inesem
business school

Cómo redactar una política de uso de IA para *tus empleados*

Hoy en día, la **política de uso de Inteligencia Artificial (IA)** en las empresas ha dejado de ser una "buena práctica" opcional para convertirse en un **imperativo legal y de gestión de riesgos**, impulsado principalmente por la plena aplicación del Reglamento Europeo de IA.

La tendencia ha pasado de ser el uso libre en base a la curiosidad a la **gobernanza estricta**, donde la máxima prioridad es la seguridad de los datos, la trazabilidad y la supervisión humana.

Redactar una política de Inteligencia Artificial (IA) para empleados es fundamental para equilibrar la innovación con la seguridad y la ética. En este sentido, una política efectiva debe ser clara, concisa y adaptarse a los riesgos específicos de la organización.

inesem
business school

01. Qué es una política de uso de IA y por qué es crítica en la empresa

02. Fundamentos Legales y Éticos

03. Diagnóstico interno y evaluación de riesgos

04. Estructura recomendada de la política

05. Implementación y Comunicación

06. Errores frecuentes en políticas de IA

07. Indicadores de efectividad

01 Qué es una política de uso de IA y por qué **es crítica** en la empresa

Una política de uso de IA es un documento interno que define las reglas, directrices éticas y legales para el diseño, implementación y supervisión responsable de la inteligencia artificial.

Este marco normativo interno establece las normas, límites y responsabilidades para el uso de herramientas de IA por parte de empleados, directivos, colaboradores y otros perfiles vinculados a la empresa.

Su objetivo principal es:

- ***Minimizar riesgos.***
- ***Garantizar la protección de datos.***
- ***Fomentar la transparencia.***
- ***Asegurar la supervisión humana.***
- ***Alinear el uso de IA con los objetivos del negocio.***

En un entorno donde herramientas como OpenAI con ChatGPT o Microsoft con Copilot están al alcance de cualquier empleado, la falta de normas claras expone a la organización a riesgos innecesarios.

[Consejo PRO]

No esperes a que aparezca una incidencia para regular el uso de la IA. La política debe anticiparse al riesgo, no reaccionar tarde ante él.

02 Fundamentos **Legales y Éticos**

La **redacción de una Política** de Uso de Inteligencia Artificial para las organizaciones es cada vez más necesaria.

No se trata sólo de permitir o prohibir el uso de herramientas, sino de establecer unas reglas que, desde una perspectiva ética y legal, sirvan para proteger a la empresa, a sus trabajadores y a terceros.

Para guiar la base legal de este documento, lo primero que debemos tener en cuenta es la definición de su **objeto y alcance**, es decir, indicar a quién va dirigido, y que se entiende por "uso de IA" dentro de la organización.

¿A quién afecta esta política?

Regulación nacional e internacional sobre IA

Desde el punto de vista legal, uno de los pilares fundamentales es la **protección de datos personales.**

En el contexto europeo, la política debe alinearse con el **Reglamento General de Protección de Datos (RGPD)**, que exige una base jurídica para tratar datos personales, así como medidas de seguridad adecuadas.

Además, el nuevo **AI Act** (Reglamento de Inteligencia Artificial de la Unión Europea) establece obligaciones específicas según el nivel de riesgo del sistema de IA utilizado.

Esto implica que la empresa debe evaluar qué tipo de herramientas emplea y si estas requieren controles adicionales, como supervisión humana o evaluaciones de impacto.

Norma o marco	Qué exige a la empresa
RGPD	Protección de datos personales, base jurídica y medidas de seguridad
AI Act	Evaluación del riesgo de los sistemas de IA y controles específicos
LOPDGDD	Garantía de derechos digitales, privacidad e intimidad laboral
Ley de propiedad intelectual	Control sobre obras, contenidos y derechos de terceros

Atendiendo a la protección de datos personales, cualquier tratamiento de datos mediante herramientas de IA debe respetar los principios del RGPD:

- ***Licitud.***
- ***Lealtad.***
- ***Transparencia.***
- ***Minimización de datos.***
- ***Limitación de finalidad.***
- ***Seguridad.***

La política interna de la organización debe establecer que está **prohibido introducir datos personales sensibles** (salud, ideología, afiliación sindical, orientación sexual, datos biométricos) en herramientas de IA no autorizadas.

