**CÓDIGO ÉTICO Y POLÍTICA DE USO DE INTELIGENCIA ARTIFICIAL**

**INDETGROUP**

## 1. Objeto y alcance

Este documento establece las normas de uso ético, legal y operativo de herramientas de Inteligencia Artificial (IA) en INDETGROUP, incluyendo modelos generativos como ChatGPT, asistentes de IA, herramientas de generación de texto, imagen, código o análisis de datos.

Aplica a todo el personal, colaboradores externos y proveedores que utilicen IA en nombre de la empresa o dentro de sus sistemas.

Incluye el uso de herramientas como:

- Modelos de lenguaje (ej. ChatGPT, Claude, Gemini u otros)
- Generadores de imágenes o diseño
- Herramientas de análisis automatizado
- Asistentes de programación o automatización
- Cualquier IA integrada en software corporativo

Referencia corporativa: INDETGROUP

## 2. Marco normativo aplicable

El uso de IA en INDETGROUP debe cumplir la normativa vigente y futura aplicable, incluyendo especialmente:

### 2.1 Normativa europea

- **Reglamento General de Protección de Datos (GDPR / RGPD)**(UE 2016/679) Protección de datos personales, limitación de tratamiento y transferencias internacionales.
- **EU AI Act(Reglamento Europeo de Inteligencia Artificial)** Establece obligaciones según nivel de riesgo de los sistemas de IA (prohibido, alto riesgo, limitado y mínimo riesgo). Incluye exigencias de transparencia, supervisión humana y gestión de riesgos.

### 2.2 Normativa española

- **LOPDGDD (Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales)**
- Legislación sobre secreto empresarial y propiedad intelectual (Código Penal y Ley 1/2019 de Secretos Empresariales)
- Normativa laboral aplicable al uso de herramientas digitales en el entorno de trabajo

### 2.3 Estándares y buenas prácticas internacionales (recomendados)

- ISO/IEC 27001 (Seguridad de la Información)
- ISO/IEC 42001 (Sistema de gestión de IA)
- Principios OCDE sobre IA confiable

## 3. Principios rectores del uso de IA

El uso de IA en INDETGROUP se regirá por:

- **Supervisión humana obligatoria**
- **Minimización de datos**
- **Confidencialidad y secreto empresarial**
- **Transparencia en el uso de IA cuando sea relevante**
- **Prohibición de decisiones automatizadas sin revisión humana**
- **Responsabilidad final siempre humana**

### 3.1 Inventario de Sistemas de Inteligencia Artificial

INDETGROUPmantendrá un inventario actualizado de todas las herramientas y sistemas de Inteligencia Artificial autorizados para uso corporativo.

Como mínimo, el inventario deberá incluir:

- Nombre de la herramienta o sistema.
- Fabricante o proveedor.
- Área o departamento usuario.
- Finalidad de tratamiento.
- Datos tratados.
- Nivel de riesgo asignado.
- Responsable interno.
- Fecha de autorización.
- Integraciones con sistemas corporativos.
- Ubicación geográfica de los datos.

Ninguna herramienta de IA podrá utilizarse en el entorno corporativo sin haber sido previamente evaluada y autorizada por la empresa.

### 3.2 Clasificación de Riesgo de los Sistemas de IA

INDETGROUP clasificará los sistemas de Inteligencia Artificial utilizados conforme a la normativa europea aplicable.

Las categorías serán:

**Sistemas de riesgo inaceptable**

No podrán utilizarse en ningún caso sistemas que:

- Vulneren derechos fundamentales.
- Realicen puntuación social.
- Manipulen comportamientos de personas mediante técnicas subliminales.
- Exploten vulnerabilidades de menores o colectivos vulnerables.
- Estén prohibidos por la legislación vigente.

**Sistemas de alto riesgo**

Requerirán evaluación previa, autorización expresa y supervisión reforzada.

**Sistemas de riesgo limitado**

Podrán utilizarse siempre que exista supervisión humana y transparencia adecuada.

**Sistemas de riesgo mínimo**

Podrán utilizarse libremente dentro de las condiciones establecidas en esta política.

### 4. Clasificación de usuarios

#### 4.1 Usuarios Business (licencia corporativa o autorizada)

Usuarios con acceso a herramientas IA aprobadas por INDETGROUP.

**Condiciones:**

- Pueden usar IA para tareas operativas y de soporte profesional.
- Pueden trabajar con información interna **solo si no es sensible o confidencial crítica**.
- Deben usar cuentas corporativas aprobadas.
- Están sujetos a auditoría y trazabilidad.

