¿Qué pasa con mis datos?
Uso responsable de IA generativa en la empresa

ÍNDICE

INTRODUCCIÓN

RIESGOS DE LA IA GENERATIVA

MITIGACIÓN

CONCLUSIONES

Introducción

Quienes somos Datua

Somos expertos en Dato e IA y formamos parte del grupo Teknei

Dato e IA

Es la empresa del **Grupo Teknei** especializada en proyectos del **DATO y de Inteligencia Artificial** que abarca toda la cadena de valor de esta industria, desde la estrategia y la gobernanza, pasando por la arquitectura e ingeniería y llegando a la ciencia de datos y la visualización.

¿Qué es la IA Generativa?

Tecnología que **crea contenido nuevo** (texto, código, imágenes) basado en patrones de datos.

Entrenamiento

DATASET

ENTRENAMIENTO

MODELO

Utilización

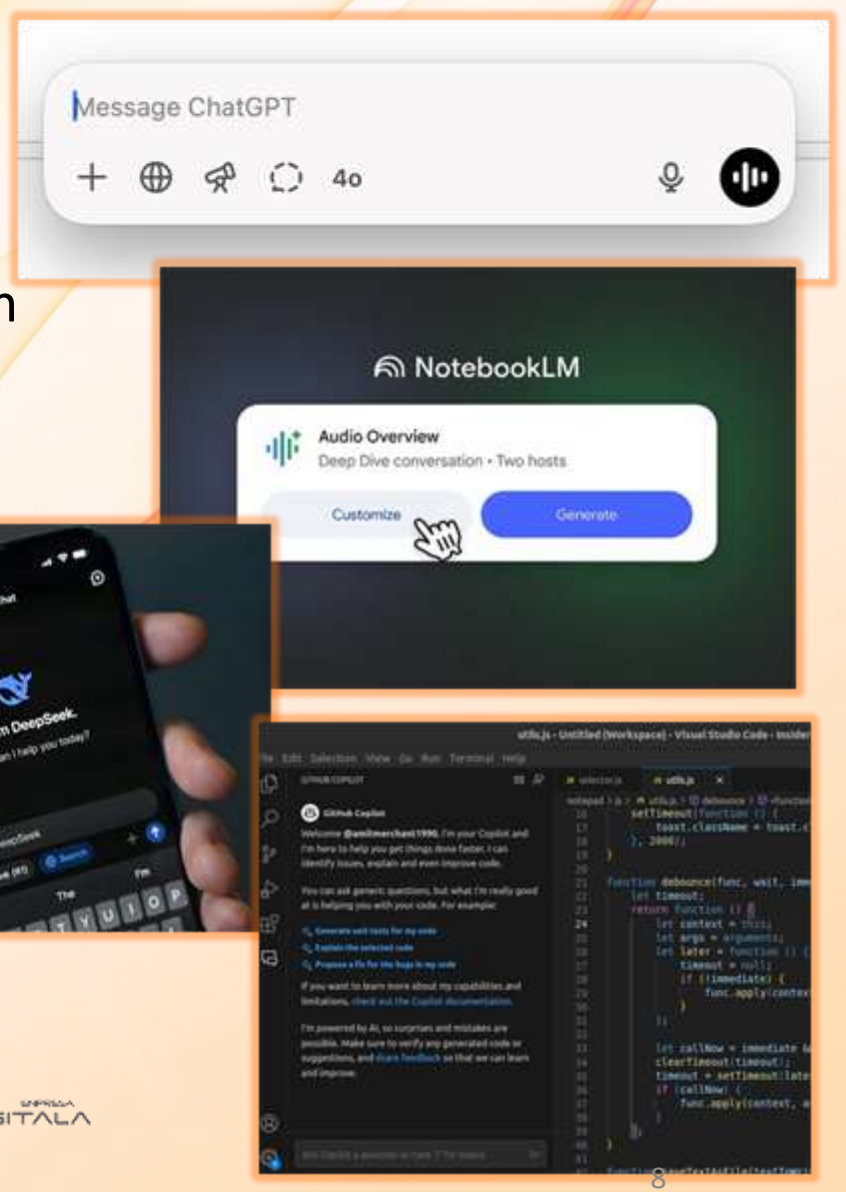
INPUT USUARIO

ASISTENTE

CONTENIDO GENERADO

Utilización

- **Productividad**: Redacción de emails, informes, documentación
- **Desarrollo**: Generación y revisión de código
- **Marketing**: Creación de contenido, ideas creativas
- **Análisis**: Resúmenes de datos, insights
- **Soporte**: Chatbots, asistentes virtuales



