REVISTA

Tecnología & Sentido Común

#67
OCTUBRE
2026



Marcelino Lominichar
NUESTRO INVITADO A #TYSC 24

El Gobernauta
JAVIER PERIS 08

Futuro y Seguridad 12
MANUEL SERRAT

Tecnoregulación en Prospectiva
NACHO ALAMILLO 16

Es tendencia
MARLON MOLINA 32

Humanos, IA, robots y otros problemas 40
MARCOS NAVARRO

La nueva Administración 44
VÍCTOR ALMONACID

El lado oscuro
DOMINGO GAITERO 20

Ojo al dato
RICARD MARTINEZ 36

Mentes Divergentes 48
MARTA MARTÍN

9 772951 818003 67

REVISTA

Tecnología & Sentido Común

EQUIPO TYSC
Javier Peris - El Gobernauta
Manuel Serrat - Futuro y Seguridad
Nacho Alamillo - Tecnoregulación en Prospectiva
Domingo Gaitero - El Lado Oscuro
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Marcos Navarro - Humanos, IA, Robots y otros problemas
Víctor Almonacid - La Nueva Administracion
Marta Martín - Mentes Divergentes

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

©2024 Business&Co.® - Todos los Derechos Reservados

9 772951 818003 67

(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

Escuela de Gobierno

eGob®

https://escueladegobierno.es

ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

LOS CURSOS DE CERTIFICACIÓN TE INVITAN A PRACTICAR CON AVENTURAS GAMIFICADAS

TRES MUNDOS, TRES AVENTURAS: ADMINISTRACIÓN PÚBLICA, EMPRESAS PRIVADAS Y STARTUPS

LA EMPRESA QUE DEJÓ A UNA IA TOMAR SUS DECISIONES DE TODOS LOS DÍAS

MUNDO: EMPRESAS PRIVADAS | CURSO: GESTIÓN DE LA INTELIGENCIA ARTIFICIAL

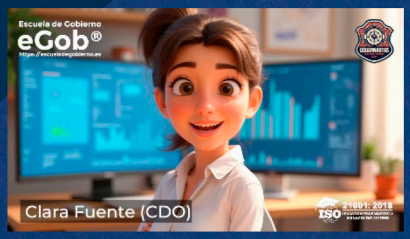
«Saludos Gobernauta.» Entra la primera videollamada y ya no hay marcha atrás. Varios sistemas de inteligencia artificial deciden sobre tus clientes, tus precios y tu dinero, y nadie responde de ellos. Cada reunión te pone delante opciones y ninguna es evidente, y la que elijas vuelve a buscarte más adelante. Al final sabrás si estás preparado para Gobernar y Gestionar la Inteligencia Artificial. ¿Aceptas el reto? Pues bienvenido a **BestPractices.Games**, donde todo lo que sucede lo decides tú.

CON QUIÉN TE VAS A TENER QUE REUNIR













- **Aprendes a decidir, a practicar.** Cada escena es una decisión de dirección, y la consecuencia llega.
- **Practica el Cambio Organizacional.** Aborda tanto la implementación como el día a día (Powered by **P4MGO!®**).
- **Gobierno y gestión, en la práctica.** Decisiones del consejo, de la dirección y la delgada línea que las separa.
- **Asume la agenda y toma el mando.** Siete episodios y un caso final, en Slots de una hora (Powered by **TSG4®**).

Vive esta experiencia en los Cursos de Certificación de la Escuela de Gobierno eGob® impartidos por Javier Peris.

Cursos en Formato Grabado con Tutorías en Directo para que, a tu ritmo, en tu horario, desde donde te encuentres y con toda comodidad puedas acceder al mejor contenido y alcanzar tu certificación.

La Visión de la Escuela de Gobierno eGob® consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

Escanea y matricúlate

BestPractices.Games es una iniciativa de **Business&Co.®** creada y dirigida por **Javier Peris** para la **Escuela de Gobierno eGob®**.

IMQ CERTIFIED QUALITY MANAGEMENT SYSTEM ISO 9001:2015

IMQ CERTIFIED MANAGEMENT SYSTEM FOR EDUCATIONAL ORGANIZATIONS ISO 21001:2018

#67

OCTUBRE 2026

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com



Marcelino Lominichar



Crónica de la XI edición de la RootedCon Valencia



La empresa del Siglo XX y los trabajadores digitales



Del caos a la oportunidad: emprender con TDAH

#67 - OCTUBRE 2026

¡hice

#TYSC

Copyright 02

Índice de Contenidos 04

Este mes te recomiedo leer...
por JAVIER PERIS 07

El Papel Higiénico no es Burocracia
EL GOBERNAUTA
JAVIER PERIS 08

Ciberseguridad en la era de la inteligencia artificial: cómo cambiará la profesión en los próximos cinco años (I)
FUTURO Y SEGURIDAD
MANUEL SERRAT OLMOS 12

Impulsando el PanEuropean Trust Framework
TECNOREGULACIÓN EN PROSPECTIVA
NACHO ALAMILLO 16

¿Por qué tantas preguntas?
EL LADO OSCURO
DOMINGO GAITERO 20

Marcelino Lominichar
NUESTRO INVITADO A TYSC 24

El contenido basura en Internet es tendencia
ES TENDENCIA
MARLON MOLINA 32

Las lecciones aprendidas en el caso Meta y el futuro de la inteligencia artificial
OJO AL DATO
RICARD MARTÍNEZ MARTÍNEZ 36

La empresa del Siglo XX y los trabajadores digitales
HUMANOS, IA, ROBOTS Y OTROS PROBLEMAS
MARCOS NAVARRO 40

En el término medio está la virtud
LA NUEVA ADMINISTRACIÓN
VÍCTOR ALMONACID 44

Del caos a la oportunidad: emprender con TDAH
MENTES DIVERGENTES
MARTA MARTÍN 48

Crónica de la XI edición de la RootedCon Valencia
EVENTOS 52

UNE celebra sus 40 años de apoyo a la industria y la sociedad
NORMALIZACIÓN 64

Premios recibidos

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



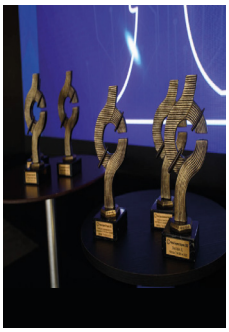
El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

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



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

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 Comuni- dad Valenciana COIICV alabó tanto la gran labor de difusión que viene realización 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.

