



ecix
be tech, be reg

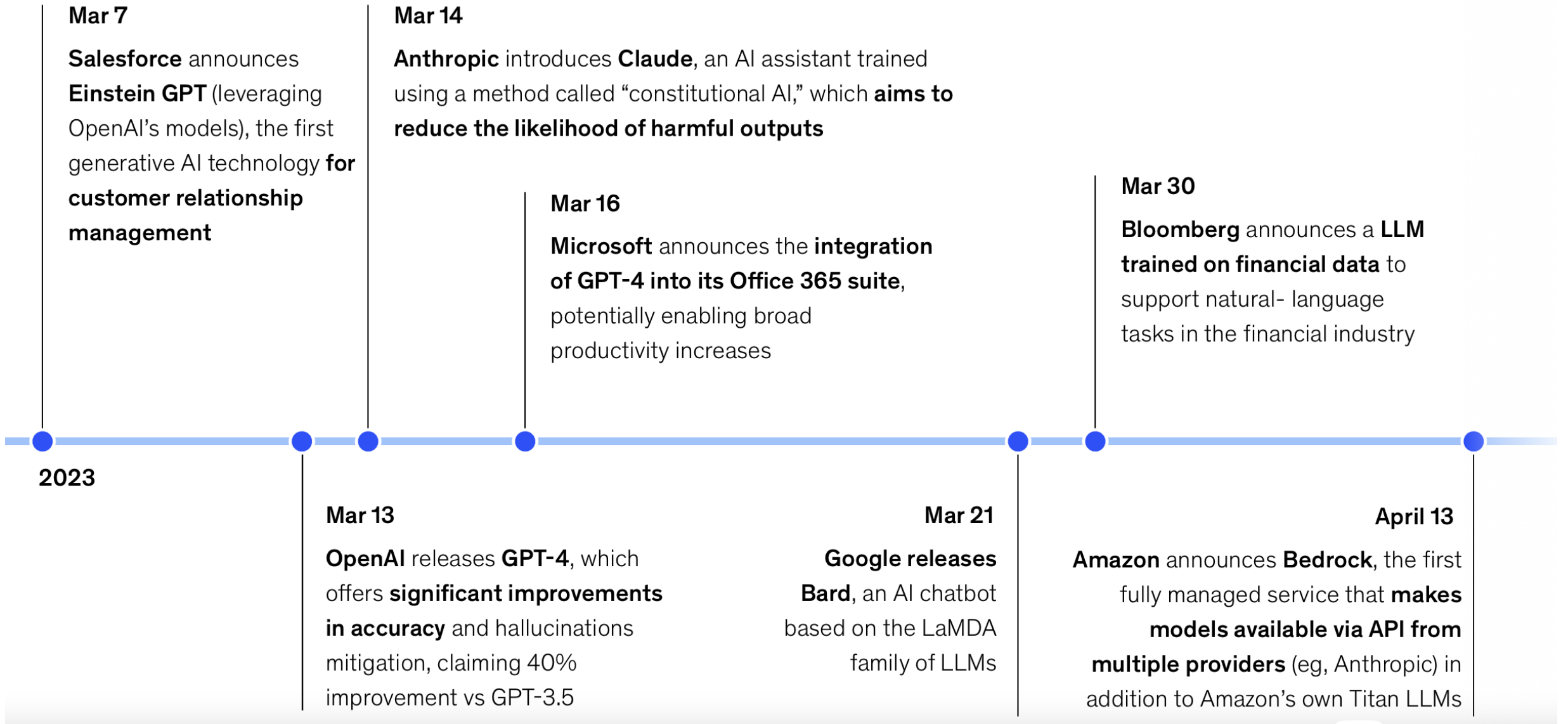
El Cibercompliance y los riesgos del uso de la IA en la empresa

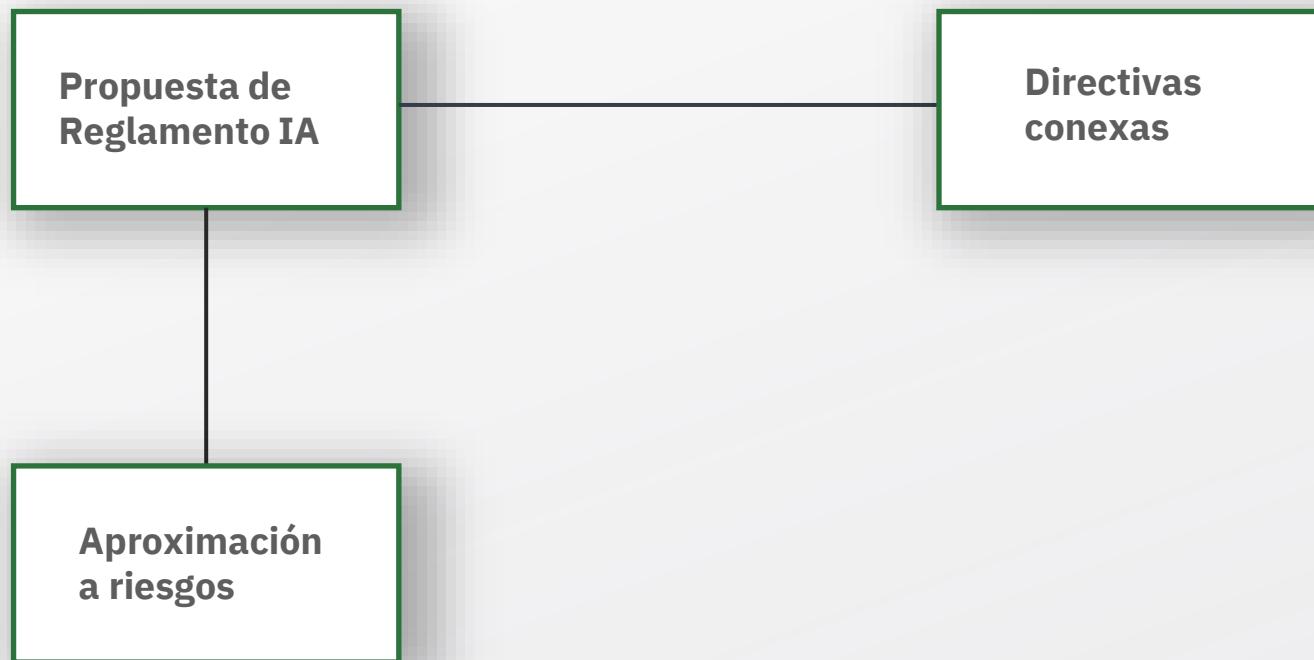
Francisco Pérez Bes
Socio Derecho Digital
Ecix Tech

