REVISTA CAP JURÍDICA CENTRAL

Legal Compliance para el uso de la inteligencia artificial en el ámbito laboral en Ecuador. Confidencialidad de la información y protección de datos personales

Autor: Raphael Andrés Palacios Mendoza[1]
Coautora: Doménica Lisbeth Palacios Mendoza[2]

RESUMEN: El presente artículo analiza el uso de la inteligencia artificial (en adelante, IA) en el ámbito laboral ecuatoriano desde una perspectiva jurídica, técnica y ética. Se identificó que la IA, como herramienta de apoyo al trabajo humano, requiere una adecuada comprensión de sus fundamentos teóricos y técnicos para evitar los riesgos de su aplicación descontrolada. Se constató que el principal desafío radica en el tratamiento inadecuado de la información confidencial y los datos personales por el estigma, desconocimiento y falta de políticas o lineamientos claros respecto a su uso. Finalmente, se establecieron lineamientos de *legal compliance* que incluyen la gestión del riesgo, la evaluación técnico-legal de las herramientas, capacitación al personal, protección de datos mediante anonimización y seudonimización, y la supervisión humana obligatoria, como estrategias clave para promover el uso ético y responsable de la IA en las organizaciones dentro del marco normativo y la realidad institucional del Ecuador.

Palabras clave: Inteligencia artificial, confidencialidad, protección de datos personales, ámbito laboral, riesgos, *legal compliance*.

ABSTRACT: This article analyzes the use of artificial intelligence (AI) in the Ecuadorian labor context from legal, technical, and ethical perspectives. It was found that AI, as a tool supporting human work, requires a proper understanding of its theoretical and technical foundations to avoid the risks of uncontrolled application. The study revealed that the main challenge lies in the improper handling of confidential information and personal data, driven by stigma, lack of knowledge, and the absence of clear policies or guidelines on its use. Finally, several legal compliance guidelines were established, including risk management, technical-legal assessment of AI tools, employee training, data protection through anonymization and pseudonymization, and mandatory human supervision, as key strategies to promote the ethical and responsible use of AI within organizations in alignment with the regulatory framework and institutional context of Ecuador.

Keywords: Artificial intelligence, confidentiality, personal data protection, workplace, risks, legal compliance.

1 Abogado graduado de la Universidad Central del Ecuador. Magíster en Derecho Mención Derecho Procesal Constitucional por la Universidad Estatal de Milagro. ORCID https://orcid.org/0009-0002-5430-5187.

2 Estudiante de Derecho en la Universidad Central del Ecuador, Asistente Legal en importante Firma de Abogados, con líneas de interés en Derecho Corporativo. ORCID https://orcid.org/0009-0003-5345-759X.

DOI: https://doi.org/10.29166/cap.v9i17.9406
pISSN 2550-6595
eISSN 2600-6014
revistacap_juridica2.1@hotmail.com

INTRODUCCIÓN

A día de hoy, la IA se ha convertido en el motor silencioso de la transformación de las relaciones laborales. Lo que antes era tan solo una ficción, hoy forma parte de la rutina. Los algoritmos *«toman decisiones»*, los sistemas *«aprenden»* y las herramientas redactan y *«predicen»*. Todo esto es producto del acelerado y expansivo proceso tecnológico que, día a día, se integra en todos los ámbitos de la vida humana, transformando la forma en que se trabaja, se comunica y se comprende la realidad.

El objetivo de este artículo es analizar los riesgos que plantea el uso de la IA en el ámbito laboral ecuatoriano, particularmente en lo relativo a la confidencialidad de la información, la protección de los datos personales y la necesidad de establecer estrategias de *legal compliance* para promover su uso responsable en las organizaciones.

Para el efecto, se emplea el enfoque de investigación cualitativo con un paradigma reflexivo y crítico. El nivel de investigación es el descriptivo. Se aplica el método de análisis-síntesis, mediante la técnica del análisis de contenido que incluye doctrina especializada y normativa vigente, en el marco de un estudio esencialmente teórico y documental, orientado al análisis crítico. Para el procesamiento de los resultados se empleó la técnica de categorización documental.

El desarrollo del estudio se justifica, en tanto, la IA inevitablemente transforma los procesos laborales y redefine el rol de los seres humanos dentro de ellos. Comprender su uso ético y responsable es una tarea ineludible para garantizar que el proceso tecnológico avance en armonía con el cumplimiento de las normas y la garantía de los derechos fundamentales.

ASPECTOS TEÓRICOS, TÉCNICOS Y APLICACIÓN EN EL ÁMBITO LABORAL DE LA IA

1. ANTECEDENTES Y DEFINICIÓN

Para comprender la naturaleza de la IA y su definición, resulta pertinente realizar un breve recorrido histórico. Uno de los primeros antecedentes se remonta a 1843 cuando la matemática inglesa Ada Lovelace elaboró el primer algoritmo destinado a ser ejecutado por una máquina analítica.[3] Su visión trascendió los límites del tiempo al prever que los dispositivos mecánicos podrían procesar información para producir resultados, anticipando así la lógica del *«aprendizaje automatizado»* que sustenta la IA moderna.

Décadas más tarde, en 1943, los neurobiólogos Warren McColloch y Walter Pitts plantearon que los procesos neuronales podrían representarse mediante modelos lógicos y matemáticos, sentando las bases de lo que se conoce como las redes neuronales artificiales, enfoque que fue complementado en 1956 con la Conferencia de Dartmouth,

3 Andrés Abeliuk y Claudio Gutiérrez, "Historia y evolución de la inteligencia artificial", *BITS de Ciencia*, núm. 21 (2021): 16, https://doi.org/10.71904/bits.vi21.2767.

considerada la cuna del nacimiento formal de la IA, a través de la idea de que las máquinas podrían razonar y resolver problemas de forma heurística.[4]

Si bien existen numerosos hitos y desarrollos que podrían mencionarse, los antecedentes expuestos resultan claves por haber delimitado los fundamentos teóricos y técnicos sobre los que se construye la IA en la actualidad. En un sentido similar, la doctrina contemporánea coincide en que establecer una definición única y precisa de la IA constituye una tarea compleja, debido a la naturaleza interdisciplinaria del concepto y su constante evolución tecnológica.

Por un lado, el autor José Cabanelas define la IA desde una perspectiva técnico-funcional, entendiéndola como la capacidad de un sistema informático, ya sea un ordenador, una red de equipos o una red de robots, para ejecutar tareas que, tradicionalmente, requerirían la inteligencia humana.[5] Es decir, la definición se centra en una especie de simulación del comportamiento inteligente a través de la aplicación de la informática.

El autor Lasse Rouhiainen, por su parte, concibe a la IA como la capacidad de las máquinas para ejecutar actividades que requieren inteligencia humana, pero esto no como una mera imitación, sino a través del uso de algoritmos capaces de procesar, aprender y aplicar el aprendizaje en la toma de decisiones.[6] Esta definición sintetiza la capacidad operativa y adaptativa de la IA considerando su *«aprendizaje»* a través de la automatización.

Siguiendo las definiciones de los autores antes mencionados, es preciso considerar también que John McCarthy y sus colegas en 1955 describieron a la IA como el intento de crear máquinas capaces de *«imitar el comportamiento humano»*, no obstante, posteriormente autores como Russel y Norving ampliaron el concepto distinguiendo cuatro aproximaciones a la IA: actuar como personas, razonar como personas, razonar racionalmente y actuar racionalmente.[7]

El conjunto de las definiciones propuestas resulta interesante, pues si bien Cabanelas y Rouhiainen se centran en la capacidad operativa y técnica de las máquinas, la propuesta de McCarthy y sus sucesores le da un sentido más amplio y filosófico: *«la IA como racionalidad autónoma»*. Coincidiendo con dicha postura, la IA más que una herramienta técnica comprende un sistema complejo de procesamiento autónomo de información que busca razonar, decidir y actuar con base en criterios algorítmicos diseñados por el ser humano.