**Ventajas:**

- Acceso a herramientas corporativas seguras.
- Mayor flexibilidad en uso profesional.
- Integración con sistemas internos autorizados.

### 4.2 Usuarios Free (herramientas gratuitas o personales)

Usuarios que utilizan versiones gratuitas o cuentas personales de herramientas de IA.

**Condiciones más restrictivas:**

- PROHIBIDO introducir cualquier información relacionada con INDETGROUP.
- PROHIBIDO usar datos de clientes, proyectos o procesos internos.
- Solo permitido uso genérico, educativo o de redacción no corporativa.
- No pueden generar contenido final para uso externo de la empresa sin revisión total.

## 5. Clasificación de información y documentos

### 5.1 Información PROHIBIDA en cualquier herramienta de IA

No se puede introducir bajo ninguna circunstancia:

- Datos personales de clientes, empleados o proveedores
- Información financiera interna (márgenes, facturación, presupuestos)
- Estrategias comerciales, pricingo negociaciones
- Contratos no públicos
- Información legal o fiscal interna
- Accesos, contraseñas o datos de seguridad
- Información técnica propietaria no publicada
- Datos de proyectos en curso con clientes

### 5.2 Documentos permitidos con IA (con supervisión)

Se permite el uso de IA para generar o asistir en:

**Comunicación y redacción:**

- Correos electrónicos no sensibles
- Comunicaciones internas generales
- Borradores de presentaciones comerciales no confidenciales
- Textos de marketing genéricos
- Descripciones de productos o servicios ya públicos

**Documentación operativa:**

- Procedimientos internos generales (SOPsno sensibles)
- Manuales de uso genéricos
- Resúmenes de reuniones sin datos confidenciales
- Traducciones de contenido no crítico

**Creatividad y soporte:**

- Brainstormingde ideas
- Propuestas de mejora de procesos
- Variantes de textos publicitarios
- Estructuras de informes

**Tecnología:**

- Ayuda en programación sin exponer código propietario sensible
- Explicaciones técnicas generales
- Ejemplos de código no productivo

**5.3 Documentos restringidos (requieren autorización previa)**

Uso de IA solo con aprobación expresa de responsable:

- Propuestas comerciales a clientes estratégicos
- Documentación contractual en fase de borrador
- Informes financieros internos
- Análisis de negocio con impacto estratégico
- Documentos legales o regulatorios
- Contenido destinado a publicación oficial externa

**5.4 Documentos prohibidos como salida directa de IA**

La IA no puede ser la fuente final sin revisión humana de:

- Contratos legales
- Documentación oficial de empresa
- Comunicados institucionales externos
- Decisiones laborales o disciplinarias
- Informes financieros auditables
- Documentos regulatorios o de cumplimiento

## 6. Uso ético y riesgos prohibidos

Está estrictamente prohibido usar IA para:

- Suplantación de identidad
- Generación de información falsa o engañosa
- Manipulación de clientes o terceros
- Automatización de decisiones críticas sin control humano
- Infracción de propiedad intelectual
- Reentrenamiento o extracción indebida de datos sensibles

### 6.1 Prohibiciones específicas de Inteligencia Artificial

Además de las prohibiciones anteriores, queda expresamente prohibido utilizar sistemas de IA para:

- Realizar discriminación directa o indirecta de personas.
- Crear perfiles automatizados que produzcan efectos jurídicos sin intervención humana.
- Elaborar decisiones laborales automáticas sobre contratación, despido, promoción o sanción.
- Realizar vigilancia masiva de empleados.
- Tratar categorías especiales de datos sin autorización legal.
- Generar información falsa con apariencia de autenticidad.
- Desarrollar contenidos destinados a engañar deliberadamente a terceros.

## 7. Seguridad y tratamiento de datos

- Se debe evitar cualquier introducción de datos personales innecesarios
- No se deben subir archivos internos a herramientas no autorizadas
- Deben usarse únicamente herramientas aprobadas por IT/Compliance
- Cualquier incidente debe notificarse inmediatamente

### 7.1 Tratamiento de Datos Personales mediante IA

Cuando una herramienta de Inteligencia Artificial implique el tratamiento de datos personales, deberá respetar en todo momento los principios establecidos en el Reglamento General de Protección de Datos (RGPD):

- Licitud.
- Lealtad.
- Transparencia.
- Limitación de la finalidad.

- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.
- Responsabilidad proactiva.

Todo tratamiento deberá contar con una base jurídica válida conforme al artículo 6 del RGPD y ser compatible con la finalidad original para la que los datos fueron obtenidos. Antes de iniciar el tratamiento, el área responsable deberá identificar y documentar la base jurídica aplicable.

### 7.2 Categorías Especiales de Datos

Queda prohibida la introducción en herramientas de Inteligencia Artificial de categorías especiales de datos personales, salvo que concurra una excepción válida del artículo 9 del RGPD, exista una base jurídica adecuada y se haya obtenido la autorización expresa de la Dirección y la validación previa del responsable correspondiente.

Se consideran categorías especiales de datos:

- Datos de salud.
- Datos biométricos.
- Datos genéticos.
- Datos relativos al origen racial o étnico.
- Opiniones políticas.
- Convicciones religiosas o filosóficas.
- Afiliación sindical.
- Datos relativos a la orientación sexual.
- Datos relativos a la vida sexual.

La misma restricción se aplicará a información relativa a condenas e infracciones penales.

### 7.3 Transferencias Internacionales de Datos

Antes de utilizar cualquier herramienta de IA, deberá verificarse la ubicación de los sistemas que procesan la información.

Si los datos pudieran ser tratados fuera del Espacio Económico Europeo, la empresa comprobará previamente:

- La existencia de una decisión de adecuación.
- Cláusulas Contractuales Tipo u otras garantías adecuadas.
- Medidas complementarias cuando proceda.
- Cumplimiento de los requisitos del RGPD.

Queda prohibido utilizar soluciones cuyo marco de cumplimiento no haya sido validado previamente por la empresa.

**7.4 Evaluación de Impacto en Protección de Datos**

La empresa realizará una Evaluación de Impacto relativa a la Protección de Datos (EIPD) antes de implantar sistemas de IA cuando estos puedan generar un alto riesgo para los derechos y libertades de las personas.

La evaluación analizará, entre otros aspectos:

- Naturaleza de los datos tratados.
- Finalidad del tratamiento.
- Riesgos para las personas afectadas.
- Posibles sesgos.
- Impacto discriminatorio.
- Medidas mitigadoras.

**7.5 Encargados de Tratamiento y Proveedores de IA**

Toda solución de IA que trate datos personales deberá ser previamente validada.

Antes de su contratación o utilización se verificará:

- Identidad del proveedor.
- Condiciones de uso.
- Política de privacidad.
- Medidas de seguridad implementadas.
- Existencia de contrato de encargado de tratamiento cuando proceda.
- Garantías frente a transferencias internacionales.
- Condiciones de reutilización de datos para entrenamiento de modelos.

No podrán utilizarse proveedores que no ofrezcan garantías suficientes de cumplimiento normativo.

### 7.6 Registro de Actividades de Tratamiento

Cuando el uso de sistemas de IA implique tratamientos de datos personales, dichos tratamientos deberán incorporarse al Registro de Actividades de Tratamiento de la organización cuando legalmente resulte exigible.

### 8. Transparencia y uso responsable

Cuando la IA contribuya significativamente a un contenido externo:

- Debe revisarse su coherencia, exactitud y adecuación legal
- Puede requerirse declaración interna de uso de IA
- La responsabilidad final recae siempre en el empleado o área responsable

### 8.1 Transparencia frente a Clientes, Proveedores y Terceros

Cuando la Inteligencia Artificial participe de forma significativa en la generación de contenidos, informes o interacciones con terceros, la empresa evaluará la necesidad de informar sobre dicho uso de acuerdo con la normativa vigente y los principios de transparencia corporativa.

La transparencia será especialmente relevante cuando:

- Existan interacciones automatizadas.
- Se generen contenidos sintéticos.
- Se utilicen asistentes virtuales.
- Se produzcan recomendaciones automatizadas.

### 8.2 Supervisión Humana Reforzada

Toda utilización de Inteligencia Artificial dentro de la empresaestará sometida a supervisión humana efectiva.

Ninguna decisión con impacto:legal, contractual, económico, financiero, laboral, reputacional, podrá adoptarse exclusivamente mediante inteligencia artificial.

La decisión final corresponderá siempre a una persona física identificable y responsable.