Panorama actual

- Adopción masiva y rápida en las organizaciones
- Beneficios evidentes vs. riesgos ocultos
- Necesidad de equilibrio entre innovación y seguridad

Panorama actual

- Adopción masiva y rápida en las organizaciones
- Beneficios evidentes vs. **riesgos ocultos**
- Necesidad de equilibrio entre innovación y seguridad

Riesgos

Fuga de Información Confidencial

Un desarrollador de software en una gran empresa tecnológica está intentando optimizar un algoritmo complejo. Para obtener ayuda, copia y pega **miles de líneas de código propietario** en ChatGPT.

Fuga de Información Confidencial

Forbes

BREAKING | BUSINESS

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

By Siladitya Ray, Forbes Staff. Siladitya Ray is a New Delhi-based Forbes new...

Follow Author

Published May 02, 2023, 07:17am EDT, Updated May 02, 2023, 07:31am EDT

Fuga de Información Confidencial

Conocimiento Interno de la Empresa

El problema: Los empleados introducen datos sensibles en herramientas externas sin considerar las implicaciones

Información en riesgo:

- Estrategias de negocio y planes futuros
- Datos financieros y métricas internas
- Información de productos no lanzados
- Análisis de competencia y positioning

Consecuencias: Pérdida de ventaja competitiva, incumplimiento normativo, filtración a competidores

Fuga de Información Confidencial

Credenciales y Datos de Acceso

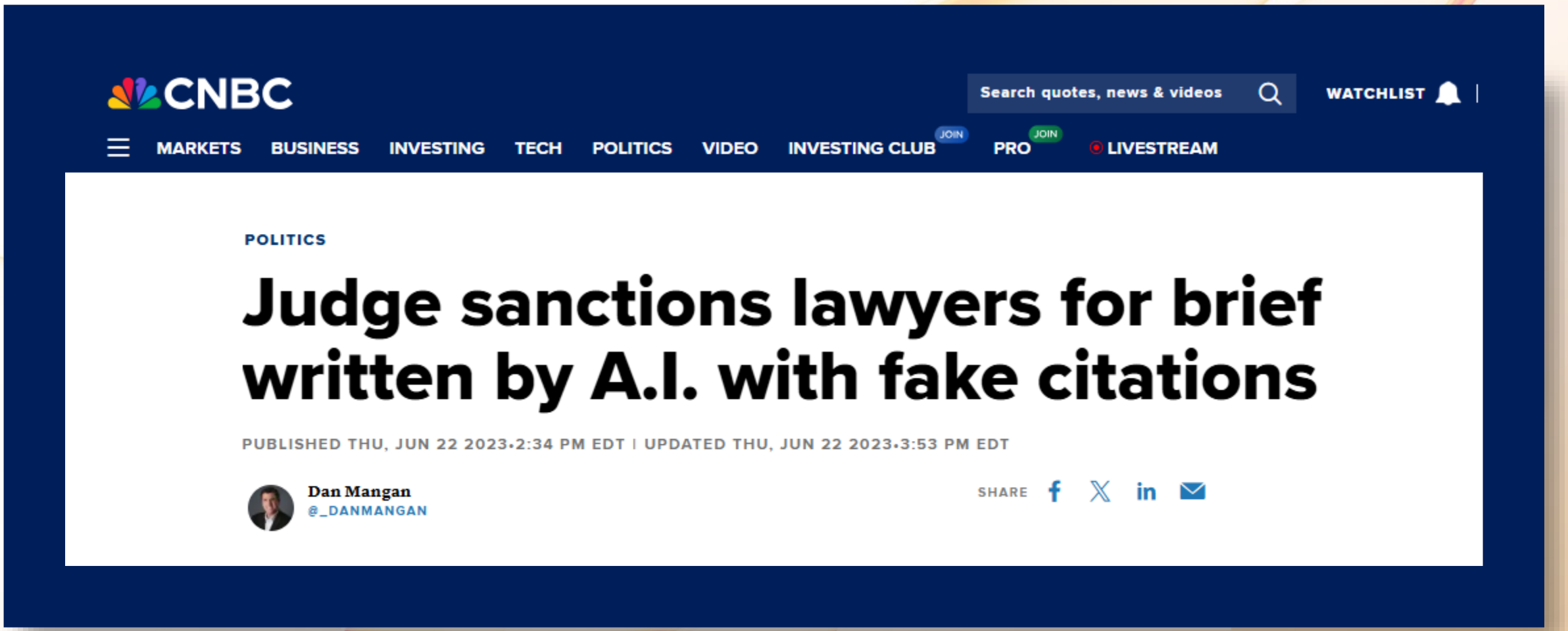
El problema: Uso inadvertido de contraseñas, tokens, APIs y credenciales en prompts

