

Programa

DÍA 2

09:15 – 10:00 **EL USO DE LA INTELIGENCIA ARTIFICIAL EN EL CAMPO DE LA PREVENCIÓN DE RIESGOS LABORALES.**

Ruben Rodriguez Elizalde. Director del Máster en PRL de la Universitat Oberta de Catalunya.

10:00-11:00: **QUE NUEVOS RIESGOS LABORALES PUEDEN HACERSE PRESENTES COMO CONSECUENCIA DEL USO DE LA IA EN UNA EMPRESA.**

Mesa Redonda:

- 1) Endika Montes Garro. Responsable PRL- áreas corporativas del Servicio de Prevención de Iberdrola.
- 2) Jorge Arce Marcos. Jefe de Seguridad y Medio Ambiente del Servicio de Prevención de la Autoridad Portuaria de Bilbao.
- 3) Representante del Servicio de Prevención de IMQ Prevención.
- 4) M^a Nieves de la Peña Loroño. Responsable de Área de Osalan en el Centro de Bizkaia y coordinadora de la Mesa.

10:45 – 11:45: **OPORTUNIDAD DE MEJORA EN EL ÁMBITO DE LA PREVENCIÓN, EL USO DE LA INTELIGENCIA ARTIFICIAL.**

Mesa Redonda:










- 1) Juan Ramón Muñoz Santos, responsable del Centro Territorial de Osalan en Álava y coordinador de la Mesa.
- 2) Paula Herraiz Lorenzo. Técnica Superior en PRL, Centro Nacional de Nuevas Tecnologías, Instituto Nacional de la Seguridad y Salud en el Trabajo.
- 3) Noelia Aragon Garcia, responsable del servicio de salud laboral del Gobierno de la Rioja.

11:45-12:15: **CAFÉ.**

12:15-12:45: **TURNO DE PREGUNTAS.**

12:45–1:15: **CONCLUSIONES Y CLAUSURA DEL CURSO.**

1. ¿QUE ES LA INTELIGENCIA ARTIFICIAL?

-  **Móviles y asistentes:** Siri, Alexa, Cámaras inteligentes y Teclado predictivo.
-  **Compras:** Recomendaciones de Amazon, Zalando y Publicidad personalizada.
-  **Entretenimiento:** Recomendaciones en Netflix, Spotify y YouTube.
-  **Movilidad:** Rutas inteligentes Google Maps , Sistemas de ayuda a la conducción
-  **Texto y lenguaje:** Traducciones, Chatbots como ChatGPT, Gemini, Copilot
-  **Banca y seguridad:** Detectores de fraude y Asistentes virtuales bancarios
-  **Salud:** Relojes inteligentes: ritmo cardiaco, caídas, IA diagnóstico por imagen
-  **Hogar inteligente:** Termostatos, luces y Robots aspiradores inteligentes
-  **Ciberseguridad:** Filtros de spam y Detectores de phishing



1. ¿QUE ES LA INTELIGENCIA ARTIFICIAL?

¿Qué es la Inteligencia Artificial (IA)?

La IA es la capacidad de las máquinas para imitar comportamientos humanos como aprender, razonar, tomar decisiones o resolver problemas.

Se basa en programas que analizan datos y actúan de forma autónoma o asistida.



1. ¿QUE ES LA INTELIGENCIA ARTIFICIAL?

Según su capacidad funcional

a) IA débil o estrecha (Narrow AI)

- Diseñada para una sola tarea específica (ej. traducir, reconocer caras, etc.).
- No tiene consciencia ni comprensión general.
- Ejemplos: Siri, ChatGPT, Google Translate, DeepL.

b) IA general (AGI – Artificial General Intelligence)

- Sería capaz de realizar cualquier tarea intelectual humana, con flexibilidad y aprendizaje autónomo.
- A día de hoy no existe realmente.
- Meta teórica de muchos laboratorios de IA.



c) IA superinteligente

- Futuro hipotético en el que la IA supera la inteligencia humana en todos los aspectos (creatividad, emociones, estrategia).
- Tema más filosófico/ético que técnico por ahora.

1. ¿QUE ES LA INTELIGENCIA ARTIFICIAL?

Según su nivel técnico y estructura interna

a) IA basada en reglas (sistemas expertos)

- Usa reglas lógicas programadas manualmente del tipo “SI... ENTONCES...”.
- Muy útil en diagnósticos, normativa, asistencia jurídica.
- Limitada: no aprende por sí sola.

b) IA basada en aprendizaje automático (Machine Learning)

- Aprende a partir de datos, no de reglas fijas.
- Detecta patrones y hace predicciones.
Dentro del ML se distinguen:
 - **Aprendizaje supervisado** (con ejemplos etiquetados)
 - **Aprendizaje no supervisado** (descubre patrones sin etiquetas)
 - **Aprendizaje por refuerzo** (aprende por ensayo y error, como AlphaGo)



c) IA basada en redes neuronales / Deep Learning

- Subtipo de Machine Learning, simula el cerebro humano usando capas de neuronas.
- Muy potente en imágenes, lenguaje, audio, etc.
- Ejemplos: ChatGPT, GPT-4, Gemini, sistemas de visión en coches autónomos.

