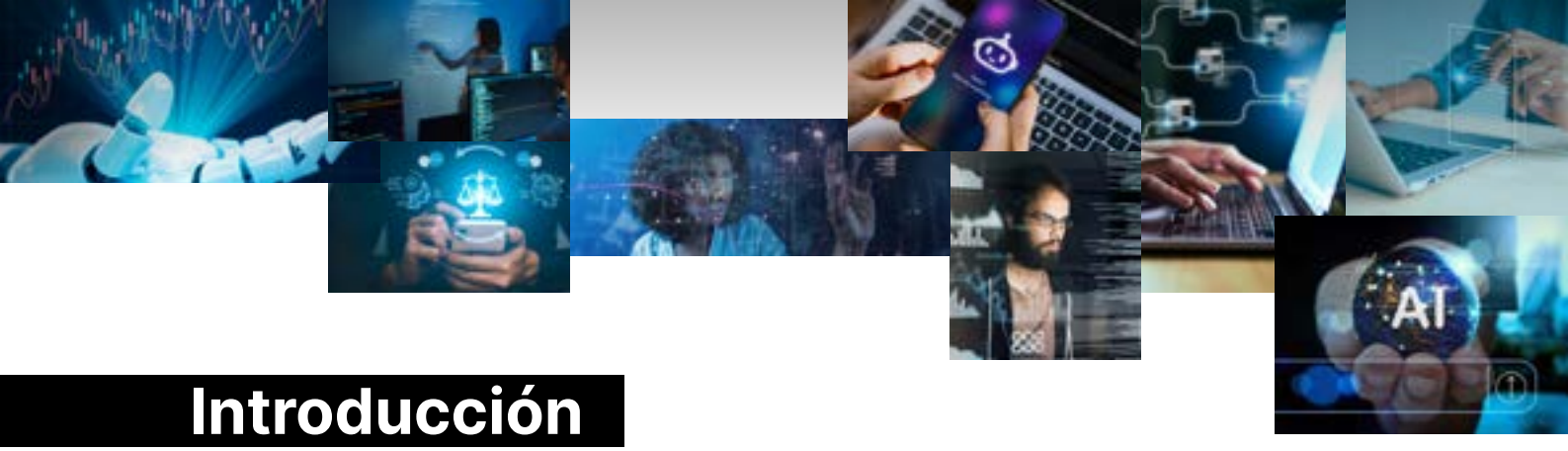
GUÍA PARA IMPLEMENTAR LA INTELIGENCIA ARTIFICIAL »

Experis ManpowerGroup

vaar

Contenidos



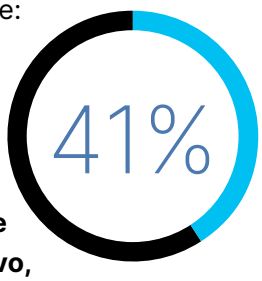
Introducción

La Inteligencia Artificial (IA) ha evolucionado rápidamente hasta convertirse en una de las tecnologías más transformadoras de nuestro tiempo, especialmente tras el lanzamiento de ChatGPT en 2022. Experis y Vaar Law han creado esta guía para ayudar a líderes, profesionales y tomadores de decisiones a aprovechar el potencial de la IA de forma responsable, sostenible y eficiente.

En toda Europa, la IA está transformando las empresas y las instituciones públicas. Una encuesta de Eurostat de 2024 reveló que el 41% de las grandes empresas ya integran la IA en sus operaciones, lo que supone un aumento del 30% respecto al año anterior. El sector público avanza aún más rápido: un estudio de 2024 del Joint Research Center de la UE reveló que el 51.8% de los 576 gestores públicos encuestados, más de la mitad, ya había implementado al menos un proyecto de IA, y el 63.1% planeaba hacerlo.

La IA abre importantes oportunidades de innovación y crecimiento. Puede optimizar las operaciones, aumentar la eficiencia y facilitar nuevos productos, servicios y modelos de negocio. Sin embargo, muchas organizaciones tienen dificultades para convertir el potencial de la IA en resultados tangibles. Los desafíos relacionados con la calidad de los datos, los dilemas éticos, la complejidad legal y los riesgos emergentes suelen obstaculizar el éxito. Esta guía aborda esta situación respondiendo a dos preguntas clave:

- **¿Cómo implementamos estratégicamente la IA para crear valor genuino y evitar desperdiciar recursos en iniciativas con resultados limitados?**
- **¿Cómo podemos adoptar la IA de forma responsable y sostenible, garantizando el cumplimiento normativo, y de riesgos alinado con nuestros valores?**



de las grandes empresas ya integran la IA en sus operaciones.

La implementación de la IA requiere un enfoque holístico: alinear las iniciativas de IA con su visión y valores estratégicos, construir estructuras de gobernanza sólidas e invertir estratégicamente en la gestión de datos, el desarrollo de habilidades, los marcos éticos y la experiencia legal. Y sí, también se debe invertir en la infraestructura tecnológica adecuada para los datos y la IA.

Esta guía ofrece información clara y práctica para ayudar a su organización a navegar por el panorama de la IA y convertir las oportunidades en éxitos duraderos.

Si tiene alguna pregunta o comentario, puede contactar con Jørgen Longva, Director de Competencias de Experis AS, al correo jorgen.longva@no.experis.com o con Thor Beke, Socio Director de Vaar Advokat AS, en thor@vaar.law.

¡Esta guía es de Código Abierto!

Experis y Vaar desean que todas las organizaciones tengan el mejor conocimiento posible sobre el uso de la IA. Por eso, puede usar libremente esta guía para adaptarla a su organización.

La guía cuenta con la licencia CC-BY. Esto significa que puede usar y modificar el texto de este documento si reconoce que se basa en el contenido desarrollado por Experis y Vaar. Tenga en cuenta que esto no aplica a logotipos, marcas ni ningún otro contenido exclusivo de Experis y Vaar.

No dude en contactarnos si desea el documento en formato Word.

Resumen de Capítulos

1 ¿Cómo la IA puede crear valor?

- Reconozca la capacidad de la IA para optimizar, transformar y cambiar radicalmente procesos y productos, en el sector privado como en el público.
- Explore diversas tecnologías de IA para comprender cómo abren nuevas oportunidades.
- Identifique aplicaciones relevantes para su organización inspirándose en ejemplos concretos de diferentes sectores.

2 ¿Cómo su organización puede generar valor a partir de la IA?

- Alinee sus ambiciones con las condiciones y la madurez tecnológica de su organización para identificar las áreas de valor más relevantes para la implementación de la IA.
- Experimente con la IA mediante pequeños proyectos piloto para comprender las oportunidades y limitaciones antes de profesionalizar y escalar las soluciones. Familiarícese con la ilusión del laboratorio y el efecto iceberg.
- Construya una infraestructura tecnológica robusta, que incluya una plataforma de datos y de IA, y establezca un centro de especialización en IA.

3 Consideraciones Éticas

- Asegúrese de que la IA apoye, y no reemplace, el juicio y la toma de decisiones.
- Mantenga la transparencia explicando los procesos de toma de decisiones y garantizando la comprensión entre todas las partes involucradas.
- Pruebe y ajuste los sistemas de forma proactiva para abordar los sesgos, garantizar la equidad y prevenir resultados discriminatorios.

4 Gobernanza, Calidad, y Riesgo

- Implementar estructuras de gobernanza que se alineen a la estrategia de IA con los objetivos de la organización, garantizando roles y responsabilidades claras.
- Supervisar continuamente los sistemas de IA para garantizar su correcto funcionamiento y mantener una alta calidad de los datos.
- Evaluar los riesgos o interrupciones del sistema de IA y establecer planes de contingencia y mecanismos de control para errores inesperados, especialmente en procesos críticos.

5 Comprender las obligaciones legales del uso de la IA en Europa

- Asegúrese de que el uso de la IA cumpla con todas las leyes y regulaciones específicas del sector, incluyendo las leyes de protección de datos y antidiscriminación, la DSA, la DMA, la DORA y la Ley de Ciberresiliencia.
- Desarrolle una estrategia de cumplimiento que integre la comprensión legal con las medidas tecnológicas y realice auditorías periódicas para demostrar el cumplimiento.
- Documente las evaluaciones legales y de privacidad a lo largo de todo el ciclo de vida del sistema de IA para cumplir con los requisitos de cumplimiento.

6 Ley de IA

- Evalúe si el uso de IA en su organización se rige por la Ley de IA.
- Determine la categoría de riesgo de sus aplicaciones de IA.
- Defina su rol como proveedor o usuario, ya que esto afecta los requisitos aplicables.
- Identifique sus obligaciones según el nivel de riesgo y el rol, e implemente las medidas de cumplimiento necesarias.

7 Privacidad y RGPD

- Realizar una evaluación de riesgos y considerar o realizar una EIPD antes de la implementación.
- Implementar las medidas necesarias para reducir los riesgos.
- Desarrollar directrices y rutinas de capacitación, actualizando el protocolo de procesamiento, la declaración de privacidad y la documentación de cumplimiento.
- Mantener las medidas de privacidad continuas con capacitación periódica, políticas accesibles, sistemas de informes y monitoreo continuo de riesgos.

8 Derecho Laboral

- Involucre a los empleados en la implementación de herramientas de IA, solicitando su opinión e informándoles sobre su uso.
- Brinde capacitación para garantizar el uso correcto y legal de las herramientas de IA, compartiendo información y facilitando la retroalimentación de los empleados.
- Asegure el cumplimiento del RGPD, la Ley IA y otras leyes correspondientes al utilizar la IA para fines de Recursos Humanos.

9 Derechos de Propiedad Intelectual

- Reconozca que el contenido generado por IA puede estar protegido por derechos de autor si expresa suficientemente el esfuerzo intelectual.
- Verificar los modelos de IA preentrenados para detectar posible incumplimiento de los derechos de propiedad intelectual, verificando las restricciones impuestas por los proveedores.
- Documentar el uso y las licencias de los datos de entrenamiento para garantizar el cumplimiento de las leyes de derechos de autor aplicables.

10 Términos y condiciones de la Licencia

- Revise cuidadosamente los términos de la solución, centrándose en la propiedad de los datos, la responsabilidad, las limitaciones de uso y los derechos de propiedad intelectual.
- Asuma la responsabilidad por errores o daños causados por los sistemas de IA, ya que la responsabilidad generalmente recae en la organización que los utiliza.
- Evite las soluciones de IA gratuitas siempre que sea posible, ya que suelen conllevar mayores riesgos de vulneración de la seguridad y la privacidad de los datos.

¿Cómo la IA puede crear valor?

La IA puede generar un valor significativo para su organización al mejorar los procesos existentes o introducir soluciones innovadoras. La IA sigue impulsando la innovación y la eficiencia en los sectores público y privado.

Cada vez más empresas deben considerar la IA como un factor competitivo clave en los próximos años. Comprender cómo esta herramienta configura su mercado, cómo aprovechar su potencial y cómo implementarla eficazmente será crucial para mantenerse a la vanguardia.

Para ayudarle a comprender cómo la IA genera valor, exploraremos diferentes tipos de IA y examinaremos cómo pueden transformar diversos aspectos de las operaciones comerciales. Comenzaremos con los tipos de IA más accesibles y utilizados, y gradualmente avanzaremos hacia modelos más avanzados y especializados.

IA Predictiva pronostica resultados futuros basándose en datos históricos. Esto es especialmente útil en la previsión financiera, la predicción de la demanda, la gestión de riesgos y el mantenimiento de equipos. Esta puede analizar grandes cantidades de datos para identificar patrones que indiquen eventos futuros.

Oda: predecir las necesidades del cliente

Oda, una tienda de supermercado en línea, utiliza modelos predictivos de IA para ofrecer recomendaciones personalizadas de productos basadas en las compras anteriores y los patrones de compra de los clientes. El sistema anticipa cuándo los clientes podrían necesitar artículos específicos y sugiere productos relevantes en el momento oportuno.

El algoritmo de IA no solo recomienda artículos de compra frecuente, sino que también sugiere productos similares para aumentar la variedad en el carrito de compra. Esto simplifica la experiencia de compra y anima a los clientes a probar nuevos productos. El objetivo es ofrecer experiencias de compra eficientes que ahorren tiempo y sirvan de inspiración.

Los Modelos de Clasificación organizan y estructuran grandes conjuntos de datos mediante la categorización de la información. Por ejemplo, pueden clasificar correos electrónicos no deseados, identificar clientes en riesgo, filtrar solicitudes de préstamos de alto riesgo o analizar imágenes médicas para diagnósticos.

Los Modelos de Transformación convierten datos de un formato a otro, por ejemplo, traduciendo texto entre idiomas, convirtiendo imágenes en texto o transcripción de grabaciones de audio a texto. También puede transformar datos no estructurados en formatos estructurados, lo que permite la automatización de procesos que antes era inviable o demasiado costosa. Esto se conoce como hiperautomatización.

Un concepto clave aquí es el "último cuello de botella" o el último paso en un flujo de trabajo y su eliminación puede reducir los tiempos de procesamiento de semanas o días a tan solo minutos o segundos. Este cambio logra dinámicas completamente nuevas: innovaciones verdaderamente transformadoras. Un ejemplo son los bancos que ofrecen verificaciones de crédito instantáneas y aprobaciones de préstamos en línea, lo que ofrece una ventaja competitiva gracias al acceso rápido y sin complicaciones al crédito.

IA Generativa, como ChatGPT que crea contenido nuevo, como texto, imágenes, audio y vídeo. Esto lo hace muy adecuado para el desarrollo de material de marketing y soluciones creativas en diseño y desarrollo de productos. También puede convertir datos no estructurados en formatos estructurados para su procesamiento automatizado en sistemas informáticos. Al permitir que las máquinas operen mediante lenguaje natural, los modelos de transformación y generativos permiten a los robots realizar tareas complejas e interactuar de forma más eficaz con los humanos.

IA Optimizada, maximiza la eficiencia en la producción, la planificación de rutas, el uso de materiales y la programación de personal. Estos modelos resuelven problemas demasiado complejos para la programación tradicional. Cuando la IA automatiza y acelera estas tareas, genera nuevas eficiencias en los procesos y permite simulaciones de escenarios para la planificación estratégica.

El Municipio de Bodø utiliza IA Generativa para el manejo de documentos legales

La solución reduce considerablemente el tiempo necesario para resumir documentos legales. Los empleados pueden encontrar rápidamente información precisa y relevante gracias al sistema que utiliza modelos de lenguaje avanzados y tecnologías de búsqueda sofisticada.

Los modelos de lenguaje generan resúmenes precisos de textos legales complejos, reduciendo la necesidad de revisión manual de documentos.

Esto reduce los costos de los servicios legales.

Diseño Generativo es un proceso avanzado en el que la IA explora numerosas posibilidades de diseño basándose en parámetros y restricciones predefinidos antes de presentar soluciones óptimas. Esta tecnología se utiliza en arquitectura e ingeniería, como la planificación de carreteras o la construcción de puentes, para desarrollar diseños innovadores y funcionales. También se aplica para optimizar componentes automotrices y aeroespaciales, reduciendo el peso y aumentando la resistencia.

El Instituto de Investigaciones de Toyota mejora el diseño de autos con IA

El modelo genera numerosas alternativas de diseño que consideran requisitos estéticos, funcionales y técnicos.

Esto permite a los diseñadores evaluar rápidamente numerosos conceptos, reduciendo el tiempo de desarrollo y mejorando la calidad del producto final.

Los Modelos de Aprendizaje Profundo detectan patrones y relaciones complejas. Estos modelos impulsan los vehículos autónomos y los sistemas de recomendación avanzados. Con miles de parámetros refinados mediante un entrenamiento exhaustivo, requieren grandes conjuntos de datos y una gran capacidad de procesamiento. Debido a su complejidad, a menudo funcionan como "cajas negras", lo que dificulta la interpretación de sus decisiones. Esta falta de transparencia plantea dudas sobre la explicabilidad, que analizaremos con más detalle al abordar la ética, la gestión de riesgos y la normativa. La investigación en curso busca desarrollar métodos para explicar las decisiones de IA, especialmente en la administración pública, salud y finanzas.

El Aprendizaje por Refuerzo entrena modelos para comprender entornos complejos, como mercados, sistemas de producción o redes logísticas. Estos modelos mejoran mediante simulación y aprendizaje por ensayo y error. Debido a su complejidad y experiencia requerida, investigadores e ingenieros lo aplican principalmente a problemas particularmente desafiantes.

Los Agentes Autónomos toman decisiones y realizan acciones sin intervención humana. Operan en entornos dinámicos y complejos, como negociaciones de compras automatizadas o robots industriales que trabajan en condiciones peligrosas. Pueden gestionar la logística, controlar las líneas de producción o realizar tareas de mantenimiento en la fabricación. Los modelos de lenguaje avanzados y la IA generativa permiten a estos agentes operar en ámbitos donde los datos no estructurados antes representaban un obstáculo.

AT&T ha desarrollado asistentes de clientes autónomos impulsados por IA

A diferencia de los chatbots tradicionales, que suelen limitarse a respuestas preprogramadas y diálogos sencillos, estos asistentes autónomos utilizan algoritmos avanzados de IA para comprender y responder a consultas complejas de los clientes en tiempo real.

Pueden gestionar una amplia gama de solicitudes, desde soporte técnico hasta consultas de facturación, sin intervención humana.

Esto se traduce en operaciones más eficientes, mayor satisfacción del cliente y la capacidad de atender a un mayor número de personas simultáneamente.

Planificación urbana mejorada

Bedrock y INRIX han desarrollado la solución Bedrock Compass, que crea simulaciones detalladas del tráfico en entornos urbanos.

Los modelos de IA se entrenan con grandes cantidades de datos relacionados con el flujo vehicular, el estacionamiento y el movimiento peatonal.

