USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL

JULIO DE 2025 // CONDIS SUPERMERCATS, S.A.

ÍNDICE

1. OBJETIVO, ALCANCE, APROBACIÓN, SUPERVISIÓN Y CUMPLIMIENTO DEL CÓDIGO DE IA

La irrupción de la Inteligencia Artificial (en adelante, "IA") es una realidad, ofreciendo grandes oportunidades para hacer nuestro trabajo más eficiente, encontrar información valiosa e impulsar la innovación en Condis.

En este sentido, y con el fin de aprovechar plenamente los beneficios de esta tecnología, es preciso abordar los diferentes principios o requisitos a tener en cuenta para el desarrollo y uso de sistemas de IA, con el con el fin de garantizar el cumplimiento de los derechos fundamentales.

Sin embargo, la IA también puede ser complicada y puede traer riesgos si no se usa correctamente. Un mal uso puede llevar a problemas como la pérdida de datos personales, filtraciones de información o el incumplimiento de leyes, lo que puede afectar los derechos de las personas. Por eso, es muy importante usar la IA de manera responsable para evitar estos problemas y aprovechar al máximo sus beneficios.

A estos efectos, se aprobó en diciembre de 2023 el Reglamento Europeo por el que se establecen normas armonizadas en materia de IA (en adelante, el "RIA") que regula los diferentes usos de la IA para limitar los riesgos que se deriven y establecer una serie de requisitos y obligaciones en relación a los usos específicos de la IA. De la misma manera, en el ámbito español se está trabajando en un anteproyecto de ley para garantizar un uso ético, inclusivo y beneficioso de la IA.

1.1 ¿Cuál es el objetivo de este documento?

Este Código de buenas prácticas para el uso responsable de la Inteligencia Artificial (en adelante, "Código de IA") tiene, como objetivo, promover una IA fiable dentro de Condis.

La fiabilidad de la inteligencia artificial (IA) se apoya en tres componentes:

- La IA debe ser lícita, es decir, debe cumplir con todas las normativas aplicables.
- La IA debe ser ética, es decir, debe garantizar el respeto a los principios y valores éticos (ver apartado 2.2 para más información).
- La IA debe ser robusta, es decir, debe proteger la seguridad de los datos e información que gestionamos, desde un punto de vista de seguridad técnica.

Siguiendo las pautas y mejores prácticas de este Código garantizaremos, como personas empleadas de Condis, un uso responsable de la IA que esté alineada con los valores de la Compañía y la normativa. De esta forma, podremos aprovechar al máximo el valor de la IA, protegiendo los datos, fomentando la transparencia y manteniendo la confianza y la seguridad en nuestras operaciones.

1.2 ¿A quién resulta aplicable?

Este Código de IA va dirigido a todas las personas empleadas de Condis que desarrollen o utilicen sistemas de IA en sus funciones profesionales dentro de la Compañía.

1.3 ¿Quién es el responsable de su supervisión?

Corresponde al Área de Ética y Compliance la revisión de este Código de IA, así como la supervisión de su cumplimiento.

Para cualquier duda respecto a la interpretación y aplicación del Código de IA y las implicaciones legales que pueda tener el uso de esta tecnología, puedes contactar con el Área de Ética y Compliance a través del correo electrónico compliance@condis.es.

1.4 ¿Quién es el responsable de su aprobación y modificación?

El Consejo de Administración aprobará el Código de IA y sus modificaciones a propuesta del Área de Ética y Compliance cuando considere que concurren circunstancias que lo hagan conveniente o necesario.

El presente Código ha sido aprobado por el Consejo de Administración en julio de 2025.

1.5 ¿Qué hacer en caso de incumplimiento?

Si tienes conocimiento de algún incumplimiento de este Código, deberás informar de ello al Compliance Officer de Condis a través del Buzón Ético y de Cumplimiento.

Indicar que, cuando una persona empleada de Condis haya realizado actividades que contravengan lo establecido en este Código y la Compañía tenga conocimiento de ello, Condis procederá a aplicar las medidas disciplinarias que corresponda conforme al Estatuto de los Trabajadores, el régimen de faltas y sanciones previsto en el convenio colectivo que resulte de aplicación o en la legislación laboral aplicable.

