

ESPECIAL

“Diario de una Tortuga Ninja”

DE Tecnología & Sentido Común



ESPECIAL

AGOSTO
2025

Arquitectura
de Inteligencia
Artificial. Los
cimientos del
futuro digital

08

NIS2 para
directivos:
claves y
desafíos

12

IA generativa y
ciberguerra: la
nueva frontera

16

IA generativa
corporativa: una
revolución
silenciosa más
allá de la nube

20

ALTAI: la guía de
evaluación para una
IA confiable según la
Comisión Europea

24

Europa y la
ciberseguridad de
hospitales:
protegiendo
vidas y datos.

28

Europa y su
compromiso
con el futuro
y la IA

32

¿Por qué un
Espacio Europeo
de Datos
de Salud?

36

IA y Salud: lo que
nos está costando
ver (y resolver)

40

Todo a la vez en
todas partes...
¿y sin control?:
la amenaza de la
IA ubicua

44

El problema
de los tres
cuerpos:
¿hacia dónde
orbitará la IA?

48

ESPECIAL

“Diario de una Tortuga Ninja”

DE **Tecnología & Sentido Común**



EQUIPO TYSC

Javier Peris - El Gubernauta

Manuel Serrat - Futuro y Seguridad

Nacho Alamillo - Tecnoregulación en Prospectiva

Juan Carlos Muria - Diario de una Tortuga Ninja

Marlon Molina - Es Tendencia

Ricard Martínez - Ojo Al Dato

Marcos Navarro - Ai Futuro

Víctor Almonacid - La Nueva Administración

Alex Aliaga - Radio Security

Marta Martín - Mentas Divergentes



JUAN CARLOS MURIA TARAZON

Licenciado en Informática y Doctor Cum Laude en Organización de Empresas por la Universidad Politécnica de Valencia (UPV). Con acreditación en Gestión de Datos para Investigación Clínica, es miembro de la Junta Directiva de la Asociación Valenciana de Informáticos de Sanidad, auditor CISA, CGEIT y está certificado en ITIL, COBIT 5 y PRINCE 2.

Con más de 20 años de experiencia en el sector de la salud, ha dirigido proyectos de interoperabilidad, seguridad y big data, y ha sido profesor de marketing digital, big data e inteligencia de negocio. Actualmente es profesor de Organización de Empresas en la UPV y consultor independiente.

LinkedIn:

<https://www.linkedin.com/in/jcmuria/>

Twitter:

<https://twitter.com/juancarlosmt>

PUBLICIDAD Y CONTRATACIÓN

Carmen Usagre

carmen.usagre@businessandcompany.com

Teléfono: +34 96 109 44 44

GABINETE JURÍDICO

Jesús López Peláz

ATENCIÓN AL LECTOR

soluciones@businessandcompany.com

EDITA

Business, Technology & Best Practices, S.L.

Av. San Onofre, 20

46930-Quart de Poblet (Valencia)

Teléfono: 96 109 44 44

Fax: 96 109 44 45

<https://tecnologiaysentidocomun.com>

soluciones@businessandcompany.com

(Business&Co.®) Business, Technology & Best Practices, S.L. en ningún caso y bajo ningún supuesto se hace responsable de las opiniones aquí expresadas por sus colaboradores o entrevistados.

Business&Co.®, Escuela de Gobierno eGob®, Master en Gobierno de Tecnologías de la Información MGEIT®, Caviar®, Telecoms®, Respalda® y AulaDatos® son Marcas y Nombres Comerciales Registrados de Business, Technology & Best Practices, S.L. "COBIT® es una Marca Registrada de ISACA.

ISSN 2951-8180

**La Escuela de Gobierno eGob®
Certifica su Sistema de Gestión
de Organizaciones Educativas
con la Norma ISO 21001**

Alcance: Formación Certificada y Programas Directivos para Alta Dirección,
Mandos Intermedios y Responsables de la Ejecución Estratégica
y el Cambio Organizacional en Organizaciones Públicas y Privadas



ESPECIAL
AGOSTO
2025



índice

DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



**IA generativa y ciberguerra:
la nueva frontera**



**ALTAI: la guía de evaluación para
una IA confiable según
la Comisión Europea**



**¿Por qué un
Espacio Europeo
de Datos de Salud?**



**Todo a la vez en todas partes...
¿y sin control?: la amenaza
de la IA ubicua**

Copyright

02

Índice de Contenidos

04

**Este mes te
recomiendo leer...**

por JAVIER PERIS

07

**Arquitectura
de Inteligencia
Artificial.
Los cimientos del
futuro digital.**

08

**NIS2 para
directivos:
claves y desafíos**

12

**IA generativa y
ciberguerra:
la nueva frontera**

16

**IA generativa
corporativa: una
revolución silenciosa
más allá de la nube**

20

**ALTAI: la guía de
evaluación para una
IA confiable según
la Comisión Europea**

24

**Europa y la
ciberseguridad
de hospitales:
protegiendo vidas
y datos.**

28

**Europa y su
compromiso con
el futuro y la IA**

32

**¿Por qué un
Espacio Europeo
de Datos de Salud?.**

36

**IA y Salud: lo que
nos está costando
ver (y resolver)**

40

**Todo a la vez en todas
partes... ¿y sin control?:
la amenaza de la
IA ubicua**

44

**El problema de los
tres cuerpos:
¿hacia dónde
orbitará la IA?**

48

**La regulación
europea es
tendencia en la
gestión de riesgos**

48

**Cierre de
Temporada 2025
Revistas “Tecnología
y Sentido Común” y
“Stakeholders.news”**

52

**UNE presenta
su Estrategia 2030
para lograr un
mayor impacto
de las normas
en la sociedad**

68

TECH

#TYSC

Premios recibidos



Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI



El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

itSMF
ESPAÑA

Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática



VI Premios ESET Periodismo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Artículo de Ricard Martínez "Seguridad en el Smartphone".

Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.

Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.

Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.



Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad



La Junta Directiva de la Asociación Profesional Española de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC



Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA



La Asociación Valenciana de Informática Sanitaria AVISA durante las XIV Jornadas Técnicas que bajo el título "20 Años Implantando TIC en Sanidad" se celebraron en Benidorm en febrero de 2024 hizo entrega de su agradecimiento a Tecnología y Sentido Común por su apoyo y visibilidad a la profesión.



Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana COIICV alabó tanto la gran labor de difusión que viene realizando Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.



Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



Gobierno del Tiempo y Gestión de la Productividad con TSG4 White Belt

Javier Peris

Tras más de veinte años en las trincheras del gobierno TI y el Cambio organizacional, he visto a demasiados profesionales brillantes ahogarse. Vivimos encadenados a las notificaciones, luchando contra un torbellino de urgencias que devora nuestra capacidad para el trabajo profundo. Creemos que el *burnout* es el precio del éxito.

He escrito “**Gobierno del Tiempo y Gestión de la Productividad TSG4 White Belt**” porque estoy convencido de que estamos equivocados y quiero demostrártelo.

Te aseguro que no es otro método de productividad; es un manifiesto para una verdadera revolución personal.

Con este libro “**Gobierno del Tiempo y Gestión de la Productividad TSG4 White Belt**”, mi objetivo es darte la dosis fundamental de

conocimientos que no sabías que necesitabas. En él, disecciono la enfermedad de nuestra era: el “Lingchi Temporal”, esa muerte por mil cortes de interrupciones que aniquila nuestro foco.

Este primer libro es un llamado a las armas. Te obliga a abandonar el rol de “Gestor eficiente del caos” para asumir tu verdadero poder y responsabilidad como “Gobernador de tu tiempo”. No ofrezco herramientas, sino algo mucho más valioso: un cambio de paradigma.

Mi meta es que veas tu semana no como una agenda que se llena, sino como un territorio soberano que debes gobernar.

“

Existe un modelo de arquitectura general de sistemas de IA que nos será de utilidad para entenderlos mejor

Arquitectura de Inteligencia Artificial.

Los cimientos del futuro digital.

Damos la bienvenida a nuestros lectores tras permitirnos un pequeño paréntesis vacacional. La vuelta al trabajo, o a las clases, viene marcada por una adopción cada vez más fuerte de los sistemas de inteligencia artificial (IA), con sistemas operativos que ya integran asistentes basados en IA (Google con Gemini, Microsoft con Copilot, Apple con AI, etc.).

Pero desde este medio, y por supuesto desde esta sección, siempre se aboga por la tecnología con sentido común, y por tanto empezamos temporada hablando de la arquitectura de los sistemas de IA. Si bien es cierto que existen variaciones según hablemos de sistemas de aprendizaje federado, aprendizaje supervisado y no supervisado, etc., el hecho es que sí existe un modelo de arquitectura general de sistemas de IA que nos será de utilidad para entenderlos mejor.

Una buena construcción arquitectónica debe empezar por unos buenos cimientos, y por eso nosotros vamos a empezar a presentar esta arquitectura de abajo hacia arriba.

En primer lugar, contamos con una **capa de percepción**, de recolección de datos. Esta capa tendrá la misión de recoger todos los datos de sensores, de sistemas de información, de los propios usuarios, o incluso de máquinas. Estos datos se recogerán de alguna manera y se trasladan a la segunda capa para ser almacenados y posteriormente procesados.



CONTINÚA EN
PRÓXIMA PÁGINA



“
La vuelta al trabajo
viene marcada por
una adopción cada vez
más fuerte de los
sistemas de IA

La segunda capa es la de **computación**, se produzca esta en la nube, en los sistemas locales, o bien en el propio dispositivo que recoge los datos (*edge computing*).

Tras la recogida de los datos y los cálculos oportunos, la siguiente capa vamos a llamarla de **gestión de datos**. En ella es donde debe aplicarse el gobierno del dato (qué datos van a utilizarse para qué y cuál es la mejor manera de que aporten valor a la organización), la preparación de estos datos si hubiera que hacer limpieza, integración, etc. y se va a medir (y si es posible, mejorar) la calidad de los datos. Posiblemente aquí ya contemos con un grafo de conocimiento básico que nos permita obtener relaciones entre los datos recogidos.

La siguiente capa es lo que llamamos la capa de **protección de los datos**. En ella, además de preservar los datos de una forma segura, contando incluso con copias de seguridad y garantizando la disponibilidad de la información y la recuperación si ocurre un desastre.

A continuación tenemos la capa más sensible al tipo de tecnología de IA que queremos aplicar, la capa de **arquitectura de procesamiento de datos**. Aquí será necesario antes contestar algunas preguntas importantes: ¿cuál es la naturaleza de nuestros datos? ¿qué volumen de datos vamos a manejar? ¿qué tolerancia a fallos debemos exigir? ¿debemos procesar los datos en tiempo real o en diferido? ¿debemos utilizar un enfoque de tipo Lambda (con flujo de proceso por lotes) o de tipo Kappa (sin flujo de proceso por lotes)? ¿cuánta latencia (tiempo que transcurre desde que el usuario realiza una acción hasta que obtiene la respuesta) podemos tolerar?

Finalmente, dos capas que quizá nos vienen a todos a la cabeza al hablar de sistemas de IA: la capa de **analítica de datos** (módulos de aprendizaje, de predicción, de feedback, etc.) y la capa de **interfaz** que cubrirá interacción con el usuario (sistema conversacional, a través de ventanas de diálogo, línea de comandos, etc.) y visualización de datos (representación gráfica, textual, explicabilidad, etc.).

Sin embargo, toda esta descripción deja de lado otras dos capas o áreas funcionales que son igualmente importantes: la de compartir o de **interoperabilidad** con otros sistemas, y la de confianza o de **seguridad**, una capa realmente compleja dedicada a velar por la confidencialidad, la integridad y la disponibilidad de estos sistemas.

Dicen que Abraham Lincoln (1809-1865) acuñó la frase: “La mejor manera de predecir el futuro es crearlo”. Para el famoso arquitecto Oscar Niemeyer, la arquitectura es un acto de fe en el futuro. En las líneas anteriores hemos desglosado la arquitectura de los sistemas de IA más extendida hoy en día, así que podríamos decir que este artículo es un acto de fe en el futuro de la IA, pero en realidad, lo que hemos hecho es ofrecer las herramientas para que ustedes mismos, nuestros pacientes lectores y nuestra tortuga ninja, puedan construir ese futuro de manera estructurada: los cimientos de nuestro futuro digital.

P4MGO![®] Essentials

Portfolio, Programme,
Project & Product
Management &
Governance



“

**La ciberseguridad
entra finalmente
en el despacho
de la dirección**



NIS2 para directivos: claves y desafíos

Como suele suceder en estos casos, este año se ha empezado a hablar con un poco más de insistencia sobre la directiva 2022/2555 del Parlamento Europeo y del Consejo, o Directiva NIS2, que entró en vigor en enero de 2023. Eso sí, en teoría debe ser traspuesta a la legislación española este mes de octubre, es decir, mientras ustedes leen estas líneas...

Esta directiva tiene como objetivo “impulsar el nivel general de ciberseguridad en la UE y la resiliencia de las infraestructuras críticas y de los servicios digitales en Europa” y evoluciona sobre la anterior directiva NIS (Directiva 2016/1148 del Parlamento Europeo y del Consejo), abarcando más sectores y cambiando la diferenciación entre operadores de servicios esenciales y proveedores de servicios digitales por una nueva entre sectores de alta criticidad (esenciales) y otros sectores críticos (importantes), que tendrán un nivel diferente de supervisión.