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática



VI Premios ESET Periodis- mo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo 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.

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.

ESTE MES TE RECOMIENDO LEER…

por Javier Peris



AI Under Attack: A Practical Guide to Threats, Defenses, and Governance for AI Systems

Kris Kimmerle, David Okeyode

"IA bajo ataque: una guía práctica sobre amenazas, defensas y gobernanza para sistemas de IA", de Kris Kimmerle y David Okeyode, invita a mirar la inteligencia artificial generativa desde una perspectiva que considero imprescindible: su seguridad. Frente al entusiasmo por sus posibilidades, esta obra sitúa en primer plano las amenazas, las defensas y la responsabilidad de quienes diseñan y utilizan estos sistemas.

Lo que más me interesa de su planteamiento es que no reduce la protección a una cuestión técnica. Su recorrido conecta los fundamentos de seguridad con los ataques, la construcción de soluciones y la gestión de programas organizativos. Esa amplitud permite entender que proteger la IA exige algo más que incorporar controles.

La inyección de instrucciones, el abuso de memoria y contexto, las vulnerabilidades RAG o la explotación de agentes muestran la diversidad de riesgos que debemos considerar. A su vez, la supervisión humana, la integridad de la cadena de suministro y la confianza cero aportan una perspectiva de defensa.

Desde mi visión, el valor de esta propuesta está en vincular seguridad y gobernanza. Me parece especialmente relevante que incluya la comunicación de riesgos y el desarrollo de capacidades sostenibles. La cuestión no es únicamente cómo construir una IA segura, sino cómo mantener esa seguridad durante todo su ciclo de vida.

Javier Peris

El Papel Higiénico no es Burocracia



Hay una frase que repito cada vez que alguien confunde documentar con complicar: nadie, jamás, ha llamado burocracia al papel higiénico. Compruébalo la próxima vez que entres al baño. No hay trámite, ni firma, ni sello. Compruebas que está ahí, lo usas y sigues con tu día. Nadie discute su utilidad ni su lugar en el proceso.

Y sin embargo, en cuanto la misma palabra —papel— aparece vestida de informe o procedimiento, una parte del mundo profesional reacciona con el mismo fastidio que si les propusieran rellenar un formulario en un ministerio. Ahí está el problema que quiero desmontar: confundir documentar con burocratizar es una de las fuentes más caras y menos discutidas de mala gestión en las organizaciones actuales.
La ignorancia sale cara y se demuestra con números: esto no es opinión, es una factura que pagan las empresas todos los años. El Índice de Burocracia 2025, del Centro Adam Smith y México Evalúa, calcula que el coste de oportunidad del exceso de trámites en América Latina supera los 110.000 millones de dólares anuales, cerca del 13% del PIB analizado. En España, distintos estudios sitúan ese coste en torno a 90.000 millones de euros al año, con empresas y autónomos dedicando de media 53 días anuales solo a papeleo.

Con estas cifras entiendo la alergia a la palabra burocracia. El problema es que esa alergia, mal dirigida, ha terminado contaminando también a la documentación bien hecha, que es justo lo contrario: no es papeleo que ralentiza, es información que protege.
Y aquí quiero ser preciso: la falta de documentación no es agilidad, es irresponsabilidad. Cuando una organización no documenta sus procesos o decisiones, no está siendo más rápida ni más moderna. Está acumulando riesgo invisible que tarde o temprano se cobra su precio, casi siempre en el peor momento posible.

Cuando no hay papel, no hay con qué limpiar el desastre. La norma ISO 30301, “Sistemas de gestión para los documentos. Requisitos”, no trata la documentación como un fin en sí mismo, sino como herramienta para que la organización consiga su misión y estrategia. Exige identificar, analizar y evaluar los riesgos de fallos en el control de documentos auténticos, fiables y usables, determinando cuándo son aceptables y cuándo requieren gestión activa. La norma de referencia parte de la misma idea que defiendo aquí: documentar es, ante todo, gestionar riesgo, no cumplir un formalismo.

CONTINÚA EN PRÓXIMA PÁGINA



La norma exige además que el sistema documental esté vinculado a la dirección estratégica, con compromiso demostrable de la alta dirección y recursos reales. Su complementaria, la ISO 30302, aporta las directrices prácticas de implementación. Entre ambas dibujan un modelo alejado del papeleo por inercia: creación, control y disposición de documentos, sometidos a medición y mejora continua, como cualquier sistema de gestión serio.
Piénsalo en concreto: una empresa sin trazabilidad documental no puede demostrar por qué tomó una decisión ni si cumplió la normativa. Ante una inspección o una discrepancia con un proveedor, la ausencia de documentación no es un vacío neutro, es una condena anticipada. No hay con qué limpiar el desastre, ni cómo demostrar qué pasó.

No es alarmismo. Tanto la ISO 30301 como las guías de la Agencia Española de Protección de Datos coinciden: cualquier tratamiento de riesgo exige documentar quién lo realiza, quién lo aprueba y qué medidas se han adoptado. Sin ese rastro, la diligencia existió solo en la cabeza de quien la ejerció, y eso no vale nada.
Ahora bien, quiero ser justo con quienes desconfían del papeleo, porque su desconfianza no siempre nace de la ignorancia: hay un punto en el que la documentación deja de proteger y empieza a asfixiar. Los estudios citados no hablan de documentación bien diseñada, sino de trámites redundantes y formularios que nadie relee. Y esto tampoco encaja con la ISO 30301: la norma no pide más documentos, pide decidir con criterio cuáles crear, basándose en necesidades reales del negocio, nunca por costumbre.
Un informe reciente sobre productividad empresarial señala que los directivos pueden invertir hasta un 34% de su jornada en tareas administrativas, y que sus equipos pierden de media 1,7 días semanales en actividades sin valor añadido. El cálculo es sencillo: un equipo de 100 personas que pierde 5 horas semanales en papeleo innecesario, a 25 euros la hora, genera una factura anual superior a 650.000 euros, sin contar el desgaste del talento.