Los urbanistas pueden generar y evaluar múltiples opciones, lo que les ayuda a encontrar las soluciones más eficientes y sostenibles para el desarrollo futuro.

La IA Causal busca descubrir las causas subyacentes, mientras que los modelos tradicionales solo identifican correlaciones. Por ejemplo, entre el consumo de helado y los ahogamientos existe una correlación pero esto no explica la causa de ninguno de ellos (el clima cálido es una explicación más probable). En la investigación médica, una comprensión más profunda de las causas de las enfermedades puede conducir a tratamientos más eficaces. La IA causal también puede mejorar la gestión financiera al descubrir explicaciones más profundas de los fenómenos económicos..

Simulación de Sistemas Complejos utiliza la IA para predecir resultados en escenarios donde los experimentos en el mundo real serían demasiado arriesgados o costosos.

Por ejemplo, este tipo de IA puede simular reacciones químicas en el desarrollo de fármacos para identificar posibles candidatos antes de las pruebas de laboratorio. En planificación urbana, puede predecir los efectos de nuevas infraestructuras antes de su implementación. Además se utiliza para simular los impactos del cambio climático, lo que ayuda a evaluar las consecuencias ambientales a largo plazo de diferentes medidas políticas. La tecnología también permite probar modelos económicos para comprender los efectos de las tendencias del mercado.

¿Quieres ver más ejemplos de cómo la IA crea valor?

Ejemplo en los sectores público y privado de la UE: AI-WATCH: Observatorio de Inteligencia Artificial de la UE
Ejemplo de Gartner (servicio de pago): Caso práctico de IA e IA Generativa

¿Cómo su Organización puede generar valor a partir de la IA?

La IA es compleja y debe alimentarse con los datos de la empresa para liberar todo su potencial. Esto requiere que la organización cuente con una gobernanza de datos adecuada. Los datos deben ser accesibles, estar bien documentados y ser de alta calidad ¡un reto considerable!. Para tener éxito, su empresa primero debe explorar, desarrollar, probar y aprender sistemáticamente. El siguiente paso es profesionalizar y escalar las iniciativas siguiendo un plan a largo plazo y ágil: una hoja de ruta para la IA.

Muchas organizaciones tienen dificultades para sacar valor de la IA. Ven ejemplos de otras empresas que han tenido éxito, pero se encuentran atrapadas en **la ilusión del laboratorio**, con experimentos estancados en una fase de prueba o no generan beneficios duraderos a gran escala.

Para evitar esta ilusión, es necesario reconocer que la IA no es una herramienta mágica que resuelva todos los problemas simplemente incorporándola a productos y procesos existentes. No se puede confiar en experimentos aislados y esperar avances. Es necesario trabajar sistemáticamente, explorar las áreas adecuadas y realizar rápidamente durante el desarrollo las pruebas antes de avanzar hacia la escalabilidad y la profesionalización. Un enfoque estructurado facilita la prevención de costosos errores y la identificación de las áreas adecuadas donde la IA puede generar valor real.

La Ilusión del Laboratorio

La ilusión de laboratorio se produce cuando una empresa logra el éxito con un prototipo de IA, pero no logra replicar los mismos resultados en producción. Algunas organizaciones ven que sus soluciones fallan de inmediato, pero con mayor frecuencia, la calidad disminuye tras unos meses o años de producción, o los costos operativos y de mantenimiento se vuelven más altos de lo esperado.

Esto puede deberse a una integración deficiente con los sistemas existentes, una calidad de datos inadecuada o la falta de la experiencia necesaria para escalar la solución.

Como resultado, las empresas no logran obtener los beneficios esperados, a pesar de los prometedores resultados iniciales.

Los Datos como prerrequisito para la IA

Los datos son la base de cualquier solución de IA. Para que los algoritmos generen información valiosa o automaticen tareas complejas, deben entrenarse con datos que reflejen la situación real de su negocio. Los datos deben ser accesibles, de alta calidad y estar bien documentados. **Las empresas que controlan sus datos están mucho mejor posicionadas para generar valor con la IA.**

En 2012, comenzó una nueva ola de avances en IA, impulsada por tres tendencias tecnológicas: avances en modelos de aprendizaje profundo para el reconocimiento de patrones, una explosión de potencia computacional fácilmente disponible en la nube y el auge de bibliotecas de software de aprendizaje automático. Estos avances permitieron construir modelos avanzados con mayor rapidez y precisión que antes. Sin embargo, muchas organizaciones pronto se dieron cuenta de que carecían de datos suficientes para aprovechar el potencial de la IA. No bastaba con contar con algoritmos y recursos computacionales potentes; necesitaban datos relevantes para sus necesidades específicas.

A finales de 2022, surgió una nueva ola de entusiasmo por la IA, ya que los modelos preentrenados y de fácil acceso redujeron los datos necesarios para usarla eficazmente. Estos modelos se habían entrenado con conjuntos de datos masivos, lo que les permitió desarrollar conocimientos fundamentales, como la comprensión del lenguaje o el reconocimiento de objetos en imágenes. Como resultado, las empresas pudieron aprovechar la IA con solo una pequeña cantidad de datos. Esto facilitó los inicios, especialmente para empresas pequeñas u organizaciones sin grandes volúmenes de datos históricos.

La ventaja competitiva a menudo se deriva de lo que hace única a una empresa, ya sea conocimiento especializado, productos propios o la capacidad de adoptar nuevas tecnologías. Es posible generar valor a partir de la IA implementando y combinando soluciones listas para usar. La disponibilidad de los llamados "zero-shots models" o aprendizaje cero (modelos que no requieren entrenamiento específico previo) ha aumentado considerablemente. Algunos ejemplos incluyen ChatGPT y Microsoft Copilot, que utilizan modelos preentrenados donde los usuarios simplemente proporcionan información mediante indicaciones o lenguaje natural, a veces combinados con técnicas de búsqueda avanzadas como la Generación Aumentada por Recuperación (RAG). Esto hace que las herramientas impulsadas por IA sean más accesibles, permitiendo a los usuarios generar valor rápidamente.

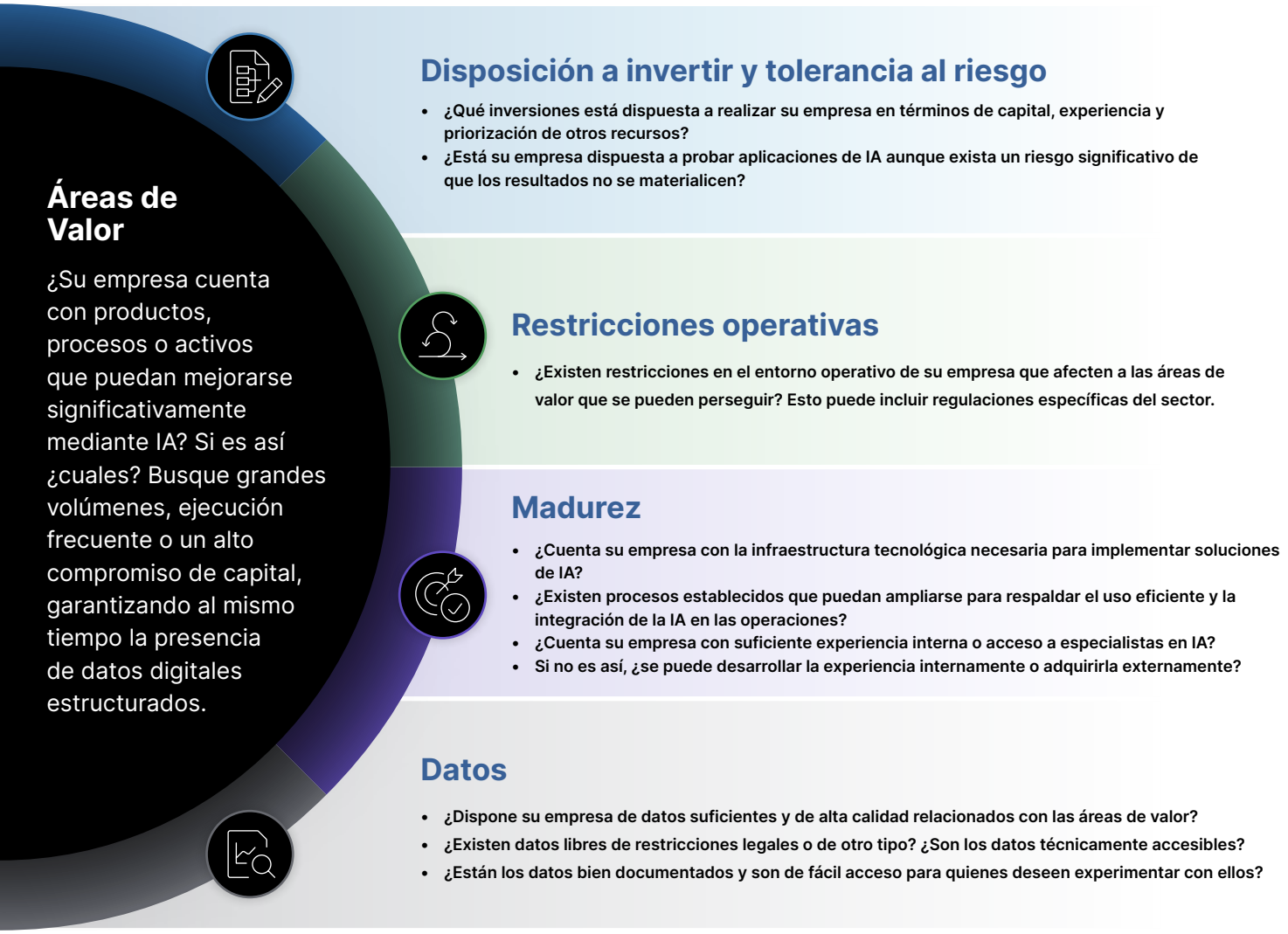
Al mismo tiempo, las organizaciones con acceso a datos completos y específicos del negocio pueden ajustar y adaptar los modelos con mayor precisión. Esto representa una ventaja competitiva clave y duradera. La IA ofrece el máximo valor cuando se aprovecha el poder de los datos de la organización. Al crear soluciones basadas en algo único, se crea una diferenciación frente a la competencia.

Para lograrlo, es fundamental contar con procesos e infraestructura de gestión de datos de alta calidad y accesibles que permiten la mejora continua de los modelos y su adaptación a las necesidades cambiantes. Además, las organizaciones deben abordar las cuestiones de privacidad y cumplir con el RGPD. No basta con tener datos: deben ser accesibles, estar bien documentados y utilizarse de forma legal y ética. Volveremos a estos temas en capítulos posteriores.

Establece el nivel adecuado de ambición

El primer paso que su empresa debe dar para generar valor a partir de la IA es establecer una ambición clara y realista, alineada con las habilidades y la capacidad de su organización.

El siguiente gráfico muestra algunas preguntas clave a considerar:



Algunas empresas comienzan con cautela, optimizando procesos internos específicos. Otras son capaces y están dispuestas a apostar por un enfoque centrado en la IA, situándola en el centro de sus productos y procesos de producción.

Las empresas con grandes ambiciones en materia de IA deben estar preparadas para invertir en una infraestructura integral, equipos dedicados, plataformas de datos avanzadas, procesos de innovación y mejora continua.

Selecciona las áreas de valor adecuadas

Una vez definido el nivel de ambición, identifique sistemáticamente las áreas de valor que se alineen con sus objetivos y capacidades. Comience explorando las aplicaciones transformadoras y disruptivas de la IA:

- **Las Aplicaciones Transformadoras** mejoran y optimizan las estructuras, procesos o productos existentes. El objetivo es aumentar la eficiencia y reducir los costos.
- **Las Aplicaciones Disruptivas** introducen cambios fundamentales al permitir productos, mercados o formas de operar completamente nuevos. Estas innovaciones pueden desafiar o reemplazar los modelos de negocio existentes o transformar industrias enteras.

Otra diferencia importante es si la IA se utiliza internamente para mejorar los procesos de negocio o externamente para crear nuevos productos y servicios:

- **Las Aplicaciones Internas** se enfocan en mejorar la eficiencia operativa, reducir costos o mejorar la calidad de los procesos existentes.
- **Las Aplicaciones Externas** buscan aprovechar la IA para desarrollar nuevas ofertas que proporcionen una ventaja competitiva.

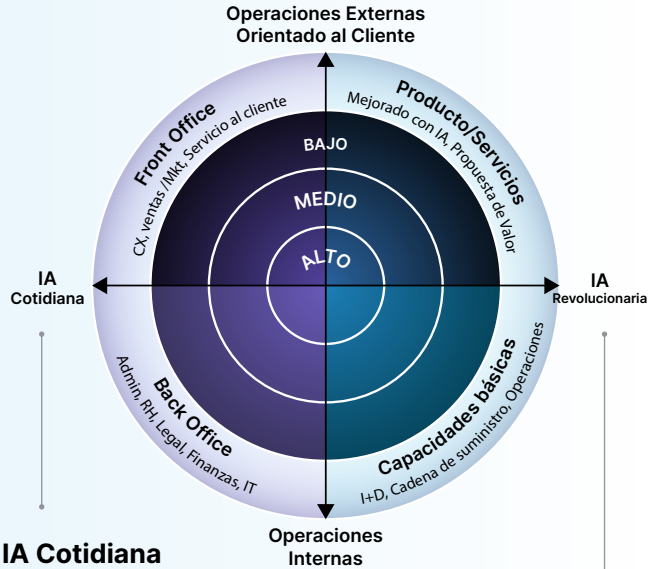
Por ejemplo, una aplicación transformadora de IA externa podría ser, el desarrollo de sistemas personalizados de recomendación en una plataforma de comercio electrónico existente. Esto influiría en la presentación de los productos a los clientes, sin salirse del modelo de negocio establecido.

Una aplicación disruptiva de IA interna podría ser la automatización completa de los flujos de trabajo mediante innovaciones en logística y producción, lo que transformaría radicalmente la gestión de recursos. En este caso, debe estar preparado para una transformación importante, tanto internamente como en colaboración con sus socios.

El radar de Oportunidades IA

La viabilidad es una combinación de:

- Viabilidad técnica
- Preparación interna
- Preparación externa



IA Cotidiana son aplicaciones transformadoras, mientras que **IA Revolucionaria** son aplicaciones disruptivas.

La firma de investigación Gartner ha desarrollado un Radar de Oportunidades de IA que clasifica las aplicaciones de IA según dos dimensiones: el nivel de impacto (transformador vs. disruptivo) y si la aplicación es interna o externa. Además, el radar evalúa la dificultad de implementación de cada aplicación, considerando la complejidad técnica, la disponibilidad interna y la madurez del mercado.

Las aplicaciones en el centro del círculo son fáciles de implementar, mientras que las que se encuentran más alejadas son más difíciles de realizar. Por ejemplo, automatizar tareas administrativas manuales como la facturación o la elaboración de informes puede ser relativamente sencillo y reportar beneficios en términos de ahorro de tiempo y reducción del riesgo de errores. Sin embargo, esto proporciona un valor estratégico limitado, ya que se centra principalmente en optimizar los procesos existentes.

La personalización impulsada por las experiencias de los clientes en todos los canales digitales es una aplicación más compleja. Requiere grandes volúmenes de datos de alta calidad, modelos avanzados de IA y un profundo conocimiento de las necesidades de los clientes. Estas soluciones pueden proporcionar una ventaja competitiva significativa y generar nuevas fuentes de ingresos. Al mismo tiempo, exige una planificación a largo plazo y recursos sustanciales para tener éxito, ya que afectan a múltiples procesos empresariales. Su organización debe estar preparada para invertir una cantidad significativa de tiempo y recursos, sin dejar de comprometerse a pesar de los retos y los contratiempos.

El uso del modelo de radar para posicionar las aplicaciones de IA proporciona un marco estructurado para evaluar dónde y cómo se crea más valor con la IA.

¡Experimenta y aprende!

Al definir su nivel de ambición y priorizar las áreas de creación de valor en consecuencia, establecerá el marco y la dirección adecuados para la creación de valor impulsada por la IA. Dentro de estos límites, deberá explorar, desarrollar, probar y aprender.

Teniendo en cuenta la ilusión del laboratorio —el fenómeno por el cual los buenos resultados de las pruebas piloto a menudo fracasan en la producción—, es fundamental evitar repeticiones excesivamente largas. Debe descubrir lo antes posible cualquier complejidad inesperada y cualquier problema relacionado con la mala calidad de los datos.

Esto significa probar nuevos enfoques de IA a través de proyectos piloto, adoptar una mentalidad de «fracaso rápido» que permita un aprendizaje rápido, ofrecer funcionalidad en muchos pequeños pasos (productos mínimos viables, o MVP) y automatizar todo el proceso, desde el desarrollo hasta la implementación. Por último, debe cerrar el ciclo para que la experiencia adquirida en la producción se retroalimente en las

fases anteriores: idea, concepto, diseño, desarrollo, pruebas y lanzamiento.

Una forma eficaz de empezar es crear un centro de competencia en IA como eje de las iniciativas y nombrar a un coordinador responsable de dirigir y apoyar los proyectos en toda la organización. Esto proporciona estructura y orientación en las primeras fases, al tiempo que garantiza que las iniciativas de IA se ajusten a la estrategia general de la empresa.

¡Profesionalízate y crece!

Su organización ha establecido sus primeras soluciones basadas en IA. Ha obtenido información sobre las fortalezas y debilidades de los diferentes tipos, la calidad de los datos de su organización, lo que se necesita para gestionar y operar soluciones de manera eficaz. **Ahora lo que es más importante, descubrir el iceberg: todo lo que se esconde bajo la superficie a la hora de implementar la IA en un proceso empresarial y garantizar su mantenimiento y desarrollo a largo plazo.** Las soluciones de IA suelen tener una proporción significativamente alta en el costo del ciclo de vida tras su implementación que otras soluciones de TI.