### 9. Supervisión, auditoría y cumplimiento

INDETGROUP podrá:

- Auditar el uso de herramientas de IA en entornos corporativos
- Revisar trazabilidad de usos en cuentas business
- Bloquear herramientas no autorizadas
- Aplicar medidas disciplinarias en caso de incumplimiento

### 9.1 Gestión de Incidentes Relacionados con Inteligencia Artificial

Además de los incidentes de seguridad informática, se considerarán incidentes relacionados con IA:

- Resultados erróneos relevantes.
- Sesgos o discriminaciones detectadas.
- Generación de contenido engañoso.
- Fugas de información.
- Uso de herramientas no autorizadas.
- Automatizaciones incorrectas.
- Incumplimientos regulatorios.

Todo incidente deberá comunicarse inmediatamente al responsable interno designado y será objeto de registro, análisis y adopción de medidas correctivas. Cuando pueda constituir una violación de seguridad de datos personales, se aplicará además el procedimiento interno previsto en materia de protección de datos.

### 9.2 Auditoría y Seguimiento de Sistemas IA

La empresa podrá realizar auditorías periódicas de los sistemas de Inteligencia Artificial autorizados para verificar:

- Cumplimiento normativo.
- Adecuación de los usos declarados.
- Calidad de los resultados.
- Gestión de riesgos.
- Protección de datos.
- Seguridad de la información.
- Cumplimiento de esta política.

## 10. Formación obligatoria

La empresa impulsará formación en:

- Uso responsable de IA
- Protección de datos (RGPD)
- Ciberseguridad aplicada a IA
- Buenas prácticas de promptingprofesional
- Riesgos del uso de IA generativa

La formación será proporcional al nivel de responsabilidad y riesgo de cada puesto.

### 10.1Responsablede Inteligencia Artificial

La Dirección designará un Responsablede Inteligencia Artificial o, alternativamente, un Comité de Gobernanza de IA.

Sus funciones incluirán:

- Aprobar nuevas herramientas.
- Evaluar riesgos.
- Mantener el inventario de sistemas.
- Controlar el cumplimiento normativo.
- Supervisar incidentes.
- Promover la formación.
- Revisar periódicamente esta política.

### 11. Actualización normativa

Este código será revisado y, cuando proceda, actualizado conforme:

- Entre en vigor nueva regulación del EU AI Acten sus fases progresivas
- Cambie la interpretación del RGPD en relación con IA generativa
- Evolucionen estándares internacionales de seguridad y compliance
- Se incorporen nuevas herramientas de IA en la empresa

### 12. Aceptación

El uso de cualquier herramienta de inteligencia artificial en INDETGROUP implica la aceptación expresa de esta política.

### 13. Guía de clasificación de documentos para uso de Inteligencia Artificial

Esta sección establece un sistema práctico de clasificación interna para determinar si un documento o información puede ser tratado con herramientas de IA.

El objetivo es garantizar el cumplimiento del presente código y reducir el riesgo de uso indebido de información.

### 13.1 Sistema de clasificación de niveles de información

INDETGROUP adopta una clasificación de 4 niveles:

**Nivel 1 — CONFIDENCIAL CRÍTICO (PROHIBIDO en IA)**

Información que **no puede introducirse en ninguna herramienta de IA**, bajo ninguna circunstancia.

Incluye:

- Datos personales sensibles (clientes, empleados, proveedores)
- Contratos no públicos o en negociación
- Información financiera interna detallada
- Estrategia empresarial, expansión o inversiones
- Datos de seguridad, accesos o sistemas internos
- Know-how propietario no publicado
- Información de proyectos en curso con clientes
- Incidencias legales o regulatorias internas

**Regla:**Si pertenece a este nivel, la IA está prohibida totalmente.

**Nivel 2 — CONFIDENCIAL INTERNO (RESTRINGIDO)**

Información interna sensible, pero no crítica.

Puede usarse en IA **solo si está anonimizada y con autorización previa**.

Incluye:

- Procesos internos no públicos
- Informes operativos internos
- Borradores de propuestas comerciales
- Análisis de negocio interno no estratégico
- Documentación técnica interna no crítica
- Comunicaciones internas sensibles

**Condición obligatoria:**

- Eliminar nombres de clientes, cifras sensibles y datos identificativos
- Usar solo en herramientas IA autorizadas (usuarios Business)

**Nivel 3 — USO INTERNO GENERAL (PERMITIDO CON IA BUSINESS)**

Información interna no sensible.

Puede usarse en IA sin grandes restricciones dentro del entorno corporativo.