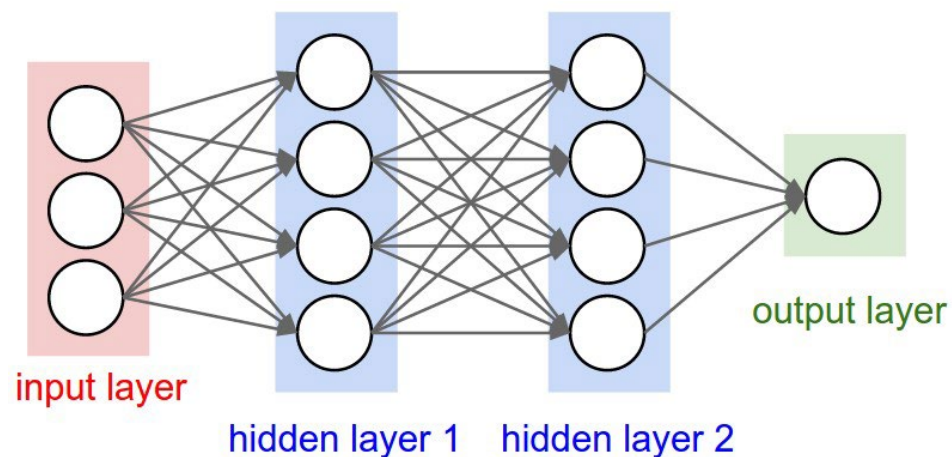
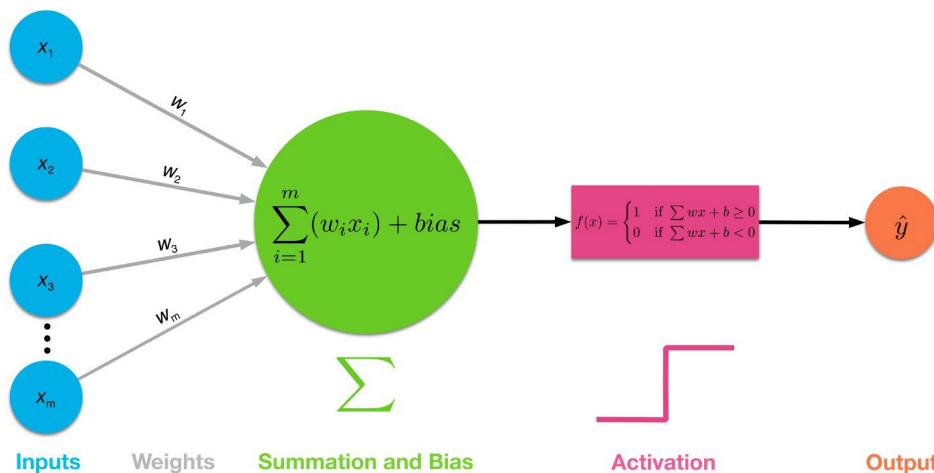
¿QUE ES UNA RED NEURONAL?

- Texto o imagen se traduce a datos numéricos → vectores o matrices. Estos datos se introducen en un software (modelo):
red de funciones matemáticas (neuronas) conectadas con pesos numéricos.
- Por sucesivas capas neuronales, el modelo ajusta funciones y pesos para obtener otros datos numéricos más próximos al resultado deseado.
- El sistema compara salida obtenida con resultado correcto, y si hay error, ajusta pesos para mejorar en siguiente iteración. Así, aprende.
- Al fin, se obtiene un resultado que representa la opción con mayor probabilidad de coincidir con realidad buscada (ej: reconocer un objeto o traducir una frase).
- Todo este conjunto de funciones, pesos y reglas de aprendizaje forma lo que llamamos red neuronal artificial.



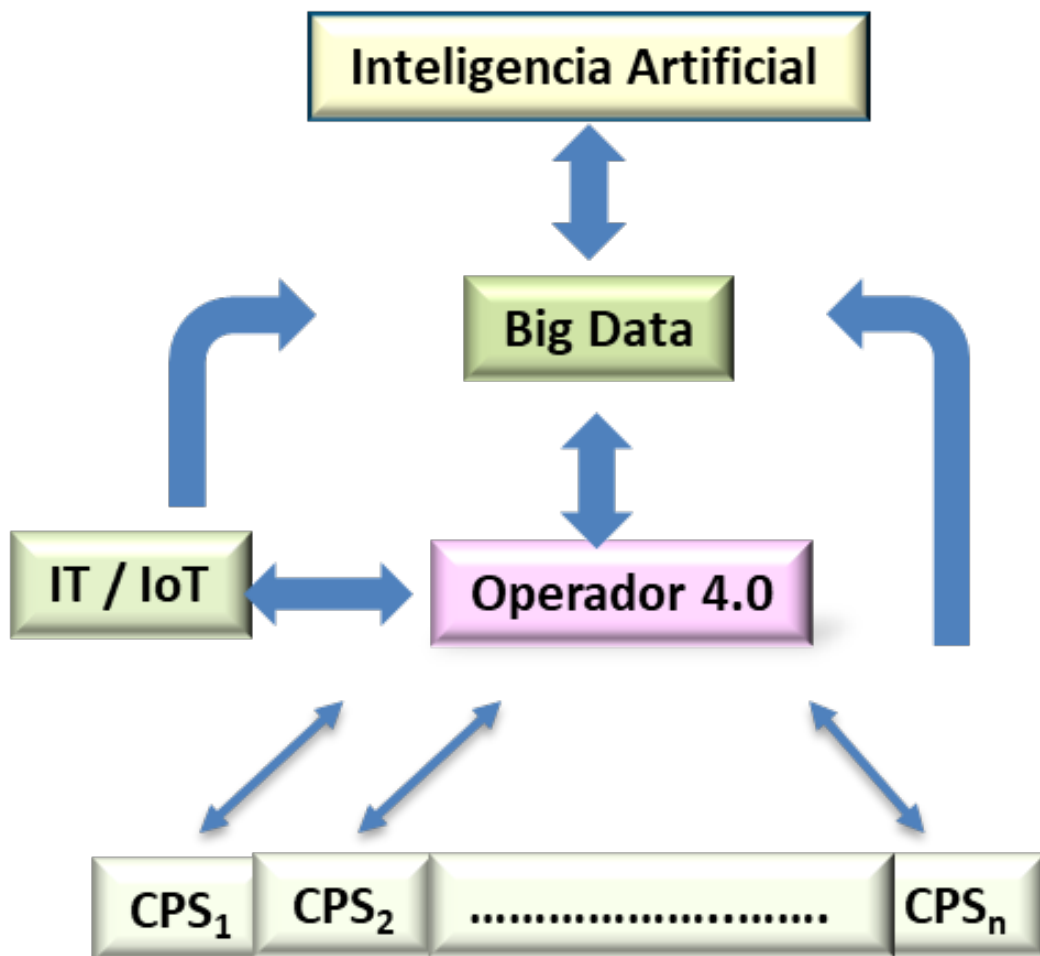
1. ¿QUE ES LA INTELIGENCIA ARTIFICIAL?