Desarrollar Modelos de IA

Conexión a los datos

Desarrollar Aplicaciones

Cambios en los procesos

Desarrollo de Competencias

Adaptar la infraestructura tecnológica a las nuevas tecnologías

Mejorar y reentrenar los Modelos de IA

Calidad de los datos

Resistencia organizacional

Obstáculos legales

Para seguir creciendo, hay que profesionalizarse y evolucionar:

Desarrollar un plan estratégico de IA – Garantizar que su uso se ajuste a los objetivos y valores de su organización mediante un plan ágil y estratégico.

Establecer una sólida gobernanza de la IA – Ante el rápido ritmo de los cambios tecnológicos, consolide la gobernanza de la IA en la alta dirección para respaldar su estrategia.

Impulsar la innovación en IA de forma sistemática – Explorar, evaluar y priorizar las oportunidades de negocio basadas en IA a través de procesos de innovación estructurados.

Construir una infraestructura de IA escalable – Se requiere grandes cantidades de datos y potencia computacional, lo que exige una infraestructura técnica que permita el entrenamiento, la evaluación y la implementación de modelos.

Proporcione datos de alta calidad y bien administrados – los datos deben ser de alta calidad, estar bien documentados, ser interfuncionables y accesibles. Aborde las preocupaciones éticas, legales y de seguridad mediante una gestión integral de datos en la que participen expertos en TI, legales y del sector.

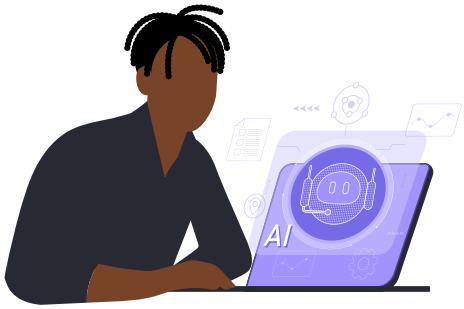
Implemente AIOps para la gestión continua de la IA – mantenga los modelos de IA actualizados con procesos sistemáticos para la integración de datos, el entrenamiento de modelos, su implementación, la evaluación del rendimiento y la supervisión de la seguridad.

Desarrollar competencias en IA en toda la organización – Contratar especialistas en IA y garantizar una formación para los empleados, posiblemente a través de un centro de competencias en IA.

Los siguientes capítulos tratarán las cuestiones **éticas, de gobernanza, riesgo, calidad y consideraciones legales.**

Consideraciones Éticas

La IA ofrece importantes oportunidades, pero también plantea retos éticos. Los sistemas de IA no son éticos ni antiéticos, solo reflejan las decisiones tomadas por quienes los diseñan, entrenan e implementan. Su organización debe garantizar que la IA se utilice de forma responsable, transparente y justa para promover la confianza, el cumplimiento normativo y la creación de valor sostenible.



La ética consiste en comprender y abordar las implicaciones morales de nuestras acciones. Al implementar la IA en su organización, debe evaluar las consecuencias éticas. ¿Se están utilizando sus sistemas de IA de acuerdo con los valores fundamentales y los principios morales de su empresa?

Pero, ¿a qué valores y principios nos referimos? Incluyen los valores de todas las personas que trabajan en la organización y de aquellas afectadas por ella. Se extienden a la sociedad, el ecosistema, la industria o el mercado en el que opera su organización. Algunos principios éticos están explícitamente incorporados en leyes, reglamentos y requisitos que deben cumplirse, mientras que otros sirven como principios subyacentes reflejados en reglamentos, normas tácitas o industriales.

Este capítulo ofrece una visión general de los retos éticos más importantes de la IA. Le ayuda a identificar y gestionar de forma sistemática las cuestiones éticas para que, al utilizarla, genere valor, al tiempo que se alinea con los valores de su organización, respetando los derechos y la integridad de las personas.

El campo de la ética de la IA está evolucionando rápidamente y, con el tiempo, surgirán muchas preguntas y retos nuevos. Debe mantenerse informado sobre estos avances y actualizar las directrices éticas de su organización a medida que se disponga de nuevos conocimientos.

IA enfocada en el Ser Humano y Responsabilidad

El principio ético que se debe priorizar y revisar constantemente es el uso de la IA centrado en el ser humano. La IA debe apoyar, no reemplazar, el juicio y la toma de decisiones humanas, estas herramientas deben mejorar el conocimiento y la experiencia humana. Este principio es especialmente crucial en procesos complejos de toma de decisiones. Los humanos siempre deben tener la última palabra en decisiones cruciales, especialmente cuando la IA influye en las personas de maneras que pueden tener importantes consecuencias sociales o económicas.

La responsabilidad requiere definir claramente quién es responsable del uso de la IA y quién toma las decisiones basadas en los sistemas. Su organización debe establecer funciones claras y garantizar que personal calificado valide y apruebe las soluciones de IA antes de su implementación. También debe indicar claramente quién es el responsable legal si algo sale mal. Deben existir mecanismos de supervisión continua para garantizar que los sistemas de IA funcionen según lo previsto y cumplan las directrices éticas. A medida que evolucionen las normativas relacionadas con la IA, esto será aún más importante.

Transparencia y entendimiento

Para generar confianza en los sistemas, todas las partes interesadas, incluidos: empleados, clientes y responsables de la regulación, deben comprender cómo se utiliza la IA en la organización y las decisiones que respalda. Esto se conoce como transparencia y se aplica tanto al desarrollo como al funcionamiento de las soluciones de IA. La transparencia también significa ser abierto sobre las medidas que se han tomado para garantizar que las decisiones impulsadas por la IA sean confiables. Si su organización no puede lograr una transparencia suficiente con respecto a cómo y cuándo se utiliza la IA, debería considerar herramientas o métodos alternativos.

Para lograr la transparencia, debes ser capaz de explicar cómo los algoritmos llegan a sus conclusiones. **El entendimiento significa que debes ser capaz de explicar los resultados generados por la IA de una manera que los humanos puedan comprender.** Por ejemplo, si se utiliza la IA para optimizar la experiencia del cliente, debe poder explicar por qué determinados segmentos de clientes reciben recomendaciones o soluciones específicas.

Si un algoritmo sugiere una estrategia o decisión concreta, debe quedar claro qué información ha utilizado y cómo ha llegado a esa conclusión. Sin embargo, si la explicación es demasiado compleja para que los seres humanos la comprendan, pierde su propósito. Aunque cada paso del cálculo sea sencillo, si hay demasiados pasos, el resultado no será comprensible. Una explicación excesivamente larga o compleja puede ser tan incomprensible como una caja negra.

El entendimiento permite a los responsables de la toma de decisiones evaluar las recomendaciones generadas por la IA y anularlas si es necesario. Debe combinar la lógica, la ciencia cognitiva y la comprensión de la psicología para garantizar que la IA proporcione explicaciones técnicamente precisas pero comprensibles para los seres humanos. En última instancia, la transparencia y el entendimiento son fundamentales para generar confianza entre quienes poseen, utilizan o se ven afectados por los sistemas de IA.

Equidad y sesgo

La equidad es uno de los problemas éticos relacionados con la IA. Los sistemas pueden reforzar involuntariamente los sesgos sociales existentes, ya que a menudo se entrenan con datos que los reflejan. Por ejemplo, un sistema de IA que evalúa solicitudes de crédito podría discriminar por motivos de género o etnia si los datos de entrenamiento contienen sesgos de este tipo.

Por lo tanto, debe evaluar y ajustar sus sistemas de IA para eliminar los sesgos no deseados. Tenga en cuenta el término «no deseados». Todas las bases de datos contienen sesgos; estos patrones permiten que los algoritmos funcionen al proporcionar señales significativas. El reto consiste en utilizar estas señales de forma constructiva, evitando al mismo tiempo que los sesgos den lugar a resultados injustos. Para lograrlo, es necesario definir la igualdad, utilizando bases de datos diversas, ajustando los algoritmos durante la implementación y estableciendo mecanismos para detectar y corregir los resultados sesgados.

Patrones obscuros y manipulación

Los patrones oscuros manipulan a los usuarios para que tomen decisiones que quizá no habrían tomado si hubieran contado con toda la información. La IA puede amplificar estas tácticas cuando se utiliza para maximizar los beneficios empresariales a corto plazo a expensas de los intereses a largo plazo de los usuarios. Por ejemplo, la fijación dinámica de precios basada en la IA puede explotar los sesgos psicológicos para empujar a los consumidores a pagar más.

Su organización debe asegurarse de que las soluciones de IA no manipulen ni exploten a los usuarios, especialmente a los grupos vulnerables. Dar prioridad a la transparencia y entendimiento ayudará a mitigar el riesgo de los patrones oscuros.

Los patrones oscuros son ilegales según la Ley de IA de la UE y la Ley de Servicios Digitales (DSA).

Dependencia de la IA

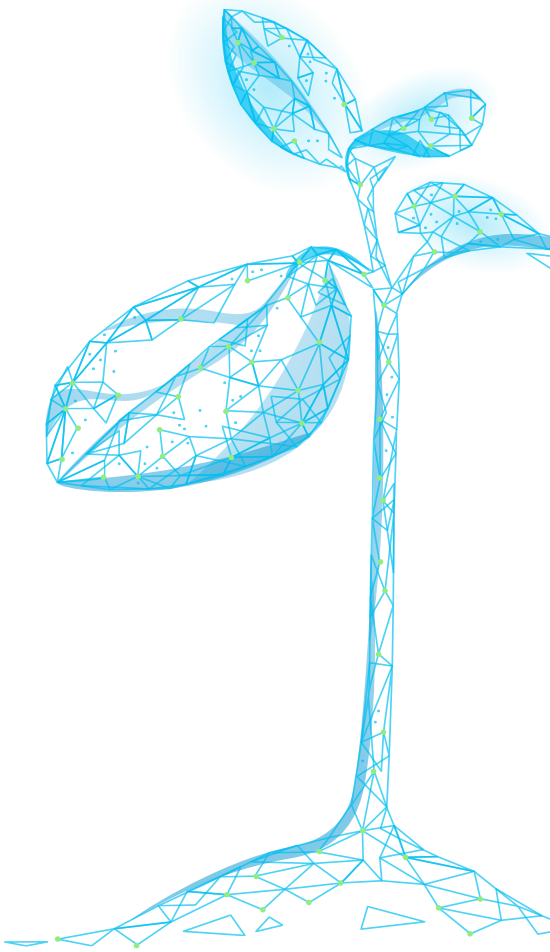
La IA puede convertirse en un problema si se integra en los procesos empresariales básicos sin una evaluación de los riesgos que puedan surgir a largo plazo. La IA es una herramienta valiosa y precisamente por esto, hay que asegurarse de que la experiencia humana y el pensamiento crítico sigan siendo fundamentales. La dependencia excesiva de la IA, especialmente en la toma de decisiones críticas, puede erosionar las habilidades empresariales y aumentar la dependencia de los proveedores de tecnología. Por ejemplo, si su empresa automatiza las interacciones con los clientes mediante IA, debe asegurarse de que la interacción humana siga estando disponible para los casos complejos o delicados.

También existe el riesgo de que la IA se integre tan profundamente en las operaciones comerciales esenciales que la empresa no pueda funcionar sin ella. Si los sistemas de IA dejaran de estar disponibles de forma repentina, debido a cambios en el modelo de precios del proveedor, la interrupción del servicio, la quiebra o cambios tecnológicos importantes, esto podría provocar graves perturbaciones operativas.

Las actualizaciones y los cambios tecnológicos también pueden requerir ajustes organizacionales, lo que aumenta los costos y la necesidad de recursos. Para mitigar este riesgo, es necesario evaluar la estabilidad a largo plazo de toda la cadena tecnológica y desarrollar planes de contingencia para soluciones alternativas.

Impacto ambiental y climático

El entrenamiento de grandes modelos de IA requiere un consumo energético considerable, lo que aumenta la huella de carbono de su organización. Por ejemplo en el caso del aprendizaje automático y el profundo, donde grandes conjuntos de datos exigen una gran potencia computacional.



Para minimizar el impacto ambiental, utilice algoritmos e infraestructura energéticamente eficientes. Optimizar modelos para que consuman menos energía y aprovechar los proveedores de nube comprometidos con las energías renovables puede reducir las emisiones. Estos esfuerzos deben alinearse con una estrategia más amplia de digitalización sostenible, que equilibre los avances tecnológicos con la responsabilidad ambiental.

Si bien los modelos de IA tienen el mayor impacto ambiental durante el desarrollo, el entrenamiento y la fase inicial de producción, su huella continúa a lo largo de su ciclo de vida. Actualizar y adaptar los modelos a medida que crecen los conjuntos de datos suele requerir más energía. La planificación a largo plazo del consumo energético puede ayudar a reducir la huella de carbono general de la IA.

Jerarquías intencionales y dilemas éticos

La adopción de la IA suele presentar dilemas éticos, que requieren un equilibrio entre las oportunidades tecnológicas y las consideraciones éticas. Una jerarquía intencional es un marco valioso para evaluar estos desafíos, ubicando las decisiones éticas en un espectro que abarca desde el cumplimiento normativo básico hasta compromisos más profundos de valores y principios éticos.

En el nivel más bajo, las organizaciones se centran en evitar errores, cumplir con las leyes y minimizar los riesgos reputacionales. En niveles superiores, las decisiones reflejan un compromiso consciente con los valores y la responsabilidad social. La aplicación de jerarquías intencionales ayuda a su organización a evaluar los desafíos éticos desde múltiples perspectivas e identificar soluciones sostenibles a largo plazo. Un enfoque centrado únicamente en el cumplimiento normativo a menudo conduce a una mentalidad reactiva, considerando la ética como una obligación en lugar de una oportunidad. Por el contrario, el trabajo ético sistemático fortalece la cultura interna y mejora la reputación externa.

Cuando nos enfrentamos a dilemas que implican valores contradictorios, existen diferentes enfoques que pueden ayudar a encontrar soluciones. Un ejemplo típico es la tensión entre la privacidad y la necesidad de grandes conjuntos de datos para entrenar modelos de IA. **Una jerarquía intencional puede guiar la toma de decisiones al definir diferentes niveles de respuesta:**

Priorización – la solución más sencilla, pero a menudo menos ideal, es dar prioridad a un valor sobre otro, por ejemplo, anteponiendo la privacidad a la disponibilidad de los datos o viceversa.

Compromiso – un enfoque intermedio que equilibre valores contradictorios, aunque puede dar lugar a resultados subóptimos que no satisfacen plenamente a ninguna de las partes.

Reconciliación – un enfoque más ambicioso busca reducir o eliminar la contradicción entre valores. Por ejemplo, desarrollar tecnologías que minimicen la dependencia de datos de identificación personal.

Beneficio mutuo – el resultado ideal se produce cuando ambas partes se benefician. En el caso de la privacidad y el acceso a los datos, los datos obtenidos mediante síntesis permiten entrenar la IA al tiempo que protegen la privacidad.

No todos los dilemas pueden resolverse por completo, pero un enfoque estructurado para la toma de decisiones éticas y el uso consciente de jerarquías intencionales pueden ayudar a su organización a desarrollar soluciones éticamente sólidas y tecnológicamente robustas. Esto, a su vez, les permite mantener su reputación mientras aprovechan todo el potencial de la IA.

Gobernanza, Calidad y Riesgo

La IA tiene un impacto directo en la calidad y el riesgo. Su organización debe adaptar sus procesos de gobernanza para tener en cuenta las características únicas de la IA en comparación con las tecnologías tradicionales.

En este capítulo, describiremos cómo la IA afecta a la calidad y al riesgo y ofreceremos consejos sobre qué hay que tener en cuenta a la hora de planificar la implementación de la IA en su organización. Para estructurar este debate, lo hemos integrado en un marco de GRC (gobernanza, gestión de riesgos y cumplimiento), abordando específicamente cómo la IA afecta a los procesos de gobernanza, la gestión de riesgos y el cumplimiento de las leyes, reglamentos y políticas.

Gobernanza

La IA desafía los procesos de gobernanza tradicionales de múltiples maneras. Una cuestión clave es que muchos sistemas de IA funcionan como «cajas negras», lo que dificulta explicar cómo los algoritmos llegan a sus decisiones. Esto a menudo genera incertidumbre en cuanto a la rendición de cuentas y el apoyo a la toma de decisiones cuando se utilizan soluciones de IA para decisiones empresariales críticas.

Gestionar eficazmente la IA requiere un enfoque estructurado que precise las responsabilidades y establezca mecanismos de supervisión garantizando la coherencia con los objetivos éticos y organizacionales. Esto comienza con una estrategia de gobernanza que define quién es responsable de los sistemas de IA, cómo se supervisan y qué procesos garantizan la calidad, el cumplimiento y la mejora continua. La estrategia debe integrar la gobernanza de la IA en las estructuras y los procesos de toma de decisiones más amplios de la organización, garantizando que las soluciones se desarrollen, implementen y utilicen de forma responsable y transparente.

Responsabilidad y Transparencia

Si un banco utiliza la IA para la evaluación crediticia, debe indicarse claramente que se está utilizando la IA y quién es responsable de supervisar el rendimiento del algoritmo, gestionar los errores y garantizar que las decisiones se ajusten a las normas establecidas.

Si el sistema de IA toma una decisión injusta o discriminatoria, deben establecerse mecanismos para detectarla y corregirla.

Lineamientos éticos y sesgos

Un modelo de reclutamiento puede favorecer indirectamente a un grupo demográfico debido a datos históricamente desequilibrados, incluso si el modelo no tiene acceso directo a los datos que distinguen a estos grupos. Esto se conoce como efecto proxy.

