JORNADAS | GIPUZKOA TECNOLÓGICA

IA con Sentido Común: Tecnología, Privacidad y Buenas Prácticas

kuik!

IA SOLUTIONS

Cámara Gipuzkoako Ganbera

GRUPO spri TALDEA

EUSKO JAURLARITZA GOBIERNO VASCO

INDUSTRIA, TRANTSIZIO ENERGETIKO ETA JASANGARRITASUN SAILA

DEPARTAMENTO DE INDUSTRIA, TRANSICIÓN ENERGÉTICA Y SOSTENIBILIDAD

spri ENPRESA DIGITALA

Tendencias de la IA

Estamos viviendo un boom, **una nueva revolución industrial,** esta vez aplicada a los trabajos cross y de servicios. Es innegable que ahora hay una **oportunidad de crecimiento** para todo tipo de empresas, puesto que este avance en lugar de estar dedicado a un sector, afecta a **todo tipo de departamentos y procesos.**

Las empresas tienen en su mano la oportunidad de **incorporar una tecnología que va a afectar directamente a su productividad** y a la calidad de sus servicios, pero es importante hacer una buena gestión del cambio y de concienciación interna para que se entienda como **un avance para todos.**

JORNADAS GIPUZKOA TECNOLÓGICA

El boom de los asistentes y agentes

Agentes vs Asistentes

- **Los asistentes** están optimizados para la comunicación y la comprensión del lenguaje natural
- **Un agente** es un sistema con mayor grado de autonomía, capaz tomar decisiones independientes sin necesidad de supervisión

Asistentes externos

- Permiten abrir un nuevo canal hacia los clientes, proporcionando una nueva forma de interacción y acceso a los servicios
- Mejora la experiencia de los clientes proporcionando soporte 24/7 con información controlada

Asistentes internos

- Están orientados a aumentar la eficiencia y agilidad operativa, explotando la información interna
- Pueden llegar a agilizar tareas repetitivas, permitiendo la especialización en tareas de mayor valor añadido

Acceso ágil al conocimiento

- Permiten combinar distintas fuentes de información para obtener respuestas completas
- Sirven de punto de acceso universal garantizando cierto control de acceso

Aprendizaje continuo

- Mediante el uso de técnicas de deep learning que permiten adaptarse a distintos contextos
- Esto proporciona interacciones más naturales y dinámicas

Versátil

- No se limitan a una única área dentro de la organización
- Desde atención al cliente, hasta administración, las soluciones de IA se pueden adaptar a múltiples procesos

Flexibilidad

- Su potencial puede ser aplicable en diferentes formatos, desde aplicaciones, hasta chats integrados en herramientas como teams

Cámara Gipuzkoako Ganbera · Grupo spri Taldea · Eusko Jaurlaritza Gobierno Vasco · spri Enpresa Digitala

LLMs como impulso tecnológico

Para consultas externas

- La herramienta más versátil sigue siendo ChatGPT, aunque existen otras muy interesantes como Claude que también proporcionan buenos resultados. Son un buen principio para empezar a manejarse con esta tecnología.
- Es importante tener en cuenta que con estas herramientas la privacidad de la información no estaría garantizada, por lo que su uso debería estar orientado a la explotación de información externa a la empresa

Para herramientas de Microsoft

- A diferencia de un chatbot independiente, Copilot vive dentro de las aplicaciones que ya usamos, siendo una herramienta muy útil en el día a día
- Podemos “hablarle” mediante indicaciones en lenguaje natural: resumir un hilo de correos en Outlook, generar un borrador de documento en Word o desarrollar las fórmulas en un Excel (incluso las macros)

Para consultas a datos internos

- Un punto interesante para las empresas es poder desarrollar sus propios agentes explotando información interna, para lo cuál existen alternativas opensource
- Hay que tener en cuenta que existen opciones intermedias antes de llegar a montar toda la infraestructura en local, que facilitan el acceso a esos modelos en un entorno seguro
- Existen multitud de modelos válidos, destacando sobre todo los de Mistral, Gemma, Deepseek y Phi4

Para consultas específicas

- En muchos sectores se están desarrollando soluciones ad hoc que pueden resultar muy útiles a la hora de realizar consultas más en detalle
- Especialmente interesantes los bots que se están desarrollando dentro del mundo Legal, muy útiles para consultas directas

JORNADAS

GIPUZKOA TECNOLÓGICA

¿Qué debe contemplar una política de IA?

