EMPRESA
CORPORACIÓN S.A.

POLÍTICA INTERNA DE USO DE INTELIGENCIA ARTIFICIAL

Gobernanza · Productividad · Transformación Digital

Versión:	1.0
Fecha de aprobación:	Mayo 2025
Departamento responsable:	Dirección de Transformación Digital
Clasificación:	CONFIDENCIAL · Uso Interno
Ámbito de aplicación:	Toda la organización

Índice de Contenidos

Sección	Título	Pág.
1	Introducción	3
2	Objetivos de la Política	3
3	Herramientas de IA Autorizadas	3
4	Riesgos del Uso No Controlado de IA	4
5	Privacidad y Protección de Datos	4
6	Validación Humana Obligatoria	4
7	Uso Responsable de la IA	5
8	Limitaciones de la Inteligencia Artificial	5
9	Usos Permitidos y Prohibidos	5
10	Responsabilidades	6
11	Buenas Prácticas	6
12	Conclusión	6

1. Introducción

La incorporación de herramientas de Inteligencia Artificial Generativa (IAG) en los entornos de trabajo corporativo representa una de las transformaciones tecnológicas más significativas de la última década. Soluciones como **Microsoft Copilot**, **ChatGPT** u otras plataformas basadas en modelos de lenguaje de gran escala (LLM) ofrecen capacidades sin precedentes para mejorar la productividad, automatizar tareas repetitivas y apoyar la toma de decisiones basada en datos.

Sin embargo, el uso no regulado de estas tecnologías conlleva riesgos relevantes para la organización: filtración involuntaria de información confidencial, generación de contenidos inexactos o sesgados, incumplimiento del Reglamento General de Protección de Datos (RGPD) y pérdida de control sobre procesos críticos del negocio.

La presente **Política Interna de Uso de Inteligencia Artificial** establece el marco de gobernanza, las normas de uso responsable y los procedimientos de supervisión que todos los empleados, colaboradores y contratistas de la organización deben observar al utilizar herramientas de IA en el desempeño de sus funciones profesionales. Esta política se alinea con los principios del **AI Act de la Unión Europea**, las directrices de Microsoft para el despliegue responsable de Copilot y las mejores prácticas internacionales en gobernanza de IA.

2. Objetivos de la Política

- Establecer un **marco de gobernanza claro** para el uso ético y responsable de herramientas de IA generativa.
- Garantizar la **protección de la información confidencial** y los datos personales de clientes, empleados y socios comerciales.
- Maximizar los **beneficios de productividad** derivados de la IA minimizando los riesgos organizacionales.
- Asegurar el **cumplimiento normativo** con el RGPD, el AI Act europeo y demás legislación aplicable.
- Promover una **cultura de uso crítico y responsable**, garantizando la supervisión humana en todas las salidas generadas por IA.
- Definir con claridad las **responsabilidades de cada nivel organizativo** en la gestión de estas tecnologías.

3. Herramientas de IA Autorizadas

Únicamente podrán utilizarse en el entorno corporativo las herramientas de IA expresamente aprobadas por el Departamento de Tecnología e Innovación. A continuación se relacionan las plataformas autorizadas en el momento de publicación de este documento:

Herramienta	Descripción y ámbito de uso
Microsoft Copilot para M365	Integrado en Word, Excel, PowerPoint, Teams, Outlook y OneNote. Asistencia en redacción, resumen de reuniones, análisis de datos y generación de presentaciones.
Microsoft Copilot Studio	Creación de agentes conversacionales corporativos sobre datos propios mediante conectores seguros de Microsoft 365.

ChatGPT Enterprise	Versión corporativa sin retención de datos para entrenamiento. Uso autorizado para tareas de análisis, síntesis de información y redacción asistida.
Azure OpenAI Service	Acceso a modelos GPT-4 dentro del entorno seguro de Azure, con datos procesados exclusivamente en la región UE designada.

Nota importante: El uso de herramientas de IA no incluidas en esta lista —incluyendo versiones gratuitas o personales de ChatGPT, Gemini, Perplexity u otras— queda expresamente prohibido para el tratamiento de información corporativa hasta su evaluación y aprobación formal por parte del equipo de Seguridad de la Información.

4. Riesgos del Uso No Controlado de IA

- **Filtración de datos confidenciales.** La introducción de información sensible —contratos, datos de clientes, estrategias comerciales o documentación financiera— en plataformas no autorizadas puede exponer dicha información a terceros o incorporarla al entrenamiento de modelos externos.
- **Alucinaciones y desinformación.** Los modelos LLM pueden generar afirmaciones factualmente incorrectas con apariencia de veracidad. El uso no supervisado de estos contenidos en informes, propuestas o comunicaciones externas puede comprometer la reputación corporativa.
- **Incumplimiento normativo.** El tratamiento de datos personales mediante herramientas IA no homologadas puede vulnerar el RGPD, con sanciones de hasta el 4% de la facturación anual global.
- **Dependencia tecnológica y pérdida de capacidad crítica.** La automatización excesiva sin supervisión puede erosionar el juicio profesional y generar dependencias no gestionadas.
- **Sesgos en la toma de decisiones.** Los modelos de IA pueden reproducir o amplificar sesgos presentes en sus datos de entrenamiento, afectando procesos de selección, análisis de clientes o evaluaciones de rendimiento.