Por otro lado, también hace hincapié en la seguridad de la cadena de suministro y en los requisitos de cara a informar de un incidente (estableciendo unos contenidos mínimos y unos plazos máximos de notificación), y toma una aproximación basada fundamentalmente en la gestión de los riesgos.

En relación con las sanciones administrativas por negligencia en la aplicación de controles, para evitar diferentes raseros en diferentes países, con respecto a las entidades esenciales, NIS2 requiere por ejemplo que la máxima sanción sea de al menos 10.000.000 € o el 2% del volumen de negocios anual total mundial del ejercicio financiero anterior (lo que sea mayor). Con respecto a las entidades importantes, NIS2 requiere que los Estados miembros establezcan una sanción máxima de al menos 7.000.000 € o el 1,4% del volumen de negocios anual total mundial del ejercicio financiero anterior, lo que sea mayor.



**CONTINÚA EN
PRÓXIMA PÁGINA**



“
NIS2 hace hincapié
en la seguridad
de la cadena de
suministro con
un enfoque de
gestión del riesgo

Además, **NIS2 contempla la responsabilidad legal de las personas que tengan posiciones directivas en estas organizaciones**, por lo que puede impactar directamente en estas el incumplimiento de algunos aspectos de la directiva.

Por otro lado, para evitar el “yo no sabía nada”, el artículo 20.2 de la directiva NIS2 indica que deberá garantizarse que **“los miembros de los órganos de dirección de las entidades esenciales e importantes deban asistir a formaciones [...] al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad”**.

Por supuesto el Centro Criptológico Nacional español ya ha iniciado el camino con la publicación de su guía CCN-STIC 892 para el perfil de cumplimiento específico para organizaciones en el ámbito de aplicación de la directiva NIS2, junto con un par de infografías, y estamos a la espera de la publicación de la transposición en España.

En España ya se amplió la anterior directiva NIS a otros sectores no incluidos inicialmente en aquella, como la industria química o la nuclear, la industria TIC o el sector de la alimentación. A falta de saber si habrá alguna ampliación en la nueva transposición, los sectores mencionados específicamente en NIS2 por considerar que contienen entidades esenciales

o de alta criticidad son: energía, transporte, banca, infraestructuras de mercados financieros, sector sanitario, agua potable, aguas residuales, infraestructura digital, gestión de servicios TI entre empresas, entidades de administración pública (excepto poder judicial, parlamentos y bancos centrales) y el sector espacial.

En cuanto a las entidades importantes (u otros sectores críticos) se incluyen al menos los siguientes: servicios postales y de mensajería, gestión de residuos, industria química, alimentación, los proveedores de servicios digitales (comercio electrónico, motores de búsqueda y redes sociales incluidos), investigación y fabricación de productos sanitarios, informáticos, material eléctrico, vehículos de motor, remolques y otro tipo de productos.

Finalizamos este artículo habiendo pues cumplido el objetivo de trasladar a nuestros lectores y a nuestra tortuga ninja de que, para el nuevo curso la ciberseguridad entra finalmente en el despacho de la dirección, y los directivos deben entrar en las aulas para mejorar la ciberresiliencia de sus organizaciones.

¿Demasiada Iniciativas?
¿Alineamiento Estratégico Cuestionable?
¿Dificultad para Priorizar?
¿Vision basada en Silos o Islas?
¿Falta de foco estratégico en el valor a largo plazo?



Alienamiento Estratégico de las iniciativas
Priorización Basada en el valor
Optimización de Recursos
Gestión de Riesgos Corporativos
Ejecución Estratégica Efectiva



soluciones@p4mgo.com
<https://p4mgo.com>

“

**Hasta ahora, nadie
sabe cómo entrenar
sistemas de IA
realmente potentes
para que sean útiles,
honestos e inocuos de
forma consistente**



IA generativa y ciberguerra: la nueva frontera

Si el mes pasado hablábamos de la importancia que otorga Europa a la ciberresiliencia mediante la directiva NIS2, hoy hablamos de como el uso de la inteligencia artificial (IA) generativa está redefiniendo un nuevo frente de guerra en el ciberespacio.

En agosto OpenAI daba ya la noticia de que había desactivado varias cuentas de usuarios, ligadas a un grupo iraní, que habían usado ChatGPT para crear contenido online en inglés y en español como artículos o publicaciones en redes sociales para sembrar polémica entre los votantes estadounidenses (tanto en el sector conservador como progresista).

Una semana antes, Microsoft también anunció que había detectado noticias falsas destinadas a generar división entre la ciudadanía americana y también algunos ataques dirigidos a funcionarios del gobierno estadounidense. Según el responsable del Microsoft's Threat Analysis Center, mientras que los grupos vinculados a Rusia intentan influir en el resultado de las elecciones, los grupos iraníes intentan que las elecciones no se celebren o que su resultado no sea considerado válido.

Esto, que no es nada nuevo porque ya ha ocurrido al menos en los tres últimos ciclos electorales americanos, es ahora más preocupante porque están utilizando la IA para generar esos contenidos

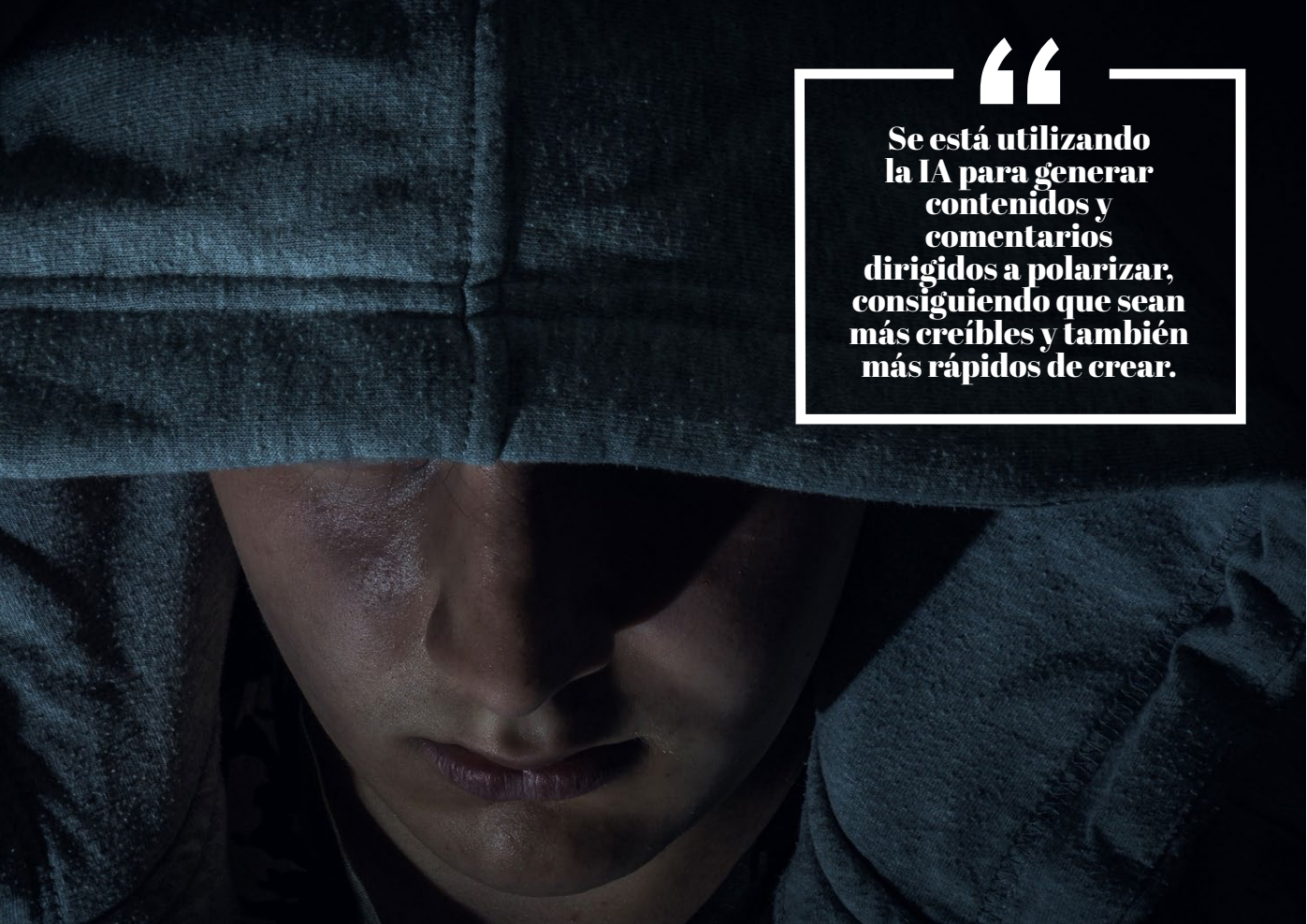
y para realizar comentarios dirigidos a polarizar, consiguiendo que sean más creíbles y también más rápidos de crear, incluso utilizan la IA para plagiar artículos ya existentes pero dándoles la orientación deseada y publicándolos en medios locales creados por estos grupos, afianzando posiciones y credibilidad de cara a publicar luego contenidos falsos más afines a sus intereses.

Recordemos que incluso desde el equipo de campaña de Trump afirmaban haber sido objetivo de un ataque de estos grupos donde se habrían obtenido documentos sensibles de carácter interno.

Otro uso que OpenAI afirma que se está dando a ChatGPT es el de realizar reconocimientos de sistemas de control industrial (controladores lógicos programables, etc.), explorando instalaciones y buscando vulnerabilidades para explotarlas. Esto habría provocado ya ataques a plantas de agua potable en Irlanda, Pensilvania, etc., si bien es cierto que al parecer estas instalaciones no estaban demasiado protegidas.



**CONTINÚA EN
PRÓXIMA PÁGINA**



**“
Se está utilizando
la IA para generar
contenidos y
comentarios
dirigidos a polarizar,
consiguiendo que sean
más creíbles y también
más rápidos de crear.”**

Aunque en los párrafos anteriores nos hemos centrado en la herramienta ChatGPT de OpenAI, en realidad, y como indicaba un post de Anthropic en marzo de 2023, “hasta ahora, nadie sabe cómo entrenar sistemas de IA realmente potentes para que sean útiles, honestos e inocuos de una manera consistente”.

De hecho, aunque según un análisis de Chatterbox Labs a los modelos LLM de Microsoft, Mistral, OpenAI, TII, Anthropic, Cohere y Meta, todos excepto el de Anthropic demostraban ser capaces de generar contenido violento o sexualmente explícito, contenido dirigido a realizar actividades fraudulentas, preparar discursos de odio, generar desinformación, aplicaciones de malware, provocarse autolesiones y cometer otras actividades ilegales, aunque ya hay evidencia que no vamos a mostrar aquí de tácticas para que incluso el modelo de Anthropic ofrezca muchos de estos contenidos.

En definitiva, y como ya hemos mencionado aquí en más de una ocasión, la aparición de estos sistemas de IA generativa nos ponen nuevos retos por delante, y aumenta la accesibilidad no solo para estudiar, investigar, crear contenidos multimedia, atender a los clientes o diagnosticar a los pacientes, sino para crear contenido o software malicioso.

Por ello se hace cada vez más necesaria la evaluación de riesgos de los sistemas de IA, la creación de “puertos seguros” donde la comunidad pueda probar nuevas estrategias de ataque que permitan aprender y proteger mejor estos modelos, y la utilización de estrategias de red team (equipos de ataque) que puedan poner a prueba los mecanismos de defensa.

Mientras tanto, podemos afirmar que estas herramientas pueden tener un funcionamiento no deseado por sus creadores, pero no seremos capaces de conocer hasta qué punto esto es posible, y esto nos lleva a asumir un riesgo desconocido, ya que estas herramientas ya se encuentran en el mercado, al alcance de todos, incluso de forma gratuita en algunos casos.

Mientras esto se soluciona, como siempre recomendamos a nuestros lectores, incluida nuestra querida tortuga ninja, esfuércense por aplicar su pensamiento crítico, hagan su análisis y contraste de fuentes, y no se crean lo primero que apoye su sesgo de confirmación. Corren tiempos difíciles para la verdad, y tenemos que cuidarla.

¿Objetivos ambiciosos?
¿Cambios transformadores fallidos?
¿Sinergias desaprovechadas?
¿Foco en entregables y no en beneficios?
¿Iniciativas sin visión de conjunto?



Maximización del Valor
Nuevas Capacidades Organizacionales
Gestión de interdependencias
Gobierno de la Transformación
Consolidación de beneficios



soluciones@p4mgo.com
<https://p4mgo.com>

IA generativa corporativa: una revolución silenciosa más allá de la nube.

Observando la evolución de los sistemas de inteligencia artificial generativa que existen en el mercado, hemos visto avances impresionantes, aunque ya se empieza a ver algún síntoma de agotamiento que trataremos en futuros artículos.

Al margen del agotamiento de este tipo de tecnología, el hecho es que aunque la punta del iceberg son sistemas muy conocidos, como ChatGPT de OpenAI, Copilot de Microsoft, Claude de Anthropic o Perplexity AI de la empresa del mismo nombre, existen sistemas de IA basados en modelos extensos del lenguaje (LLM en inglés) que pueden funcionar de forma local, tanto de pago como gratuitos, y que nos permiten entrenarlos con información propia de nuestros

sistemas de información y nuestra base de conocimiento.