2. DEFINICIÓN, PRINCIPIOS, RIESGOS Y USOS DE LOS SISTEMAS DE IA

2.1 ¿Qué es un sistema de IA?

Un sistema de IA es una herramienta tecnológica que puede trabajar de forma autónoma y adaptarse después de ser utilizada. Estos sistemas obtienen información de entrada (input) y la usan para generar resultados (output) como predicciones, contenidos, recomendaciones o decisiones. Estos resultados pueden afectar tanto a entornos físicos como virtuales.

Debido a los rápidos avances en la tecnología de IA, no se puede hacer una lista completa de todos los tipos de sistemas de IA. Por eso, cada sistema debe ser evaluado según sus características específicas.

2.2 ¿Cuáles son los principios éticos que deben cumplir los Sistemas de IA?

Existen 4 principios éticos que se deben cumplir para garantizar que los sistemas de IA se desarrollen, desplieguen y utilicen de manera fiable. Éstos son los siguientes:

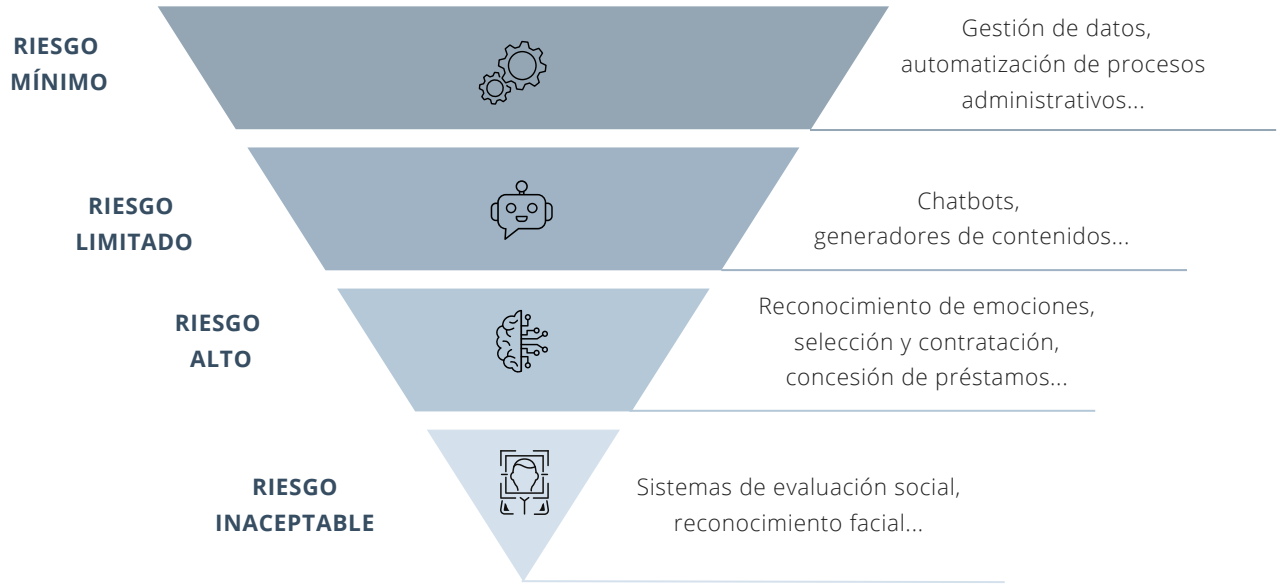
1. RESPETO A LA AUTONOMÍA HUMANA	Los sistemas de IA no deberían subordinar, coaccionar, engañar, manipular, condicionar o dirigir a las personas de manera injustificada. En consecuencia, estos sistemas deberían seguir principios de diseño centrados en las personas, y dejar amplias oportunidades para la elección humana.
2. PREVENCIÓN DEL DAÑO	Los sistemas de IA no deberían provocar daños ni perjudicar de cualquier otro modo a las personas.
3. EQUIDAD	La equidad implica garantizar un acceso justo y no discriminatorio a las capacidades y beneficios de la IA por parte de diferentes grupos y asegurar que los resultados y aplicaciones de la IA no generen impactos desproporcionados o perjudiciales para grupos vulnerables.
4. EXPLICABILIDAD	La explicabilidad implica poder explicar, en la medida de lo posible, los resultados o decisiones generadas por un sistema de IA a las partes que se vean afectadas de manera directa o indirecta por dichos resultados o decisiones.