A efectos del presente artículo, tomando en consideración la problemática que ha sido planteada, así como las definiciones antes desarrolladas, se entenderá a la IA como el *conjunto de sistemas informáticos capaces de ejecutar procesos de análisis, aprendizaje y toma de decisiones*. A esto se le debe agregar la exigencia de apegarse a un marco jurídico y ético que garantice el uso responsable y consciente, así como la protección de la información confidencial y los datos personales, tema que se desarrollará más adelante.

4 Ávila-Tomás, José F., Mayer-Pujadas, Miguel A. y Quesada-Varela, Víctor J., "La inteligencia artificial y sus aplicaciones en medicina I: introducción, antecedentes a la IA y robótica", *Atención Primaria*, núm. 52 (2020): 780, https://doi.org/10.1016/j.aprim.2020.04.013.

5 José Cabanelas, "Inteligencia artificial ¿Dr. Jekyll o Mr. Hyde?", *Mercados y Negocios*, núm. 40 (2019), https://www.redalyc.org/journal/5718/571860888002/html/.

6 Lasse Rouhiainen, *Inteligencia artificial. 101 cosas que debes saber hoy sobre nuestro futuro* (Madrid: Editorial Planeta S.A., 2018): 17, https://planetadelibrosar0.cdnstatics.com/libros_contenido_extra/40/39307_Inteligencia_artificial.pdf.

7 Vicenç Torra, "La inteligencia artificial", *Revista Lychnos*, núm. 7 (2011): 2, https://www.mdai.cat/vtorra/docs/ref.Torra.Lychnos.2011.pdf.

2. TIPOLOGÍAS DE LA IA: DÉBIL, FUERTE, GENERATIVA Y PREDICTIVA

Para comprender el desarrollo y la potencialidad actual de la IA es necesario distinguir entre sus principales tipologías. Tradicionalmente, la IA se ha clasificado en dos categorías basadas en sus capacidades: la IA débil y la IA fuerte. Para el efecto, se tomará en consideración las definiciones propuestas por Pérez-Ugena:

- **IA débil. -** Es aquella especializada en una tarea concreta. Carece de autonomía para aprender o adaptarse más allá de su función específica, pues su operatividad está limitada a la programación de una tarea predefinida.[8]
- **IA fuerte. -** Es aquella con capacidades cognitivas de aprendizaje autónomo, como, por ejemplo, razonar, aprender, y tomar decisiones sin limitarse a un ámbito predefinido.[9]

La evolución tecnológica ha permitido además identificar la aparición de nuevas tipologías de IA con capacidades cada vez más sofisticadas, entre ellas:

- **IA generativa. -** Se distingue por su capacidad de crear contenido original, como textos, imágenes, videos o audios, a partir de una construcción formulada en lenguaje natural.[10]
- **IA predictiva. -** Está orientada a elaborar algoritmos y modelos capaces de anticipar eventos o resultados futuros a partir del análisis de datos históricos y la identificación de patrones estadísticos. Sigue fases como recolección, preprocesamiento, entrenamiento y evaluación de modelos.[11]

En palabras más sencillas, la *IA débil* cumple funciones específicas y repetitivas, siendo útil en labores administrativas o de soporte técnico. La *IA fuerte*, en cambio, busca la autonomía cognitiva para aprender y razonar, sirviendo para la gestión estratégica y la toma de decisiones. La *IA generativa*, por su parte, cuenta con la capacidad de producción de contenidos, siendo ideal para temas comunicacionales y la redacción de informes. Por último, la *IA predictiva* está orientada al análisis de datos y anticipación de resultados, pudiendo aplicarse en procesos de recursos humanos o gestión de los riesgos laborales.

Esto demuestra que, la IA forma parte de los distintos ámbitos del trabajo contemporáneo, por lo que garantizar su uso responsable es una labor indispensable.

3. PILARES METODOLÓGICOS DE LA IA: *MACHINE LEARNING* Y *DEEP LEARNING*

La metodología en el conocimiento científico se refiere al proceso mediante el cual se obtiene la información relevante para entender, verificar, corregir o aplicar el

8 María Pérez-Ugena, "La inteligencia artificial: Definición, regulación y riesgos para los derechos fundamentales", *Estudios de Deusto*, vol. 1 (2024): 314, https://doi.org/10.18543/ed.3108.

9 Ibíd.

10 Francisco García-Peñalvo, Faraón Llorens-Largo y Javier Vidal, "La nueva realidad de la educación ante los avances de la inteligencia artificial generativa", *Revista Iberoamericana de Educación a Distancia*, (2023): 4, https://doi.org/10.5944/ried.27.1.37716.

11 María García, "La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal", *Ciencia Policial*, vol. 183 (2024): 95, https://doi.org/10.14201/cp.32177.

conocimiento.[12] En el caso de la IA, los pilares metodológicos se refieren a los fundamentos técnicos que permiten el procesamiento de los datos para su análisis, identificación de patrones y generación de respuestas o decisiones.

El *machine learning* (ML) está orientado a que los sistemas aprendan de datos mediante algoritmos capaces de identificar patrones y generar predicciones.[13] Por otra parte, el *deep learning* (DL) es una extensión avanzada del ML, basada en redes neuronales multicapa que emulan el funcionamiento del cerebro humano, haciendo posible el procesamiento de información compleja con altos niveles de precisión.[14]

En otras palabras, la IA se refiere al todo, el ML corresponde al método de *«aprendizaje»* y el DL a la forma más compleja de dicho *«aprendizaje»*. Para más claridad se puede imaginar tres círculos concéntricos: el más amplio representa a la IA, dentro de él se encuentra el ML y en el centro, el DL.

4. *«MEMORIA»* EN LA IA: ALMACENAMIENTO DE DATOS

El concepto de memoria se encuentra presente en el lenguaje cotidiano con expresiones como *«tengo mala memoria»*, *«Pedro tiene memoria fotográfica»*, *«Juan tiene memoria de pez»*, no obstante, no siempre se conoce su definición concreta y sentido científico.[15] Pero, *¿por qué resulta relevante hablar de la memoria en un estudio sobre IA?* La respuesta radica en que comprender cómo la IA almacena y utiliza la información permite, a nivel legal, identificar los riesgos asociados a la gestión de la información, como la confidencialidad y la protección de los datos personales.

Para el autor Germán Abeleira la memoria puede definirse como *«el proceso psicológico encargado de almacenar, codificar y recuperar acontecimientos, conceptos o procedimientos para poder adaptarnos a las distintas demandas de la vida diaria»*.[16] De forma análoga, en la IA la memoria cumple una función similar, pues almacena y organiza los datos que luego son utilizados para generar respuestas o tomar decisiones basadas en experiencias previas, perfeccionando sus resultados a través del tiempo.

Entendiendo aquello, *¿la memoria de la IA no es entonces un mero almacenamiento de datos?* Según la definición propuesta por Bill Inmon y R.D. Hackathorn, un almacén de datos, es una colección estructurada de información integrada, orientada a temas y no volátil, diseñada para apoyar los procesos analíticos y la toma de decisiones en una organización.[17]

Es decir, el almacenamiento de datos se limita a guardar esa información con una finalidad específica, no obstante, la IA no solo conserva esos datos, sino que también aprende de ellos, los analiza y los utiliza dinámicamente. Entonces, el almacenamiento de datos es parte del proceso de la IA.

12 Mario Tamayo y Tamayo, *El proceso de la investigación científica* (México D.F.: Editorial Limusa, 2003): 37, https://www.gob.mx/cms/uploads/attachment/file/227860/El_proceso__de_la_investigaci_n_cient_fica_Mario_Tamayo.pdf.

