimiento de la actividad (control del tiempo, ritmo o finalización de tareas) y la evaluación del desempeño (establecimiento de objetivos, medición de resultados o apoyo a decisiones sobre incentivos o sanciones). En Europa, su uso es significativo, aunque generalmente más prudente que en Estados Unidos, especialmente en lo relativo a la evaluación automatizada del rendimiento.

Desde la perspectiva de las personas trabajadoras, los datos de la encuesta AIM-WORK muestran que España presenta niveles elevados de gestión algorítmica. Un 32 % de las personas trabajadoras declara tener turnos asignados automáticamente y un 30 % recibir tareas mediante sistemas digitales. También se observan prácticas de monitorización digital, como el control del tiempo de trabajo o el seguimiento del uso de herramientas digitales, aunque con porcentajes más moderados. Paralelamente, alrededor del 30 % de las personas trabajadoras en la Unión Europea afirma haber utilizado herramientas de inteligencia artificial en el último año, especialmente en tareas relacionadas con la redacción, traducción o tratamiento de texto, con una clara concentración en ocupaciones de cuello blanco.

Tomando los datos de la encuesta ESSENER 2024, en España:

- un 8,9% de las empresas utiliza máquinas, sistemas o programas informáticos que asignan automáticamente tareas, tiempo de trabajo o turnos a las personas trabajadoras.
- un 4,8%, utiliza máquinas, sistemas o programas informáticos que supervisan el rendimiento y/o el comportamiento de las personas trabajadoras.
- un 8% utiliza dispositivos portátiles (wearables), como relojes inteligentes, gafas inteligentes o equipos de protección individual.
- Un 4,6%, utiliza máquinas que utilizan IA para realizar tareas de trabajo.

En cuanto al uso empresarial de la inteligencia artificial en España, la Encuesta sobre el uso de TIC de 2025 indica que el 13,4 % de las empresas de menos de 10 empleados y el 21,1 % de las empresas de 10 o más personas empleadas utilizan tecnologías de IA. Su implantación aumenta claramente con el tamaño de la empresa y es especialmente elevada en el sector TIC. En general, las grandes empresas industriales y de servicios muestran una mayor integración de herramientas de aprendizaje automático y automatización de flujos de trabajo, mientras que la construcción presenta niveles más reducidos, aunque con una tendencia creciente en las empresas de mayor tamaño.

Por último, el tipo de aplicaciones utilizadas revela que las empresas adoptan con mayor rapidez herramientas generativas y de tratamiento del lenguaje, mientras que la automatización de procesos y los sistemas de apoyo a la toma de decisiones avanzan de forma más gradual. En todos los sectores se observa una brecha por tamaño empresarial, lo que sugiere que la disponibilidad de recursos y capacidades tecnológicas condiciona la implantación.

Las experiencias recabadas en los workshops con delegados y delegadas llevados a cabo para este folleto, confirman en grandes rasgos los datos estadísticos en cuanto a implantación de la digitalización avanzada en sus sectores (a excepción del sector bancario, uno de los sectores excluidos de la Encuesta sobre el uso de TIC y comercio electrónico en las empresas).

- En el sector industrial, en 2025, el 26,4% de las empresas de 50 a 149 trabajadores declaraba usar IA y alcanza al 62,4% entre las empresas de más de 250 personas trabajadoras. Los delegados y delegadas del sector industrial afirmaban tener conocimiento de aplicación de herramientas digitales en sus centros de trabajo, tales como robots, gemelos industriales o análisis predictivos para la maquinaria.
- En el sector bancario, los delegados y delegadas están ampliamente familiarizados con las aplicaciones y sistemas de IA en sus trabajos y manifiestan altas sospechas de que las entidades utilizan aplicaciones para vigilar su desempeño.

- En el sector de la construcción, por el contrario, el conocimiento de la aplicación de estas herramientas es más limitado, aunque en empresas grandes —de más de 250 trabajadores— las estadísticas recogen que se aplica en cerca de la mitad de ellas.

Esta expansión desigual de la inteligencia artificial tiene implicaciones directas sobre la organización del trabajo, la supervisión y las condiciones laborales, así como sobre la necesidad de regulación y control adecuados.

Este marco general es relevante para la prevención de riesgos laborales por dos motivos.

En primer lugar, porque la misma infraestructura tecnológica que permite organizar y supervisar el trabajo (datos, sensores, algoritmos y plataformas) es la que está empezando a utilizarse para detectar peligros, anticipar incidentes y apoyar decisiones preventivas.

Conviene distinguir entre la gestión algorítmica del trabajo y el uso de sistemas digitales inteligentes con finalidad preventiva, ya que, aunque ambas realidades se apoyan en tecnologías similares —datos masivos, sensores, plataformas digitales y algoritmos— responden a lógicas distintas. La gestión algorítmica se orienta principalmente a organizar, dirigir y evaluar la actividad laboral, pudiendo influir en la asignación de tareas, el ritmo de trabajo o la valoración del desempeño. Por el contrario, la digitalización preventiva tiene como finalidad identificar peligros, anticipar riesgos y mejorar la seguridad y salud en el trabajo. Esta diferencia no depende tanto de la tecnología utilizada como del objetivo para el que se emplea, de las variables que se analizan y de las consecuencias asociadas a su uso.

Cuando los datos recogidos con finalidad preventiva se utilizan para controlar el rendimiento, adoptar decisiones disciplinarias o evaluar individualmente a las personas trabajadoras, el sistema deja de operar exclusivamente como herramienta de prevención y pasa a integrarse en mecanismos de dirección empresarial. Por ello, delimitar claramente finalidades, usos y garantías resulta esencial para asegurar que la digitalización contribuya efectivamente a la prevención de riesgos laborales y no derive en formas encubiertas de supervisión o control del trabajo.

Y, en segundo lugar, porque estas herramientas pueden impactar en la seguridad y salud tanto por sus oportunidades preventivas como por los riesgos asociados a la monitorización, la intensificación del trabajo o el uso de datos personales. A partir de este punto, el análisis se centra en el uso de la IA y de los sistemas digitales inteligentes aplicados específicamente a la Seguridad y Salud en el Trabajo (*en adelante SST*).

2. LA INTELIGENCIA ARTIFICIAL Y LOS SISTEMAS DIGITALES INTELIGENTES APLICADOS A LA PREVENCIÓN DE RIESGOS LABORALES

La incorporación de la inteligencia artificial (IA) y, en general, de sistemas digitales inteligentes basados en algoritmos automatizados tiene una gran capacidad para transformar la gestión de SST.

La EU-OSHA define las herramientas digitales inteligentes (*Smart digital tools*), como “nuevos sistemas de control de la seguridad y la salud en el trabajo que utilizan tecnología digital para recopilar y analizar datos con el fin de identificar y evaluar riesgos, prevenir y/o minimizar los daños, y proteger la seguridad y la salud en el trabajo” (EU-OSHA, 2025). Estas tecnologías permiten estudiar grandes volúmenes de información en tiempo real, generar predicciones y ofrecer recomendaciones operativas que facilitan un enfoque más anticipativo de la prevención.

Se ha publicado ampliamente sobre las oportunidades, los desafíos y los riesgos que implica la utilización de sistemas algorítmicos y la Inteligencia artificial en el ámbito laboral, tanto desde el ámbito académico por parte de organismos internacionales, por parte del ámbito sindical y por instituciones españolas.

A la hora de abordarlos en su aplicación concreta para la prevención de riesgos, cabe analizarlos desde una perspectiva similar:

- La digitalización avanzada tiene una **enorme capacidad de transformación**, dada la amplitud de aplicaciones que existen y que se desarrollan a un ritmo vertiginoso.
- Su aplicación no es **neutra**, tiene efectos de amplio espectro y relacionados entre sí.
- Su impactos positivos y negativos no están determinados por la propia tecnología, sino que **dependen de decisiones humanas** que hay detrás de su diseño, desarrollo y aplicación. Desde las personas trabajadoras que desarrollan el código hasta las políticas públicas, pasando por las empresas tecnológicas, las empresas que hacen uso de estas aplicaciones o las condiciones de uso que se negocian colectivamente.
- Los sistemas digitales inteligentes **no sustituyen a la gestión preventiva** ni a la toma de decisiones humanas, sino que actúan como herramientas de apoyo que proporcionan información adicional para mejorar la evaluación de riesgos y orientar las medidas preventivas.
- Su impacto depende del **sistema de gestión preventiva** donde se integra.

Aunque los sistemas digitales inteligentes no sustituyen la gestión preventiva ni el juicio profesional humano, sí modifican la forma en que se desarrollan algunas funciones dentro del ciclo preventivo. Estas tecnologías permiten automatizar tareas como la medición continua de exposiciones, el cribado inicial de riesgos o el seguimiento permanente de determinadas condiciones de trabajo, reforzando especialmente las fases de identificación de peligros, evaluación dinámica y control de las medidas preventivas. Sin embargo, la interpretación de los resultados, la contextualización de las condiciones reales de trabajo y la toma de decisiones preventivas siguen requiriendo intervención humana y participación de las personas trabajadoras. Cuando la evaluación del riesgo se apoya exclusivamente en indicadores o sistemas digitales de monitorización, puede producirse una visión parcial de la realidad laboral, ya que estos sistemas no captan plenamente factores organizativos, psicosociales o informales del trabajo. Por ello, estas herramientas deben entenderse como instrumentos de apoyo integrados en la mejora continua de la prevención, y no como sustitutos de la evaluación profesional ni del análisis del trabajo en situación real.

Los tres talleres llevados a cabo como acercamiento a las experiencias de delegados y delegadas en los centros de trabajo han permitido aseverar que el uso de sistemas de inteligencia artificial por parte de las empresas es probablemente anecdótico por el momento. Si bien cada vez hay más conocimiento sobre aplicaciones de IA por parte de las empresas, las personas participantes conocían algunos usos concretos para la PR, como dispositivos con sensores para detectar situaciones de peligro concreto. En el sector de la construcción mencionaron pulseras que alertaban de posibles encierros en ascensores en procesos de reparación o revisión y en industria identificaron algunos dispositivos concretos, como sistemas de video que permitían alertar de interacciones peligrosas entre maquinaria y personas.

Estos talleres permitieron igualmente valorar los usos de la IA para la prevención, no solamente por parte de la empresa en el desempeño de su obligación preventiva, sino para la propia labor de los delegados y delegadas de prevención. Para estos usos se identificaron herramientas de IA generativa con capacidad de facilitar y acompañar su actividad

Tomando esto como marco, en el siguiente apartado se van a presentar las aplicaciones de la Inteligencia artificial y sistemas algorítmicos inteligentes para la prevención de riesgos laborales.

2.1. Usos de la inteligencia artificial y los sistemas digitales inteligentes para la prevención de riesgos laborales

La IA y, en general, los sistemas digitales inteligentes aplicados a la SST tienen la capacidad de transformar la salud laboral, al mejorar la protección de las personas trabajadoras en industrias potencialmente peligrosas, especialmente en aquellos sectores de alto riesgo. Estas tecnologías pueden cumplir un papel proactivo de gran relevancia, avanzando hacia una prevención basada en datos, capaz de identificar señales tempranas de riesgo y activar intervenciones antes de que se produzca el daño.

En la práctica, muchas de estas aplicaciones combinan IA con otras tecnologías digitales (sensores, conectividad, plataformas y sistemas inmersivos), por lo que se describen conjuntamente.