También deber establecer que sólo podrán utilizarse **datos previamente anonimizados o seudonimizados** cuando sea posible.

EVITA ESTO

No permitas que los empleados introduzcan información confidencial o datos personales en herramientas públicas de IA sin autorización previa.

Una sola acción de este tipo puede generar un riesgo legal y reputacional importante.

Control de herramientas externas de IA

Toda herramienta externa de IA debe ser evaluada por el Delegado de Protección de Datos, el departamento jurídico o el área responsable de compliance.

En tratamientos de alto riesgo, deberá realizarse una Evaluación de Impacto en Protección de Datos.

Además, el uso de plataformas de IA puede implicar transferencias internacionales de datos fuera del Espacio Económico Europeo.

En estos casos, la política debe exigir:

- Verificación de garantías adecuadas (cláusulas contractuales tipo o decisiones de adecuación).
- Uso exclusivo de cuentas corporativas.
- Firma de contratos de encargado de tratamiento cuando proceda.
- Control interno sobre almacenamiento y conservación de resultados generados.

Propiedad intelectual y resultados generados por IA

En España, la protección de obras intelectuales se rige por el **Real Decreto Legislativo 1/1996, Texto Refundido de la Ley de Propiedad Intelectual.**

La política de la empresa debe aclarar que la titularidad de los contenidos generados por empleados mediante IA, en el ejercicio de sus funciones, corresponde a la empresa conforme a la normativa laboral y contractual aplicable.

Además, el empleado debe revisar que el contenido generado no infrinja derechos de terceros.

No podrán reproducirse obras protegidas, marcas registradas ni software sin licencia.

También es recomendable establecer:

- Revisión humana antes de publicar o comercializar contenido generado por IA.
- Registro interno del uso de IA en procesos creativos o técnicos.
- Criterios claros sobre reutilización, edición y validación de contenidos.

Principios éticos de uso responsable.

Los principios éticos que este documento debería reflejar van alineados con el marco europeo de la IA confiable.

Principio

Aplicación práctica

Transparencia

Informar cuando el uso de IA sea relevante

Responsabilidad

Definir quién supervisa y valida los resultados

Igualdad y no discriminación

Evitar sesgos algorítmicos

Proporcionalidad

Usar IA solo cuando sea adecuada al fin perseguido

Supervisión humana

No delegar decisiones sensibles exclusivamente en IA

Formación

Capacitar a los empleados en el uso seguro de estas herramientas

03 Diagnóstico interno y evaluación **de riesgos**

Antes de implementar o escalar soluciones basadas en IA, la empresa debe identificar brechas, amenazas y oportunidades.

Este diagnóstico permite conocer qué herramientas se utilizan, con qué finalidad, bajo qué condiciones contractuales y con qué nivel de riesgo.

Identificación de herramientas de IA utilizadas en la empresa

La identificación de herramientas de IA es un paso crítico dentro del diagnóstico interno.

Este análisis debe incluir tanto las herramientas oficialmente autorizadas como aquellas utilizadas de manera informal por los empleados.

El resultado debe ser un inventario de herramientas IA que puedan usarse oficialmente en la empresa.

Este inventario servirá como base para:

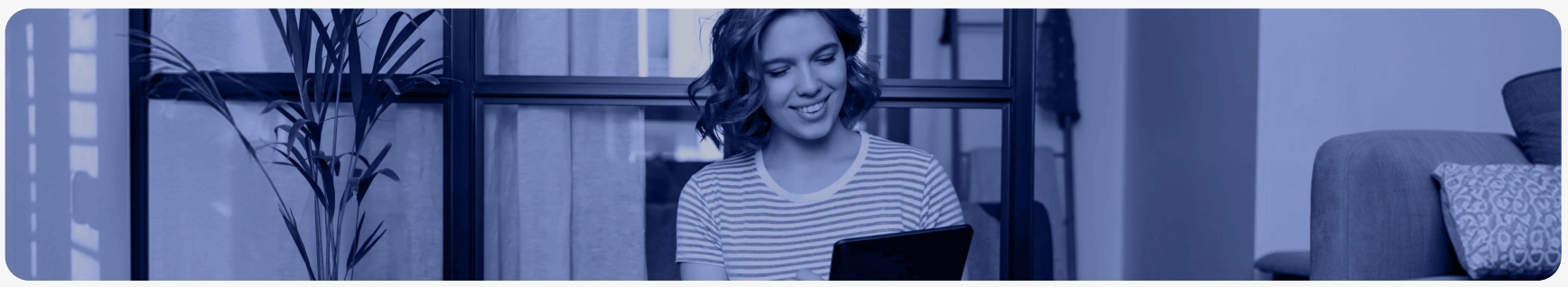
- ***Evaluar riesgos.***
- ***Definir controles.***
- ***Realizar auditorías internas.***
- ***Establecer responsabilidades.***
- ***Actualizar la política cuando sea necesario.***

CONSEJO

Empieza con una pregunta sencilla a cada departamento:

"¿Qué herramientas de IA utilizáis actualmente y para qué tareas?"

La respuesta puede revelar más riesgos de los que imaginas.



También es importante identificar las áreas de impacto y las funciones críticas.

Nos referimos a aquellos procesos donde la IA puede generar efectos significativos en resultados operativos, derechos de las personas, cumplimiento normativo o reputación corporativa.

Areas de impacto Organizacional	**IMPACTO**	**FUNCIONES CRÍTICAS**	**RIESGOS**
Dirección y Gobierno Corporativo.	Estratégico y reputacional		Decisiones basadas en información incorrecta.
Recursos Humanos.	Derechos laborales y no discriminación.	Selección de personal, evaluaciones disciplinarias y promociones internas.	Sesgos algorítmicos, discriminación indirecta y falta de transparencia.
Finanzas y Control.	Económico y regulatorio.	Aprobación de pagos, evaluación de riesgos financieros y cumplimiento fiscal.	Errores en cálculos. Incumplimiento normativo. Manipulación de modelos predictivos.
Área Comercial y Marketing.	Clientes y reputación.	Atención a la cliente automatizada. Ofertas personalizadas. Gestión de datos de clientes.	Uso indebido de datos personales. Publicidad engañosa generada por IA. Pérdida de confianza del cliente.
Operaciones y Producto.	Continuidad del negocio.	-Gestión de cadena de suministro. -Seguridad operativa. -Planificación de producción.	Fallos técnicos. Dependencia excesiva del sistema. Interrupciones operativas.
Tecnología y Seguridad.	Seguridad de la información.	Seguridad de la información.	Protección de datos. Gestión de accesos. Supervisión de infraestructuras IA.
Legal y Compliance.	Responsabilidad jurídica.	Interpretación normativa. Gestión de litigios. Protección de datos personales.	Protección de datos. Interpretaciones incorrectas. Incumplimiento regulatorio. Sanciones económicas.

Igualmente, en cualquier organización hay que tener presentes ciertas funciones que deben considerarse críticas y que son trasversales a cualquier área de la empresa.

En este sentido encontramos la toma de decisiones que afectan derechos individuales, el procesamiento de datos personales o sensibles, los procesos financieros de alto impacto económico, los sistemas que afectan seguridad física o salud, los procesos estratégicos o confidenciales o la interacción directa automatizada con clientes o usuarios.

Necesidades de formación y concienciación

Dentro de la empresa el **nivel de formación de los trabajadores** debe de ir acorde con el **nivel de riesgo** y el **rol** que tenga el trabajador.

Así, podemos considerar la formación que a nivel general debe recibir cualquier trabajador, y, por otra parte, la formación específica que deberán recibir los trabajadores que se encuentren en áreas que llamaremos críticas.

A. *Formación general*

Debe incluir contenidos mínimos sobre:

- Conceptos básicos de IA.
- Limitaciones de estas herramientas.
- Riesgos asociados.
- Prohibición de introducir datos confidenciales en herramientas no autorizadas.
- Normativa aplicable en protección de datos y propiedad intelectual.
- Responsabilidad individual en el uso de IA.