13 Santosh Kumar, Mokhade Anil, y Dhanraj Neeraj, "An Overview of Machine Learning, Deep Learning, and Reinforcement Learning-Based Techniques in Quantitative Finance: Recent Progress and Challenges", *Applied Sciences*, (2023): 21, https://doi.org/10.3390/app13031956.

14 Ibíd, 3.

15 Germán Abeleira, "La memoria concepto, funcionamiento y anomalías", *Cuadernos del Tomás*, núm. 5 (2013): 178, https://dialnet.unirioja.es/descarga/articulo/4462486.pdf.

16 Ibíd.

17 Rius Ángels, Montse Serra y Josep Curto, "Introducción al almacenamiento de datos", *Universitat Oberta de Catalunya*, (2013): 7, https://openaccess.uoc.edu/server/api/core/bitstreams/a3cbc1ac-9150-4df4-bc32-1727f8d41590/content.

Ahora bien, el filósofo de la mente y ciencia cognitiva, Daniel Dennet ha señalado que «la naturaleza hace un uso intensivo del principio de mínimo conocimiento y diseña criaturas muy capaces, expertas e incluso astutas que no tienen la más mínima idea de lo que hacen ni de por qué lo hacen».[18]

Esta afirmación resulta interesante, pues ilustra la esencia de la memoria en los sistemas de IA. Estos no *«comprenden»* la información como lo haría la mente humana, sino que almacenan, procesan y reutilizan los datos de forma estructurada para generar respuestas. Esto implica, a nivel técnico, que la memoria de la IA no implica conciencia ni entendimiento, sino la capacidad de conservar patrones de información derivados del entrenamiento de los modelos.

En definitiva, la memoria de la IA integra el almacenamiento de datos como una fase esencial dentro de la totalidad del proceso. Es precisamente en este punto, cuando la IA transforma la información almacenada que ha sido aportada por el usuario en conocimiento operativo, donde surge el conflicto central de este artículo.

5. APLICACIÓN DE LA IA EN EL ÁMBITO LABORAL

Antes de abordar este apartado, es necesario precisar que el interés de este estudio no radica en el debate tradicional sobre si la IA sustituirá el trabajo humano. Pues, si bien las tecnologías de la IA contribuyen al mejoramiento de la vida laboral, no implican el desplazamiento total de las habilidades humanas, por lo que los trabajadores deben mantener el liderazgo y control de sus procesos productivos.[19] Entonces, queda claro que la IA no implica un reemplazo al trabajador, sino una herramienta destinada a potenciar sus capacidades, mejorar su productividad y ayudar en la toma de decisiones.

Sin perjuicio de aquello, la IA redefine los roles existentes en el ámbito laboral, promoviendo la colaboración constante entre humanos y máquinas.[20] En este marco, la IA se convierte en una herramienta de apoyo que complementa el trabajo humano mientras las personas aportan con conocimiento técnico.

Esto puede aplicarse en múltiples ramas del conocimiento, no obstante, para efectos del presente estudio, el análisis se enfoca en el ámbito corporativo de manera amplia, donde la IA se aplica como un recurso estratégico para la optimización de procesos, el fortalecimiento de la gestión y la toma de decisiones.

Es así que, una de las formas en las que se manifiesta el uso de la IA en el ámbito laboral es mediante los procesos informáticos, donde se integra como una herramienta destinada a automatizar tareas y optimizar la interacción con los usuarios. Por ejemplo, con chatbots, asistentes virtuales, reconocimiento facial y de voz, traducción automatizada, generación de contenidos, entre otros.[21]

18 Daniel Dennett, *De las bacterias a Bach. La evolución de la mente* (Barcelona: Pasado & Presente, 2017) citado en Francisco García-Peñalvo, Faraón Llorens-Largo y Javier Vidal, "La nueva realidad de la educación ante los avances de la inteligencia artificial generativa", *Revista Iberoamericana de Educación a Distancia*, núm. 1 (2023): 4, https://doi.org/10.5944/ried.27.1.37716.

19 Nidia Pacanchique y Ruby Rodríguez, *El impacto de la inteligencia artificial en el trabajo* (Bogotá: Universidad Libre de Colombia, 2021): 5, https://hdl.handle.net/10901/20588.

20 Marek Hoehn, "La IA en el trabajo, la innovación, la productividad y las habilidades", Biblioteca del Congreso Nacional de Chile, (2025): 3, https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/36969/1/Informe_03_25_IA_en_el_Trabajo_innovacion_productividad_y_habilidades.pdf.

21 Laura García-Huguet y Magdalena Mut-Camacho, "La deshumanización del arte: inteligencia artificial y ética corporativa", *adComunica*, núm. 28 (2024): 322.

Entre los usos frecuentes se puede destacar, por ejemplo, el uso de la IA para redacción de informes técnicos, ejecutivos o jurídicos a partir de datos estructurados, permitiendo optimizar el tiempo, emplear un lenguaje claro y, sobre todo, adaptado al contexto y estilo de cada organización. En otra área, dentro de la misma organización, se podría utilizar para sistematizar o analizar grandes bases de datos, reduciendo al mínimo el tiempo que tomaría hacerlo normalmente.

Otro caso puede ser utilizar la IA para la traducción automatizada de documentos, permitiéndoles a las organizaciones y a los trabajadores manejar información y trabajar en distintos idiomas a pesar de no dominarlos completamente. En el ámbito comunicacional y publicitario, la generación de contenidos audiovisuales permite optimizar las campañas de marketing e inclusive, fortalecer la identidad visual de las marcas. Incluso en actividades administrativas cotidianas, la IA puede asistir para el manejo de agendas, contestar correos electrónicos o priorizar actividades.

Todo lo anterior representa solo una muestra general de cómo la IA ha pasado a integrarse en las actividades cotidianas de los trabajadores, transformando la manera en que se ejecuta el trabajo. Pero, si la IA permite aumentar la productividad, reducir tiempos y potenciar las capacidades humanas, *¿dónde está el problema?* El conflicto no está en la herramienta, sino en el uso no regulado y poco responsable que puede comprometer la confidencialidad de la información o derivar en un tratamiento inadecuado de los datos personales. Esto, además, sumado a la reserva y estigmatización que existen respecto al uso de la IA, demuestra la necesidad de desarrollar estrategias de *compliance* para fomentar su uso ético y responsable en el ámbito laboral ecuatoriano.

INFORMACIÓN CONFIDENCIAL Y PROTECCIÓN DE DATOS PERSONALES EN EL USO DE LA IA

1. DATO, INFORMACIÓN Y CONOCIMIENTO

Para comprender adecuadamente la relación entre la información confidencial, protección de datos personales y la IA, es necesario distinguir claramente los conceptos dato, información y conocimiento. Aquello permite diferenciar cómo cada uno de estos elementos participa en el almacenamiento, análisis y resultados que aporta la IA, así como comprender los riesgos que pueden derivar del uso inadecuado.

Por un lado, el dato puede entenderse como la unidad mínima del conocimiento, compuesta por hechos o representaciones que permiten medir y describir la realidad.[22] Su característica clave es que por sí solo carece de significado interpretativo, pero sirve de materia prima para generar información. Es decir, el dato constituye una especie de *«pequeñas parcelas o trozos de realidad»*.[23]

Por su parte, la información puede definirse como el resultado de interpretar y organizar datos, dotándolos de significados a partir de su relación con el contexto.[24] En

22 Ennio Prada, "Los insumos invisibles de decisión: datos, información y conocimiento", *Anales de Documentación*, núm. 11 (2008): 4, https://www.redalyc.org/pdf/635/63501110.pdf.