La aplicación de la IA en el ámbito preventivo puede contribuir a:

- **Mejorar el cumplimiento normativo**, mediante el seguimiento en tiempo real del uso de equipos de protección individual (EPI), el control de accesos a zonas de riesgo o la supervisión de parámetros de seguridad en instalaciones y maquinaria.

- **Optimizar la toma de decisiones preventivas**, gracias a la generación rápida y precisa de datos sobre condiciones de trabajo, exposición a riesgos y patrones de siniestralidad.
- **Incrementar la precisión en la identificación de riesgos**, mediante el análisis automatizado de información procedente de sensores, equipos de trabajo, incidentes y variables ambientales.
- **Desarrollar modelos predictivos**, capaces de anticipar accidentes o fallos en equipos antes de que se materialicen.
- **Ampliar las oportunidades formativas**, utilizando entornos de realidad virtual y aumentada que permiten entrenar situaciones de emergencia o tareas peligrosas sin exposición real al riesgo.
- **Favorecer la accesibilidad y la inclusión**, adaptando tareas y herramientas a personas con necesidades específicas, como trabajadores de mayor edad o con determinadas limitaciones funcionales.
- **Mejorar el bienestar colectivo**, al facilitar entornos laborales más controlados y al permitir intervenciones preventivas más ajustadas a las condiciones reales de trabajo.

La **característica esencial** de un sistema de SST basado en IA es su capacidad de evaluación predictiva de riesgos. Al procesar grandes volúmenes de datos, se mejora significativamente las evaluaciones de riesgos y la identificación de peligros, permitiendo la activación de alertas inmediatas y la adopción de medidas de seguridad proactivas antes de que ocurran incidentes. De este modo, contribuye a la prevención de lesiones y la detección precoz de riesgos para la salud, siempre con el entendimiento de que debe complementar —no reemplazar— la decisión humana en la intervención del sistema de SST (OIT, 2025).

Estos sistemas digitales no deben entenderse únicamente como herramientas tecnológicas aisladas, sino como elementos integrados en el ciclo continuo de mejora de la SST. La información generada permite identificar riesgos, adoptar medidas preventivas, evaluar su eficacia y reajustar las intervenciones de forma permanente. De este modo, la digitalización introduce una lógica de prevención dinámica basada en datos, donde la gestión preventiva deja de apoyarse exclusivamente en evaluaciones periódicas para evolucionar hacia modelos de seguimiento continuo.

La Agencia Europea de Seguridad y Salud en el Trabajo lleva años desarrollando una línea de trabajo en torno a los Sistemas digitales inteligentes para la OSH, planteando oportunidades y retos (EU-OSHA, 2023), generando fichas informativas (EU-OSHA, 2025). La agencia subraya que, si se diseñan e implantan con un enfoque centrado en las personas, estas tecnologías pueden ser seguras y productivas, pero sus efectos dependen de cómo se gestionen y utilicen en el trabajo.

2.2. Una tipología de usos de sistemas digitales inteligentes para la PRL

A continuación, se van a detallar algunos usos de la IA y, en general, de los sistemas digitales inteligentes aplicados a la SST, sin intención de ser un listado exhaustivo, algo que resultaría estéril dada la velocidad del despliegue de nuevas tecnologías y aplicaciones. Para ejemplificar, se han añadido como referencia los casos de estudio recopilados por la EU-OSHA.

Estos sistemas digitales pueden agruparse en cuatro grandes categorías funcionales, que se integran en el ciclo continuo de mejora de la SST.

1. Sistemas de detección y monitorización del riesgo

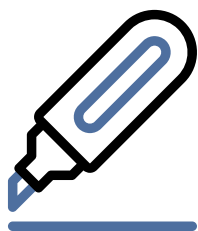
Este primer grupo incluye aquellas tecnologías cuya finalidad principal es identificar la presencia de peligros o medir la exposición antes de que se produzca el daño. Aquí se integran sensores ambientales conectados, dispositivos portátiles o wearables, equipos de protección individual inteligentes, cámaras con sistemas de visión artificial, sistemas *RFID*, redes *IoT* o drones de inspección.

Su aportación principal consiste en transformar la medición puntual en vigilancia continua y, en muchos casos, en tiempo real. Permiten conocer con mayor precisión los niveles de ruido, vibraciones, contaminantes químicos, radiaciones, temperatura o esfuerzo físico, así como detectar comportamientos inseguros o accesos a zonas restringidas.

Una característica relevante de estos sistemas es que permiten combinar la monitorización del entorno de trabajo con la medición individual de la exposición. Sensores ambientales, dispositivos portátiles y equipos inteligentes pueden recoger datos tanto sobre condiciones del lugar de trabajo —ruido, temperatura, radiación o contaminantes— como sobre respuestas fisiológicas o comportamientos asociados al riesgo. Esta doble perspectiva facilita una comprensión más completa de la exposición real y permite ajustar las medidas preventivas con mayor precisión.

Además, algunos sistemas incorporan funciones de retroalimentación inmediata, proporcionando avisos, recomendaciones o alertas directamente a la persona trabajadora cuando se detectan situaciones de riesgo. Este tipo de apoyo “en el puesto de trabajo” permite corregir conductas inseguras o adoptar medidas preventivas sin esperar a evaluaciones posteriores, reforzando la prevención primaria.

Desde el punto de vista preventivo, estos sistemas refuerzan la evaluación de riesgos, mejoran la trazabilidad de las exposiciones y facilitan la intervención temprana. Se sitúan principalmente en el ámbito de la prevención primaria y secundaria.



ALGUNAS EXPERIENCIAS

EU-OSHA. [Digitalisation of health and safety supervision, involvement and communication at construction sites: YIT LATVIJA Ltd \(Letonia\), 2025](#)

EU-OSHA. [Preventing Hand-Arm Vibration Syndrome \(HAVS\) \(CASE STUDY\), 2024](#)

EU-OSHA. [Digital solutions to reduce risks in glass production: AGC Glass Europe \(Belgium\), 2025](#)

EU-OSHA. [Digital systems for occupational safety and health monitoring, prevention and alerting in waste management: Amarsul – Treatment and Valuation of Solid Waste, S.A. \(Portugal\), 2025](#)

2. Sistemas de análisis y anticipación (inteligencia predictiva)

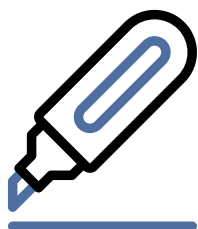
El segundo grupo no se centra tanto en la captación de datos como en su procesamiento. Incluye tecnologías como el Big Data, la inteligencia artificial, el aprendizaje automático y los modelos predictivos.

Estos sistemas permiten analizar grandes volúmenes de información procedente de accidentes, incidentes, condiciones ambientales y parámetros organizativos para identificar patrones de siniestralidad o prever fallos en equipos y procesos. Su valor reside en la capacidad de anticipar escenarios de riesgo y orientar la toma de decisiones preventivas.

El valor preventivo de estos sistemas no reside únicamente en la acumulación de datos, sino en su capacidad para transformarlos en conocimiento operativo. El análisis automatizado permite identificar relaciones entre condiciones de trabajo, organización del trabajo y aparición de incidentes o accidentes, facilitando decisiones preventivas basadas en evidencia y no únicamente en la experiencia previa o la reacción ante accidentes ya ocurridos. Esto también tiene aplicación en la prevención de accidentes aquellos derivados de riesgos psicosociales, analizando la relación entre cargas y ritmos de trabajo, número, momento y tipo de comunicaciones que se intercambian, mapas de interacción entre miembros de los equipos para identificar el aislamiento, patrones de organización de trabajo que se asocian a mayor incidencia de IT o rotación de personal.

Estos sistemas permiten avanzar hacia modelos de evaluación dinámica del riesgo, en los que la identificación y revisión de riesgos deja de ser un proceso puntual para convertirse en una actividad continua basada en datos en tiempo real.

Desde una perspectiva técnica, este bloque representa el paso de la prevención reactiva a la prevención predictiva. Se apoya en datos generados por los sistemas de monitorización y los integra en modelos que permiten planificar mejor la actividad preventiva, priorizar intervenciones y optimizar recursos.



ALGUNAS EXPERIENCIAS

EU-OSHA. [Digital app for workers' safety and reporting of incidents in electronic manufacturing: Intel Corporation \(Ireland\)](#), 2025

EU-OSHA. [Interactive space for AI-supported assistance to employees and stakeholders in the packaging industry: Focke & Co. and Stubbe \(Germany\)](#), 2025

EU- OSHA. [An OSH Smart Control Centre \(CASE STUDY\)](#), 2024

3. Sistemas de intervención y reducción directa de la exposición

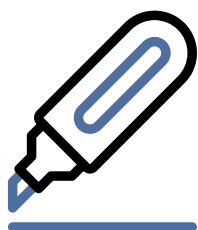
En este grupo se pueden ubicar aquellas tecnologías que no solo detectan o analizan el riesgo, sino que actúan directamente sobre él reduciendo o eliminando la exposición humana. Se incluyen la automatización avanzada, la robótica industrial, los vehículos autónomos, los robots colaborativos y los exoesqueletos.

Su función es sustituir o transformar tareas peligrosas, disminuir la manipulación manual de cargas, reducir la presencia de personas en zonas de alto riesgo o limitar la exposición a agentes nocivos. Desde

el punto de vista de los principios preventivos, este bloque se alinea con la eliminación o reducción del riesgo en origen.

Desde la perspectiva preventiva, estas tecnologías adquieren especial relevancia cuando contribuyen a aplicar los principios generales de la acción preventiva, especialmente la eliminación del riesgo en origen o la sustitución de tareas peligrosas. No obstante, su eficacia depende de que se integren junto con medidas organizativas y técnicas, evitando que la tecnología sustituya mejoras estructurales necesarias en el diseño del trabajo.

Los exoesqueletos, aunque no eliminan el riesgo en origen, actúan como medida de apoyo biomecánico. Por tanto, deben considerarse una medida complementaria y no sustitutiva de mejoras organizativas o de rediseño del puesto.



ALGUNAS EXPERIENCIAS

EU-OSHA. [Collaborative robots and automation to improve ergonomics in electronics solutions: Dinamica Generale \(Italy\)](#), 2025

EU-OSHA. [Digital solutions for safety and health in precision farming in vineyard work: Perla del Garda \(Morenica Società Agricola a Responsabilità Limitata\) \(Italy\)](#), 2025

EU- OSHA. [Smart Armband for Real-Time Data Analysis for Health & Safety \(CASE STUDY\)](#), 2024

EU-OSHA. [Robotic barrel unloading system to reduce risk of musculoskeletal injuries: Midleton Distillery of Irish Distillers, Pernod Ricard Group \(Ireland\)](#), 2025

EU-OSHA. [Wearables to Monitor & Improve Posture Ergonomics \(CASE STUDY\)](#), 2024

4. Sistemas de apoyo, formación y respuesta ante emergencias

El cuarto grupo engloba tecnologías orientadas a mejorar la capacitación, la respuesta ante situaciones críticas y la gestión posterior al accidente. Incluye la realidad virtual y aumentada para formación, sistemas de localización y “man-down” para personas trabajadoras aisladas, sistemas automáticos de alerta y plataformas digitales que facilitan la investigación de accidentes.

Estos sistemas pueden tener una dimensión preventiva (formación en entornos simulados sin exposición real) y una dimensión reactiva (minimización de consecuencias, mejora del rescate, recogida automática de datos para investigación).