B. *Formación específica por áreas críticas*

La formación específica debe adaptarse a cada departamento.

Por ejemplo, en puestos de alta dirección deberá centrarse en riesgos estratégicos y reputacionales.

En Recursos Humanos, deberá abordar sesgos, no discriminación y toma de decisiones automatizadas.

En Legal y Compliance, deberá centrarse en obligaciones normativas, responsabilidad y trazabilidad.

Las medidas deben combinar controles organizativos, técnicos y jurídicos.

Controles organizativos:

- Política formal de uso de IA aprobada por dirección.
- Inventario actualizado de herramientas. Comité de IA o ética digital.
- Procedimiento de aprobación previa de nuevas herramientas.
- Supervisión humana en decisiones críticas.

Controles técnicos

- Restricción de acceso a herramientas no autorizadas.
- Sistemas DLP (Data Loss Prevention).
- Registro de actividad y logs.
- Control de APIs.
- Monitorización de uso.
- Evaluaciones periódicas de modelos.

Controles jurídicos y contractuales

- Revisión contractual con proveedores.
- Acuerdos de tratamiento de datos.
- Evaluaciones de impacto cuando proceda.
- Cláusulas de responsabilidad y confidencialidad.

04 Estructura **recomendada** de la política

Una Política de Uso de IA eficaz no debe limitarse a enumerar prohibiciones.

Debe convertirse en una guía práctica que ayude a los empleados a utilizar estas herramientas de forma segura, responsable y alineada con los objetivos de la organización.

A continuación, se muestra una estructura recomendada para elaborar este documento.

Introducción y objetivos

Aquí debemos contextualizar la necesidad de la política dentro del proceso de transformación digital de la organización.

Este apartado debe incluir:

- Reconocimiento del uso creciente de herramientas de IA.
- Identificación de riesgos legales, éticos y operativos.
- Compromiso con el cumplimiento normativo.
- Objetivos perseguidos por la organización.

El fundamento jurídico del objetivo debe ir en línea con el principio de responsabilidad proactiva previsto en el art. 5.2 del Reglamento General de Protección de Datos.

¿Qué pretende conseguir una Política de Uso de IA?

- Proteger datos e información sensible
- Garantizar el cumplimiento normativo
- Definir responsabilidades claras
- Impulsar la innovación segura
- Mejorar la productividad

La IA debe generar valor sin generar riesgos innecesarios

Ámbito de aplicación

El **ámbito de aplicación** de un documento interno de la empresa se refiere a quienes son las personas que se van a ver obligadas a cumplirlo en la empresa.

En este caso el ámbito de aplicación debe incluir a:

- Directivos.
- Empleados.
- Colaboradores externos.
- Proveedores (cuando proceda).
- Becarios o personas en prácticas formativas.

El ámbito de aplicación puede tener relevancia disciplinaria ya que se integra en el marco contractual.

Reglas de uso aceptable e inaceptable

El siguiente punto que debemos atender en la redacción es las **reglas de uso y principios generales de uso de la IA**.

Como principios fundamentales debemos respetar los siguientes:

- ***Legalidad – Cumplimiento de la normativa aplicable.***
- ***Transparencia – No ocultar el uso de IA cuando sea relevante.***
- ***Supervisión humana – No delegar completamente decisiones sensibles.***
- ***Proporcionalidad – Uso adecuado al fin perseguido.***
- ***No discriminación – Evitar sesgos algorítmicos.***

Desde el punto de vista jurídico, estos principios se conectan con el principio de licitud (art. 6 RGPD) y la prohibición de decisiones automatizadas sin garantías (art. 22 RGPD).

✅ Usos permitidos

Redacción preliminar de documentos.

Automatización de tareas administrativas.

Generación de ideas o borradores.

Análisis de información no sensible.

Apoyo a tareas de investigación.

❌ Usos prohibidos

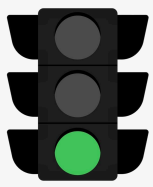
Introducir datos personales sin autorización.

Compartir información confidencial en herramientas públicas.

Delegar decisiones disciplinarias exclusivamente en IA.