Estos principios deben traducirse en requisitos concretos para hacer realidad una IA fiable. Éstos requisitos son los siguientes:

1. ACCIÓN Y SUPERVISIÓN HUMANAS	Los sistemas de IA deben permitir que las personas tomen decisiones con conocimiento de causa y favorecer sus derechos fundamentales. Para ello, es necesaria la intervención de seres humanos durante el ciclo de diseño del sistema de inteligencia artificial y en el monitoreo de su funcionamiento.
2. SOLIDEZ TÉCNICA Y SEGURIDAD	Los sistemas de IA deben ser seguros y estar protegidos frente a posibles vulnerabilidades, garantizar un plan de retroceso en caso de que algo salga mal, así como ser exactos, fiables y reproducibles.
3. GESTIÓN DE LA PRIVACIDAD Y DE LOS DATOS	Los sistemas de IA deben garantizar la protección de la intimidad y de los datos a lo largo de todo el ciclo de vida del sistema. Esto incluye la información inicialmente facilitada por el usuario, así como la información generada sobre el usuario en el contexto de su interacción con el sistema. Además, se debe asegurar que los datos no contengan sesgos sociales, imprecisiones u errores y garantizar la integridad de los datos, ya que la introducción de datos malintencionados en un sistema de IA puede alterar su comportamiento.
4. TRANSPARENCIA	Las decisiones que adopte un sistema de IA deben poder explicarse de manera adaptada a las partes interesadas afectadas. Asimismo, los sistemas IA no deberían presentarse a así mismos como humanos ante los usuarios. Las personas tienen derecho a saber que están interactuando con un sistema de IA. Por lo tanto, los sistemas de IA deben ser identificables como tales. Además, cuando sea necesario, se debería ofrecer al usuario la posibilidad de decidir si prefiere interactuar con un sistema de IA o con una persona, con el fin de garantizar el cumplimiento de los derechos fundamentales.
5. DIVERSIDAD, NO DISCRIMINACIÓN Y EQUIDAD	Los sistemas de IA deben ser accesibles para todas las personas, independientemente de su edad, género, capacidades o características. Deben evitarse los sesgos injustos, ya que podría dar lugar a prejuicios y discriminación (in)directos e involuntarios contra determinados grupos o personas, lo que podría agravar los estereotipos y la marginación.
6. BIENESTAR SOCIAL Y AMBIENTAL	Los sistemas de IA deben beneficiar a todos los seres humanos, incluidas las generaciones futuras. Por lo tanto, debe garantizarse que sean sostenibles y respetuosos con el medio ambiente. Además, deben tener en cuenta a la sociedad en su conjunto, al resto de seres sensibles y al medio ambiente como partes interesadas a lo largo de todo el ciclo de vida, y debe estudiarse detenidamente su impacto social.
7. RENDICIÓN DE CUENTAS	Deben implantarse mecanismos que garanticen la responsabilidad y la rendición de cuentas de los sistemas de IA y de sus resultados. La auditabilidad, que permite la evaluación de algoritmos, datos y procesos de diseño, desempeña un papel clave, especialmente en aplicaciones críticas. Además, debe garantizarse una reparación accesible.

2.3 ¿Cómo se clasifican los sistemas de IA en términos de nivel de riesgo?

El RIA aborda los riesgos asociados a usos específicos de la IA, los clasifica en cuatro niveles de riesgo y establece normas diferentes para cada nivel.



