

BUENAS PRÁCTICAS PREVENTIVAS EN EL USO DE LA INTELIGENCIA ARTIFICIAL EN LA GESTIÓN DE LA PRL



28/04/2025

Impactos de la digitalización y la inteligencia artificial
en la seguridad y salud de las personas trabajadoras

La implantación de la inteligencia artificial y otros algoritmos, en el ámbito laboral, puede contribuir a la mejora de las condiciones de trabajo, pero también, el desconocimiento o incorrecto uso, puede implicar una seria amenaza, repercutiendo en la integridad moral de las personas trabajadoras, así, como en su seguridad, salud y bienestar.

Plan General de Actividades Preventivas 2025

Índice

0.	Introducción	2
1.	Objetivo de la guía	3
2.	Inteligencia artificial	3
	2.1 Definiciones	3
	2.2 Marco normativo	5
	2.2.1 Reglamento europeo de IA	6
3.	Situación actual de la IA y la digitalización en el ámbito laboral	13
4.	Beneficios e inconvenientes del uso de la IA en el ámbito de la PRL	19
5.	Principios éticos de la inteligencia artificial	23
6.	Gestión de la PRL en la implantación de la IA y otros algoritmos	26
7.	Principales aplicaciones de la IA y algoritmos en PRL	27
	7.1 Internet de las cosas (IoT)	28
	7.2 Big Data	29
	7.3 Uso de la IA para gestionar personas trabajadoras	30
	7.4 Robots colaborativos	31
	7.5 Chatbots	32
	7.6 Realidad virtual	32
8.	Bibliografía	33

0. Introducción

Hoy en día el **avance tecnológico, la digitalización y el desarrollo de la inteligencia artificial u otros algoritmos** han irrumpido con fuerza en todos los ámbitos de nuestra vida, especialmente en el ámbito laboral. Generan progreso y desarrollo socioeconómico al **aumentar la productividad y la competitividad en nuestras empresas; el bienestar y la inclusión social de las personas trabajadoras** y consiguen una **mayor sustentabilidad medioambiental**.

Esta **transición digital** conlleva a un **gran cambio en el mercado laboral**. Su **alto ritmo e incesante evolución** en los procesos de innovación y desarrollo requieren de una rápida familiarización y adaptación.

Algunas tecnologías con inteligencia existen desde hace años, pero los **avances informáticos, la disponibilidad de grandes cantidades de datos y la creación de nuevos algoritmos** han permitido un gran avance en los últimos años.

Hoy en día, la inteligencia artificial (IA) es la tecnología que más interés despierta. En nuestro día a día usamos múltiples aplicaciones y servicios con IA, por ejemplo: compras por internet, fuentes de búsqueda en internet, asistentes personales digitales, programas de traducción de idiomas, casas inteligentes, dispositivos de seguridad de los vehículos, ciberseguridad, y como no en el ámbito laboral, es usada en sectores como el sanitario, la educación, el transporte, la industria (uso de robots), agricultura, administración pública y servicios, etc.

Centrándonos en el **ámbito preventivo laboral**, la presencia de la digitalización y la inteligencia artificial puede afectar a la prevención de riesgos laborales. Su **gran logro** es la mejora de las condiciones de trabajo de las personas trabajadoras, al conseguir **transformar muchas tareas en simples, seguras y eficientes**, pero, a su vez implica **grandes desafíos** como:

- **Garantizar la seguridad y salud** de las personas trabajadoras frente a la aparición de nuevos riesgos emergentes.
- **Evitar la desaparición de numerosos puestos de trabajo o la precariedad de las condiciones de trabajo** por la automatización impulsada del uso de estas tecnologías.
- **Garantizar la accesibilidad y usabilidad** de la tecnología.
- **Garantizar las competencias digitales de las personas trabajadoras** (constante formación).
- **Garantizar la privacidad y la viabilidad de fuentes en el tratamiento de datos.**
- **Garantizar la desconexión digital de las personas usuarias** preservando el derecho a la conciliación de la vida personal y laboral.
- **Evitar la generación de una brecha social digital** que convierta en vulnerables a numerosos grupos de personas o colectivos. Por ello, es imprescindible establecer unos **criterios éticos** en el uso de la inteligencia artificial y algoritmos, bajo una **responsabilidad social**, que potencie los efectos positivos derivados del uso de estas tecnologías a la vez que evite desigualdades o contextos de exclusión de ciertas personas trabajadoras.

1. Objetivo de la guía

En esta guía proporcionaremos unas **pautas** de buenas prácticas preventivas, en el ámbito laboral, para **implantar correctamente la inteligencia artificial y algoritmos en las empresas**, dando a conocer sus **ventajas e inconvenientes de su uso** y **cuáles son algunas de las principales aplicaciones en IA** más utilizadas en la actualidad destinadas a **mejorar la gestión preventiva y/o las condiciones de trabajo de las personas trabajadoras**.

2. Inteligencia artificial y su marco normativo

2.1 Definiciones

La **digitalización** es la mejora de los procesos, las funciones y operaciones mediante el uso de la tecnología adecuada para **incorporar un nuevo espacio digital** a la empresa. Es el **traspaso de la información en formato físico a digital**. Así se permite:

- **Almacenar** grandes cantidades de datos en formatos compactos y realizar análisis complejos con ellos.
- **Automatizar de procesos**. Se puede procesar, clasificar y actuar sobre la información sin intervención humana, aumentando la eficiencia y minimizando errores.
- **Innovar y desarrollar** nuevos productos y servicios digitales con estos datos.

La **inteligencia artificial (IA)** es un campo de la informática que se ocupa del diseño de **sistemas inteligentes** que tienen la **capacidad de realizar funciones asociadas a la inteligencia humana**, de tal manera que una máquina puede presentar las mismas capacidades que los seres humanos, como la **percepción, el análisis, la comprensión, el aprendizaje, la creatividad, la adaptación, el razonamiento y la capacidad de interacción**.

La IA utiliza **algoritmos y modelos matemáticos** para **procesar las grandes cantidades de datos** de las que se alimenta para, entre otras tareas específicas, **tomar decisiones**, basadas en patrones y reglas, establecidas **a través del aprendizaje automático** (capacidad de una máquina para aprender de forma autónoma a partir de los datos sin necesidad de ser programada específicamente para hacerlo). De esta manera, se consigue que la IA gane en precisión y eficiencia con el tiempo.



La Comisión Europea la define como **sistemas de software** (y, posiblemente también de hardware) diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital:

- *Percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados.*
- *Razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado.*

La definición por el Reglamento Europeo de Inteligencia Artificial:

“Un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales”.

Las **principales características** de la IA son:

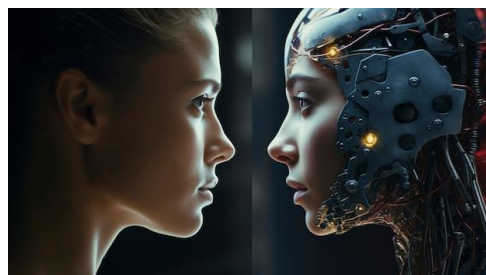
- **Aprendizaje automático (Machine Learning):** es capaz de aprender de los datos, a través de algoritmos de aprendizaje automático. Estos algoritmos permiten que las máquinas **mejoren su rendimiento con el tiempo a medida que se les proporciona más información y experiencia.**
- **Procesamiento del lenguaje natural (Natural Language Processing - NLP):** puede entender y procesar el lenguaje humano como lo haría un ser humano. Esto incluye la **capacidad de comprender y generar texto, traducir idiomas y comunicarse de manera efectiva con los usuarios.**
- **Visión por computadora (Computer Vision):** puede interpretar y comprender imágenes y vídeos, lo que **permite la detección de objetos, reconocimiento facial, comportamientos,** etc.
- **Razonamiento y toma de decisiones:** puede utilizar la información disponible para **razonar, evaluar diferentes opciones y tomar decisiones** basadas en algoritmos y modelos predefinidos.

Por lo tanto, la IA permite que los sistemas tecnológicos **perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico.** El **funcionamiento de la IA** se lleva a cabo en las siguientes **etapas:** **recopilación de datos** (imágenes, texto, sonidos, medidas, etc.), **procesamiento de los mismos** (filtrado, ordenación, aplicación de algoritmos), **aprendizaje o entrenamiento** (predecir o tomar de decisiones repetidas veces), **evaluación y ajuste de su rendimiento e implementación** en aplicaciones concretas destinadas a fines concretos: automatizar tareas, tomar decisiones basadas en monitorización de datos en tiempo real, predecir situaciones, desarrollar contenidos, etc.

La IA **recopila datos**, incluso en tiempo real, del espacio de trabajo, de las personas y del trabajo que realizan, a través de gran variedad de tecnologías digitales. Estos datos **son procesados** por algoritmos para extraer información que permite hacer **recomendaciones, predicciones y decisiones** sobre diversas gestiones. Después, se **comunican a otros sistemas digitales** (proceso de toma de **decisiones automatizado**, sujeto a regulación) o **a otras personas** (proceso de toma de **decisiones semiautomatizado**), como las responsables de RRHH, la responsable de la empresa, el responsable inmediato y, a veces, las personas trabajadoras. Esta información permite gestionar el trabajo de las personas con el objetivo **de mejorar los procesos, la organización del trabajo, la productividad, la gestión de los recursos humanos, el rendimiento del personal, la motivación y, la seguridad, la salud y el bienestar de las personas.**

La **transformación digital** integra la tecnología digital, y por lo tanto la IA, a todas las áreas de una empresa.

No se debe reemplazar el factor humano en esta integración, debe ser elemento esencial de dicho proceso.



La digitalización y el uso de la inteligencia artificial deben ser un recurso para **mejorar las condiciones de los puestos de trabajo, aumentar la productividad de las empresas y garantizar la seguridad, salud y bienestar de las personas trabajadoras.**

Los sistemas digitales inteligentes de Seguridad y Salud en el Trabajo (SST) son los que utilizan tecnologías digitales para **recopilar y analizar datos con el fin de identificar y evaluar cuyo propósito es el de prevenir y/o minimizar los daños derivados del trabajo**, a la vez que se **promueve la salud y el bienestar**. Los dispositivos de recopilación de datos consisten en sensores, cámaras, micrófonos, etc. que transmiten, normalmente, los datos por Bluetooth, identificación por radiofrecuencia o Internet de las cosas a una plataforma en la nube. Los algoritmos de IA procesan los datos y los traducen en información útil para las empresas con el fin de prevenir o reaccionar ante los riesgos.