Esa es la otra cara de la irresponsabilidad: documentar por documentar, sin medir el retorno de esa inversión, es tan dañino como no documentar nada. Un procedimiento que nadie consulta es ruido con apariencia de orden, justo lo que la ISO 30301 busca evitar con su exigencia de evaluación periódica y gestión de no conformidades.
La medida justa: documentar lo que aporta, no lo que tranquiliza y por tanto la pregunta correcta no es "¿documentamos sí o no?", sino "¿qué documentación genera más retorno que el tiempo que cuesta producirla?". La propia ISO 30301 obliga a esa disciplina: exige medir y evaluar los resultados del sistema documental, no solo



implantarlo, para evitar que se convierta en burocracia acumulada sin revisión. Cada documento debería responder a tres preguntas: ¿reduce un riesgo identificado?, ¿alguien lo va a usar de verdad?, ¿el tiempo de crearlo es menor que el coste de no tenerlo cuando haga falta?

Cuando la respuesta a las tres es sí, ese documento es una inversión con retorno claro: menos riesgo legal, más rapidez en decisiones futuras, menos dependencia de la memoria de una sola persona. Cuando la respuesta es no, ese documento no debería existir, y quien insiste en producirlo por costumbre está creando la misma burocracia que dice combatir.

Vuelvo al principio. La ignorancia no está en documentar, ni en cuestionar la documentación excesiva, sino en no saber distinguir entre ambas cosas. Es ignorante quien confunde cualquier papel con un obstáculo, porque le impide reconocer el valor de la trazabilidad cuando de verdad la necesita. Y es igual de ignorante quien confunde cualquier papel con una garantía de calidad, acumulando procedimientos sin preguntarse si alguien los usa.

El papel higiénico nos da la pista más sencilla: nadie lo cuestiona porque su función es evidente y su coste es mínimo frente al problema que evita. Esa es la vara de medir que le falta a la gestión documental en la mayoría de las organizaciones, la misma que persigue la familia de normas ISO 30300: no más papel, no menos papel, el papel justo, en el lugar justo, para que cuando llegue el problema haya con qué limpiarlo y cómo demostrar qué pasó.



JAVIER PERIS

Javier Peris es Socio Director y CKO (Chief Knowledge Officer) de Business Technology & Best Practices (Business&Co.®) especializado en Gestión del Portfolio, Programas y Proyectos, Centros de Excelencia así como Marcos de Gobierno y Gestión de Tecnologías de la Información con más de 20 años de experiencia tanto en empresas como en Organismos Oficiales y Administración Pública. Es Profesor de IE Business School e IE Executive Education y dispone de las Acreditaciones Internacionales CGEIT®, CRISC®, COBIT5® Certified Assessor, ITIL® Expert & Trainer, PRINCE2® MSP® MoP® MoV® MoR® P3O® Practitioner & Trainer, Sourcing Governance®, VeriSMTM SIAMTM, OKR, Lean, Kamban, Design Thinking, Scrum & AgileSHIFT® Accredited Trainer ejerce como Business Coach, Business Angel e Interim Manager.

LinkedIn: https://es.linkedin.com/in/javierperis Twitter: https://twitter.com/JavierPeris
Blog: https://javierperis.com

Escuela de Gobierno eGob®

https://escueladegobierno.es

Competencias Directivas en **Gobierno y Gestión**











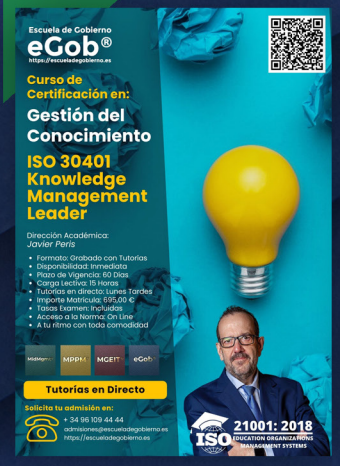


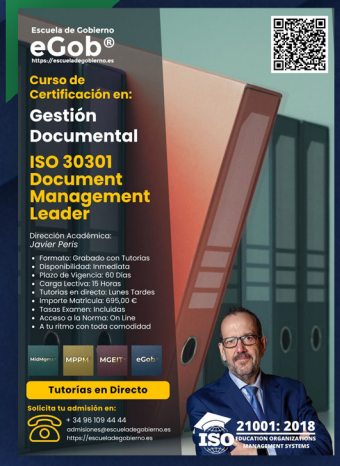












ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

IMQ CERTIFIED
QUALITY MANAGEMENT SYSTEM
ISO 9001:2015

IMQ CERTIFIED
MANAGEMENT SYSTEM FOR EDUCATIONAL ORGANIZATIONS
ISO 21001:2018

Manuel Serrat Olmos



Ciberseguridad en la era de la inteligencia artificial: cómo cambiará la profesión en los próximos cinco años (i)

En esta sección de Tecnología y Sentido Común llevamos seis temporadas hablando de temas relacionados con la seguridad de la información, los riesgos, las ciberdelincuencia, y otros temas relacionados. Sin embargo, como en otros sectores de la sociedad, quizá ha llegado el momento de tratar de hacer algo de futurología por lo que al impacto que la Inteligencia Artificial va a tener sobre los profesionales de la ciberseguridad. ¿Van a seguir siendo necesarios? ¿Se va a reducir el empleo en el sector? ¿O por el contrario, son aún más necesarios, pero sus tareas y roles han de evolucionar?

Primera parte: La IA llega al puesto de trabajo

Durante años, hablar del futuro de la ciberseguridad significaba hablar de una pugna permanente entre atacantes y defensores. A medida que las organizaciones incorporaban nuevas tecnologías, también aparecían nuevas formas de atacarlas, incentivadas por el retorno económico que la ciberdelincuencia parece tener. El crecimiento de la nube, los dispositivos conectados o el trabajo remoto fueron ampliando la superficie de exposición de las organizaciones, obligando a los profesionales de seguridad a adaptarse a estos nuevas situaciones.

Pero desde hace un par de años hay un nuevo protagonista: la inteligencia artificial, que tenemos hasta en la sopa. Y, a diferencia de muchas tecnologías anteriores, la IA no es simplemente otra herramienta que los profesionales de ciberseguridad, o de los demás sectores del conocimiento, tienen que aprender a utilizar. Es una tecnología completamente diferente, disruptiva, y capaz de modificar intrínsecamente la forma en la que trabajan.