ELEMENTO SIMULADO	REPRESENTACIÓN FÍSICA REAL
Neurona artificial	Una función matemática en código
Conexiones (pesos)	Números guardados en matrices
Red neuronal	Programa ejecutado en chips (GPU, CPU, TPU)
Aprendizaje	Ajuste de valores matemáticos mediante cálculos

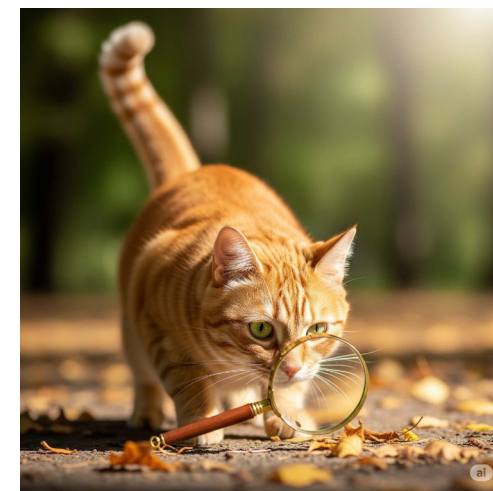


Stanford course [CS231n Convolutional Neural Networks for Visual Recognition](#)

Operador 4.0 en Lugares de Trabajo inteligentes



- ✓ CPS: Cyber Physical System
- ✓ IT: Tecnologías de la Información
- ✓ IoT: Internet de las cosas
- ✓ HCPS: Human – Cyber Physical System



2. IA & PRL

PILARES TECNOLÓGICOS	Tecnologías		Casos
1. Datos (Big Data)	“La consultora ACME (...) para diseñar sensores e implantarlos en ropa, cascos y gafas especiales y monitorizar a los operarios. A través de big data y la gestión masiva de datos, recopilan, analizan e interpretan grandes cantidades de información sobre su trabajo”.		
2. Captación	Sensórica	Covid	
	Wearable	Gestión del estrés (pulseras actividad), Sensor colocado en gorra busca señal de fatiga.	
	Geolocalización	App's y localización vehículos flota	
	Visión artificial	Aplicaciones anti-intrusismo, Covid, ETC.	
3. Almacenamiento	Cloud storage	Google, MS, etc.	
	Gemelo digital	Software gestión de maquinaria	
4. Comunicación (ICT)	IoT / Rfid	Detector gases, radiación ultravioleta, gestión epi's, gestión acceso y mando máquinas, etc.	
	5G	Apps con requisitos de baja “latencia” y alto “ancho de banda”.	
	Realidad aumentada	Mantenimiento 4.0	
	Realidad virtual	Formación	
5. Data analytics	Inteligencia artificial (machine learning)	Software que “toma decisiones” en tiempo real en materia de PRL	
	Computación en la nube	Software de PRL de gestión delegada	
	Análisis semántico textos	Software introducción masiva datos: coordinación actividades, vigilancia salud, etc.	
	Gaming	Formación	
6. CPS	App's	Play store	
	Robótica (cobot)	Alimentador CNC, Pick & place y despaletizado	
	Exoesqueletos	Guía de exoesqueletos en PRL	
	Smart epi's	Anulación activa de ruido, chalecos anticaídas, ...	
	Conducción autónoma	Carretillas elevadoras automatizadas	