Los sistemas inteligentes SST, en ese monitoreo de datos continuo, pueden **reaccionar** ante los riesgos laborales, pueden **identificar fuentes de riesgo rediseñando el puesto y/o lugares de trabajo**, pueden **predecir** situaciones de riesgo, pueden **alertar** a las personas trabajadoras cuando están realizando una tarea que implique un peligro para su salud, **proporcionándoles formación o facilitándoles instrucciones para la implantación correcta de medidas preventivas precisas a cada momento y trabajador/a.**

Las **aplicaciones de sistemas inteligentes SST**, en el ámbito laboral, hoy en día sirven para: **automatizar procesos, conteo de personal y asignación de tareas, detectar el uso de EPIs, detectar situaciones peligrosas** (riesgo de caídas en altura, riesgo de atropellos u otros riesgos existentes), **detectar el acceso a zonas restringidas, realizar mediciones de agentes físicos y químicos, llevar a cabo análisis predictivos de las condiciones de trabajo y/o de comportamiento de las personas trabajadoras, análisis o evaluación de tipo ergonómico y/o psicosocial, impartir formación**, etc.

2.2 Marco normativo

Para el uso de las aplicaciones en IA debe cumplirse una serie de requerimientos que están sujetos a un **marco normativo laboral y de protección de datos**, con el fin de **velar por los derechos fundamentales de las personas trabajadoras.**

Sobre la protección de datos, el art. 22 (Decisiones individuales automatizadas, incluida la elaboración de perfiles) del Reglamento General de Protección de Datos (RGPD) reconoce el **derecho de toda persona a “no ser objeto de una decisión únicamente basada en el tratamiento automatizado de sus datos, si ello produce efectos jurídicos en la persona o le afecta significativamente de modo similar”**. Esto implica a que el uso de herramientas tecnológicas basadas en la IA sea un **recurso complementario, pero no sustitutivo** a los recursos humanos disponibles en las empresas.



Del mismo modo, en dicho reglamento establece que, la utilización de herramientas basadas en sistemas algorítmicos conlleva la **obligación de las empresas de informar a sus personas trabajadoras** (conforme a los art. 13.2 f, 14.2g) y 15.1h)) sobre la lógica aplicada en la decisión automatizada en cuestión, *“así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado”*.

Por otro lado, en el marco normativo laboral, el art. 64.4 d) del Estatuto de los Trabajadores establece una obligación similar en favor de la representación legal de las personas trabajadoras, que tendrá **derecho a ser informada sobre los “parámetros, reglas e instrucciones de los algoritmos o sistemas de inteligencia artificial que puedan incidir en las condiciones de trabajo, el acceso y mantenimiento de empleo”**.

2.2.1 Reglamento europeo de IA

El **Reglamento europeo 2024/1689 de la IA** tiene como **objetivo mitigar el impacto negativo de la IA en la salud, la seguridad y los derechos fundamentales** de las personas trabajadoras, de tal manera que se **garantice un uso responsable y ético**.

El 2 de agosto del 2024 entró en vigor, 20 días después de su publicación en el Diario Oficial de la Unión Europea. El Reglamento será de aplicación **dos años después de su entrada en vigor**, es decir, el 2 de agosto de 2026, con excepción de las disposiciones específicas siguientes:

- Serán aplicable a partir del 2 de febrero de 2025 las disposiciones generales (capítulo I del Reglamento) y las prácticas de IA prohibidas (capítulo II del Reglamento).
- Serán aplicables a partir del 2 de agosto del 2025:
 - Organismos notificados (capítulo III, sección 4 del Reglamento)
 - Modelos GPAI (capítulo V del Reglamento)
 - Gobernanza (capítulo VII del Reglamento)
 - Confidencialidad (artículo 78 del Reglamento)
 - Sanciones (artículos 99 y 100 del Reglamento)
- El 2 de agosto de 2027 comenzarán a aplicarse las obligaciones para los sistemas de IA de alto riesgo integrados en productos regulados por la legislación armonizada de la Unión (artículo 6.1 del Reglamento).

Su **ámbito de aplicación** se extiende a:

- Los **proveedores** que introduzcan en el mercado o pongan en servicio sistemas de IA o modelos de IA de uso general en la UE, con independencia de si están o no establecidos en la UE o en un tercer estado.
- Los **responsables del despliegue** de sistemas de IA que estén establecidos o ubicados en la UE o cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión.
- Los **importadores y distribuidores** de sistemas de IA.
- Los **fabricantes** de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca.
- Los **representantes autorizados de los proveedores** que no estén establecidos en la Unión.
- Las **personas afectadas** que estén ubicadas en la Unión.

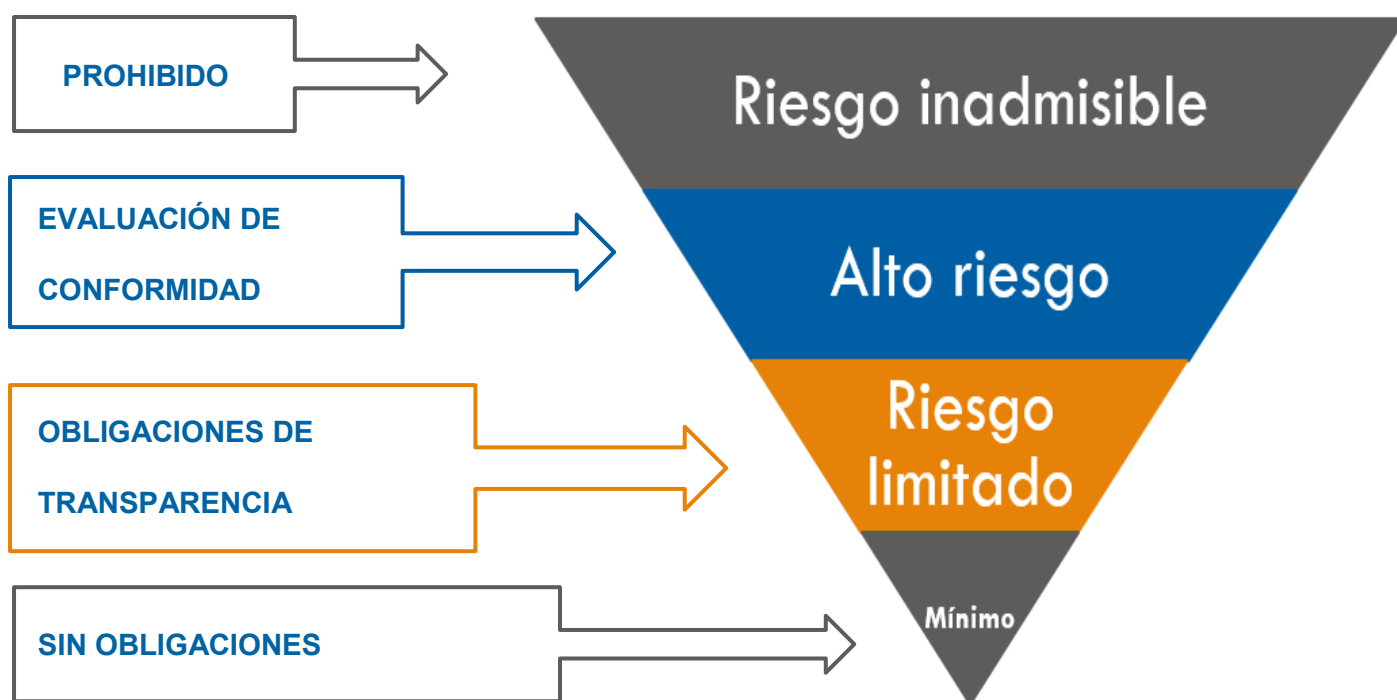
No entran dentro del ámbito de aplicación de este Reglamento los sistemas de inteligencia artificial diseñados exclusivamente con fines militares, de defensa o de seguridad nacional, así como las actividades de investigación, desarrollo y de prototipos que tengan lugar antes de la comercialización de un sistema de inteligencia artificial.

El Reglamento de IA **establece**:

- **Normas armonizadas** para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial en la UE.
- **Prohibiciones de determinadas prácticas** de IA en el entorno de la Unión.
- **Requisitos específicos para los sistemas de IA de alto riesgo** y obligaciones para los operadores de dichos sistemas.
- **Normas armonizadas de transparencia** aplicables a determinados sistemas de IA de riesgo limitado.
- **Normas armonizadas para la introducción en el mercado** de modelos de IA de uso general, bien sean de riesgo sistémico o no.
- **Normas sobre el seguimiento del mercado, la vigilancia de mercado, la gobernanza y una serie de garantías de cumplimiento.**
- Por primera vez, un reglamento europeo también introduce **medidas de apoyo a la innovación, prestando especial atención a las pymes**, incluidas las empresas emergentes o startups.

Los **proveedores e implantadores** de sistemas de inteligencia artificial **adoptarán, entre otras medidas, garantizar, en la medida de lo posible, un nivel suficiente de conocimientos de inteligencia artificial de su personal y de otras personas que se ocupen del funcionamiento y uso de los sistemas de inteligencia artificial en su nombre**, teniendo en cuenta sus conocimientos técnicos, experiencia, educación y formación y el contexto en el que vayan a utilizarse los sistemas de inteligencia artificial, y considerando las personas o grupos de personas sobre los que vayan a utilizarse los sistemas de inteligencia artificial.

El Reglamento establece unos **niveles de riesgo en función del uso de la IA** y, sobre las categorías detectadas, establece una serie de obligaciones.



➤ Riesgo inadmisibles

El reglamento **prohíbe algunos usos de los sistemas de IA** porque suponen un riesgo inaceptable para la Unión. Se trata de un **conjunto muy limitado de usos especialmente nocivos** que se oponen a los valores de la UE porque **vulneran los derechos fundamentales y afectan gravemente a la seguridad o a la salud de las personas**. Estos usos son:

- **Despliegue de técnicas subliminales, manipuladoras o engañosas** para distorsionar el comportamiento y perjudicar la toma de decisiones con conocimiento de causa, causando un daño significativo.
- **Explotar las vulnerabilidades relacionadas con la edad, la discapacidad o las circunstancias socioeconómicas** para distorsionar el comportamiento, causando daños significativos.
- **Sistemas de categorización biométrica que infieran atributos sensibles** (raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual), excepto el etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente o cuando las fuerzas de seguridad categoricen datos biométricos.
- Puntuación social, es decir, **evaluar o clasificar a individuos o grupos basándose en comportamientos sociales o rasgos personales**, causando un trato perjudicial o desfavorable a esas personas.
- **Evaluar el riesgo de que un individuo cometa delitos penales basándose únicamente en perfiles o rasgos de personalidad**, excepto cuando se utilice para aumentar las evaluaciones humanas basadas en hechos objetivos y verificables directamente relacionados con la actividad delictiva.
- **Compilación de bases de datos de reconocimiento facial** mediante el raspado no selectivo de imágenes faciales de Internet o de grabaciones de CCTV.
- **Inferir emociones en lugares de trabajo o centros educativos**, salvo por razones médicas o de seguridad.
- **Identificación biométrica remota "en tiempo real" en espacios públicos para las fuerzas de seguridad** excepto en:
 - búsqueda de personas desaparecidas, víctimas de secuestros y personas víctimas de la trata de seres humanos o la explotación sexual;
 - prevenir una amenaza sustancial e inminente para la vida, o un ataque terrorista previsible; o
 - identificar a sospechosos de delitos graves (por ejemplo, asesinato, violación, robo a mano armada, tráfico de estupefacientes y armas ilegales, delincuencia organizada y delitos contra el medio ambiente, etc.).