Los sesgos puede generar problemas éticos, y las organizaciones deben monitorear estos riesgos mediante auditorías periódicas para prevenir su ilegalidad o indeseabilidad.

Monitoreo y Auditorías constantes

Un proveedor de seguros que utilice IA para la evaluación de riesgos descubrirá que el algoritmo pierde precisión con el tiempo, a medida que las condiciones del mercado o el comportamiento del cliente se alejan de los datos con los que se entrenó el modelo.

Por lo tanto, la empresa debe contar con sistemas para realizar auditorías periódicas y ajustes a los modelos para mantener un alto rendimiento.

Para implementar la estrategia de gobernanza de la IA, es necesario establecer estructuras de gobernanza con esta finalidad. **Además de procedimientos, roles y responsabilidades claras, esto puede incluir un comité de ética de la IA o una junta de gobernanza encargada de supervisar las iniciativas de IA en toda la organización. Estos organismos deben garantizar que el uso de la IA cumpla con las políticas internas, los estándares éticos y los requisitos regulatorios.**

Una gobernanza eficaz depende de la definición clara de responsabilidades en toda la organización. ¿Quién es responsable de la estrategia general de IA? ¿Quién supervisa las soluciones tecnológicas? ¿Quién garantiza que las soluciones de IA se alineen con los objetivos éticos y estratégicos de la organización? Una división clara de responsabilidades garantiza que todas las partes interesadas (equipos técnicos, liderazgo y unidades de negocio) comprendan su papel en la gobernanza de los sistemas de IA.

Una gobernanza eficaz de la IA incluye una gestión de calidad estructurada con directrices y procedimientos internos claros.

Otro aspecto de la gestión de calidad de la IA es establecer métodos para validar y probar los modelos de IA antes de su implementación, durante las actualizaciones y mediante evaluaciones de calidad continuas en las operaciones diarias. Garantizar datos de entrenamiento de alta calidad es esencial, desde el desarrollo inicial como en el reentrenamiento posterior. La gobernanza de la IA también debe incluir medidas para mantener la calidad de los datos de entrada utilizados en producción. Las organizaciones pueden fortalecer la gobernanza de la IA mediante el uso de entornos de simulación, validación cruzada y proyectos piloto para probar los modelos antes de su implementación a gran escala.

Gestión de riesgos

A diferencia de los sistemas de TI tradicionales, las soluciones de IA son más dinámicas y, a menudo, difíciles de predecir, lo que dificulta la gestión de riesgos. Estos riesgos incluyen amenazas tecnológicas, como ciberataques a sistemas de IA, y riesgos empresariales y éticos que surgen cuando los sistemas de IA toman decisiones incorrectas.

Antes de implementar soluciones de IA, las empresas deben realizar evaluaciones de riesgos examinando las superficies de ataque, los errores algorítmicos imprevistos y los problemas relacionados con el uso de datos y la toma de decisiones.

También debe evaluar la solidez, es decir, cómo la solución de IA gestiona eventos inesperados. Esto incluye influencias externas como fallos tecnológicos o cambios en las condiciones de los datos. Una solución robusta debe adaptarse a estas situaciones y mantener su funcionalidad o mínimo garantizar un apagado controlado de las funciones en eventos críticos como desastres naturales o incendios.

También debe tener en cuenta y como señala **Inga Strümke** en su libro **Maskiner som tenker (Máquinas Pensantes)**, que los proveedores de soluciones de IA pueden potencialmente insertar un número ilimitado de puertas traseras que los clientes no pueden detectar. Por lo tanto, debe evaluar cuidadosamente los riesgos asociados con los datos antes de agregar información confidencial a una solución de IA.

Los riesgos operativos son una parte crucial de esta evaluación. Los sistemas de IA pueden fallar de forma inesperada, y los fallos de los modelos pueden tener graves consecuencias, especialmente cuando se utilizan en procesos críticos. Recomendamos crear escenarios para explorar cómo podrían comportarse los modelos de IA en diferentes condiciones y planificar posibles escenarios de fallo.

Riesgo Operativo como resultado de la dependencia de la IA

Una solución de IA que supervisa el riesgo financiero en tiempo real puede empezar a realizar evaluaciones incorrectas si se encuentra con nuevos patrones fuera de sus datos de entrenamiento. Si la organización carece de controles manuales o procesos alternativos de toma de decisiones, esto podría tener consecuencias significativas.

Para gestionar el riesgo operativo en el uso de la IA, **es necesario implementar mecanismos de control para detectar errores y medidas de contingencia** — procedimientos alternativos — para garantizar que los procesos empresariales no se paralicen.

En primer lugar, debe evaluar los riesgos asociados al modelo de IA, incluida la seguridad de los datos de entrenamiento y la resistencia frente a ataques como la inversión de modelos y la alteración de datos. Para ello, es necesario comprender bien cómo funcionan los modelos de IA y ser capaz de identificar posibles vulnerabilidades. Además, **debe supervisar continuamente el rendimiento del modelo para mantener su funcionalidad, incluso cuando surjan nuevos patrones de datos o tendencias de mercado.**

Para mitigar estos riesgos, implemente mecanismos de control que monitoreen los sistemas de IA en tiempo real y detecten desviaciones en el rendimiento del modelo o los datos. Estos mecanismos pueden incluir alertas automáticas si un modelo produce resultados inesperados. Esto reduce el riesgo de que decisiones erróneas afecten las operaciones o la reputación de la organización. Monitorear también garantiza que los humanos puedan revisar decisiones cruciales cuando sea necesario.

Ataques de inversión de modelos

Mediante ataques de inversión de modelos, **los atacantes pueden reconstruir información confidencial consultando un modelo de IA entrenado.** Esto es especialmente peligroso para las soluciones de IA que gestionan datos personales, como información de salud o financiera.

La dependencia de proveedores externos de tecnología de IA también tiene riesgos. Al utilizar servicios o modelos externos de IA, las empresas deben evaluar la seguridad, la credibilidad y el cumplimiento de las normativas pertinentes. Es fundamental realizar evaluaciones exhaustivas de los proveedores externos y establecer acuerdos claros que protejan los intereses y los datos de la organización.

Las organizaciones deben establecer procesos de supervisión específicos para cada proveedor para abordar estos desafíos, supervisar el rendimiento de los modelos externos de IA y garantizar la conformidad con los requisitos operativos. Esto ayuda a detectar posibles fallos de inmediato y reduce la dependencia de proveedores sin las medidas de seguridad adecuadas.

Los riesgos legales deben ser considerados. El uso irresponsable de la IA puede dar lugar a infracciones de leyes y regulaciones, como violaciones de la privacidad, vulneraciones de derechos de propiedad intelectual o discriminación. Además, las regulaciones de IA exigen cada vez más que las empresas evalúen, gestionen y mitiguen sistemáticamente los riesgos relacionados con la tecnología. Por lo tanto, debe asegurarse de que sus sistemas de IA cumplan con la legislación aplicable y de que existan procedimientos para abordar posibles desafíos legales. Analizaremos esto con más detalle en el siguiente capítulo.

Sistema automatizado de compra de viviendas de Zillow

Zillow desarrolló un sistema automatizado para la compra de casas **basado en su modelo Zestimate, que utilizaba IA para estimar los valores de las propiedades.**

Cuando la pandemia de COVID-19 provocó fluctuaciones significativas en el mercado inmobiliario, se produjo un evento inesperado, algo para lo que el modelo no estaba entrenado. El sistema carecía de mecanismos para detectar anomalías, lo que provocó que Zillow siguiera comprando viviendas a precios inflados. Esto generó pérdidas financieras y, finalmente, condujo a la decisión de descontinuar el programa.

Además de los controles técnicos, las empresas deben desarrollar un plan de contingencia para gestionar los riesgos operativos asociados a la dependencia de la IA. Este puede incluir el establecimiento de procedimientos manuales y sistemas de emergencia que puedan tomar el control si la solución. Las organizaciones deben estar preparadas para que los modelos de IA pierdan precisión con el tiempo y requieran actualizaciones frecuentes, especialmente en entornos dinámicos, como la predicción del comportamiento del usuario o las tendencias del mercado.

Como se mencionó anteriormente, también es fundamental abordar los riesgos relacionados con la calidad de los datos. Los sistemas de IA dependen de grandes cantidades de datos para funcionar de manera eficaz, y una mala calidad puede dar lugar a resultados inexactos o sesgados. Las empresas deben implementar prácticas eficaces de gestión para garantizar que los datos de entrenamiento sean representativos, precisos y libres de sesgos. Las auditorías periódicas de los datos y los modelos ayudan a mantener una alta calidad y confiabilidad en los sistemas de IA.

Los sistemas de IA pueden presentar riesgos de reputación significativos. Las decisiones incorrectas o discriminatorias tomadas por un modelo de IA pueden atraer rápidamente la atención negativa de los medios y dañar la confianza de su organización entre clientes y socios. Por lo tanto, debe integrar esta amenaza en su estrategia general de gestión de riesgos para abordarlo. Esto incluye estrategias de comunicación claras para responder si los sistemas de IA producen errores o generan resultados controvertidos.

Resultados algorítmicos impredecibles y riesgo reputacional

Los sistemas de IA son complejos, lo que puede dar lugar a situaciones en las que los algoritmos toman decisiones que parecen impredecibles o ilógicas para los usuarios. Incluso si estas decisiones se basan en los datos, estos resultados pueden suponer un riesgo para la reputación de la organización, especialmente si se perciben como discriminatorios.

Para gestionarlo es necesario implementar pruebas automatizadas exhaustivas y límites de seguridad para detectar y abordar situaciones anómalas.

Cumplimiento

La IA presenta nuevos desafíos de cumplimiento normativo a medida que las empresas adoptan estos sistemas. Garantizar que funcione dentro de los marcos legales requiere una estrategia de cumplimiento que integre tecnología, gobernanza y consideraciones legales.

Desarrolle procedimientos sólidos para supervisar, documentar y evaluar las decisiones de IA y el uso de datos. Las auditorías y los reportes periódicos ayudan a demostrar el cumplimiento normativo mitigando riesgos legales.

Aproveche la tecnología para mejorar el cumplimiento normativo, como herramientas para supervisar la toma de decisiones de IA, anonimato de datos o automatizar auditorías para supervisar sistemas de IA complejos.

La colaboración con expertos legales y autoridades reguladoras le ayuda a mantenerse informado sobre las novedades jurídicas y le proporciona orientación sobre las mejores prácticas para cumplir con los requisitos de cumplimiento. Esto puede incluir la participación en foros del sector, grupos de trabajo o programas de certificación sobre el uso responsable de la IA.

El cumplimiento no se trata solo de evitar multas y sanciones, sino también de generar confianza con clientes, socios y organismos reguladores. Las regulaciones tecnológicas suelen basarse en principios éticos fundamentales, transparencia y rendición de cuentas. El objetivo debe ser garantizar que su organización utilice la IA de forma segura y responsable, con procesos sostenibles que se ajusten a los valores internos y requisitos externos. El cumplimiento se vuelve más fácil de gestionar al alinearse con estos principios manteniendo un sistema eficaz de supervisión y mejora continua.

Uso de datos personales en el entrenamiento de IA

Si un modelo de IA se entrena con datos personales sin consentimiento o si estos no pueden eliminarse a petición del usuario, podría infringir el RGPD. Por lo tanto, los sistemas de IA deben desarrollarse e implementarse con mecanismos integrados que permitan a los usuarios ejercer sus derechos, como el derecho de acceso y el derecho al olvido o supresión.

Para cumplir con el RGPD, las organizaciones deben contar con procesos transparentes que regulen el manejo de los datos personales por parte de los modelos de IA, incluyendo el anonimato y protección. Profundizaremos en el siguiente capítulo.

Comprender las Obligaciones legales del uso de la IA en Europa

La regulación de la IA, como la Ley de IA, supone un cambio fundamental en su gobernanza. Sin embargo, las empresas deben tener presentes los marcos legales vigentes que rigen su implementación en materia de protección de datos, administración pública, lucha contra la discriminación, derechos del consumidor y responsabilidad civil siguen siendo igualmente importantes, y cada uno de ellos ya se aplica a la IA.

Comprender la legislación sobre IA en Europa no es tarea fácil, pero se puede decir mucho sobre los principios generales a pesar de las diferencias en las legislaciones nacionales. Si bien las regulaciones de la UE se implementan con variaciones nacionales, a pesar del Brexit y de los países fuera de la UE, Europa comparte una tradición jurídica común que sigue principios similares en muchos ámbitos.

Estos principios generales y similitudes se abordarán en los próximos capítulos de esta guía. Además, en los capítulos anteriores se describieron enfoques para el uso responsable, seguro y ético de la IA que también se alinean con los fundamentos generales para la implementación legal de la IA en Europa.

Como punto de partida general, las organizaciones deben adherirse a las mismas normas regulatorias y requisitos de cumplimiento que rigen el trabajo manual tradicional y las TI. Las leyes y regulaciones vigentes siguen siendo plenamente aplicables, pero presentan desafíos legales para adaptarse a las nuevas capacidades tecnológicas..

Guía de documentos

Esta guía aborda los marcos jurídicos generales de la UE para la IA. Las implementaciones locales pueden variar, por lo que las organizaciones deben consultar con profesionales jurídicos calificados que conozcan la normativa específica aplicable en su jurisdicción antes de implementar y utilizar sistemas de IA. La información proporcionada en esta guía es general y no representa asesoramiento jurídico.

Si bien las aplicaciones pueden variar, varios marcos regulatorios merecen especial atención debido a los riesgos específicos relacionados con la IA. **Los derechos humanos siguen siendo la base de numerosas directrices que rigen el uso de la IA, al igual que en otros contextos. Las leyes de secreto profesional y confidencialidad son particularmente críticas, ya que los sistemas de IA pueden exponer inadvertidamente información sensible mediante el reconocimiento de patrones o resultados no deseados.** En el sector público, los principios de derecho administrativo que rigen la toma de decisiones justa se enfrentan a nuevos desafíos cuando los algoritmos toman o respaldan determinaciones que afectan los derechos individuales. La legislación contra la discriminación es cada vez más relevante, ya que los sistemas de IA pueden perpetuar o amplificar los sesgos presentes en los datos de entrenamiento, lo que podría generar impactos dispares e ilícitos sin una justificación transparente.

Las iniciativas regulatorias digitales de la UE

En los últimos años, la UE ha introducido importantes regulaciones tecnológicas, incluido el RGPD y la Ley de IA, que establecen estándares para la protección de datos, la transparencia de la IA y la rendición de cuentas.

En 2025, la agenda regulatoria de la UE continúa evolucionando, con la Comisión Europea impulsando iniciativas en materia de sostenibilidad, finanzas, ciberseguridad y regulación digital.

Cabe destacar que algunas propuestas anteriores se han retirado o reconsiderado. La Directiva sobre Responsabilidad de la IA se ha descartado debido a la falta de un acuerdo previsible sobre la regulación. De igual manera, las actualizaciones propuestas a las regulaciones de privacidad en línea para los servicios de mensajería se han estancado. La prioridad se ha centrado en implementar las regulaciones existentes y perfeccionar los marcos antiguos para las tecnologías emergentes, la ciberseguridad y la gobernanza de la IA. Las áreas de enfoque actuales incluyen la creación de guías de apoyo a la Ley de IA, la actualización de la Ley de Ciberresiliencia y la implementación de garantías financieras a través de la Ley de Resiliencia Operativa Digital (DORA).

Si bien el proceso regulatorio de la UE sigue siendo metódico, en 2025 se producirán avances continuos en gobernanza digital, junto con esfuerzos para optimizar el cumplimiento normativo en todos los marcos regulatorios. Las partes interesadas deben prepararse para los nuevos requisitos específicos del sector como para la implementación de leyes previamente adoptadas a medida que se desarrollen los mecanismos de cumplimiento.

Las normas de responsabilidad en toda Europa también siguen principios similares. Las empresas que utilizan IA son las principales responsables de prevenir estos daños mediante procedimientos exhaustivos de evaluación de riesgos y protocolos de prueba exhaustivos. Sin embargo, esto experimentará algunos cambios a medida que la Ley de IA se implemente plenamente en los países de la UE, creando responsabilidades escalonadas según los niveles de riesgo.

Este cambio probablemente significará que las empresas deberán esperar requisitos de certificación similares al marcado CE antes de implementar sistemas de IA de alto riesgo. Este panorama requiere un enfoque proactivo tanto para el cumplimiento normativo actual como para la anticipación de los requisitos emergentes.

Para navegar por este panorama de transformación, tanto en términos de responsabilidad como en otras áreas legales, las empresas deben:

Integrar la supervisión legal en el desarrollo de la IA desde el principio.

Asegúrese de cumplir con las regulaciones existentes mientras se prepara para las regulaciones futuras.

Establecer marcos de gobernanza para dar seguimiento a los cambios regulatorios.

Adoptar modelos de IA transparentes y comprensibles para alinearse con los principios de equidad y responsabilidad.

Documentar evaluaciones de riesgos y estrategias de mitigación para escenarios de responsabilidad general como de productos.