RIESGO MÍNIMO	La mayoría de los sistemas de IA utilizados en tareas rutinarias como la gestión de datos o la automatización de procesos administrativos entran en esta categoría. Estos sistemas no están sujetos a regulaciones específicas más allá de las normativas generales de seguridad y privacidad de datos.
RIESGO LIMITADO	Los sistemas de IA que comportan un riesgo limitado, como los chatbots o los sistemas de IA generadores de contenido, también deben cumplir con las normativas generales de seguridad y privacidad de datos. Pero, adicionalmente, también están sujetos a obligaciones de transparencia, como la de informar a los usuarios de que su contenido se ha generado mediante IA para que puedan tomar decisiones con conocimiento de causa sobre su uso posterior.
RIESGO ALTO	Son sistemas de IA de alto riesgo, entre otros, los sistemas de IA destinados a ser utilizados... • Para reconocimiento de las emociones. • Como componentes de seguridad en infraestructuras críticas. • Para la contratación, selección de personas o para la toma de decisiones en el ámbito laboral. • Para evaluar la solvencia de las personas o establecer su calificación crediticia Los sistemas de IA de alto riesgo deberán cumplir con los requisitos dispuestos en el RIA para que puedan implementarse en la Compañía.
RIESGO INACEPTABLE	Está prohibido en la UE el uso de sistemas de IA que supongan una amenaza para la seguridad, los derechos o los medios de subsistencia de las personas. En el apartado 2.4 se explican en más detalle cuales son las prácticas de IA que quedan prohibidas, según lo dispuesto en el RIA.

2.4 ¿Cuáles son los usos permitidos y prohibidos de los sistemas de IA?

Prácticas Prohibidas: Las siguientes prácticas de IA quedan prohibidas, según lo dispuesto en el Art. 5 del RIA:

TÉCNICAS SUBLIMINALES	No se permite el uso de IA que manipule o influya en las personas sin que se den cuenta, para que tomen decisiones que no tomarían normalmente.
EXPLOTACIÓN DE VULNERABILIDADES	No se puede usar IA que aproveche las debilidades de personas (por ejemplo, por su edad o situación económica) para cambiar su comportamiento de manera que les perjudique.
EVALUACIÓN INJUSTA DE PERSONAS	No se puede usar IA para clasificar a personas basándose en su comportamiento social o características personales de forma que les trate injustamente.
EVALUACIONES DE RIESGO BASADAS EN PERFILES	No se puede usar IA para predecir si alguien cometerá un delito solo por su perfil o características personales, a menos que se base en hechos verificables.
RECONOCIMIENTO FACIAL SIN CONSENTIMIENTO	No se puede usar IA para crear bases de datos de reconocimiento facial extrayendo imágenes de internet o cámaras sin permiso.
INFERIR EMOCIONES EN EL TRABAJO O ESCUELA	No se puede usar IA para adivinar las emociones de las personas en estos lugares, a menos que sea por razones médicas o de seguridad.
CLASIFICACIÓN BIOMÉTRICA INJUSTA	No se puede usar IA para clasificar a las personas según su raza, creencias, orientación sexual, etc., a partir de sus datos biométricos.
IDENTIFICACIÓN BIOMÉTRICA A TIEMPO REAL	No se puede usar IA para identificar personas en público, a menos que sea para: • Buscar víctimas de delitos graves. • Prevenir amenazas inminentes a la vida. • Identificar sospechosos de delitos graves.

Resto de Prácticas: El resto de las prácticas requerirán de la revisión y aprobación del:

- Área de Ética y Compliance respecto de la ética del sistema de IA e involucración de información de carácter personal o información confidencial.
- Área de Sistemas respecto de la robustez del sistema de IA desde el punto de vista técnico.

Indicar que, la IA está surgiendo en un entorno altamente regulado, con regulaciones específicas que afectan a diversos sectores como la salud, el trabajo o la propiedad intelectual. Además, las regulaciones específicas de IA (por ejemplo, el RIA) imponen requisitos adicionales para garantizar que su desarrollo y uso sean tanto éticos como seguros.

Para garantizar un uso responsable de la IA en Condis y cumplir con la normativa aplicable, ambas áreas implementaran sistemas de gestión de riesgos efectivos para identificar y mitigar cualquier riesgo asociado a la IA de manera eficiente.

Prácticas de alto riesgo: En el caso de querer implantar sistemas de IA de alto riesgo se deberá, a efectos del RIA:

a) Cumplir con una serie de **obligaciones**. En concreto, se deberá:

- Adoptar medidas técnicas y organizativas adecuadas para garantizar que se utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen.
- Encomendar la supervisión humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias.
- Asegurar de que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema de IA de alto riesgo.
- Vigilar el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso. Cuando se tengan motivos para considerar que utilizar el sistema de IA de alto riesgo conforme a sus instrucciones puede dar lugar a que ese sistema de IA presente algún riesgo que afecte a la salud, la seguridad o los derechos fundamentales de las personas, se suspenderá su uso y se deberá informar, de ello y sin demora indebida, al proveedor o distribuidor y a la autoridad competente.
- Conservar los archivos de registro que los sistemas de IA de alto riesgo generen automáticamente, durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que se disponga otra cosa en la normativa aplicable en materia de protección de datos personales.
- Informar, antes de implantar un sistema de IA de alto riesgo en el lugar de trabajo, a los representantes de las personas trabajadoras de Condis y a las personas afectadas de que estarán expuestos a la utilización del sistema de IA de alto riesgo.
- Llevar a cabo una evaluación de impacto relativa a la protección de datos cuando proceda.
- Informar a las personas físicas de que están expuestas a la utilización de los sistemas de IA de alto riesgo en el caso que dichos sistemas tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas.

b) Adicionalmente, y antes de desplegar uno de los sistemas de IA de alto riesgo, se deberá llevar a cabo una **evaluación del impacto** que la utilización de dichos sistemas puede tener **en los derechos fundamentales**, debiéndose comunicar los resultados de dicha evaluación a la autoridad competente. Esta evaluación consistirá en:

- Una descripción de los procesos en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista.
- Una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo.
- Las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico.
- Los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos identificadas en el punto anterior, teniendo en cuenta la información facilitada por el proveedor.
- Una descripción de la aplicación de medidas de supervisión humana, de acuerdo con las instrucciones de uso.
- Las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.

3. IMPLEMENTACIÓN DE UN SISTEMA DE IA EN CONDIS

3.1 ¿Cuáles son las fases a seguir para la implementación de un sistema de IA en Condis?

Si, como persona empleada de Condis, deseas usar o proponer una nueva herramienta de IA, debes seguir estos pasos:

1 *Identificación de la necesidad o problema*

Piensa en áreas de tu trabajo donde la IA podría ayudar a mejorar procesos, resolver problemas o hacer las tareas más eficientes y define una propuesta.

2 *Selección de tecnologías*

- Identifica qué tecnologías existen en el mercado que puedan dar cobertura a la necesidad o problema previamente identificado. Ten en cuenta que hay prácticas que están prohibidas y que, por tanto, no se pueden implementar (ver apartado 2.4 para más información).
- Solicita información detallada, incluido presupuesto y demostraciones, de aquellas tecnologías que sean de tu interés.
- Haz una valoración de dichas tecnologías y realiza una elección preliminar.

3 *Presentación de la propuesta*

Deberás documentar y presentar la propuesta al:

- Área de Ética y Compliance para que pueda revisar y evaluar la ética del sistema de IA y el nivel de cumplimiento de la normativa de protección de datos en el caso que haya datos de carácter personal involucrados.
- Área de Sistemas para que pueda revisar y evaluar el nivel de robustez del sistema de IA desde el punto de vista técnico.

Ejemplo 1:

Una persona empleada de Condis se entera, por un amigo, de que otra empresa está utilizando una nueva solución de IA como herramienta de apoyo para preparar presentaciones de PowerPoint. Siguiendo el Código de IA de Condis, el empleado se pone en contacto con las áreas de Ética y Compliance y Sistemas para preguntar si esta solución de IA es segura o si se puede adquirir una licencia profesional.

4 *Revisión y evaluación de la propuesta*

Las áreas de Ética y Compliance y de Sistemas compartirán los resultados de las evaluaciones y determinaran, de forma conjunta, si se aprueba el sistema de IA presentado en la propuesta.

Aunque el sistema de IA se acabe aprobando, de las revisiones y evaluaciones realizadas se pueden derivar directrices, recomendaciones, acciones a realizar, etc.

Ejemplo 2:

Siguiendo el ejemplo 1 anterior, una vez se ha puesto en contacto con las áreas de Ética y Compliance y Sistemas para proponer una herramienta de IA, éstas hacen un análisis detallado sobre sus funcionalidades.

Una vez revisada, dichas áreas afirman que la solución de IA se puede utilizar siempre que sea con fines de soporte, como mejorar la redacción o los diseños, pero no se pueden incluir datos confidenciales o sensibles (por ejemplo, no se puede compartir la lista completa de nombres y cargos de los empleados para crear gráficos).