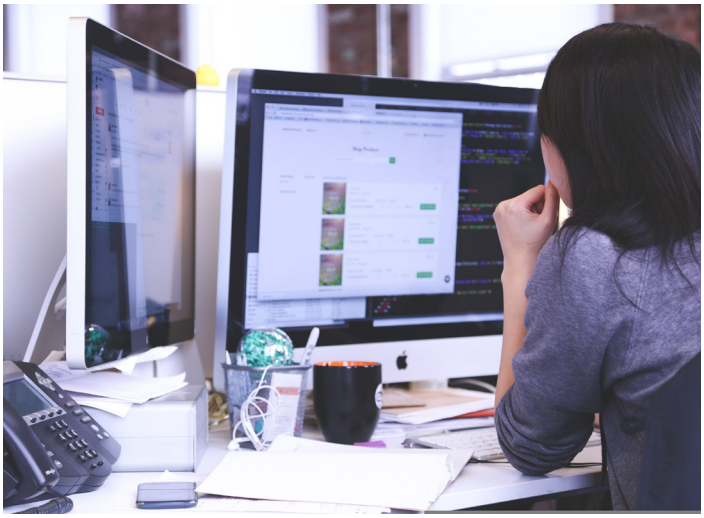
Mucho se habla en ciertos sectores sobre la pérdida de empleo que va a tener la integración de la IA en las organizaciones. Incluso hay organizaciones poco prudentes que ya han comenzado un proceso de reducción de personal sin tener madura ni la tecnología que va a hacer ese trabajo, ni los procesos para integrarla correctamente en la operativa de la misma.

En los próximos cinco años veremos probablemente una transformación considerable de la profesión de la ciberseguridad. No significa que los analistas de seguridad, especialistas en respuesta a incidentes, ingenieros o responsables de seguridad vayan a desaparecer. Significa que buena parte de las tareas que hoy realizan cambiarán, y algunas dejarán de requerir la intervención humana constante, y ésta se limitará a la supervisión de los procesos o de los resultados.

Un estudio de ISC2 publicado en 2025 señalaba que el 30% de los profesionales encuestados ya utilizaba herramientas de inteligencia artificial en sus tareas de seguridad, y otro 42% las estaba evaluando o probando. Entre la organizaciones que ya las utilizaban, siete de cada diez percibían una mejora de la eficacia de sus equipos. Sin embargo, la encuesta no entraba en otras cuestiones importantes sobre el mercado de trabajo de estos profesionales, como los empleos "de entrada" o "juniors", los posibles ajustes en plantillas "senior", o los efectos salariales de la integraciçon de la IA en las tareas de ciberseguridad.

Para entender el impacto de la IA basta con pensar en uno de los trabajos más habituales dentro de un centro de operaciones de seguridad (SOC): **analizar alertas**. Una organización puede generar miles de avisos relacionados con posibles amenazas. La mayoría no representan un ataque grave, y quizá sean simples falsos positivos. El problema es que alguien tiene que revisar esos avisos, relacionarlos con otros acontecimientos y decidir cuáles merecen atención inmediata del equipo de respuesta.
Es una tarea imprescindible, pero también repetitiva, estresante, y agotadora, ya que obliga a un nivel de atención importante, y a saber relacionar información procedente de diversas fuentes para establecer una conclusión fundamentada.

CONTINÚA EN PRÓXIMA PÁGINA



La inteligencia artificial puede hoy en día asumir una parte importante de ese trabajo. A nadie se le escapa que puede analizar grandes cantidades de registros de log, buscar patrones en esos registros, comparar comportamientos diagnosticados con comportamientos maliciosos conocidos, y establecer prioridades mucho más rápidamente que una persona. En lugar de presentar al analista cientos de alertas aparentemente independientes, un sistema de IA puede ofrecerle una visión más elaborada: varias señales diferentes podrían estar relacionadas con el mismo incidente, cuya gravedad estimada incluso puede ser evaluada por el propio sistema de IA.

El profesional, por tanto, deja de dedicar tanto tiempo a buscar la aguja en el pajar y puede concentrarse en determinar qué hacer cuando encuentra la aguja. Y este cambio es importante. La IA no tiene por qué sustituir al analista, sino que puede convertirse en una especie de asistente capaz de filtrar el ruido y preparar el terreno para que el experto tome una decisión. Precisamente, las organizaciones esperan obtener ventajas de los sistemas de IA en áreas como la monitorización de redes, la detección de intrusiones, la respuesta ante incidentes, la gestión de vulnerabilidades y las pruebas de seguridad.

Otro de los grandes cambios llegará específicamente de la mano de la inteligencia artificial generativa. Un profesional puede pedir a un sistema de IA que explique un fragmento de código, resuma un informe de inteligencia de amenazas, compare dos comportamientos sospechosos o ayude a construir una hipótesis sobre lo que está sucediendo. Incluso, puede servir para una tarea aparentemente sencilla, pero que consume mucho tiempo y es habitualmente la menos apreciada por los profesionales de la ciberseguridad: redactar documentación o informes.

Después de un incidente, hay que explicar qué ocurrió, qué sistemas fueron afectados, qué medidas se adoptaron durante el incidente y qué recomendaciones deben seguirse para mejorar la seguridad y minimizar la probabilidad de recurrencia del mismo tipo de incidente. Una IA puede generar un primer borrador a partir de la información disponible, y el profesional tendrá que revisarlo, corregirlo y validarlo, pero no tendrá que empezar necesariamente desde una página en blanco. El resultado puede ser una profesión menos centrada en procesar información y más centrada en interpretarla.

Y esta distinción será fundamental. Porque la información nunca ha sido el principal problema de la ciberseguridad. El problema ha sido convertir cantidades enormes de información en decisiones acertadas. Es muy probable, pues, que, en cinco años, muchas herramientas de seguridad funcionen de una manera que hoy empieza a resultar familiar en otros ámbitos: el profesional planteará un objetivo y el sistema realizará una parte importante del trabajo necesario para alcanzarlo. Por ejemplo: identificar los sistemas más expuestos, buscar indicios de compromiso, comprobar determinadas configuraciones o proponer medidas de contención.

Pero habrá una diferencia esencial respecto a un sistema completamente autónomo: alguien tendrá que decidir hasta dónde se puede confiar en él. **Porque la IA puede equivocarse**. Puede interpretar mal una señal, generar una explicación convincente pero incorrecta, o recomendar una acción que tenga consecuencias inesperadas y potencialmente destructivas.