Las ventajas más importantes, como nuestros lectores estarán suponiendo, son las relativas a la seguridad, la personalización y la autonomía que este tipo de sistemas pueden ofrecer a una organización de cualquier tipo.

No nos engañemos: para aprovechar a fondo las capacidades de un sistema LLM vamos a necesitar añadir ciertos datos de nuestra organización que pueden tener un carácter confidencial o requieren un marco legal de privacidad muy estricto.



CONTINÚA EN
PRÓXIMA PÁGINA

“

Las ventajas más importantes de un sistema de IA local son la seguridad, la personalización y la autonomía que este tipo de sistemas puede ofrecer





Además, estos sistemas necesitarán a corto o medio plazo interactuar con nuestros sistemas corporativos para consultar, añadir, modificar o eliminar información, algo que de nuevo les da unas capacidades que van a hacer que la seguridad sea un valor importante en la elección de un LLM.

La personalización es otro valor que las organizaciones van a buscar a corto plazo: si nos apoyamos en la misma herramienta todo el mundo, es fácil que nos ofrezca respuestas similares y por tanto nos cueste diferenciarnos. También es posible que las respuestas que nos ofrezca el sistema no tengan en cuenta nuestra cultura organizativa, cobertura geográfica, gama de productos, patentes, etc. Esta necesidad de personalización es también uno de los motivos para optar por un sistema de IA generativa corporativo en local.

En cuanto a la autonomía, los sistemas de IA generativa en la nube ha demostrado ya que pueden caer, la propia web de OpenAI contabiliza 13 caídas importantes de ChatGPT en 2024 hasta la fecha, y 7 de su API, de la que dependen muchos chatbots y otras utilidades basadas en IA generativa. Además, de vez en cuando ocurre lo que se llama un colapso del modelo, perdiendo la capacidad de representar la realidad correctamente, generando sesgos, propagando errores y dificultando su reacción ante datos nuevos no vistos anteriormente.

Es cierto que esto ocurre en cualquier modelo de tipo LLM, pero los sistemas en local permiten evitar más fácilmente ciclos de compresión o de colapso, especialmente si las respuestas generadas no se reinyectan al modelo para entrenamiento de forma automática. La necesidad de alta disponibilidad y de resistencia a estos ciclos de colapso pueden hacer recomendable una instalación local del LLM.

Sin embargo, no todo son aspectos positivos, los sistemas actuales de IA generativa, de tipo LLM, necesitan muchos recursos, como GPUs (procesadores gráficos) de 24 GB de VRAM, una o varias según el tamaño del modelo, con el consumo eléctrico que provocan. Un ejemplo realista de sistema LLM local pequeño como Mistral 7B, suponiendo que dispone de una GPU que está activa 8 horas diarias y que su consumo es de 400 vatios hora generaría un consumo de 3,2 kW hora diarios (96 kW hora al mes). Un modelo con 4 GPUs como Llama 2-70B podría suponer unos 400 kW hora al mes, equivalente al consumo de una oficina pequeña de 5 empleados en el mismo periodo. Esto solo tiene en cuenta el tiempo de uso, no el tiempo de entrenamiento del modelo que requeriría de varias GPUs trabajando al 100% de su capacidad durante días, semanas o meses, según tamaño del modelo.

La mayoría de sistemas existentes sin embargo vienen ya preentrenados y solo queda pendiente que hagamos el ajuste fino, que no requiere tanta demanda de recursos, pudiendo necesitar en el caso de un LLM pequeño una sola GPU durante unos pocos días.

Además, en cuanto al coste de estos sistemas en local, sería necesario disponer de algún especialista en estos sistemas aunque no fuera a tiempo completo, adquirir el hardware necesario, analizar si tenemos un coste de licencia, así como la integración con sistemas existentes.

En conclusión, la decisión de desplegar un sistema de IA generativa local en lugar de optar por otro compartido en la nube no es únicamente técnica o económica, tiene implicaciones estratégicas y de seguridad que debemos analizar previamente.

Aún así, el abaratamiento de la infraestructura necesaria y la popularización de estos sistemas y del conocimiento necesario para configurarlos hace que cada vez más organizaciones opten por un LLM local, algo que quizá pronto verá nuestra tortuga ninja y también ustedes, estén atentos.

Escuela de Gobierno
eGob®
<https://escueladegobierno.es>

**En la Escuela de Gobierno eGob®
impartimos Cursos de Doble Certificación
y nos certificamos por partida doble
ISO 9001:2015 + ISO 21001:2018**

Alcance: Formación Certificada y Programas Directivos para Alta Dirección,
Mandos Intermedios y Responsables de la Ejecución Estratégica
y el Cambio Organizacional en Organizaciones Públicas y Privadas



ISO 9001:2015

ISO 21001:2018



ALTAI: la guía de evaluación para una IA confiable según la Comisión Europea

Estimadas lectoras y lectores, es 2025, el futuro ya está aquí, así que bienvenidos y mientras van preparando sus propósitos de mejora, pónganse cómodos y disfruten del principio de todo.

Hace unos meses una persona me pidió consejo sobre cómo evaluar el uso ético de un sistema de Inteligencia Artificial (IA). Para evitar enfoques excesivamente académicos o comerciales, le remití a una publicación de la Comisión Europea que aborda esta evaluación desde siete perspectivas muy interesantes. Se trata de la Guía de evaluación para una IA confiable (ALTAI), una especie de cuestionario rápido que permite a cualquier organización identificar algunos riesgos que pueden surgir en la puesta en marcha y la utilización de un sistema de IA.

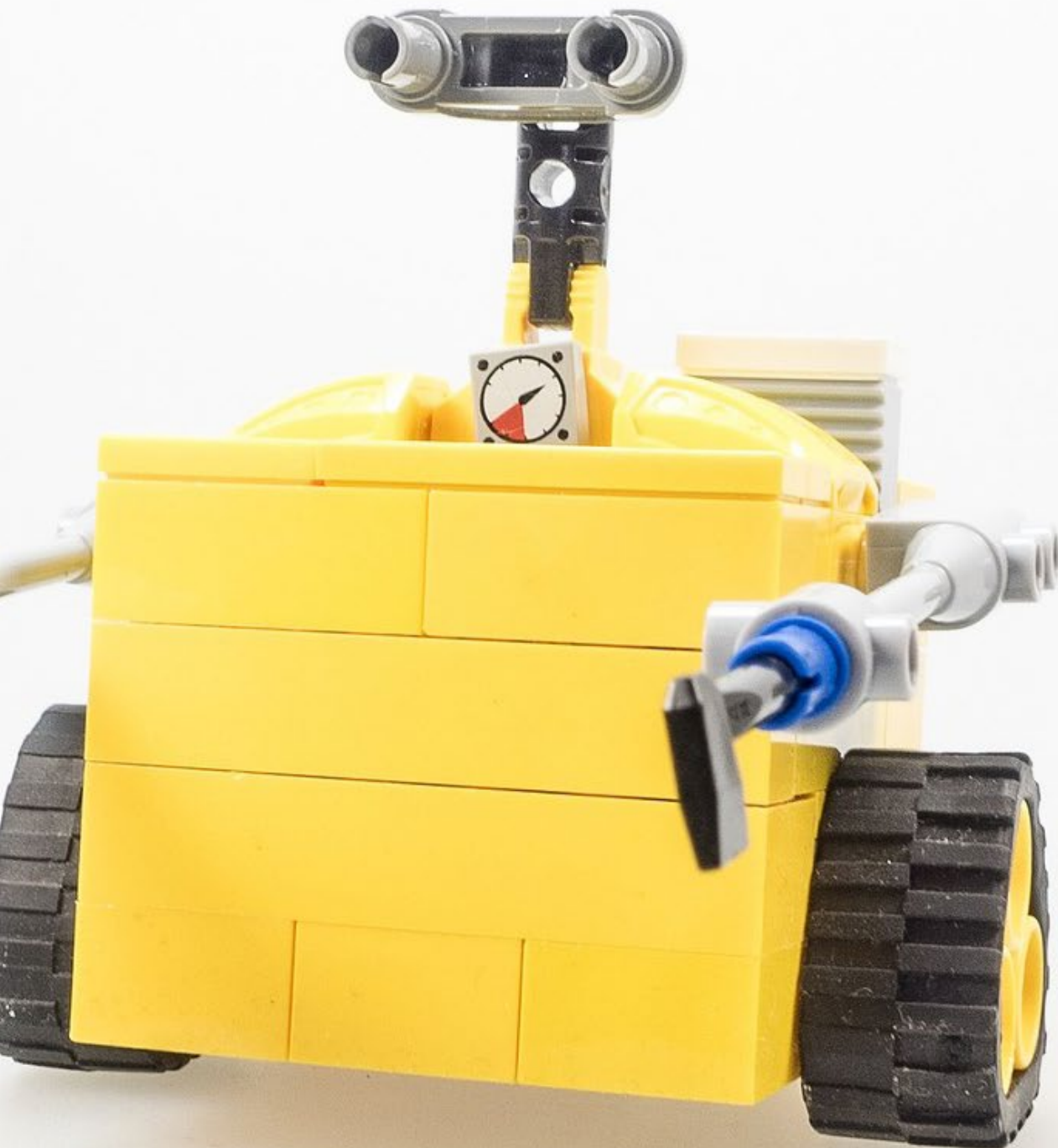
El cuestionario tiene 122 preguntas y subpreguntas agrupadas en 7 secciones, y además dice que se enfatiza la flexibilidad de uso, indicando que las organizaciones pueden “utilizar elementos relevantes para el sistema de IA particular de esta lista o añadir elementos a la misma según lo consideren oportuno, teniendo en cuenta el sector en el que operan”, por lo que no es una cosa que se haga en una tarde y tampoco da garantías de cubrir todos los aspectos necesarios para nuestra organización, pero puede ser un comienzo.

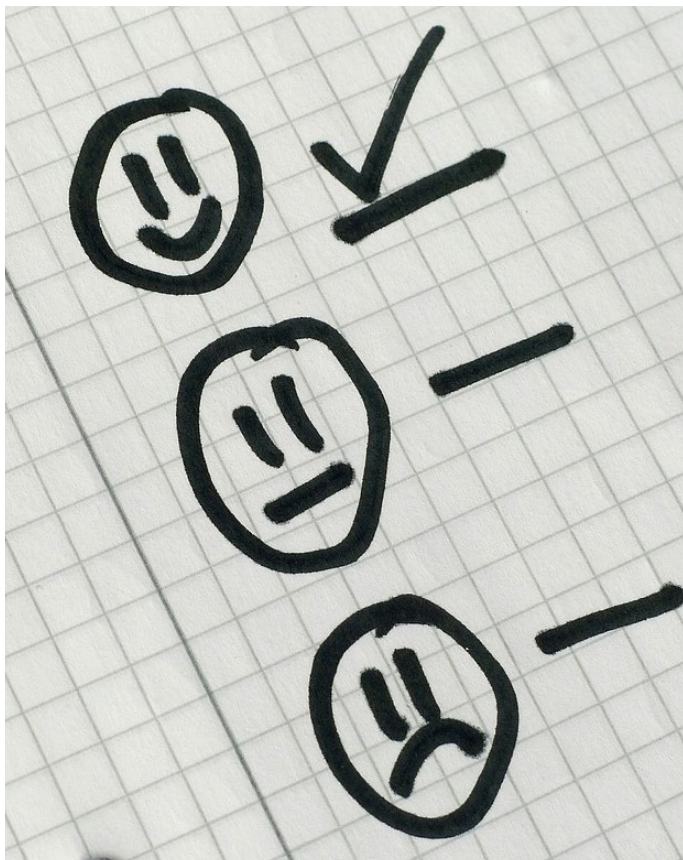


CONTINÚA EN
PRÓXIMA PÁGINA

“

**ALTAI evalúa la
transparencia
con tres aspectos
clave: trazabilidad,
explicabilidad y
comunicación de
las capacidades y
limitaciones del
sistema a los usuarios**





que no se nos escapa como indicábamos en el artículo anterior que estos sistemas hacen un uso exigente de recursos, especialmente para el entrenamiento del modelo.

La privacidad y la gobernanza de los datos también se aborda en el cuestionario ALTAI, por ejemplo preguntando si se ha considerado el impacto del sistema de IA en el derecho a la privacidad, el derecho a la integridad física, mental y/o moral y el derecho a la protección de datos.

Finalmente, también se pregunta por aspectos de ciberseguridad, preguntando si se han implementado medidas para garantizar la integridad y la seguridad del sistema durante todo su ciclo de vida, incluyendo test de intrusión, mecanismos de actualización, envenenamiento de datos, si tiene alguna certificación de seguridad, si se han identificado amenazas y evaluado los riesgos, etc. También si se tiene información del periodo de cobertura de seguridad y de actualizaciones del sistema.