23 Mario Pérez-Montoro, "El documento como dato, conocimiento e información", *Revista Tradumàtica*, núm. 2 (2003): 3, https://revistes.uab.cat/tradumatica/article/view/158/n3-pdf-es.

24 Prada Madrid, "Los insumos invisibles de decisión: datos, información y conocimiento", 4.

tal sentido, constituye el contenido semántico que surge del dato una vez que ha sido codificado o decodificado.[25] Es decir, lo esencial de la información es que transforma los datos en conocimiento útil.

Por último, el conocimiento puede entenderse como el encuentro entre el sujeto y el objeto, donde al existir coherencia entre la realidad observada y su representación interna, se genera una comprensión válida y verificable de aquello que se conoce.[26] Lo esencial del conocimiento es su carácter aplicable, pues convierte la información en criterio para actuar. En dicho contexto, los datos, la información y el conocimiento forman parte de la operatividad y estrategia de las organizaciones.

El dato es la base sobre la que se construye cualquier sistema de IA. La información surge cuando esos datos son procesados y adquieren significado. El conocimiento se materializa cuando la empresa o el trabajador utilizan esa información para tomar decisiones concretas. Entendiendo, entonces, que la IA no solo procesa datos, sino que también interviene en la gestión del conocimiento organizacional, resulta responsabilidad de las empresas garantizar la confidencialidad, la protección de datos personales y, en general, el uso ético de la información.

2. CONFIDENCIALIDAD DE LA INFORMACIÓN EN EL TRABAJO

El Diccionario de la Lengua Española define lo confidencial como «aquello que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho».[27] En otras palabras, alude a todo aquello que se comparte bajo confianza y resguardo, con la intención de que se mantenga en reserva y no sea divulgado. La confidencialidad de la información en el trabajo se ve vinculada al deber de no revelar la información obtenida en el ejercicio de una función o actividad determinada.

En Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública (en adelante, LOTAIP), en su artículo 4, define la información confidencial en los siguientes términos:

> Información o documentación, en cualquier formato, final o preparatoria, haya sido o no generada por el sujeto obligado, derivada de los derechos personalísimos y fundamentales, y requiere expresa autorización de su titular para su divulgación, que contiene datos que, al revelarse, pudiesen dañar los siguientes intereses privados:
>
> a) El derecho a la privacidad (...); b) Los derechos personales cuya difusión requiera el consentimiento de sus titulares y deberán ser tratados según lo dispuesto en la Ley Orgánica de Protección de Datos Personales; c) Los intereses comerciales y económicos legítimos; y, d) Las patentes, derechos de autor y secretos comerciales.[28]

La definición de la LOTAIP en esta materia es sumamente relevante, pues si bien, podría pensarse que la confidencialidad está ligada únicamente a los datos personales, se amplía su alcance incluyendo elementos estratégicos de las organizaciones. En la práctica, esto implica que, todo trabajador está obligado a manejar la información propia de las organizaciones con la debida reserva, evitando su difusión o uso indebido. Por ende,

25 Pérez-Montoro, "El documento como dato, conocimiento e información", 4.

26 Andrés Martínez y Francy Ríos, "Los Conceptos de Conocimiento, Epistemología y Paradigma, como Base Diferencial en la Orientación Metodológica del Trabajo de Grado", *Cinta de Moebio*, núm. 25 (2006), https://dialnet.unirioja.es/descarga/articulo/1997015.pdf.

27 Real Academia Española, *Diccionario de la Lengua Española*, 23 ed., "confidencial".

28 Ecuador, *Ley Orgánica de Transparencia y Acceso a la Información Pública*, Segundo Registro Oficial Suplemento 245 (7 de febrero de 2023), art. 4.

en entornos donde la IA facilita el acceso, almacenamiento y procesamiento de todo tipo de información, valorar la confidencialidad se convierte en un deber de las empresas.

Es importante añadir que, tanto el empleador como el trabajador, tienen obligaciones a la hora de cuidar la información confidencial, pues, la doctrina laboral considera que, es el empleador quien tiene la obligación de determinar qué información o documento debe considerarse confidencial, particularmente, cuando se refiera al desarrollo del negocio, estrategias, métodos comerciales, desarrollo tecnológico, entre otros; así también, el trabajador tiene la obligación inherente de guardar la confidencialidad como parte de la relación laboral, incluso así no exista una cláusula o acuerdo expreso al respecto.[29]

3. PROTECCIÓN DE DATOS PERSONALES EN EL TRABAJO

La protección de datos personales corresponde a un derecho fundamental autónomo e independiente reconocido en la Constitución de la República del Ecuador en su artículo 66, numeral 19:

> Se reconocerá y garantizará a las personas: 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán autorización del titular o mandato de la ley.[30]

En un sentido similar, la Corte Constitucional, acogiéndose a la definición del Consejo Europeo de Protección de Datos de la Unión Europea define a los datos personales de la siguiente forma:

> Toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.[31]

Ahora bien, en el ámbito laboral, la protección de datos personales se configura como una garantía esencial frente al uso masivo de información que realizan, tanto las instituciones públicas como privadas. Es evidente que, en diferentes magnitudes, las empresas asumen una gran responsabilidad y rol clave en el tratamiento de datos personales, tanto de sus trabajadores como de los usuarios que hacen uso de sus servicios, por lo que la gestión apegada a las normas se vuelve indispensable.[32]

Dicho tratamiento deberá realizarse en apego estricto a los principios establecidos en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (en adelante, LOPDP), entre los más importantes: *Juridicidad*, que exige actuar conforme a la Constitución y normativa vigente (lit. a); *lealtad*, garantizando que el titular conozca que sus datos están siendo tratados y con qué fines (lit. b); *transparencia*, que obliga a brindar información clara, accesible y comprensible (lit. c); *finalidad* legítima y previamente informada (lit. d); *pertinencia* y *minimización* que limita el tratamiento estrictamente a los datos necesarios para cumplir el propósito establecido (lit. e); *proporcionalidad*,

29 Daniela Grau, Jorge Parker y José Uzal, "Confidencialidad de la información reservada en la relación laboral", *Universidad de Chile*, (2007).

30 Ecuador, *Constitución de la República del Ecuador*, Registro Oficial 449, (20 de octubre de 2008), art. 66.19.

31 CCE, sentencia 2064-14-EP/21, caso 2064-14-EP (27 de enero de 2021), párrafo 76.

32 Raquel Aguilera, "El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización", *Revista de Trabajo y Seguridad Social CEF*, núm. 442 (2020): 99, https://doi.org/10.51302/rtss.2020.886.

evitando el uso excesivo de datos personales (lit. f) y *confidencialidad*, asegurando el debido sigilo durante todo el proceso (lit. g).[33]

3.1 Tratamiento de datos personales en la relación empleador-trabajador. Subordinación y límites al control empresarial

La relación laboral es el vínculo de *carácter subordinado* entre el trabajador y el empleador, donde, en varios ámbitos, el consentimiento difícilmente puede considerarse libre debido al desequilibrio de poder existente.[34] Por subordinación, en este contexto, se entiende la situación en la que el trabajador está obligado a acatar las directrices, supervisión y facultades del empleador, derivadas de su poder de organización y dirección.[35]

Esta *«asimetría»* implica que el trabajador no puede oponerse al tratamiento de datos ni controlar plenamente cómo se utilizan en los sistemas automatizados, pues su posición de dependencia limita su capacidad de decisión y lo expone a cumplir instrucciones aun desconociendo el alcance de las mismas. Esta desigualdad responde a lo que la doctrina ha denominado un *«desequilibrio estructural del poder»*, en el que, como advierten Baylos y Kahn-Freud, la subordinación se oculta bajo la apariencia de un contrato entre las partes *«libres»*, pese a la evidente asimetría que condiciona la voluntad del trabajador.[36]

Pero, *¿por qué esto es relevante?* En contextos de subordinación, el consentimiento informado del trabajador pierde eficacia real, ya que la posibilidad de negarse es prácticamente inexistente por temor a repercusiones.[37] En materia laboral, solo puede hablarse de un consentimiento auténtico cuando el trabajador recibe información suficiente y tiene la posibilidad real de negarse sin sufrir consecuencias negativas.[38]

En la práctica, el consentimiento enfrenta límites estructurales derivados del desequilibrio del poder. Esto obliga al trabajador a aceptar instrucciones, sin considerar previamente las implicaciones a la seguridad de la información y protección de datos personales. Por ello, la información previa, clara y transparente acerca de las implicaciones de dicho tratamiento y los riesgos, resulta importante para reducir ese desequilibrio e impulsar la autodeterminación del trabajador.