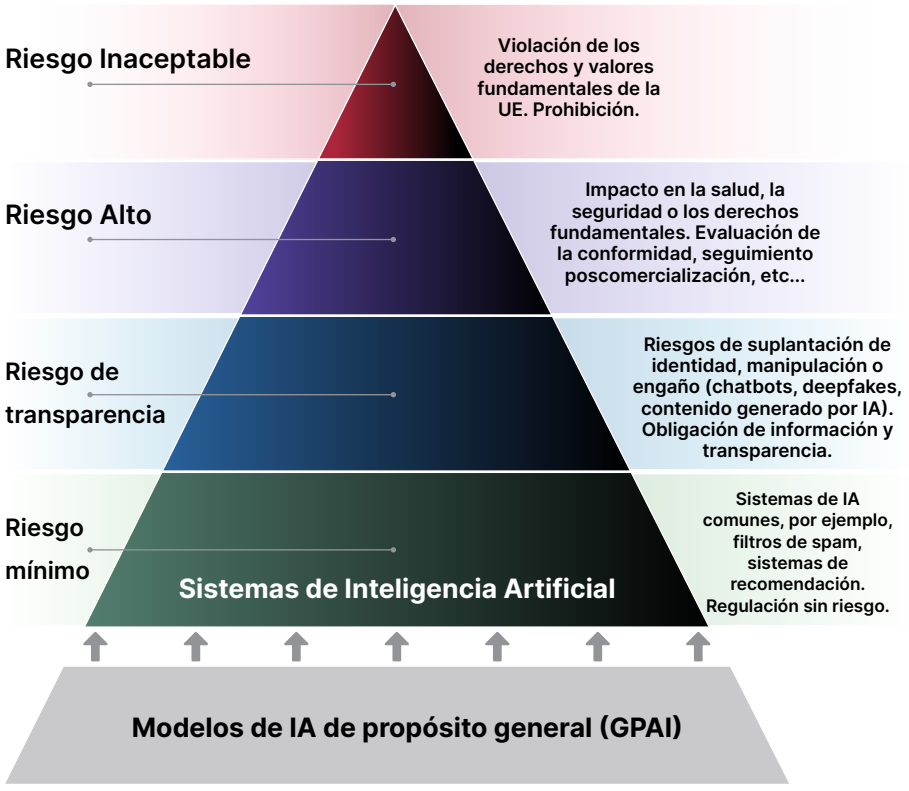
Manténgase informado sobre las regulaciones específicas del sector que pueden aplicarse a sus aplicaciones de IA.

Una empresa que aborda estos desafíos de forma proactiva no solo reduce el riesgo, sino que también fortalece su posición como líder responsable e innovador en los mercados impulsados por la IA.

Ley de IA

La Ley de IA es el nuevo marco legal de la UE para promover el uso seguro y responsable de la inteligencia artificial. Tiene como objetivo equilibrar la necesidad de innovación con la de proteger contra el mal uso de la IA. Esto se hace a través de dos enfoques principales: riesgo y funciones.

La Ley de IA es una regulación basada en el riesgo. Esto significa, que las normas aplicables varían en función de la clasificación de riesgo del sistema de IA.



Modelos GPAI: requisitos de transparencia
GPAI con riesgo sistémico: requisitos de transparencia, evaluación de riesgos y mitigación de riesgos

La Ley de IA prohíbe los sistemas que se consideren un riesgo inaceptable. Esto incluye, por ejemplo, la IA utilizada para manipular o engañar deliberadamente a las personas, los sistemas de "calificación social" o los sistemas utilizados para evaluar la probabilidad de que una persona cometa un acto delictivo basándose únicamente en la elaboración de perfiles. La gran mayoría de los sistemas de IA no estarán prohibidos por la ley y muchos plantean un riesgo mínimo y no tienen requisitos especiales en virtud de la ley. Esto se aplica, por ejemplo, a los filtros de spam y a los sistemas de recomendación.

Las normas para sistemas de alto riesgo son especialmente importantes. Estos sistemas están permitidos, pero deben cumplir con requisitos específicos de cumplimiento y seguridad. Ya que dependen de su función en relación con el sistema.

El artículo 6 de la Ley de IA define dos formas principales de clasificar un sistema de IA como de alto riesgo:

- **La primera forma es cuando el sistema de IA es, o está integrado en, un producto que ya cumple con la legislación de seguridad de productos de la UE.** Esto se aplica a productos cuya seguridad es fundamental, como juguetes infantiles, ascensores y equipos de protección —véase Anexo I de la Ley de IA.
- **La segunda forma es cuando el sistema de IA se utiliza para los fines mencionados en el Anexo III de la Ley de IA.** Si su sistema de IA se utiliza para alguno de estos fines, generalmente se considerará de alto riesgo. El factor común es que pueden afectar directamente la vida y la seguridad de las personas, los errores o sesgos pueden afectar significativamente los derechos fundamentales, la seguridad pública o el trato justo.

Ejemplos de sistemas avanzados en la Ley de IA

Biometría: Sistemas para la identificación biométrica, la categorización biométrica basada en características sensibles y el reconocimiento de emociones.

Infraestructura crítica: Sistemas utilizados como componentes de seguridad en la infraestructura digital crítica y el suministro de agua, electricidad, gas y calefacción.

Educación: Sistemas utilizados para evaluaciones de admisión, resultados de aprendizaje, niveles educativos y seguimiento durante los exámenes.

Empleo y contratación: Sistemas utilizados para el reclutamiento, toma de decisiones de contratación, evaluación de desempeño y el comportamiento de los empleados.

Servicios de bienestar: Sistemas utilizados para evaluar la elegibilidad de servicios públicos, solvencia crediticia y seguros médicos.

Aplicación de la ley: Sistemas utilizados para evaluar el riesgo de delincuencia, la detección de mentiras y la evaluación de pruebas en las investigaciones.

Inmigración y control de fronteras: Sistemas utilizados para evaluaciones de seguridad, solicitudes de asilo e identificación en el control fronterizo.

Justicia y democracia: Sistemas utilizados para el procesamiento de casos legales e influencia en los resultados electorales y la votación.

En cuanto a sistemas de IA de alto riesgo, ya existen varios en uso. **Algunos ejemplos son:**

Uso de IA para evaluar a los estudiantes en las escuelas

Turnitin Gradescope: Una herramienta basada en IA para evaluar y proporcionar retroalimentación sobre las tareas de los estudiantes. El sistema utiliza aprendizaje automático para analizar las respuestas, detectar posibles plagios y ayudar con la calificación según criterios predefinidos. La herramienta está diseñada para agilizar el proceso de calificación para los docentes, pero también plantea dudas sobre la imparcialidad y la precisión de las evaluaciones de estudiantes basadas en IA.

Uso de la IA para la vigilancia policial específica

Palantir Gotham: Ofrece una plataforma basada en IA que las fuerzas del orden utilizan para el análisis predictivo de datos y la inteligencia. El sistema integra grandes cantidades de datos de diversas fuentes para identificar patrones relacionados con la actividad delictiva. Si bien la herramienta puede mejorar la eficiencia policial, también ha recibido críticas por posibles violaciones de la privacidad y el riesgo de reforzar los sesgos existentes en el sistema judicial. Las autoridades aduaneras noruegas utilizan Palantir para identificar a posibles contrabandistas mediante métodos que van desde el reconocimiento de matrículas hasta el análisis de redes sociales. En 2016, la policía noruega firmó un contrato con Palantir, pero el proyecto se detuvo en 2020 antes de su implementación. En ambos casos, la Autoridad de Protección de Datos de Noruega expresó su preocupación. De igual manera, la policía alemana ha recibido críticas por utilizar el sistema, principalmente debido al riesgo de que personas inocentes se vean involucradas en las investigaciones.

Uso de IA como componente de seguridad en la gestión de infraestructuras críticas

Manejo del tráfico impulsada por IA en Verona: En Porta Nuova, una importante intersección vial de Verona, la ciudad está probando un sistema de sensores inteligentes que utiliza inteligencia artificial para analizar datos de tráfico en tiempo real. El sistema combina radares y cámaras para clasificar vehículos, medir la velocidad y detectar infracciones de tráfico. Los datos facilitan la gestión del tráfico, como la regulación de los semáforos. Si bien esto puede mejorar la fluidez del tráfico y reducir las emisiones, plantea inquietudes sobre la seguridad de los datos y el posible uso indebido de la información recopilada.

Para determinar si su sistema de IA se considera de alto riesgo, debe comprobar si su uso previsto se ajusta a alguna de las descripciones del Anexo III. Sin embargo, incluso si su sistema de IA se utiliza de la forma descrita en el Anexo III, no se clasifica automáticamente como de alto riesgo. **Existen excepciones a esta regla general. Su sistema no se considera de alto riesgo si puede documentar que:**

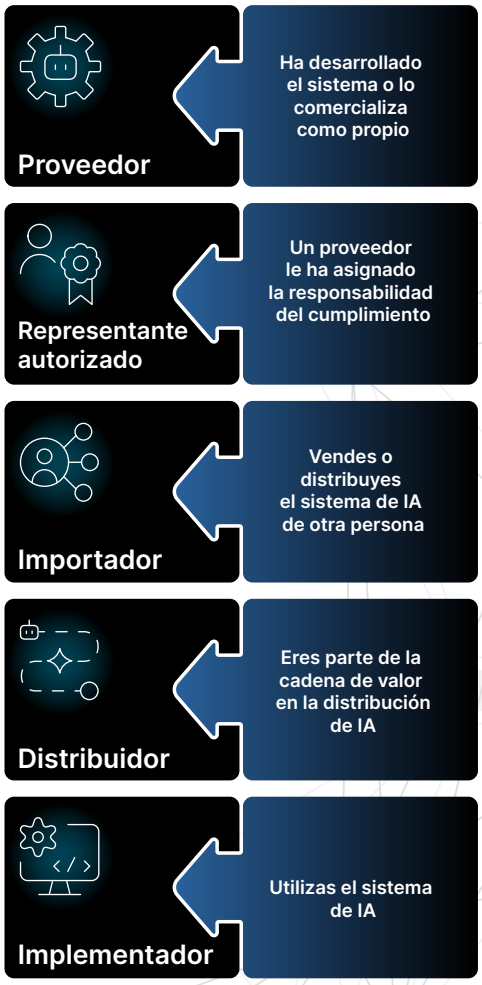
- Realiza tareas sencillas y repetitivas con un margen de error muy bajo.
- Garantiza el control de calidad del trabajo realizado por personas.
- Identifica patrones sin sustituir ni influir en el juicio humano.
- Solo prepara la base para una evaluación mencionada en el Anexo III.

Roles del operador en la Ley de IA

La Ley de IA asigna responsabilidades y obligaciones según el rol específico de cada organización en relación con un sistema de IA. Estos roles determinan las medidas que la organización debe implementar para cumplir con la normativa. Por ejemplo:

- Se le considera **proveedor** si ha desarrollado una herramienta de reclutamiento basada en IA y la ha comercializado o puesto en servicio bajo su propio nombre. Esto significa que es responsable de la clasificación de riesgos y la documentación técnica.
- Se le considera **implementador** si utiliza una herramienta de IA para analizar datos de clientes. Esto significa que tiene ciertas obligaciones de supervisión, implementa medidas de gestión de riesgos y garantiza que los empleados o usuarios finales reciban la información necesaria sobre el sistema.

Roles del operador definidos



Modelos Generales – GPAI

Como se mencionó anteriormente, han surgido numerosos modelos de IA capaces de realizar una amplia gama de tareas. Estos se conocen como IA de propósito general (GPAI). Estas soluciones se entrenan con grandes cantidades de datos diversos y pueden gestionar múltiples tareas. Pueden utilizarse directamente o integrarse en otros sistemas de IA. Por ejemplo modelos de lenguaje de gran tamaño como ChatGPT de OpenAI. Otros modelos GPAI pueden procesar imágenes, audio o datos científicos.

La Ley de IA incluye un capítulo específico con normas específicas para la GPAI. Según la Ley, un modelo GPAI se define como un modelo de IA entrenado con grandes cantidades de datos mediante autosupervisión a escala, capaz de realizar de forma competente una amplia gama de tareas distintas e integrable en diversos sistemas o aplicaciones posteriores. Los modelos con al menos mil millones de parámetros entrenados con grandes conjuntos de datos generalmente cumplen este criterio.

Si implementa un modelo GPAI, debe seguir las normas estándar de la Ley de IA en función de cómo lo utilice y el nivel de riesgo que implique. Sin embargo, se aplican regulaciones específicas si comercializa o desarrolla un modelo GPAI.

Los modelos GPAI están sujetos a un enfoque basado en el riesgo. Los modelos que son especialmente capaces o tienen un impacto social significativo pueden clasificarse como modelos con riesgo sistémico. El riesgo sistémico en los modelos GPAI surge cuando un modelo se encuentra entre los más avanzados, como los que requieren al menos 10^{25} FLOPs (operaciones de punto flotante) para su entrenamiento, un proceso que actualmente cuesta millones de euros, o cuando tiene un impacto social equivalente debido a su escalabilidad, alcance o potencial de daño significativo. Estos modelos están sujetos a requisitos más estrictos, entre los que se incluyen:

- **Documentar cómo funciona el modelo y sus limitaciones**
- **Divulgar los datos utilizados para el entrenamiento**
- **Garantizar el cumplimiento de las leyes de derechos de autor.**

Para el 9 de abril de 2025, el Código de prácticas de IA de uso general de la UE proporcionará orientación detallada para ayudar a los proveedores de modelos GPAI a cumplir con sus obligaciones en virtud de la Ley de IA, en particular en lo que respecta a la transparencia, los derechos de autor y la mitigación de riesgos.

Aprobación de la Ley de IA

El Parlamento Europeo adoptó formalmente la Ley de IA a mitad de 2024 y entró en vigor el 1 de agosto de 2024. **En los Estados miembros de la UE, sus disposiciones se aplicarán gradualmente a lo largo de varios años:**

- **2 de febrero de 2025** – Entra en vigor la prohibición de las prácticas de IA no permitidas, como la puntuación social, las técnicas de manipulación, ciertos sistemas de identificación biométrica y los requisitos de alfabetización en IA.
- **2 de agosto de 2025** – Se vuelven aplicables los marcos de gobernanza y supervisión, incluida la designación de Oficinas de IA por parte de los Estados miembros y las obligaciones de los proveedores de modelos de IA de propósito general (GPAI) y disposiciones sobre sanciones.
- **2 de agosto de 2026** – Fecha de entrada en vigor principal, en la que entrarán en efecto la mayoría de las disposiciones de la Ley de IA, en particular las que regulan los sistemas de IA de alto riesgo. Los Estados miembros deberán tener en funcionamiento al menos un entorno de pruebas regulatorio para la IA en esa fecha.
- **2 de agosto de 2027** – Fecha para la total aplicación de los sistemas de IA de alto riesgo integrados en productos regulados por otras normas de la UE, como los productos médicos, los juguetes y la maquinaria.

La Ley de IA también se incorporará al Acuerdo EEE, lo que garantizará su aplicación en Noruega, Islandia y Liechtenstein. El calendario para su incorporación depende del proceso de decisión del Comité Mixto del EEE y de la posterior aplicación nacional. Cada país del EEE debe establecer las estructuras administrativas necesarias para ajustarse a las disposiciones de la Ley de IA. El lapso de tiempo entre la aplicación de la UE y la incorporación al EEE significa que la aplicación en estos países se retrasará con respecto al calendario de la UE.

Cada país del EEE debe establecer las estructuras administrativas necesarias para ajustarse a las disposiciones de la Ley de IA.

Entorno de pruebas regulatorio

Un entorno de pruebas regulatorio es un entorno controlado donde las empresas pueden desarrollar, probar y validar sistemas innovadores de IA bajo la supervisión de las autoridades competentes. Este enfoque busca fomentar la innovación, garantizando al mismo tiempo el cumplimiento de las leyes y regulaciones aplicables.

De conformidad con el artículo 57 de la Ley de Inteligencia Artificial (Ley de IA) de la Unión Europea, los Estados miembros deben establecer al menos un entorno de pruebas regulatorio de IA, que deberá estar operativo en agosto de 2026. Estos entornos de pruebas proporcionan un marco para la colaboración entre desarrolladores de IA y organismos reguladores, facilitando la implementación segura y ética de las tecnologías de IA.

Algunos países ya han puesto en marcha este tipo de programas **por ejemplo, la Autoridad de Protección de Datos de Noruega (Datatilsynet) ha operado un entorno de pruebas regulatorio desde 2020, centrado en soluciones de IA que mejoran la privacidad.** Esta iniciativa ofrece orientación gratuita a empresas seleccionadas, promoviendo el desarrollo de sistemas de IA responsables y compatibles.

Si bien están surgiendo iniciativas similares en otros Estados miembros de la UE, la implementación y el alcance de los entornos de pruebas regulatorios de IA varían según el país.

Impacto en el Reino Unido y Suiza

Desde su salida de la UE, el Reino Unido ha adoptado un enfoque diferente para la regulación de la IA. El gobierno británico ha decidido no introducir una regulación general de la IA, como la Ley de IA, sino basarse en un marco sectorial que emite directrices específicas para cada ámbito. Sin embargo, las empresas británicas que comercializan sistemas de IA en el mercado de la UE o los utilizan dentro de la UE deben cumplir los requisitos de la Ley de IA.

Además, en virtud del Acuerdo de Windsor, Irlanda del Norte sigue alineada con algunas normativas del mercado único de la UE, lo que da lugar a una posible división normativa en materia de gobernanza de la IA entre Irlanda del Norte y el resto del Reino Unido. Irlanda del Norte puede aplicar la Ley de IA de la UE, mientras que el marco mencionado anteriormente es aplicable al resto de Gran Bretaña.

Suiza, que no es miembro ni de la UE ni del EEE, no se ve directamente afectada por la Ley de IA, aunque las empresas suizas que comercializan sistemas de IA en la UE deben cumplirla. Suiza está evaluando actualmente su enfoque regulatorio en materia de IA.