2. IA & PRL

Desafíos Legales

Pilares	Tecnologías		Casos	Claves	Legislación	Normativa	Nivel de riesgo legal	
1. Datos (Big Data)	“La consultora ACME (...) para diseñar sensores e implantarlos en ropa, cascos y gafas especiales y monitorizar a operarios. A través de big data y gestión masiva de datos, recopilan, analizan e interpretan grandes cantidades de información sobre su trabajo”.			Ciberseguridad Privacidad / know-how Territorialidad	LOPD / Reglamento (UE) 2016/679 de protección de datos Delegado de protección de datos (DPO)		Medio	
2. Captación	Sensórica	Covid						Medio
	Wearable	Gestión del estrés (pulseras de actividad). Sensor colocado en gorra busca señal de fatiga.						
	Geolocalización	App’s y localización vehículos flota						
3. Almacenamiento	Visión artificial	Aplicaciones anti-intrusismo, Covid, etc.						
	Cloud storage	Google, MS, etc.					Alto	
4. Comunicación (ICT)	Gemelo digital	Software gestión de maquinaria						
	IoT / Rfid	Detectores de gases, radiación ultravioleta, gestión de epi’s, gestión de accesos y mando sobre máquinas, etc.		Ciberseguridad versus interoperabilidad Privacidad Intermediarios	COM (2009) 278		Bajo	
5G	Aplicaciones con requisitos de baja “latencia” y/o alto “ancho de banda”.							
Realidad aumentada	Mantenimiento 4.0							
5. Data analytics	Realidad virtual	Formación						
	Inteligencia artificial (machine learning)	Software que “toma decisiones” en tiempo real en materia de PRL			Comunicación Comisión Europea		Medio	
	Computación en la nube	Software de PRL de gestión delegada		Ciberseguridad Territorialidad				
	Análisis semántico de textos	Software de introducción masiva de datos: coordinación actividades, vigilancia salud, etc.						
	Gaming	Formación						
App’s	Play store							
6. CPS	Robótica (cobot)	Alimentador CNC Pick & place y Despaletizado			Resolución Parlamento Europeo (2017)	ISO / TS	Alto	
	Exoesqueletos	Guía de exoesqueletos en PRL			Directiva Máquinas Reglamento Epi’s Dir. Productos Sanitarios			
	Smart epi’s	Anulación activa de ruido, chalecos anticaídas, ...			Reglamento Epi’s			
	Conducción autónoma	Carretillas elevadoras automatizadas			Directivas de Máquinas Dir. vehículos a motor			

3. Cumplimiento normativo



Resumen de los principales reglamentos europeos relacionados con la IA

Reglamento	Ámbito principal	Tipo de norma	Obligaciones clave	Aplicación
AI Act (Reglamento de IA)	Uso y desarrollo de sistemas IA	Obligatorio	Clasificación por riesgo, requisitos técnicos, EIPD, supervisión humana	Desde 2025–26
Cybersecurity Act	Certificación ciberseguridad TIC	Voluntario	Crea esquemas de certificación comunes (EUCC) para TIC	Desde 2019
Cyber Resilience Act (CRA)	Seguridad obligatoria: productos con componentes digitales	Obligatorio	Seguridad por diseño, parches, gestión de vulnerabilidades, notificación de incidentes	Desde 2027
RGPD (Rgto General de Protección de Datos)	Protección de datos personales	Obligatorio	Consentimiento, transparencia, derechos interesado, seguridad, EIPD	Desde 2018

Comentario final:

- El **AI Act** regula cómo debe desarrollarse y usarse la IA según riesgo que implica.
- El **Cybersecurity Act** es un marco de certificación voluntaria para mejorar la confianza.
- El **Cyber Resilience Act** impone requisitos obligatorios de ciberseguridad por diseño a todos los productos digitales.
- El **RGPD** protege datos personales y se aplica a cualquier sistema que los trate, incluyendo IA.

3. Cumplimiento normativo

¿QUÉ DEBE HACER UNA EMPRESA PARA RESPETAR EL RGPD? (1 de 2)

1. Informar con transparencia

- Incluir una política de privacidad clara en su web o documentos.
- Indicar qué datos recoge, para qué los usa, cuánto tiempo y con qué base legal.
- Identificar al responsable del tratamiento y cómo contactar con él.

2. Recoger datos de forma legal

- Solo tratar datos si tiene una base legal válida de Consentimiento, de Contrato, de Obligación legal, de Interés legítimo, etc.
- Consentimiento expreso y verificable si necesario (newsletters o análisis de datos).

3. Respetar los derechos de las personas

- Permitir que cualquier persona pueda: Acceder a sus datos, Rectificarlos, Borrarlos (derecho al olvido), Oponerse a su uso o Solicitar una copia (portabilidad).

4. Aplicar medidas de seguridad

- Proteger los datos frente a accesos no autorizados, pérdidas o filtraciones.
- Cifrar, controlar accesos, hacer copias de seguridad y formar al personal.



3. Cumplimiento normativo

¿QUÉ DEBE HACER UNA EMPRESA PARA RESPETAR EL RGPD? (2 de 2)

5. Registrar los tratamientos

- Llevar un registro de actividades de tratamiento (obligatorio salvo para empresas muy pequeñas sin riesgo).
- Describir qué datos se tratan, con qué finalidad, a quién se ceden, etc.

6. Evaluar riesgos

- Hacer una Evaluación de Impacto (EIPD) cuando se traten datos sensibles o haya riesgo alto (ej. IA, vigilancia, salud).
- Consultar a la autoridad de protección de datos si hay dudas.

7. Designar un Delegado de Protección de Datos (DPO)

- Obligatorio en organismos públicos o si se tratan datos sensibles de forma habitual.
- También recomendable en empresas medianas o grandes.