Riesgos asociados:

- Acceso no autorizado a sistemas críticos
- Compromiso de la seguridad corporativa
- Exposición de datos sensibles de clientes
- Violaciones de datos con implicaciones legales

Uso sin Supervisión

Un abogado en un bufete reconocido redacta un escrito judicial urgente. Para ahorrar tiempo, utiliza ChatGPT para incluir jurisprudencia. Sin saberlo, presenta ante el juez varias citas completamente inventadas por la IA.



CNBC

Search quotes, news & videos

WATCHLIST

MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING CLUB JOIN PRO JOIN LIVESTREAM

POLITICS

Judge sanctions lawyers for brief written by A.I. with fake citations

PUBLISHED THU, JUN 22 2023•2:34 PM EDT | UPDATED THU, JUN 22 2023•3:53 PM EDT

Dan Mangan
@_DANMANGAN

SHARE

Uso sin Supervisión

El problema:

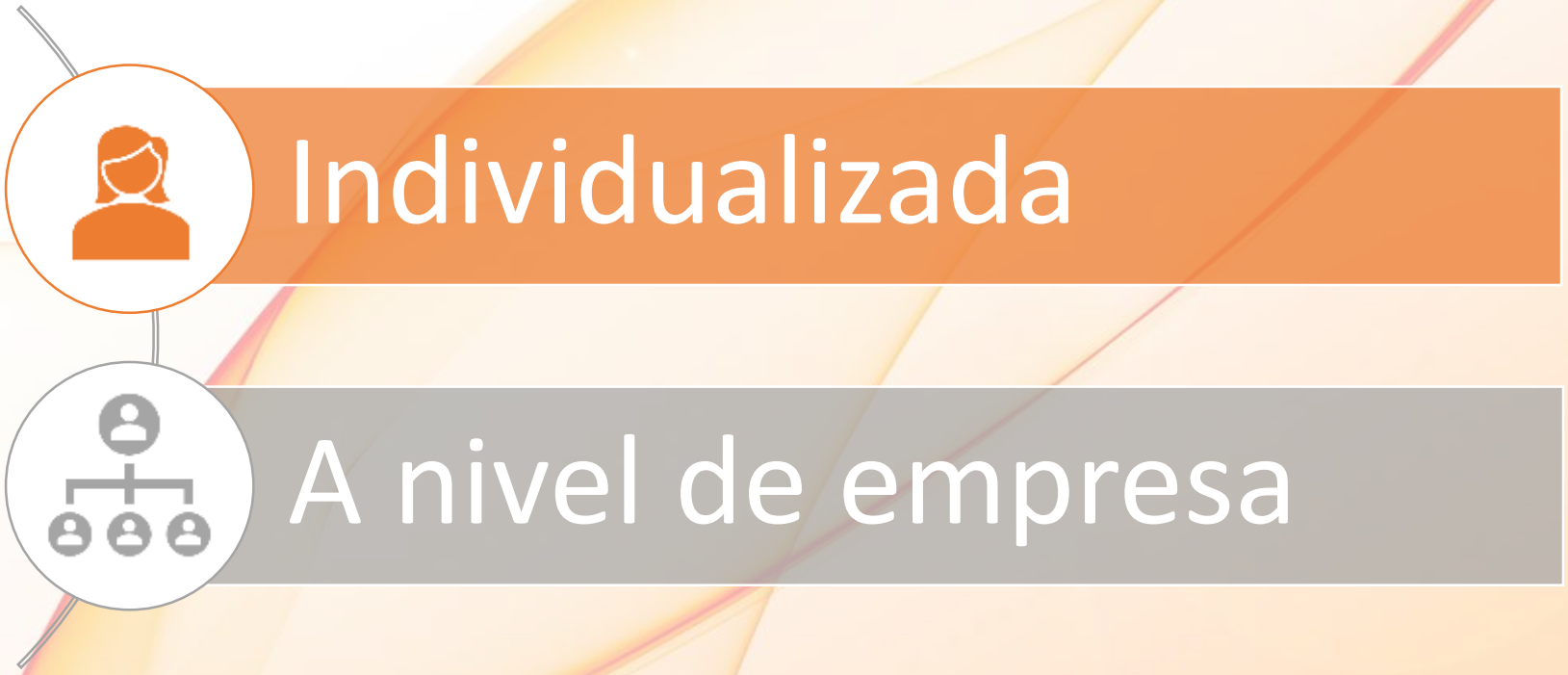
Dependencia excesiva en las respuestas de IA sin validación