Esto exige establecer límites al control empresarial, pues si bien no se desconoce la facultad del empleador de supervisar las actividades de sus trabajadores, así como disponer el cumplimiento de funciones específicas, dicha potestad no es absoluta y debe ejercerse en el marco del respeto de los derechos fundamentales.

Así, la protección de datos personales en relaciones marcadas por la subordinación, como en el caso de estudio, requiere un rol activo del empleador. No es suficiente con entregar y disponer el cumplimiento de las políticas internas, sino que debe liderar, transparentar y procurar el tratamiento de datos personales justificado y alineado a los

33 Ecuador, *Ley Orgánica de Protección de Datos Personales*, Quinto Registro Oficial Suplemento 459, (26 de mayo de 2021), art. 10.

34 Agencia Española de Protección de Datos. *La protección de datos en las relaciones laborales*. Madrid: AEPD, 2021, https://www.aepd.es/sites/default/files/2021-05/la-proteccion-de-datos-en-las-relaciones-laborales.pdf.

35 Carlos Freire-Montoya y Daniela López-Moya, "La subordinación como elemento necesario en la existencia de la relación laboral", *Revista Metropolitana de Ciencias Aplicadas*, (2023): 40, https://remca.umet.edu.ec/index.php/REMCA/article/download/531/527/1610.

36 Adrián Goldin, "Algunos rasgos definitorios de un derecho del trabajo en proceso de cambio", *Revista Relaciones Laborales*, (2014): 31, https://revistas.pucp.edu.pe/index.php/themis/article/download/10847/11353/43088.

37 Agencia Española de Protección de Datos. "La protección de datos en las relaciones laborales", 8.

38 Henar Álvarez, "El consentimiento individual y su alcance en la inteligencia artificial aplicada al ámbito laboral", *Documentación Laboral*, (2022), https://dialnet.unirioja.es/servlet/articulo?codigo=8653043.

principios de tratamiento que establece la LOPDP, equilibrando la dinámica laboral y fortaleciendo la confianza entre las partes.

4. RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES EN LA IA

Para el desarrollo de este subtema, es necesario partir de la aclaración de que, el análisis de los riesgos no se plantea desde la afectación que genera el uso de la IA hacia los trabajadores, como la discriminación o desigualdad que ha señalado el Parlamento Europeo respecto al uso de macro datos y algoritmos predictivos.[39] El sentido que se pretende señalar se enfoca en la gestión interna, es decir, cómo los propios trabajadores, al utilizar la IA, podrían exponer información sensible o confidencial de la empresa, así como comprometer el adecuado tratamiento de los datos personales.

En un sentido amplio, el *riesgo* puede entenderse como la posibilidad de que ocurra un resultado negativo o indeseado, cuya magnitud dependerá tanto de la probabilidad de que suceda como de la gravedad de sus consecuencias.[40] Entonces, el riesgo es, básicamente, la posibilidad de que una acción produzca un resultado negativo o una pérdida.

Aplicado al tema del presente artículo, Yates y Stone señalan que el riesgo se compone esencialmente de pérdidas potenciales, su gravedad y la incertidumbre de que ocurran,[41] por lo que, el riesgo asociado al uso de la IA en el trabajo surge de la exposición de información confidencial o datos personales sin las debidas medidas de control, a través de un uso irresponsable y poco informado, generando vulnerabilidades que pueden afectar gravemente a la organización. Estos riesgos pueden ser legales, reputacionales y operativos.

4.1 Riesgos Legales, Reputacionales y Operativos por el Uso de IA en el Trabajo

El *riesgo legal*, en las relaciones bilaterales, se refiere a la incapacidad de cumplir los compromisos asumidos, no existir formalización clara o no ajustarse al marco legal establecido.[42] A nivel corporativo, el riesgo legal es la posibilidad de enfrentar sanciones, pérdidas o conflictos jurídicos derivados del incumplimiento normativo o ausencia de mecanismos de cumplimiento y control dentro de la organización.

El uso irresponsable o poco informado de la IA en el trabajo puede generar múltiples riesgos legales, especialmente, en materia de protección de datos personales y confidencialidad de la información. Cuando los trabajadores utilizan herramientas de la IA, sin lineamientos u orientación clara, pueden exponer datos sensibles de los clientes, otros trabajadores, proveedores, y otros sujetos, vulnerando así, el consentimiento y la finalidad legítima del tratamiento.

39 Ibíd, 58.

40 Belkis Echemendía, "Definición acerca del riesgo y sus implicaciones", *Revista Cubana de Higiene y Epidemiol*, núm. 3 (2011): 471, http://scielo.sld.cu/pdf/hie/v49n3/hie14311.pdf.

41 Mariona Portell, María Dolors Riba y Ramón Bayés, "La definición de riesgo: Implicaciones para su reducción", *Revista de Psicología de la Salud*, núm. 1 (1997): 10, https://doi.org/10.21134/pssa.v9i1.819.

42 Pascual López y Altina Gonzáles, *Gestión bancaria: factores claves en un entorno competitivo*, (Madrid: McGraw-Hill, 2008): 230.

Otro tema importante, que tiene el gran avance de la tecnología y la globalización, es el flujo transfronterizo de datos.[43] La transferencia de datos puede entenderse como el envío o transmisión de información personal desde un responsable o entidad hacia otro destinatario, dentro o fuera del país, con el propósito de que dicha información sea tratada o almacenada fuera del entorno original en el que fue recolectada.[44] Cuando esta sea fuera del país, será una transferencia internacional de datos.

El *riesgo reputacional* es la posibilidad de que una organización sufra daños en su imagen o credibilidad pública, afectando no solo su percepción externa, sino generando pérdidas económicas, disminución de confianza y en general, debilitamiento organizacional.[45] Esto ocurre cuando las acciones, decisiones o comportamientos ligados a las empresas no cumplen con las expectativas de sus grupos de interés, o cuando directamente, ha ocurrido una afectación.

En el contexto del uso de la IA como herramienta incorporada en los procesos cotidianos de las empresas, el riesgo reputacional se amplifica cuando se produce un uso inadecuado o poco controlado. Cuando los trabajadores emplean sistemas de IA sin lineamientos éticos y sin comprender sus implicaciones por mal uso, puede ocurrir una divulgación de información confidencial o datos personales, comprometiendo la imagen organizacional.

Por ejemplo, la filtración de datos o mal manejo de la información sensible, puede volverse viral en cuestión de horas, afectando gravemente la confianza del público y la credibilidad de la empresa, a tal punto, de que recuperar el prestigio podría ser muy poco probable.

El *riesgo operativo*, por su parte, se refiere a la posibilidad de sufrir pérdidas derivadas de fallos humanos, deficiencias en los procesos internos, errores tecnológicos o cualquier evento que afecte el funcionamiento normal de una organización.[46] Este riesgo se caracteriza y diferencia de otros por no depender de factores estratégicos o de mercado, sino de la gestión interna y capacidad para mantener la continuidad operativa eficiente, es decir, se encuentra en el núcleo funcional de la empresa.