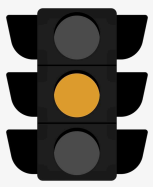
Generar contenido engañoso o discriminatorio.

Utilizar herramientas no autorizadas por la organización.



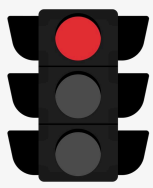
Zona *verde*

Herramientas autorizadas + supervisión humana



Zona *amarilla*

Contenido generado pendiente de revisión



Zona *amarilla*

Datos confidenciales + herramientas públicas

Protocolos de seguridad y privacidad

El protocolo de seguridad y privacidad no es un anexo secundario, sino el núcleo operativo de la Política de Uso de IA.

Es el conjunto de medidas organizativas y técnicas que garantizan que el uso de sistemas de IA respete la normativa de protección de datos, la confidencialidad empresarial y los derechos fundamentales.

No se trata solo de una declaración de principios, sino de un sistema operativo de cumplimiento alineado con el principio de responsabilidad proactiva del Reglamento General de Protección de Datos y con el enfoque basado en riesgo del AI Act.

La estructura para seguir es la siguiente:

1. Evaluación previa de riesgos.

- Análisis de riesgos.
- Evaluación del Impacto en Protección de Datos.

2. Clasificación de la información.

Aquí debemos clasificar la información atendiendo a si es pública, interna, confidenial, si son datos personales o son datos personales sensibles.

3. Control de herramientas autorizadas.

Como ya hemos comentado, no todas las herramientas de IA pueden utilizarse libremente en el entorno de la empresa. El protocolo debe incluir aquellas que aprueba su uso y aquellas que prohíbe su uso.

Además, debe establecer la prohibición del uso de cuentas personales para fines corporativos.

Pueden añadirse otros aspectos referentes a la ubicación de servidore, transferencias internacionales de datos, medidas de cifrado o cláusulas contractuales tipo.

4. Principios de tratamiento de datos.

Deben respetarse principios como la minimización (uso de los datos estrictamente necesarios), la seudonimización y anonimización (eliminar indicadores directos, cuando se pueda), La limitación de la finalidad y la transparencia.

5. Seguridad técnica.

En base al art. 32 RGPD, Deben introducirse medidas concretas sobre seguridad técnica, como son:

- Cifrado en tránsito y en reposo.
- Autenticación multifactor.
- Control de accesos por rol.
- Registro de actividad (logs).
- Sistemas de detección de incidentes.

6. Supervisión humana obligatoria.

En este sentido se debe establecer que ninguna decisión con efectos jurídicos significativos será adoptada exclusivamente por IA y que todo resultado generado será validado por un responsable humano. Esto conecta directamente con el articulo 22 RGPD y con las exigencias de control humano que marca el AI Act.

7. Gestión de incidentes y brechas de seguridad.

Este apartado es fundamental en cuando a responsabilidad civil y sancionadora. Aquí el protocolo debe ser claro y conciso:

- Detección del incidente.
- Notificación inmediata al responsable interno o DPO.
- Evaluación del impacto.
- Notificación a la autoridad de control en 72 horas si procede.
- Comunicación a los afectados cuando exista alto riesgo.

8. Formación y concienciación.

La formación de todas las personas a las que afecta este protocolo es fundamental para su correcta implantación y funcionamiento. La falta de formación puede considerarse incumplimiento del deber de diligencia organizativa.

Podemos incluir en este apartado todo lo referente a formación sobre uso responsable de la IA en la empresa. Desde manuales prácticos de buenas prácticas, pasando por cursos de formación obligatoria, simulacros de incidentes o canales de consultas internas.

9. Protocolo de conservación y eliminación de datos.

En este apartado debe regularse:

- Plazos máximos de conservación.
- Eliminación automática cuando ya no sean necesarios.
- Derecho de supresión y rectificación.

10. Auditoria y revisión periódica.

El protocolo debe someterse a auditorías internas, revisión anual y actualización conforme a cambios normativos o tecnológicos.

El AI Act introduce obligaciones adicionales para sistemas clasificados como de alto riesgo, incluyendo documentación técnica y trazabilidad.