01

Principios legales

Compromiso con un uso responsable, justo y seguro de la IA.Declaración de alineación con el AI Act, RGPD y normas locales

02

Principios éticos

Entre ellos podríamos identificar como la no discriminación, transparencia, privacidad y seguridad, protección de datos sensibles…

03

Niveles de riesgo de la IA

Clasificar e identificar las diferentes soluciones según los niveles de riesgo y aplicar controles proporcionales: auditorías, explicabilidad, revisión humana….

04

Protección de los datos

Asegurar que están protegidos conforme al RGPD, son de calidad, están actualizados y no sesgados. Además, se deben marcar condiciones de acceso, conservación y anonimización.

05

Responsabilidad

Asignar roles claros como responsables técnicos, legales, éticos. Crear un comité o canal de revisión ética para proyectos sensibles

06

Transparencia

Informar a usuarios cuando están interactuando con una IA. Explicar, de forma comprensible, en qué se basan las decisiones el sistema. Ofrecer siempre la opción de revisión humana en decisiones importantes

07

Auditorías

Probar los sistemas de IA antes de su puesta en marcha. Establecer un proceso de auditoría continua para: detección de errores o sesgos. Documentar todo el ciclo de vida del sistema.

08

Formación continua

Formación obligatoria sobre el uso seguro y ético de la IA. Sensibilización a empleados sobre derechos, riesgos y limitaciones

Cámara Gipuzkoako Ganbera · Grupo SPRI Taldea · Eusko Jaurlaritza Gobierno Vasco · SPRI Empresa Digitala

JORNADAS GIPUZKOA TECNOLÓGICA

¿Cómo abordamos un proyecto de IA?

Definición de los KPIs que validan la hipótesis
Ej. si tuvieramos un bot de consultas, reduciríamos en un 20% los clientes desatendidos

Selección del tipo de proyecto o tecnología más adecuada para la problemática descrita, con la decisión de hacerlo de forma interna o externalizarlo

Monitorización y ajuste continuo de la solución implantaada

Hipótesis principal

Iterativo hasta definir la solución que más se ajusta a la necesidad

Conceptualización técnica y funcional de la solución que resuelve la hipótesis

Implantación y programa de gestión del cambio

Validación de los usuarios de negocio y ajustes finales

Desarrollo de la solución adecuada para la necesidad definida

Clasificación de los tipos de proyecto

Alto riesgo

Estos sistemas no están prohibidos, pero deben cumplir requisitos estrictos de seguridad, transparencia, trazabilidad y supervisión.

Requiere de ciertos elementos para poder publicarse: registro obligatorio en una base de datos europea, evaluación de riesgos previa al uso, documentación técnica completa y actualizada, supervisión humana para minimizar sesgos y auditorías periódicas

Ejemplos:

- Soluciones de IA utilizadas para procesos de contratación
- Sistemas de predicción de accidentes en los que puedan verse afectadas las personas

Riesgo limitado (transparencia obligatoria)

Son sistemas de IA que interactúan con personas o generan contenido, pero cuyo impacto directo sobre decisiones o acciones finales es más limitado.

En cualquiera de los casos, deben informar de forma clara a los usuarios que están interactuando con un sistema de IA y se debe ofrecer la capacidad de respuesta.

Ejemplos:

- Bot asistente que responda a los pedidos y consultas de un área de negocio
- Bot asistente para resolver dudas internas de los trabajadores

Riesgo mínimo o nulo

Muchas de las aplicaciones de IA actuales que están enfocadas a trabajar directamente sobre procesos de negocio.