La formación mediante entornos virtuales o aumentados permite reproducir situaciones de riesgo poco frecuentes, pero de alta gravedad, facilitando el aprendizaje práctico sin exposición real al peligro. Este tipo de entrenamiento favorece la adquisición de habilidades preventivas y mejora la capacidad de respuesta ante emergencias, especialmente en actividades complejas o de alto riesgo.

Además, estos sistemas no solo mejoran la preparación preventiva, sino que permiten minimizar las consecuencias del accidente mediante la localización inmediata de las personas trabajadoras, la activación automática de alertas o el apoyo digital a las operaciones de rescate.



ALGUNAS EXPERIENCIAS

EU-OSHA. [State-of-the-art simulators for handling machinery in underground mining: Hellas Gold \(Greece\), 2025](#)

EU-OSHA. [Digital app for workers' safety and reporting of incidents in electronic manufacturing](#)

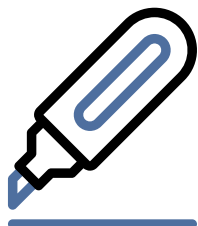
5. Otros usos

Los asistentes de IA y las herramientas de IA generativa pueden ser útiles para la asistencia, análisis documental, formación y comunicación.

Estas herramientas pueden acompañar y facilitar la elaboración y la mejora de la documentación preventiva. Se pueden llevar a cabo evaluaciones preliminares de riesgos por puesto o tarea, procedimientos de trabajo seguro, apoyo para planes de emergencia y evacuación, creación de instrucciones operativas, generación de checklists de inspección de seguridad, verificar legislación actualizada y apoyar la elaboración de políticas de SST ajustadas a la actividad de la empresa.

Los sistemas algorítmicos también pueden reforzar la labor de la Inspección de Trabajo en el control del cumplimiento de la normativa de prevención en todas las empresas. Gracias a la recopilación masiva de datos y a la capacidad predictiva de los algoritmos, la selección de las empresas a inspeccionar podría basarse en análisis del riesgo de incumplimiento, en lugar de criterios aleatorios o subjetivos. La selección de empresas para inspección debería apoyarse en una evaluación de la probabilidad y la gravedad de los riesgos de accidentes, exposiciones perjudiciales y, en general, de los incumplimientos de la normativa preventiva.

En esta línea, la OCDE o la EU-OSHA consideran que la inspección laboral en materia de SST podría implantar sistemas para acompañar la toma de decisiones basados en evaluaciones de riesgo realizadas mediante algoritmos, como un complemento a las percepciones de las y los inspectores. (Todolí, 2023)



ALGUNAS EXPERIENCIAS

MAX. El algoritmo MAX es una herramienta de Inteligencia Artificial implementada por el Ministerio de Trabajo de España, en funcionamiento desde 2022, diseñada para auxiliar a la Inspección de Trabajo y Seguridad Social (ITSS) en la detección de fraudes laborales, específicamente centrada en el abuso de horas extras y la falta de pago de las mismas.

3.

EL IMPACTO DE LA ADOPCIÓN DE IA Y SISTEMAS DIGITALES INTELIGENTES PARA LA PREVENCIÓN

La incorporación de sistemas digitales inteligentes en los entornos laborales está transformando de manera significativa la forma en que se organiza, supervisa y previene el trabajo. Tecnologías como la inteligencia artificial aplicada a la gestión laboral, los sistemas de monitorización mediante sensores, los dispositivos portátiles, la robótica colaborativa, los drones o las tecnologías inmersivas permiten recopilar y analizar datos en tiempo real sobre la actividad laboral, las condiciones ambientales y el comportamiento operativo.

Desde una perspectiva organizativa, la digitalización introduce una suerte de ilusión según la cual, los sistemas algorítmicos estarían transformando estructuralmente el poder y la organización laboral. Señala Todolí (2023), que la expansión de los sistemas algorítmicos implica que “hemos entrado en la era del trabajo dirigido por la inteligencia artificial”, que altera las dinámicas preventivas clásicas, ya que la supervisión humana directa puede verse parcialmente reemplazada por métricas digitales y procesos automatizados. Si bien, esto no implica una pérdida de control empresarial, que, por el contrario, se ve reforzado por el “efecto caja negra” generado por la opacidad de los datos y algoritmos, lo que ahonda en la asimetría de información entre la dirección de la empresa y los trabajadores.

Estas tecnologías introducen **nuevos factores de riesgo** o modifican factores ya existentes, alterando las condiciones en las que se desarrolla el trabajo.

Si bien el conocimiento por parte de los delegados y delegadas participantes en los tres talleres sobre la aplicación de sistemas inteligentes era limitado, sus experiencias en los centros de trabajo con la utilización de sistemas inteligentes por parte de las empresas para otros fines, se traducen en un alto nivel de desconfianza. Al hablar de inteligencia artificial y dispositivos y sensores de identificación de riesgos, la percepción es ambivalente. A pesar de las oportunidades que estos sistemas ofrecen, las personas muestran recelo ante las PRL, razones por las que una empresa podría decidir hacer una inversión tecnológica sin un claro beneficio económico ligado a la productividad. Ante esta percepción, emerge la desconfianza ante las posibilidades de sobrevigilancia, control y evaluación constante sobre la productividad medida al momento.

La evidencia analizada por la EU-OSHA muestra que los efectos sobre la SST dependen principalmente de cómo estas tecnologías transforman:

- la interacción persona-tecnología,
- la organización del trabajo,
- y el funcionamiento del propio sistema preventivo.

Por ello, el análisis preventivo se puede estructurar en **tres niveles de factores de riesgo**:

1. **Nivel tecnológico**, factores de riesgo derivados de la interacción directa con sistemas digitales.
2. **Nivel organizativo**, factores asociados a los cambios en la gestión y control del trabajo.
3. **Nivel preventivo**, aquellos relacionados con la propia integración de estas tecnologías en la gestión de la PRL.

En cada nivel se identifican los factores de riesgo, los riesgos laborales asociados y los posibles daños para la salud.

3.1. Factores de riesgo tecnológicos

Son los factores de riesgos y daños generados ante la interacción directa entre personas y los sistemas digitales introducidos en determinados procesos.

3.1.1. Interacción humano-máquina

La introducción de sistemas digitales inteligentes implica una creciente coexistencia entre personas trabajadoras y sistemas automatizados capaces de operar con distintos niveles de autonomía. A diferencia de la automatización industrial tradicional —caracterizada por espacios segregados entre máquinas y personas—, las tecnologías actuales se diseñan para interactuar directamente con el trabajo humano, compartiendo espacios físicos, tareas e información en tiempo real (EU-OSHA, 2023).

Esta nueva **forma** de interacción constituye un **factor de riesgo emergente**, ya que modifica los patrones tradicionales de control y previsibilidad del entorno de trabajo.



EJEMPLOS PRÁCTICOS

Drones de inspección en instalaciones industriales

En tareas de inspección de infraestructuras o espacios confinados, los drones permiten reducir la exposición a riesgos físicos. Sin embargo, cuando operan en zonas donde también trabajan personas, pueden producirse situaciones de riesgo si la persona trabajadora desconoce la trayectoria prevista del dispositivo, si se producen cambios automáticos de ruta o si existen interferencias que alteran su estabilidad.

Los estudios sobre vehículos aéreos no tripulados destacan que compartir espacios de trabajo con dispositivos autónomos exige nuevas estrategias de comunicación operativa, formación específica y adaptación conductual para evitar incidentes.

EU-OSHA, 2023b



Robots colaborativos en líneas de producción

En entornos industriales donde robots colaborativos ayudan en tareas de ensamblaje, la persona trabajadora puede confiar en que el robot se detendrá automáticamente ante la proximidad humana. Sin embargo, errores de calibración, sensores parcialmente obstruidos o interpretaciones incorrectas del movimiento humano pueden generar situaciones de contacto inesperado.

Sistemas de asistencia automatizada en mantenimiento

En operaciones de mantenimiento asistidas por IA, el sistema puede sugerir acciones o validar procedimientos. Si la persona trabajadora sigue automáticamente la recomendación sin verificación crítica —especialmente bajo presión temporal— pueden producirse errores técnicos con consecuencias materiales o de seguridad.

En conjunto, la interacción humano-máquina en entornos digitalizados no elimina el riesgo laboral, sino que lo transforma. La prevención debe orientarse no sólo a la seguridad técnica del sistema, sino también a garantizar la comprensión humana del funcionamiento tecnológico, la previsibilidad operativa y el mantenimiento del control humano efectivo sobre las tareas críticas.

3.1.2. Uso de pantallas de visualización de datos y tecnologías inmersivas

La digitalización del trabajo implica un uso creciente de interfaces digitales como elemento central de la actividad laboral. Pantallas múltiples, dispositivos móviles, sistemas de asistencia visual, gafas inteligentes o entornos de realidad virtual y aumentada forman parte cada vez más habitual de tareas de producción, mantenimiento, formación o supervisión remota (EU-OSHA, 2024).

A diferencia de los equipos informáticos tradicionales, estas tecnologías introducen una interacción más intensa y continua entre la persona trabajadora y el entorno digital, lo que modifica tanto las demandas perceptivas como la carga cognitiva asociada al trabajo. Desde el punto de vista preventivo, esta transformación constituye un **factor de riesgo emergente**, especialmente cuando el diseño tecnológico no se adapta adecuadamente a las capacidades humanas.



EJEMPLOS PRÁCTICOS

Formación mediante realidad virtual

En sectores industriales o de emergencias se utilizan simuladores de realidad virtual para entrenar situaciones de riesgo sin exposición real. Aunque estos sistemas mejoran el aprendizaje, sesiones prolongadas pueden provocar mareos, desorientación o fatiga visual, especialmente cuando los movimientos virtuales no coinciden con **los movimientos físicos del usuario**.



EJEMPLOS PRÁCTICOS

Supervisión remota mediante múltiples pantallas

En centros de control o logística digitalizada, las personas operarias supervisan simultáneamente múltiples flujos de información. La necesidad de vigilancia continua y procesamiento rápido de datos puede generar fatiga mental progresiva y aumentar la probabilidad de errores tras periodos prolongados de atención sostenida.

3.1.3 Automatización cognitiva y supervisión tecnológica

La automatización de determinadas tareas con el objetivo de reducir tareas repetitivas o peligrosas, tiende a desplazar la carga laboral desde el esfuerzo físico hacia demandas cognitivas y atencionales.



EJEMPLOS PRÁCTICOS

En entornos sanitarios digitalizados, sistemas de apoyo a la decisión clínica o monitorización automatizada permiten reducir tareas manuales repetitivas. Sin embargo, la persona profesional pasa a supervisar múltiples flujos de información generados por el sistema, debiendo detectar anomalías poco frecuentes pero críticas. Esta situación combina baja actividad física con elevada carga mental y responsabilidad, aumentando el riesgo de fatiga cognitiva y errores por disminución de la atención sostenida.

Diversos estudios sobre gestión algorítmica del trabajo señalan que la automatización de funciones cognitivas puede reducir la autonomía operativa y modificar el papel de la persona trabajadora hacia tareas de control y supervisión, incrementando las demandas cognitivas y la presión psicológica asociada a la responsabilidad sobre sistemas automatizados.

Se puede decir que la automatización no elimina la carga laboral, sino que tiende a redistribuirla hacia dimensiones mentales y atencionales del trabajo. Desde la perspectiva preventiva, resulta esencial evaluar no sólo la reducción del esfuerzo físico, sino también el incremento potencial de la carga cognitiva y sus efectos sobre la SST.