En materia del uso de la IA en el trabajo, cuando no se gestiona adecuadamente su implementación y supervisión, tienen lugar los riesgos operativos. La productividad y calidad de los servicios podría verse afectada por errores en la configuración de un sistema automatizado, falta de valoración humana en los resultados, pérdida de información o decisiones erradas.

Un ejemplo ilustrativo es el siguiente: El uso abusivo de la IA puede distorsionar la evaluación del desempeño laboral, *¿por qué?* Si un trabajador que emplea herramientas de IA puede completar tareas con mayor rapidez que otro que no las utiliza, se genera una falsa percepción de que su rendimiento es superior o que puede asumir mayores cargas de trabajo, impidiéndoles a los supervisores medir con precisión las habilidades reales y la productividad de su área. Esto genera asignación de tiempos imprecisos para realización de tareas o asignación errónea de personal entre las áreas.

43 Vicente Guasch, "La transferencia internacional de datos de carácter personal", *Revista de Derecho UNED*, núm. 11 (2012): 415, https://revistas.uned.es/index.php/RDUNED/article/view/11139/10667.

44 Vicente Guasch, "Las transferencias internacionales de datos en la normativa española y comunitaria", *Universidad Internacional a Distancia*, (2013): 52, https://hdl.handle.net/20.500.14468/21066.

45 Miguel Vichique De Gasperín, "Riesgo reputacional y gestión institucional de crisis", *Universitat Pempeu Fabra*, (2015): 200, http://hdl.handle.net/10803/292734.

46 Edgardo Castañeda, "Riesgo operativo: medición y gestión", *Revista Académica ECO*, núm. 10 (2024): 25, https://doi.org/10.36631/.

ESTRATEGIAS DE *COMPLIANCE* PARA EL USO ÉTICO Y RESPONSABLE DE LA IA EN EL ÁMBITO LABORAL

1. *LEGAL COMPLIANCE* EN EL TRABAJO

El *legal compliance* puede entenderse como la actividad jurídica orientada a garantizar que una empresa cumpla con las normas, obligaciones y compromisos que le son aplicables, sean estos impuestos por la ley o asumidos voluntariamente.[47] En esencia, implica consolidar una cultura organizacional basada en la legalidad y ética corporativa, a través de la obediencia al marco normativo y la implementación de mecanismos internos que aseguren su cumplimiento.

En ese sentido, se proponen a continuación lineamientos de *legal compliance* orientados a enfrentar la problemática expuesta en líneas anteriores.

2. LINEAMIENTOS DE *LEGAL COMPLIANCE* APLICADOS AL USO DE LA IA EN EL ÁMBITO LABORAL

2.1 Prevención en la gestión del riesgo por el uso de la IA

La *gestión del riesgo* consiste en un proceso sistemático de identificación, evaluación y control de los posibles incumplimientos que puedan afectar, en este caso, el cumplimiento de la normativa aplicable a la organización.[48] En el ámbito de la IA, este enfoque resulta esencial para anticipar y mitigar los riesgos del uso inadecuado, como el manejo indebido de datos personales o información confidencial, o la toma de decisiones sin supervisión humana.

Las empresas deben incorporar la gestión del riesgo como eje central del uso de la IA, estableciendo, en primera instancia, procedimientos que permitan identificar, evaluar y mitigar los posibles impactos legales, operativos y reputacionales derivados de su implementación. Esto incluye:

- Desarrollar mapas de riesgo específicos respecto a la vulneración de la información confidencial y tratamiento indebido de datos personales. El mapa de riesgos es una herramienta, basada en sistemas de información, que permite identificar los procesos sujetos a riesgos, cuantificando la probabilidad de que ocurran y medir su daño potencial.[49]
- Implementar mecanismos de control interno y auditorías internas periódicas que aseguren la identificación de los riesgos y adopción de medidas correctivas oportunas. Mientras que el control interno es el conjunto de medidas orienta-

47 Mariano Teijeira, "Conceptualización en el marco de la regulación corporativa", *Estudios Sobre el Futuro Código Mercantil*, (2015): 936, https://hdl.handle.net/10016/21026.

48 Ibíd, 939.

49 Manuel Rodríguez, Carlos Piñeiro y Pablo De Llano, "Mapa de riesgos: identificación y gestión de riesgo", *Atlantic Review of Economics*, (2013): 2, https://dialnet.unirioja.es/descarga/articulo/4744304.pdf.

das a garantizar el cumplimiento de los objetivos organizacionales, la auditoría interna actúa como una función de evaluación que analiza la eficacia de dichos controles, siendo complementarios entre sí.[50]

- Desarrollar, en el marco de la gestión del riesgo reputacional, mecanismos de prevención, comunicación y defensa de la reputación corporativa, entendida como un activo estratégico.[51] Eso permite la transformación de potenciales amenazas en oportunidades de fortalecimiento de la confianza ante posibles crisis.

2.2 Estudio técnico-legal acerca de las herramientas IA específicas para el giro de negocio de la organización

Un *estudio técnico-legal* es aquel que permite proponer y analizar, en este caso, las diferentes herramientas de IA disponibles, para producir los bienes o servicios que se requieren, en este caso, para las actividades laborales.[52]

Las empresas deben conformar equipos interdisciplinarios integrados por profesionales con formación tecnológica, legal y administrativa para las siguientes actividades:

- Identificar y seleccionar las herramientas de IA disponibles en el mercado que pueden aplicarse a los distintos procesos de la organización, enfocadas en optimizar la productividad.
- Revisar las políticas de privacidad, almacenamiento y tratamiento de datos en cada una de las herramientas de IA, verificando a nivel técnico y legal aquellas cuyas políticas se adecúen al cumplimiento de la normativa vigente en Ecuador.
- Elaborar un registro o listado organizacional, debidamente firmado por los responsables del análisis, que determine qué herramientas de IA pueden utilizarse, según las áreas de gestión.

2.3 Capacitación de sensibilización y aprendizaje práctico sobre el uso responsable de la IA

El *estigma* puede entenderse como una marca social o atributo que, producto de la categorización colectiva, desvaloriza o desacredita a una persona ante los demás.[53] Como se mencionó anteriormente, el uso de la IA en el entorno laboral suele generar estigma entre jefes y trabajadores, percibiéndolo como una amenaza o señal de falta de capacidad, creando desconfianza, juicios erróneos y desigualdades en la valoración del desempeño profesional o calidad de los productos entregados.

Las empresas deben implementar programas de capacitación continua, dirigidos a todo el personal de la organización, conforme a los niveles jerárquicos, desde directivos hasta personal operativo, con la finalidad de fomentar el uso responsable y consciente de la IA, las capacitaciones deberán incluir:

50 Nelson Alarcón, Robinson Aguagallo, Joseane Cevallos y Diego Velasteguí, "Auditoría y control interno en la gestión gubernamental", *Revista Caribeña de Ciencias Sociales*, (2018): 1, https://dialnet.unirioja.es/descarga/articulo/9623141.pdf.

51 Vichique De Gasperín, "Riesgo reputacional y gestión institucional de crisis", 154.

52 Elvira López, Nora González, Susana Osobampo, Adolfo Cano, Rosario Gálvez, "Estudio técnico. Elemento indispensable en la evaluación de proyectos de inversión", *Instituto Tecnológico de Sonora*, (2025): 2, https://www.itson.mx/publicaciones/pacioli/documents/no56/estudiotecnico.pdf.

53 Leopoldo Callejas y Cupatitzio Piña, *La estigmatización social como factor fundamental de la discriminación juvenil*, El Cotidiano, núm. 134 (2005): 65, https://www.redalyc.org/articulo.oa?id=32513409.