Por eso, una de las competencias más importantes del profesional de ciberseguridad del futuro no será únicamente saber utilizar inteligencia artificial. **Será saber cuándo no confiar en ella.**

Y eso nos lleva a la segunda cara de esta revolución, que analizaremos en el siguiente artículo de esta serie, en el próximo número de Tecnología y Sentido Común.



MANUEL SERRAT OLMOS

Doctor en Informática por la Universitat Politècnica de València y Master en Dirección TIC de la UPM-INAP, dispone de varias certificaciones internacionales en Operación, Gestión y Gobierno de TI, tales como ITIL, FITSM, PRINCE2 y COBIT. Escritor técnico, ha sido profesor asociado en varias universidades y actualmente coordina el servicio de TI de una organización pública.

LinkedIn: https://www.linkedin.com/in/manuel-david-serrat-olmos/
Twitter: https://twitter.com/mdserrat

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Certificación en:

Gestión por Procesos de Negocio

P4MGO! BPM Business Process Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el P4MGO! BPM BoK
- 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



TECNOREGULACIÓN EN PROSPECTIVA

Nacho Alamillo



Impulsando el PanEuropean Trust Framework

El mes pasado tuve el honor de participar en Ginebra en el Global Digital Collaboration, posiblemente uno de los foros más importantes del mundo en materia de identidad digital en sentido amplio, moderando una sesión co-organizada por el Comité Europeo de Normalización y el European Decentralisation Institute, think thank al que pertenezco.

En dicha sesión, con participación de la OCDE, del Consejo de Europa, el W3C y el propio CEN, entre otras entidades, hemos presentado la iniciativa en pro de un PanEuropean Trust Framework, porque, como explicamos en nuestro manifiesto, Europa no está creando un único sistema de identidad digital, sino varios, al mismo tiempo y en el marco de distintos instrumentos jurídicos.

La Unión Europea cuenta con eIDAS 2.0 y la cartera EUDI, cuya aplicación se extiende a los Estados del EEE. Suiza cuenta con la Ley de Identidad Electrónica, ratificada mediante referéndum en septiembre de 2025, cuya implantación se lleva a cabo a través de la cartera Swiyu. El Reino Unido cuenta con el Marco de Confianza en la Identidad y los Atributos Digitales, gestionado por la Oficina de Identidades y Atributos Digitales, junto con GOV.UK One Login. Ucrania cuenta con Diia, implantado a escala nacional en condiciones de guerra y que ahora forma parte de su proceso de adhesión. Los Balcanes Occidentales, los países candidatos a la UE, Noruega, Islandia y Liechtenstein, así como el conjunto de los miembros del Consejo de Europa, avanzan cada uno a su propio ritmo, con arreglo a su propia legislación. También Andorra dispone ya de su cartera de identidad digital.

Cada uno de estos casos constituye un ejercicio legítimo de las competencias nacionales o de la Unión. En conjunto, plantean un problema que ninguno de ellos puede resolver por sí solo. Un empresario suizo que verifica un título de la UE, una cualificación profesional ucraniana reconocida en un Estado miembro de la UE, un servicio de verificación del Reino Unido que opera en todo el continente y una empresa que acredita a sus representantes autorizados en treinta o más jurisdicciones se topan todos con el mismo obstáculo.

CONTINÚA EN PRÓXIMA PÁGINA

Existen amplias pruebas de esta problemática. El análisis de la OCDE sobre el G7 de 2024 no encontró ninguna norma internacional compartida por todos los miembros del G7, y solo seis que se compartieran entre dos de ellos. La encuesta realizada por el Reino Unido en febrero de 2026 a los proveedores de verificación digital reveló que el 79 % citaba la diversidad normativa como un obstáculo para operar a nivel internacional, y el 62 % pedía un acuerdo normativo o político transfronterizo. La armonización superficial se superpone a una profunda fragmentación técnica e institucional. Por lo tanto, la armonización no es la cuestión pendiente. Lo que sí lo es son las condiciones en las que se lleva a cabo.

Algunos de los principios de diseño del PanEuropean Trust Framework son:

Subsidiariedad digital. Las funciones se sitúan en el nivel de competencia más bajo. Las credenciales pertenecen a sus titulares, su emisión corresponde a las autoridades más cercanas a ellos, su verificación se realiza dentro de los límites de la transacción y, por encima de ello, solo se aplica la gobernanza mínima necesaria. La subsidiariedad es un requisito constitucional en virtud del artículo 5 del TUE y un principio fundamental del federalismo suizo. También debería ser un requisito arquitectónico.

Reconocimiento mutuo frente a centralización. La interoperabilidad debe lograrse mediante criterios de conformidad compartidos y el reconocimiento entre jurisdicciones y sectores, no a través de un único registro, un único proveedor o una única plataforma técnica. El reconocimiento debe funcionar entre distintos ordenamientos jurídicos, no solo dentro de uno mismo. Este es precisamente el problema específico que el PanCanadian Trust Framework se creó para resolver dentro de una federación, mientras que su versión europea abarca a Estados soberanos.

No vinculabilidad por defecto. Dos verificaciones distintas no deberían, por defecto, poder correlacionarse con la misma persona o entidad, ya sea porque un verificador observe interacciones repetidas, porque los verificadores actúen de forma colusoria o porque la infraestructura de emisión y revocación actúe como superficie de correlación. El re-vinculado solo debería ser posible mediante un procedimiento judicial definido con garantías procesales. Se trata de un requisito arquitectónico vinculante, no de una adición posterior, y se deriva de las obligaciones del artículo 8 del CEDH, que se aplican mucho más allá de la Unión.

Estándares abiertos y neutralidad tecnológica. El marco debe poder ser aplicado por cualquier sistema que cumpla con los



requisitos, no debe generar dependencia de soluciones propietarias en las infraestructuras adquiridas con fondos públicos y no debe exigir a ninguna jurisdicción que renuncie a una arquitectura nacional técnicamente sólida como condición para su reconocimiento.

Control responsable de los cambios. Las modificaciones de la infraestructura de confianza raíz deben someterse a un proceso de revisión transparente, de duración limitada y en el que participen múltiples partes interesadas, con participación de las autoridades de protección de datos. El rechazo del referéndum de 2021 en Suiza y su posterior aprobación demuestran que estas garantías no suponen un obstáculo procedimental. Son la fuente del consenso público.

Inclusión desde el diseño. Las vías no digitales, los mecanismos de delegación para quienes no pueden actuar por sí mismos y la facilidad para emitir y revocar son condiciones de legitimidad, no características opcionales.