Cuadro 3.1. Factores, riesgos y daños de tipo tecnológico

Tipo de Riesgo	Factores de Riesgo	Riesgos Generados	Posibles Daños
SEGURIDAD	Coexistencia con robots colaborativos, drones, vehículos autónomos y sistemas de inspección. Diseño ergonómico deficiente del hardware.	Incertidumbre operativa (comportamiento imprevisible), interferencia física entre dispositivos de seguridad y necesidad de elegir entre tecnología o protección física, fallos de coordinación humano-máquina y exceso de confianza en el automatismo.	Colisiones, atrapamientos, golpes y lesiones traumáticas. Errores operativos. Estrés por entorno impredecible.
PSICOSOCIALES Y ORGANIZATIVOS	Gestión algorítmica, supervisión pasiva de sistemas, teleoperación y dependencia de decisiones digitales.	Carga mental excesiva por vigilancia constante, pérdida de control sobre la tarea (infra-carga por monotonía) y deshumanización de la supervisión.	Fatiga mental crónica, estrés laboral, desmotivación, pérdida de competencias profesionales y síndrome de "burnout" digital.
ERGONÓMICOS Y VISUALES	Uso de pantallas, visores (VR/AR), interfaces cerebro-máquina y uso de exoesqueletos.	Sobrecarga visual (focalización), conflicto sensorial (incongruencia visual-vestibular) y alteración de la distribución del esfuerzo corporal.	Fatiga ocular (astenopia), cefaleas, mareos (cyberenfermedad), náuseas y trastornos musculoesqueléticos por posturas fijas.
HIGIENE Y EMERGENTES	Uso compartido de visores de realidad virtual y realidad aumentada, condiciones ambientales del hardware.	Transmisión de patógenos por fómites, exposición a bacterias resistentes.	Infecciones cutáneas y sistémicas, afectación a trabajadores de mayor vulnerabilidad.
TRANSVERSALES	Reducción de actividad física y delegación total de funciones de seguridad.	Reducción de la detección autónoma del peligro y retraso en la capacidad de reacción ante fallos críticos del sistema.	Enfermedades cardiovasculares derivadas del sedentarismo e incremento de la probabilidad de accidentes graves por respuesta tardía.

Fuente: EU-OSHA.2023a, 2023b, 2023c, 2024a, 2024b, 2024c, 2024d.

3.2. Factores de riesgo organizativos

La incorporación de sistemas de inteligencia artificial en la PRL introduce nuevas formas de monitorización y análisis del trabajo orientadas a anticipar peligros, detectar exposiciones y mejorar la toma de decisiones preventivas. Sin embargo, la evidencia disponible muestra que estas tecnologías no solo afectan a la identificación de riesgos, sino también a la organización del trabajo y a la forma en que las personas trabajadoras interactúan con el sistema preventivo. De la misma forma, estos sistemas cambian los procesos de interacción social en el seno de la empresa, reduciendo los espacios de comunicación y apoyo social y redimensionando las relaciones jerárquicas.

Cuando los sistemas preventivos basados en IA se integran mediante mecanismos de monitorización continua y análisis automatizado de datos, pueden modificar los ritmos de trabajo, los márgenes de autonomía y las dinámicas de supervisión, generando factores organizativos que influyen directamente en la salud laboral.

EU-OSHA señala la existencia de “límites difusos entre la supervisión de la salud laboral y la supervisión del desempeño, lo que puede erosionar la confianza si la plantilla percibe los sistemas como mecanismos de vigilancia más que como herramientas preventivas. En línea con ello, Todolí destaca que “el trabajador puede llegar a sentir que es el algoritmo el que manda” y que la falta de claridad sobre el funcionamiento algorítmico reduce la capacidad real de control por parte de trabajadores y organizaciones colectivas, alterando el equilibrio del contrato de trabajo (Todolí, 2023).

Los talleres realizados con delegados y delegadas de los distintos sectores pusieron de manifiesto que este tipo de riesgos son los que mayor incertidumbre y recelo generan en los centros de trabajo. A pesar del escaso conocimiento sobre la aplicación de sistemas de IA para la PRL, las personas trabajadoras sí conocen los riesgos del uso de sistemas de digitalización avanzada en procesos productivos que tienen impacto organizativo en sus empresas con consecuencias en sus condiciones de trabajo.

3.2.1. Intensificación derivada de la monitorización preventiva inteligente

Los sistemas de IA aplicados a la PRL permiten recopilar datos en tiempo real sobre comportamientos, movimientos, condiciones ambientales o uso de equipos de protección. Aunque su objetivo es mejorar la seguridad, su funcionamiento puede introducir dinámicas organizativas similares a las observadas en la gestión algorítmica del trabajo cuando la información generada se utiliza para ajustar continuamente la actividad laboral.



EJEMPLO

En el sector de fabricación electrónica, la introducción de aplicaciones digitales de seguridad basadas en datos permite a las personas trabajadoras registrar incidentes y recibir alertas preventivas en tiempo real. Aunque estos sistemas mejoran la detección temprana de riesgos, los estudios muestran que la necesidad de interactuar continuamente con la aplicación durante la jornada puede introducir interrupciones frecuentes de la actividad y aumentar la carga cognitiva asociada al cumplimiento simultáneo de objetivos productivos y preventivos.

3.2.2. Reducción de autonomía del trabajador y mayor control algorítmico

La incorporación de sistemas de inteligencia artificial en la PRL introduce herramientas capaces de analizar datos en tiempo real y generar recomendaciones, alertas o decisiones automatizadas orientadas a reducir la exposición a riesgos. Sin embargo, cuando estos sistemas influyen directamente en la ejecución de las tareas o en la forma en que se aplican las medidas preventivas, pueden modificar los márgenes de autonomía profesional y los mecanismos tradicionales de supervisión humana.

La evidencia disponible indica que los sistemas digitales inteligentes utilizados para monitorizar la SST pueden asumir parcialmente funciones de evaluación, supervisión o validación preventiva que anteriormente dependían del criterio humano, transformando las relaciones organizativas dentro del sistema preventivo.



EJEMPLO

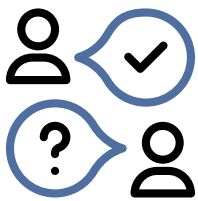
En sistemas de monitorización preventiva mediante dispositivos portátiles o plataformas digitales de seguridad, las alertas automáticas pueden indicar posturas incorrectas o comportamientos considerados inseguros. Aunque estas herramientas buscan reducir riesgos ergonómicos, cuando las recomendaciones se aplican de forma rígida pueden limitar la capacidad de las personas trabajadoras para adaptar la tarea a las condiciones reales del entorno, generando una percepción de control automatizado y reduciendo la interacción directa con supervisores o técnicos de prevención.

3.2.3 Vigilancia digital continua

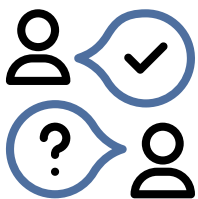
La incorporación de sistemas de inteligencia artificial en la PRL permite recopilar y analizar de forma continua información sobre las condiciones de trabajo, los comportamientos preventivos o la exposición a riesgos mediante sensores, dispositivos portátiles y plataformas digitales de monitorización. Estas herramientas facilitan la detección temprana de situaciones peligrosas y el seguimiento de indicadores de seguridad en tiempo real. Sin embargo, cuando la monitorización preventiva se basa en la recogida permanente de datos individuales, puede generar efectos organizativos y psicosociales relevantes.

La evidencia disponible señala que los sistemas digitales inteligentes aplicados a la SST pueden modificar la percepción del control laboral cuando la monitorización continua se asocia a la evaluación individual del comportamiento o del desempeño preventivo.

Los delegados y delegadas de prevención que participaron en los talleres identificaron este riesgo como el más alarmante, dado el nivel de intromisión que implican estos sistemas y, en consecuencia, como generadores de riesgos psicosociales en sus trabajos.



“En mi empresa de mantenimiento de ascensores nos han puesto unas pulseras que detectan si te has podido quedar encerrado. Si no te mueves durante un rato, activan una alerta y te llaman o incluso pueden mandar un equipo a ayudarte. Cuando vas al baño tienes que estar moviendo la mano”.



“Nosotras sabemos que nuestro banco funciona con sistemas de IA, aunque no lo reconocen, y que lo usan para saber lo que decimos a los clientes por teléfono. Hay gente que ha recibido avisos por parte de la empresa por dar determinada información por equivocación”.



Cuadro 3.2. Factores, riesgos y daños de tipo organizativo

Tipo de Riesgo	Factores de Riesgo	Riesgos Generados	Posibles Daños
SEGURIDAD	Dependencia de indicadores automáticos, sustitución de la supervisión humana y decisiones preventivas guiadas por algoritmos.	Pérdida de criterio humano: Menor capacidad de adaptación ante excepciones, reducción del juicio profesional y validación de seguridad basada solo en datos.	Fallos preventivos por evaluaciones incompletas, incidentes por pérdida de control manual y adopción de medidas inadecuadas.
PSICOSOCIALES Y ORGANIZATIVOS	Monitorización continua (sensores/cámaras), trazabilidad individual, evaluación permanente del cumplimiento y desuso de mandos intermedios.	Efecto Panóptico: Sensación de vigilancia constante, pérdida de autonomía, deterioro del apoyo social, presión temporal y desconfianza en el uso de datos.	Estrés laboral crónico, ansiedad, agotamiento emocional (burnout), desmotivación y miedo a la supervisión anticipatoria.
ERGONÓMICOS Y VISUALES	Generación masiva de alertas en tiempo real, señales digitales simultáneas a la tarea productiva y adaptación dinámica de ritmos.	Sobrecarga Cognitiva: Interrupciones frecuentes, atención dividida (tarea vs. alertas) y falta de ajuste de los ritmos algorítmicos a la realidad física.	Fatiga mental, saturación informativa y trastornos musculoesqueléticos indirectos por ritmos impuestos no ergonómicos.
HIGIENE Y EMERGENTES	Recopilación constante de datos biométricos y psicofisiológicos (como reflejos oculares, tono de voz o fatiga y uso de dispositivos portátiles (wearables) para detectar riesgos químicos/físicos.	Intrusividad y sesgo: Difuminación de la frontera entre prevención y control de desempeño, perfilado predictivo, pérdida de huella cinemática y dependencia de sensores para la higiene teórica.	Inseguridad laboral percibida, malestar psicológico por monitorización corporal, deshumanización y posibles reacciones dermatológicas por dispositivos.
OTROS (Gobernanza y Transparencia)	Falta de transparencia en los algoritmos, uso de datos para fines no comunicados y estandarización rígida de procedimientos.	Inseguridad Competencial: Desconexión con el sistema preventivo, reducción de la cooperación de la plantilla y percepción de trato desigual.	Deterioro del clima laboral, rechazo o sabotaje de sistemas tecnológicos y reducción de la eficacia global de la prevención.

Fuente: EU-OSHA. 2023a, 2024b, 2024e

3.3. Factores de riesgo preventivos

Desde la perspectiva preventiva, la digitalización introduce una dependencia creciente de sistemas automatizados de información que modifica los procesos tradicionales de evaluación del riesgo.

3.3.1. Digitalización de la vigilancia preventiva

La introducción de sistemas de monitorización digital permite recopilar información en tiempo real sobre condiciones ambientales, comportamientos laborales y parámetros de seguridad. Este cambio introduce una lógica preventiva basada en datos continuos que puede mejorar la anticipación de riesgos, pero que también puede alterar los equilibrios tradicionales entre tecnología, organización y experiencia profesional.