La Comisión Europea ha publicado las Directrices sobre prácticas prohibidas de inteligencia artificial (IA), tal como se definen en el Reglamento de IA.

> Alto riesgo

La mayor parte del Reglamento está enfocado a regular los sistemas de IA de alto riesgo, también conocidos por como **HRAIS** (High Risk AI Systems), que **pueden suponer un perjuicio para la salud, la seguridad o los derechos fundamentales de las personas**, contenidos en la **Carta de los Derechos Fundamentales de la UE**. Se dividen en dos categorías:

- > Los **componentes de seguridad de los productos** contemplados en la legislación sectorial de la Unión cuando estén sujetos a una evaluación de la conformidad por terceros con arreglo a esa legislación sectorial, recogidos en el anexo I del Reglamento de IA.



- > Los **sistemas de IA pertenecientes a ocho ámbitos específicos**, recogidos en el anexo III del Reglamento de IA, que son:
 - > **Biometría no prohibida.** Sistemas de identificación biométrica a distancia, excluida la verificación biométrica que confirma que una persona es dice ser. Sistemas de categorización biométrica que infieren atributos o características sensibles o protegidos. Sistemas de reconocimiento de emociones.
 - > **Infraestructuras críticas:** Componentes de seguridad en la gestión y explotación de infraestructuras digitales críticas, tráfico rodado y suministro de agua, gas, calefacción y electricidad.
 - > **Educación y formación profesional.** Sistemas de IA que determinan el acceso, la admisión o la asignación a instituciones educativas y de formación a profesionales a todos los niveles. Evaluación de los resultados del aprendizaje, incluidos los utilizados para dirigir el proceso de aprendizaje del alumno. Evaluar el nivel de educación adecuado para un individuo. Supervisión y detección de comportamientos prohibidos de los alumnos durante los exámenes.
 - > **Empleo, gestión de trabajadores y acceso al autoempleo.** Sistemas de IA utilizados para el reclutamiento o la selección, en particular anuncios de empleo específicos, análisis y filtrado de solicitudes, y evaluación de candidatos. Promoción y rescisión de contratos, asignación de tareas en función de rasgos de personalidad o características y comportamiento, y seguimiento y evaluación del rendimiento.
 - > **Acceso y disfrute de servicios públicos y privados esenciales.** Sistemas de IA utilizados por las autoridades públicas para evaluar el derecho a prestaciones y servicios, incluida su asignación, reducción, revocación o recuperación. Evaluación de la solvencia, excepto para detectar fraudes financieros. Evaluación y clasificación de llamadas de emergencia, incluida la priorización de envíos de la policía, los bomberos, la asistencia médica y los servicios de triaje de pacientes urgentes. Evaluación de riesgos y tarificación de seguros de salud y de vida.

- **Aplicación de la ley.** Sistemas de IA utilizados para evaluar el riesgo de una persona de convertirse en víctima de un delito. Polígrafos. Evaluación de la fiabilidad de las pruebas durante investigaciones o procesos penales. Evaluación del riesgo de delincuencia o reincidencia de una persona no basada únicamente en la elaboración de perfiles o en la evaluación de rasgos de personalidad o comportamientos delictivos anteriores. Elaboración de perfiles durante detecciones, investigaciones o enjuiciamientos penales.
- **Gestión de la migración, el asilo y el control fronterizo.** Polígrafos. Evaluaciones de migración irregular o riesgos sanitarios. Examen de solicitudes de asilo, visados y permisos de residencia, y reclamaciones relacionadas con la admisibilidad. Detección, reconocimiento o identificación de personas, excepto verificación de documentos de viaje.
- **Actividad jurisdiccional y procesos democráticos.** Sistemas de IA utilizados en la investigación e interpretación de hechos y en la aplicación de la ley a hechos concretos o utilizados en la resolución alternativa de conflictos. Influencia en los resultados de elecciones y referendos o en el comportamiento electoral, excluidos los productos que no interactúan directamente con las personas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas.

Los sistemas de alto riesgo **han de cumplir determinados requisitos y se imponen obligaciones específicas tanto a los proveedores como a los responsables de despliegue de los sistemas.**

¿Cuáles son los requisitos para los sistemas de alto riesgo?

El Reglamento impone una **serie de obligaciones que los sistemas de IA de alto riesgo deben cumplir:**

➤ Sistema de Gestión de Riesgos

El **proveedor de un sistema de IA de alto riesgo** deberá **establecer, aplicar, documentar y mantener un sistema de gestión de riesgos**. Se identificarán y valorarán amenazas, se adoptarán medidas de mitigación, y se monitorizarán sus efectos, en un ciclo de mejora continua que se prolongará durante todo el ciclo de vida del sistema.

➤ Datos y Gobernanza de Datos

Los sistemas de IA de alto riesgo que utilizan técnicas de entrenamiento de modelos con datos se desarrollarán a partir de **conjuntos de datos de entrenamiento, validación y prueba que se someterán a prácticas adecuadas de gobernanza y gestión de datos**. Entre estas prácticas destacan:

- Elegir un diseño adecuado.
- Adoptar los procesos adecuados de recopilación de datos.
- Operaciones de tratamiento de datos oportunas, como anotación, etiquetado, depuración, enriquecimiento y agregación.
- Análisis y depuración de los posibles sesgos.
- Evaluación previa de disponibilidad, cantidad y adecuación de los datasets necesarios.

> Documentación Técnica

Los **proveedores deben suministrar a los usuarios y a las autoridades documentación técnica del sistema de IA**. La documentación demostrará que se cumplen los requisitos del Reglamento que estamos comentando, y explicará cómo comprobarlo.

> Registros

Los sistemas generarán **permanentemente registros**, o logs, que tienen que garantizar un nivel de trazabilidad de su funcionamiento adecuado para su finalidad prevista.

Además, durante toda la vida del sistema, se recogerán y analizarán evidencias para asegurar que el sistema funciona normalmente y cumple las disposiciones del Reglamento, a través de un proceso continuo de monitorización post-comercialización.

> Transparencia y Comunicación de Información a los Usuarios

Los sistemas deben diseñarse de una forma que se garantice a los usuarios un funcionamiento suficientemente transparente, es decir, que les permita comprenderlo y utilizarlo adecuadamente. Con el sistema, **el proveedor tendrá que proporcionar instrucciones de uso con información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios**.

> Vigilancia Humana

Los sistemas se **diseñarán y desarrollarán de forma que su uso pueda ser supervisado por personas físicas**. Esta vigilancia debe prevenir o minimizar los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir tanto si el HRAIS se utiliza conforme a su finalidad prevista como si se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persisten a pesar de aplicar los demás requisitos.

> Precisión, Solidez y Ciberseguridad

Los sistemas de IA de alto riesgo se diseñarán, desarrollarán y mantendrán de forma que alcancen, según su finalidad prevista, **un nivel adecuado de precisión de los resultados**. Las **instrucciones de uso que los acompañarán indicarán los niveles de precisión y los parámetros de precisión pertinentes**.

Los sistemas deberán **ofrecer un grado adecuado de resiliencia ante las limitaciones en los sistemas o en el entorno en el que estos funcionan** (p. ej., errores, fallos, incoherencias o situaciones inesperadas).

Los sistemas **han de diseñarse de forma que sean resistentes a los intentos de terceros de aprovechar las vulnerabilidades del sistema**, en particular de las vulnerabilidades específicas de los sistemas de IA, como pueden ser la corrupción intencionada de los datos de entrenamiento para manipular las salidas que producen.



Por lo tanto, podemos concluir que, previo a la **comercialización de un sistema de inteligencia artificial de alto riesgo**, en el mercado de la UE, **los proveedores deberán someterlo a una evaluación de conformidad**. Esto les permitirá demostrar que su sistema cumple con los requisitos obligados de una inteligencia artificial de confianza. Adicionalmente también deben de cumplir con las siguientes obligaciones:

- Contar con un **sistema de gestión de calidad**.
- Mantener la **documentación del sistema**.
- Custodiar los **registros de actividad**.
- **Colaborar con las autoridades** demostrando cumplimiento, y **notificando incumplimientos** y riesgos detectados.

En cuanto a las **obligaciones de las personas usuarias (responsables del despliegue** según la nomenclatura contemplada en el ámbito de aplicación del Reglamento) son: supervisión humana, monitorizar los sistemas, guardar registros y colaborar con las autoridades.

➤ Riesgo limitado

Para determinados sistemas de inteligencia artificial, como cuando **exista riesgo claro de manipulación**, por ejemplo, mediante el uso de robots conversacionales o **ultra falsificación**, el Reglamento de IA establece **obligaciones específicas de transparencia para que los usuarios sean conscientes de que están interactuando con una máquina**.

➤ Riesgo mínimo

La mayoría de los demás sistemas de inteligencia artificial pueden programarse y utilizarse con arreglo a la legislación vigente, **sin obligaciones jurídicas adicionales**. De forma voluntaria, los proveedores de estos sistemas pueden optar por aplicar los requisitos de una inteligencia artificial y adherirse a códigos de conducta facultativos. Algunos ejemplos de ellos son aplicaciones de IA en **videojuegos, o filtros de spam para el correo electrónico**.



Como respuesta al compromiso con el Reglamento europeo IA, en España se ha definido una **Estrategia Nacional de Inteligencia Artificial**, un plan diseñado para desarrollar y expandir, a través de planes sectoriales, estatales y otras estrategias regionales, el uso de la inteligencia artificial de forma transparente y ética, y está enfocado a facilitar su uso en los sectores público y privado. El impulso de la inteligencia artificial también está contemplado en la **Agenda España Digital 2026** como un elemento clave de carácter transversal para transformar el modelo productivo e impulsar el crecimiento de la economía española.



En España ya se ha creado, por el Real Decreto 729/2023, de 22 de agosto, la **Agencia Española de Supervisión de Inteligencia Artificial**, que ejerce las funciones de inspección, comprobación, y sanción de conformidad con el Reglamento de IA. En definitiva, será la principal autoridad supervisora nacional.

Finalmente, el pasado 11 de marzo de 2025, se ha aprobado en el Consejo de Ministros el anteproyecto de la **Ley de gobernanza de la Inteligencia Artificial (IA)**, una normativa que busca garantizar un uso ético, inclusivo y beneficioso de la IA, alineado con el Reglamento Europeo de IA ya en vigor. Este marco regulador tiene como objetivo impulsar la innovación mientras protege los derechos fundamentales y refuerza la seguridad en el desarrollo y aplicación de la IA. El anteproyecto de ley, que se tramitará por la vía de urgencia, deberá completar los trámites preceptivos antes de su aprobación definitiva y envío a las Cortes Generales.