8. Gestionar brechas de seguridad

- Notificar en 72 horas a la AEPD cualquier filtración o acceso indebido a datos personales.
- Comunicarlo también a los afectados si hay riesgo.



3. Cumplimiento normativo

OBLIGACIONES DEL RGPD

1. Registro de actividades de tratamiento
2. Análisis de riesgos
3. Evaluación de impacto (EIPD)
4. Nombramiento de un Delegado de protección de datos

3. Cumplimiento normativo

ÓRGANO	ÁMBITO	FUNCIÓN PRINCIPAL
EDPB	Todos los Estados miembros	Coordina y asegura una aplicación homogénea del RGPD. Emite directrices y decisiones vinculantes.
EDPS	Instituciones europeas	Supervisa el tratamiento de datos dentro de las propias instituciones de la UE, y asesora legalmente.



RECOMENDACIONES O GUIAS DE LA EDPB

1. Informe del “ChatGPT Taskforce” (mayo 2024)

El EDPB creó un grupo de trabajo específico para evaluar ChatGPT, publicando un informe preliminar el **23 -05-24**:

- **Transparencia:** OpenAI debe informar claramente a los usuarios sobre cómo se usan sus datos, especialmente si se emplean para entrenar los modelos.
 - **Precisión:** informar sobre limitaciones del modelo y su característica probabilística — capacidad de generar información imprecisa— .
 - **Derechos de los interesados:** facilitar el acceso, rectificación y borrado de datos personales
- El informe incluye un **cuestionario en su anexo**, diseñado para que las autoridades supervisen a OpenAI.

2. Opinión 28/2024 sobre modelos de IA (diciembre 2024)

No es específica de ChatGPT, pero sí abarca su categoría (modelos de lenguaje):

- **¿Cuando un modelo es “anónimo”?** Solo si es muy improbable (con medios razonablemente accesibles) que pueda extraer datos personales identificables.
- **Legitimación jurídica:** se permite que se base en el “interés legítimo”, siempre que sea necesario, proporcional y exista un equilibrado de derechos .
- **Procesamiento ilícito:** si el modelo usó datos ilegales en su entrenamiento, no puede valer su uso salvo que haya sido despersonalizado efectivamente .
- Se enfatiza la **responsabilidad documental** (accountability), la protección por diseño y por defecto (erga omnes las etapas de desarrollo y despliegue), y una **evaluación del impacto (DPIA)** si hay alto riesgo.

3. Documento de apoyo: ciclo de vida y herramientas de auditoría

El **informe del Taskforce** también ofrece un análisis del ciclo de vida de sistemas de IA, que abarca:

Se espera que este contenido se haga público en GitHub bajo licencia open-source, facilitando la colaboración comunitaria

3. Cumplimiento normativo

Resumen práctico

El EDPB no ha publicado una “guía ChatGPT” específica pero sí:

1. Un **informe del Taskforce**, con recomendaciones directas para OpenAI.
2. La **Opinión 28/2024**, aplicable a cualquier modelo de IA, incluido ChatGPT.
3. Un enfoque claro en:
 - Transparencia
 - Derechos de los usuarios
 - Anonimización efectiva
 - Base legal como el “interés legítimo”
 - Evaluación de impacto y protección por diseño



Etapa	Contenido destacado
Desarrollo	Buenas prácticas de codificación, entornos seguros y pruebas edpb.europa.eu
Despliegue	Monitorización, sostenibilidad y desactivación segura
Auditoría	Listas de verificación (checklists) para revisiones técnicas y legales

3. Cumplimiento normativo

LA AEPD PUBLICA RECOMENDACIONES SOBRE CHATBOTS IA

Infografía titulada *“Recomendaciones para usuarios en la utilización de chatbots con inteligencia artificial”*:

- Verificar **política privacidad** y **aviso legal**, que incluyan la identificación del responsable, referencia al RGPD, canales para ejercer derechos y explicaciones sobre si el chatbot sigue aprendiendo con las conversaciones.
- **No facilitar datos innecesarios**, rechazar solicitudes de información sin propósito claro, y asegurarse de que se pueda retirar consentimiento en cualquier momento .
- Limitar los datos personales que se comparten, no proporcionar información de terceros sin autorización, y ser conscientes de que el chatbot puede generar contenido incorrecto o engañoso,
- En caso de menores, **no permitir su uso sin supervisión adulta**



3. Cumplimiento normativo

AUTORIDAD VASCA PROTECCIÓN DE DATOS (AVPD) SE POSICIONA SOBRE USO RESPONSABLE DE IA (HERRAMIENTAS COMO CHATGPT)



1. Promoción del modelo catalán FRIA para la IA

El 5-6-25, la AVPD firmó un acuerdo con la Autoridad Catalana de Protección de Datos (APDCAT) para implementar en Euskadi el modelo FRIA —*Evaluación de Impactos en Derechos Fundamentales* para sistemas de IA.