ALTAI incluye una evaluación de los mecanismos de rendición de cuentas, planteando si existen mecanismos de logs, si se realizan auditorías externas, concienciación a usuarios, y si se ha habilitado algún tipo de mecanismo para anticipar y planificar la respuesta a posibles errores o impactos negativos del sistema de IA, por ejemplo estableciendo procedimientos para que los afectados por la decisión de un sistema de IA puedan solicitar una revisión humana de su caso,

ALTAI aborda la agencia y la supervisión humana a través de varias preguntas, evaluando si el sistema de IA está diseñado para guiar o influir en la toma de decisiones humanas y si existe el riesgo de que los usuarios confundan las decisiones algorítmicas con las humanas. También se valora si el sistema de IA podría generar una excesiva dependencia. Evalúa también la necesidad de supervisión humana, aunque no contempla específicamente nuevos riesgos que están apareciendo como el exceso de confianza o el abuso de agencia de un sistema de IA.

ALTAI evalúa la transparencia con tres aspectos clave: trazabilidad (documentar adecuadamente los procesos de desarrollo y de decisión del sistema de IA), explicabilidad (capacidad de explicar las decisiones y predicciones realizadas por el sistema), y comunicación de las capacidades y limitaciones del sistema a los usuarios.

La equidad y la no discriminación también forman parte de la autoevaluación de ALTAI, invitando a elaborar una estrategia para evitar sesgos injustos y valorar la representación de grupos potencialmente vulnerables en el entrenamiento del sistema, además de valorar la accesibilidad y diseño del sistema de IA para el uso por personas con diversidad funcional.

Otro aspecto evaluado por este cuestionario es el impacto del sistema de IA en la sociedad (mercado laboral y procesos democráticos, entre otras cosas) y en el medio ambiente, ya

La pregunta que pueden estar haciéndose simultáneamente nuestros lectores y la tortuga ninja mientras escribe este diario es: ¿respondiendo este cuestionario de autoevaluación tengo la seguridad de que el sistema de IA que estoy utilizando es confiable?

La respuesta es que puede servir para identificar algunas carencias, pero el contexto es bastante complejo, existiendo otras fuentes igualmente importantes para evaluarlo, como las normas ISO 42001 y 23894, y la propia evaluación de impacto de un sistema de IA, algo obligatorio para sistemas de IA de alto riesgo, según el artículo 27 de la AI Act europea (a excepción de sistemas de IA para algunas infraestructuras críticas), por lo que lo más aconsejable como propósito de Año Nuevo es ponerse en manos de expertos independientes que puedan aportar una visión objetiva (no ligada a una herramienta ni a una tecnología concreta) y que tengan un conocimiento profundo del sector en el que nos movemos.

Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



Business&Co.®
Business, Technology & Best Practices, S.L.



Europa y la ciberseguridad de hospitales: protegiendo vidas y datos.

La Comisión Europea ha publicado en 2025 un plan de acción para proteger el sector salud a nivel europeo. Según la rueda de prensa de presentación del plan, en 2023 se registraron 309 incidentes significativos de ciberseguridad en el sector sanitario. Esta cifra es superior a la de cualquier otro sector crítico, según indicaron también. El reto de proteger al sector sanitario de ciberataques es pues importante, especialmente si consideramos que pronto se pondrá en marcha el Espacio Europeo de Datos de Salud.

En dicho plan se recopilan iniciativas que ya venían tiempo planteándose y que parece que ahora al fin se van a hacer realidad, como el apoyo de la Unión Europea a sus socios a través de un Centro de Ciberseguridad para Hospitales y otros Proveedores Sanitarios de la mano de ENISA, la Agencia de Ciberseguridad de la Unión Europea, o las iniciativas de formación y concienciación para profesionales sanitarios. También se va a activar un servicio de alerta temprana a nivel europeo y un catálogo de vulnerabilidades conocidas en dispositivos médicos.

Otra de las iniciativas a tener en cuenta es un servicio de respuesta rápida a incidentes, específico para el sector salud, que complementará a los servicios nacionales existentes en incidentes a gran escala.

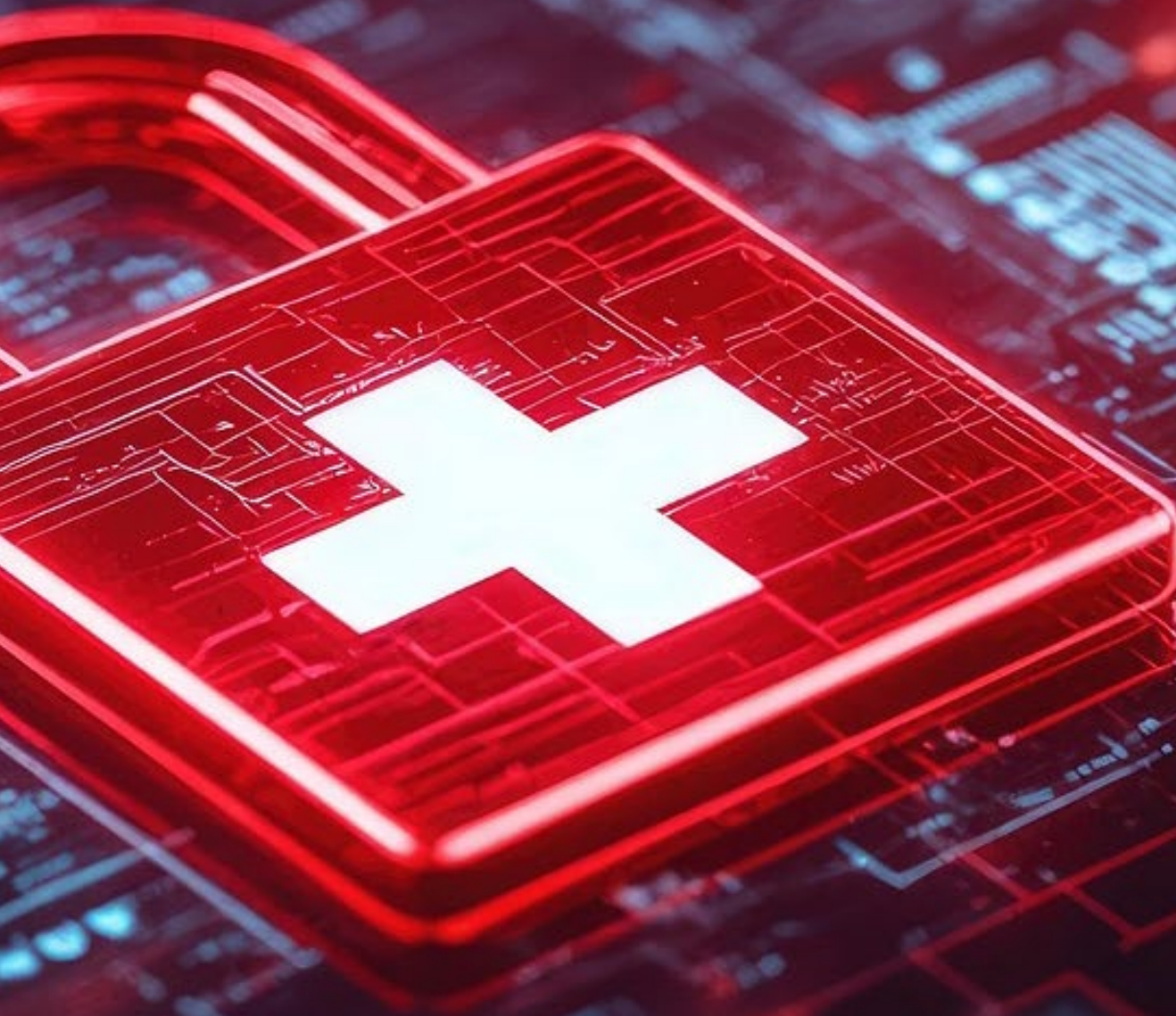
Hemos de tener en cuenta que el sector de la salud, especialmente en el caso de los hospitales, tiene diferencias significativas en comparación con otros sectores: tiene un horario de 24x7x365 en muchos casos, maneja una información altamente sensible y persistente (como siempre digo, uno no puede cambiar de enfermedad aunque se haga público que la padece, a diferencia del número de tarjeta de crédito o la contraseña de un servicio), y tiene una superficie de ataque enorme, debido sobre todo a la conexión de equipamiento médico raramente actualizado a la misma red que las aplicaciones que manejan la información clínica de los pacientes, y a que estas mismas aplicaciones tienen un ciclo de vida extraordinariamente largo y un soporte normalmente escaso.



CONTINÚA EN
PRÓXIMA PÁGINA

“

**El reto de proteger
al sector sanitario
de ciberataques es
importante, y más
si consideramos que
pronto se pondrá en
marcha el Espacio
Europeo de
Datos de Salud**





Es de esperar que iniciativas como el catálogo de vulnerabilidades conocidas, los requisitos de ciberseguridad para dispositivos médicos que exige la certificación europea MDR (Medical Device Regulation), las directrices para la adquisición de equipamiento médico, y el diálogo con los fabricantes pueda mejorar esta situación.

El plan busca en resumen fortalecer la ciberseguridad del sector salud aumentando su madurez en ciberseguridad, fortaleciendo las cadenas de suministro, y ofreciendo los servicios mencionados anteriormente de alerta y respuesta rápida.

Sin embargo, como suele pasar en estos casos, se pide también el compromiso de cada uno de los Estados miembros, como el establecimiento de centros de apoyo de ciberseguridad nacionales específicos para hospitales y otros proveedores sanitarios, planes de actuación nacionales con el foco en el sector de la salud, y el análisis y la compartición de información sobre los incidentes a través, por ejemplo, de centros de análisis y compartición de información (ISACs). También se les pide la realización de ejercicios de ciberseguridad nacional para probar sus protocolos de respuesta y reforzarlos si fuera necesario, entre otras cosas. Para esto también se plantea que existan presupuestos finalistas que no se detraigan de los presupuestos para la atención sanitaria.

Por otro lado, la visión europea del plan, con sistemas sanitarios a menudo centrados en hospitales y pequeñas clínicas, hace que en ningún momento se mencione a la Atención Primaria (bueno, solo una vez: para explicar que el 79% de ciudadanos de la UE tiene acceso a su historia clínica electrónica de Primaria), aunque sí habla de pequeños centros de atención sanitaria.

Es cierto que la superficie de ataque en un centro de Atención Primaria es menor en términos de variedad y número de puestos de trabajo en relación con un hospital, pero el impacto de un ciberataque sobre sistemas de información centralizados de Atención Primaria sería notorio y podría interrumpir servicios esenciales o provocar la pérdida de confianza de los ciudadanos, además de colapsar los hospitales de manera indirecta, así que esperemos que los Estados miembros con un sistema de Atención Primaria semejante al español tomen nota y presten atención también a este nivel asistencial en términos de ciberseguridad.

Tampoco tiene en especial consideración actividades de concienciación a los pacientes, algo que tendrá que acompañar estas iniciativas, porque los atacantes siempre van a ir al eslabón más débil, y prefiero no desgarnar aquí el interés y las posibles maneras en que pueden hacerlo.

En definitiva, para que este plan realmente tenga éxito hace falta un compromiso mutuo como es habitual entre la Unión Europea y sus Estados miembros, y presupuesto para financiarlo, algo que tradicionalmente ha sido escaso ya que había que decidir entre el gasto de farmacia, de hospitalización y de bloque quirúrgico y el gasto en medidas de ciberseguridad, algo que se busca evitar con este plan.

Ojalá tenga un resultado muy positivo este conjunto de iniciativas, y que tanto ustedes, lectores, como este mismo que escribe, y la tortuga ninja, podamos disfrutar por muchos años de la confianza en nuestro sistema sanitario.

Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



Business&Co.®
Business, Technology & Best Practices, S.L.



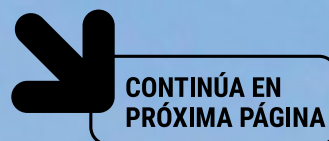
Europa y su compromiso con el futuro y la IA

En septiembre de 2024 la Comisión Europea presentó las conclusiones del “Informe Draghi: una estrategia competitiva para Europa”, la primera parte de un informe muy completo sobre la competitividad europea de la mano de un expresidente del Banco Central Europeo, es decir, alguien que ha sido el encargado de diseñar y aplicar la política económica y monetaria de la Unión Europea, influyendo nada menos que en el crecimiento económico y en la creación de empleo.

Dicho informe basa la estrategia competitiva europea en tres grandes transformaciones: reducir la brecha de innovación con respecto a China y EE. UU., la descarbonización, o un mayor uso de energías renovables, y la seguridad económica, reduciendo su dependencia de países no miembros y haciendo valer su peso global en la política económica exterior y en su estrategia industrial de defensa.

Ahora supongamos que los dirigentes europeos toman buena nota de estas recomendaciones y se ponen de acuerdo en aplicarlas. ¿Por dónde empezaría en el mundo en el que estamos? La industria de defensa parece una de las claves, pero ¿acaso no es también importante el liderazgo tecnológico?

Actualmente estamos presenciando una carrera industrial por la inteligencia artificial (IA). Solo en el primer mes de 2025 se ha producido una sucesión de notas de prensa separadas solo por unos pocos días, a veces hasta unas pocas horas: al anuncio conjunto del nuevo Gobierno de EE. UU., OpenAI, Softbank, Oracle y MGX de la creación de una empresa denominada The Stargate Project con una inversión prevista de 500.000 millones de dólares y la firma por Donald Trump dos días después de una orden de eliminación de “barreras” al liderazgo americano en IA (se refería a retirar la orden ejecutiva de su antecesor de octubre de 2023 sobre un desarrollo y uso seguro y confiable de la IA y a establecer un Plan de Acción de la IA) le siguió el anuncio de DeepSeek R1, un modelo open source chino que muestra un rendimiento muy superior a los modelos de la competencia (el consumo de energía será un caballo de batalla en la industria de la IA en breve, ya se ha dicho en anteriores artículos de esta misma sección), y luego el anuncio de la Comisión Europea de una inversión de 37,4 millones de euros en el modelo OpenEuroLLM.