Privacidad y RGPD

AI adoptar la IA en su empresa, es fundamental evaluar cuidadosamente si el sistema procesa datos personales y en qué medida. Los sistemas de IA suelen trabajar con grandes cantidades de datos, que pueden contener información sobre las personas. Para cumplir con las normativas de privacidad del Reglamento General de Protección de Datos (RGPD), debe implementar medidas que garanticen que los datos personales se gestionen de forma legal, justa y segura.

Recuerde que el RGPD se aplica sin excepciones al implementar IA. Debe seguir el mismo proceso de cumplimiento que con cualquier otro tratamiento de datos personales, o incluso con mayor rigor. Deben cumplirse los requisitos generales de evaluación de riesgos, establecimiento de una base jurídica para el tratamiento y protección de los derechos de los interesados (como el acceso, rectificación, cancelación y oposición). Dado que el RGPD aplica una amplia gama de medidas detalladas, este capítulo solo cubrirá los principios generales del marco.

Cumplir con el RGPD puede ser un desafío al utilizar un sistema de IA ya que a menudo es difícil comprender completamente cómo funciona y qué datos se procesan. Por ejemplo, explicar cómo el sistema toma decisiones puede ser complejo, lo que exige cumplir con las obligaciones de transparencia y proporcionar información significativa sobre la lógica implicada en la toma de decisiones automatizada. Seguir las medidas técnicas y éticas descritas en capítulos anteriores es especialmente importante para abordar estos desafíos.

Evaluación de riesgos y Evaluación de Impacto en la Protección de Datos (EIPD)

El RGPD se basa en la protección de datos desde el diseño hasta el cumplimiento en la posibilidad de riesgo. **Para cumplir con estos estándares, debe proteger activamente los datos personales durante todo su procesamiento mediante la implementación de medidas técnicas que minimicen los riesgos para la privacidad. Esto incluye realizar evaluaciones de riesgos y la integración de medidas de protección de la privacidad en sus soluciones desde el principio.**

Para realizar una evaluación de riesgos exhaustiva, proponemos:

- **Identificar** qué datos personales procesa y dónde se almacenan
- **Reconocer** las amenazas externas e internas a los datos personales
- **Detectar** las debilidades en sus sistemas y procedimientos
- **Evaluar** las posibles consecuencias de las infracciones o la aplicación indebida

El ejemplo destacado de gestión de riesgos en el RGPD es el requisito de la Evaluación de Impacto en la Protección de Datos (EIPD). Se realizará una EIPD cuando el tratamiento pueda suponer un alto riesgo para los derechos y libertades de las personas físicas. Esta evaluación es especialmente importante si utiliza nuevas tecnologías, trata datos personales a gran escala, monitorea sistemáticamente a personas, combina datos personales de múltiples fuentes o trata datos sobre personas vulnerables. En este sentido, siempre recomendamos realizar una EIPD al implementar un nuevo servicio de IA.

Al realizar una EIPD, debe evaluar periódicamente los datos personales que se tratan y su flujo de datos posterior. Además, debe evaluar la probabilidad de que se produzcan incidentes, el posible impacto de las consecuencias y las medidas de seguridad adecuadas para mitigar el riesgo. Esto puede incluir el cifrado, la seudonimización u otras formas de proteger sus sistemas, como procedimientos de formación de usuarios.

Debe realizar una gestión continua de riesgos y realizar una EIPD siempre que el sistema de IA esté sujeto a cambios importantes. También, si lo tiene, debe recordar involucrar a su Delegado de Protección de Datos (DPD).

Requisito de EIPD

Tenga en cuenta que incluso herramientas de IA sencillas como Copilots requieren una Evaluación de Impacto de Protección de Datos (EIPD). Esto no depende del nivel de desarrollo de la herramienta, sino del uso y alcance. Un problema con las herramientas de IA es que los proveedores a menudo no ofrecen información completa sobre su funcionamiento. Esto puede dificultar el cumplimiento de los requisitos de acceso y cancelación.

Documentación

Una documentación adecuada es crucial para el cumplimiento del RGPD. Si no está documentada, no se ha llevado a cabo. Antes de adquirir una herramienta de IA, debe documentar su análisis de compras, las evaluaciones de riesgos, la justificación para elegir soluciones específicas, el proceso de implementación y las modificaciones posteriores. Tras seleccionar una solución, asegúrese de actualizar su Registro de Actividades de Tratamiento (RoPA), la política de privacidad, el registro de consentimiento y documentación relevante.

Si estos procesos se documentan cuidadosamente, completar una EIPD se vuelve mucho más fácil. Considere este ejemplo: Al documentar la justificación para la implementación de una herramienta de IA, incluyendo una descripción del servicio o herramienta de IA, lo que la adquisición pretende mejorar o hacer más eficiente, las ventajas y desventajas de la herramienta, y actualizar la RoPA, ya ha completado varios aspectos de una evaluación.

Un proceso de documentación integral cumple objetivos empresariales que van más allá del cumplimiento normativo. Integrar consideraciones de privacidad en la documentación general de adquisiciones garantiza los principios de transparencia, responsabilidad y equidad. En términos de cumplimiento normativo, la documentación demuestra el enfoque proactivo de la organización para gestionar los riesgos de privacidad asociados con la implementación de la IA.

Categorías especiales de datos personales

Debe conocer los requisitos legales específicos al procesar datos de salud, origen étnico, opiniones políticas o creencias religiosas (categorías especiales de datos personales). Se aplican regulaciones más estrictas a este tipo de datos, tanto para su recopilación como para su uso en sistemas de IA. Las bases legales para el procesamiento de estos datos son limitadas en comparación con los datos personales generales.

Por lo tanto, debe evaluar cuidadosamente si el uso de categorías especiales de datos personales es necesario y proporcionado para la finalidad del sistema de IA. De ser posible, explore soluciones alternativas que no impliquen categorías especiales. Si dicho requerimiento sigue siendo necesario, es importante establecer mecanismos de control de acceso y revisiones periódicas del procesamiento.

Es importante reconocer que los sistemas de IA pueden recopilar datos personales generales para inferir categorías especiales de datos personales. Un ejemplo de esto es cuando investigadores, en colaboración con Facebook, analizaron las publicaciones de texto de los usuarios para predecir la depresión. Basándose en publicaciones y comentarios comunes, el sistema de IA pudo detectar el riesgo de depresión meses antes de que el médico como la propia persona lo supieran.

Preparación de sus empleados

No basta con contar con medidas técnicas y legales, **sino que debe implementar acciones concretas para garantizar que la documentación refleje los procesos y decisiones reales. Una formación eficaz de los empleados es esencial para garantizar el cumplimiento de las normativas de privacidad. Debe integrar la privacidad en los programas de formación existentes, abordando retos prácticos de la IA, como la equidad y cómo identificar y mitigar los sesgos en los sistemas.**

Para garantizar el cumplimiento, su organización debe revisar y actualizar periódicamente los procedimientos de privacidad como parte de su marco de gobernanza.

Privacidad e Innovación

La implementación de nuevas herramientas de IA planteará nuevos retos relacionados con la privacidad, al procesar grandes cantidades de datos de formas que pueden resultar difíciles de auditar o interpretar, lo que se conoce como el fenómeno de la "caja negra". Por ejemplo, puede surgir un reto cuando un sistema de IA procesa datos personales para fines que van más allá de los definidos por la base jurídica original. En tales casos, puede ser necesario obtener un nuevo consentimiento o identificar una base jurídica alternativa para el procesamiento. **Sin embargo, el fenómeno de la caja negra también puede crear otros retos a la hora de cumplir con los derechos de los interesados. Puede resultar difícil proporcionarles información sobre cómo se utilizan sus datos o cumplir con la obligación de cancelarlos. Estos retos se analizarán en este capítulo.**

Es importante recordar que las normativas de privacidad existen para proteger los derechos de las personas, no para obstaculizar la innovación sostenible. El uso de la IA puede introducir nuevos tipos de riesgos para la privacidad pero esto no significa necesariamente que su uso sea ilegal. Algunos riesgos pueden ser aceptables y proporcionados, siempre que se establezcan las medidas adecuadas para minimizarlos en la medida de lo posible y se sopesen cuidadosamente los beneficios del uso de la IA frente a los riesgos. De hecho, las normativas de privacidad ofrecen una flexibilidad considerable cuando se comprenden y se aplican correctamente. En la mayoría de los casos, se pueden desarrollar enfoques que protejan los datos personales y permitan a su organización seguir innovando.

La IA y los principios fundamentales del RGPD

Al desarrollar y utilizar soluciones de IA en su organización, debe aplicar los siete principios fundamentales del RGPD en todo el proceso. Incorporar estos principios en sus prácticas de IA le permite desarrollar soluciones que cumplan con los requisitos normativos, a la vez que promueve la innovación responsable. Este enfoque no solo mejora la protección de la privacidad, sino que también genera confianza con sus clientes y la sociedad en general.

En las siguientes páginas, examinaremos algunos desafíos comunes que pueden surgir al utilizar la IA y ejemplos de estrategias eficaces para abordarlos.

- Limitación de la finalidad
- Reducción de datos
- Precisión
- Limitación de almacenamiento
- Legalidad, equidad y transparencia
- Integridad y confidencialidad
- Responsabilidad

Limitación de la finalidad

Los datos personales sólo deben recopilarse para fines específicos, explícitos y legítimos y no deben procesarse de una manera que sea incompatible con dichos fines.

Desafíos potenciales:

La limitación de la finalidad es un reto en el contexto de la IA, ya que los modelos suelen requerir la recopilación de grandes cantidades de datos durante largos periodos. Esto significa que los datos podrían haberse recopilado sin que el uso de la IA se hubiera planificado o comunicado a los interesados. Si las organizaciones desean utilizar posteriormente estos datos para entrenar modelos de IA, esto podría entrar en conflicto con el principio de limitación de la finalidad, ya que la finalidad original no contempla este nuevo uso.

Además, los sistemas de IA pueden identificar patrones en los datos que las organizaciones desean aprovechar para nuevos fines, lo cual podría ser ilegal y contradecir el principio de limitación de la finalidad.

Nuestro consejo:

Para abordar estos desafíos, su organización debe considerar los usos futuros al seleccionar la base legal para el procesamiento. El entrenamiento y el uso de la IA a menudo requieren una base legal actualizada o nueva, que puede implicar la obtención de un nuevo consentimiento para el procesamiento de datos.

Recuerde que el consentimiento es solo una posible base legal. Dependiendo de su aplicación de IA, otras bases podrían ser más apropiadas.

Al desarrollar marcos claros y predefinidos para el uso de la IA, la organización puede anticipar y gestionar mejor cualquier necesidad de una nueva base legal para el procesamiento.

Reducción de datos

El tratamiento de los datos personales debe ser adecuado, relevante y limitado a lo necesario en relación con los fines para los que se tratan, únicamente si el fin del tratamiento no pudiera alcanzarse razonablemente por otros medios.

Desafíos potenciales:

La reducción de datos resulta especialmente difícil en IA, ya que los modelos de aprendizaje automático suelen requerir grandes cantidades de datos para su entrenamiento y desarrollo.

Determinar qué datos específicos se necesitan antes de evaluar el rendimiento del modelo puede ser complicado. Como resultado, se pueden recopilar más datos de los necesarios para mejorar la precisión del modelo, lo que podría no estar alineado con el principio de reducción de datos.

Además, los sistemas de IA pueden generar nuevas necesidades de datos a medida que evolucionan.

Nuestro consejo:

Comience por definir el propósito y los datos necesarios para lograrlo. El primer paso es eliminar los datos de entrada innecesarios durante el proceso de desarrollo. Esto suele ser beneficioso para la calidad del modelo, la estabilidad, el tiempo de respuesta, los costos operativos y el impacto ambiental.

Métodos como los datos sintetizados pueden reducir la necesidad de datos personales en los conjuntos de entrenamiento. Otro enfoque que puede ayudar a limitar el uso de datos personales es el aprendizaje federado, que entrena modelos localmente en los dispositivos de los usuarios sin necesidad de recopilar datos sin procesar en una base de datos centralizada.

Si bien los datos sintetizados y el aprendizaje federado pueden reducir la necesidad de procesar datos personales, aún presentan desafíos en cuanto al principio de reducción de datos. Los datos sintetizados a menudo requieren un conjunto inicial de datos reales, y el aprendizaje federado implica la recopilación de datos, aunque estos no se transmitan a un tercero.

Precisión

Los responsables del tratamiento deben garantizar que los datos personales sean precisos y, cuando sea necesario, se mantengan actualizados. Deben tomar todas las medidas razonables para eliminar o rectificar los datos personales inexactos, teniendo en cuenta los fines para los que se tratan.

Desafíos potenciales:

Garantizar la precisión de las soluciones basadas en IA puede resultar complejo, ya que los modelos de IA aprenden a partir de datos reales, que pueden ser inexactos u obsoletos. Los errores en los datos pueden amplificarse durante el proceso de entrenamiento, lo que da lugar a decisiones incorrectas o sesgos en los resultados del modelo.

Esto puede dar lugar al procesamiento y almacenamiento de datos personales incorrectos, lo que viola el requisito de precisión y actualización de los datos personales.

Otra cuestión es que muchos modelos de IA funcionan como "cajas negras", lo que dificulta comprender cómo se toman las decisiones y, por lo tanto, resulta más complicado identificar y rectificar los errores.

Nuestro consejo:

Implementar un seguimiento y una validación continuos de las fuentes de datos y del rendimiento de los modelos de IA.

Utilizar algoritmos de IA explicable (XAI) que proporcionen información sobre cómo se toman las decisiones, lo que facilita la detección y rectificación de errores.

Establecer procedimientos sólidos y un seguimiento automatizado para garantizar que los datos de entrenamiento se mantengan actualizados y reflejen con precisión las condiciones relevantes, al mismo tiempo que se evalúa si los resultados del modelo cumplen los requisitos de precisión para el tratamiento de datos personales.

Limitación de almacenamiento

Los datos personales sólo deben conservarse en una forma que permita la identificación de los interesados durante el tiempo que sea necesario y para los fines para los que se procesan.

Desafíos potenciales:

En el contexto de la IA, la limitación de almacenamiento va más allá de la eliminación de datos personales, ya que también se aplica a cómo los datos de aprendizaje influyen en los modelos completamente entrenados.

Incluso después de eliminar los datos, la información sobre las personas incluidas en el conjunto de datos de entrenamiento puede seguir presente indirectamente en el modelo. Esto crea el riesgo de "ataques de inversión", donde los atacantes pueden reconstruir datos personales del modelo basándose en su resultado.

Esto supone un reto importante para el cumplimiento de los requisitos del RGPD sobre el derecho al eliminar y el principio de limitación de almacenamiento, ya que es difícil garantizar que los datos se olviden por completo.

Nuestro consejo:

Las organizaciones deben utilizar técnicas que garanticen que los datos personales individuales no puedan identificarse ni reconstruirse a partir de los resultados del modelo de IA. Un enfoque consiste en introducir ruido controlado en los datos: ligeras variaciones controladas en los datos utilizados por el modelo de IA, lo que dificulta o imposibilita la vinculación de los resultados del modelo con una persona específica. Esto ayuda a proteger los datos personales incluso cuando se han utilizado en el entrenamiento.

Sin embargo, el RGPD exige que los datos se eliminen por completo cuando ya no sean necesarios para el fin indicado. Este método no es suficiente para cumplir con los requisitos de borrado del RGPD se deben implementar procedimientos claros para la eliminación de datos, no solo para su procesamiento, sino también para la gestión de los datos de entrenamiento y los resultados del modelo.

Legalidad, equidad y transparencia

Todo tratamiento de datos personales debe ser legal, equitativo y transparente para las personas. Deben de conocer para qué se recopilan, utilizan y consultan y en qué medida se tratan o se tratarán dichos datos.

Desafíos potenciales:

Surge un desafío legal cuando los modelos de IA identifican patrones en datos personales sin que el procesamiento esté amparado por una base legal clara y explícita.

Los modelos que funcionan como una "caja negra" también pueden dificultar la imparcialidad de las decisiones. El sesgo en los datos de entrenamiento puede cuestionar el principio de imparcialidad al generar involuntariamente resultados discriminatorios por motivos de género, etnia o edad.

Además, la naturaleza compleja e impredecible de los sistemas de IA dificulta explicar cómo se toman las decisiones. Esto puede cuestionar los requisitos de transparencia del RGPD, ya que las personas tienen derecho a comprender cómo se procesan sus datos personales.

Cuando se utiliza la IA para la toma de decisiones automatizada con efectos significativos en las personas, se aplican protecciones adicionales, incluido el derecho a la revisión humana.

Nuestro consejo:

Para garantizar la legalidad, debe existir una base jurídica para todo tratamiento de datos, como el consentimiento o el interés legítimo, y las organizaciones deben mantener registros al respecto. Deben realizarse auditorías y supervisiones periódicas para garantizar que el modelo siga siendo justo y transparente en sus decisiones.

Los sistemas de IA y sus conjuntos de datos deben someterse a una evaluación de sesgos para garantizar que las decisiones no discriminen en función de categorías especiales de datos personales, como el estado de salud o el origen étnico. Utilice métodos de prueba de sesgos, como la comprobación de resultados en diferentes grupos demográficos, para identificar posibles problemas de discriminación.

Las organizaciones deben implementar modelos de IA explicables (XAI) que proporcionen información clara de los procesos de toma de decisiones.

Integridad y Confidencialidad

Los datos personales deben ser tratados para garantizar una seguridad y confidencialidad adecuadas, incluida la protección contra el acceso no autorizado o ilegal, la pérdida accidental, la destrucción o el daño, mediante medidas técnicas y organizacionales adecuadas.

Desafíos potenciales:

La IA suele procesar grandes volúmenes de datos, lo que aumenta el riesgo de vulneraciones de seguridad, como hackeos, filtraciones o accesos no autorizados. Esto puede provocar la exposición de datos personales.