5. Privacidad y Protección de Datos

El uso de herramientas de IA en la organización se rige por los principios establecidos en el **Reglamento (UE) 2016/679 (RGPD)** y la normativa nacional aplicable. Toda herramienta de IA autorizada debe contar con un **Acuerdo de Tratamiento de Datos (ATD)** suscrito con el proveedor y, cuando proceda, una **Evaluación de Impacto en la Protección de Datos (EIPD)**.

- Queda **prohibido introducir datos personales** de empleados, clientes o terceros en herramientas de IA, salvo en entornos técnicamente aislados y expresamente autorizados.
- Las conversaciones con herramientas de IA corporativas son registrables con fines de auditoría de seguridad. Los empleados son informados de ello mediante la aceptación de esta política.
- **Microsoft Copilot para M365** procesa los datos dentro del tenant corporativo y no los utiliza para entrenar modelos globales, conforme a los compromisos de Microsoft para clientes empresariales.
- Cualquier nueva herramienta IA que requiera acceso a datos corporativos deberá pasar por el proceso de **Due Diligence de Seguridad** antes de su activación.

6. Validación Humana Obligatoria

La organización establece como principio irrenunciable que **ningún output generado por una herramienta de IA podrá ser utilizado, publicado, enviado o aprobado sin revisión humana previa**. Este principio

aplica con especial rigor en los siguientes contextos:

- Comunicaciones externas con clientes, proveedores o medios de comunicación.
- Informes financieros, memorandos ejecutivos o documentación legal.
- Contenido destinado a publicación en canales corporativos (web, RRSS, newsletter).
- Propuestas comerciales, contratos o acuerdos de cualquier naturaleza.
- Resúmenes de reuniones generados por Copilot en Microsoft Teams antes de su distribución.
- Análisis de datos o dashboards generados mediante prompts en Copilot para Excel o Power BI.

Principio de responsabilidad: El empleado que utilice una herramienta de IA para generar un contenido es responsable de su exactitud, adecuación y cumplimiento normativo, con independencia de la herramienta utilizada.

7. Uso Responsable de la Inteligencia Artificial

El uso responsable de la IA implica adoptar una actitud crítica, informada y ética en cada interacción con estas herramientas. La organización promueve los siguientes principios:

- **Transparencia:** Cuando un documento, análisis o comunicación haya sido elaborado con apoyo de IA, el autor debe indicarlo en los metadatos o en la sección correspondiente del documento.
- **Proporcionalidad:** La IA debe utilizarse para amplificar las capacidades humanas, no para sustituir el juicio profesional en decisiones de alto impacto.
- **Verificación de fuentes:** Todo dato, cifra o referencia generada por IA debe ser contrastado con fuentes primarias antes de su uso en contextos formales.
- **Confidencialidad de prompts:** Los prompts utilizados en herramientas corporativas pueden contener información sensible y deben tratarse con el mismo nivel de protección que los documentos internos.
- **Actualización continua:** Los empleados tienen la responsabilidad de mantenerse al día en las capacidades y limitaciones de las herramientas autorizadas mediante los programas de formación corporativa.

8. Limitaciones de la Inteligencia Artificial

Los empleados deben ser conscientes de las siguientes limitaciones estructurales de los modelos de IA generativa actualmente disponibles:

- **Corte de conocimiento:** Los modelos LLM tienen una fecha límite de entrenamiento y no disponen de información actualizada en tiempo real, salvo que se les proporcione mediante conectores o Retrieval-Augmented Generation (RAG).
- **Ausencia de razonamiento causal:** La IA genera respuestas estadísticamente plausibles, no razonamientos causales verificados. No «entiende» el contexto empresarial ni las implicaciones estratégicas de sus salidas.
- **Inconsistencia entre sesiones:** Las herramientas de IA pueden generar respuestas distintas ante el mismo prompt en momentos diferentes, lo que las hace inadecuadas como fuente única en análisis críticos.
- **Sesgos heredados:** Los modelos pueden reflejar sesgos sociales, culturales o de género presentes en sus datos de entrenamiento, especialmente en análisis de personas o grupos.
- **Incapacidad para el secreto profesional:** Ninguna herramienta de IA está habilitada para asesorar en materia jurídica, fiscal o médica con garantías de responsabilidad profesional.

9. Usos Permitidos y Usos Prohibidos

✔ USOS PERMITIDOS	✘ USOS PROHIBIDOS
✔ Redactar o mejorar correos electrónicos internos con Copilot en Outlook.	✘ Introducir datos personales de clientes o empleados en cualquier herramienta no autorizada.
✔ Generar resúmenes de reuniones en Teams con posterior revisión.	✘ Publicar contenido generado por IA sin revisión y aprobación humana previa.