3.3.2. Individualización de la prevención

La introducción de sistemas digitales inteligentes en la SST permite recopilar y analizar grandes volúmenes de información sobre la actividad laboral mediante sensores, dispositivos portátiles y sistemas de monitorización digital. Estas tecnologías facilitan la obtención de datos a nivel individual sobre exposición, comportamiento y condiciones de trabajo, lo que puede contribuir a mejorar la identificación temprana de determinados riesgos.

No obstante, la EU-OSHA señala que el uso creciente de sistemas digitales de monitorización puede influir en la forma en que se desarrollan las actividades preventivas, especialmente cuando la evaluación del riesgo se basa principalmente en datos cuantificables generados por estos sistemas. En estos casos, resulta necesario asegurar que la digitalización complemente —y no sustituya— los enfoques preventivos tradicionales basados en el análisis del trabajo real y de la organización del trabajo.

Un riesgo crítico derivado de esta individualización es el potencial incumplimiento de la jerarquía de controles, un principio fundamental de la acción preventiva. Al centrar la tecnología en la respuesta fisiológica o el comportamiento de las personas trabajadoras a través de dispositivos portátiles (wearables), las empresas pueden verse tentadas a omitir la eliminación del riesgo en origen, que debe ser siempre la prioridad.

3.3.3. Gobernanza de datos y confianza preventiva

La implantación de sistemas digitales inteligentes en el ámbito laboral implica la recopilación, tratamiento y utilización de grandes volúmenes de datos relacionados con la actividad de las personas trabajadoras. Estos datos pueden incluir información sobre rendimiento, tiempos de trabajo, localización, interacción con equipos o exposición a riesgos laborales. Como consecuencia, la digitalización introduce nuevas cuestiones relacionadas con la gobernanza de los datos, la transparencia de los sistemas algorítmicos y la participación de las personas trabajadoras en su diseño e implementación.

3.3.4. Desigualdad sectorial y precariedad

El impacto de la inteligencia artificial (IA) y los sistemas digitales inteligentes diseñados específicamente para la PRL no se distribuye de manera homogénea ni universal en las empresas. Aunque estas tecnologías se comercializan bajo la premisa de garantizar entornos más seguros, su implantación no opera sobre un tejido laboral neutro. Al interactuar con las desigualdades estructurales previas del mercado de trabajo, los sistemas de monitorización y analítica preventiva pueden actuar, paradójica-

mente, como factores de amplificación de la desigualdad. Es fundamental reconocer esta heterogeneidad, analizando cómo las herramientas inteligentes de PRL generan riesgos asimétricos en función de la segmentación sectorial, el género y la edad de las personas trabajadoras (EU-OSHA 2024b).

La primera gran asimetría se observa en la forma en la que se integran hasta ahora los sistemas algorítmicos en los distintos entornos. En sectores intensivos en mano de obra, caracterizados por una alta temporalidad y subcontratación —tales como la logística de grandes almacenes, el reparto o los servicios de atención al cliente—, la IA se introduce prioritariamente bajo la modalidad de gestión algorítmica corporativa (Fernández-Macías et al., 2025). Estos sistemas están orientados de manera casi exclusiva a la optimización de los flujos de producción, la monitorización biométrica en tiempo real y la evaluación automatizada del rendimiento.

En plantillas con escasa flexibilidad y con menor capacidad de negociación sectorial, el riesgo de que las herramientas de monitoreo puedan convertirse en vigilancia extrema, con posibilidad de fiscalizar los *microtiempos* de descanso o los movimientos físicos, transforma un mecanismo de protección en un estresor crónico.

3.3.5. Desigualdades y sesgos en la prevención digital

La incorporación de sistemas digitales inteligentes en la PRL puede generar efectos diferenciados sobre distintos colectivos de personas trabajadoras cuando los sistemas se diseñan o aplican sin considerar la diversidad existente en edad, género, capacidades digitales o nivel socioeducativo. Los sistemas basados en datos y algoritmos tienden a reproducir patrones presentes en los datos utilizados para su entrenamiento o funcionamiento, lo que puede introducir sesgos indirectos en la identificación de riesgos, en la asignación de medidas preventivas o en la evaluación del comportamiento seguro.

En estudios de caso se ha identificado el “sesgo del operador medio virtual” (*“virtual average operator”*) es un riesgo preventivo que surge cuando los sistemas de gestión algorítmica diseñan las cargas y ritmos de trabajo basándose en un “artefacto estadístico” o media matemática idealizada, en lugar de considerar a las personas reales. Al equilibrar las líneas de producción bajo el supuesto de que todas las personas trabajadoras poseen la misma fuerza, velocidad y resistencia, el sistema ignora la diversidad humana de edad, género o capacidad física, lo que provoca que cualquier persona que no encaje exactamente en ese promedio sufra una sobrecarga física y mental desproporcionada que resulta invisible para el control digital.

Desde una perspectiva preventiva, estos sesgos pueden traducirse en una protección desigual frente a los riesgos laborales cuando determinados perfiles de personas trabajadoras quedan infrarrepresentadas en los datos o cuando las soluciones tecnológicas se diseñan tomando como referencia perfiles laborales estándar.

3.3.6. Brecha de formación y capacitación preventiva digital

La eficacia preventiva de los sistemas digitales inteligentes depende en gran medida del nivel de comprensión y capacitación de las personas trabajadoras respecto a su funcionamiento. La introducción de tecnologías avanzadas sin una formación adecuada puede transformar una herramienta preventiva en un nuevo factor de riesgo, especialmente cuando la plantilla debe interpretar alertas, recomendaciones automatizadas o información generada por algoritmos complejos.

La falta de formación constituye un elemento crítico en la implantación tecnológica, ya que puede generar dependencia excesiva de los sistemas, errores de interpretación o pérdida de control operativo.

Cuadro 3.3. Factores, riesgos y daños de tipo preventivo

Tipo de Riesgo	Factores de Riesgo	Riesgos Generados	Posibles Daños
SEGURIDAD	Dependencia de alertas automáticas, juicio profesional relegado y confianza excesiva en la capacidad predictiva de la IA.	Sesgo de automatización: Falsa sensación de seguridad, detección incompleta de riesgos no monitorizables y errores por mala interpretación de alertas.	Accidentes e incidentes por fallos no detectados. Mantenimiento de exposiciones peligrosas por "ceguera" del sistema digital.
PSICOSOCIALES Y ORGANIZATIVOS	Monitorización individual constante, falta de transparencia algorítmica y uso de datos preventivos para otros fines.	Quiebra de la confianza: Percepción de vigilancia intensificada, tensión laboral, desconfianza hacia la tecnología y reducción del compromiso preventivo.	Estrés laboral crónico, agotamiento emocional (burnout), deterioro del clima laboral y ansiedad por evaluación continua.
ERGONÓMICOS Y COGNITIVOS	Interfaces no adaptadas a la diversidad (edad/ capacidad), falta de formación técnica y comprensión limitada de los límites del sistema.	Inseguridad competencial: Saturación informativa, brecha digital entre colectivos y fatiga mental por incertidumbre tecnológica.	Fatiga mental acumulada, disminución del rendimiento cognitivo y accidentes derivados de la desadaptación tecnológica.
HIGIENE Y EMERGENTES	Enfoque exclusivo en indicadores individuales cuantificables y omisión de factores organizativos o contextuales complejos.	Evaluación incompleta: Priorización de lo "fácilmente medible" (ruido, temperatura) frente a riesgos multifactoriales o emergentes.	Adopción de medidas preventivas ineficaces y mantenimiento de riesgos laborales crónicos no reflejados en los sensores.
OTROS (Gobernanza y Ética)	Ausencia de participación laboral en el diseño, sesgos en los datos de la plantilla y falta de accesibilidad. Ambigüedad y complejidad de la normativa vigente	Desigualdad preventiva: Percepción de trato discriminatorio, exclusión de grupos vulnerables y posible sabotaje o evitación de los sistemas. Difuminación de la responsabilidad, incertidumbre en la asignación de responsabilidades.	Inseguridad laboral percibida, desigualdad en la protección de la salud y menor eficacia global del sistema preventivo.

Fuente: EU-OSHA., 2023a, 2023b, 2023c, 2024a, 2024b, 2024c, 2024e, 2024d, 2024f

En conclusión, el análisis de los factores de riesgo asociados a la inteligencia artificial demuestra que la digitalización no es un proceso neutro en el ámbito de la salud laboral. Si la implantación de algoritmos y sistemas inteligentes se guía exclusivamente por criterios de productividad y control, el resultado inevitable es la aparición de riesgos psicosociales emergentes, la intensificación del trabajo, la pérdida de autonomía y una peligrosa individualización de la prevención que debilita los sistemas colectivos de seguridad. Por tanto, ante este diagnóstico técnico, se hace evidente que el verdadero blindaje de la salud de las personas trabajadoras no vendrá de la tecnología en sí misma, sino de la capacidad de intervención del factor humano. Es aquí donde la negociación colectiva y la acción directa de los delegados y delegadas de prevención adquieren un papel estratégico insustituible, transformando estos riesgos identificados en regulaciones concretas y herramientas de control dentro de la empresa, tal como se detalla en el siguiente apartado.



4.

LA INCORPORACIÓN DE SISTEMAS INTELIGENTES PARA LA PRL

La integración de sistemas digitales inteligentes y herramientas de inteligencia artificial en la gestión de la SST representa un avance cualitativo hacia una prevención de precisión. Esta tecnología permite transformar los entornos laborales mediante la identificación temprana de riesgos ocultos, el análisis de grandes volúmenes de datos en tiempo real y la implementación de medidas preventivas más exactas. De este modo, la IA se posiciona como un aliado estratégico para anticipar accidentes y enfermedades profesionales antes de que ocurran.

La decisión empresarial de introducir sistemas de digitalización avanzada en el ámbito preventivo no debe entenderse como un evento meramente técnico o una simple actualización de software. Se trata, en realidad, de un proceso organizativo, social y regulatorio de alta complejidad. Como advierten diversos organismos (EU-OSHA, 2024; EU-OSHA, 2026; OIT, 2025; ETUI, 2024), el impacto final de estas herramientas no está predeterminado por la tecnología en sí, sino por la interacción de diversas variables estratégicas y el contexto laboral donde aterrizan.

Estos sistemas, tal como se ha adelantado, pueden ser origen de amplios riesgos, siendo la amplificación de las brechas de poder entre las corporaciones tecnológicas, las empresas con más y menos recursos de diverso tamaño y las personas trabajadoras uno de los más alarmantes. Para mitigar esta asimetría, resulta clave esclarecer los criterios mínimos que se han de cumplir en la integración de estos sistemas digitales en la SST. Entre estos criterios destacan la transparencia informativa respecto a las lógicas algorítmicas, la implicación activa de la Inspección de Trabajo y las Agencias de protección de datos y de supervisión de la IA, y la participación de los delegados y delegadas de prevención en la evaluación previa de los riesgos organizativos y psicosociales. Solo mediante un seguimiento técnico riguroso y un control participativo será posible asegurar que la innovación tecnológica se supedita a su función de protección colectiva, manteniendo siempre el bienestar integral de la plantilla en el centro de la gestión laboral. Para lograrlo, la viabilidad de los sistemas inteligentes como herramientas preventivas eficaces dependerá de la consideración de una serie de factores.