3. Situación actual de la IA y la digitalización en el ámbito laboral

La **Oficina Europea de Estadística (Eurostat)** ha publicado a principios del 2025, su **informe anual sobre el uso de las TIC y el comercio electrónico en las empresas europeas**, a partir de los datos obtenidos en la encuesta de 2024. Según este informe, en el año 2024, el número de empresas con 10 o más empleados y autónomos, en Europa, que utilizó tecnologías de Inteligencia Artificial para llevar a cabo sus negocios **aumentó hasta el 13,5%**, respecto al 8% registrado en 2023. Dichas empresas utilizaron al menos una de las siguientes IA:

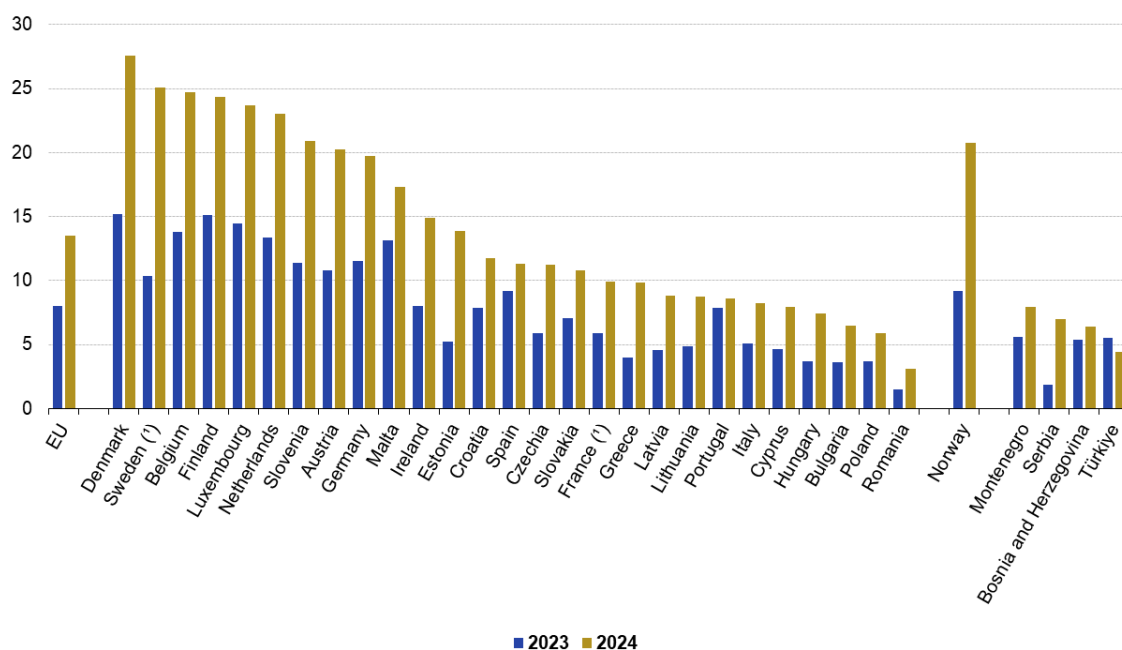
- Tecnologías que analizan el lenguaje escrito (minería de textos).
- Tecnologías que convierten el lenguaje hablado en un formato legible por máquina (reconocimiento de voz).
- Tecnologías que generan lenguaje escrito o hablado (generación de lenguaje natural).
- Tecnologías que identifican objetos o personas basándose en imágenes (reconocimiento de imágenes, procesamiento de imágenes).
- Aprendizaje automático (por ejemplo, aprendizaje profundo) para el análisis de datos.
- Tecnologías que automatizan diferentes flujos de trabajo o ayudan en la toma de decisiones (automatización de procesos robóticos de software basado en IA).

- Tecnologías que permiten a las máquinas moverse físicamente observando su entorno y tomando decisiones autónomas.

La comparación de empresas que utilizan al menos una tecnología de IA entre los países de la UE (Figura 1) muestra que la proporción de empresas que utilizan IA osciló entre el 3,07% y el 27,58%. **En 2024, todos los Estados miembros de la UE registraron una mayor proporción de empresas que utilizaban tecnologías de IA en comparación con 2023.**

Extrapolando a **España**, en 2024 el **11,31%** de las empresas han utilizado tecnologías de IA, frente al 9,18% en 2023.

Enterprises using AI technologies, 2023 and 2024
(% of enterprises)



(*) 2023: Break in the time series.

Source: Eurostat (online data code: isoc_eb_ai)

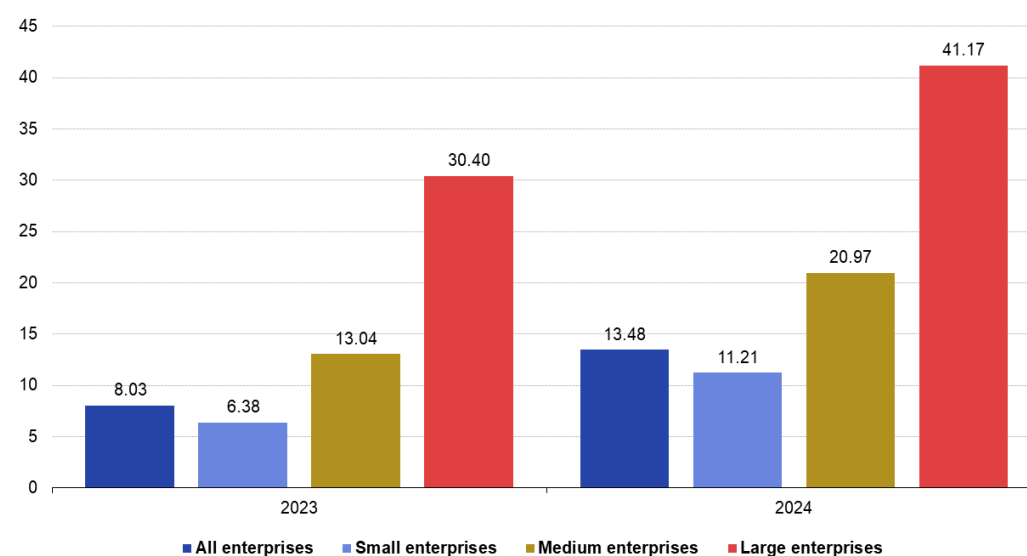
eurostat 

Figura 1. Empresas de la UE (por países) que usan IA, comparativa 2023 vs 2024 (%empresas) Fuente: Eurostat

Como se muestra en la Figura 2, **las grandes empresas europeas utilizaron la IA más que las pequeñas y medianas empresas**. En 2024, el 11,21% de las pequeñas empresas, el 20,97% de las medianas empresas y el 41,17% de las grandes empresas utilizaron IA. Esta diferencia podría explicarse, por ejemplo, por la complejidad de implementar tecnologías de IA en una empresa, las economías de escala (es decir, las empresas con mayores economías de escala pueden beneficiarse más de la IA) o los costos (es decir, la inversión en IA puede ser más asequible para las grandes empresas).

Enterprises using AI technologies by size class, EU, 2023 and 2024

(% of enterprises)



Source: Eurostat (online data code: isoc_eb_ai)

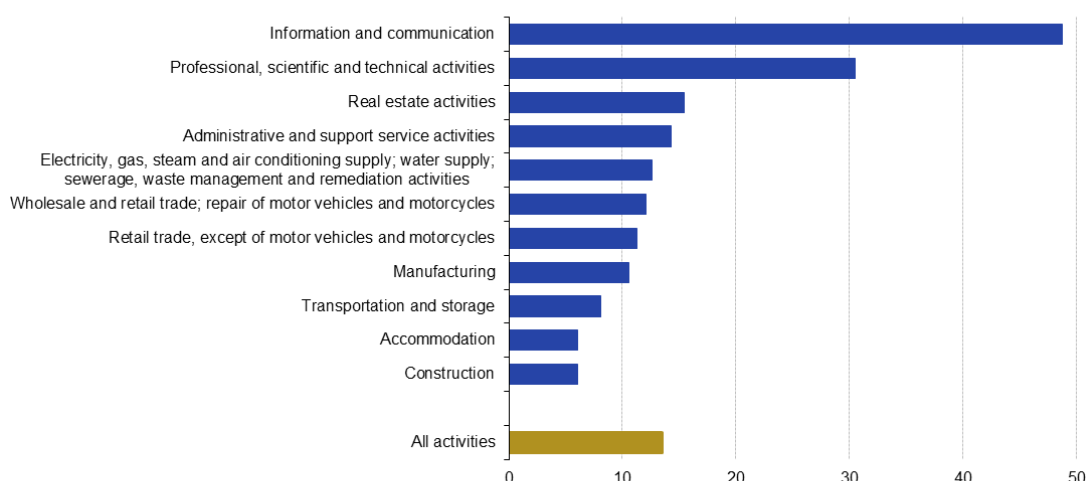
eurostat

Figura 2. Empresas europeas que utilizan tecnologías de IA por clase de tamaño, UE, 2023 y 2024 (% de empresas)
Fuente: Eurostat

Como se muestra en la Figura 3, en algunas **actividades económicas** la IA se utiliza mucho más que en otras. Esto podría indicar que la IA es más relevante para determinadas actividades. En 2024, el **sector de la información y las comunicaciones** (con un 48,72%) y **las actividades de servicios profesionales, científicos y técnicos** (con un 30,53%) destacaron con la mayor proporción de empresas que utilizaron IA. En todas las demás actividades económicas, la proporción de empresas que utilizan IA estuvo por debajo del 16%. Esta oscilaba entre el 15,45% (actividades inmobiliarias) y el 6,09% (alojamiento y construcción).

Enterprises using AI technologies by economic activity, EU, 2024

(% of enterprises)



Source: Eurostat (online data code: isoc_eb_ain2)

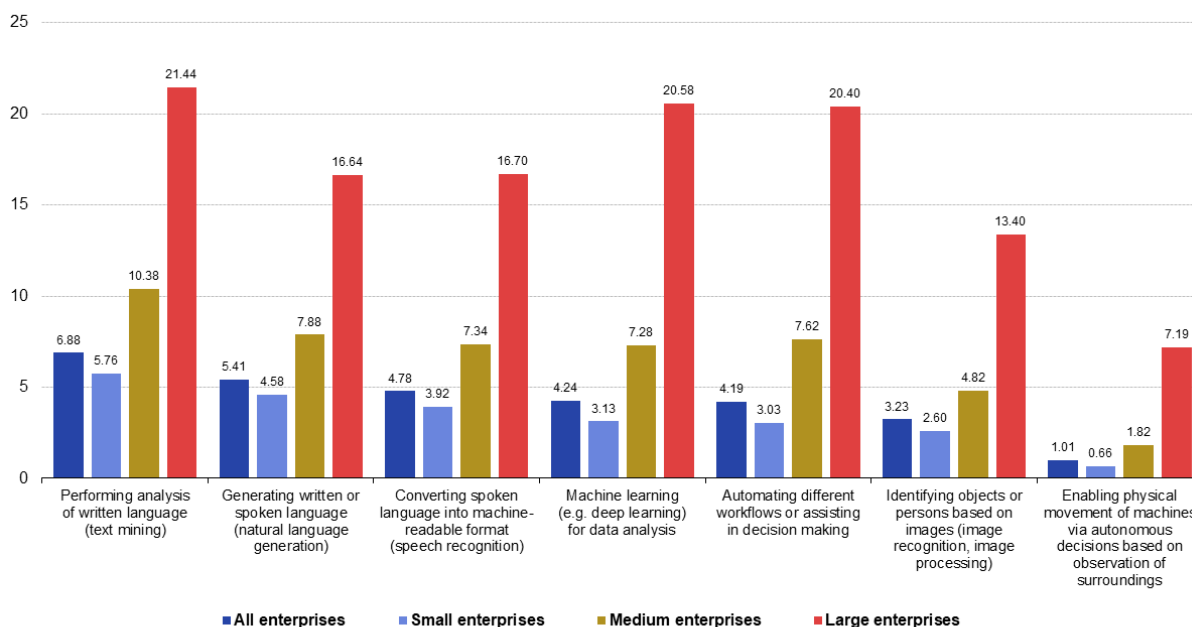
eurostat

Figura 3. Empresas europeas que utilizan tecnologías de IA por actividad económica, UE, 2024 (% de empresas)
Fuente: Eurostat