Riesgos asociados:

- Errores operativos: Información incorrecta en procesos críticos
- Desinformación: Propagación de datos falsos o desactualizados
- Decisiones erróneas: Estrategias basadas en análisis defectuosos

Mitigación

Mitigación



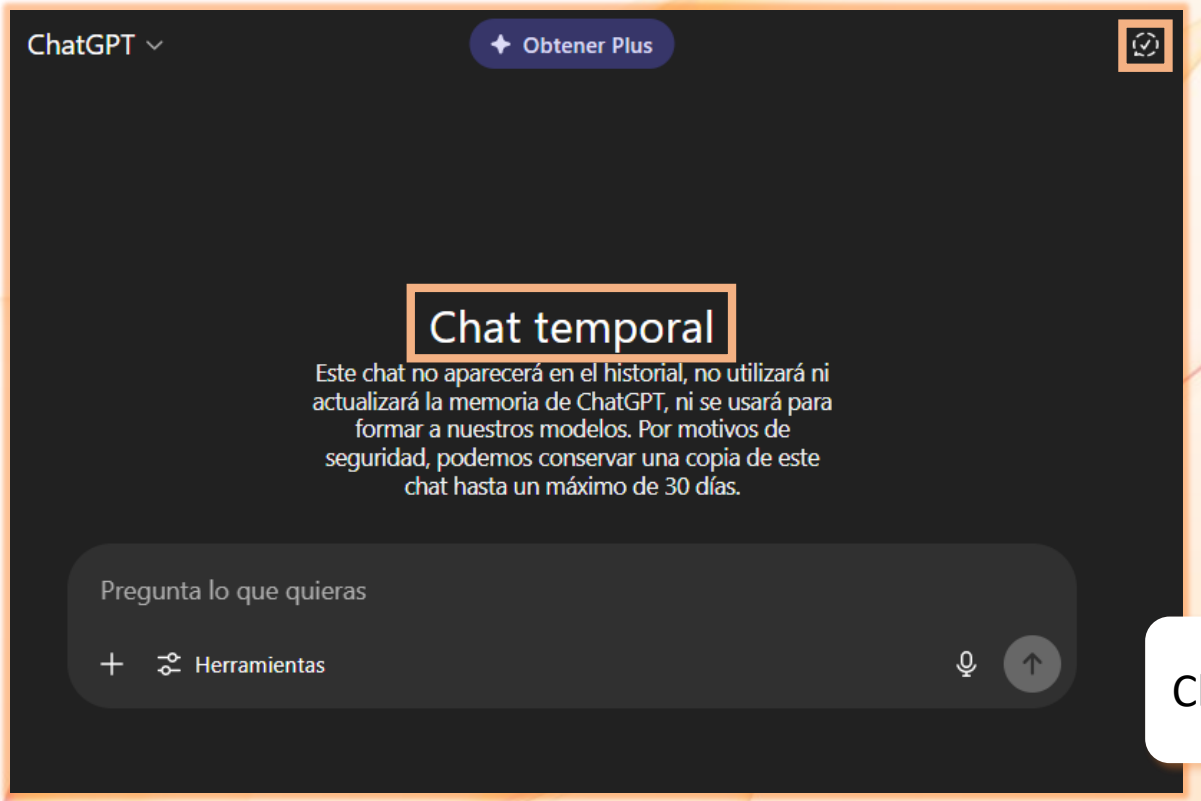
Mitigación individualizada

Privacidad

- Chats temporales
- Desactivar entrenamiento de modelos con nuestros datos

Supervisión activa

Mitigación individualizada



Chats temporales

Mitigación individualizada

Desactivar entrenamiento de modelos con nuestros datos

Mitigación a nivel de empresa

¿Alguien está utilizando IA Generativa?
¿En qué procesos está siendo utilizado?
¿Qué tecnologías están siendo utilizadas?
¿En qué se puede utilizar?
¿Qué requerimientos de privacidad tienen nuestros datos?