Procedimiento ante incidencias o mal uso

Este apartado es fundamental para una buena implantación de la política de uso de IA. El procedimiento debe contemplar:

- *El canal interno de reporte.*
- *Evaluación del incidente.*
- *Medidas correctivas.*
- *Posibles sanciones disciplinarias.*

Capacitación y actualización continua

En cualquier acción enfocada a la mejora de aspectos trasversales en una empresa, como es el que aquí nos ocupa, ésta debe garantizar la formación periódica a sus empleados en materia de protección de datos conforme al Reglamento General de Protección de Datos, la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales y las exigencias del Reglamento de Inteligencia Artificial de la Unión Europea.

Esta formación debe incluir aspectos tan importantes como los riesgos legales y éticos del uso de IA, identificación de sesgos, validación de resultados generados, protección de información confidencial y buenas prácticas en la redacción de instrucciones, etc. Asimismo, la organización debe actualizar sus programas formativos de manera continua para adaptarse a cambios tecnológicos y regulatorios, fomentando una cultura de responsabilidad, supervisión humana y uso seguro de estas herramientas.

¿Está preparada tu organización?

- ☐ Existe una política formal de IA.
- ☐ Disponemos de inventario de herramientas autorizadas.
- ☐ Los empleados reciben formación específica.
- ☐ Existen controles de seguridad definidos.
- ☐ Se supervisan los resultados generados.
- ☐ Hay procedimientos para gestionar incidentes.
- ☐ Se realizan revisiones periódicas.
- ☐ La dirección respalda la iniciativa.

05 Implementación y **Comunicación**

La eficacia del documento que creemos no va a depender solo de la calidad normativa, sino que es muy importante la manera de implementar, comunicar y supervisar el proceso dentro de la empresa.

Por ello, la fase de implementación debe concebirse como un proceso estructurado, transversal y continuo.