“

El informe Draghi basa la estrategia competitiva europea en tres grandes transformaciones: la reducción de la brecha de innovación, la descarbonización y la seguridad económica



A los que por cuestiones laborales estamos viviendo todo esto de cerca ni Deepseek ni OpenEuroLLM nos resultaban del todo desconocidos, pero la rápida sucesión de notas de prensa muestra el interés geopolítico de los avances de la IA. ¿Y cómo podemos aprovechar desde la industria europea las oportunidades que nos brinda la IA para nuestro desarrollo económico?

En primer lugar, debemos dejarnos de complejos “regulatorios”: decir que la regulación europea de la IA impide que innovemos es como decir que la regulación de la industria farmacéutica no nos deja innovar, olvidando que tenemos empresas como Novo Nordisk, Sanofi o Menarini que son grandes innovadores en su sector.

Lo que sí deberíamos tener en cuenta es que para tener éxito y ocupar posiciones destacadas en la carrera de la IA necesitamos inversores que crean en el proyecto, y ahí sí que quizá el mercado europeo no maneje cifras tan grandes como el norteamericano o el chino.

Un dato clave que se menciona en el informe Draghi es que la estructura industrial europea es estática: la UE alberga a empresas con una capitalización bursátil mayor de 100.000 millones de euros, pero casi ninguna se ha creado desde cero en los últimos 50 años (quizá Spotify sea una de las pocas excepciones).

Además, son empresas en sectores “tradicionales”, automóviles, medicamentos, ... Si miramos en EE. UU., las tres primeras empresas por capitalización bursátil son tecnológicas, un sector que exige una mayor inversión en I+D+i.

Ahora mismo, con la quinta revolución industrial acelerada por la IA (ver Diario de Una Tortuga Ninja de febrero de 2024), Europa tiene una nueva oportunidad para ganar posiciones innovando. Para ello, según el ya mencionado informe Draghi, es fundamental apostar por la educación en estas tecnologías.

Además, esto mejoraría nuestra soberanía y, dado que la IA es algo transversal, podría estar ayudando a innovar en otros campos en los que sí destacamos como la robótica, la ciberseguridad, la energía o la farmacia.

Es decir, que aumentar la inversión y la educación en el desarrollo y el uso de sistemas de IA eficientes, transparentes y confiables nos permitiría cerrar la brecha de innovación existente en la actualidad, aumentando el dinamismo empresarial, e integrando estos sistemas en industrias existentes.

El último informe del World Economic Forum sobre el futuro del trabajo, publicado en enero de 2025 afirma que se perderán 92 millones de puestos de trabajo en los próximos años pero se crearán 170 millones más. Esto es lo que se juegan los ciudadanos europeos en el futuro más cercano.

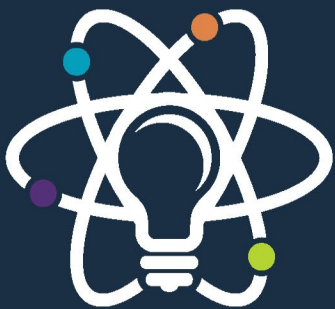
Así pues, invitamos a nuestros lectores y a nuestra tortuga ninja a no ser meros espectadores, sino los directores y directoras de la película de nuestras vidas. Nos leemos en el próximo número.

Gov Book

Governance

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

¿Por qué un Espacio Europeo de Datos de Salud?.

En diciembre de 2019 la Comisión Europea encarga a la Comisaria para la Salud y Seguridad Alimentaria que trabaje en la creación de un Espacio Europeo de Datos de Salud con el objetivo de promover el intercambio de datos de salud y apoyar la investigación de nuevas estrategias de prevención de enfermedades. Ya ven, justo antes del pico más alto de la pandemia de COVID-19.

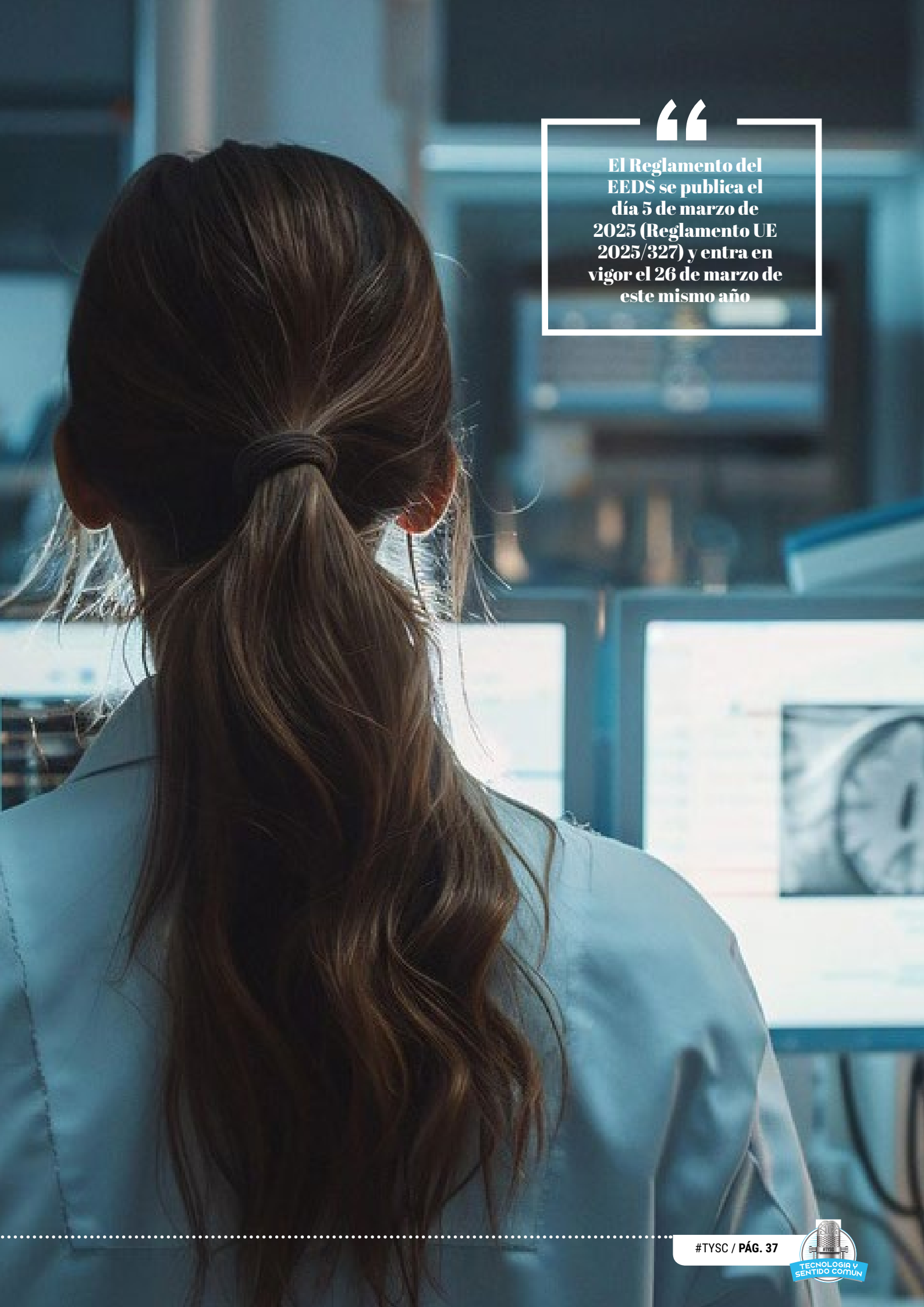
En realidad, esto formaba parte de una estrategia de la Comisión para crear espacios de datos de valor con distintos grados de apertura en diversas áreas estratégicas, como la movilidad, la energía, las finanzas o la fabricación industrial.

La primera propuesta del Espacio Europeo de Datos de Salud (en adelante, EEDS) se publicó en mayo de 2022, y desde entonces ha ido evolucionando hasta este momento, con su publicación el día 5 de marzo de 2025 (Reglamento UE 2025/327) y su entrada en vigor por tanto el 26 de marzo de este mismo año.

¿Cómo nos afecta esto como **ciudadanos**? Bueno, en principio el EEDS permitirá a los pacientes un acceso más sencillo a sus datos de salud en toda Europa y un mayor control sobre el uso de estos, lo que mejorará la calidad de la atención sanitaria que se les presta, incluso debe permitirse que añadan su propia información a su historia clínica, aunque esta debe diferenciarse claramente de la aportada por el profesional. El uso de estos datos para investigación también puede acelerar el avance científico y descubrir nuevos tratamientos o mejorar los existentes. Además nos permitirá estar mejor preparados ante amenazas para la salud pública, como la pasada pandemia.



CONTINÚA EN
PRÓXIMA PÁGINA



**El Reglamento del
EEDS se publica el
día 5 de marzo de
2025 (Reglamento UE
2025/327) y entra en
vigor el 26 de marzo de
este mismo año**



¿Cómo puede afectar a los **prestadores de asistencia sanitaria**? Además de los beneficios de cara a la investigación antes mencionados y por tanto para un tratamiento más eficaz y eficiente a los pacientes, el EEDS aplica los principios FAIR a los datos de salud (estos han de ser fáciles de encontrar, accesibles, interoperables y reutilizables), lo que les permitirá atender mejor a los pacientes, accediendo a su historia clínica a través de MiSalud@UE aunque estos estén siendo tratados por otros prestadores de asistencia sanitaria. Sin embargo, es cierto que para ello también tienen que poner de su parte y conectar sus sistemas de información con el punto de contacto nacional de su país.

También las farmacias (físicas u online) estarán conectadas para poder dispensar recetas electrónicas expedidas en otros Estados miembros.

¿Cómo afecta a las **empresas proveedoras de tecnología**? Pues ciertamente son las más afectadas. Aunque se les da de plazo hasta marzo de 2029 para poner a punto sus sistemas informáticos de historia clínica electrónica (HCE), a los que trabajamos en este sector no se nos escapa que el reto es importante: en un sector tradicionalmente “estable” y con clientes “cautivos” esto puede ser una revolución si no se reacciona a tiempo, ya que los sistemas de HCE deben cumplir unas condiciones de interoperabilidad, seguridad y registro indicadas por el Reglamento, además de disponer de una documentación técnica y de usuario para poder certificarse. Si un sistema

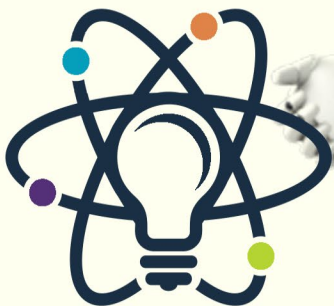
de HCE no cuenta con dicha certificación, este no se podrá introducir en el mercado ni ponerse en servicio a partir de esa fecha. Algo similar ocurrirá con las aplicaciones de bienestar.

El Reglamento distingue entre uso primario (uso para la asistencia sanitaria propiamente dicha) de los datos de salud, a través de **MiSalud@UE**, y el uso secundario (para investigación, formulación de políticas, salud pública, etc.) de estos mismos datos a través de **DatosSalud@UE**. Ambas infraestructuras tienen sus características y sus requisitos en dicho Reglamento, pero en definitiva lo que se persigue es dar la importancia que se merece a los datos sanitarios, unos datos que, como suelo recalcar, **pueden compartirse sin deterioro y cuyo valor, aunque disminuye con el tiempo, puede aumentar con el uso y también al combinarlos con otros.**

En definitiva, si bien el Espacio Europeo de Datos de Salud introduce unas obligaciones para prestadores de asistencia sanitaria, para las autoridades nacionales de los Estados miembros y para proveedores de HCE y de aplicaciones de bienestar que quieran seguir comercializando sus productos en la Unión Europea, es un pilar importante de la estrategia de la Unión Europea para mejorar la calidad de vida de los ciudadanos y para reforzar el avance científico, algo que para nuestros lectores de este lado del charco y para nuestra tortuga ninja va a ser muy relevante en los próximos años.

CoE Book

Centres of Excellence Body of Knowledge P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**



“

Un sistema de IA para la salud debe asentarse sobre uno o varios de los tres ejes (calidad, accesibilidad y costes) para ofrecer beneficios destacables



IA y Salud: lo que nos está costando ver (y resolver)

Al sistema sanitario le ha surgido un nuevo desafío, por si no tenía bastantes: parece que la inteligencia artificial (IA) ha llegado para salvar al sistema de salud, lo que ocurre es que no es la primera vez que aparece alguna tecnología salvadora que luego muestra sus limitaciones, por rendimiento, por costes, por la solvencia... En definitiva, porque como Peter Drucker decía refiriéndose a los hospitales, el sistema sanitario es la organización humana más compleja de gestionar.

Esta complejidad obedece a factores como las diferentes partes involucradas (pacientes, familiares, profesionales sanitarios, proveedores de asistencia sanitaria, aseguradoras, etc.), el alto volumen de interacciones de cada uno de esas partes involucradas y la trascendencia de estas, el gran número de profesiones que dependen unas de las otras (médicos, enfermeras, farmacéuticos, administrativos, etc.), y porque cada paciente es un caso, dificultando la estandarización y la escalabilidad de cuidados.