Las empresas de la UE utilizaron **diferentes tipos de tecnologías de IA**. Como se presenta en la Figura 4, no había ninguna tecnología de IA predominante. Las tecnologías de IA utilizadas con un poco más de frecuencia fueron tecnologías de IA que realizaban **análisis del lenguaje escrito**. En 2024, estas tecnologías de IA fueron utilizadas por el **6,88% de las empresas**. Le siguieron las tecnologías de inteligencia artificial que **generan lenguaje escrito o hablado (generación de lenguaje natural)** con el 5,41% de las empresas. Las tecnologías de inteligencia artificial que convierten el lenguaje hablado en un formato legible por máquina (**reconocimiento de voz**), el **aprendizaje automático** (por ejemplo, aprendizaje profundo) **para el análisis de datos**, las **tecnologías que automatizan diferentes flujos de trabajo o ayudan en la toma de decisiones** y las **tecnologías que identifican objetos o personas basándose en imágenes (reconocimiento de imágenes, procesamiento de imágenes)** fueron utilizadas por entre el 4,78% y el 3,23% de las empresas. El 1,01% de las empresas utilizaron tecnologías de inteligencia artificial que permiten a las **máquinas moverse físicamente observando su entorno y tomando decisiones autónomas** (por ejemplo, vehículos autónomos).

Aunque no hubo una tecnología de IA predominante utilizada por todas las empresas, la Figura 4 muestra una situación diferente **cuando se observa el tamaño de las empresas**, en particular las **grandes empresas**, donde las tecnologías de IA que realizan **análisis del lenguaje escrito (minería de textos)** fueron las tecnologías más utilizadas con un **21,44%**, seguidas por el **aprendizaje automático para el análisis de datos (20,58%)** y las **tecnologías de IA que automatizan diferentes flujos de trabajo o ayudan en la toma de decisiones (20,40%)**. Las tecnologías de IA menos utilizadas fueron las que permiten el movimiento físico de las máquinas mediante decisiones autónomas basadas en la observación del entorno (7,19%).

Enterprises using AI technologies by type of AI technology and size class, EU, 2024
(% of enterprises)



Source: Eurostat (online data code: isoc_eb_ai)

eurostat

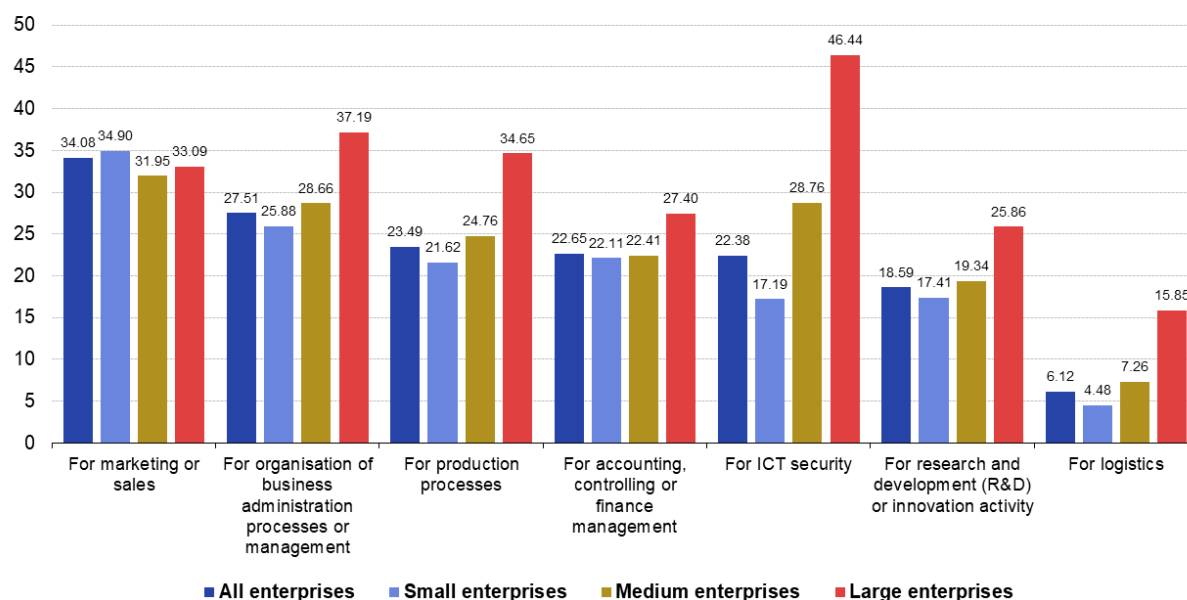
Figura 4. Empresas europeas que utilizan tecnologías de IA por tipo de tecnología de IA y clase de tamaño, UE, 2024 (% de empresas). Fuente: Eurostat

Atendiendo a la **finalidad del uso de las tecnologías IA**, las empresas de la UE utilizaron software o sistemas de inteligencia artificial para diferentes fines. En 2024, el **34,08%** de las empresas que utilizan tecnologías de IA utilizaron estos **software o sistemas para marketing o ventas y el 27,51% para la organización de procesos o gestión de administración empresarial**. El software o los sistemas de IA para logística fueron los que menos se utilizaron, con una proporción del 6,12% de las empresas que utilizan tecnologías de IA (Figura 5).

Los propósitos para los que las empresas utilizaban software y sistemas de IA **difierían según su tamaño**. La mayor diferencia entre las pequeñas y las grandes empresas se registró entre aquellas que utilizaban **software o sistemas de IA para la seguridad de las TIC (46,44% grandes empresas, 17,19% pequeñas empresas)**, seguidas de aquellas que los utilizaban **para procesos de producción (34,65% grandes empresas, 21,62% pequeñas empresas)** y aquellas que los utilizaban **para logística (15,85% grandes empresas, 4,48% pequeñas empresas)** (Figura 5).

Enterprises using AI technologies by type of purpose and size class, EU, 2024

(% of enterprises using at least one AI technology)



Source: Eurostat (online data code: isoc_eb_ai)

eurostat 

Figura 5. Empresas que utilizan tecnologías de IA por tipo de finalidad y clase de tamaño, UE, 2024 (% de empresas que utilizan al menos una tecnología de IA)

Por otro lado, centrándonos en España, de acuerdo con lo detallado en el Informe por país sobre la **Década Digital 2024 en España de la Comisión Europea**, en 2023, **España avanzó notablemente en el uso de la inteligencia artificial (IA) por parte de las empresas**, aunque persisten retos para algunos indicadores relacionados con la digitalización de las empresas, incluida la adopción de la nube. Si bien el número de especialistas en TIC en el empleo sigue siendo bajo, el nivel general de competencias digitales básicas entre la población ha aumentado.

> Dos fortalezas principales o áreas de progreso

> Adopción de la IA por las empresas

España aporta una contribución positiva al objetivo de la Década Digital de la UE y muestra una dinámica muy fuerte. **El 9,2 % de las empresas españolas habían adoptado soluciones de IA en 2023, lo que supera la media de la UE del 8,0 %.** Además, el crecimiento medio anual de España (9,3 %) es casi cuatro veces superior a la media de la UE (2,6 %).

> Competencias digitales básicas

En 2023, el **66,2 % de la población española tenía al menos un nivel básico de capacidades digitales, por encima de la media de la UE del 55,6 %.**

> Dos debilidades principales o áreas a mejorar

> Adopción de la nube por las empresas

España muestra **una dinámica muy limitada en la adopción de los servicios en la nube. El 27,2 % de las empresas españolas utilizan servicios en la nube, muy por debajo de la media de la UE del 38,9 %.** Además, la tasa de crecimiento de España (0,4 %) se sitúa por debajo de la tasa de la UE (7 %).

> Especialistas en TIC

Como porcentaje de la población ocupada total en España, **el 4,4 % son especialistas en TIC, por debajo de la media de la UE del 4,8 %.** Además, el país establece un objetivo inferior a las expectativas de la UE en su hoja de ruta nacional.

Otro estudio **“Uso de inteligencia artificial y Big data en empresas españolas año 2023”** elaborado por el Observatorio Nacional de Tecnología y Sociedad (ONTSI), órgano consultivo adscrito al Ministerio de Asuntos Económicos y Transformación Digital establece que **el 11,8% de las empresas españolas con más de 10 personas trabajadoras ya han adoptado el uso de la IA,** cuatro puntos más que en 2021, para:

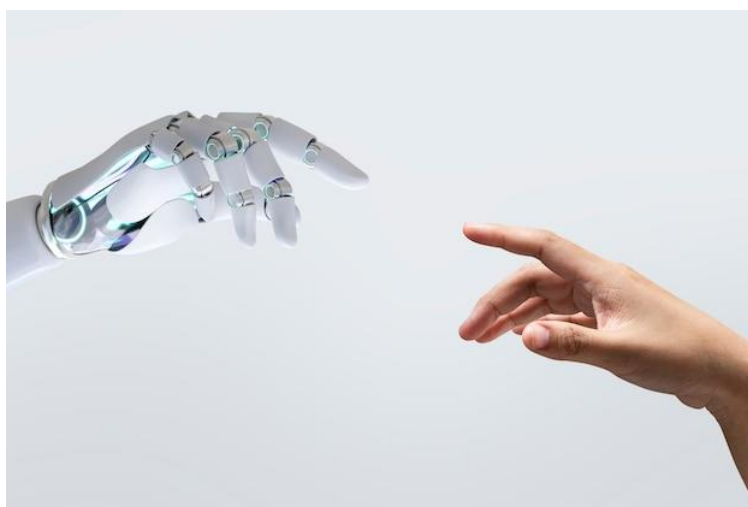
- > El **46,2% automatizar flujos de trabajo y ayudar en la toma de decisiones**
- > El **39,7% identificación de personas y objetos en función de imágenes**
- > En el caso de las **microempresas, el 48% convertir el lenguaje hablado en formato legible.**

En cuanto a sectores de actividad, las empresas españolas cuya actividad se centra en **la información y las comunicaciones (41,9%) y las dedicadas al sector TIC (41,3%)** son las que aglutinan la mayor parte del uso de la IA.

