EL DELEGADO DE PREVENCION.

DIGITALIZACION E INTELIGENCIA ARTIFICIAL

EL DELEGADO DE PREVENCIÓN.

DIGITALIZACION E INTELIGENCIA ARTIFICIAL

Subvencionado por:

GOBIERNO de CANTABRIA
CONSEJERÍA DE INDUSTRIA, EMPLEO, INNOVACIÓN Y COMERCIO

Instituto Cántabro
DE SEGURIDAD Y SALUD EN EL TRABAJO

Elaborado por:

UGT Cantabria

Índice:

1. INTRODUCCION

La irrupción de la digitalización y la inteligencia artificial en la sociedad y en las empresas plantea retos y genera oportunidades en lo concerniente a su aplicación.

Esta implementación en el campo laboral, tanto de la digitalización como en el uso de la inteligencia artificial, generará nuevos riesgos o cambios organizacionales, con lo que afectará a la prevención de riesgos laborales.

En este sentido, la representación de las personas trabajadoras en esta materia, los delegados y las delegadas de prevención tienen que tener la formación e información concerniente a los conceptos básicos de la digitalización y de la inteligencia artificial y de cómo pueden afectar a las condiciones de trabajo y cómo se debe actuar ante estas nuevas condiciones.

La presencia de la digitalización y de la inteligencia artificial en nuestras vidas ha aumentado en los últimos años de manera significativa.

No obstante, el avance más significativo de este cuarto de siglo ha sido la inteligencia artificial, cuyo impacto ha sido transversal y profundo.

La inteligencia artificial ha evolucionado, pasando de la teoría conceptual a transformarse en una herramienta presente en la mayoría, por no decir todos, de todos los aspectos de nuestra vida en sus diferentes ámbitos.

Es capaz de generar texto, imágenes e incluso tomar decisiones ante situaciones complejas; como en el sector de la medicina, que ha revolucionado la investigación farmacéutica, facilitando el desarrollo de tratamientos innovadores y mejorando la atención que se realiza a cada paciente.

En otros sectores, como el financiero, ha transformado la gestión de riesgos y la detección de fraudes, permitiendo a las instituciones tomar decisiones más informadas y eficientes.

Existen claros beneficios en lo referente al uso tanto de la inteligencia artificial como de la digitalización, en la mayoría de los aspectos de la vida cotidiana, y facilitando, por tanto, las tareas diarias.

Sin embargo, tanto la digitalización como la inteligencia artificial presentan un espectro de uso más amplio que presenta un trasfondo más incisivo e interesante, con los consiguientes desafíos y riesgos para las personas trabajadoras.

El más significativo, en lo referente a la acepción para las personas trabajadoras, es el referente a la automatización que promueve la inteligencia artificial, con la consiguiente amenaza en lo referente a la destrucción de puestos de trabajo.

Además, tanto la digitalización como la implementación de la inteligencia artificial en el mundo laboral plantean serios problemas éticos relativos a las personas trabajadoras, lo que se debe tener en cuenta de cara al impacto que puedan generar.

Sin olvidar, por supuesto, las implicaciones que estas dos tecnologías, tanto la digitalización como la inteligencia artificial tienen con la prevención de riesgos laborales en sus diferentes aspectos, puesto que aunque presente interrelaciones, tienen diferencias.

El objetivo que se pretende alcanzar con este documento es facilitar una aproximación a los conceptos de digitalización e inteligencia artificial y los factores de riesgos que pueden repercutir en el entorno laboral, así como la prevención que se puede considerar ante estos factores de riesgo.

2. DIGITALIZACION

Concepto:

La digitalización se puede definir como el conjunto de procesos mediante los cuales los datos de toda la organización y sus activos se procesan a través de tecnologías digitales avanzadas, lo cual conduce a cambios fundamentales en los procesos que pueden resultar en nuevos modelos de negocio y cambios sociales. Se puede simplificar como el traspaso de la información de un formato físico a un entorno digital.

El traspaso de información más común de dígitos en la computación y la digitalización es el sistema binario, donde cada dígito, llamado bit, puede tener un valor de 0 o 1.

La digitalización convierte información analógica en dígitos, facilitando su manipulación, almacenamiento, y transmisión, lo que permite:

- Ahorro de espacio. Al evitarse el almacenaje físico de diferentes tipos de documentos o archivos, el espacio que no se utiliza se puede utilizar para otros fines. O en determinados casos, puede servir para encontrar ubicaciones con menos metros cuadrados, con el consiguiente ahorro de costes económicos.

- Protección de los documentos. Los riesgos físicos más directos (como humedades, deterioros por el paso del tiempo o casos más extremos y menos probables como incendios o inundaciones) a la hora de sufrir daños de los materiales, desaparecen con almacenajes en memorias externas y/o en la nube.

- Rapidez en la consulta. El ahorro de tiempo en las consultas de los datos es otra de las ventajas de la digitalización. Esto es especialmente importante en perfiles profesionales que puedan tener que realizar estas consultas de manera recurrente, puesto que el tiempo no invertido en esta tarea será muy elevado a lo largo de la jornada laboral, pudiéndose dedicar ese tiempo a otras tareas. Así pues, la productividad también se verá mejorada.