Diseñado para la interoperabilidad global. El marco debería ser un modelo de gobernanza exportable, en lugar de un sistema regional cerrado. El PanCanadian Trust Framework, el Memorándum de Cooperación entre la UE y Japón y la Recomendación de la OCDE demuestran que la armonización entre jurisdicciones es posible cuando la gobernanza se diseña con ese fin.

No puedo dejar pasar la ocasión para invitaros a participar de tan interesante iniciativa.



NACHO ALAMILLO

Es Doctor en Derecho por la Universidad de Murcia. Licenciado en Derecho por la UNED. Auditor de Sistemas de Información certificado, CISA. Director de Seguridad de la Información certificado, CISM. Ingeniero Certificado en Soluciones de Protección de Datos, CDPSE, por ISACA.
En la actualidad, es Abogado del Ilustre Colegio de Reus, Asesor de Logalty y Director General de Astrea La Infopista Jurídica SL. Asimismo, colabora con el Grupo de Investigación iDerTec de la Universidad de Murcia.
También es miembro del grupo de Infraestructura de Seguridad de Firma Electrónica del Instituto Europeo de Normas de Telecomunicaciones, que normaliza los servicios de confianza, miembro de UNE CTN71/SC307, de CEN-CLC/JTC 19 y de ISO TC 307, relativos a Blockchain.
Dispone de más de 100 publicaciones y ha impartido más de 400 ponencias en identidad digital, servicios de confianza y materias relacionadas.

Escuela de Gobierno

eGob®

https://escueladegobierno.es



Curso de Certificación en:

Gestión de la Innovación

ISO 56002 Innovation Management Leader

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Incluye BestPractices.Games
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es
https://escueladegobierno.es

ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

Domingo Gaitero

¿Por qué tantas preguntas?



Martes 12:00 de la mañana, en la planta 10 de un moderno edificio de una gran avenida de una gran ciudad. Asamblea del consejo de administración.
Don José llega apurado a la reunión porque le han comunicado, por teléfono, que hay una auditoria nueva de una "cosa" nueva que tiene que ver con la tecnología y que como el proviene de ahí pues que es el candidato para hablar con los auditores.
Mientras va camino de la reunión va discutiendo consigo mismo, incluso maldiciendo, porque el pensaba que "ascender" al consejo significaba no volver a hablar de tecnología nunca más en la vida.
¿Por qué los consejeros de casi todas las empresas piensan que la tecnología no va con sus obligaciones? Esta reflexión es mía.
Al llegar a la reunión, vio muchas sillas vacías y a un elemento que no le sonaba conocido y que además le resultaba extraño en la reunión por su extremada juventud.

La primera duda se la resolvieron enseguida:
- "José como la reunión va de tecnología y la mayoría ya sabes que no tienen ni idea, han pensado que con tu presencia bastaría".
La segunda duda tenía nombre: Almudena, CISO de la empresa, 40 años con más de quince de experiencia en seguridad de la información.
A partir de ahí, Don Alejandro, consejero delegado, les invitó a que comentaran el problema.
Almudena, como buena informática, fue muy escueta:
- "mira vienen de una big four a hacernos un simulacro de auditoria de NIS2 y quieren preguntar al consejo de administración como máximos responsables de la ciberseguridad algunas cosas".
- "¿y por qué no te lo preguntan a ti que eres la responsable y te pagamos por ello? Respondió José rápidamente.
Almudena frunció el ceño y respondió: "porque la NIS2 dice que la máxima responsabilidad ante un ataque o una crisis de ciberseguridad los responsables son los miembros del consejo.
José sonrió y preguntó: Me puedes decir donde dice y por cierto ¿hemos tenido alguna crisis?
Don Alejandro intervino porque presumia que la conversación iba para largo y de unamanera tajante ordenó directamente a José que se hiciera cargo y cerrara el tema.
Esta escena todavía no es frecuente en las empresas españolas, pero va a existir y muy pronto, quizás el año que viene como muy tarde sino es este mismo 2026.
La Alta dirección de las empresas y por supuesto los consejos de administración todavía no comprenden la necesidad de su implicación y llegan a pensar que los riesgos de la ciberseguridad no son nada más que eso: unos riesgos más.

CONTINÚA EN PRÓXIMA PÁGINA



A esto podemos añadir sin ningún tipo de duda el impacto de la IA y no su uso ni su buen uso, sino su mal uso o su uso descontrolado, es decir, un uso imprevisible, sin ninguna estrategia ni gobierno basada en la valentía y conocimiento o desconocimiento de algunos empleados.
Y en este aspecto quiero ser muy simple a la hora de resolver este dilema con un ejercicio que os comparto. Mañana por la mañana ir al despacho de vuestro director general (no creo que tengáis acceso al consejo) y pedirles diez minutos para hacerles unas cuentas preguntas:

1.- Don/Doña X ¿quién toma el mando si mañana sufrimos un ataque?, simplemente con que se haya nombrado un comité de ciberseguridad con la definición de quien toma las decisiones durante una crisis, y que la CISO, en este caso, cada mes le actualice un cuadro de mando de ciberseguridad podría saber responder a la pregunta.
2.- Don/Doña X ¿sabemos que activos mantienen viva a la empresa?, obviamente no podemos proteger lo que no conocemos. Si hay un inventario de activos actualizado y completo y tenemos clasificados por criticidad los activos con sus propietarios, sabremos responder.
3.- Don/Doña X ¿Qué proveedor podría para nuestra empresa mañana?, aquí seria bueno hacer un ejercicio de humildad y pensar que nuestra ciberseguridad es tan buena como el peor eslabón de nuestra cadena. Tener clasificados y evaluados a nuestros proveedores ya no es una burocracia de la ISO 9000, es una necesidad vital para nuestro negocio.
4.- Do/Doña X ¿cuántas personas podrían abrir hoy el correo equivocado? Es eslabón más débil no es la tecnología, es la confianza mal colocada. Nuestros empleados empiezan a estra hartos de tanta formación, tanta concienciación y tantas “píldoras”, pero no son suficientes, la formación continua y realizar simulaciones periódicas forman parte de este adiestramiento continuo tan necesario hoy en día. Aquí tengo que hacer hincapié en la existencia de unas políticas claras del uso de la IA.