Mitigación a nivel de empresa

Bufete de abogados

Empresa de construcción

Mitigación a nivel de empresa

Bufete de abogados

Análisis de documentos fiscales complejos para generar argumentos legales que permitan reducir o impugnar las cantidades reclamadas por la administración tributaria.

- Información altamente confidencial
- Procesos legales críticos

Mitigación a nivel de empresa

Bufete de abogados

→ Desarrollo de aplicación web propia

Mitigación a nivel de empresa

Bufete de abogados

Confidencialidad

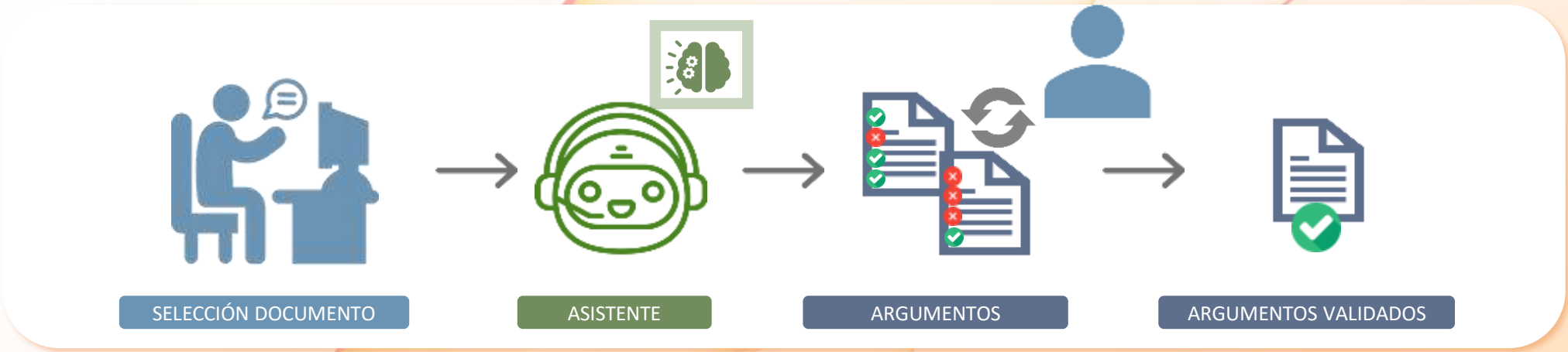
- Implementación de asistente propio basado en modelos vía API
  - Selección rigurosa de modelos: análisis de términos y condiciones de uso
  - Evaluación del tratamiento de datos por parte del proveedor