Debe aplicarse obligatoriamente a desarrollos de IA que impongan riesgos, conforme al Reglamento de Inteligencia Artificial, permitiendo evaluaciones y mitigación de riesgos previas a su uso

2. Responsabilidad preventiva y normativa

La AVPD, al igual que la APDCAT, actúa como autoridad supervisora para asegurar el cumplimiento de la normativa de protección de datos en todos los ámbitos, incluyendo la IA:

- Fomentar que las empresas e instituciones realicen evaluaciones FRIA en proyectos de IA con alto impacto.
- Emitir recomendaciones, formación y directrices buenas prácticas para sector vasco

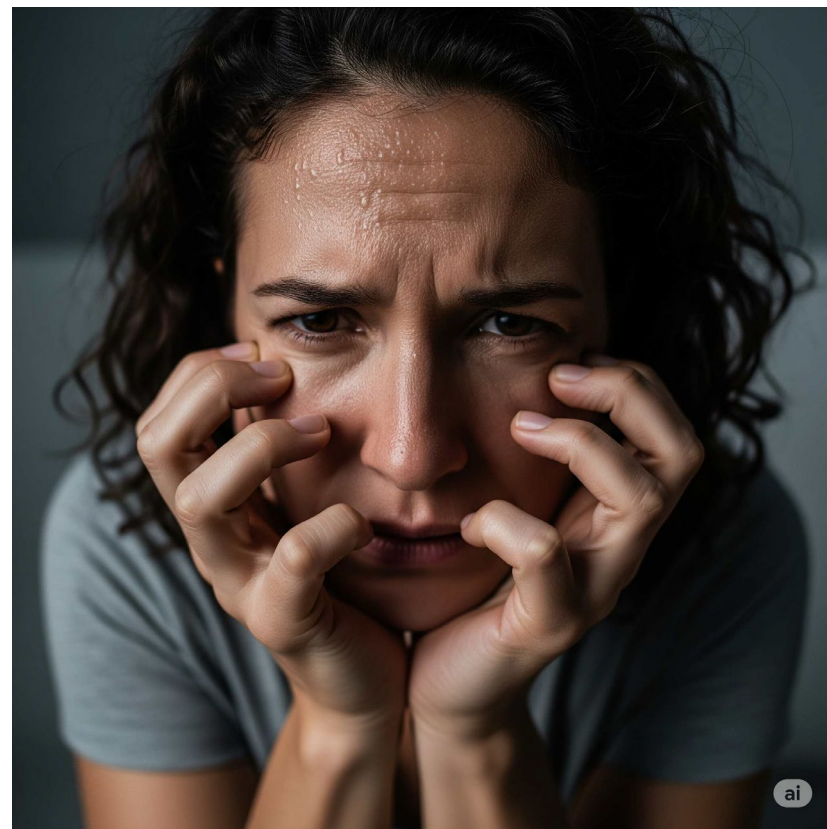
3. Cumplimiento normativo

1.- Brecha de seguridad datos especialmente protegidos.

2.- Sesgo por entrenamiento del modelo: racial, género, legal, etc.

3.- Servidores extracomunitarios.

4.- Inexactitud: respuesta más probable.







4. RECOMENDACIONES CHATBOTS

Chatbot / Plataforma	Versión	Riesgo estimado 	¿Almacena fuera de la UE? 	¿Usa tus datos para entrenar? 	¿Permite evitarlo? 	Precauciones necesarias
ChatGPT (Gratuito / Plus)	Gratuita / Plus	Alto	Sí (EE. UU.)	Sí, por defecto	Parcial (requiere ajuste manual)	No apto sin contrato + residencia UE
ChatGPT Enterprise / Edu	Pago institucional	Bajo	No (residencia UE disponible)	No	Sí (por defecto)	EIPD + contrato art. 28 + uso restringido
Microsoft Copilot (Word, Outlook, etc)	Entra ID / Workspace	Bajo	No (datos permanecen en tenant)	No	Sí	Solo con Entra ID + EIPD interna
Microsoft Copilot (versión web gratis)	Gratuita	Medio-Alto	Sí	Sí	No configurable	Evitar datos sensibles + no usar cuenta personal
Gemini (cuenta personal)	Gratuita / Google One	Alto	Sí	Sí, salvo que se desactive	Parcial (opcional en configuración)	No apto sin entorno controlado
Gemini Workspace (empresa / edu)	Pago	Bajo	No (residencia UE)	No	Sí	EIPD + cuenta corporativa + contrato DPA
Claude (Anthropic)	Gratuita / Pago	Alto	Sí (EE. UU.)	Sí	Parcial (solo Claude Team)	No apto sin garantías UE
DeepSeek	Gratuita	Máximo	Sí (China)	Sí, sin opción de exclusión	No configurable	Prohibido para datos sensibles


4. RECOMENDACIONES CHATBOTS



Leyenda de riesgos

-  **Bajo:** uso seguro si se cumplen las condiciones del RGPD (contrato, EIPD, datos UE).
-  **Medio:** requiere cautela, depende de configuración o entorno (personal vs. corporativo).
-  **Alto:** uso problemático o incompatible con el RGPD sin medidas adicionales.
-  **Prohibido:** no debe usarse en ningún caso para datos sensibles ni por organismos públicos.

5. ¡La pregunta del millón!

 Una Administración Pública / Empresa, que maneje “datos protegidos” (la gran mayoría), ¿puede usar un Chatbot tipo ChatGPT o Gemini?



5. ¡La pregunta del millón!

No, una Administración Pública / Empresa que maneja “datos protegidos” o “especialmente protegidos” —como datos médicos o relativos a accidentes laborales— no puede usar chatbots (como ChatGPT, Gemini, Copilot, etc.) sin aplicar medidas específicas de protección de datos.