Hay que tener una vigilancia sobre su uso en cuestiones de ética y realizar revisiones mínimas para asegurar que se está comportando como debe y sin acceder a ningún apartado al margen de lo que se le ha pedido.

Ejemplos:

- Automatización para identificar y volcar facturas de proveedores al ERP
- Clasificación de los mensajes de satisfacción que dejan los clientes para extracción de métricas

JORNADAS GIPUZKOA TECNOLÓGICA

Foco en el control de los datos

Propiedad de los datos

El sistema debería garantizar que la propiedad de los datos recae siempre en propietario, brindando control total sobre su información y sobre las decisiones.

Privacidad de las BDD

En cualquier formato, se debe garantizar el acceso diferenciado entre las BDD propias y las externas para que no haya mezcla de información, asegurando que no se llega a exponer al exterior

Entrada autenticada

Habrá que valorar que según el tipo de sistema que se desarrolle, habrá que asegurar que hay una entrada autenticada para determinados tipos de información

LLM on premise

Otro punto diferencial es el uso de LLMs open office, instalados modo local. Esto da mayor control pudiendo garantizar que no se utilizan para entrenamientos de los modelos.

Control de accesos

Para acceder a cualquier información, es importante plantear niveles de acceso dependiendo de los roles o tipos de usuarios que van a tratar la información.

Responsables de datos

Cada organización debería tener identificados posibles responsables con respecto a la propiedad y el seguimiento de los datos en general.

Cámara Gipuzkoako Ganbera · Grupo SPRI Taldea · Eusko Jaurlaritza Gobierno Vasco · SPRI Enpresa Digitala

Apostar por una infraestructura privada

Puedes escalar horizontalmente sin costes prohibitivos. Inviertes en talento interno y tecnología controlada por la empresa.

En lugar de enviar datos a plataformas externas se mantienen on-premise o en cloud, pero evitando riesgos de compliance. Puedes aplicar estrategias de anonimización, logging y cifrado de forma personalizada y tener una mayor trazabilidad sobre el uso de los datos.

Los agentes open source se pueden conectar más fácilmente con ERP, CRM, bases de datos, APIs internas, etc, garantizando un acceso más seguro a los datos y pudiendo realizar cruces entre los datos.

Flexibilidad para personalización, pudiendo diseñar los agentes a medida, con lógica específica para tu negocio o sector. Independencia con respecto a actualizaciones del modelo ‘sin avisar’.

Facilita abordar el desarrollo de soluciones core de negocio sin transmitir a terceros aspectos como los procedimientos propios o datos sensibles, evitando la dependencia ni el pago de licencias especiales.

Adaptarse a modelos más eficientes que salgan a la luz, pudiendo volver en cualquier momento a las soluciones de terceros

Un caso práctico

Interfaz

El equipo interno y los clientes tendrán disponibles **dos canales** independientes desde los que podrán lanzar consultas sobre documentos separados

Clientes desde la web

Interno desde whatsapp (o teams)

Desde **el administrador**, el equipo podrá revisar las consultas que se van realizando al agente para poder extraer estadísticas o tomar medidas.

Será también un punto de entrada para incorporar nueva documentación

Se podrán configurar múltiples aspectos de los chats, como el tono, o el número de palabras por respuesta, entre otras

Se puede sincronizar con herramientas como Sharepoint o Drive, o proporcionar un entorno independiente y seguro dentro del ecosistema

IA

Con un enfoque multi-idioma y un tono amigable para usuarios no técnicos

Se alimenta de la documentación e información incorporada al gestor documental

ESKERRIK ASKO

Cámara Gipuzkoako Ganbera
GRUPO spri TALDEA
EUSKO JAURLARITZA GOBIERNO VASCO
INDUSTRIA, TRANTSIZIO ENERGETIKO ETA JASANGARRITASUN SAILA
DEPARTAMENTO DE INDUSTRIA, TRANSICIÓN ENERGÉTICA Y SOSTENIBILIDAD
spri ENPRESA DIGITALA