Si los modelos no se diseñan o entrenan correctamente con medidas de anonimato, pueden exponer inadvertidamente datos personales en sus resultados. Esto crea un conflicto entre la necesidad de accesibilidad a los datos para el rendimiento del modelo y la necesidad de proteger la confidencialidad de las personas.

El uso de proveedores externos para servicios de IA también conlleva riesgos considerables. La organización puede ser responsable de las vulneraciones de confidencialidad si no implementa las medidas de seguridad adecuadas y deben garantizar que todos los encargados del tratamiento de datos cumplan con los requisitos del RGPD.

El control de acceso puede ser complicado cuando varios departamentos o empleados utilizan sistemas de IA. Sin embargo, el acceso no autorizado puede comprometer tanto la integridad como la confidencialidad de los datos.

Nuestro consejo:

Para garantizar la integridad y la confidencialidad de las soluciones de IA, su organización debe establecer protocolos de seguridad como el cifrado de datos, el control de acceso y el monitoreo periódico para reducir el riesgo de acceso no autorizado y fugas de datos.

Priorice el entrenamiento de los modelos de IA con datos anonimos siempre que sea posible. Implemente limitaciones de acceso a lo estrictamente necesario y desarrolle medidas de seguridad que impidan que los modelos revelen información personal.

Al utilizar proveedores externos, establezca acuerdos de procesamiento de datos seguros (APD) o limite el uso de servicios que no garanticen la seguridad adecuada de los datos personales.

Desarrolle políticas internas claras de control de acceso. Otorgue a los empleados acceso basado en el principio del mínimo privilegio y garantice la capacitación en privacidad y seguridad de los datos. Solucione rápidamente los errores y los datos dañados para mantener la integridad de los mismos.

Responsabilidad

El responsable del procesamiento de datos personales y del cumplimiento de otros principios será el controlador, quien implementará las medidas y registros adecuados para demostrar dicho cumplimiento.

Desafíos potenciales:

La complejidad de los sistemas de IA, especialmente aquellos propensos al fenómeno de la «caja negra», crea importantes obstáculos para los requisitos de documentación y protección de datos.

Su organización debe demostrar que ha tomado las precauciones necesarias y ha implementado las medidas de seguridad adecuadas. Esto requiere una documentación exhaustiva del diseño del sistema de IA, los datos de entrenamiento y el razonamiento que hay detrás de las decisiones del sistema.

El principio de responsabilidad exige a las organizaciones mantener un control total sobre todo el ciclo de vida del sistema de IA, incluidas las evaluaciones de impacto de la protección de datos (DPIA).
.

Nuestro consejo:

Para garantizar la rendición de cuentas, las organizaciones deben diseñar e implementar marcos de gobernanza que documenten el cumplimiento de las normativas de protección de datos a lo largo de todo el ciclo de vida del sistema de IA. En el caso de los sistemas de IA de alto riesgo, se deben realizar evaluaciones de impacto para identificar y mitigar los posibles riesgos para la privacidad antes de su implementación. Esto incluye la creación y el mantenimiento de documentación técnica detallada sobre el diseño del sistema de IA, los datos de entrenamiento y los procesos de toma de decisiones, con el fin de garantizar la transparencia para las autoridades supervisoras y los interesados.

Los sistemas de IA deben someterse a auditorías sistemáticas para garantizar el cumplimiento del RGPD, incluidas pruebas de sesgo y actualizaciones de seguridad según sea necesario.

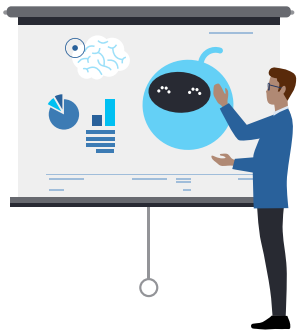
Es fundamental contar con lineamientos claros y una asignación de responsabilidades en materia de privacidad de los datos, formar a los empleados pertinentes para garantizar un seguimiento adecuado, implementarse medidas de seguridad, como el cifrado, controles de acceso y el registro de las actividades relacionadas con los datos, para proteger eficazmente los mismos.

Derecho Laboral

La IA está transformando el entorno laboral y desafiando los marcos legales tradicionales. Si bien mejora la eficiencia y crea nuevas oportunidades, también plantea importantes cuestionamientos y consideraciones éticas sobre los derechos y la privacidad de los empleados.

Como se mencionó anteriormente, la IA puede mejorar fundamentalmente la eficiencia empresarial. El enfoque más directo es proveer a los empleados de herramientas de IA que mejoren su productividad. Como empleador, puede determinar la organización y los métodos de trabajo bajo su autoridad. Sin embargo, dentro de la UE y el EEE, esta facultad directiva está limitada por los derechos de los trabajadores a la información, la consulta y la participación, según lo define la legislación nacional. Si bien estos requisitos de consulta varían en detalle entre los Estados miembros, comparten principios en común.

La legislación laboral europea exige que los empleadores consideren factores como la formación, el desarrollo de competencias y la participación de los empleados, aunque los requisitos específicos varían según la jurisdicción. En algunos países, es necesario consultar a los comités de empresa o a los representantes de los trabajadores antes de implementar cambios significativos en los procesos de trabajo. Los empleadores deben consultar la legislación laboral nacional y los convenios colectivos aplicables para comprender las obligaciones precisas en su país antes de implementar sistemas de IA.



Se requiere formación especializada cuando los empleados deben adaptarse a nuevos flujos de trabajo integrados con IA. Como empleador, asegúrese de que los empleados reciban formación y apoyo continuo para incorporar eficazmente estas herramientas en sus tareas diarias. También debe promover el uso responsable de la IA, teniendo en cuenta los diferentes niveles de competencia de su plantilla.

Algunos miembros del personal pueden mostrar incertidumbre, escepticismo o resistencia al cambio tecnológico. Abordar estas inquietudes es esencial para una implementación exitosa.

Formación y Competencia

Antes de exigir a los empleados que utilicen IA, debe asegurarse de que reciban una formación adecuada y específica. Deben dominar el uso de herramientas de IA y comprender las implicaciones éticas y legales que rigen su uso.

Justificación y Responsabilidad

Como empleador, debe establecer un argumento comercial claro para implementar la IA. Debe existir una necesidad operativa legítima para mejorar la eficiencia o la calidad del trabajo, por ejemplo, para mantener la competitividad en el mercado. También debe evaluar cómo afectará el uso de la IA al entorno laboral. Si se identifican posibles impactos negativos, debe implementar las medidas de protección adecuadas para mitigarlos. Esto se conoce como el requisito de implementación responsable.

Participación e implicación de los empleados

Si la implementación de la IA cambia la forma de trabajar de los empleados, la legislación nacional podría exigir la participación de los empleados y sus representantes antes de finalizar el cambio. El momento de aplicación de esta obligación y su forma de cumplimiento pueden variar según el país. Los empleados deben tener oportunidades significativas para aportar su opinión sobre cómo se integrarán las herramientas de IA en las operaciones diarias.

RGPD: Requisitos y restricciones en el ámbito laboral

Las herramientas de IA ahora también pueden aplicarse a los recursos humanos, la administración y la gestión. Durante la última década, han aparecido en el mercado herramientas para los procesos de contratación, supervisión, evaluación y retroalimentación. Antes de implementar dichas herramientas, usted, como empleador, debe evaluar minuciosamente su funcionalidad, aplicación y resultados a la luz de la normativa aplicable.

Es importante señalar que el RGPD también se aplica al tratar datos de empleados. Para garantizar el cumplimiento, debe:

- Informar a los empleados sobre cómo se utiliza la IA y cómo se procesan los datos personales en este contexto.
- Permitir a los empleados acceder a la información que el sistema de IA procesa sobre ellos.
- Corregir la información inexacta cuando los empleados lo soliciten o cuando se detecten errores.

También es importante tener en cuenta que las decisiones basadas en IA en el entorno laboral pueden tener consecuencias significativas para cada empleado. El RGPD incluye requisitos específicos para la toma de decisiones automatizada y la elaboración de perfiles de los interesados. Estos requisitos se aplican si se utiliza IA para tomar decisiones que afectan a las condiciones laborales, como ascensos o evaluaciones de rendimiento.

La regla general es que los interesados, y por lo tanto los empleados, tienen derecho a solicitar que una persona, y no solo una máquina, participe en las decisiones que tengan consecuencias legales o que les afecten significativamente. En el RGPD, esto se denomina el derecho a no estar sujeto a una toma de decisiones automatizada.

Base legal para el procesamiento

Si desea utilizar sistemas de IA que procesen datos personales de empleados, el RGPD exige que se garantice una base legal para el tratamiento de estos datos.

Para obtener esta base legal, puede resultar tentador solicitar el consentimiento de los empleados, pero a menudo no es una solución adecuada ni legal. Dada la dinámica de poder entre el empleador y el empleado, este puede sentirse presionado a dar su consentimiento. Para que el consentimiento sea válido, debe otorgarse libremente: sin ningún elemento de coacción, presión o imposibilidad de negarse.

Es recomendable considerar bases legales alternativas para el tratamiento. Si el sistema de IA es necesario para las operaciones comerciales, el tratamiento a menudo puede basarse en intereses legítimos o en la necesidad de ejecutar un contrato laboral, en lugar del consentimiento. La base legal adecuada dependerá de la aplicación específica de la IA y de la finalidad del tratamiento.

Ley de Inteligencia Artificial: Requisitos y Restricciones en el Lugar de Trabajo

La Ley de IA de la UE afecta la implementación de las herramientas de IA en el entorno laboral. La ley clasifica aplicaciones específicas, como las utilizadas en la contratación, la supervisión de empleados y la toma de decisiones en el entorno laboral, como de alto riesgo. En el caso de estas aplicaciones, no solo se ven afectados los desarrolladores o quienes comercializan el sistema en Europa, sino que los implementadores también deben cumplir con los requisitos de cumplimiento. **Las siguientes aplicaciones de IA se clasifican como de alto riesgo en la Ley de IA:**

Sistemas de IA para el reclutamiento y la clasificación/selección de CV. Esto incluye sistemas que publican y segmentan anuncios de empleo, filtran y clasifican solicitudes o evalúan a candidatos.

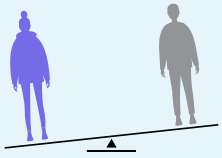
- En segundo lugar, se aplica a los sistemas de IA que influyen en las condiciones laborales. Esto incluye los sistemas que toman decisiones sobre las condiciones laborales, los ascensos o los despidos. También abarca los sistemas que asignan tareas laborales en función del comportamiento o las características de los empleados, así como los sistemas que supervisan y evalúan su rendimiento y conducta en el lugar de trabajo.

Como empleador que utiliza un sistema de IA de alto riesgo, debe cumplir con varios requisitos como implementar medidas técnicas y organizacionales para garantizar que el sistema se utilice conforme al propósito previsto. Tiene la obligación de supervisar el rendimiento, la supervisión humana, garantizar la transparencia y realizar una evaluación de riesgos. En particular, debe asegurarse de que el sistema no discrimine.

Por ejemplo, si utiliza IA para filtrar currículums, el sistema debe ser capaz de explicar la justificación de su evaluación de las solicitudes. También debe ser consciente y mitigar eficazmente el riesgo de que los sistemas de IA puedan amplificar los sesgos existentes en el proceso de selección.

Herramienta de reclutamiento con IA de Amazon

La herramienta de reclutamiento con IA de Amazon fue descontinuada en 2018 debido a que discriminaba a las mujeres en el proceso de selección de currículums. El sistema de IA se había entrenado con solicitudes de empleo de un período de diez años, la mayoría de las cuales provenían de hombres. Como resultado, el sistema aprendió a priorizar las solicitudes que contenían la palabra "mujeres" o provenían de universidades predominantemente femeninas. Incluso después de intentar corregir estos sesgos, Amazon consideró la herramienta poco confiable y finalmente suspendió su uso, alegando la preocupación de que el sistema no pudiera ajustarse adecuadamente para garantizar resultados justos e imparciales en el proceso de reclutamiento.



La Ley de IA también prohíbe ciertos tipos de sistemas de IA en el lugar de trabajo, ya que se consideran un riesgo inaceptable. Se prohíbe el uso de sistemas de IA que intenten interpretar emociones mediante el análisis de datos biométricos. Un ejemplo de ello son los sistemas de IA diseñados para evaluar si un solicitante de empleo dice la verdad en una entrevista mediante el análisis de las expresiones faciales o la voz. La UE ha determinado que estos sistemas suponen un riesgo tan significativo para los derechos humanos fundamentales que no pueden permitirse en absoluto.

Guía de IA en el lugar de trabajo

A medida que la IA se convierte en una parte importante de la fuerza laboral, es cada vez más importante implementar lineamientos claros sobre cómo utilizar estas herramientas. Una guíade IA ofrecen varias ventajas como:

Para los empleados, proporciona respuestas claras sobre cómo utilizar las herramientas de IA de forma correcta y responsable. Esto facilita la comprensión de su uso y se evitan malentendidos e incertidumbre entre los empleados.

Para los empleadores, una guía es esencial para establecer límites claros. Al explicar qué está permitido y qué no al usar IA, se reduce el riesgo de incumplimiento involuntario, ya sea en relación con los derechos de los empleados o con los requisitos regulatorios. Unos límites claros también constituyen la mejor base para abordar el uso indebido repetido de las herramientas.

Lo más importante es que una guía bien diseñada puede ayudar a generar confianza entre empleadores y empleados al demostrar un enfoque proactivo hacia el uso ético de la IA. Crear una guía completa también demuestra que se toma en serio la implementación de la IA.

Metáfora del semáforo

La metáfora del semáforo puede ser una forma práctica y sencilla de estructurar la guía de IA:

Rojo – Prohibido su uso. No está permitido bajo ninguna circunstancia. Ejemplo: IA de reconocimiento de emociones en entrevistas (prohibida por la Ley de IA).

Amarillo – Uso que requiere evaluación adicional. Consulte con el personal de protección de datos o de TI antes de continuar. Ejemplo: IA para la clasificación de currículums (requiere evaluación de impacto de protección de datos (EIPD), transparencia y supervisión humana).

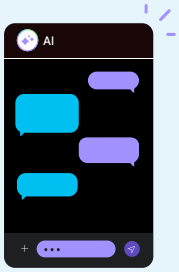
Verde – Uso autorizado y legal de herramientas de IA. Se trata de un uso seguro que cumple con los lineamientos de la empresa. Ejemplo: IA para traducción automática de uso interno, sin procesamiento de datos personales.

Caso: La supervisión en el lugar de trabajo bajo una nueva perspectiva

A medida que el lugar de trabajo se vuelve más digital, los empleadores adquieren más capacidades técnicas para supervisar las actividades de los empleados. La supervisión del lugar de trabajo está, de una forma u otra, sujeta a regulaciones en toda Europa, ya sea a través del RGPD o de la legislación nacional. Mientras que algunos países imponen fuertes restricciones a la supervisión de los empleados, otros la permiten bajo ciertas condiciones, como cuando es necesaria por motivos de seguridad o cumplimiento normativo.

AI implementar herramientas de IA en el lugar de trabajo, es necesario tener en cuenta qué se considera supervisión y en qué condiciones está legalmente permitida. Tomemos como ejemplo los asistentes de IA (copilotos). Estas herramientas tienen acceso a correos electrónicos, archivos y carpetas compartidas, y pueden realizar análisis que antes eran difíciles o imposibles de llevar a cabo para las personas. Técnicamente, un gerente podría revisar todo lo que ha escrito un empleado y evaluar su rendimiento basándose en ello. Sin la IA, esto rara vez sería un medio práctico de supervisión, ni siquiera sería posible hacerlo manualmente, ya que requeriría demasiados recursos.

Con los asistentes de IA, los empleadores ahora pueden analizar fácilmente grandes cantidades de contenido para evaluar a los empleados. Los sistemas de IA pueden revisar archivos y documentos, correos electrónicos, el uso de emojis de reacción, declaraciones realizadas en reuniones y mucho más. Pero recuerde: el hecho de que la tecnología lo haga posible no significa que sea legal. Dicho monitoreo requiere un propósito legítimo que cumpla con los requisitos de la legislación sobre protección de datos y el derecho laboral.



Derechos de Propiedad Intelectual

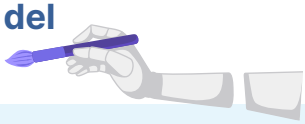
La propiedad intelectual otorga el uso exclusivo de inventos técnicos, marcas registradas y obras creativas. La IA presenta nuevos desafíos para estos derechos, en particular en lo que respecta al uso de datos de entrada, de salida y datos de entrenamiento. Si bien existen soluciones prácticas, es fundamental comprender cómo la IA impacta los derechos de propiedad intelectual, tanto propios como ajenos.

El término "propiedad intelectual" abarca ampliamente diversos derechos que las personas o empresas pueden obtener mediante la creación de obras originales. Estos derechos incluyen derechos de autor, patentes, marcas registradas, derechos de diseño y secretos comerciales. Los derechos de propiedad intelectual otorgan a su titular control exclusivo sobre activos intangibles protegidos, que abarcan desde obras literarias y artísticas hasta inventos técnicos, identidades de marca y diseños distintivos. La aparición de la IA desafía las interpretaciones establecidas del derecho de propiedad intelectual en diversas áreas.

Derechos de autor del contenido generado por IA

¿Puede el contenido creado por IA recibir protección de derechos de autor? Para que una obra esté protegida por derechos de autor, debe ser el resultado de la expresión creativa original de un autor humano. Por lo tanto, los sistemas de IA no pueden ser titulares de derechos de autor de forma independiente.

¿Quién es el dueño del arte de IA?