- Conceptos básicos de la IA, tipos y beneficios en la productividad en el trabajo.
- Riesgos asociados al mal uso de la IA, enfocados en la confidencialidad de la información y protección de datos personales.
- Estrategias de sensibilización para combatir el estigma asociado al uso de la IA.
- Ámbito práctico de enseñanza sobre cómo se debe utilizar la IA, con la finalidad de cerrar brechas generacionales o tecnológicas asociadas, por ejemplo, a la edad de los trabajadores.

En síntesis, este lineamiento cumple una doble función. Por un lado, busca sensibilizar a los trabajadores y directivos sobre la importancia del uso de la IA como herramienta de innovación y mejora de la productividad, combatiendo los prejuicios y temores asociados a su uso; y por otro, promueve la formación práctica diferenciada según las áreas de gestión, orientada al manejo adecuado de las herramientas de IA, previamente identificadas en el estudio técnico-legal, garantizando su uso ético, responsable y eficiente.

2.4 Protección de la información mediante anonimización y seudonimización

Una vez evaluada la gestión del riesgo, seleccionadas las IAs aprobadas por la organización, y capacitado el personal acerca del uso consciente y responsable de dichas herramientas, corresponde a los responsables, la aplicación de mecanismos de protección de la información confidencial y los datos personales, para ello, las empresas deben:

- Identificar qué tipo de información puede ser procesada, cargada o compartida en las herramientas de IA previamente autorizadas, delimitándolo en la política interna.
- Aplicar mecanismos de protección de datos personales, entre ellas:
  - *Anonimización de datos:* Es la transformación de los datos personales de tal manera que sea imposible identificar directa o indirectamente a la persona a la que pertenecen.[54]
  - *Seudonimización de datos:* Implica sustituir los datos identificativos por códigos o claves que impiden reconocer a la persona, de modo que solo el personal autorizado pueda revertir la identificación.[55]

En general, las empresas deben adecuar el uso de la IA al marco jurídico vigente, cumpliendo lo dispuesto en la LOPDP, su Reglamento General, y las Resoluciones emitidas por la Superintendencia de Protección de Datos Personales, así como los criterios internacionales establecidos en instrumentos como el Reglamento General de Protección de Datos del a Unión Europea (GDPR, por sus siglas en inglés). Además, deben incorporar las buenas prácticas de gobernanza y cumplimiento ético, garantizando así la protección efectiva de la información confidencial y de los datos personales.

54 Yolanda Cano, "La seudonimización y la anonimización de datos personales en las sentencias del orden jurisdiccional social", *Documentación Laboral*, núm. 119 (2020): 41, https://dialnet.unirioja.es/descarga/articulo/7544416.pdf.

55 Ibíd, 40.

2.5 Supervisión humana como obligación ineludible en el uso de la IA en el ámbito laboral

La supervisión humana implica la presencia activa y responsable de una persona capaz de revisar, validar y corregir las decisiones generadas por una IA, garantizando que se ajuste a criterios éticos, legales y técnicos.[56]

Las empresas deben adoptar, como requisito obligatorio e ineludible, que en todos los procesos que involucren el uso de la IA, especialmente, cuando las decisiones derivadas puedan afectar derechos, responsabilidades, información confidencial o relativa a datos personales, la supervisión humana, la cual implica:

- Definir claramente las tareas en las que el juicio humano es insustituible, distinguiendo aquellas que requieren razonamiento ético, aplicación de conocimiento técnico y profesional o tomar decisiones estratégicas, de aquellas tareas de apoyo o naturaleza repetitiva en las que la IA actúa como herramienta auxiliar.
- Para el primer caso, garantizar que, en dichas tareas, toda información o resultado generado por la IA sea revisado y validado por un responsable humano antes de su entrega, aplicación o difusión.

CONCLUSIONES

La IA representa una herramienta de alto potencial en el ámbito laboral, no obstante, su uso inadecuado podría generar impactos negativos y generar perjuicios a la organización y afectación a los derechos fundamentales. La ausencia de una política clara y debidamente definida acerca del uso de la IA, trae consigo riesgos legales, operativos y reputacionales, lo que demuestra que la IA no debe sustituir el juicio humano, sino complementarlo con criterios de responsabilidad y transparencia.

En relación con la confidencialidad y la protección de datos personales, se verificó que la IA introduce desafíos poco trabajados al permitir el procesamiento masivo e inmediato de información. El manejo responsable de dicha información requiere de prevención y gestión del riesgo, estudios de carácter técnico-legal con un equipo interdisciplinario, capacitación y sensibilización para vencer estigmas y brechas, la aplicación de mecanismos claros como la anonimización, la seudonimización y la supervisión humana, así como el empoderamiento del empleador para la reducción de los efectos de la subordinación laboral, en conjunto con el apego estricto a la normativa vigente en la materia.

En referencia a lo anterior, las estrategias de *legal compliance* deben consolidarse como una obligación institucional ineludible. Las empresas están llamadas a implementar políticas claras, meditadas y realizables que garanticen la adaptación tecnológica en el trabajo y mejoren la eficiencia y el cumplimiento normativo. No se trata de resistirse a la innovación, y por ende ocultarla, sino de visibilizarla, comprenderla y aplicarla de forma ética, responsable y consciente, asegurando que la tecnología sirva al ser humano, y no al contrario.

Finalmente, para asegurar la aplicación práctica, la Autoridad de Protección de Datos Personales, quien desempeña un papel clave en el fortalecimiento de esta materia, puede promover códigos de conducta sectoriales conforme lo establece el artículo

56 Ilustre Colegio de la Abogacía de Madrid, "Guía ICAM de Buenas Prácticas para el Uso de la Inteligencia Artificial (IA) en la Abogacía", (2025): 21, https://web.icam.es/wp-content/uploads/2025/10/Guia-ICAM_IA_2025_2.pdf.

53 de la LOPDP y el ejercicio de sus atribuciones de supervisión, control, emisión de directrices y evaluación del cumplimiento previstas en el artículo 76 de la misma norma. En coordinación con el Ministerio de Trabajo y la Asamblea Nacional se debe avanzar hacia la regulación del uso ético, responsable e informado de la IA en el trabajo, asegurando la armonía del ordenamiento jurídico con la tecnología que ya no espera, sino que transforma.

BIBLIOGRAFÍA

Abeleira, Germán. «La memoria: concepto, funcionamiento y anomalías.» *Cuadernos del Tomás*, (2013): 177-190. https://dialnet.unirioja.es/descarga/articulo/4462486.pdf.

Abeliuk, Andrés, y Claudio Gutiérrez. «Historia y evolución de la inteligencia artificial». *Bits de Ciencia* (2021): 14-21. https://doi.org/10.71904/bits.vi21.2767.

Agencia Española de Protección de Datos. *La protección de datos en las relaciones laborales*. Madrid: AEPD, 2021, https://www.aepd.es/sites/default/files/2021-05/la-proteccion-de-datos-en-las-relaciones-laborales.pdf.

Aguilera, Raquel. «El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización». *Revista Trabajo y Seguridad Social, CEF* (2020): 91-134. https://doi.org/10.51302/rtss.2020.886.

Alarcón, Nelson, Robinson Aguagallo, Joseane Cevallos y Diego Velasteguí. «Auditoría y control interno en la gestión gubernamental». *Revista Caribeña de Ciencias Sociales*, (2018). https://dialnet.unirioja.es/descarga/articulo/9623141.pdf.

Álvarez, Henar. «El consentimiento individual y su alcance en la inteligencia artificial aplicada al ámbito laboral». *Documentación Laboral* (2022): 51-68. https://dialnet.unirioja.es/servlet/articulo?codigo=8653043.