4. Beneficios e inconvenientes del uso de la IA en el ámbito de la PRL

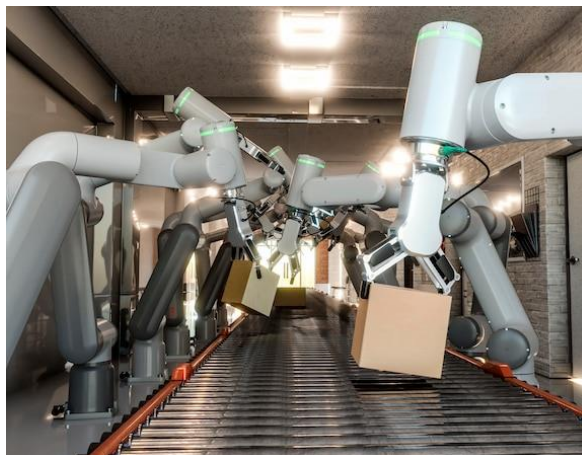
La inteligencia artificial es una herramienta que se utiliza cada vez más en el ámbito de la prevención de riesgos laborales, destinada a **garantizar la seguridad, salud y bienestar de las personas trabajadoras** a través de su **contribución en la creación de entornos laborales más seguros y eficientes**.

- Ofrece soluciones innovadoras que permiten **mejorar la seguridad y el bienestar** de las personas trabajadoras, al ser capaz de analizar enormes volúmenes de datos, consiguiendo: **identificar riesgos específicos, simular actividades peligrosas y proponer medidas preventivas con un alto nivel de precisión**.
- **Permite valorar la eficacia de las acciones en materia de seguridad y salud laboral** y plantear puntos de mejora.
- Al identificar patrones en datos históricos de accidentes, la IA tiene un enfoque proactivo, puede **predecir qué situaciones tienen mayor probabilidad de ocurrir y recomendar acciones para evitarlas**. Se consigue, así, **reducir el absentismo laboral y aumentar la productividad**.
- Además, **personaliza la prevención de riesgos**. Gracias a su capacidad de aprendizaje, **adapta soluciones a las características individuales de cada persona trabajadora**. Esta personalización no solo mejora la eficacia de las medidas preventivas, sino que también se consigue fomentar una mayor confianza y compromiso por parte de los trabajadores y trabajadoras.



- **Administra y gestiona las tareas, personaliza las rutinas de trabajo ajustándolas a las capacidades individuales** de cada persona trabajadora, considerando factores como su nivel de experiencia, sus habilidades específicas y su estado de salud, **aumentando el aprovechamiento de los recursos humanos y la satisfacción laboral**.
- **Analiza las pautas de comunicación del personal**, siendo capaz de **evaluar el riesgo de acoso o desgaste profesional (burnout)**.
- Del mismo modo, **facilita la implementación de programas de promoción de la salud**, a través de **planes personalizados de bienestar** en base a las características individuales de las personas trabajadoras.

- **Automatiza los procesos, eliminando o minimizando la exposición a ciertos riesgos.** Integra **robots /sistemas robóticos colaborativos para tareas peligrosas, evitando la intervención** de las personas trabajadoras, **consiguiendo eliminar la exposición a riesgos potenciales** (desde caídas en altura, acceso a espacios confinados, riesgos derivados de uso de máquinas, exposición a agentes físicos y/o químicos, sobreesfuerzos por manipulación manual de cargas, por mantenimiento de posturas forzadas o ejecución de movimientos repetitivos, etc.).



- Además, la IA permite **monitorizar los datos, supervisando las condiciones de trabajo y generando alertas inmediatas que ayudan a evitar accidentes.**
 - Los **sistemas de monitoreo en tiempo real** pueden alertar sobre condiciones peligrosas como la postura, los niveles de estrés, etc. El potencial de la monitorización es enorme pudiendo **mejorar la vigilancia y detectar no solo riesgos del entorno o los que se encuentra expuesta la persona**, sino que, en base a la observación de los comportamientos de las personas trabajadoras pueden, también, **prevenirse situaciones que afecten al clima laboral de la organización, casos de acoso, etc.**
 - **Permite detectar anomalías y alertar al personal sobre peligros inminentes.**
- En **términos de formación**, a través de la IA las personas trabajadoras aprenden a manejar situaciones de riesgo. A través de la **simulación en realidad virtual**, las personas trabajadoras pueden **experimentar escenarios peligrosos en un entorno controlado, mejorando su capacidad de respuesta ante emergencias reales.** Esto no solo optimiza la formación, sino que también reduce los costes asociados a la necesidad de impartir formaciones constantemente, sobre todo formaciones iniciales individualizadas de nuevas incorporaciones.



Sin embargo, junto a estos beneficios, el uso de la IA también plantea **importantes desafíos**.

- Uno de los más destacados es el **impacto psicosocial** que puede tener sobre las personas trabajadoras. La monitorización constante, facilitada por cámaras y sensores inteligentes, puede generar una **sensación de vigilancia permanente**, lo que podría ser percibida como una **invasión de la privacidad**, especialmente si no existe una comunicación e información sobre cómo se recopilan y utilizan los datos. Esto puede hacer aumentar el estrés y puede afectar negativamente el bienestar emocional de los trabajadores y trabajadoras. Además, los sistemas inteligentes en IA son capaces de descubrir el potencial máximo alcanzable por cada persona trabajadora y exigirlo, pueden generar una valoración global del rendimiento de una persona, estableciendo distintas categorías o perfiles en la empresa, dando lugar a un **entorno competitivo**. Como consecuencia, es posible que las personas no puedan tomar pausas o descansos cuando sea necesario, lo que provoca estrés, fatiga y un mayor riesgo de accidentes, trastornos musculoesqueléticos, etc. El **aumento de la supervisión y la calificación del rendimiento** también se utilizan para incentivar y penalizar/disciplinar a las personas. Se debe **fomentar la consulta y participación de las personas trabajadoras en todo el proceso de implantación y uso de sistemas inteligentes**. Para ello se deben establecer **canales de comunicación** en la empresa que facilite dicha actuación y permita mantener a la plantilla informada en diversas cuestiones derivadas del uso de la IA.

Para más información sobre cómo mejorar y establecer canales de comunicación en la empresa, desde **Umivale Activa** hemos desarrollado una **Guía de Comunicación efectiva en PRL**. Puede descargarla a través del siguiente [enlace](#).

Del mismo, desde **Umivale Activa** promovemos el **bienestar emocional** de las personas trabajadoras. Para más información sobre las herramientas desarrolladas acceda al siguiente [enlace](#).

- Por otra parte, la dependencia excesiva de la IA en los procesos laborales plantea el riesgo de una **pérdida gradual de habilidades humanas y descualificación**. La automatización también podría llevar a la reducción de puestos de trabajo, generando tensiones sociales y económicas.
- Los avances constantes de la tecnología digital también implican un **continuo plan de formación para garantizar una correcta capacitación y desarrollo de habilidades de la persona trabajadora** en el uso de dichas aplicaciones. Cuando esta medida no se implanta correctamente las personas trabajadoras ofrecen **resistencia al cambio**.
- La implantación de dicha tecnología implica unos **elevados costes de implantación** que no están al alcance de muchas empresas.
- Un aspecto ético crucial relacionado con la IA en la PRL es la posible perpetuación de **sesgos en los algoritmos**. Aunque estas herramientas son diseñadas para ser objetivas, los datos que alimentan su aprendizaje pueden contener prejuicios históricos que se reflejan en **decisiones discriminatorias, como la exclusión de ciertos grupos de trabajadores y trabajadoras en procesos de selección**. Esto subraya la importancia de la **supervisión humana**, para garantizar que las **decisiones algorítmicas sean adecuadas, justas y equitativas**. Frente a estos desafíos, la Organización Mundial de la Salud (OMS) ha establecido una serie de principios rectores que buscan asegurar un **uso responsable y ético de la IA** en el ámbito laboral. Estos incluyen **garantizar la transparencia en el uso de datos, preservar la autonomía de las personas trabajadoras y promover la equidad en el acceso y la implementación de estas tecnologías**.

Además, la OMS enfatiza la importancia de **capacitar a las personas trabajadoras y a los responsables en la gestión de la IA**, para que esta sea utilizada de manera **complementaria y no como un sustituto de las decisiones humanas**.

- En el contexto de la prevención de riesgos laborales, la IA también ha contribuido a abordar nuevos desafíos que surgen con el avance tecnológico, conocidos como **riesgos emergentes**. Entre ellos, el **tecnoestrés** destaca como un problema creciente, manifestándose tanto en la dificultad para adaptarse a las nuevas tecnologías como en la dependencia excesiva de las mismas. Este fenómeno, junto con la **tecnofatiga y la tecnoadicción**, pone de manifiesto la necesidad de un enfoque equilibrado en la implementación de estas herramientas, que considere tanto las oportunidades como los riesgos asociados.



Desde **Umivale Activa**, ponemos a su disposición materiales divulgativos sobre el tecnoestrés con el objetivo de conocer este riesgo emergente y poder gestionarlo tanto dentro como fuera de las organizaciones. Para más información acceda al siguiente [enlace](#).

La conexión constante que implican las tecnologías digitales puede conducir a una sobrecarga de trabajo, falta de conciliación entre el plano laboral y familiar/social, afectando a la salud física y mental de las personas trabajadoras. Del mismo modo, desde **Umivale Activa**, se han desarrollado una serie de materiales con el objetivo de garantizar una desconexión digital adecuada. Para más información acceda al siguiente [enlace](#).

- **Falta de interacción** entre las personas trabajadoras, por automatización de los procesos, conduciendo a un **aislamiento social**.
- **Falta de transparencia en la implantación de sistemas IA**, generando ansiedad y frustración en las personas trabajadoras al desconocer qué datos se recopilan, cómo se procesan y con qué finalidad.
- Por otra parte, el uso de sistemas inteligentes en IA **puede reducir drásticamente el control y la autonomía en el trabajo**, anulando las iniciativas y decisiones por parte de las personas trabajadoras sobre cómo ejecutar su trabajo, lo que puede provocar frustración y estrés.



- La IA requiere el acceso a grandes volúmenes de datos, planteando grandes **riesgos relacionados con la seguridad y privacidad de las personas trabajadoras**. El **tratamiento inadecuado de estos datos puede conllevar a violaciones de la privacidad y exposición a riesgos de ciberseguridad**.

Con todo, llegamos a la conclusión de que la inteligencia artificial ofrece la gran ventaja de mejorar la seguridad y la salud en el trabajo, determinando soluciones innovadoras y eficaces para prevenir riesgos. Sin embargo, su implementación debe hacerse correctamente, asegurando un **equilibrio entre los beneficios tecnológicos y la protección de los derechos y el bienestar de las personas trabajadoras** a través de un **enfoque ético y humano**.

5. Principios éticos de la inteligencia artificial

Un **sistema IA fiable**, se apoya sobre tres pilares: debe ser **legal** (cumplir la legislación aplicable), **ético** (respetar los principios éticos), y **robusto** (funcionar de manera segura, para no provocar daños accidentales).