De hecho, hacerlo sin precauciones podría vulnerar gravemente el Reglamento General de Protección de Datos (RGPD) y otras normas sectoriales.

¿Por qué no puede hacerlo “sin más”?

1. Datos sensibles = categoría especial

El RGPD (art. 9) considera que los datos de salud, sobre accidentes de trabajo, discapacidad, etc., son categorías especiales y no pueden tratarse salvo en condiciones muy estrictas (base legal, medidas de seguridad reforzadas, confidencialidad, etc.).

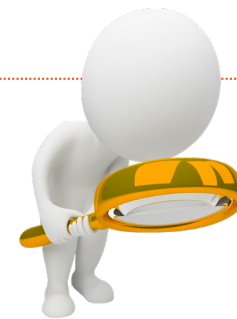
2. Evaluación de Impacto (EIPD / DPIA)

Cualquier tratamiento de datos sensibles mediante sistemas automatizados o IA, como un chatbot:

- Requiere una Evaluación de Impacto relativa a la Protección de Datos (EIPD) antes de su puesta en marcha (art. 35 RGPD).
- Debe incluir: riesgos para los derechos y libertades, medidas de mitigación, principios de minimización, acceso controlado, etc.



5. ¡La pregunta del millón!



3. Prohibido enviar datos fuera del EEE sin garantías

La mayoría de estos chatbots (ChatGPT, Gemini, etc.):

- No garantizan residencia de datos en la UE en sus versiones estándar.
- Pueden transferir datos a EE. UU. u otros países, lo cual requiere cláusulas contractuales tipo o escudo de privacidad válido (actualmente el Data Privacy Framework para EE. UU.).






4. Responsabilidad del responsable del tratamiento

La administración sigue siendo responsable del tratamiento, incluso si usa un tercero (OpenAI, Google, Microsoft...). Debe:

- Verificar si el proveedor actúa como encargado y firmar un contrato conforme al art. 28 RGPD.
- Controlar que no haya tratamiento posterior con fines incompatibles (como el entrenamiento de modelos con los datos).

5. ¡La pregunta del millón!

¿Qué precauciones debe tomar?

Obligación	Requisito
 EIPD obligatoria	Evaluar y documentar riesgos para los derechos de los interesados.
 Medidas técnicas y organizativas	Cifrado, seudonimización, registros de acceso, control de terceros, etc.
 Contrato con el proveedor	El chatbot debe actuar como encargado del tratamiento con contrato art. 28 RGPD.
 Garantías para transferencias internacionales	Solo usar servicios con residencia en la UE o cláusulas legales adecuadas.
 Transparencia y consentimiento	Informar al interesado. En algunos casos, requerir su consentimiento expreso.

En resumen

NO, una administración pública / empresa **no puede** utilizar chatbots con datos sensibles **sin una evaluación jurídica y técnica exhaustiva**.

De hacerlo, se expone a **graves sanciones administrativas** y a posibles vulneraciones de derechos fundamentales de las personas.



6. Posibles soluciones


Existen modelos de IA entrenados que podemos ejecutarlos desde nuestro propio hardware sin conexión a Internet.



Esta práctica se llama **inferencia local** y es muy útil si queremos:

- Garantizar privacidad total (nada sale de nuestro equipo/red).
- Trabajar offline (sin enviar datos a la nube/internet).
- Tener más control sobre el rendimiento o el entorno (entrenamiento continuo del modelo).

Ejemplos de modelos que puedes usar sin conexión

 Modelos de lenguaje (como ChatGPT, pero locales)

 Usan herramientas como **llama.cpp**, **Ollama**, **LM Studio** o **GPT4All GUI** para ejecutarlos localmente.

Modelo	¿Qué hace?	¿Dónde funciona?	Peso aproximado
LLaMA 2 / 3	Texto, preguntas, chat	PC, Linux, Mac (con 8–16 GB RAM)	4 GB a 13 GB
Mistral	Chat, asistencia general	Muy rápido, eficiente	4–7 GB
GPT4All	Interfaz amigable para usuarios	Windows/Linux/macOS	4–8 GB
BLOOMZ, Alpaca, Vicuna, etc.	Modelos de código abierto	Portátiles o servidores	Variable

6. Posibles soluciones



Ventajas de usar modelos locales



Privacidad total: no se envía nada a servidores externos.

Independencia de internet: útil para entornos cerrados o con mala conexión.

Personalización: puedes modificar, afinar o combinar modelos.

6. Posibles soluciones

Criterio	Entorno Abierto (Nube Pública)	Entorno Cerrado (Privado On-Premise)	Entorno Híbrido (Mixto)
Control de datos	Bajo – Datos alojados en servidores de terceros (riesgo de exposición).	Alto – Datos permanecen dentro de la organización.	Medio – Datos sensibles se mantienen locales; otros pueden ir a la nube.
Cumplimiento normativo	Requiere confiar en garantías del proveedor en materia de RGPD, etc. Cumplir soberanía de datos puede ser difícil si servidores fuera del país.	Directo – La empresa implementa sus propias medidas alineadas con la ley. Fácil cumplimiento de estándares internos y europeos	Depende – Debe diseñarse cuidadosamente para que la parte en nube cumpla normativas, mientras la local asegura control sobre datos críticos.
Seguridad y privacidad	Debe evaluarse seguridad del proveedor; riesgo de accesos no autorizados externos. Esencial: Cifrado datos en tránsito y almacenados.	Máxima privacidad – Sin envío de datos a terceros, reduciendo superficie de ataque externa. Se aplica seguridad corporativa al entorno.	Variable – Ofrece mayor seguridad que solo nube, pero introduce complejidad. Necesario robustecer la conexión entre los entornos y vigilar puntos de integración.
Coste inicial (CapEx)	Bajo – Modelo de pago por uso, sin inversión inicial fuerte en hardware.	Alto – Adquisición de servidores, infraestructura y su mantenimiento.	Intermedio – Requiere infraestructura propia, pero menor que un entorno privado.