4.1. Gestión de la seguridad y salud en el trabajo: criterios a tener en cuenta

A. Estrategia empresarial y cultura de prevención

La relevancia que la dirección otorga a la salud laboral es el principal determinante del funcionamiento adecuado de los sistemas inteligentes para la prevención. En empresas con una **cultura preventiva sólida**, la tecnología se integra como un pilar proactivo para consolidar el bienestar y la seguridad. Por el contrario, en organizaciones que optan por un sistema preventivo de “mínimos”, los sistemas inteligentes pueden aplicarse con el objetivo único de automatizar el cumplimiento normativo o reducir costes

administrativos. Si bien estos mínimos pueden resultar útiles para empresas con menores recursos, su capacidad para apoyar una adecuada política preventiva es menor o incluso podría derivar en un incumplimiento de la Ley de Prevención de Riesgos Laborales (Ley 31/1995), al supeditar la seguridad al ahorro de costes administrativos.

La tecnología sólo resulta preventiva cuando se integra en el ciclo continuo de mejora de la gestión de la SST. Implantaciones aisladas o tecnológicamente impulsadas —sin adaptación organizativa— generan efectos no previstos y reducen la eficacia preventiva. Es necesario que la tecnología esté imbricada, en conexión con la evaluación de riesgos, en coordinación con servicios de prevención, que esté sujeta a revisión periódica de resultados y que esté adaptada al contexto laboral real.

La aplicación adecuada de los sistemas inteligentes debería respetar la jerarquía de controles, aspirando en primer lugar a utilizar la automatización y la robótica avanzada para retirar a las personas de entornos peligrosos (eliminación y sustitución) y relegando los sistemas de vigilancia biométrica o sensores de comportamiento al papel de último recurso para gestionar únicamente los riesgos residuales.

B. La brecha de recursos y capacidades

La adopción de sistemas inteligentes exige una infraestructura que no es accesible por igual para todo el tejido productivo. Una implantación eficaz requiere no sólo recursos económicos, sino una infraestructura digital robusta y segura, así como personal cualificado capaz de auditar y gestionar los datos masivos. Mientras las grandes empresas cuentan con la capacidad técnica para implementar y controlar sistemas predictivos avanzados, las pequeñas y medianas empresas enfrentan barreras de inversión y conocimiento que limitan drásticamente sus posibilidades de implantación, supervisión y éxito.

C. Requisitos técnicos

Desde el punto de vista tecnológico, la **fiabilidad** de la prevención inteligente depende de la calidad de su arquitectura. Los sensores y modelos deben ser precisos, robustos y capaces de interoperar entre sí, que hayan sido testados adecuadamente para no incurrir en peligros derivados de su uso o de las interferencias con otros elementos preventivos.

Además, la seguridad laboral en la era digital depende de la seguridad informática. El sistema debe demostrar una alta **resiliencia frente a fallos técnicos o ataques externos**. Una vulnerabilidad en el software de un sistema de PRL podría traducirse en un riesgo físico real para el trabajador; por tanto, la ciberseguridad se convierte en una condición previa y transversal a toda la implantación.

D. Principio de precaución.

En el contexto de la SST, la incorporación de nuevas tecnologías no puede regirse por el criterio de “ensayo y error”. El **principio de precaución** actúa como una salvaguarda esencial: ante la incertidumbre científica sobre los efectos a largo plazo de ciertos algoritmos o dispositivos en la salud física y mental de las personas trabajadoras, la empresa debe adoptar una postura de cautela proactiva, en sintonía con los principios de la acción preventiva. Esto implica que, si existe una sospecha razonable de que una innovación tecnológica puede generar riesgos (como estrés algorítmico, tecnofatiga o fallos de seguridad imprevistos), su despliegue debe detenerse o limitarse hasta que se realicen evaluaciones de impacto exhaustivas.



Artículo 15 de la Ley 31/1995, de Prevención de Riesgos Laborales

4. La efectividad de las medidas preventivas deberá prever las distracciones o imprudencias no temerarias que pudiera cometer el trabajador. Para su adopción se tendrán en cuenta los riesgos adicionales que pudieran implicar determinadas medidas preventivas, las cuales sólo podrán adoptarse cuando la magnitud de dichos riesgos sea sustancialmente inferior a la de los que se pretende controlar y no existan alternativas más seguras.

Bajo este enfoque, la prioridad absoluta no es la eficiencia técnica, sino la ausencia de daño, exigiendo que cualquier herramienta sea sometida a un escrutinio riguroso, participativo y reversible antes de ser considerada apta para el entorno productivo. En este sentido es clave que los sistemas hayan superado testeos previos de seguridad e idoneidad, certificados preferiblemente por agencias públicas como la Agencia Estatal de Supervisión de la Inteligencia Artificial (AESIA).

E. Evaluaciones de impacto

Estas evaluaciones deberían realizarse tanto antes de la implantación (ex ante) como a posteriori (ex post), bajo los principios de la PRL para evitar los riesgos en su origen.

Evaluaciones previas (ex ante)

De acuerdo con la *Ley de Prevención de Riesgos Laborales*, el empresario tiene la obligación ineludible de realizar una evaluación de riesgos ante cualquier cambio en las condiciones de trabajo, incluyendo la introducción de nuevas tecnologías. En una fase previa a la implantación, esta evaluación cumple una función esencialmente preventiva y anticipatoria: su objetivo es identificar, antes de que la tecnología entre en uso, los posibles riesgos derivados de su diseño, de su finalidad y de la forma en que se prevé integrar en la organización del trabajo. En este momento resulta clave analizar aspectos como los cambios en las tareas y en los ritmos de trabajo, el aumento de la carga mental, la introducción de nuevos sistemas de control o supervisión, la intensificación del trabajo o la aparición de riesgos psicosociales.

Evaluaciones posteriores (ex post)

La vigilancia de la tecnología no termina con su puesta en marcha; requiere de una evaluación posterior (ex post) de carácter corrector y sistemático. Esta fase permite verificar el funcionamiento real del sistema y la interacción humana con la máquina, detectando efectos no previstos, riesgos emergentes por actualizaciones o desviaciones en el diseño original.

En este marco, la evaluación de impactos psicosociales adquiere una relevancia crítica para analizar específicamente cómo la aplicación de sistemas inteligentes para la PRL y la supervisión automatizada alteran la carga mental, la presión por tiempos y la fatiga cognitiva.

Estas evaluaciones no deben ser meros trámites estáticos, sino procesos dinámicos y participativos que permitan aplicar correcciones inmediatas si se detectan riesgos no previstos para la salud física o mental de los trabajadores.

F. Humano al frente

Es necesario que el papel de los algoritmos sea apoyar las decisiones pero que no sustituyan el juicio profesional en materia de SST, tal como recogen los reglamentos europeos y la Ley de Prevención de Riesgos Laborales. La responsabilidad final siempre es de la empresa y las **responsabilidades** concretas deben quedar claramente definidas. Se debería dar a conocer la empresa responsable del desarrollo de la tecnología, comprometiendo que los estándares éticos coincidan con los de la organización. Asimismo, debe quedar establecida de forma inequívoca la persona física responsable de la supervisión del sistema dentro de la empresa, garantizando que siempre haya un interlocutor humano ante cualquier incidencia o reclamación. En todo momento, el sistema debe permitir el derecho al desistimiento y garantizar una intervención humana significativa. Ninguna decisión automatizada debe ser irrevocable; el trabajador debe tener siempre la seguridad de que un humano puede revisar y corregir cualquier decisión del algoritmo.

G. Protección de la intimidad y *perimetraje* de los datos

El sistema solo debería tratar aquella información estrictamente necesaria para el fin preventivo perseguido. Para ello, es vital establecer un **perimetraje de los datos, estableciendo límites a qué datos, cuándo y dónde se recogen, hasta cuándo se guardan y quién accede a ellos**. Por un lado, definiendo qué información entra en el sistema y cuál queda fuera, generando un marco de materias excluidas, protegiendo así la esfera privada de las personas trabajadoras de una recolección masiva o innecesaria y la compartición de datos sensibles. Por otro lado, delimitar los límites de espacio y de tiempo en los que se pueden registrar tales datos. Implica delimitar el perímetro de acceso, es decir, quién tendrá acceso a esos datos. Y por último, qué empresas o departamentos tendrán acceso a ellos. Ciertas decisiones críticas, por su carga ética, humana o por la sensibilidad de los derechos en juego, no pueden ser delegadas a un sistema diseñado para un fin concreto. No se debe perder como referencia que existen los derechos de oposición y supresión.

H. Evaluación y prevención de sesgos algorítmicos

El mayor desafío técnico reside en la calidad de los datos. Si los registros históricos contienen errores o prejuicios, el sistema heredaré y amplificará **sesgos algorítmicos**. Identificar y corregir estos posibles sesgos es una obligación innegociable antes del despliegue, pero también reevaluado en función de los resultados. Cuando se establecen mecanismos de control y seguimiento a modo de auditorías de sesgos, el uso preventivo de las tecnologías digitales mejora sus posibilidades de éxito y aceptación por parte de la plantilla, ya que un algoritmo defectuoso puede derivar en decisiones erróneas que comprometan directamente la integridad física o la equidad en el trato a las personas trabajadoras.

I. La transparencia e inventario de sistemas inteligentes

La transparencia es una condición clave para evitar la opacidad en la toma de decisiones. Debe existir una claridad sobre los criterios establecidos para los algoritmos, sobre la procedencia y naturaleza de los datos utilizados para alimentar el sistema, así como sobre las evaluaciones de impacto. La delimitación de los distintos sistemas utilizados por la empresa y la especificación del uso concreto y declarado de cada uno de ellos permite detectar y corregir de forma proactiva sesgos discriminatorios o errores lógicos que podrían comprometer la integridad de la prevención.

J. Participación

La legislación ampara los derechos de información y consulta de las personas trabajadoras y su representación en materias relacionadas con la PRL, con la gestión algorítmica y con la protección de datos.

Ningún sistema digital puede ser plenamente efectivo si se diseña sin la participación de quienes lo utilizan. La adopción de la tecnología debe ser un proceso participativo dentro de la empresa. La articulación de **mecanismos de implantación y seguimiento participativo** favorecen la confianza de la plantilla.

La aceptación tecnológica por parte de la plantilla está directamente ligada a la **participación proactiva** desde las fases iniciales del diseño, la evaluación continua del funcionamiento de los sistemas y las evaluaciones de impacto psicosocial en la plantilla. Al involucrar a las personas trabajadoras, se permite ajustar la tecnología a la realidad del trabajo real y no solo a los criterios técnicos o de eficiencia productiva de los desarrolladores.

K. Formación

Cuando las empresas garantizan la adquisición de **competencias digitales** mediante formación continua, aseguran que la digitalización no profundice brechas generacionales, de género o socioeducativas. Para que una herramienta sea aceptada y eficaz, debe ser comprendida. La empresa debe facilitar información comprensible que esclarezca la utilidad, los límites y las garantías del sistema. Esta transparencia informativa se completa con una formación previa específica para las personas trabajadoras y sus representantes, dotándoles de las capacidades necesarias para interactuar con la tecnología de forma crítica y segura. De este modo, se evita dejar a parte de la plantilla en una situación de vulnerabilidad y por otro, se gana en aceptación.

L. Marco legal

Toda herramienta de digitalización avanzada debe asentarse sobre una base de estricta **legalidad**. Esto no solo implica el respeto a la Ley de Prevención de Riesgos Laborales, que obliga a evaluar el impacto de cualquier nueva tecnología en la salud de las personas trabajadoras, sino también toda la nueva legislación que se ha ido aprobando a lo largo de la última década para establecer garantías y límites que aseguren los derechos ante la utilización de dispositivos digitales en los distintos ámbitos y en el laboral entre ellos.