La ética en la inteligencia artificial (IA) se basa en **principios y normas para el desarrollo y aplicación de la IA de manera responsable y ética**. Esto implica considerar cómo se diseñan los algoritmos, cómo se recopilan y utilizan los datos, y cómo se aplican los sistemas de IA en diferentes contextos.

En noviembre de 2021, la UNESCO elaboró la primera norma mundial sobre la ética de la IA: la "Recomendación sobre la ética de la inteligencia artificial". La Recomendación se basa en **cuatro valores fundamentales que sientan las bases para que los sistemas de IA trabajen por el bien de la humanidad, las personas, las sociedades y el medio ambiente**.

Especialmente, el uso de dichas tecnologías **no debe comprometer los valores y los derechos fundamentales de las personas**.



Por eso a continuación se detallan **10 principios éticos**, establecidos en dicha Recomendación centrados en los **derechos humanos**:

➤ Proporcionalidad e inocuidad

El uso de sistemas de IA **no debe ir más allá de lo necesario para alcanzar un objetivo legítimo**. La evaluación de los riesgos debe utilizarse para prevenir los daños que puedan derivarse de usos ilegítimos. La IA **debe utilizarse para el beneficio de las personas y la sociedad en general**. Se debe priorizar la seguridad, la salud, el bienestar humano, la equidad y el interés público en todas las aplicaciones de la IA. Los sistemas de IA deben contribuir a mejorar la calidad de vida y las condiciones de trabajo de las personas trabajadoras.

> Seguridad y protección

Los daños no deseados (riesgos de seguridad) y las vulnerabilidades a los ataques (**riesgos de protección**) deberían **ser evitados y tomados en consideración**.

> Derecho a la intimidad y protección de datos

La privacidad se refiere a la protección de los datos personales y la información confidencial en el contexto de la IA. La privacidad debe **protegerse y promoverse** a lo largo de todo el ciclo de vida de la IA. También deben **establecerse marcos adecuados de protección de datos**. Es esencial que los sistemas de IA respeten la privacidad de los individuos y cumplan con las regulaciones y políticas de protección de datos. Esto implica obtener el consentimiento informado de los usuarios y garantizar la seguridad y confidencialidad de los datos utilizados.

> Gobernanza y colaboración adaptativas y de múltiples partes interesadas

En el uso de datos, deben **respetarse el derecho internacional y la soberanía nacional**. La **participación de diversas partes interesadas** a lo largo del ciclo de vida de los sistemas de IA es **necesaria** para el desarrollo de enfoques inclusivos de gobernanza.

> Responsabilidad y rendición de cuentas

Los sistemas de IA deben ser **auditables y trazables**. Deben existir mecanismos de supervisión, evaluación de impacto, auditoría y diligencia debida para evitar conflictos con las normas de derechos humanos y amenazas al bienestar medioambiental. La responsabilidad se relaciona con la atribución de responsabilidad por las decisiones y acciones de los sistemas de IA. Es importante establecer mecanismos para determinar quién es responsable en caso de daños o consecuencias negativas causadas por la IA. **Los desarrolladores, proveedores y usuarios de los sistemas deben de asumir la responsabilidad de las decisiones y acciones de estos sistemas**. Se deben establecer mecanismos adecuados para atribuir responsabilidad en caso de daños o consecuencias negativas causadas por la IA. La **rendición de cuentas es esencial para promover la confianza y la responsabilidad ética en el desarrollo y uso de la IA**.

> Transparencia y explicabilidad

El despliegue ético de los sistemas de IA depende de su transparencia y explicabilidad. El nivel de transparencia y explicabilidad debe ser adecuado al contexto. Es importante que los algoritmos y modelos de IA sean **comprensibles y explicables**, de manera que las decisiones tomadas por estos sistemas puedan ser comprendidas y evaluadas por los usuarios y las partes afectadas. La transparencia también implica **proporcionar información clara sobre cómo se utilizan los datos y cómo se toman las decisiones**.

> Supervisión y decisiones humanas

Los Estados Miembros deberían **velar** por que siempre sea posible atribuir la responsabilidad ética y jurídica a personas físicas o a entidades jurídicas existentes. **Se debe asegurar que el desarrollo y uso de las tecnologías IA sea responsable, justa y beneficiosa para las personas, respetando sus derechos humanos.**

> Sostenibilidad

Las tecnologías de IA deben evaluarse en función de su **impacto en la "sostenibilidad"**, entendida como un conjunto de objetivos en constante evolución, incluidos los establecidos en los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas.



> Sensibilización y educación

La sensibilización y la comprensión del público respecto de la IA y el valor de los datos deberían **promoverse mediante una educación abierta y accesible, la participación cívica, las competencias digitales y la capacitación, y la alfabetización mediática e información.**



> Equidad y no discriminación

Los actores de la IA deberían **promover la justicia social, salvaguardar la equidad y luchar contra todo tipo de discriminación**, adoptando un enfoque inclusivo para garantizar que los beneficios de la IA sean accesibles para todos. La justicia implica **garantizar que los beneficios y los riesgos de la IA se distribuyan de manera equitativa** en la sociedad. Es importante **evitar la discriminación y asegurarse de que los sistemas de IA no refuercen sesgos o desigualdades existentes**. Esto implica considerar la diversidad de datos y perspectivas durante el desarrollo de la IA, así como abordar posibles sesgos en los conjuntos de datos utilizados.

6. Gestión de la PRL en la implantación de la IA y otros algoritmos

A la hora de llevar a cabo la **implantación de un sistema inteligente en la empresa**, debe llevarse a cabo de **forma transparente, comprensible y con enfoque motivador, garantizando la igualdad de acceso a la información y a la participación de todas personas trabajadoras, integrándose en todos los sistemas de gestión empresarial, incluido el sistema de gestión preventiva.**

Para que dicha **integración sea efectiva**, dicha implantación debe realizarse en los siguientes pasos:

- **Análisis y realización de pruebas exhaustivas del sistema inteligente que se quiere implantar.** Esto implica un estudio de cómo funciona (en todas sus fases desde recopilación de datos hasta toma de decisiones) el/los algoritmo/s que aplica dicho sistema, poniéndolo a prueba antes de su implantación, para identificar posibles **riesgos emergentes** derivados de su uso que puedan comprometer la seguridad, posibles **sesgos de discriminación** y riesgos que puedan comprometer **la privacidad** de las personas trabajadoras derivado del tratamiento de datos.
- **Revisar y/o modificar la evaluación de riesgos de la empresa**, aplicando cuando se requiera, **nuevas medidas preventivas, enfocadas al control técnico y organizativo** de las nuevas condiciones de trabajo. Establecer una planificación de implantación de dichas medidas, estableciendo una prioridad de plazos y responsables de ejecución.
- **Establecimiento de nuevos procedimientos e instrucciones de trabajo**, o revisión de los ya existentes, teniendo en cuenta los distintos procesos y actividades que se ven afectados por la implantación de dicho sistema.
- Garantizar la **consulta y participación de todas las personas trabajadoras en todas las etapas de implantación de un sistema inteligente**. De esta manera se consigue que las personas trabajadoras se sientan involucradas y comprometidas desde el principio hasta el fin de la implantación. De esta manera se consigue mitigar la resistencia al cambio, abordando proactivamente las preocupaciones de los trabajadores y trabajadoras. Se deberá informar sobre:
 - los riesgos emergentes derivado del uso del sistema implantado
 - el propósito y uso del sistema
 - el uso de los datos (como se recopilan, que tipo de datos se recopilan, como se almacenan los datos para mantenerlos seguros, para qué se utilizan los datos, etc.)
 - las responsabilidades derivadas del uso del sistema
 - etc.
- **Formación e información** a las personas trabajadoras de los riesgos derivados del uso del sistema a implantar y de las medidas preventivas que se deben adoptar. Dicha actuación tiene la finalidad de **capacitar y dotar de suficientes habilidades** a la persona trabajadora para una interacción segura con el sistema, sabiendo cómo se utiliza, que datos se manejan y su deber de protección, su finalidad y la aplicación de medidas oportunas ante posibles riesgos que se presenten.
- **Garantizar la vigilancia de la salud de las personas trabajadoras** que trabajan con sistemas inteligentes con el fin de determinar y controlar cómo afectan dichas tecnologías en su salud (por ejemplo, visión derivadas de uso de pantallas, gafas de realidad virtual, etc.).

- **Supervisión continua y seguimientos periódicos** de las medidas implantadas para verificar el **uso correcto y seguro** de los sistemas inteligentes, llevando a cabo los ajustes o mejoras necesarias.
- Todo ello, bajo la premisa de unos **principios éticos derivados del uso de la IA** en el que se adopte un compromiso por todas las partes implicadas en el desarrollo e implantación de un sistema inteligente, de tal manera que se obtenga el mayor beneficio tecnológico, preservando los derechos humanos y laborales de las personas trabajadoras:
 - **Transparencia y comprensión**, por parte de las personas trabajadoras, de la toma de decisiones del sistema e interpretación de resultados.
 - **Accesibilidad a la información.**
 - **Protección de datos, garantizando la privacidad de las personas trabajadoras.**
 - **Consentimiento informado de la persona trabajadora.**
 - **Diseño centrado en el humano**, herramienta complementaria para enriquecer el potencial de la persona trabajadora, no sustitutoria.
 - **Prevención de sesgos algorítmicos, evitando decisiones discriminatorias o injustas.**
 - **Responsabilidad de las distintas partes intervinientes** en el desarrollo y uso de dichos sistemas, incluyendo mecanismos de rendición de cuentas en caso de incidentes o daños.
 - **Derechos de autor y propiedad intelectual**, asegurándose que el sistema implantado no usa información sin permiso de explotación (revisar las declaraciones y garantías realizadas por el proveedor) con el fin de evitar riesgos en materia de infracción de derechos de terceros.



7. Principales aplicaciones de la IA y algoritmos en PRL

A continuación, detallamos algunos ejemplos de los **sistemas inteligentes más utilizados en el ámbito preventivo**, mostrando sus **principales aplicaciones, factores de riesgos** que comportan su uso y qué **medidas preventivas** debemos adoptar para mitigar sus efectos.

7.1 Internet de las cosas

El Internet de las Cosas (IoT) es un sistema conformado por varios **dispositivos físicos (objetos, instalaciones, máquinas, personas) conectados a red que tienen la capacidad de enviar datos sin necesidad de intervención humana directa**. Permite conectar los elementos físicos cotidianos con Internet. Los **dispositivos IoT se utilizan para monitorizar una amplia gama de parámetros** (ambientales, el rendimiento de las máquinas, etc.) **convirtiendo fenómenos físicos en datos digitales**. Estos datos **se pueden analizar en tiempo real para identificar y predecir patrones, tendencias y anomalías o fallos**, respondiendo de manera inteligente a dichas condiciones cambiantes de tal manera que puedan ayudar a las empresas a mejorar la seguridad, la salud y el bienestar de sus personas trabajadoras, optimizar sus operaciones y mejorar sus resultados.