Incluye:

- Procedimientos operativos estándar (SOPs)
- Documentación de soporte interna
- Textos de formación
- Resúmenes de reuniones sin datos sensibles
- Contenido de marketing no confidencial
- Descripciones generales de servicios

**Condición:**

- Siempre revisión humana antes de uso externo

**Nivel 4 — PÚBLICO (LIBRE USO EN IA)**

Información ya pública o no sensible.

Puede usarse libremente en IA (incluyendo herramientas gratuitas).

Incluye:

- Contenido de la web corporativa INDETGROUP
- Catálogos públicos de productos o servicios
- Material marketing publicado
- Comunicados de prensa
- Contenido de redes sociales públicas
- Información general del sector

**Regla:**Aun siendo público, debe revisarse coherencia antes de su uso final.

### 13.2 Árbol de decisión rápido (cómo saber si puedo usar IA)

Antes de usar IA, el empleado debe responder:

**PASO 1 — ¿Contiene datos internos de INDETGROUP?**

- Sí → pasar a Paso 2
- No → Nivel 4 (permitido)

**PASO 2 — ¿Contiene datos de clientes, dinero o estrategia?**

- Sí → PROHIBIDO (Nivel 1)
- No → Paso 3

**PASO 3 — ¿Es información operativa o interna no crítica?**

- Sí → o (requiere IA Business y posible anonimización)
- No → Paso 4

**PASO 4 — ¿Es solo contenido genérico o público?**

- Sí → permitido
- No → consultar a responsable

### 13.3 Reglas de anonimización obligatoria

Si un documento es Nivel 2 (Confidencial Interno), antes de usar IA debe:

- Eliminar nombres de clientes → sustituir por “Cliente A”, “Cliente B”
- Eliminar cifras reales → usar rangos o porcentajes
- Eliminar ubicaciones específicas si son sensibles
- Evitar descripciones que identifiquen proyectos reales
- No incluir fechas exactas de proyectos estratégicos

### 13.4 Ejemplos prácticos

**MAL (prohibido en IA)**

“Cliente Telefónica nos ha contratado un proyecto de 250.000€ para implementar X en Madrid”

Nivel 1 → PROHIBIDO

**ACEPTABLE CON ANONIMIZACIÓN**

“Cliente del sector telecomunicaciones ha contratado un proyecto de gran volumen para implementar una solución en Europa”

Nivel 2 → solo IA Business

**PERMITIDO**

“Ejemplo de estructura de propuesta comercial para un cliente del sector telecomunicaciones”

Nivel 3

**LIBRE**

“Mejores prácticas para redactar propuestas comerciales”

Nivel 4

### 13.5 Responsabilidad del usuario

Cada empleado es responsable de:

- Clasificar correctamente la información antes de usar IA
- No introducir datos sin revisar su nivel de sensibilidad
- Consultar al responsable de complianceen caso de duda

### 13.6 Regla final de oro

“Si existe la más mínima duda sobre si un dato es sensible, se considera automáticamente CONFIDENCIAL CRÍTICO y no se introduce en IA.”

## 14. Derechos de Propiedad Intelectual y Contenidos Generados mediante IA

Los usuarios serán responsables de verificar que la utilización de contenidos generados mediante Inteligencia Artificial no infringe derechos de terceros.

Antes de utilizar contenidos generados por IA con fines comerciales o contractuales se revisará:

- Titularidad de los derechos.
- Restricciones del proveedor.
- Derechos de autor.
- Derechos de imagen.
- Marcas registradas.
- Licencias aplicables.

Los contenidos generados mediante IA deberán ser revisados antes de su explotación comercial o publicación externa.

**15. Cláusula Final de Responsabilidad**

La Inteligencia Artificial constituye una herramienta de apoyo a la actividad profesional, pero no sustituye el juicio profesional, la responsabilidad legal ni la toma de decisiones humanas.

Toda persona que utilice herramientas de Inteligencia Artificial en INDETGROUP continuará siendo plenamente responsable de la información generada, revisada, validada o difundida mediante dichas herramientas.

**16. Control de aprobación y revisión**

La presente política deberá ser aprobada por la Dirección de INDETGROUP. Se revisará periódicamente y siempre que se produzcan cambios normativos, tecnológicos, organizativos o en los sistemas de IA utilizados. Cada versión deberá identificar, como mínimo, la fecha de aprobación, la versión vigente, el órgano aprobador y la persona responsable de su mantenimiento.