Sin embargo, conocemos las metas de cualquier organización sanitaria: proporcionar una asistencia de la máxima calidad siendo accesible para los pacientes y al mismo tiempo ejerciendo un control sobre los costes que asegure la sostenibilidad del sistema.

Pero por si esto fuera poco, el sector sanitario está siendo constantemente asediado por los ciberdelincuentes y ciberterroristas, como hemos comentado aquí en anteriores ocasiones.

Y entonces ¿qué puede aportar la IA al sistema de salud? Un sistema de inteligencia artificial para la salud debe asentarse sobre uno o varios de los tres ejes anteriores (calidad, accesibilidad y costes) para ofrecer beneficios destacables al sistema de salud.



CONTINÚA EN
PRÓXIMA PÁGINA

Sin embargo, para abordar la calidad asistencial con mayor accesibilidad los sistemas de IA y con un coste razonable, deberán acceder a los sistemas de información corporativos donde se encuentran los datos de los pacientes (historia clínica electrónica, laboratorio, farmacia, radiología, facturación, etc.) y asegurar al mismo tiempo que cumplen con el marco regulatorio y legal (Reglamento (UE) 2024/1689 de inteligencia artificial, Reglamento (UE) 2016/679 de protección de datos, Reglamento (UE) 2022/2555 NIS2, Reglamento (UE) 2017/745 MDR, ISO/IEC 42001, ISO/IEC 23894, ...).

¿Y cuáles son los principales retos de la aplicación de la IA al campo de la salud?

Podríamos empezar hablando de la **calidad y accesibilidad de los datos** para que los modelos entrenados que pasan a formar parte de los sistemas de IA tengan suficiente fiabilidad y sean robustos. A menudo los datos que usamos para entrenar u operar los sistemas de IA no son de la calidad necesaria o incluso hay datos que no tenemos.

Seguiríamos hablando de la **explicabilidad**: si un sistema de IA toma una decisión que afecte a uno o varios pacientes, debería mostrar cómo ha llegado a esa decisión, para permitir a los humanos saber cómo ha llegado el sistema a una decisión determinada, sea o no correcta. Solo con un buen grado de explicabilidad vamos a poder auditar el funcionamiento de estos sistemas y justificar también sus decisiones ante terceros.

Por supuesto, estos sistemas de IA deberán conseguir una **validación clínica** antes de ser usados, y en muchos casos sin embargo están dando muestras de que un buen funcionamiento en un hospital no ofrece garantías de que al ser usado en otro hospital alcance unos resultados similares.

Cuando hablamos de algo tan serio como las vidas humanas o el bienestar de las personas es fundamental que la **responsabilidad ética y legal** de los resultados esté bien acotada, ya que en caso de que el sistema de IA cometa un error con un paciente ¿quién es el responsable legal? ¿el fabricante de software? ¿el contratante? ¿el profesional sanitario?

Finalmente, la **sostenibilidad económica y social** también es clave: existen sistemas de IA que, por su propio diseño, requieren un consumo elevado de recursos. También pueden generar desigualdades que podrían acabar generando no solo un sistema de salud



de primera y de segunda, sino unos profesionales de primera y de segunda por un doble motivo: en primer lugar al sustituir los júnior por los sistemas de IA se “rompe la tubería” que lleva a los júnior a convertirse en sénior ya que no tienen oportunidad de adquirir la experiencia práctica necesaria, siendo cada vez los profesionales sénior más escasos y cotizados, y en segundo lugar puede ocurrir una erosión de las capacidades clínicas conocida por deskilling, provocando el uso de sistemas de IA la pérdida de habilidad manual o cognitiva de los profesionales. Es justo lo que nos ha sucedido a muchos con el GPS y nuestro sentido de la orientación.

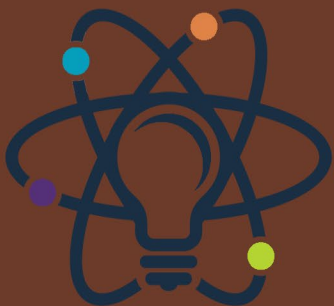
Como verán nuestros estimados lectores y lectoras y por supuesto también nuestra tortuga ninja, quedan otros retos en nuestro tintero digital, pero los señalados en este artículo consideramos humildemente que son los más importantes a abordar y que necesitan colaboración de todas las partes involucradas indicadas al principio de esta sección. Es posible que no haya una solución simple e inmediata, pero si nos ponemos a pensar fuerte ahora que todavía no tenemos esa “erosión” de capacidades cognitivas estoy seguro de que podremos encontrar soluciones satisfactorias, ¿acaso no ha sido siempre así?

PMO Book

Management Offices

Body of Knowledge

P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**



Todo a la vez en todas partes... ¿y sin control?: la amenaza de la IA ubicua

Decir que usas inteligencia artificial hoy es como decir que vas al gimnasio: muchos lo afirman, pocos lo hacen de verdad, y solo una minoría obtiene resultados visibles. Pero el caso es que está ahí, y que no podemos (ni debemos) ignorarla.

Se cumplen diez meses de la entrada en vigor del Reglamento Europeo de la Inteligencia Artificial (Reglamento UE 2024/1689 de la IA). Diez meses en los que algunos han aprovechado para echarse las manos a la cabeza porque, según ellos, “la regulación perjudica la innovación”, como si la industria farmacéutica, un sector ampliamente regulado, no innovara. La regulación solo perjudica la mala innovación: la innovación que no tiene en cuenta los derechos y el bienestar.

Como muchas otras tecnologías, su uso puede entrañar riesgos, riesgos que vamos a desgranar brevemente en este artículo para el interés (esperamos) de nuestras lectoras y lectores.

Ya existe un cuerpo abundante sobre los riesgos existentes en los sistemas de IA, algunos heredados de los sistemas informáticos en general, puesto que no dejan de serlo, pero las particularidades de los sistemas de IA han hecho que entidades como MITRE, ENISA, o NIST hayan hecho unas guías específicas sobre riesgos en los sistemas de IA. Incluso contamos con normas, en concreto con la norma ISO 23894, norma en cuya adaptación al español he tenido el privilegio de participar, y hasta una regulación europea, como ya hemos mencionado anteriormente.



CONTINÚA EN
PRÓXIMA PÁGINA

A low-angle, upward-looking photograph of a person climbing a thick rope. The person is silhouetted against a bright, cloudy sky. They are wearing a harness and are in the middle of a pull, with one hand on the rope above and the other below. The rope is part of a larger structure, possibly a climbing wall or a zipline.

**Decir que usas IA hoy
es como decir que vas
al gimnasio: muchos
lo afirman, pocos
lo hacen de verdad,
y solo una minoría
obtiene resultados
visibles**



En primer lugar, como corresponde a cualquier gestión de los riesgos, debemos identificar los activos a proteger, en este caso, desde un punto de vista organizativo tenemos activos tangibles como los datos, los modelos y el propio sistema de IA, y los intangibles, como la reputación y la confianza en nuestra organización.

Desde un punto de vista de las personas, los activos intangibles pueden ser su privacidad o su seguridad, y los tangibles sus propios datos personales.

Finalmente, desde el punto de vista de la sociedad, algunos activos intangibles podrían ser las creencias, la equidad o el acceso a la atención sanitaria, al mercado laboral o a la educación, y un activo tangible podría ser por ejemplo el medio ambiente.

La organización, las personas, los procesos, los datos de entrenamiento o la configuración del propio sistema de IA, entre otros, pueden ser orígenes de estos riesgos. La realidad es que hay estudios que indican que más del 50% de interacciones de los usuarios con chatbots basados en IA incluyen información personal sensible, y que más del 11% de empleados en las organizaciones comparte información confidencial de su empleador con estos chatbots.

Esto aumenta el atractivo de los sistemas de IA para los ciberdelincuentes, y algunas de las estrategias habituales para atacar estos sistemas van desde la inyección de prompts en sistemas de IA generativa al envenenamiento de los datos o del modelo y los ataques de cadena de suministro.

Además, están los ataques tradicionales que se ven potenciados por la IA, como los ataques de denegación de servicio, los ataques de phishing o los deep fakes. Ya hemos visto que la IA tiene una facilidad enorme para imitar nuestra voz y nuestra cara, incluso nuestra forma de escribir.

Pero también tenemos riesgos que no aparecen intencionadamente, sino de manera inadvertida, como los que resultan de la introducción de información sensible por parte de los usuarios, el manejo inapropiado de los resultados, o un exceso de confianza en los resultados (imagínense un sistema de IA que acierta un 85% de las veces, ¿creen que el usuario va a revisar los resultados con la meticulosidad necesaria cuando las últimas 85 veces el sistema ha dado el resultado correcto?).

Pensemos en las organizaciones que prohíben el uso de la IA ¿es realista pensar que nuestros empleados no van a encontrar una manera, a través de su ordenador, de su móvil o de cualquier otro dispositivo de utilizar la IA para ahorrarse trabajo? Intentar limitar su uso es como ponerle cadenas al aire, y esto no va a mejorar...

Además, ¿se imaginan cómo de productivos pueden ser sus competidores, suponiendo una capacitación similar de sus trabajadores, haciendo uso de los sistemas de IA mientras su organización los prohíbe?

Por todo esto es importante que las organizaciones aceleren su estrategia de concienciación y de "alfabetización" de sus trabajadores en estas herramientas para asegurar, en definitiva, un uso responsable y ético de los sistemas de IA.

Y si me permiten un segundo consejo antes de despedirme de ustedes lectores y lectoras, y de nuestra tortuga ninja, evalúen los riesgos de cualquier tecnología que incorporen a sus procesos de negocio apoyándose en profesionales expertos, también la IA, porque como dice Yudkowsky, el mayor peligro de la IA, con diferencia, es que las personas tienden a pensar que la entienden antes de tiempo.

El mayor peligro de la IA, con diferencia, es que las personas tienden a pensar que la entienden antes de tiempo

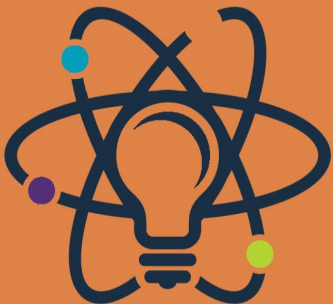
PgM Book

Programme

Management

Body of Knowledge

P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**



El problema de los tres cuerpos: ¿hacia dónde orbitará la IA?

El problema de los tres cuerpos es un problema fundamental en la física y las matemáticas, especialmente en la mecánica de los cuerpos celestes. Hace referencia al desafío de predecir el movimiento de tres cuerpos celestes (como el Sol, la Tierra y la Luna, o tres estrellas) que interactúan gravitacionalmente entre sí.

Las leyes de gravitación de Newton resolvieron el modelo de interacción entre dos cuerpos celestes, la Tierra y el Sol. Pero cuando añades un tercer cuerpo celeste, la Luna o un planeta, los tres cuerpos empiezan a tirar cada uno de los otros dos y no existe una solución analítica general y cerrada. Solo con añadir un cuerpo más, la cosa se complica sustancialmente.

Ahora pensemos en el desafío que tenemos delante: por primera vez, los sistemas de IA son accesibles para el público en general (y las organizaciones de cualquier tamaño en particular) y su impacto en nuestra sociedad puede ser altísimo, tanto en lo positivo como en lo negativo.

Además, al igual que las personas, los sistemas de IA pueden ir perfeccionándose, pero también corrompiéndose, de manera que la eficacia de un sistema de IA puede ser muy diferente un año más tarde, ya que son sistemas de información dinámicos, no estáticos como eran hasta hace poco la mayoría de sistemas de información.

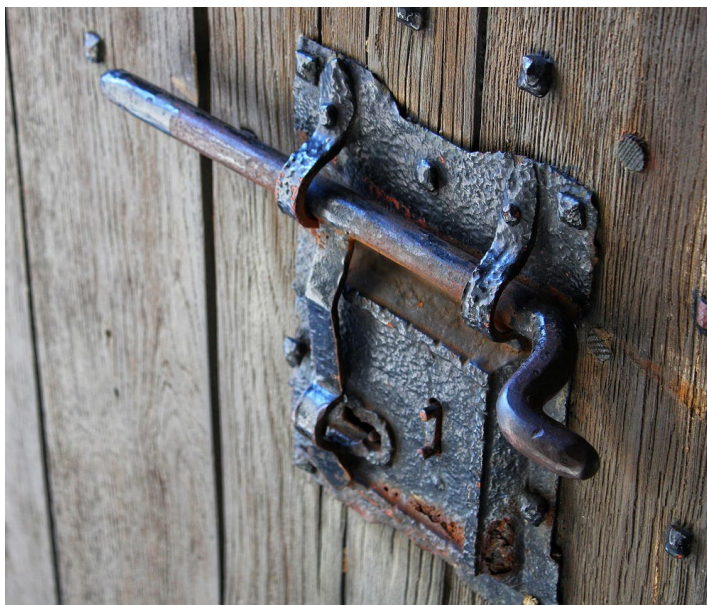


CONTINÚA EN
PRÓXIMA PÁGINA



“

La evolución de los sistemas de IA va a depender de tres cuerpos: la tecnología, la sociedad, y la regulación



Por otro lado, y también por primera vez para un sistema informático, no solo se les va a evaluar por su eficiencia y por la calidad de sus resultados, y por la protección de los datos que manejan, sino por su impacto en los derechos fundamentales, de acuerdo con el Reglamento Europeo de la IA, y en el ámbito europeo tenemos cincuenta libertades, principios y derechos fundamentales relativos a dignidad, libertad, igualdad, solidaridad, ciudadanía y justicia, según la Carta de los Derechos Fundamentales de la Unión Europea.