- Ahorro de consumo de papel. En un mundo cada vez más concienciado con las cuestiones medioambientales, la digitalización implica también una reducción en el uso de papel en las oficinas, al no tener que imprimir los documentos.

- Acceso a la información. Al permitirse acceder en remoto a la información se pueden ofrecer mayores medidas de seguridad, así como conocer quién puede o no entrar a dichos documentos. También en relación con esta cuestión, una de las ventajas es que se facilita el acceso desde diferentes lugares sin tener que estar físicamente en el mismo lugar.

La evolución de la digitalización así como las tecnologías inherentes a ella, evolucionan a un ritmo vertiginosamente rápido, aun cuando se están se está adoptando en las empresas.

Esto no quiero decir que sea agregar tecnología por agregar; es básico que exista un rumbo marcado dentro de la organización para fomentar nuevos caminos y enfoques sobre su papel dentro de este proceso, con un liderazgo claro y definido.

La digitalización permite la creación de nuevas cadenas de valor y experiencias que sean colaborativas, interactivas, sostenibles y rentables; por este motivo se tiene que definir el rumbo, para saber la dirección a seguir y que el proceso de digitalización no se quede únicamente en una automatización de procesos internos sin cohesión.

Estos progresos tecnológicos carecen de valor si no se enmarcan en una perspectiva humana y humanista, colocando a las personas en el núcleo de la digitalización. Nos enfrentamos cada vez más a efectos negativos derivados de una aplicación inadecuada de los avances digitales, desde el aumento de la desigualdad, agraviada ya por una era de recortes sociales y económicos, hasta la precarización laboral.

La transformación digital debe priorizar a las personas, con el fin de que nadie quede excluido.

3. INTELIGENCIA ARTIFICIAL.

Concepto:

La inteligencia artificial es la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear.

La inteligencia artificial permite que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico. La máquina recibe datos (ya preparados o recopilados a través de sus propios sensores, por ejemplo, una cámara), los procesa y responde a ellos.

Los sistemas de inteligencia artificial son capaces de adaptar su comportamiento en cierta medida, analizar los efectos de acciones previas y de trabajar de manera autónoma. Estos sistemas son capaces de realizar funciones asociadas a la inteligencia humana, como la percepción, el aprendizaje, la comprensión, la adaptación, el razonamiento y la interacción, imitando un comportamiento inteligente humano.

- Percepción:

La inteligencia artificial puede procesar datos sensoriales como por ejemplo imágenes, sonido y texto, para entender el mundo que lo rodea. Esto incluye la visión por computadora, el procesamiento del lenguaje natural y la interpretación de datos.

- Aprendizaje:

El aprendizaje automático es un sub campo de la inteligencia artificial que permite a las máquinas aprender de los datos. Este aprendizaje puede ser supervisado (donde los datos de entrenamiento incluyen la entrada y la salida deseada), no supervisado (donde los datos de entrenamiento solo incluyen la entrada) o por refuerzo (donde un agente aprende a tomar decisiones basándose en recompensas y penalizaciones).

- Comprensión:

La inteligencia artificial puede comprender el contexto, las relaciones y las implicaciones de los datos que procesa. Esto puede incluir la comprensión del lenguaje, la interpretación de las emociones y la comprensión de los conceptos abstractos.

- Adaptación:

La inteligencia artificial puede adaptarse a nuevas situaciones y cambios en el entorno. Esto puede incluir el aprendizaje en línea (donde la máquina continúa aprendiendo mientras recibe nuevos datos) y el aprendizaje transferible (donde la máquina aplica el aprendido en una tarea a otras tareas que sean similares).

- Razonamiento:

La inteligencia artificial puede tomar decisiones basadas en los datos que ha procesado. Esto puede incluir la toma de decisiones basada en reglas, la planificación y la ejecución de tareas y la resolución de problemas.

- Interacción:

La inteligencia artificial puede interactuar con humanos y otras máquinas. Esto puede incluir la generación de lenguaje natural, la síntesis de voz humana y la interacción con otros sistemas informáticos de inteligencia artificial.

La inteligencia artificial funciona mediante la creación de modelos matemáticos que se implementan a través de algoritmos computacionales diseñados para hacer tareas específicas, como por ejemplo reconocer patrones, tomar decisiones basadas en datos o incluso aprender de nuevas informaciones de manera autónoma.

Los componentes y procesos clave que permiten el funcionamiento de la inteligencia artificial son:

- Recopilación de datos:

Todo empieza con el conjunto de datos (bytes). La inteligencia artificial necesita datos para aprender y mejorar. Estos datos pueden ser imágenes, textos, registros de sonido, entre otros.

- Pre procesamiento de datos:

Los datos crudos suelen necesitar ser limpiados y organizados antes de ser utilizados para el entrenamiento: eliminar datos irrelevantes, corregir errores o convertir datos en formato adecuado.

- Modelado y algoritmos:

  Se seleccionan y diseñan algoritmos específicos para procesar los datos.

- Aprendizaje:

Durante la fase de aprendizaje, el modelo de inteligencia artificial se entrena utilizando un gran conjunto de datos. El modelo hace predicciones o toma decisiones basadas en los datos de entrada, y después se ajusta en función de la precisión de sus resultados. Este proceso se repite muchas veces, y el modelo mejora gradualmente su rendimiento.