Internet de las cosas (IoT)

APLICACIONES EN PRL

Sensores IoT en instalaciones
Equipos de protección individual IoT
Sistemas IoT en equipos de trabajo
Dispositivos portátiles IoT (wearables) en la persona trabajadora
Geolocalización
Drones
Exoesqueletos

FACTORES DE RIESGO

Fiabilidad
Comprometer la integridad física de la persona trabajadora por fallo del dispositivo o caída de la red
Sobrecarga de trabajo por disponibilidad permanente de las personas trabajadoras
Fatiga visual
Factores psicosociales por:
Sensación de vigilancia permanente y pérdida de privacidad
Conectividad y monitorización permanente

MEDIDAS PREVENTIVAS

Selección adecuada de dispositivos IoT
Establecimiento protocolos de uso y mantenimiento de dispositivos IoT
Adaptación ergonómica a la persona trabajadora
Homologación y cumplimiento normativa
Establecimiento de políticas de privacidad en el puesto de trabajo y límites de la monitorización
Descansos y pausas periódicas

7.2 Big Data

El Big Data es una **fuentes enorme de datos difícilmente de procesar, por tecnologías tradicionales, debido a su complejidad y velocidad de crecimiento.**



En el ámbito preventivo, se utiliza para **identificar, predecir y eliminar o reducir los riesgos presentes en el puesto de trabajo, garantizando la seguridad, salud y bienestar de la persona trabajadora.**

Big Data		
<u>APLICACIONES EN PRL</u> Identificación de patrones y tendencias en las que se producen los accidentes de trabajo Análisis predictivo de situaciones de riesgo Formaciones individualizadas Mejora el sistema de gestión PRL al generar informes más precisos Análisis de las sensaciones y preocupaciones de las personas trabajadoras	<u>FACTORES DE RIESGO</u> Falta de transparencia, información y consentimiento de las personas trabajadoras sobre el tratamiento de los datos Garantizar la privacidad y seguridad de los datos Factores psicosociales por: Posible aparición de sesgos discriminatorios Sensación de vigilancia permanente	<u>MEDIDAS PREVENTIVAS</u> Consulta, participación y consentimiento de las personas trabajadoras en el uso de datos Establecimiento de canales de comunicación para recopilar preocupaciones de las personas trabajadoras Garantizar la seguridad y privacidad de datos mediante controles de acceso, encriptación y anonimización. Establecimiento de medidas informáticas que garanticen la seguridad de los datos (firewalls, antivirus, etc.) Supervisión constante para evitar posibles sesgos algorítmicos

7.3 Uso de la IA para gestionar personas trabajadoras

El uso de la IA en la gestión de personas, se basa en la aplicación de algoritmos destinados a **organizar el trabajo de las personas trabajadoras distribuyendo tareas, programando actividades, categorizando puestos de trabajo en función de las habilidades y capacitación de cada trabajador o trabajadora, evaluar el rendimiento de trabajo de los mismos, incluso participando en los procesos de contratación.**



IA EN GESTIÓN DE PERSONAS

APLICACIONES EN PRL

Análisis predictivo de situaciones de riesgo
Formaciones individualizadas
Categorización de puestos de trabajo
Adaptación de tareas y asignación de rutinas a cada persona trabajadora
Análisis de las emociones de las personas trabajadoras

FACTORES DE RIESGO

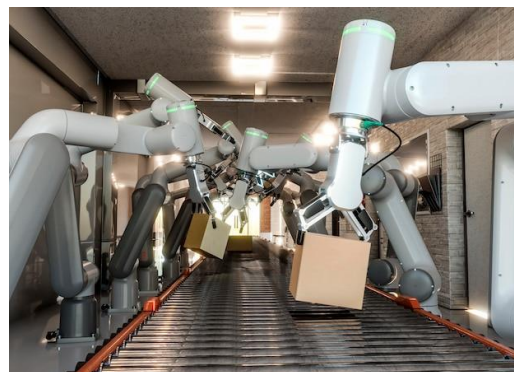
Factores psicosociales por:
Incremento de presión laboral para alcanzar rendimientos predeterminados por los algoritmos
Aumento de la carga mental
Falta de autonomía
Pérdida confianza y desmotivación de las personas trabajadoras
Pérdida de creatividad e innovación
Posible aparición de sesgos discriminatorios
Sensación de vigilancia permanente

MEDIDAS PREVENTIVAS

Fomentar la consulta y participación de las personas trabajadoras
Comprobación de la viabilidad de cumplimiento de los objetivos de rendimiento de las personas predeterminados por los algoritmos
Fomentar el apoyo psicológico y bienestar emocional de las personas trabajadoras
Supervisión constante para evitar posibles sesgos algorítmicos
Supervisión humana en la aplicación de la IA en procesos de gestión de personas trabajadoras
Comprobación del ajuste correcto de las tareas y cargas de trabajo asignadas por los algoritmos, a las distintas personas trabajadoras

7.4 Robots colaborativos

Los robots colaborativos (cobot) están diseñados para **interaccionar con la persona trabajadora, dentro de un espacio colaborativo**. Las tareas más frecuentes que requieren su uso son: ensamblaje, soldadura, paletizado, atornillado, empaquetado, paletizado u otras operaciones de inspección y calidad. Pueden ser utilizados sin conexión, conectado a un dispositivo IoT o aplicarle algún algoritmo con un fin concreto.



ROBOTS COLABORATIVOS

APLICACIONES EN PRL

Prevención de trastornos musculoesqueléticos por reducción de tiempos de ejecución de manipulación de cargas y movimientos repetitivos
Trabajos en entornos peligrosos
Realización de altas tareas de precisión

FACTORES DE RIESGO

Factores de seguridad: golpes, atrapamientos con partes móviles, contacto eléctrico con partes activas, proyección de partículas (chispas, salpicaduras), quemaduras (contacto con partes calientes). Otros derivados de errores de programación o mal funcionamiento

Factores higiénicos: exposición a radiaciones derivadas de la soldadura, exposición a vibraciones durante el guiado manual, exposición a productos químicos peligrosos (vapores de la pintura, humos de soldadura), exposición al ruido derivado del mismo proceso.

Factores psicosociales: aumento de la carga mental, adecuación al ritmo del cobot, disminución de la autonomía, reducción de los descansos.

Factores ergonómicos: movimientos repetitivos debido al guiado manual, posturas forzadas y estáticas durante el mantenimiento

Falta de conocimiento o capacitación inadecuada

MEDIDAS PREVENTIVAS

Regular la carga y ritmos de trabajo adaptándolos a la persona trabajadora y no al cobot.

Proporcionar formación e información sobre los riesgos del cobot y las medidas preventivas al personal.

Uso de los equipos de protección individual y ropa de trabajo adecuados a los riesgos expuestos.

Uso, revisiones y mantenimiento de los cobots según las instrucciones indicadas por el fabricante.

Impedir el acceso a la zona peligrosa cuando el cobot esté en funcionamiento.

Los cobots deben realizar de forma previa a la entrada de personas al espacio de trabajo colaborativo una parada automática.

7.5 Chatbots

Un chatbot es un programa diseñado para **simular conversaciones con humanos a través de Internet**.



CHATBOTS		
APLICACIONES EN PRL Formación interactiva Consultas rápidas Reporte de incidentes y condiciones peligrosas de forma más rápida y sencilla Elaboración de evaluaciones de riesgo y planificación preventiva Envío de notificaciones y alertas Recopilación y análisis de datos que almacena para una mejora continua Redacción de informes u otros documentos	FACTORES DE RIESGO Factores ergonómicos por uso de pantallas de visualización de datos Factores psicosociales por: Temor al reemplazo Aumento de las expectativas de productividad Cambios en las estructuras de trabajo Conectividad permanente	MEDIDAS PREVENTIVAS Capacitación y desarrollo de habilidades de las personas trabajadoras para el uso de Chatbots Apoyo psicológico. Fomento del bienestar emocional Diseño ergonómico del puesto de trabajo (PVDs) Garantizar la desconexión digital Fomentar la interacción y supervisión humana Consulta y participación de las personas trabajadoras en el proceso de implantación y uso de los chatbots

7.6 Realidad virtual

La realidad virtual es la tecnología que permite **recrear entornos simulados en los cuales las personas interactuar de manera tridimensional**.



REALIDAD VIRTUAL		
APLICACIONES EN PRL Formación Simulación de trabajos peligrosos Evaluación de planes de emergencia Realización de simulacros Simulación de diseño ergonómico de puestos de trabajo	FACTORES DE RIESGO Mareos y vértigos Exigencia física por posturas y ejecución de movimientos repetitivos Desorientación y pérdida de percepción espacial Alteración en la visión Pérdida temporal de la cognición	MEDIDAS PREVENTIVAS Limitación de uso con descansos y/o pausas frecuentes Ajuste de la configuración Establecer periodos de aclimatación Formación previa sobre su correcto uso Promover la salud ocular Garantizar una vigilancia de la salud visual Habilitar espacio adecuado para su uso Promover la higiene postural

8. Bibliografía

- **Digitalización, inteligencia artificial y prevención de riesgos laborales.** Oficina Técnica de Prevención de Riesgos Laborales. UGT Cataluña.
- **Reglamento Europeo de Inteligencia Artificial.** Comisión Europea 2024.
- **Reglamento IA.** Sandbox IA. Ministerio de Asuntos Económicos y Transformación Digital.
- **Uso de la inteligencia artificial en las empresas.** Eurostat 2025
- **Qué es la inteligencia artificial.** Plan de Recuperación, Transformación y Resiliencia. Gobierno de España.
- **Estrategia Nacional de Inteligencia Artificial.** Ministerio de economía, comercio y empleo.
- **Agenda España Digital 2026.** Ministerio para la transformación digital y de la función pública.
- **Robots colaborativos características, riesgos y medidas preventivas.** Instituto Nacional de Seguridad y Salud en el Trabajo (INSST).
- **Ética de la inteligencia artificial.** UNESCO.
- **Ética y normativa de la IA. Guía para su uso responsable.** Basque Artificial Intelligence Center (BAIC)
- **Uso de la inteligencia artificial y Big data en las empresas españolas Año 2023.** Observatorio Nacional de Tecnología y Sociedad. Red.es. Secretaría de Estado de Digitalización e Inteligencia Artificial. Ministerio de Asuntos Económicos y Transformación Digital.
- **Informe por país sobre la Década Digital 2024 en España.** Comisión Europea.
- **Sistemas digitales inteligentes: guía de aplicación para mejorar la seguridad y la salud de las personas trabajadoras.** Agencia Europea de Seguridad y Salud en el Trabajo (EU-OSHA).
- **Principios para el diseño y el desarrollo: sistemas digitales inteligentes para mejorar la seguridad y la salud de las personas trabajadoras.** Agencia Europea de Seguridad y Salud en el Trabajo (EU-OSHA).
- **Hacia sistemas de gestión del personal basados en algoritmos y en IA para conseguir unos lugares de trabajo más productivos, más seguros y más saludables.** Agencia Europea de Seguridad y Salud en el Trabajo (EU-OSHA).
- **Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial.** Boletín oficial del Estado.
- **Gestión de personal mediante inteligencia artificial (AI): implicaciones para la SST.** Agencia Europea de Seguridad y Salud en el Trabajo (EU-OSHA).