Llegados a este punto, ¿podemos predecir la evolución de esta tecnología en los próximos años de manera precisa o nos encontramos también aquí ante una versión del “problema de los tres cuerpos”?

La evolución de los sistemas de IA en el mundo que conocemos va a depender, en efecto, de tres cuerpos, aunque no sean “celestes”: el cuerpo de la tecnología, el de la sociedad, y el de la regulación.

La tecnología se ha constituido como un cuerpo que acelera estos sistemas de IA: los avances en nuevos modelos “agénticos”, redes neuronales, etc. con nuevas técnicas de aprendizaje; los avances en hardware con cada vez mayor potencia computacional y con la llegada de la computación cuántica, y la disponibilidad cada vez más masiva de datos y nuevas formas de procesarlos, más eficientes y rápidas. La tecnología empuja los límites, crea nuevas posibilidades y, a menudo, se adelanta respecto a los otros dos cuerpos. Sus avances generan presión y oportunidades que la sociedad y la regulación deben asimilar y responder. Sin embargo, su potencia sin control puede llevar a desarrollos descontrolados o con consecuencias no deseadas.

La sociedad es el segundo cuerpo, un cuerpo con entidad propia, con culturas y valores diversos, con su gestión de unos recursos limitados para producir bienes y servicios (esta al fin y al cabo es la definición de economía), y los seres humanos que formamos parte de ella, y que nos vemos afectados por los otros dos cuerpos. La velocidad de adopción, la percepción

pública, el impacto y los valores éticos son parte de esa sociedad, que se ve afectada por la IA, pero también la presión social puede ser un factor determinante en lo que se acepta y lo que se rechaza en lo que respecta a la regulación y a la tecnología.

El tercer cuerpo es la regulación: la fuerza de este cuerpo busca el equilibrio entre los otros dos, se compone del marco legal, los estándares, las políticas públicas y las directrices éticas que buscan gobernar el desarrollo y despliegue de la IA en nuestra sociedad. La regulación intenta poner orden en el potencial caos, estableciendo límites, fomentando la innovación responsable y protegiendo los derechos y el bienestar de la sociedad, pero no es un cuerpo “estático”, sino que evoluciona en respuesta a los otros dos.

Como comentaba al principio de este artículo, las interacciones entre tres cuerpos son extremadamente complejas de modelar analíticamente y pueden tener consecuencias altamente peligrosas, y también beneficiosas.

Pero como sociedad no podemos permitirnos ser conformistas, al contrario, debemos ser conscientes de que podemos, y debemos, actuar sobre estos tres cuerpos. Somos todos nosotros y nosotras los que debemos adoptar una conducta responsable y exigir una IA segura y confiable, porque ni la tecnología, ni la sociedad, ni la regulación pueden existir al margen de los derechos humanos.

Y con este cierre, que no puede resolver pero sí intentar anticipar humildemente el futuro más cercano, llegamos al último artículo del diario de nuestra querida tortuga ninja en Tecnología y Sentido Común. A aquellas personas que hayan llegado hasta aquí, mi enhorabuena, mi agradecimiento, y mis deseos de que pasen un muy feliz verano.

**“
Ni la tecnología, ni
la sociedad, ni la
regulación pueden
existir al margen
de los derechos
humanos**”

¿Entregas Caóticas?
¿Insatisfacción con los resultados?
¿Descoordinación de esfuerzos?
¿Ausencia de progreso o incumplimiento de plazos?
¿Falta de visión de la actividad transformadora?



Regularidad, progreso y cumplimiento
Entregas predecibles y satisfactorias
Credibilidad en la actividad transformadora
Claridad de responsabilidades
Ganancia rápidas y logros que motivan



soluciones@p4mgo.com
<https://p4mgo.com>

Cierre de Temporada 2025 Revistas “Tecnología y Sentido Común” y “Stakeholders.news”

El Evento de Cierre de Temporada 2025 de las Revistas “Tecnología y Sentido Común” y “Stakeholders.news” celebrado el viernes 11 de julio quedará grabada en la memoria de todos los asistentes como una fecha especial, no solo por marcar el cierre de la décima temporada de dos revistas de referencia, sino por condensar, en un solo acto, el espíritu de una década entera de trabajo, aprendizaje y crecimiento compartido. La sede de UNE, la Asociación Española de Normalización, se impregnó desde bien temprano de un ambiente animado, mezcla de solemnidad y calidez. Al abrirse las puertas, la sensación era la de asistir a una gran reunión de familia profesional, un reencuentro anual que cada vez gana en prestigio, asistencia y profundidad de lazos personales.

La bienvenida, realizada por Javier Peris en su doble faceta de director de ambas revistas, así como por Fernando Machicado en representación de la entidad que acoge el evento, marcó el tono de la mañana. Ambos recordaron a los presentes que, más allá del recuento de logros o de un simple cierre de curso, el encuentro de final de temporada persigue renovar el compromiso de todos los que integran las comunidades de Tecnología y Sentido Común y Stakeholders.news, ya sea desde la primera línea como expertos, columnistas y responsables de áreas, o desde la imprescindible labor de los lectores y socios estratégicos. Subyacía en sus palabras la presencia constante de la tradición, compañera inseparable de toda evolución significativa, así como la importancia de la normalización y la excelencia, valores irrenunciables para el futuro inmediato del sector.



CONTINÚA EN
PRÓXIMA PÁGINA

Suscríbete gratis

REVISTA MENSUAL DE DIRECCIÓN Y GESTIÓN DE PROYECTOS, PROGRAMAS Y PROYECTOS

Stakeholders .news

PORTFOLIO, PROGRAMAS Y PROYECTOS MANAGEMENT

NÚMERO 11 DICIEMBRE 2022

PROTAGONISTA DEL MES

MARC
RUGHMANS

FONDOS, ESTOS LÓBOS

PRENDIDAS

REGULARES

U

VER EN CUENTA

NO

V DIGITAL

CIÓN

ESCA PARA

ISO 51.000

Even
CIER
Revista
y "Stak

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Stakeholder

En este contexto, la primera intervención de la jornada adquiere todo su sentido. Elena Ordozgoiti, responsable de negocio del sector servicios de UNE, supo captar la atención de la sala no solo con datos y argumentos, sino con una visión estratégica que puso de relieve el papel esencial que juega la normalización en el desarrollo de las industrias, las administraciones y, en definitiva, en la vida cotidiana de la población.

Ordozgoiti explicó la compleja red de colaboraciones y sinergias entre los organismos nacionales, europeos y globales de normalización, y cómo la participación española en el Subcomité CTN 309/SC 01 ha permitido situar a nuestro país en la vanguardia de la excelencia. Destacó también el profundo impacto de la normalización en la generación de confianza, interoperabilidad y competitividad, recordando que el establecimiento de estándares no es solo una labor técnica, sino también ética y social. Su exposición abierta y comprometida no solo resultó didáctica, sino que afianzó la convicción de la audiencia sobre la necesidad de participar activamente en la construcción de estándares de calidad para el conjunto de la sociedad.

Así, la meta de facilitar marcos de referencia sólidos se presenta como una oportunidad estratégica de futuro, y una responsabilidad compartida por todos los presentes, desde los autores de artículos hasta quienes ocupan responsabilidades de dirección y toma de decisiones.



CONTINÚA EN
PRÓXIMA PÁGINA

CIÓN DE PORFOLIOS, PROGRAMAS Y PROYECTOS

holders

.news

AGEMENT

CONISTA DEL MES

MARC
BERGHMANS

NDOS, ESTOS LODOS

PRENDIDAS

INGULARES
ega

NER EN CUENTA

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

años, de 1470 a 1484

El tono inspirador de la mañana se mantuvo durante la intervención de Marcelino Lominchar, cuyo discurso supuso un viaje inesperado, enriquecedor y muy humano por la historia de España. A partir de los relatos recogidos en su obra "Historias de la Historia de España", Lominchar desenmascaró mitos, ofreció detalles sorprendentes y recuperó figuras cuyo legado ha sido frecuentemente eclipsado por prejuicios y narrativas ajenas.

Lejos de limitarse a una crónica tradicional, su charla estuvo plagada de guiños al presente, extrayendo lecciones de gestión, resiliencia y liderazgo de episodios históricos. Sorprendió a los presentes mostrando monedas icónicas como el real de a ocho o el maravedí, verdaderos símbolos de la pujanza hispánica que influyeron decisivamente en la economía global. Detalló cómo personajes como Colón o Magallanes debieron desplegar una impresionante cantidad de habilidades de persuasión para sacar adelante sus proyectos, anticipándose así a lo que actualmente conocemos como gestión del cambio, emprendimiento y defensa de la innovación.

Pero uno de los momentos más celebrados de su exposición fue la reivindicación de Gonzalo Fernández de Córdoba, el Gran Capitán, a quien Lominchar atribuyó – con sólidos argumentos – la invención de una suerte de "agilismo" aplicado al arte de la guerra y, por extensión, a la administración y gestión de proyectos en épocas de incertidumbre.



CONTINÚA EN
PRÓXIMA PÁGINA



STA

logía & Común



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Estas reflexiones sirvieron de nexo para el siguiente bloque de la jornada, la mesa redonda en la que participaron siete colaboradores de las revistas, una suerte de gabinete de expertos en el que confluyeron voces de disciplinas tan variadas como la inteligencia artificial, el derecho, la gestión pública y la creatividad.

El diálogo, hábilmente moderado por Javier Peris, permitió repasar aquellas tendencias, inquietudes y expectativas que han marcado el último año editorial. Los ponentes compartieron reflexiones sobre cómo escogen sus temas, cómo detectan tendencias y qué importancia conceden al rigor y a la originalidad a la hora de abordar asuntos de actualidad, desde la expansión de la inteligencia artificial hasta los desafíos regulatorios o el potencial transformador de la creatividad en los procesos de cambio. Hubo consenso respecto a la urgente necesidad de que la sociedad saque partido a las mentes

divergentes, esas voces innovadoras, a menudo incómodas pero imprescindibles para que cualquier organización y ecosistema profesional pueda reinventarse y crecer.

Muy lejos de un debate corporativo y riguroso, en varios momentos la conversación adoptó un tono cercano y humorístico, rebajando la solemnidad y recordando la importancia del factor humano para el éxito de cualquier iniciativa. Se insistió en la importancia de mantener la independencia intelectual de los colaboradores, de seguir apostando por la pedagogía aplicada y de construir puentes de entendimiento entre generaciones y perfiles profesionales muy distintos.



CONTINÚA EN
PRÓXIMA PÁGINA



TECNOLOGÍA Y SENTIDO COMÚN

12:15 a 13:00

					
RICARD MARTÍNEZ	ALEJANDRO ALIAGA	MARLON MOLINA	MARCOS NAVARRO	VICTOR ALMONACID	MARTA MARTÍN
Sección: Ojo al dato	Sección: Radio Security	Sección: Es Tendencia	Sección: AI Futuro	Sección: La Nueva Administración	Sección: Mentes Divergentes

Susíbete gratis

REVISTA

Tecnología & Sentido Común

2022

PREMIOS SAPIENS



REVISTA

Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>

La mañana prosiguió con la segunda de las mesas redondas, en este caso consagrada a la comunidad internacional de Stakeholders.news.

La mesa reunió tanto a colaboradores presentes como a los corresponsales internacionales, que aportaron sus reflexiones en formato de mensaje grabado, conectando así Madrid con América Latina y el Caribe.

Entre los aspectos más destacados del debate figuraron las diferencias regionales en la percepción y aplicación de la innovación social y empresarial, el impacto de la regulación en los procesos de sostenibilidad y la creciente importancia de la ética, la transparencia y las alianzas multinacionales.

Cada colaborador expuso aquello que considera el mayor aporte de su sección durante el año, detallando no solo las temáticas, sino también las reacciones suscitadas entre los lectores y el valor añadido de contar con una red plural y cosmopolita. La interacción entre moderador y ponentes sirvió para poner de manifiesto la transversalidad de los retos contemporáneos y la urgencia de compartir aprendizaje y experiencias más allá de fronteras y disciplinas.



CONTINÚA EN
PRÓXIMA PÁGINA



MESA REDONDA
moderada por Javier Per



LUIS
MORÁN

Sección:
Personas Y
Procesos



#TYSC / PÁG. 60

Sharing

13:00 a 13:30

DA "STAKEHOLDERS.NEWS"

					
JOSE ANTONIO PUENTES	JOSE LUIS PORTELA	RICARDO SASTRE	LUIS GUARDADO	NESTY DELGADO	DANIEL SOROKINS
Sección: Tendencias Puentes	Sección: Empleo y Futuro	Sección: Super PMO	Embajador: El Salvador	Embajador: Puerto Rico	Embajador: Uruguay



Suscríbete gratis

REVISTA

Tecnología & Sentido Común

#10

2022 PREMIOS SAPIENS

Llanos Cuenca

NUESTRA INVESTIGACIÓN A FUTURO

Talento y Liderazgo

Es tend

Alejandro Blasco

La nueva Administración

Por Procesos

Consejo de amigo

REVISTA

Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>

REVISTA

Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>



Este espíritu de apertura y renovación se evidenció de nuevo durante la presentación en sociedad de los nuevos colaboradores y secciones que integrarán la próxima temporada.