- Evaluación y ajuste:

Una vez que el modelo ha sido entrenado, se evalúa su rendimiento utilizando un conjunto de datos de prueba que no se utilizó durante el entrenamiento. Esto ayuda a garantizar que el modelo puede generalizar bien a nuevos datos. Basándose en los resultados de la evaluación, el modelo puede ser ajustado o afinado para mejorar su precisión.

- Implementación:

Finalmente, el modelo de inteligencia artificial entrenado y evaluado se implementa en aplicaciones del mundo real, donde puede automatizar tareas, tomar decisiones basadas en datos en tiempo real o proporcionar insights (conocimientos / percepciones) que antes no eran accesibles.

La inteligencia artificial alcanza varios campos y técnicas, incluyendo el aprendizaje automático (Machine Learning), el procesamiento del lenguaje natural (NLP), la visión por computadora y la robótica, entre otras. Cada uno de estos campos utiliza enfoques y algoritmos especializados para resolver problemas y hacer tareas de manera inteligente.

4. FACTORES DE RIESGO

Concepto:

Se puede definir de factor de riesgo a cualquier condición, situación o elemento que aumenta la probabilidad de que ocurra un incidente que afecte la seguridad, salud o bienestar de las personas en el entorno laboral.

Los factores de riesgo, se pueden asociar a:

- Condiciones físicas: Espacios de trabajo peligrosos, equipos defectuosos.
- Factores químicos o biológicos: Exposición a sustancias tóxicas o microorganismos peligrosos.
- Factores psicosociales: Estrés, acoso laboral, jornadas excesivas.

La implantación de esta tecnologías, tanto la digitalización como la inteligencia artificial, introducen varios factores de riesgo que tienen su consiguiente impacto en la prevención de riesgos laborales. Estos riesgos se relacionan con los diferentes aspectos asociados, desde la seguridad física hasta los psicosociales, pasando por los ergonómicos. Para poder disponer de un entorno de trabajo saludable y seguro, es fundamental identificar y evaluar estos factores de riesgo, para posteriormente aplicar las medidas preventivas pertinentes.

Los posibles "nuevos riesgos emergentes" que la Agencia Europea para la Seguridad y Salud define como «cualquier riesgo nuevo que va en aumento» que provengan de los factores de riesgos de la digitalización o de la inteligencia artificial, deben ser investigados en el ámbito de la prevención de riesgos laborales para identificar y comprender los peligros que estas nuevas tecnologías conllevan a los puestos de trabajo.

- Seguridad de datos y privacidad

La inteligencia artificial requiere acceso a grandes volúmenes de datos, con riesgos de seguridad de datos y la privacidad de las personas trabajadoras. Recopilar, almacenar y analizar inadecuadamente expone a las personas trabajadoras a estos riesgos.

- Falta de transparencia

Uno de los factores que contribuye en gran medida a generar ansiedad y frustración es no saber qué datos y cómo se recopilan, y qué criterios usa el algoritmo para llegar a la decisión concreta.

- Errores en el sistema y mal funcionamiento

La dependencia de sistemas digitales o de inteligencia artificial para tareas que se consideren críticas de seguridad puede ser peligrosa si ocurren fallos o si estos sistemas funcionan incorrectamente. El resultado de estos errores de los sistemas de inteligencia artificial que controlan o monitorizan estos trabajos considerados peligrosos puede acabar en accidentes laborales.

- Despersonalización de las relaciones laborales.

La rapidez en lo referente a la toma de decisiones que se gestionan a través de los algoritmos, así como unas relaciones laborales que cada vez están más automatizadas, conllevan una completa despersonalización de las mismas. La automatización excesiva en aspectos tales como la evaluación del rendimiento y de desempeño y la designación de tareas, obviará un aspecto fundamental, el humano, en el desempeño del trabajo, lo que acarreará de forma más que posibles errores de juicio sobre las decisiones que se tomen de forma automática. Esto se verá percibido por las personas trabajadoras como una falta de justicia y les acabará afectando en lo concerniente a los aspectos psicosociales y terminará por enrarecer el clima laboral.

- Monitorización constante

El control tecnológico y la falta de privacidad generan tecno estrés, debido a la sensación de estar permanentemente observado. La observación constante provoca conductas antinaturales de las personas trabajadoras, lo que a su vez provoca esfuerzos físicos o psicológicos, mermando las relaciones sociales laborales.

- Utilización del Machine Learning o Aprendizaje Automático en las empresas

Los sistemas tienen métodos de aprendizaje, lo que permite una especie de aprendizaje automático. Las empresas pueden tomar decisiones en base a estos aprendizajes automáticos para exigir a cada persona su máximo. De esta forma, se "personaliza" la exigencia a cada persona trabajadora, obviando el trato igualitario que se empleaba hasta la irrupción de las nuevas tecnologías. A través del método de prueba y error, la inteligencia artificial tiene la capacidad de revelar la máxima productividad de cada persona trabajadora en función de sus características, en una especie de robotización de las personas. El aprendizaje automático también permite definir diferentes perfiles de personas trabajadoras y dividirlos en función de los rendimientos. Además, se puede utilizar la técnica del latigazo digital (digital whip) para exigirlo.