Ejemplo 3:

Una persona empleada de Condis quiere implantar un sistema de IA para personalizar las experiencias de los clientes en la plataforma de comercio electrónico de la empresa, Condisline, adaptando las sugerencias en función de las compras anteriores de los clientes.

Para cumplir con los principios de protección de datos, la persona empleada de Condis contacta con el Área de Ética y Compliance para que: (i) realice, en el caso de ser necesario, una evaluación de impacto para determinar el nivel de riesgo de este tratamiento de datos; (ii) garantizar que se procesen los datos personales esenciales y relevantes para mejorar la experiencia de compra, como el historial de navegación y las preferencias de compra; (iii) se actualice el registro de actividades de tratamiento para reflejar esta nueva actividad de tratamiento de datos; (iii) se modifique la política de privacidad del cliente para informar de forma transparente a los usuarios sobre cómo el sistema de IA utiliza sus datos; y (iv) se implementen mecanismos que permitan a los usuarios dar su consentimiento u oponerse a este tratamiento de datos.

Se ha elaborado el diagrama que se muestra a continuación para ilustrar un ejemplo de una herramienta que está regulada por Condis y otra que no.

*Herramienta de IA **Regulada** por Condis*	*Herramienta de IA **No Regulada** por Condis*
COPILOT Software de IA para el cual Condis dispone de una licencia específica, que, al estar en un entorno cerrado, protege los datos. En el caso que desde Condis se ofrezca una herramienta de IA adicional, se comunicará debidamente para que las personas empleadas de la Compañía puedan utilizarla.	**CHAT GPT** Software de IA de código abierto. Estas soluciones no protegen los datos y, por tanto, los pueden utilizar para entrenar los modelos de gran tamaño (LLM). En este sentido, solo se puede utilizar para búsquedas generales o para artículos de interés y **no se pueden introducir datos personales ni información que pueda ser objeto de secreto profesional.**

Asegúrate siempre de validar y comprobar los resultados de estas herramientas

5 *Registro en el inventario de sistemas de IA*

Para garantizar que el desarrollo, despliegue y uso de los sistemas de IA cumpla con los requisitos para una IA fiable, según lo previsto en la normativa, es necesario disponer de un inventario actualizado de todas las herramientas de IA que se encuentren en uso o se estén desarrollando, ya sea internamente o con el apoyo de un externo, y que contengan complementos de IA o consistan en sí mismas en un sistema IA. El Área de Ética y Compliance será la responsable de elaborar y mantener actualizado este inventario.

6 *Formación y capacitación*

Antes de implementar un sistema de IA, y una vez aprobado por las áreas de Ética y Compliance y de Sistemas, es imprescindible realizar una formación para garantizar que haya un nivel suficiente de conocimiento acerca de dicho sistema IA en la Compañía, siguiendo la obligación establecida en el Art. 4 RIA. Las personas empleadas de Condis que vayan a utilizar este sistema de IA deben realizar formación sobre el funcionamiento del mismo, así como sobre la privacidad de los datos y la ética en el uso de la IA. Las áreas de Ética y Compliance y de Sistemas se coordinaran con el Área de Desarrollo y Formación para la realización de esta formación.

Ejemplo 4:

Condis está implementando Copilot en la Compañía para mejorar la eficiencia y apoyar a las personas empleadas de oficinas en sus tareas diarias. Antes de utilizar Copilot, las personas que vayan a utilizarlo deben realizar una formación obligatoria que cubra el funcionamiento del sistema, la privacidad de los datos y la ética en el uso de la IA. Esta formación es esencial para asegurar que dichas personas comprendan cómo utilizar Copilot de manera responsable y efectiva.

Antes de usar cualquier sistema de IA, ten en cuenta los posibles riesgos y tus obligaciones como empleado. Completa todas las formaciones para adquirir los conocimientos necesarios para usar la IA correctamente. Esto es especialmente importante para las personas que implementan y supervisan el uso de la IA.

Si tienes alguna duda sobre el uso de los sistemas de IA, contacta con el Área de Ética y Compliance.

Asimismo, comparte información y recursos sobre el uso responsable de la IA con tus compañeros/as.