Con ellas se han definido los límites éticos o los derechos de información, tanto individuales como colectivos. Pero, además de la normativa actualizada, no pueden obviarse que otros derechos preexistentes deben verse salvaguardados también ante la introducción de nuevas herramientas digitales, desde el derecho a la igualdad y no discriminación, a la salud en el trabajo o a la protección de datos y la intimidad. Estos derechos deben ser salvaguardados de igual manera, ante el uso de sistemas algorítmicos o de IA para la PRL.

Para canalizar estos desafíos, se ha desarrollado un sólido marco jurídico que establece garantías fundamentales y protege los derechos de las personas trabajadoras, tanto a nivel individual como colectivo. En España, esta protección se articula principalmente a través de la normativa de la Unión Europea, que incluye reglamentos de aplicación directa como el *Reglamento Europeo de Inteligencia Artificial* (RIA) y el *Reglamento General de Protección de Datos* (RGPD). Estas normas aseguran que el uso de algoritmos en el trabajo sea transparente, ético y respetuoso con la dignidad del empleado.

Una herramienta de apoyo a la PRL debe asegurarse de cumplir con los requisitos normativos de transparencia, de supervisión humana y de control del sesgo algorítmico. Para ello debe cumplir el RIA (2024), junto a la normativa de protección de datos y no discriminación, establecen el suelo ético mínimo, los límites y las garantías. Bajo el marco del RIA, los sistemas de gestión algorítmica en el ámbito laboral son clasificados como de 'alto riesgo'. Esta categorización responde a la capacidad de estos sistemas para perpetuar sesgos históricos. En este sentido, la discriminación algorítmica por género (derivada de la falta de representatividad en los sets de entrenamiento) y por edad (mediante la penalización de trayectorias laborales extensas o brechas digitales) constituye una infracción directa de los derechos fundamentales, exigiendo una 'Evaluación de Impacto en los Derechos Fundamentales' previa a su implantación.

El RIA introduce límites específicos y obliga a aplicar mecanismos de supervisión humana para que la tecnología no vulnere los derechos fundamentales de las personas. Y para esto aplica un criterio de proporcionalidad, aumentando las exigencias legales en función del riesgo potencial que el sistema represente para la integridad de las personas.



NIVELES DE RIESGO DE LOS SISTEMAS DE IA

- **Riesgo Inaceptable (Prohibido):** Prácticas que suponen una amenaza clara a la dignidad o los derechos. Un ejemplo serían los Sistemas de IA que realicen reconocimiento de emociones en el lugar de trabajo. Estos podrían utilizarse para monitorizar el estado de ánimo de los empleados con fines disciplinarios, o sistemas de puntuación social que penalizasen a los trabajadores fuera de su jornada laboral.
- **Alto Riesgo (Muy regulado):** Sistemas que afectan directamente al empleo y la seguridad física. Los sistemas de IA de alto riesgo solo pueden utilizarse si se diseñan y gestionan para proteger la salud, la seguridad y los derechos fundamentales, incluida la no discriminación. Esto exige que el proveedor implante un sistema continuo de gestión de riesgos mediante **control humano** durante todo el ciclo de vida del sistema: identificar riesgos previsibles (también los derivados de usos indebidos razonablemente previsibles), evaluarlos y mitigarlos prioritariamente mediante el diseño y, cuando no sea posible, mediante controles, información y formación.
Un ejemplo serían los algoritmos de visión artificial diseñados para prevenir atropellos entre maquinaria y operarios en almacenes, o sistemas que monitorizan la fatiga de conductores profesionales para prevenir accidentes de tráfico. También se incluyen las IA que gestionan el acceso al empleo o evalúan el desempeño.
- **Riesgo Limitado (Obligación de transparencia):** Los sistemas de IA de riesgo limitado son aquellos cuyo uso está permitido porque, en principio, no generan un impacto grave sobre los derechos fundamentales, pero que pueden inducir a error si las personas no saben que están interactuando con una inteligencia artificial. Por ello, las personas usuarias deben saber que interactúan con una máquina.
Se categorizan aquí un chatbot de formación interactivo que resuelve dudas de los trabajadores sobre cómo utilizar correctamente los Equipos de Protección Individual (EPIs) o cómo actuar ante una emergencia química.
- **Riesgo Mínimo o Nulo (Sin obligaciones adicionales):** La gran mayoría de las aplicaciones actuales que no afectan a derechos fundamentales, como un filtro de correo electrónico que ayuda a prevenir el phishing corporativo o aplicaciones de calendario que automatizan los recordatorios de las revisiones médicas periódicas obligatorias.

Fuente: RIA, 2024.

Junto a la normativa comunitaria, el ordenamiento jurídico español integra leyes estatales que refuerzan esta vigilancia, además de la *Ley de Prevención de Riesgos Laborales*, el *Estatuto de los Trabajadores* en materia de información algorítmica y la *Ley Rider*, pionera en la regulación de la transparencia de los sistemas de gestión automatizados. El cumplimiento de estas normas es lo que permite que la innovación tecnológica se traduzca en un verdadero progreso social y laboral¹.

4.2. El papel estratégico de la RLPT de prevención ante la IA

Los delegados y delegadas de prevención desempeñan un papel estratégico fundamental para asegurar que la implantación de tecnologías digitales inteligentes se traduzca en una mejora real de la SST. Esta intervención permite que la digitalización trascienda el ámbito puramente técnico, transformándola en un proceso democrático que incorpora el conocimiento directo de la plantilla. Al participar activamente, la representación sindical garantiza que la innovación no suponga una pérdida de autonomía profesional ni se oculte bajo la opacidad algorítmica, sino que se oriente exclusivamente a la protección colectiva y al respeto de la dignidad en el entorno de trabajo.

En este escenario, el control sindical debe priorizar la salud mental, evitando que la optimización automática derive en una intensificación lesiva del trabajo. Es esencial monitorizar de manera constante la aparición de nuevos riesgos psicosociales, como el estrés por vigilancia electrónica o la deshumanización de la gestión del rendimiento. Los delegados actúan como garantes de que la tecnología se adapte a la persona y no a la inversa, asegurando que las herramientas digitales funcionen como un apoyo eficaz para la prevención de accidentes y no como una fuente de presión productiva inasumible.

Para que esta labor sea efectiva, la acción sindical debe apoyarse en un ecosistema jurídico robusto donde las leyes de prevención de riesgos, protección de datos y antidiscriminación actúen de forma coordinada. Mientras que la normativa de prevención y protección de datos salvaguarda la integridad y la privacidad frente a la vigilancia masiva, las leyes antidiscriminación operan como un cortafuegos indispensable contra los sesgos algorítmicos. No obstante, es la negociación colectiva la herramienta que permite aterrizar este marco legal a la realidad de cada centro, transformando los principios generales en garantías concretas y derechos exigibles.

Los delegados y delegadas de prevención han de activar las competencias y facultades que los artículos 36 y 37 de la Ley 31/1995 de Prevención de Riesgos Laborales (LPRL) otorgan a la representación sindical. Los delegados de prevención están legalmente facultados para ser consultados, con carácter previo y de forma obligatoria, sobre la adopción de nuevas tecnologías y las consiguientes modificaciones en la organización del trabajo que puedan afectar a la salud física o mental de las personas trabajadoras. Esta prerrogativa les permite exigir que la implantación de cualquier sistema de inteligencia artificial vaya acompañada de una evaluación de riesgos tecnológicos *ex ante*, así como fiscalizar los programas de vigilancia de la salud para evitar el sesgo del operador medio virtual y asegurar que las herramientas digitales inteligentes se limiten a complementar el juicio profesional humano en la acción preventiva.

¹ Existen normas que hacen referencia a la implantación de la tecnología en los centros de trabajo: Estatuto de los Trabajadores (Real Decreto Legislativo 2/2015); Protección de Datos y Derechos Digitales (Ley Orgánica 3/2018); Trabajo a Distancia (Real Decreto-ley 28/2020); Ley Rider (Ley 12/2021); y también existen normas que, aunque no regulan la tecnología per se, son de obligado cumplimiento siempre que la introducción de IA o sistemas digitales afecte a las condiciones de trabajo: Constitución Española de 1978; Ley de Prevención de Riesgos Laborales (Ley 31/1995); Igualdad de Trato y No Discriminación (Ley 15/2022); Libertad Sindical (Ley Orgánica 11/1985); Ley sobre Infracciones y Sanciones en el Orden Social (LISOS).



Por otra parte, para realizar esta vigilancia con seguridad y garantías, los representantes de los trabajadores están protegidos por el Estatuto de los Trabajadores. Este marco legal asegura que ningún delegado de prevención pueda sufrir represalias o discriminación por investigar cómo funcionan los sistemas automatizados o la IA en la empresa. Además, debido a la complejidad de estas tecnologías y al uso de datos internos, los delegados tienen la obligación de mantener un estricto sigilo profesional (confidencialidad), tal como exige el artículo 65 del Estatuto de los Trabajadores. Este deber no solo protege los secretos comerciales de la empresa, sino que también da tranquilidad y respaldo jurídico a los propios representantes, permitiéndoles auditar el funcionamiento del algoritmo a fondo sin vulnerar las leyes de competencia ni las normas de protección de datos (RGPD).

El comité de empresa tiene, por un lado, derecho colectivo a “ser informado por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles” (art. 64.4d ET).

Pero, además, la RLPT puede exigir que se cumplan los derechos individuales de información ante decisiones automatizadas que puedan tener efectos jurídicos sobre él o que le afecte de modo similar (Art 14 RDPD), de transparencia y explicación en sistemas de IA que son considerados de alto riesgo (RIA).

Este cuadro sintetiza los derechos individuales y colectivos frente a la digitalización y la IA, vinculándolos con la normativa que los ampara para servir como guía operativa de la representación sindical. Su propósito es facilitar la detección de vulneraciones, fundamentar la negociación colectiva y orientar las actuaciones ante las autoridades de control, asegurando que cualquier proceso de automatización se ajuste a la legalidad y al respeto de los derechos fundamentales en el centro de trabajo.