- Comparación constante

Informar a las personas trabajadoras sobre su rendimiento en relación y comparación con el resto de personas integrantes de la plantilla, genera más presión, estrés, ansiedad y problemas con la autoestima.

- Sesgos y discriminación

La toma de decisiones basada en los algoritmos es, en teoría, más objetiva que la que realizan las personas. No obstante, existen riesgos en esta toma de decisiones si se basan en datos que presenten sesgos digitales y que carezcan de la perspectiva humana. Estos sesgos provienen de variables parametrizadas o usadas incorrectamente por el modelo o el algoritmo, con lo que el sesgo de partida se mantiene en el proceso decisional y sesga también la decisión final, con el consiguiente perjuicio en las decisiones.

- Tecno-estrés

El término tecno estrés se refiere al estrés específico derivado de la introducción y el uso de las nuevas tecnologías en el trabajo, que comporta efectos psicosociales negativos derivados del uso de las tecnologías de la información y comunicación.

- Tecno-ansiedad

Variante del tecno estrés que genera ansiedad, tensión y malestar por el uso de las nuevas tecnologías; con sentimientos negativos sobre las competencias y las capacidades de utilización respecto de estas.

- Tecno-fatiga

Variante del tecno estrés que genera fatiga o cansancio mental por del uso de las nuevas tecnologías; con sentimientos relativos a agotamiento mental y cognitivo por su uso.

- Tecno-adicción

Variante del tecno estrés que genera un incontrolable impulso sobre el uso constante las nuevas tecnologías, en todo momento y lugar y durante largos periodos de tiempo.

- Síndrome del trabajador quemado (Burn-out)

Este síndrome se identifica por ser generador de agotamiento físico y mental intenso que viene provocado y es derivado por un estado de estrés laboral crónico o frustración prolongada. La relación con las nuevas tecnologías viene por la frustración que puede producir.

- Falta de control

Debido a la que las tareas se automatizan en gran parte, las personas trabajadoras sienten que no tienen, o tienen menos control sobre el trabajo que realizan. Esta percepción de falta de control puede aumentar el estrés, especialmente si las personas trabajadoras son responsables de obtener resultados, al no tener control directo sobre todos los aspectos del proceso y quedar a expensas de la automatización.

- Sobrecarga de trabajo

La implantación de nuevas tecnologías en el entorno laboral requiere de la adquisición de nuevas competencias tecnológicas. La falta de visión estratégica en la formación de las personas trabajadoras por parte de las empresas, sin planes de formación adecuados y consensuados con las plantillas, no tiene en cuenta el tiempo de inversión personal que requiere.

- Aislamiento y disminución de la cohesión del Equipo

La introducción de la inteligencia artificial cambia la dinámica de trabajo, reduciendo la Interacción humana y aumentando el riesgo de aislamiento entre las personas trabajadoras. Esto puede afectar la cohesión del equipo y el apoyo social en el puesto de trabajo.

- Brecha digital

La brecha digital es la desigualdad en cuanto al acceso y capacidad para usar las nuevas tecnologías de la información y comunicación (Internet, ordenadores, y otras tecnologías digitales…)
La brecha digital presenta varias dimensiones: el acceso a la tecnología (disponibilidad de las infraestructuras para conectarse a Internet); las habilidades digitales (capacidad de usarlas eficazmente); el uso de la tecnología (referente al uso desigual), la brecha generacional (diferencias de acceso y uso entre jóvenes y mayores) y la brecha de género (diferencias de uso entre mujeres y hombres). Reducir la brecha digital es un desafío importante que afecta a toda la sociedad, no solamente a las empresas y el objetivo de esta reducir es el de garantizar la inclusión y equidad en la era digital.

- Incertidumbre y miedo a lo desconocido

Especialmente en relación con la posibilidad de perder el trabajo o la incapacidad de adaptarse a las nuevas tecnologías. Esta incertidumbre puede aumentar los niveles de estrés y ansiedad entre las personas trabajadoras. Esto no solo afecta la salud mental, sino que también puede tener consecuencias físicas, como problemas cardiovasculares, trastornos del sueño y fatiga.

- Resistencia al cambio

Existe una resistencia innata del ser humano al cambio. La implantación de nuevas herramientas de digitalización o herramientas conectadas o controladas por parte de la inteligencia artificial no es una excepción. La resistencia al cambio tiene implicaciones para la seguridad y la salud incluida la mental. Puede variar en gravedad y manifestarse de diferentes maneras, relacionadas con la magnitud y la naturaleza del cambio y de cómo se gestiona por las personas implicadas sobre el impacto del cambio en su entorno laboral.

- Sensación de pérdida de control

La implementación de la inteligencia artificial puede hacer que algunas personas trabajadoras sientan que pierden control sobre su trabajo o su entorno laboral, lo cual puede contribuir a sentimientos de desapoderamiento y afectar negativamente a su bienestar mental.