Mitigación a nivel de empresa

Bufete de abogados

Supervisión

- ❑ Generación de argumentos mediante aplicativo
- ❑ Obligación de lectura y aprobación manual de los argumentos mediante el aplicativo



Mitigación a nivel de empresa

Empresa de construcción

- Traducciones
- Consultas de normativa
- Extracción de información desde pliegos

⚠ Información altamente confidencial

⚠ Procesos complejos, necesidad de estándares

Mitigación a nivel de empresa

Empresa de construcción

- Traducciones
- Consultas de normativa

Asistencia

<u>Selección de plataforma estándar</u> →

ChatGPT

Enterprise

IA para empresas, seguridad y asistencia a escala

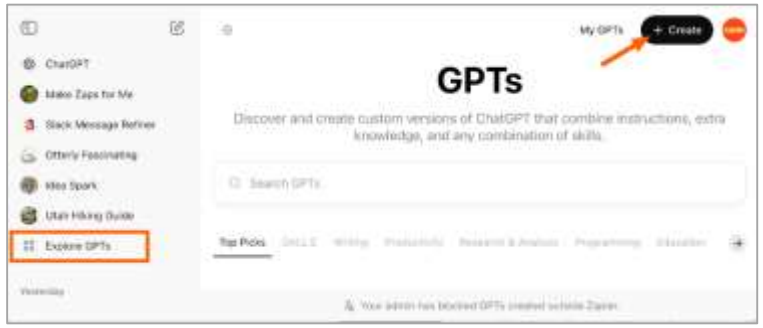
Mitigación a nivel de empresa

Empresa de construcción

- Traducciones
- Consultas de normativa

Asistencia

Acompañamiento



Mitigación a nivel de empresa

Empresa de construcción

Extracción de información desde pliegos — **PoC**

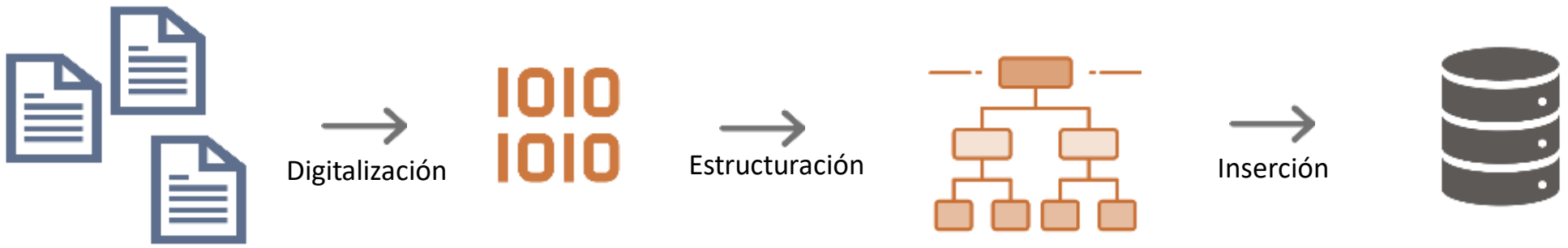
- Datos de entrada complejos
  - Documentos Word o PDF con formatos variados
  - Documentos con tablas e imágenes
- Necesidad de digitalizar y estructurar los datos

Mitigación a nivel de empresa

Empresa de construcción

Extracción de información desde pliegos

PoC



Mitigación a nivel de empresa

Empresa de construcción

Extracción de información desde pliegos — **PoC**

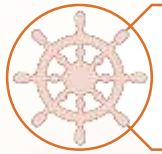
Conclusiones

CONCLUSIONES

La IA generativa ofrece grandes beneficios, pero conlleva riesgos reales: fuga de datos, errores y uso indebido.

Es clave equilibrar innovación con privacidad y seguridad.

Mitigar riesgos requiere acciones tanto individuales como empresariales.



Necesitamos control, supervisión y uso consciente en todos los procesos.

Con una estrategia clara, la IA puede ser un gran aliado.

ESKERRIK ASKO