Cuadro 1. Derechos individuales y colectivos ligados a la IA y prevención de riesgos laborales, 2024

Materia	Derecho individual	Derecho colectivo	Legislación
Inteligencia artificial y decisiones automatizadas	Derecho a no ser objeto de decisiones basadas sólo en el tratamiento automatizado, incluida la elaboración de perfiles, que tenga efectos jurídicos en él o le afecte de modo similar. Aunque con consentimiento explícito o por necesidad para la celebración del contrato, la persona responsable del tratamiento ha de salvaguardar los derechos, libertades e intereses legítimos del interesado. Esto implica, al menos, el derecho a la intervención humana por parte del responsable, a expresar sus puntos de vista y a impugnar la decisión.	Derecho a ser informados sobre el uso de algoritmos que afecten a condiciones laborales. La representación puede exigir transparencia sobre sistemas algorítmicos y su impacto laboral.	RGPD art. 22;
	Derecho a no ser discriminada por categorías personales o comportamientos en el uso de sistemas de IA categorizados como de alto riesgo: contratación, evaluación, promoción, despido, supervisión y asignación de tareas.	Derecho de información ante la introducción de sistemas de IA considerados de alto riesgo.	ET art. 64.4.
	Derecho a recibir explicaciones claras y significativas del responsable del despliegue del sistema de IA, acerca del papel que ha tenido en el proceso de toma de decisiones que produzcan efectos jurídicos o que le afecten considerablemente sobre su salud, seguridad o derechos fundamentales.	Derecho de información y consulta sobre la utilización de sistemas automatizados de seguimiento o de sistemas automatizados de toma de decisiones en el trabajo de plataformas	Reglamento (UE) 2024/1689
	Las personas que realizan trabajo en plataformas: derecho a ser informadas sobre la utilización de sistemas automatizados de seguimiento o de sistemas automatizados de toma de decisiones.		Directiva (UE) 2024/2831 (art.9 al art.15)
Prevención de riesgos laborales	El deber de protección empresarial es ilimitado, abarcando también el entorno digital. Este deber se expresa en:	La dimensión colectiva es fundamental en términos preventivos: el deber de protección empresarial se realiza sobre los derechos de información, consulta y participación de las personas trabajadoras y la RLPT.	Arts. 14.2, 15.1, 19.1 y 22 LPRL (individual)
	La vigilancia de la salud ante la implementación de nuevas tecnologías (sometida al consentimiento de la persona trabajadora, salvo excepciones legales o de seguridad).		Arts. 18 y 33 LPRL (colectivo)
	Derecho a la formación e información específica sobre riesgos del entorno digital, en lo relativo al uso de herramientas o la desconexión digital.		Arts. 4.2.d) y 64 ET
	Derecho a la adaptación del trabajo, un principio preventivo especial ante la “elección de los equipos y métodos de trabajo”.		

Fuente: elaboración propia a partir de la normativa vigente.

En ocasiones, determinadas herramientas digitales inteligentes con impacto en las condiciones de trabajo no se presentan en las empresas como innovaciones ajenas al desempeño laboral, o incluso omitiendo su naturaleza de sistema inteligente. Sin embargo, incluso un sistema diseñado para la prevención de riesgos laborales, tiene capacidad para monitorizar el comportamiento, asignar cargas de trabajo o evaluar el desempeño en materia de seguridad. Por todo ello, tanto se activan las competencias de consulta y participación recogidas en la normativa.

Cuando concurren transparencia, participación, control humano, integración preventiva y finalidad orientada a la salud laboral, los sistemas inteligentes pueden convertirse en herramientas eficaces para anticipar riesgos y mejorar la prevención. En ausencia de estas condiciones, pueden reforzar dinámicas de vigilancia, intensificación del trabajo y generación de nuevos riesgos laborales.

Operativamente, la participación de la RLPT debe articularse mediante el seguimiento técnico y la auditoría de los sistemas, interviniendo en la definición de su alcance y contando, si fuera necesario, con el apoyo de expertos independientes. Estas evaluaciones deben verificar la trazabilidad de las decisiones automatizadas y la efectividad de la supervisión humana. Asimismo, la institucionalización de este control es clave, ya sea mediante la creación de comisiones tecnológicas específicas o el refuerzo de los Comités de Seguridad y Salud, dotándolos de competencias para revisar, modificar o incluso proponer la suspensión de sistemas que generen impactos negativos no previstos.

Es clave que la RLPT en el centro de trabajo es identificar los riesgos asociados a los procesos de transformación digital y analizar su impacto sobre las condiciones de trabajo. Evaluar resulta imprescindible para identificar, prevenir y corregir posibles sesgos, discriminaciones e impactos negativos sobre la salud y las condiciones de trabajo. Estas evaluaciones constituyen una herramienta clave de anticipación de riesgos y permiten exigir a las empresas garantías efectivas de equidad, transparencia y control humano en el uso de este tipo de tecnologías. Se pueden negociar evaluaciones conjuntas de impacto: evaluaciones de impacto organizativas, de impacto psicosocial, de salud laboral vinculadas a la tecnología o de impacto en privacidad y control.

En este contexto, resulta especialmente recomendable incorporar metodologías específicas de evaluación de riesgos psicosociales participativas, como el método CoPsoQ-istas²¹ o FPSICO. Su utilización está plenamente justificada en los procesos de digitalización e implantación de sistemas algorítmicos o de inteligencia artificial, ya que permite identificar de manera sistemática cómo estos cambios afectan a la organización del trabajo, las exigencias psicológicas, el ritmo de trabajo, la autonomía, la inseguridad laboral, el reconocimiento, el apoyo social o la doble presencia.

Estas evaluaciones deben realizarse con la participación de la representación legal de las personas trabajadoras, tal y como establecen el RIA sobre inteligencia artificial y los compromisos asumidos en los acuerdos derivados del diálogo social, tanto a nivel europeo como estatal. Asimismo, esta intervención es legalmente obligatoria bajo la normativa de protección de datos cuando el tratamiento pueda implicar un alto riesgo para los derechos y libertades. Esto sucede específicamente en el uso de sistemas de monitorización o control digital, el tratamiento intensivo de datos personales o biométricos, y el empleo de algoritmos de evaluación de rendimiento o sistemas automatizados de toma de decisiones que impacten directamente en la vida laboral de la plantilla.

Finalmente, la intervención sindical debe culminar en una gestión proactiva de medidas correctoras bajo los principios de proporcionalidad, necesidad y transparencia. Solo desde esta visión global y participativa es posible ejercer un control democrático efectivo sobre los sistemas que organizan y evalúan el trabajo. Al situar la salud psicosocial y los derechos laborales en el centro de la estrategia digital, la representación legal de los trabajadores garantiza que la innovación tecnológica se desarrolle de manera plenamente compatible con el bienestar integral y el interés general de la plantilla.

5.

REFERENCIAS

- Bastante Velázquez, C. C., y Rodríguez Fernández, M. L. (2025). Los derechos digitales y la inteligencia artificial en la negociación colectiva. *Temas Laborales*, 176, 239-269. <https://dialnet.unirioja.es/descarga/articulo/10296305.pdf>
- Confederación Sindical de Comisiones Obreras. (2025). *Guía para la intervención sindical en la gestión algorítmica*. Secretaría Confederal de Comunicación. <https://www.ccoo.es/ac72e664ccfc51f97a31e47eb0e159a3000001.pdf>
- EU-OSHA. (2023a). *Sistemas digitales inteligentes de supervisión de la seguridad y la salud en el trabajo: Oportunidades y desafíos* (Policy brief). <https://healthy-workplaces.osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-opportunities-and-challenges>
- EU-OSHA. (2023b). *Robótica avanzada, inteligencia artificial y automatización de tareas: Definiciones, usos, políticas y estrategias en el contexto de la seguridad y la salud en el trabajo*. https://osha.europa.eu/sites/default/files/documents/Summary_Advanced_Robotics_and_AI-based_Systems_es.pdf
- EU-OSHA. (2023c). *Unmanned aerial vehicles: Implications for occupational safety and health*. https://osha.europa.eu/sites/default/files/Unnamed-aerial-vehicles-and-OSH_en.pdf
- EU-OSHA. (2024a). *Worker exposure to virtual and augmented reality and metaverse technologies: How much do we know?* (Discussion paper). https://osha.europa.eu/sites/default/files/documents/worker-exposure-virtual-reality-discussion-paper_EN.pdf
- EU-OSHA. (2024b). *Worker management through AI: From technology development to the impacts on workers and their safety and health* (Discussion paper). <https://healthy-workplaces.osha.europa.eu/en/publications/worker-management-through-ai-technology-development-impacts-workers-and-their-safety-and-health>
- EU-OSHA. (2024c). *AI-based worker management in an automotive parts manufacturer in Italy: Implications for occupational safety and health*. https://osha.europa.eu/sites/default/files/documents/AI-worker-management-automotive-manufacturing-Italy_EN.pdf
- EU-OSHA. (2024d). *Automation of cognitive and physical tasks in the health and social care sector: Implications for safety and health*. https://osha.europa.eu/sites/default/files/documents/Automation%20of%20cognitive%20and%20physical%20tasks%20in%20health%20and%20social%20care%20sector_EN.pdf
- EU-OSHA. (2024e). *Risks and opportunities of AI-based worker management systems in an automotive manufacturing plant in Belgium*. https://osha.europa.eu/sites/default/files/documents/AI-worker-management-automating-manufacturing-plant_EN.pdf
- EU-OSHA. (2024f). *Digital technologies for worker management: Implications for safety and health. A comparative study of two automotive companies in Belgium and Italy*. https://osha.europa.eu/sites/default/files/documents/AIWM-OSH-automotive-companies-Belgium-Italy_EN.pdf
- EU-OSHA. (2025). *Sistemas digitales inteligentes para mejorar la seguridad y la salud en el trabajo* (Folleto informativo). Oficina de Publicaciones de la Unión Europea. <https://doi.org/10.2802/8631041>

- EU-OSHA. (2026). *Enhancing worker health and safety through AI-driven systems: Implications of the Artificial Intelligence Act* (Discussion paper). https://osha.europa.eu/sites/default/files/documents/worker-health-safety-ai-systems-artificial-intelligence-act_w996_EN.pdf
- Galanos, V., y Stewart, J. K. (2024). Navigating AI beyond hypes, horrors and hopes: Historical and contemporary perspectives. En A. Ponce del Castillo (Ed.), *Artificial intelligence, labour and society* (pp. 27-46). ETUI. <https://www.etui.org/publications/artificial-intelligence-labour-and-society>
- Gonzalez Vazquez, I., Fernandez Macias, E., Wright, S., y Villani, D. (2025). *Digital monitoring, algorithmic management and the platformisation of work in Europe*. Publications Office of the European Union. <https://data.europa.eu/doi/10.2760/9406086>
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (1995, 10 de noviembre). Boletín Oficial del Estado, (269). <https://www.boe.es/eli/es/l/1995/11/08/31/con>
- Ministerio de Trabajo y Economía Social. (2022). *Información algorítmica en el ámbito laboral: Guía práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral*. https://www.mites.gob.es/ficheros/ministerio/inicio_destacados/Guia_Algoritmos_ES.pdf
- Organización Internacional del Trabajo. (2025). *Revolución de la seguridad y salud: Papel de la IA y la digitalización en el trabajo*. Oficina Internacional del Trabajo. <https://doi.org/10.54394/KLPU4071>
- Organización para la Cooperación y el Desarrollo Económicos. (2025). *Gobernar con la inteligencia artificial: Panorama actual y hoja de ruta en las funciones centrales de gobierno*. OECD Publishing. <https://doi.org/10.1787/dc00e56a-es>
- Ponce del Castillo, A. (Ed.). (2024). *Artificial intelligence, labour and society*. ETUI. <https://www.etui.org/publications/artificial-intelligence-labour-and-society>
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. (2015, 24 de octubre). Boletín Oficial del Estado, (255). <https://www.boe.es/eli/es/rdlg/2015/10/23/2>
- Todolí Signes, A. (2023). *Algoritmos productivos y extractivos: Cómo regular la digitalización para mejorar el empleo e incentivar la innovación*. Aranzadi.
- Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, L 2024/1689. <http://data.europa.eu/eli/reg/2024/1689/oj>
- Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). *Diario Oficial de la Unión Europea*, L 119/1. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

CON LA FINANCIACIÓN DE:

AI2024-0012



GOBIERNO
DE ESPAÑA

MINISTERIO
DE TRABAJO
Y ECONOMÍA SOCIAL



FUNDACIÓN
ESTATAL PARA
LA PREVENCIÓN
DE RIESGOS
LABORALES, F.S.P.