- Conexión constante

La conexión constante con el trabajo, facilitada por las tecnologías digitales, conduce al agotamiento laboral, al difuminarse la línea entre la vida laboral y personal. Las personas trabajadoras se sienten obligadas a estar disponibles más allá de las horas laborales.

5. PREVENCION EN LA DIGITALIZACION.

"…La prevención de riesgos laborales deberá integrarse en el sistema general de gestión de la empresa, tanto en el conjunto de sus actividades como en todos los niveles jerárquicos de ésta, a través de la implantación y aplicación de un plan de prevención de riesgos…" Esto es lo que indica el Artículo 16, Apartado 1 de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.

Por lo tanto, la implantación de las nuevas tecnologías deberá integrarse en el plan de prevención de riesgos, así como realizarla mediante una planificación cuidadosa con la participación activa de todos los niveles de la organización incluidos las delegadas y delegados de prevención y un compromiso continuo con la mejora. Es vital la anticipación que se realice de los potenciales riesgos potenciales con el fin de adelantarse a sus efectos con el fin de erradicarlos o minimizarlos y evitar que se conviertan en accidentes.

Por ello, el primer paso a realizar según los principios de la acción preventiva contemplados indicados en el Artículo 15, Apartado 1 de la Ley 31/1995, en el caso de que no se pueda evitar el riesgo, es llevar a cabo el análisis de riesgos para identificar y evaluar los peligros potenciales.

A continuación, se tienen que establecer las medidas preventivas y proporcionar la información y formación a la que las personas trabajadoras tienen derecho, acorde a lo estipulado en la legislación (Artículo 18 y 19 de la Ley 31/1995)

Otros capítulos a tener en cuenta es la participación de las personas trabajadoras, que se puede favorecer si se actualiza y revisa la documentación referente a los cambios que se quieren introducir respecto de las nuevas tecnologías. Además, esta participación puede paliar la resistencia al cambio, al incluir las consideraciones de las personas trabajadoras en el sistema de gestión de la prevención sobre estos nuevos procesos y fomentar la participación activa de los trabajadores en el cambio.

La vigilancia de la salud también se tendrá que revisar, actualizando los protocolos existentes para determinar la afección de las nuevas tecnologías a la salud de las personas trabajadoras.

Este proceso de introducir e implantar nuevas tecnologías en los centros de trabajo, se traduce en un desafío constante, puesto que afecta a una serie de aspectos como son poder garantizar una transición digital justa, fomentar el derecho a la desconexión digital más allá de lo que indica la legislación y mitigar la resistencia al cambio. Estos aspectos fundamentales se deben abordar para asegurar una evolución tecnológica equitativa, efectiva y justa en las empresas.

- Transición digital justa

Concepto:

El concepto de transición digital justa hace referencia al proceso de cambio hacia una economía más sostenible —tanto en términos ambientales como sociales— que no deje a nadie atrás. En otras palabras, no se trata solo de implementar tecnologías verdes o digitalizar servicios, sino de asegurar que estos avances beneficien también a las personas en situación de vulnerabilidad y no generen nuevas formas de exclusión.

A diferencia de la transformación digital, que se puede definir como una iniciativa de estrategia empresarial que incorpora la tecnología digital en todas las áreas de una organización para evaluar y modernizar los procesos, productos, operaciones de una organización para permitir una innovación continua, rápida y orientada al cliente; la «transición digital justa» es un proceso planificado y equitativo para avanzar hacia una economía y sociedad más digitalizadas, asegurando que los beneficios de esta digitalización se compartan ampliamente entre todos los sectores de la sociedad, y que se mitiguen sus posibles impactos negativos. De esta forma implica y contiene más componentes.

La transición digital justa se basa en la idea de que, aunque la digitalización ofrece enormes oportunidades para mejorar la eficiencia, la innovación, la creación de nuevas profesiones y puesto de trabajo y el acceso a los servicios, también plantea una serie de desafíos significativos, como la obsolescencia de ciertas ocupaciones que conllevará a la eliminación de puestos de trabajo, la ampliación de la brecha digital y las preocupaciones sobre la privacidad y seguridad de los datos.

Con el fin de evitar la brecha digital se pueden llevar a cabo diferentes acciones:

I. Desarrollar programas de formación digital:

Ofrecer cursos y talleres que aborden desde habilidades digitales básicas hasta avances, asegurando que todas las personas trabajadoras puedan usar las herramientas y plataformas digitales utilizadas en su entorno laboral.

II. Personalizar la formación:

Adaptar los programas de capacitación a las necesidades específicas de las personas trabajadoras, considerando diferentes niveles de habilidad y conocimiento previo.

III. Inclusión y diversidad:

Promover estrategias de inclusión que aseguren que todas las personas trabajadoras, independientemente de su edad, género o antecedentes, tengan oportunidades iguales para desarrollarse en un entorno digital.

IV. Promover una cultura de aprendizaje digital:

Fomentar un entorno laboral que valore y promueva el aprendizaje y reciclaje continuo de nuevas tecnologías y herramientas digitales.

V. Apoyo y asistencia técnica:

Ofrecer apoyo técnico accesible y efectivo para ayudar a las personas trabajadoras a resolver problemas tecnológicos y fomentar su autonomía digital.