El público recibió con interés las propuestas de Domingo Gaitero, dispuesto a arrojar luz sobre la cara más amenazante y menos conocida de la ciberseguridad; la de Angie López Gea, quien acercará la cultura hacker a lectores de todas las edades; y la de Ismael Novo, que analizará el impacto y las aplicaciones prácticas de la inteligencia artificial en los negocios. A ellas hay que sumar la presencia internacional de Estuardo Castañeda, que aportará un enfoque desde Centroamérica mediante contenidos audiovisuales.

Estas nuevas incorporaciones dan fe de la apuesta continua de ambas revistas por la renovación, la pluralidad y el abordaje de tendencias emergentes con relevantes implicaciones sociales y culturales.



CONTINÚA EN
PRÓXIMA PÁGINA

Suscríbete gratis

DIRECCIÓN Y GESTIÓN DE PORFOLIOS, PROGRAMAS Y PROYECTOS

Stakeholders

.news

PROGRAMME & PROJECT MANAGEMENT

NOVIEMBRE #011 - NOVIEMBRE 2022

»» STAKEHOLDERS.NEWS

PROTAGONISTA DEL MES

MARC BERGHMANS

DE AQUELLOS FONDOS, ESTOS LOGROS
en EDITORIAL
con Javier Paris

LECCIONES NO APRENDIDAS
DE LA PANDEMIA
en PROYECTOS SINGULARES
con Carlos Pampliega

DIMENSIONES A TENER EN CUENTA
EN UN PROCESO (SERIO)
DE TRANSFORMACIÓN DIGITAL
en TECNOTRANSFORMACIÓN
con Juan Jesús Urbizu

ESTÁNDARES DE REFERENCIA PARA
LA GESTIÓN DE RIESGOS ISO 21.000
en STEERING COMMITTEE
con Pedro Balas

¿CÓMO MEDIMOS LA RESILIENCIA
DE LAS ORGANIZACIONES?
en ORGANIZACIONES RESILIENTES
con Juan Manuel Domínguez

LAS PMOS EN EL METAVERSO
en SUPER PMOS
con Ricardo Sastre

CONTRATOS ÁGILES
en TRANSFORMACIÓN ÁGIL
con Ángela Plaza

¿CÓMO GENERAR AUTORIDAD
COMO INTERIM MANAGER?
en EMPLEO Y FUTURO
con José Luis Portella

MANEJANDO LAS EXPECTATIVAS
DE UN PROYECTO
en EL LADO HUMANO
con Chayo Fresneda

ENTOCARSE EN EL BIEN SER DE LA
PERSONAS, UNA DIMENSIÓN MÁS
HUMANA DENTRO DE LA DIRECCIÓN
en PROYECTOS
con Chayo Fresneda

51 8



#TYSC / PÁG. 62

13:30 a 13:45

NUEVOS COLABORADORES



**DOMINGO
GAITERO**
El lado oscuro
(TVSC)



**ESTUARDO
CASTANEDA**
Guatemala
(Stakeholders.news)



**ANGIE
LOPEZ GEA**
Hack & News
(Stakeholders.news)



**ISMAEL
NOVO**
Power AI
(Stakeholders.news)





Uno de los momentos más esperados de la mañana fue, como cada año, la entrega de los premios anuales con los que ambas publicaciones reconocen la labor de personas y entidades fundamentales para el progreso del sector. El Premio Tecnología y Sentido Común 2025 recayó sobre la Subdirección de Sistemas de Información del Hospital Universitari i Politècnic La Fe, una distinción más que merecida por su firme compromiso con la modernización digital, la eficiencia clínica y, sobre todo, la calidad asistencial a través de soluciones tecnológicas innovadoras.

Cayetano M. Hernández Marín recogió el premio en nombre de todo su equipo, acompañando el agradecimiento con un breve y emotivo discurso de gratitud, memoria y optimismo, recordando que todo avance tecnológico es, en última instancia, una apuesta por el bienestar del paciente y la dignidad del profesional sanitario.

En el ámbito de la responsabilidad social, Stakeholders.news reconoció a la Fundación The Pink Force por su extraordinaria iniciativa de acompañamiento emocional a niñas en tratamiento oncológico, haciéndolo en colaboración con el entrañable droide rosa R2-KT, inspirado en la historia real de Katie Johnson. El momento en que Andoni Serrano y el propio R2-KT se acercaron al estrado fue, sin duda, uno de los capítulos más conmovedores del evento. La ovación que recibieron, sincera y prolongada, recordó a todos que la tecnología, por avanzada que sea, solo tiene sentido cuando se pone al servicio de las personas más vulnerables.



**CONTINÚA EN
PRÓXIMA PÁGINA**

Suscríbete gratis

REVISTA MENSUAL DE DIRECCIÓN Y GESTIÓN DE PORTFOLIOS
Stakeholders

PORTFOLIO, PROGRAMME & PROJECT

NÚMERO #011 - NOVIEMBRE

PROYECTOS · GESTIÓN · EXCELENCIA · CALIDAD · PROFESIONALES



ENTREGA DE PREMIOS

PREMIO REVISTA

**Tecnología &
Sentido Común**
20

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Llegados a este punto de la jornada, la sucesión de testimonios espontáneos, agradecimientos y recuerdos personales dibujó un ambiente único de comunidad y pertenencia. Los asistentes revivieron anécdotas de pasadas ediciones, mencionaron logros y desafíos superados, e incluso hubo espacio para la emoción y la lágrima compartida, fruto del profundo compromiso y afecto construido entre los colaboradores. Se homenajeó también la memoria de quienes, por motivos personales o profesionales, no pudieron estar presentes, dejando constancia del legado intergeneracional que caracteriza a las revistas.

La mañana se cerró, como manda la tradición, con un exclusivo catering que sirvió para prolongar la conversación y multiplicar las oportunidades de networking. Con mesas repletas de propuestas gastronómicas, la comunidad disfrutó de un momento de distensión en el que las fronteras jerárquicas desaparecen, permitiendo una interacción franca y productiva entre autores, lectores, directores, expertos y nuevos colaboradores. Este ambiente informal y dinámico, lejos de ser un simple complemento social, se ha revelado como uno de los espacios más fructíferos para el surgimiento de ideas, proyectos y futuras colaboraciones.

Culminado el acto, lo que queda es mucho más que el recuerdo de una celebración o el repaso a una década de publicaciones: es precisamente la constatación de que detrás de cada artículo, cada premio, cada panel y cada colaboración hay una apuesta decidida por el humanismo tecnológico, la ética profesional y la convicción de que el conocimiento debe ser compartido, discutido y puesto en acción colectiva. La décima edición del evento de cierre de temporada de Tecnología y Sentido Común y Stakeholders.news se reafirma, así, como un espacio de encuentro, inspiración y referencia para el ecosistema innovador en habla hispana.

El horizonte que se adivina tras esta cita es aún más prometedor. Los desafíos de la próxima década serán, si cabe, todavía más complejos y apasionantes. Nuevos colaboradores y lectores se sumarán a la conversación, las disciplinas seguirán expandiéndose y las alianzas, tanto nacionales como internacionales, pondrán a prueba la capacidad de adaptación, resiliencia y sentido común de toda la comunidad. Pero, como quedó patente a lo largo de toda la jornada, si algo distingue a los protagonistas de esta historia es su voluntad de cielo abierto y mirada larga. Porque, en definitiva, la tecnología y el compromiso social solo son motores de cambio si encuentran a mujeres y hombres dispuestos a caminar juntos, sumar talento y soñar, cada día, una sociedad mejor.



**Curso de
Certificación en:**

Gobierno Corporativo

**ISO 37000
Corporate
Governance
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695€
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>

UNE presenta su Estrategia 2030 para lograr un mayor impacto de las normas en la sociedad

Se basa en tres objetivos estratégicos: poner el conocimiento recogido en las normas al servicio del progreso compartido de España; impulsar la comunicación sobre los beneficios de las normas y su aplicación; y aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto.

La Estrategia 2030 de la Asociación Española de Normalización, UNE, aprobada en Asamblea General por sus miembros, se basa en tres objetivos y 14 prioridades, con los que la Entidad cumplirá su propósito: contribuir al progreso compartido de la sociedad.

Para lograr la Estrategia, UNE ampliará el alcance de su actividad y generará soluciones para facilitar su aplicación, poniendo el foco en visibilizar los beneficios de los estándares: la normalización aporta un 14,7 % al crecimiento medio anual del PIB en España.

La Asociación Española de Normalización, UNE, ha puesto en marcha su Estrategia 2030, que tiene como objetivo lograr un mayor impacto de las normas en la economía y en la sociedad.

Este ambicioso plan, aprobado por los miembros de UNE en Asamblea General, se basa en tres objetivos estratégicos: poner el conocimiento recogido en las normas al servicio del progreso compartido de España; impulsar la comunicación y el apoyo a la aplicación de las normas; y aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto.

Con ellos, el Organismo español busca ampliar el alcance de la actividad de normalización y dar respuesta eficaz a los grandes desafíos de las organizaciones españolas, potenciando la generación de soluciones que faciliten su implementación; para ello, adaptará el contenido de las normas a sus necesidades con las nuevas herramientas que ofrece la digitalización y, en especial, la inteligencia artificial (IA).

El vicepresidente de UNE, Luis Rodulfo, ha señalado: “La Estrategia UNE 2030 es una hoja de ruta que marca con claridad y suficiente nivel de detalle hacia dónde debemos dirigir todos nuestros esfuerzos y capacidades los próximos años para lograr nuestro propósito: contribuir al progreso compartido de la sociedad y a la creación de un mundo más seguro, sostenible y competitivo a través del desarrollo de estándares”.

En la definición de la Estrategia UNE 2026-2030 se han contemplado los elementos que definen el contexto geopolítico, económico, digital, social, legal y medioambiental, en los que las actividades de normalización y cooperación deben contribuir a lograrla. Además, se ha contemplado la contribución de UNE y de las normas técnicas a la consecución de los 17 Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de Naciones Unidas.



CONTINÚA EN
PRÓXIMA PÁGINA

Estos objetivos estratégicos aterrizan la ambición de UNE de seguir aportando un valor único a la sociedad y a la economía española, consolidando su impacto positivo. De hecho, la normalización aporta un 14,7 % al crecimiento medio anual del PIB en España, lo que se traduce en una contribución de más de 140.000 millones de euros en las últimas cuatro décadas, según el reciente Estudio “Impacto económico de la normalización en España”, realizado por el Centro de Estrategia y Prospectiva Industrial (CEPI), entidad impulsada por el Ministerio de Industria y Turismo y la Fundación EOI.

Los tres objetivos estratégicos son:

1.Poner el conocimiento recogido en las normas técnicas al servicio del progreso compartido de España

Para lograrlo, UNE se ha marcado cinco prioridades: reforzar la Norma como un servicio para las entidades públicas y privadas; dar respuesta a los retos a los que se enfrenta la empresa española con un catálogo de normas actualizado y alineado con sus necesidades; impulsar el liderazgo internacional y europeo de la normalización española; desarrollar un ecosistema equilibrado de alianzas de colaboración entre el ámbito público, privado y la sociedad civil; y ser ejemplar en materia de buen gobierno corporativo.

UNE es depositaria del mejor conocimiento generado por los 12.500 expertos de organizaciones españolas que participan en el desarrollo de estándares en los 200 Comités UNE.

2.Impulsar la comunicación sobre los beneficios de las normas y su aplicación

UNE reforzará la comunicación sobre los beneficios de las normas y generará soluciones para facilitar su aplicación a través de cinco prioridades: incrementar la aplicación de las normas en apoyo a las Administraciones públicas para simplificar la legislación y el despliegue de políticas públicas; garantizar la adecuación del contenido de las normas a las necesidades de aplicación del mercado; impulsar la difusión y aplicación de las normas mediante la actividad de cooperación a nivel nacional, internacional y multilateral, fijando una senda de crecimiento reputacional y económico; promover la cultura de cumplimiento de las normas apoyando la vigilancia de mercado y la evaluación de la conformidad en el marco de la infraestructura de la calidad; y fortalecer la comunicación de UNE.

3.Aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto

Mediante la contribución de todos los actores de su cadena de valor. El tercer objetivo se basa en cuatro prioridades: lograr una mayor contribución económica de las Administraciones públicas a la sostenibilidad de UNE; garantizar la aportación de la explotación del contenido de las normas a la sostenibilidad de UNE en el entorno cambiante de las necesidades de los usuarios; aumentar la contribución de los proyectos de cooperación fijando objetivos de rentabilidad económica y reputacional; y analizar otras líneas potenciales de crecimiento orgánico derivadas del valor generado por UNE



**Hace mucho
tiempo que
hablas.**

**¿Pero hace
cuánto no
dialogas?**



Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

NUEVOS MASTERS

MasterPPM®
Gobierno, Dirección, Gestión y Ejecución de
Portfolios, Programas y Proyectos

MPPM®
eGob®



Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
<https://escueladegobierno.es>