✔ Crear borradores de presentaciones en PowerPoint con Copilot.	✘ Utilizar IA para tomar decisiones autónomas sobre contratación, despido o evaluación.
✔ Analizar hojas de cálculo y extraer tendencias con Copilot en Excel.	✘ Compartir credenciales corporativas con servicios IA externos no homologados.
✔ Sintetizar documentación técnica o normativa extensa.	✘ Usar IA para generar contenido engañoso, sesgado o discriminatorio.
✔ Automatizar generación de informes periódicos con plantillas validadas.	✘ Introducir estrategias comerciales, M&A; o información financiera no pública.
✔ Brainstorming y generación de ideas para proyectos creativos internos.	✘ Generar contenido que infrinja derechos de propiedad intelectual de terceros.

Ejemplos de aplicación corporativa autorizada:

- **Automatización de documentación interna.** El equipo de Operaciones utiliza Copilot en Word para generar borradores de procedimientos internos a partir de notas de reunión. El responsable del área revisa y valida el documento antes de su publicación en el repositorio corporativo.
- **Análisis de información comercial.** El Departamento de Ventas emplea Copilot en Excel para identificar patrones en los datos de pipeline de CRM exportados, generando visualizaciones que el equipo analiza y complementa con su criterio antes de presentar al Comité de Dirección.
- **Comunicación corporativa.** El equipo de Marketing usa ChatGPT Enterprise para generar primeros borradores de comunicados de prensa o artículos de blog, que posteriormente son revisados, adaptados y aprobados por el Director de Comunicación.
- **Resumen de reuniones.** Copilot en Teams transcribe y resume automáticamente las reuniones de proyecto. El coordinador revisa el resumen, corrige imprecisiones y lo distribuye como acta oficial, indicando que fue generado con apoyo de IA.

10. Responsabilidades

ROL	RESPONSABILIDAD PRINCIPAL
Dirección General	Aprobar la política y garantizar su cumplimiento estratégico.
Dir. Transformación Digital	Mantener actualizado el inventario de herramientas y la formación.
Responsable de RRHH	Comunicar la política a todos los empleados y registrar la aceptación.
Responsable de IT / Seguridad	Supervisar el acceso, la integración y los controles técnicos de las herramientas IA.
Delegado de Protección de Datos	Evaluar el impacto en privacidad (EIPD) de nuevas herramientas IA.
Empleados y colaboradores	Utilizar las herramientas autorizadas conforme a esta política y reportar incidencias.

11. Buenas Prácticas en el Uso de IA

- **Diseña prompts claros y contextualizados.** Cuanta más información relevante proporciones a la herramienta, mayor será la calidad y pertinencia de la respuesta. Incluye siempre el rol, el objetivo y el contexto de la tarea.
- **Nunca copies y pegues sin leer.** Antes de insertar cualquier output de IA en un documento oficial, léelo íntegramente, verifica los datos y adapta el tono a los estándares corporativos.
- **Mantén un registro de tus interacciones relevantes.** Para proyectos de importancia, conserva los prompts utilizados y las respuestas obtenidas para garantizar la trazabilidad del proceso.
- **Reporta comportamientos anómalos.** Si una herramienta genera contenido inapropiado, inexacto o que comprometa datos sensibles, repórtalo de inmediato al Departamento de IT a través del canal de incidencias de seguridad.
- **Participa en la formación continua.** La organización ofrecerá sesiones de actualización trimestrales sobre el uso de herramientas IA corporativas. La asistencia es obligatoria para todos los usuarios con acceso a estas plataformas.
- **Distingue entre apoyo y delegación.** La IA puede apoyarte en la ejecución, pero la estrategia, el criterio ético y la responsabilidad sobre el resultado son siempre del profesional.

12. Conclusión

La Inteligencia Artificial generativa representa una oportunidad transformadora para nuestra organización: permite reducir tiempos de ejecución, elevar la calidad de los entregables y liberar capacidad humana para actividades de mayor valor estratégico. Sin embargo, aprovechar ese potencial de forma sostenible exige un marco de gobernanza robusto, cultura de uso responsable y supervisión permanente.

Esta política no pretende limitar la innovación, sino **canalizarla de forma segura y ética**. La organización se compromete a actualizar este documento de forma periódica —al menos anualmente o ante cambios normativos o tecnológicos significativos— para garantizar que su contenido refleje las mejores prácticas del sector y las capacidades reales de las herramientas disponibles.

Todos los empleados, una vez notificados de la existencia de esta política, deberán firmar el **Acuse de Recibo y Compromiso de Cumplimiento** correspondiente, disponible en el portal de RRHH de Microsoft SharePoint. El incumplimiento de las disposiciones aquí recogidas podrá dar lugar a medidas disciplinarias

conforme a lo establecido en el Convenio Colectivo y el Reglamento Interno de Conducta.

Aprobado por	Revisado por	Fecha de vigencia
Dirección General _____	Dir. Transformación Digital _____	Mayo 2025 Versión 1.0 Próxima revisión: Mayo 2026