VI. Llevar a cabo evaluaciones regulares:

Para identificar las necesidades de capacitación digital de las personas trabajadoras y adaptar, en consecuencia, las estrategias de formación.

VII. Actualizar regularmente los equipos de trabajo:

Mantener la tecnología actualizada, modernizando los equipos de trabajo relativos a las nuevas tecnologías, para no dejar a nadie atrás a causa de obsolescencia tecnológica

VIII. Promover redes de aprendizaje:

Fomentar espacios donde las personas trabajadoras puedan compartir conocimientos, habilidades y experiencias relacionadas con el uso de tecnologías digitales, potenciando el aprendizaje colaborativo.

- Mitigación de la resistencia al cambio

Para evitar la resistencia al cambio y sus consecuencias negativas, es necesario gestionar cuidadosamente la introducción de las nuevas tecnologías como la digitalización y la inteligencia artificial y abordar proactivamente las preocupaciones de las personas trabajadoras anticipándose a ellas.

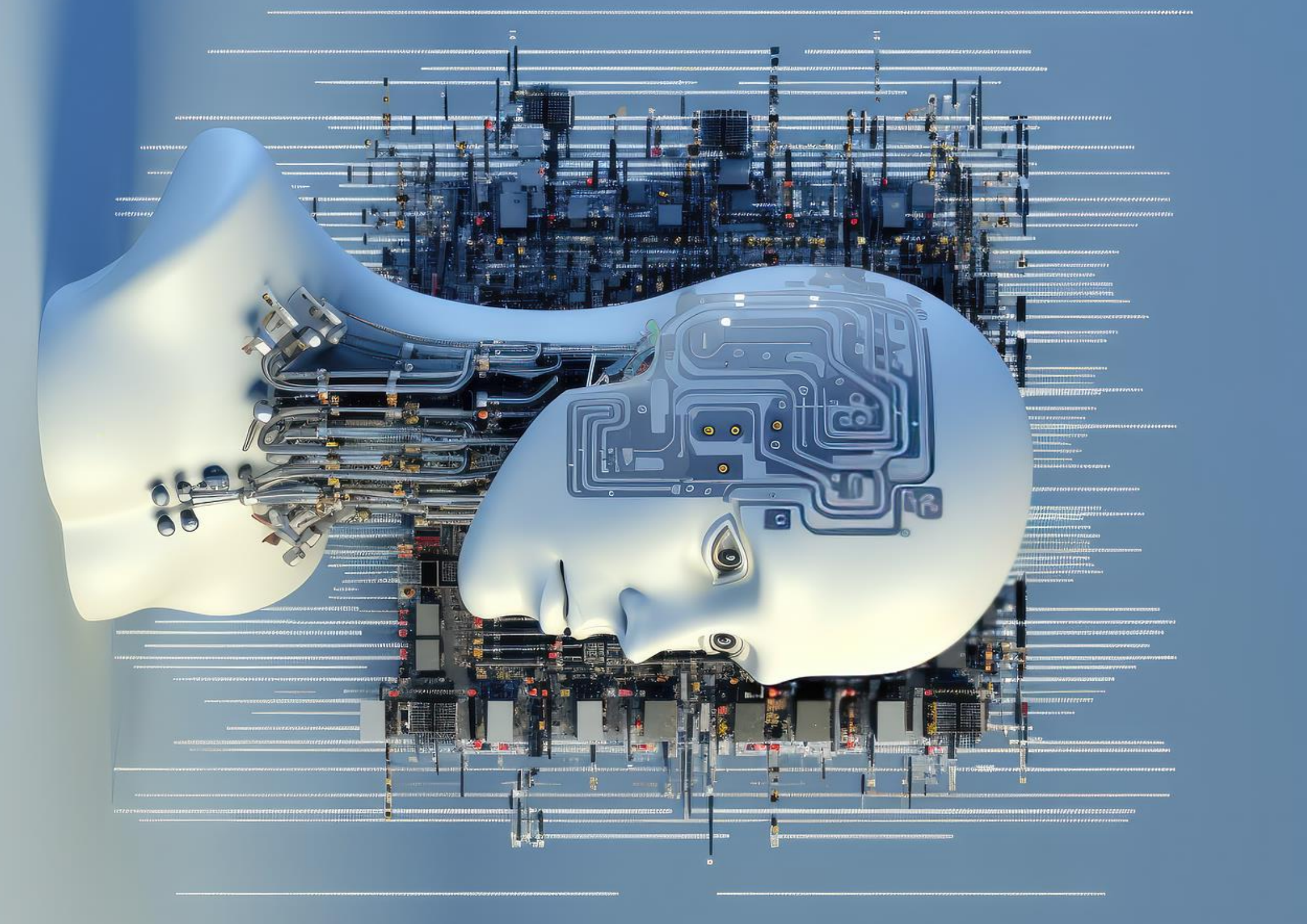
Esto puede ayudar a minimizar los impactos negativos en la seguridad, la salud y el bienestar mental, asegurando una transición más suave y justa hacia la digitalización de los puestos de trabajo.