Un artista presentó una demanda contra la Oficina de Derechos de Autor de Estados Unidos tras la negación de los derechos de autor de la imagen Theatre D'opera Spatial, creada con la herramienta de IA Midjourney.

La imagen, ganadora de un concurso artístico, se creó probando numerosas indicaciones diferentes en la herramienta de IA y luego perfeccionándola en Photoshop. **La Oficina de Derechos de Autor rechazó la solicitud porque la imagen contenía demasiado contenido generado por IA como para ser protegida por derechos de autor.**

Pero ¿qué ocurre con el usuario del sistema de IA? La opinión predominante es que las obras creadas con la asistencia de IA pueden optar a la protección de los derechos de autor, siempre que el resultado refleje la contribución intelectual y creativa original del usuario humano. El factor decisivo es el grado de control creativo y la toma de decisiones humanas durante todo el proceso.

grado de participación humana necesario para la protección de los derechos de autor sigue siendo incierto. En Estados Unidos, se ha denegado la protección de los derechos de autor a personas por imágenes generadas por IA cuando su contribución se limitaba a proporcionar indicaciones de texto "prompts". Sin embargo, ejercer un control creativo sustancial, como dar instrucciones detalladas al sistema de IA y editar la obra resultante, puede ser suficiente para establecer la protección de los derechos de autor en la UE. El factor decisivo es si la persona demostró suficiente originalidad y control creativo sobre el producto final.

Juego limpio de Material de origen

Getty Images presentó una demanda contra la empresa de inteligencia artificial Stability AI por usar sus imágenes sin permiso para entrenar una IA capaz de generar nuevas imágenes. **Getty afirma que esto viola los derechos de autor y vulnera los derechos de los fotógrafos. Stability AI argumenta que usar las imágenes es legal, ya que se considera "uso legítimo" según la doctrina de derechos de autor.**

Riesgo de infringir los derechos de propiedad intelectual de terceros

El uso de herramientas de IA, en particular aquellas que generan texto, imágenes o código, conlleva el riesgo de infringir los derechos de propiedad intelectual de terceros.

Como empresa, es importante reconocer que el contenido generado por IA puede parecerse inadvertidamente a obras existentes protegidas por derechos de propiedad intelectual. Incluso sin intención de copiar, los sistemas de IA pueden producir contenido que infrinja dichos derechos. Si esto ocurre, los titulares de los derechos pueden solicitar una compensación o iniciar acciones legales, independientemente de si la infracción fue intencional. Las empresas que utilizan IA suelen estar sujetas a estándares más estrictos que los particulares.

Para mitigar este riesgo, las empresas de IA están implementando medidas de seguridad para evitar que los sistemas de IA generen contenido protegido por derechos de autor. La Ley de IA de la UE también exigirá que las herramientas de IA incluyan medidas técnicas adecuadas para evitar la creación de contenido que infrinja su normativa, incluidas las leyes de derechos de autor.

Datos de Entrenamiento

AI utilizar modelos de IA proporcionados por desarrolladores externos, es fundamental que las empresas comprendan los materiales empleados en el proceso de entrenamiento. **El entrenamiento de modelos de IA suele implicar el almacenamiento temporal de un gran conjuntos de datos, lo que podría constituir una infracción de derechos de autor si se realiza sin el consentimiento de los titulares de los derechos.**

Importantes empresas de IA se han enfrentado a litigios por el uso no autorizado de materiales con derechos de autor durante la fase de entrenamiento. Por ejemplo, Getty Images ha demandado a Stability AI, alegando el uso de millones de imágenes con derechos de autor sin permiso. De igual forma, varios autores han iniciado procedimientos legales contra OpenAI por usar sus libros como datos de entrenamiento para ChatGPT.

La UE ha buscado abordar este problema mediante la exención de derechos de autor para la **Minería de Texto y Datos (TDM)** en virtud de la Directiva sobre Derechos de Autor en el Mercado Único Digital (DSM). Además, la Ley de IA introduce requisitos de transparencia más estrictos respecto a los datos de entrenamiento, exigiendo a los desarrolladores de IA que documenten qué obras protegidas por derechos de autor se han utilizado.

Cambiando las leyes de datos con IA

La Directiva sobre Derechos de Autor en el Mercado Único Digital (DSM) introduce nuevas normas de derechos de autor para el mundo digital. **Un cambio significativo es que será legal analizar grandes cantidades de texto y datos (TDM) sin obtener previamente la autorización de los titulares de los derechos.**

Esto significa que, si realiza una investigación o dirige un negocio, puede analizar cualquier material al que tenga acceso legal. Esto incluye contenido disponible en línea con la aprobación del titular de los derechos y, probablemente, también contenido al que se accede a través de servicios de suscripción.

Los dueños de derechos pueden optar por que su contenido no se utilice para la minería de textos y datos, pero la directiva no especifica cómo deben hacerlo. Una solución práctica para los sitios web podría ser implementar una señal legible por máquina que indique que el contenido no puede utilizarse para dicho análisis.

Protección contra demandas al utilizar modelos de IA preentrenados

Muchos proveedores de IA renuncian a los derechos sobre los resultados generados por sus modelos. Como usuario, esto significa generalmente que puede estar seguro de que el proveedor de IA no reclamará derechos sobre el contenido que usted cree utilizando su servicio. Sin embargo, sigue siendo fundamental garantizar que los datos de entrenamiento utilizados en estos modelos no infrinjan los derechos de propiedad intelectual de terceros. Si no se obtienen las licencias adecuadas para los datos de entrenamiento, su empresa podría verse expuesta a reclamaciones legales o litigios.

Algunos de los principales proveedores de IA ofrecen medidas de protección para dar mayor seguridad a los usuarios. Entre ellas se pueden incluir:

Acuerdos de indemnización

El proveedor puede asumir la responsabilidad de los costes legales y los posibles daños y perjuicios si se determina que el sistema de IA infringe los derechos de propiedad intelectual.

Garantías sobre los datos de entrenamiento

Algunos proveedores garantizan que sus datos de entrenamiento cuentan con las licencias adecuadas, lo que le ofrece una mayor seguridad de que no se le considerará responsable en caso de infracción.

Asistencia Legal

El proveedor puede ofrecer asistencia jurídica o representación legal si surgen reclamaciones relacionadas con la infracción de la propiedad intelectual por el uso de su sistema de IA.

Estas medidas de protección pueden proporcionar cierta seguridad, pero es necesario revisar cuidadosamente los términos del servicio y las limitaciones de responsabilidad del proveedor para asegurarse de que su negocio esté adecuadamente protegido.

Términos y condiciones de la licencia

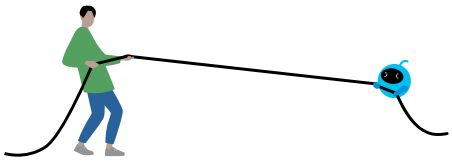
El mercado actual de la IA está dominado por unas pocas grandes corporaciones estadounidenses, lo que limita el poder de negociación al adoptar herramientas de IA. Aunque las condiciones contractuales no sean negociables, comprender los términos que se aceptan sigue siendo esencial.

Los contratos de estas empresas suelen estar basados en las tradiciones legales estadounidenses y suelen consistir en documentos extensos con un lenguaje complejo que se actualiza con frecuencia. Si bien las condiciones generales suelen ser similares entre los proveedores, identificar pequeñas pero cruciales diferencias puede ser difícil.

Si su organización planea utilizar servicios de IA, debe:

- **Revisar exhaustivamente los términos y condiciones antes de comenzar a usarlos.**
- **Supervisar continuamente las actualizaciones de estos términos.**

Dada la naturaleza no negociable de estos contratos, seleccionar al proveedor de IA adecuado es crucial. El proveedor debe impulsar la innovación y, al mismo tiempo, garantizar el cumplimiento de los requisitos de privacidad y seguridad de los datos. Un factor clave es equilibrar los costos con las medidas de seguridad del proveedor.



Servicios gratuitos de IA

Las herramientas de IA gratuitas pueden parecer rentables, pero pueden tener desventajas ocultas. Muchos proveedores monetizan estas herramientas utilizando los datos personales y las aportaciones de los usuarios, lo que puede generar anuncios dirigidos, menor seguridad de los datos y menor control sobre la información compartida. Con los modelos gratuitos, los proveedores suelen utilizar los datos de los usuarios para mejorar y perfeccionar sus sistemas de IA. Esta práctica genera inquietudes para las empresas en relación con la privacidad de los datos, las obligaciones de confidencialidad y la protección de secretos comerciales. Puede dar lugar a un posible incumplimiento del RGPD (falta de un acuerdo de tratamiento de datos, transferencia fuera de la UE) y, después a incumplimientos de las obligaciones contractuales para las empresas que procesan datos como encargados del tratamiento. **Para las organizaciones que gestionan datos personales sensibles o información confidencial, se recomienda encarecidamente invertir en una solución de IA de pago con sólidas garantías de seguridad.**

Al revisar los contratos de servicio de los principales proveedores de IA, por lo general encontrará amplias limitaciones de responsabilidad y detalladas restricciones de uso. Los proveedores reconocen explícitamente que sus sistemas de IA pueden producir errores a pesar de su tecnología avanzada. Muchos contratos prohíben expresamente el uso de sistemas de IA en sectores de alto riesgo, como los servicios jurídicos, la asesoría financiera y la atención médica. Estas restricciones sirven como escudos de responsabilidad y como reconocimiento de las limitaciones actuales de la IA. En estos sectores, donde los errores pueden tener consecuencias significativas, el comprador y el implementador de los sistemas de IA asumen una responsabilidad sustancial por los resultados.

Antes de celebrar acuerdos para servicios de IA, revise cuidadosamente los términos y las condiciones de la licencia. Los aspectos clave a tener en cuenta incluyen cómo regula el acuerdo:

Procesamiento de datos y derechos: determine quién conserva la propiedad de los datos que usted introduce y cómo puede utilizarlos el proveedor. Preste especial atención sobre la autorización del proveedor a utilizar sus datos para entrenar sus modelos de IA.

Limitaciones de responsabilidad: aclare la responsabilidad del proveedor por errores o resultados inexactos. Revise cualquier nivel de servicio garantizado relacionado con la confiabilidad y el tiempo de actividad del sistema.

Restricciones de uso: identifique cualquier limitación en cuanto al uso del modelo, incluidas las restricciones en el procesamiento de datos o las áreas de aplicación prohibidas.

Privacidad y seguridad de la información: evaluar los períodos de retención de datos, los tipos de datos almacenados, las medidas de seguridad aplicables y los fines para los que se conservan los datos.

IA personalizada: uso de API

Para muchas empresas, aprovechar eficazmente la IA implicará desarrollar modelos personalizados utilizando API (Interfaces de Programación de Aplicaciones) a partir de Modelos de Lenguaje Grandes (LLM). Este enfoque permite a las empresas adaptar las soluciones de IA a sus necesidades específicas, al tiempo que se benefician de potentes modelos preentrenados.

Este enfoque permite a las empresas adaptar las soluciones de IA a sus necesidades específicas, al tiempo que se benefician de potentes modelos preentrenados.

Las API ofrecen una gran flexibilidad a la hora de configurar un servicio, pero cuando se trata de las condiciones de uso de los principales proveedores, el margen de negociación suele ser mínimo. En la práctica, las condiciones fundamentales para los LLM son muy similares entre los distintos proveedores.

Al utilizar API, es especialmente importante tener en cuenta el derecho del proveedor a modificarla según sus condiciones y cómo esto podría afectar a la solución personalizada.

Historia del documento y agradecimientos

Fuentes y Colaboradores

Por parte de Experis, han participado en sesiones de trabajo o han aportado otras valiosas contribuciones:

- Jørgen Longva, Director de Competencias
- Ekaterina Kuzmina, Experta en Datos y Aprendizaje Automático
- Robert Grønås, Experto en Seguridad Digital
- Rune Aasgaard, Líder de Estrategia y Transformación de la Comunidad

Por parte de Vaar Law, han participado:

- Thor Beke, Socio Director
- Johanne Mustad, Abogada Asociada

Documentos y fuentes

- AT&T. Asistentes autónomos: el siguiente paso en la revolución GenAI para empoderar a los empleados y atender a los clientes. Consultado en octubre de 2024. https://about.att.com/blogs/2024/autonomous-assistants.html
- Bastigkeit Ericstam, Sonia. IA en el lugar de trabajo: Regulación de la explicabilidad y el consentimiento en la gestión algorítmica. Facultad de Derecho, Universidad de Estocolmo, Documento de investigación n.º 135, 4 de marzo de 2024.
- CNN Business. El desastre de la compra de viviendas de Zillow demuestra lo difícil que es usar la IA para valorar bienes raíces. Consultado en octubre de 2024. https://edition.cnn.com/2021/11/09/tech/zillow-ibuying-home-zestimate/index.html
- Digital Norway. Vaktplaner, ruteoptimalisering og prognoser: Derfor er data en nøkkel til Odas suksess, consultado en octubre de 2024, https://digitalnorway.com/ruteoptimalisering-vaktplaner-prognoser-derfor-er-data-en-nokkel-til-odas-suksess/

- Ley de IA de la UE. Anexo I: Lista de legislación de armonización de la Unión. Consultado en octubre de 2024. https://artificialintelligenceact.eu/annex/1/
- Ley de IA de la UE. Anexo II: Lista de delitos a que se refiere el artículo 5, apartado 1, párrafo primero, letra h), inciso iii). Consultado en octubre de 2024. https://artificialintelligenceact.eu/annex/2/
- Ley de IA de la UE. Anexo III: Sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2. Consultado en octubre de 2024. https://artificialintelligenceact.eu/annex/3/
- Catálogo de datos del Centro Común de Investigación de la UE. Casos seleccionados de IA en el sector público (JRC129301). Recuperado en octubre de 2024. https://data.jrc.ec.europa.eu/dataset/7342ea15-fd4f-4184-9603-98bd87d8239a
- Futurity.org. Las publicaciones de Facebook con estas palabras pueden predecir la depresión. Consultado en septiembre de 2024. https://www.futurity.org/depression-facebook-prediction-1893812
- Gartner. Casos prácticos de IA e IA generativa. Consultado en octubre de 2024. https://www.gartner.com/document-reader/document/5191663
- Gartner. Radar de oportunidades de IA de Gartner: Establezca la ambición de IA de su empresa. Consultado en octubre de 2024. https://www.gartner.com/document-reader/document/4836831
- INRIX. INRIX anuncia Compass, una nueva tecnología de inteligencia de movilidad impulsada por más de 20 años de datos propios y la IA generativa de Amazon Bedrock. Consultado en octubre de 2024. https://inrix.com/press-releases/bedrock-compass-gen-ai/
- Microsoft y LinkedIn, 2024. Informe Anual del Índice de Tendencias Laborales: La IA en el Trabajo ya está aquí, ahora viene la parte difícil. Microsoft WorkLab. Consultado en agosto de 2024. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part
- Reuter. Artista demanda tras el rechazo de EE. UU. a los derechos de autor de una imagen generada por IA. Consultado en octubre de 2024. https://www.reuters.com/legal/litigation/artist-sues-after-us-rejects-copyright-ai-generated-image-2024-09-26/
- Section. Informe de Competencia en IA. Section School, 2024. Consultado en septiembre de 2024. https://www.sectionschool.com
- Strümke, Inga. Maskiner som tenker. Kagge forlag, 2023.
- Instituto de Investigación Toyota. El Instituto de Investigación Toyota presenta una nueva técnica de IA generativa para el diseño de vehículos. Consultado en octubre de 2024. https://pressroom.toyota.com/toyota-research-institute-unveils-new-generative-ai-technique-for-vehicle-design/

ChatGPT, Perplexity.ai y Claude.ai tienen preguntas con el siguiente formato: "¿Puedes darme algunos ejemplos de [tema]?". Las respuestas se evaluaron en función de mi experiencia y conocimientos personales, se adaptaron a contextos específicos, se utilizaron para investigaciones posteriores y se incorporaron a la expansión de ideas originales.

Historial de revisiones

Versión	Fecha	Descripción	Personas responsables
1.0	2024-11-25	Primera edición	Director de Competencias de Experis Noruega, Jørgen Longva, y el Socio Gerente de Vaar Law, Thor Beke
1.0.1	2025-02-18	Se corrigió un error en la pirámide de riesgos de la Ley de IA	Director de Competencias de Experis Noruega, Jørgen Longva
1.0.1	2025-03-16	Traducción al inglés	Director de Competencias, Jørgen Longva y Rune Aasgaard, Líder Comunitario en Estrategia y Transformación, ambos de Experis Noruega. Johanne Mustad, Abogada socia de Vaar Advokat.
1.0.2	2025-10-21	Globalización del informe	Jefe del Departamento Jurídico de ManpowerGroup Noruega, Emil Skjærvø Sætereng

SOBRE EXPERIS

Experis es líder mundial en atracción de talento TI y soluciones tecnológicas, potenciando a las organizaciones en el proceso de adopción de tecnología, proporcionando soluciones flexibles que se adaptan a sus necesidades, a medida que seguimos evolucionando en la transformación digital. Con experiencia en Business Transformation, Cyber Security, Digital Workspaces, Cloud & Infrastructure Services, y Enterprise Applications, Experis ofrece la potente combinación de talento calificado en demanda, con soluciones tecnológicas claves para el éxito empresarial. Experis forma parte de la familia de marcas de ManpowerGroup® (NYSE: MAN), que también incluye Manpower y Talent Solutions.

Para más información, visita *https://servicios.manpowergroupcolombia.co/experis-colombia*, **o síguenos en *LinkedIn*.**

¡SÍGUENOS!

Manpower® Experis® ManpowerGroup Talent Solutions® ManpowerGroup® | ManpowerGroup®