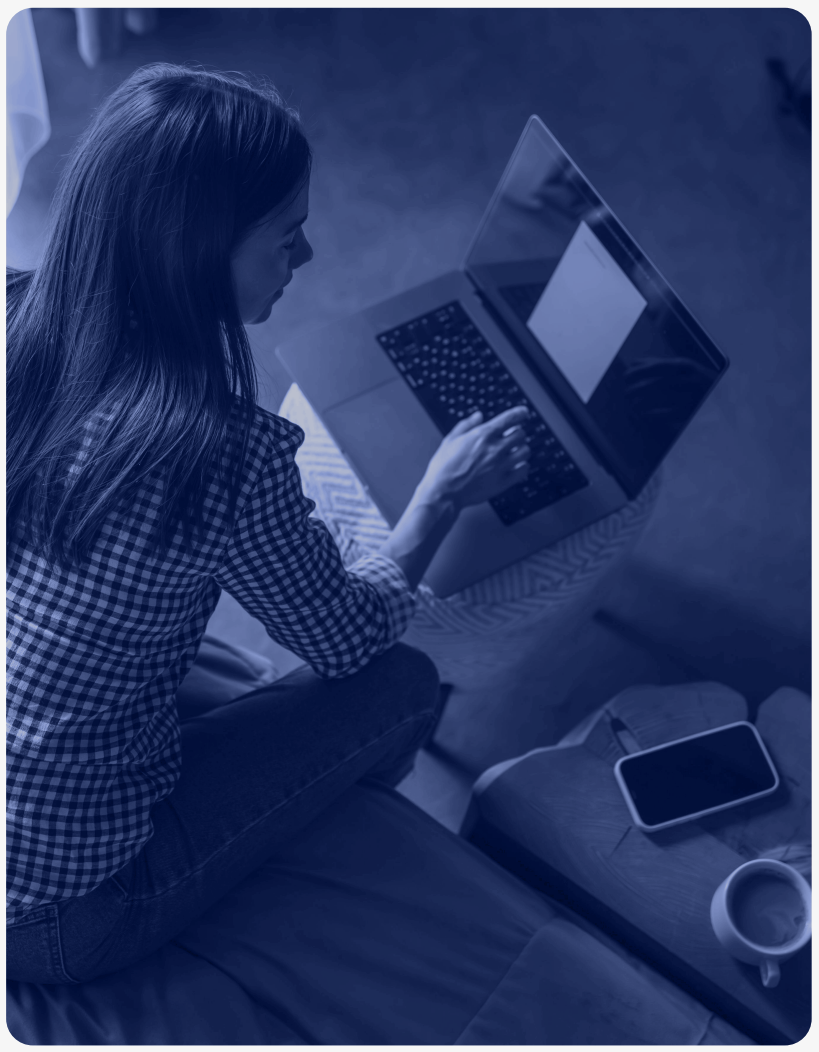
Difusión interna de la política

La difusión interna debe garantizar que todos los empleados comprendan la existencia, alcance y obligatoriedad de la política. Esto implica utilizar diferentes canales de comunicación corporativa.

Por ejemplo, intranet, correo institucional, reuniones departamentales y sesiones informativas dirigidas por liderazgo.

El respaldo de esta política por parte de la dirección es muy importante, ya que así refuerza su importancia estratégica.

Asimismo, debe asegurarse que el documento sea accesible, comprensible y adaptado a los distintos niveles organizativos, evitando tecnicismos excesivos cuando no sean necesarios.



Capacitación y talleres prácticos

No basta con entregar un PDF. Los empleados necesitan ejemplos reales.

Las sesiones formativas deben incluir:

- Casos prácticos.
- Simulaciones.
- Ejemplos de uso correcto.
- Errores frecuentes.
- Buenas prácticas.

Confirmación de lectura y aceptación por empleados

Es importante tener confirmación de forma formal de que los empleados han leído y aceptado la política. Para ello, podemos hacer uso de la firma electrónica, la aceptación digital en plataformas internas de la empresa o incluso introducir o integrarlo en el proceso de onboarding.

Desde una perspectiva de cumplimiento normativo y gestión de riesgos, la confirmación ayuda al fortalecimiento de la seguridad jurídica de la empresa.

Integración con manuales de empresa y códigos de conducta

La integración es fundamental. La Política de Uso de IA no debe operar de manera aislada. Para ellos se hace uso de otros documentos como:

- El código de ética corporativo.
- Las políticas de protección de datos.
- Los protocolos de ciberseguridad.
- Los reglamentos internos de trabajo.

Esta integración asegura coherencia normativa y evita contradicciones.

Seguimiento y auditorías internas

Los mecanismos de control son también una herramienta y una parte de la implementación.

Mediante
las auditorías internas evaluaremos qué herramientas de IA están siendo utilizadas, si se respetan las directrices de confidencialidad, el nivel de supervisión humana aplicado y la trazabilidad de decisiones automatizadas, entre otras.

El seguimiento periódico permite identificar desviaciones y adoptar medidas correctivas oportunas.

06 Errores frecuentes en **políticas de IA**

Los errores más frecuentes en la elaboración de una política pueden debilitar su eficacia. Por ello debemos controlarlos.

Los 5 errores que hacen fracasar una política de IA

Redacción ambigua o genérica.

No considerar la legislación vigente.

Falta de actualización ante nuevas herramientas.

Ausencia de responsabilidades claras.

No incluir formación o seguimiento.

07 Indicadores de **efectividad**

La evaluación de una Política de Uso de IA requiere **indicadores medibles que permitan valorar su impacto organizacional.**

Los indicadores que vamos a tener presentes son:

- Cumplimiento de la política por parte de los empleados.
- Reducción de incidencias o riesgos legales.
- Nivel de concienciación interna sobre IA.
- Integración de buenas prácticas en procesos internos.
- Revisión periódica y mejoras implementadas.

De la teoría a la acción

La inteligencia artificial ya forma parte del entorno laboral.

La diferencia entre una organización preparada y otra expuesta al riesgo no está en utilizar más o menos IA.

Está en contar con las normas adecuadas para utilizarla de forma responsable, segura y alineada con los objetivos del negocio.

Una Política de Uso de IA bien diseñada permite proteger a la organización, potenciar a los empleados y convertir la innovación en una ventaja competitiva sostenible.

inesem

business school