- Desconexión digital

El Artículo 88 de Ley Orgánica 3/2018, sobre el derecho a la desconexión digital en el ámbito laboral establece en su apartado 1 que: "…Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar…"

En este artículo se establece la potestad de la persona trabajadora a responder o no a las comunicaciones que reciba por parte de su empresa fuera del horario laboral.

Debido a la hiperconectividad a la que estamos expuestos, es más que necesario el cumplimiento del derecho a la desconexión digital garantizando el derecho. Las personas trabajadoras no tienen que renunciar a su tiempo de descanso, a permisos o vacaciones para atender asuntos laborales.



6. PREVENCION EN LA INTELIGENCIA ARTIFICIAL.

Al igual que en el caso de la implementación de la digitalización, en el caso de la inteligencia artificial se deberá integrar en el plan de prevención de riesgos y también planificar esta implementación, asegurándose la participación de todos los estamentos de la empresa, incluida la representación de las personas en la materia preventiva, las delegadas y delegados de prevención.

Bien es cierto que existe un paso previo, y aunque no es un aspecto preventivo, sí que tiene consecuencias preventivas. Antes llevar a cabo la prevención en sí, se debe revisar la parte concerniente a la inteligencia artificial que afecte a aspectos preventivos, con el fin de evitar sesgos o procesos que discriminen a personas trabajadoras, entre otros. La información debe ser transparente para poder controlar sus riesgos.

Estas revisiones están fuera del alcance de la mayoría de las personas trabajadoras, por lo que se debería realizar una auditoría algorítmica sobre el uso de algoritmos de alto riesgo en el ámbito laboral, y antes de implantarlos, hacer una evaluación de los riesgos potenciales que puedan generar el tratamiento de datos. No se trata de la evaluación de riesgos laborales, sino de la evaluación jurídica de los riesgos de la inteligencia artificial que pueda afectar a derechos fundamentales de las personas, incluido el derecho a la salud.

Realizada la auditoría algorítmica, es cuando aplicamos la prevención, incluyendo la utilización de la inteligencia artificial. En este sentido, se tendrá que revisar y modificar la evaluación de los riesgos, incluidas las específicas, y aplicar las medidas preventivas necesarias para cada puesto de trabajo específico.

Existen una serie de medidas de prevención generales por el uso de la inteligencia artificial, que son:

- Formación e información de riesgos y medidas preventivas

La formación e información de las personas trabajadoras sobre cómo interactuar con la inteligencia artificial y sobre las medidas de protección de datos son básicas para los de centros de trabajo seguros.

Esta formación e información permite a su vez a las personas trabajadoras poder colaborar con la empresa desde el punto de vista de las personas que emplea esta tecnología de forma cotidiana.

I. Operación segura de la inteligencia artificial:

Instrucciones detalladas sobre cómo utilizar de manera segura las herramientas y sistemas de inteligencia artificial, incluyendo la interpretación correcta de las salidas de la inteligencia artificial y la toma de decisiones basada en estas.

II. Conciencia sobre riesgos y su prevención:

Educación sobre los riesgos laborales potenciales que presenta la inteligencia artificial, incluyendo fallos del sistema, y cómo responder eficazmente en tales situaciones para poder minimizar los daños causados.

III. Protección de datos:

Formación para las personas trabajadoras que utilicen las nuevas tecnologías sobre las mejores prácticas de manejo y protección de datos personales y sensibles, entendiendo la legislación aplicable y cómo cumplir con ella en el día a día.

- Desarrollo ético de la inteligencia artificial:

El desarrollo ético de la inteligencia artificial en los centros de trabajo requiere un gran compromiso colaborativo entre las personas desarrolladoras, empresas, personas trabajadoras y sus representantes, personas reguladoras de la normativa y legisladores, buscando siempre equilibrar la innovación tecnológica con el respeto que se debe a los derechos humanos y laborales. Este enfoque no solo promueve un entorno de trabajo más seguro y justo, sino que también contribuye a la aceptación y confianza en la inteligencia artificial como una herramienta valiosa para el futuro del trabajo y, por ende, de las personas trabajadoras.

Para llevar a cabo su desarrollo, se tienen que cumplir una serie de características.

I. Transparencia y comprensión:

Los sistemas de inteligencia artificial tienen que ser diseñados de forma que sus procesos de toma de decisiones puedan ser entendidos y explicados tanto a los desarrolladores como a las personas usuarias finales. Esto incluye proporcionar información clara sobre cómo opera la inteligencia artificial, bajo qué criterios toma decisiones y cómo se pueden interpretar estos resultados.

II. Accesibilidad de la información:

Asegurar que las personas trabajadoras tengan acceso a información sobre los sistemas de inteligencia artificial con los cuales interactúan, incluyendo posibles riesgos y las medidas de protección que se hayan previsto.

III. Pruebas rigurosas:

Antes de su implementación, los sistemas de inteligencia artificial tienen que someterse a pruebas exhaustivas para identificar y corregir posibles fallos que puedan comprometer la seguridad de las personas trabajadoras o la operación segura en el entorno laboral.

IV. Monitorización continúa:

Establecer sistemas de monitorización continua para detectar y responder rápidamente a cualquier fallo operativo o seguridad comprometida.

V. Protección de datos:

Incorporar medidas de protección de datos desde el diseño de los sistemas de inteligencia artificial, asegurando que se respete la privacidad de las personas trabajadoras mediante el tratamiento adecuado de sus datos personales.