Puedo ser más duro y pedir a Don José que pregunte cuando fue la última vez que se probó la recuperación de un desastre, e incluso que pregunte cuales son



los tres riesgos que actualmente se están solventado en la organización, o si quiere hacer más daño que se acerque a una mesa y pregunte a cualquier empleado su opinión por la política de seguridad y que le parece más interesante.

Pero llegado a este punto quiero ver donde se adentra la organización en el lado oscuro.

Opción primera, los miembros del consejo no sabrían responder a alguna de esas preguntas. Esto se arregla con formación.

Opción dos, el/la CISO no sabe responder a las preguntas de Don José. Quizás por eso las nuevas normativas involucran a los consejeros. Aquí hay algo más que formación.

Opción tercera; los empleados no saben contestar. Aquí no hay nada implantado, hay trabajo por hacer.

Pero la pertenencia al lado oscuro no viene por ninguno de estas tres opciones, sino que viene porque estamos hablando de una organización certificada en la 27000 y posiblemente en el ENS, ahí es donde el lado oscuro entra de pleno.

Espero que este articulo os genere MUCHAS PREGUNTAS POR HACER



DOMINGO GAITERO

Domingo Gaitero es un consultor y emprendedor que, pese a haber sufrido varias adversidades desde su temprana juventud, ha logrado construir una carrera distinguida en el sector de las Tecnologías de la Información.

Domingo se caracteriza por ser un ponente excepcional dotado de un enorme sentido del humor, así como por ser un maestro de la resiliencia. Con su amplio bagaje de conocimientos y experiencia, su pasión es ayudar a todo aquel que quiera mejorar o cambiar su forma de vida.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Certificación en:

Gestión de Programas

P4MGO! PgM Programme Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el P4MGO! PgM BoK
- 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



ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

Marcelino Lominchar

¿Quién es Marcelino Lominchar?

Marce es un tipo de la Mancha toledana, de un pueblo llamado Corral de Almaguer. Me resulta muy raro hablar de mí mismo en tercera persona -nunca me ha gustado-, pero, contestando a la pregunta, diría que soy alguien sencillo, curioso y bastante apegado a mi familia, a mis amigos y a mis raíces.
Disfruto de una buena comida en compañía y considero que un café es, sobre todo, la excusa perfecta para mantener una buena conversación. Siempre tengo dos o tres libros encima de la mesilla, me encanta descubrir una película con un buen guion y me considero un poco friki porque acumulo bastantes aficiones y siempre tengo algún proyecto nuevo rondándome la cabeza.
Supongo que conservo bastante de aquel muchacho que salió de Corral de Almaguer sin imaginar del todo los caminos por los que terminaría llevándolo la vida.

Háblanos de tus éxitos y logros profesionales.

Destacaría cuatro: El primero, haber llegado a liderar Open Programs de IE Executive Education, una institución reconocida internacionalmente y que se exige a sí misma el máximo nivel académico.
El segundo, haber terminado impartiendo sesiones ante alumnos que, en su mayoría, son directivos con una amplia experiencia profesional. Confieso que todavía siento cierto vértigo cuando lo pienso.
El tercero es que cada vez me llaman de más medios de comunicación, de hecho, ahora tengo una sección en “No son horas” de Onda Cero, y me divierto muchísimo.
Y el cuarto, haber publicado dos libros con Sekotia, sello de AlmuzaraLibros. El primero, Historias de la historia de España, ha alcanzado cuatro ediciones y acaba de publicarse también en formato de bolsillo, todo ello en poco más de año y medio. Algo que jamás habría imaginado cuando comencé a escribirlo. Evidentemente, la única explicación posible es que la gente está fatal: ¡se está comprando mis libros!

CONTINÚA EN PRÓXIMA PÁGINA



REVISTA
Tecnología & Sentido Común
https://tecnologiaysentidocomun.com

¿Cuáles han sido los hitos más importantes de tu trayectoria profesional?

Aunque no me considero profesor -la palabra todavía me produce cierto vértigo-, me enorgullece haber abierto un pequeño camino dentro de una institución académica como el IE. Todo comenzó con la intención de mejorar la experiencia de los alumnos mediante visitas históricas a lugares como Segovia, El Escorial o el Madrid de los Austrias. Con el tiempo, aquellas visitas fueron dando paso a sesiones en las que utilizo episodios y personajes históricos para reflexionar sobre cuestiones relacionadas con el management. Porque la historia no consiste únicamente en recordar nombres y fechas: también permite hablar de liderazgo, estrategia, innovación, finanzas, geopolítica o toma de decisiones.
Que cada vez cuenten más conmigo para ofrecer esa mirada histórica aplicada al mundo de la empresa es, probablemente, uno de los hitos profesionales que más ilusión me hacen. En cierto modo, he conseguido unir mi formación como profesor de Historia con mi experiencia en Executive Education, dos caminos que durante mucho tiempo parecían avanzar por separado.

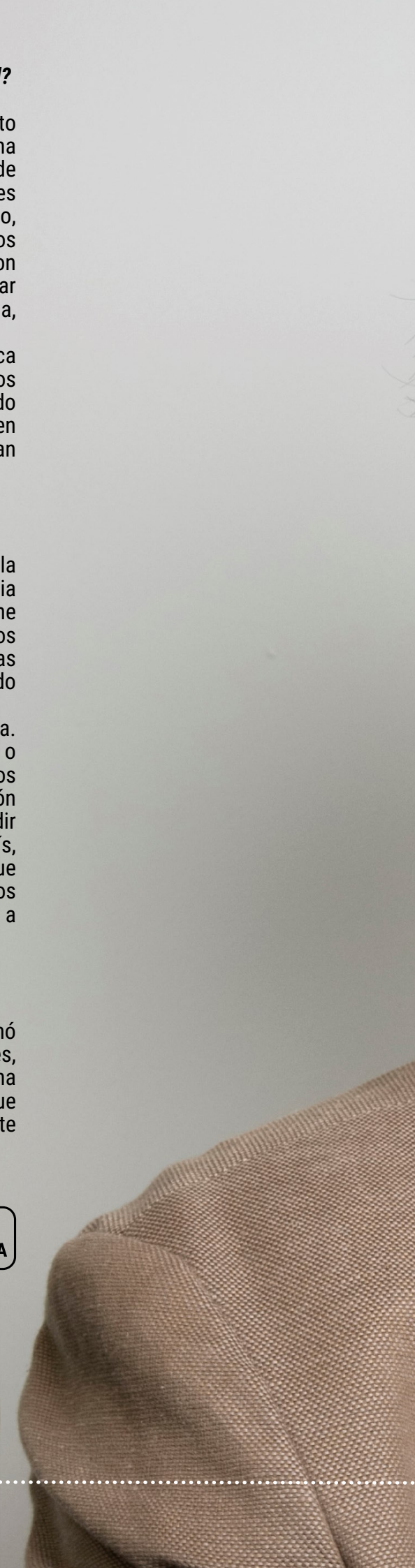
¿Háblanos de tu último libro publicado?