7 *Funcionamiento, normas de uso y revisión del sistema de IA*

- Tómate tu tiempo para aprender el funcionamiento del sistema de IA que vas a utilizar y conoce sus limitaciones. Esto te ayudará a no depender demasiado de sus resultados.
- Ten cuidado con los datos que usas en el sistema de IA. Si no estás en un entorno seguro, los datos pueden ser revelados a otros usuarios, incluidos terceros, lo que puede causar una Violación de Datos Personales o pérdida de información confidencial.
- Usa solo contenido para el que tengas los permisos necesarios, ya que pueden estar involucrados derechos de autor y propiedad intelectual.
- La IA es útil para tareas concretas, mejorar trabajos hechos por personas, preparar tareas, y encontrar patrones o cambios. No debe reemplazar ni influir en las decisiones de las personas. Asimismo, es importante tener en cuenta que la IA es una herramienta auxiliar para las personas empleadas de Condis, sin que en ningún caso se pretenda que reemplace sus decisiones.
- Asegúrate de revisar las decisiones que toma la IA, especialmente aquellas que puedan afectar los derechos, la salud o la seguridad de las personas, o tener un gran impacto en la sociedad y la economía.

Ejemplo 5:

Condis está implementando Copilot para mejorar la gestión de determinadas tareas. Uno de los usos de Copilot puede ser, por ejemplo, el análisis de las ventas y previsión de la demanda de los productos. Sin embargo, es crucial que las personas empleadas de Condis revisen estos análisis y tomen las decisiones finales, asegurándose de que se consideren todos los factores relevantes. Esto asegura que las decisiones importantes las tomen las personas, y que la IA solo sirva de ayuda, no de sustituto.

8 *Transparencia y explicabilidad*

- Asegúrate de que los resultados generados por IA estén claramente marcados como tales.
- Inserta avisos claros que informen a las personas de que están interactuando con un sistema de IA, desde el primer momento.
- Proporciona una explicación clara a las personas de cómo la IA toma las decisiones y las consecuencias que puede tener para ellas. Explícales también que tienen el derecho de pedir la intervención de una persona, expresar su opinión y cuestionar la decisión de la IA en el caso que les pueda afectar significativamente.

Ejemplo 6:

El equipo de marketing planea lanzar una nueva campaña de marketing para promocionar un nuevo producto de Condis. Deciden utilizar una herramienta impulsada por IA para generar imágenes que resalten el aspecto de los productos. En las publicaciones, el equipo de marketing debe incluir un aviso escrito para informar que las imágenes se han creado con la ayuda de la tecnología de IA.

Además, tal y como se explica en el apartado 7 anterior ('Funcionamiento, normas de uso y revisión del sistema de IA'), es fundamental comprobar las fuentes utilizadas para generar los contenidos y si Condis cuenta con todos los permisos de licencia de propiedad intelectual.

Recuerda que, al desplegar cualquier nueva iniciativa de IA, se debe involucrar a a las áreas de Ética y Compliance y de Sistemas para que puedan verificar las posibles exenciones de responsabilidad o cláusulas informativas a incluir, realizar las evaluaciones de riesgos de protección de datos y revisar las cláusulas de IA de los proveedores, entre otros aspectos relevantes.

9 *Justicia, igualdad y no discriminación*

Asegúrate de que los datos estén actualizados y sean representativos para evitar sesgos.

Ejemplo 7:

El Área de RRHH busca agilizar su proceso de contratación empleando un sistema de IA para la selección preliminar de currículums. Dicho sistema está diseñado para analizar los currículums y preseleccionar a los candidatos en función de las cualificaciones, la experiencia y las habilidades relevantes para el trabajo.

Dado que Condis se compromete a garantizar que el sistema de IA no discrimine por motivos de raza, sexo, edad o cualquier otra característica personal, el Área de RRHH deberá solicitar al proveedor información detallada sobre cómo el sistema de IA evita prácticas discriminatorias y verificar los criterios y la lógica utilizados para evitar posibles sesgos.

El Área de RRHH debe evitar el uso de filtros generales (p.ej. quién es "el mejor" candidato) y, en su lugar, filtrar los currículums según parámetros concretos (p.ej. nivel de inglés, años de experiencia, especialización, etc.). Además, el Área de RRHH deberá verificar los resultados con regularidad para evitar decisiones discriminatorias.

10 *Reporte de incidencias*

Cuando veas que un sistema de IA no funciona correctamente o hay un incidente de seguridad, comunícalo inmediatamente a Helpdesk o SCC, según corresponda.