6. Posibles soluciones

Criterio	Entorno Abierto (Nube Pública)	Entorno Cerrado (Privado On-Premise)	Entorno Híbrido (Mixto)
Coste operativo (OpEx)	Variable – Costes mensuales según uso (pueden escalar con volumen de datos o usuarios).	Estable – Costes fijos de energía, personal técnico, licencias; aprovechamiento pleno tras inversión.	Mixto – Combina pagos por la parte en nube y costos fijos de parte local. Permite optimizar qué cargas van a cada entorno.
Escalabilidad	Muy alta – La nube pública ofrece recursos prácticamente ilimitados bajo demanda.	Limitada – Sujeto a la capacidad del hardware instalado; escalar implica comprar más equipos.	Alta – La porción en nube puede escalar para picos de trabajo, mientras la local maneja la carga base.
Flexibilidad y personalización	Amplia oferta de servicios pre-entrenados y htas del proveedor, pero menos personalización del entorno.	Total – Se puede personalizar la solución de IA al 100% (modelos, configuraciones) y adaptarla a procesos internos.	Moderada – Posibilita usar servicios cloud estándar para ciertas tareas y soluciones a medida en local para otras.
Ejemplos de uso	Empresas que utilizan APIs de IA públicas (ej.: servicio de reconocimiento de imágenes en la nube) o chatbots generales en la web pública. Rápido despliegue de pilotos con mínima inversión.	Sectores sanitarios que procesan datos sensibles (historiales médicos) suelen optar por IA en entornos cerrados para garantizar confidencialidad También organizaciones con política estricta de seguridad.	Organizaciones que requieren cumplir regulaciones pero quieren beneficios de la nube: ej. hospital que analiza datos clínicos localmente (para privacidad) pero usa la nube para entrenar modelos complejos con dato anonimizado.

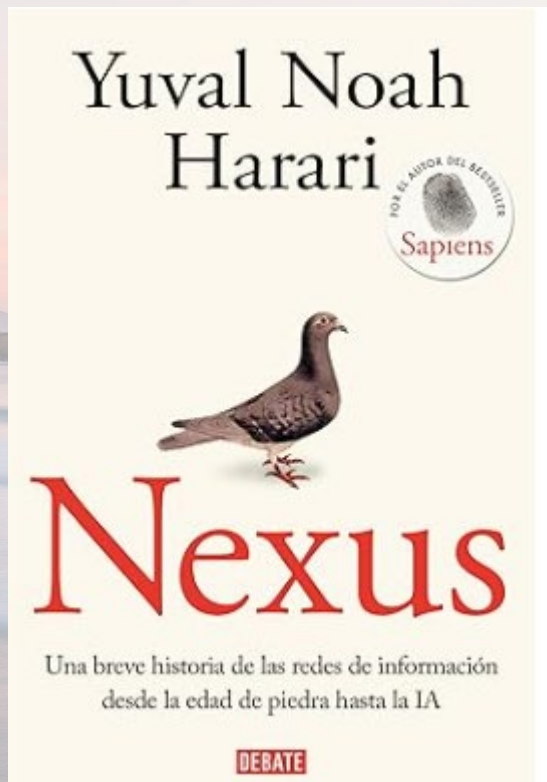
7. Conclusiones

En conclusión, la IA aplicada a la PRL abre un panorama prometedor tanto para el sector privado, como para el público, proporcionando entornos más seguros, decisiones más informadas y actuaciones más eficaces y eficientes.

Para materializar ese potencial, las organizaciones deben:

- **actuar con rigurosidad y anticipación**
- **formarse en las nuevas tecnologías**
- **fortalecer sus marcos de cumplimiento normativo**
- **involucrar a expertos legales y de ciberseguridad en los proyectos de IA**
- **fomentar una cultura en la que la colaboración entre humanos e IA sea armónica**

Solo así la “inteligencia” de las máquinas se traducirá en mejor prevención y protección de la Seguridad y Salud Laboral.



Eskerrik asko

OSALAN SERVICIOS CENTRALES

Camino de la Dinamita s/n (Monte Basatxu)
48903 Cruces-Barakaldo (Bizkaia)



94.403.21.90



94.403.21.00



osalansc@ej-gv.es

OSALAN ZERBITZU OROKORRAK

Dinamita bidea, z/g (Basatxu mendia)
48903 Gurutzeta-Barakaldo (Bizkaia)



OSALAN

Laneko Segurtasun eta
Osasunerako Euskal Erakundea
Instituto Vasco de
Seguridad y Salud Laborales



EUSKO JAURLARITZA
GOBIERNO VASCO