VI. Consentimiento informado:

Obtener el consentimiento informado de las personas trabajadoras antes de recopilar, almacenar o analizar sus datos, explicando claramente los propósitos y usos previstos a los que se van a destinar estos datos.

VII. Diseño centrado en el humano:

Los sistemas de inteligencia artificial tienen que diseñarse con un enfoque humano, buscando complementar y enriquecer el trabajo de las personas trabajadoras, en lugar de reemplazarlos o marginarlos.

VIII. Prevención de sesgos:

Implementar medidas para identificar y mitigar sesgos en los algoritmos que se usen en los procesos o sistemas de inteligencia artificial que puedan llevar a decisiones discriminatorias o injustas, protegiendo así el bienestar y los derechos de las personas trabajadoras.

IX. Participación de las personas trabajadoras:

Fomentar la participación de las personas trabajadoras usuarias en el proceso de desarrollo y despliegue de la inteligencia artificial, recogiendo sus aportaciones y preocupaciones para asegurar que los sistemas se alineen con sus necesidades y expectativas, sirviendo también para mitigar la resistencia al cambio al hacerles partícipes de la implementación.

X. Establecer mecanismos de responsabilidad:

Definir claramente las responsabilidades legales y éticas de las empresas y desarrolladores en relación con los sistemas o procesos de inteligencia artificial, incluyendo mecanismos para la rendición de cuentas o responsabilidades, en el caso que se produzcan incidentes o daños.

XI. Políticas de privacidad de datos:

Implementar políticas estrictas de privacidad y seguridad de datos para proteger la información personal de las personas trabajadoras.

XII. Derechos de autor y propiedad intelectual:

La utilización de contenido digital puede plantear cuestiones complejas sobre los derechos de autor y la propiedad intelectual, especialmente cuando se usan imágenes, textos, u otros materiales protegidos sin permiso. Asegurarse que la inteligencia artificial no usa esta información sin permiso de explotación.

7. ACTUACION DE DELEGADAS Y DELEGADOS DE PREVENCION.

Los delegados y las delegadas de prevención en el ejercicio de sus funciones, pueden desarrollarlas mediante las competencias y facultades que están establecidas en el Artículo 36 de la Ley 31/1995, las competencias en el primer apartado y las facultades en el segundo.

Mediante las competencias y facultades podrán velar por la correcta implantación de la digitalización y la transformación digital en los centros de trabajo, defendiendo un uso correcto de la digitalización para promover su aprovechamiento eficaz y social y reivindicando las necesidades de todas las personas trabajadoras.

Los cambios tecnológicos van a llegar irremediablemente, y estos cambios tienen que repercutir en unas mejores las condiciones laborales de las personas trabajadoras, incluyendo, como no puede ser de otra manera, unos trabajos más seguros y más saludables que eviten que la implantación de nuevas tecnologías provoque efectos adversos en las condiciones de trabajo.

Por este motivo, los delegados y delegadas de prevención deben comprobar que las nuevas tecnologías se incorporan en la gestión preventiva, y estar alerta sobre posibles delegaciones de la empresa de cualquier tratamiento y uso de la información en la toma de decisiones a los algoritmos o inteligencia artificial que puedan afectar la seguridad y la salud de los trabajadores y trabajadoras, y controlar este uso.

Se tiene que contar con los representantes de las personas trabajadoras en el diseño de la implantación de nuevas tecnologías, conocer el impacto de estas en las condiciones de seguridad y salud y de trabajo, y asegurarnos que se aplican las medidas de prevención adecuadas.

La legislación española, específicamente con las reformas introducidas en el Estatuto de los Trabajadores y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), establece que las empresas tienen la obligación de informar los representantes de las personas trabajadoras sobre los sistemas de algoritmos o inteligencia artificial que afecten las condiciones de trabajo, la toma de decisiones laborales, y el acceso y mantenimiento de la ocupación.

Esta obligación incluye informar sobre la lógica aplicada por estos sistemas algorítmicos y cómo su uso puede afectar las condiciones laborales y la toma de decisiones respecto a los trabajadores y trabajadoras.

El objetivo es garantizar la transparencia y permitir a los representantes de las personas trabajadoras verificar y, en su caso, impugnar las decisiones que se tomen basándose en el procesamiento algorítmico, para proteger los derechos de las personas en un entorno laboral cada vez más digitalizado.

Los delegados y las delegadas de prevención tienen que intervenir en la afectación a la seguridad y la salud de las personas trabajadoras, solicitar la eliminación de los riesgos y la inclusión de la inteligencia artificial dentro de la gestión preventiva para que se apliquen medidas de prevención como hemos visto en los apartados anteriores, tanto en el uso de la inteligencia artificial como herramienta de prevención, como la gestión de los riesgos que pueda producir.

Subvencionado por:

GOBIERNO de CANTABRIA
CONSEJERÍA DE INDUSTRIA, EMPLEO, INNOVACIÓN Y COMERCIO

Instituto Cántabro
DE SEGURIDAD Y SALUD EN EL TRABAJO

Elaborado por:

UGT Cantabria