11 *Comunicación*

Se difundirá a través de los canales habituales - intranet, correo electrónico, revista, etc.- las diferentes iniciativas formativas y las campañas de concienciación que organice Condis, así como las comunicaciones periódicas que se realicen con el objetivo de reforzar el compromiso de mantener informados a las personas empleadas de Condis sobre los avances que se produzcan en este tipo de tecnologías y las actualizaciones del presente Código de IA.

Te en cuenta que el uso que, como persona empleada de Condis, puedas realizar de los sistemas IA debe estar consensuado con tu superior.

4. ASPECTOS CLAVE A TENER EN CUENTA

4.1 ¿Qué aspectos clave debes tener en cuenta como usuario de un sistema de IA en Condis?

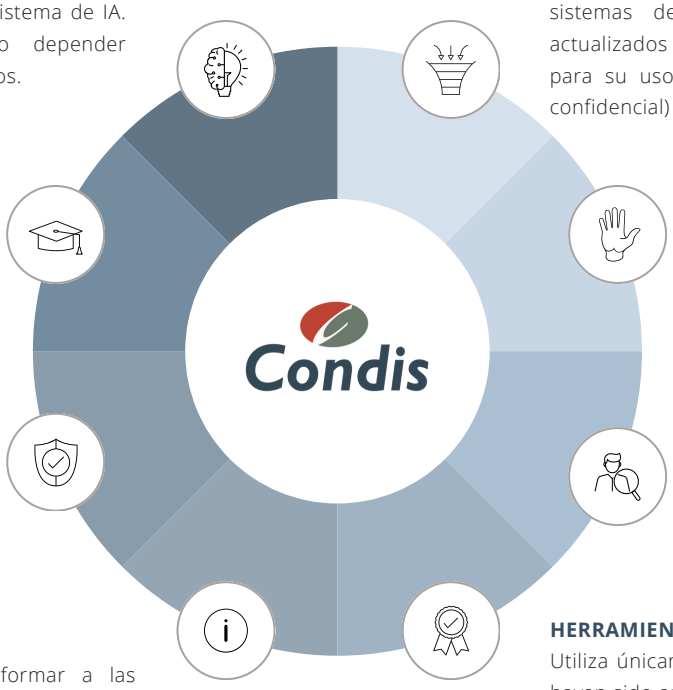
Como persona empleada de Condis y con el objetivo de que la IA dentro de la Compañía sea fiable, debes proceder de la siguiente forma:

RESPONSABILIDAD
Ten en cuenta los potenciales riesgos y limitaciones al utilizar un sistema de IA. .Esto te ayudará a no depender demasiado de sus resultados.

CALIDAD DE LOS DATOS DE ENTRADA
Asegúrate de que los datos que introduces en los sistemas de IA sean representativos, estén actualizados y tengas los permisos necesarios para su uso (evita usar contenido protegido o confidencial)

FORMACIONES
Sé consciente de tus obligaciones al utilizar un sistema de IA, completando las formaciones obligatorias.

REPORTE DE INCIDENCIAS
Cuando veas que un sistema de IA no funciona correctamente o hay un incidente de seguridad, comunícalo inmediatamente a Helpdesk o SCC, según corresponda.



PROTECCIÓN DE DATOS
Cumple con los principios y obligaciones de protección de datos al procesar datos personales dentro de los sistemas de IA. Para ello, antes de utilizar / contratar un nuevo sistema de IA, contacta con el Área de Ética y Compliance.

SUPERVISIÓN HUMANA
Verifica siempre los resultados generados por los sistemas de IA para minimizar su impacto y las consecuencias y daños imprevistos.

TRANSPARENCIA
Inserta avisos escritos para informar a las personas cuando interactúen con un sistema de IA, cuando se hayan generado contenidos artificialmente o cuando se hayan procesado sus datos personales. Si tienes cualquier duda al respecto, contacta con el Área de Ética y Compliance.

HERRAMIENTAS AUTORIZADAS
Utiliza únicamente los sistemas de IA que hayan sido aprobados previamente por las áreas de Ética y Compliance y de Sistemas. Si quieres utilizar o contratar un nuevo sistema de IA, contacta con el Área de Ética y Compliance.