Ángels Rius, Serra Montse y Curto Josep. «Introducción al almacenamiento de datos». *Universitat Oberta de Catalunya* (2013): 5-28. https://openaccess.uoc.edu/server/api/core/bitstreams/a3cbc1ac-9150-4df4-bc32-1727f8d41590/content.

Ávila-Tomás, José F., Miguel Mayer-Pujadas y Víctor Quesada-Varela. «La inteligencia artificial y sus aplicaciones en medicina I: Introducción antecedentes a la IA y robótica». *Atención Primaria* (2020): 778-784. https://doi.org/10.1016/j.aprim.2020.04.013.

Cabanelas, José. «Inteligencia artificial ¿Dr. Jekyll o Mr. Hyde?». *Mercados y Negocios* (2019): 5-22. https://www.redalyc.org/journal/5718/571860888002/html/.

Callejas, Leopoldo, y Cupatitzio Piña. «La estigmatización social como factor fundamental de la discriminación juvenil». *El Cotidiano* (2005): 64-70. https://www.redalyc.org/articulo.oa?id=32513409.

Cano, Yolanda. «La seudonimización y la anonimización de datos personales en las sentencias del orden jurisdiccional social». *Documentación Laboral* (2020): 31-56. https://dialnet.unirioja.es/descarga/articulo/7544416.pdf.

Castañeda, Edgardo. «Riesgo operativo: medición y gestión». *Revista Académica ECO* (2024): 23-32. https://doi.org/10.36631/.

Echemendía, Belkis. «Definiciones acerca del riesgo y sus implicaciones». *Revista Cubana de Higiene y Epidemiología* (2011): 470-481. http://scielo.sld.cu/pdf/hie/v49n3/hie14311.pdf.

Ecuador, *Constitución de la República del Ecuador*, Registro Oficial 449, (20 de octubre de 2008).

Ecuador, *Ley Orgánica de Protección de Datos Personales*, Quinto Registro Oficial Suplemento 459, (26 de mayo de 2021).

Ecuador, *Ley Orgánica de Transparencia y Acceso a la Información Pública*, Segundo Registro Oficial Suplemento 245 (7 de febrero de 2023).

Freire-Montoya, Carlos y López-Moya, Daniela, «La subordinación como elemento necesario en la existencia de la relación laboral», *Revista Metropolitana de Ciencias Aplicadas*, (2023):

40, https://remca.umet.edu.ec/index.php/REMCA/article/download/531/527/1610.
García, María. «La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal». *Ciencia Policial* (2024): 91-132. https://doi.org/10.14201/cp.32177.
García-Huguet, Laura, y Magdalena Mut-Camacho. «La deshumanización del arte: inteligencia artificial y ética corporativa». *adComunica* (2024): 329-334.
García-Peñalvo, Francisco, Faraón Llorens-Largo y Javier Vidal. «La nueva realidad de la educación ante los avances de la inteligencia artificial generativa». *Revista Iberoamericana de Educación a Distancia* (2023): 1-28. https://doi.org/10.5944/ried.27.1.37716.
Grau, Daniela, Jorge Parker y José Uzal. «Confidencialidad de la información reservada en la relación laboral». *Universidad de Chile*, 2007.
Guasch, Vicente. «La transferencia internacional de datos de carácter personal». *Revista de Derecho UNED* (2012): 413-453. https://revistas.uned.es/index.php/RDUNED/article/view/11139/10667.
Guasch, Vicente. «Las transferencias internacionales de datos en la normativa española y comunitaria». *Universidad Nacional de Educación a Distancia* (2013). https://hdl.handle.net/20.500.14468/21066.
Hoehn, Marek. «La IA en el trabajo, la innovación, la productividad y las habilidades». *Biblioteca del Congreso Nacional de Chile* (2025): 1-20. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/36969/1/Informe_03_25_IA_en_el_Trabajo_innovacion_productividad_y_habilidades.pdf.
Ilustre Colegio de la Abogacía de Madrid. *Guía ICAM de Buenas Prácticas para el uso de la Inteligencia Artificial (IA) en la Abogacía*. Madrid, 2025. https://web.icam.es/wp-content/uploads/2025/10/Guia-ICAM_IA_2025_2.pdf.
Kumar, Santosh, Anil Mokhade y Neeraj Dhanraj. «An Overview of Machine Learning, Deep Learning, and Reinforcement Learning-Based Techniques in Quantitative Finance: Recent Progress and Challenges». *Applied Sciences* (2023): 1-27. https://doi.org/10.3390/app13031956.
López, Elvira, Nora González, Susana Osobampo, Adolfo Cano y Rosario Gálvez. «Estudio técnico: elemento indispensable en la evaluación de proyectos de inversión». *Instituto Tecnológico de Sonora* (2025). https://www.itson.mx/publicaciones/pacioli/documents/no56/estudiotecnico.pdf.
López, Pascual, y Altina Gonzáles. *Gestión bancaria: factores claves en un entorno competitivo*. Madrid: McGraw-Hill, 2008.
Madrid, Ennio Prada. «Los insumos invisibles de decisión: datos, información y conocimiento». *Anales de Documentación* (2008): 183-196. https://www.redalyc.org/pdf/635/63501110.pdf.
Manuel López, Carlos Piñeiro y Pablo De Llano. «Mapa de riesgos: identificación y gestión de riesgos». *Atlantic Review of Economics* (2013). https://dialnet.unirioja.es/descarga/articulo/4744304.pdf.
Martínez, Andrés, y Francy Ríos. «Los conceptos de conocimiento, epistemología y paradigma, como base diferencial en la orientación metodológica del trabajo de grado». *Cinta de Moebio* (2006). https://www.redalyc.org/articulo.oa?id=10102508.
Pacanchique, Nidia, y Ruby Rodríguez. «El impacto de la inteligencia artificial en el trabajo». *Universidad Libre de Colombia* (2021). https://hdl.handle.net/10901/20588.
Pérez-Montoro, Mario. «El documento como dato, conocimiento e información». *Revista Tradumática* (2003): 1-8. https://revistes.uab.cat/tradumatica/article/view/158/n3-pdf-es.
Pérez-Ugena, María. «La inteligencia artificial: definición, regulación y riesgos para los derechos fundamentales». *Estudios de Deusto* (2024): 307-337. https://doi.org/10.18543/ed.3108.
Portell, Moriona, María Dolors Riba y Ramón Bayés. «La definición de riesgo: implicaciones para su reducción». *Revista de Psicología de la Salud* (1997): 3-27. https://doi.org/10.21134/pssa.v9i1.819.
Real Academia Española. «Confidencial». *Diccionario de la Lengua Española*. Último acceso: 29 de octubre de 2025. https://dle.rae.es/confidencial.

Rouhiainen, Lasse. *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro*. Madrid: Planeta, 2018. https://planetadelibrosar0.cdnstatics.com/libros_contenido_extra/40/39307_Inteligencia_artificial.pdf.

Tamayo y Tamayo, Mario. *El proceso de la investigación científica*. México D. F.: Limusa, 2003. https://www.gob.mx/cms/uploads/attachment/file/227860/El_proceso__de_la_investigaci_n_cient_fica_Mario_Tamayo.pdf.

Teijeira, Mariano. «Legal compliance: conceptualización en el marco de la regulación corporativa». *Estudios sobre el futuro Código Mercantil* (2015): 935-948. https://hdl.handle.net/10016/21026.

Torra, Vicent. «La inteligencia artificial». *Revista Lychnos* (2011): 1-8. https://www.mdai.cat/vtorra/docs/ref.Torra.Lychnos.2011.pdf.

Vichique De Gasperín, Miguel. «Riesgo reputacional y gestión institucional de crisis». *Universitat Pompeu Fabra*, (2013). http://hdl.handle.net/10803/292734.