Usos de la Inteligencia artificial en empresas

Función	Área afectada	Solución de IA
Traducción de documentos	Internacional	DeepL
Transcripción de reuniones	Secretaría del Consejo	Whisper
Creatividades	Marketing	Gen2
Presentaciones	Todas	Canva, Slidebot
Verificación de contenidos	Jurídico	GPTZero
Redacción de documentos	Todas	ChatGPT / Claude
Asistente virtual	Administrativa	HeyPi
Análisis de ventas	Ventas	Bloom AI
Investigación académica	I+D+i	LLaMa
Gestión de Excel	Financiero	PowerExcelAI
Generación de código	IT	Palm
Revisión legal documentos	Jurídico	MiA

La dificultad de regular la IA





"ChatGPT may offer inaccurate information about people, places, or facts".

- Riesgo de falta de veracidad de la fuente.
- Toma de decisiones empresariales sobre información falsa.
- Responsabilidad de la empresa de verificar contenidos.

Ejemplos: antecedentes penales de Alcalde australiano. Credenciales de profesor condenado por abuso sexual. Jurisprudencia falsa en juicio.

Los empleados pueden subir contenido confidencial y secreta de la empresa.

Impacto en la responsabilidad del empleado y de la empresa.

Ejemplo: Empleados de Samsung filtran código confidencial y la empresa prohíbe ChatGPT

Riesgo de revelación ilícita de información personal de terceros sin su autorización ni conocimiento.

Ejemplo: uso de gestores de buzones de correo corporativo.

- La autoridad de control italiana prohibió el uso de ChatGPT por considerar que no cumplía con las exigencias legales.
- La AEPD ha anunciado una acción coordinada con autoridades de control de Iberoamérica para abordar las cuestiones que afecten a la privacidad.

- En marzo de 2023, **openIA sufría una brecha de seguridad** provocada por un bug en sus sistemas, que expuso información confidencial propia y de terceros.
- INCIBE alerta del uso de herramientas de generación de textos para optimizar los ataques de **ingeniería social**.
- Expertos en ciberseguridad alertan del riesgo que asumen las empresas por la **descarga** de sus empleados de aplicaciones y herramientas supuestamente basadas en IA, o extensiones del navegador con falsas promesas acerca de sus funcionalidades.

- Riesgo por usar herramientas que no garantizan el respeto por los derechos de **propiedad intelectual** (caso Rapero Drake o Dall-e).
- Oportunidad de proteger intangibles: el caso de marca JP Morgan
- En un eventual uso en la **actividad publicitaria**, podrían generarse mensajes comerciales ilícitos.



- Cumplir con la normativa aplicable a la protección de los **consumidores** (nacional y autonómica), especialmente los vulnerables. Pe. derecho de información.
- Actividades **promocionales** (LOCM).
- Problema de **reseñas** falsas (LCD).
- Prácticas **discriminatorias** del algoritmo sobre un grupo de consumidores.

- La IA puede tomar decisiones autónomas con impacto en el mercado (caso Glovo Italia).
- Riesgo de **prácticas colusorias** entre algoritmos.
- Acuerdos que impidan, restrinjan o falseen la competencia en el mercado.
- En situaciones de **posición dominante**, el uso de algoritmos puede resultar una barrera de entrada.

- Agilizar procesos: contratación, promoción o despido.
- Decisiones basadas en análisis con procesamiento automatizado de datos.
- Impacto en los derechos de las personas: proceso legal, justo y no discriminatorio.
- Control de los empleados.



- IA generativa para **influir en las creencias, emociones y comportamientos** de las personas (chatbots).
- Riesgo de que las personas confíen en las máquinas creyendo que son imparciales o neutrales.
- ChatGPT no se rige por principios éticos.
- Estas herramientas arrastran **sesgos cognitivos**.





- Generar actas de reuniones, transcribir reuniones con **acuerdos societarios** confidenciales.
- Delito de revelación de **información privilegiada**.
- Impacto en temas de **ESG**.

Recomendaciones y buenas prácticas



be tech, be reg

ecix.tech

Madrid

C/Lagasca, 88 7º Planta
28001 Madrid
(+34) 91 001 67 67

Barcelona

Avenida Diagonal, 427 bis – 429
08036 Barcelona
(+34) 93 807 48 50