Mi último libro -el segundo para ser exactos- se titula “Historias de la contrahistoria de España”. Me resistí a llamarlo “Historias de la historia de España 2”, porque quería que tuviera una identidad propia. El libro me ha permitido rescatar del olvido a personajes aparentemente secundarios que, sin embargo, desempeñaron un papel fundamental. Sin ellos, muchas de las grandes figuras que todos conocemos quizá no habrían alcanzado la misma relevancia.
España mantiene una relación bastante compleja con su historia. Con frecuencia nos acercamos a ella desde el complejo, la culpa o el presentismo, juzgando hechos de hace siglos únicamente con los valores actuales. No se trata de negar errores ni de ofrecer una visión complaciente, sino de contar nuestra historia con rigor y sin pedir perdón de antemano. Tenemos episodios oscuros, como cualquier país, pero también personajes y acontecimientos extraordinarios de los que podemos sentirnos legítimamente orgullosos. De hechos, estos episodios brillantes son mucho más numerosos Este libro pretende devolver a algunos de ellos el lugar que merecen.

¿Cuál es el libro con el que más has disfrutado?

Como lector, elegiría “El mundo según Garp”, de John Irving. Me fascinó porque es una novela capaz de hacerte reír y, pocas páginas después, golpearte con una enorme dureza. Tiene personajes inolvidables, una imaginación desbordante y una mezcla de humor, tragedia y ternura que convierte una historia aparentemente disparatada en algo profundamente humano.

CONTINÚA EN PRÓXIMA PÁGINA





Nuestro invitado a #TYSC

REVISTA
Tecnología & Sentido Común
https://tecnologiaysentidocomun.com



Además, habla de la vida sin idealizarla, con toda su belleza, sus contradicciones y su permanente fragilidad. Creo que la historia -la real, la que escribimos con mayúsculas- también es así: conviven en ella la grandeza, el drama, el absurdo y, en ocasiones, una ironía extraordinaria. Por eso intento introducir cierto sentido del humor en los capítulos de mis libros, incluso cuando trato asuntos serios. Otra cosa, naturalmente, es que siempre lo consiga.

Y, como escritor, con lo que más he disfrutado ha sido con la novela que acabo de terminar. Es una sensación muy curiosa porque, de pronto, te conviertes en una especie de pequeño dios: decides lo que hacen los personajes, adónde van, de quién se enamoran y, si alguno tiene que morir, pues te lo cargas. Aunque también es verdad que, a medida que la historia avanza, algunos personajes comienzan a adquirir vida propia y no siempre se dejan llevar por donde uno había previsto.

Háblanos de tu experiencia, de tus vivencias e incluso de alguna anécdota.

Estudié Geografía e Historia en la Universidad Complutense de Madrid y obtuve también el título de profesor. Antes de llegar al mundo de la educación pasé por sectores muy diferentes, como el cartográfico, el comercio electrónico o la industria farmacéutica. Finalmente recalé en IE, donde llevo ya veintitrés años. ¡Madre mía, cómo pasa el tiempo!

Recuerdo que, durante la entrevista de trabajo, me preguntaron si era fácil desmoralizarme. No recuerdo exactamente cómo formularon la pregunta, pero aquello no se le puede preguntar a alguien de La Mancha que, además, ha vendimiado. Creo que, llevado por los nervios, llegué a mencionar mi experiencia en la vendimia. El entrevistador me miró con una expresión que parecía decir: «Creo que es la primera vez que me responden algo así».

Tengo también muchas aficiones y colecciono, entre otras cosas, monedas y apellidos. En una entrevista de radio con Javier Fontán y Domingo Gaitero (éste último nombre debe sonar en esta revista) conté que había reunido 1.600 apellidos en mi árbol genealógico. La cifra provocó bastantes carcajadas y terminó ocupando buena parte de la conversación. Debo reconocer que la afirmación no era del todo exacta: no tengo 1.600 apellidos, sino 1.600 antepasados con sus correspondientes apellidos, muchos de los cuales, afortunadamente para mi cordura, se repiten.

Volviendo a ti, ¿de qué te sientes más orgulloso en tu carrera profesional?

Me siento especialmente orgulloso de haber comenzado desde abajo y haber llegado a liderar un equipo de veinte personas. Un equipo que, desde el ámbito académico, hace posible cada año la puesta en marcha de una cantidad importante de programas de Executive Education dirigidos a alumnos con una enorme experiencia profesional y un nivel de exigencia muy elevado.

CONTINÚA EN PRÓXIMA PÁGINA

Nuestro invitado a #TYSC



Pero, más allá del cargo, me enorgullece comprobar lo que somos capaces de sacar adelante juntos. Detrás de cada programa hay muchísimo trabajo que no siempre se ve: coordinación, atención al detalle, resolución de imprevistos y una preocupación constante por ofrecer la mejor experiencia posible a los alumnos. Haber crecido profesionalmente dentro de IE y poder contribuir ahora al crecimiento de otras personas es, probablemente, aquello de lo que más orgulloso me siento. Siempre he dicho que la formación es una de las actividades más nobles.

¿Qué libros tienes pendientes de escribir?

La editorial me propuso escribir un tercer libro, que ya tengo bastante avanzado y que estará dedicado a diferentes historias del Imperio español. Mantendrá, en buena medida, el tono de mis dos libros anteriores: episodios poco conocidos, personajes sorprendentes y cierta ironía a la hora de acercarnos al pasado.

Además, y como ya he comentado, me he tomado la licencia de terminar una novela histórica que comencé en 2002 y abandoné en 2008, cuando pensé que sería muy difícil que algún día viera la luz. Está ambientada en la invasión napoleónica de España y llevaba demasiados años esperándome en un cajón. Ahora que tengo una editorial que confía en mis libros, me ha parecido un buen momento para recuperarla y terminarla.

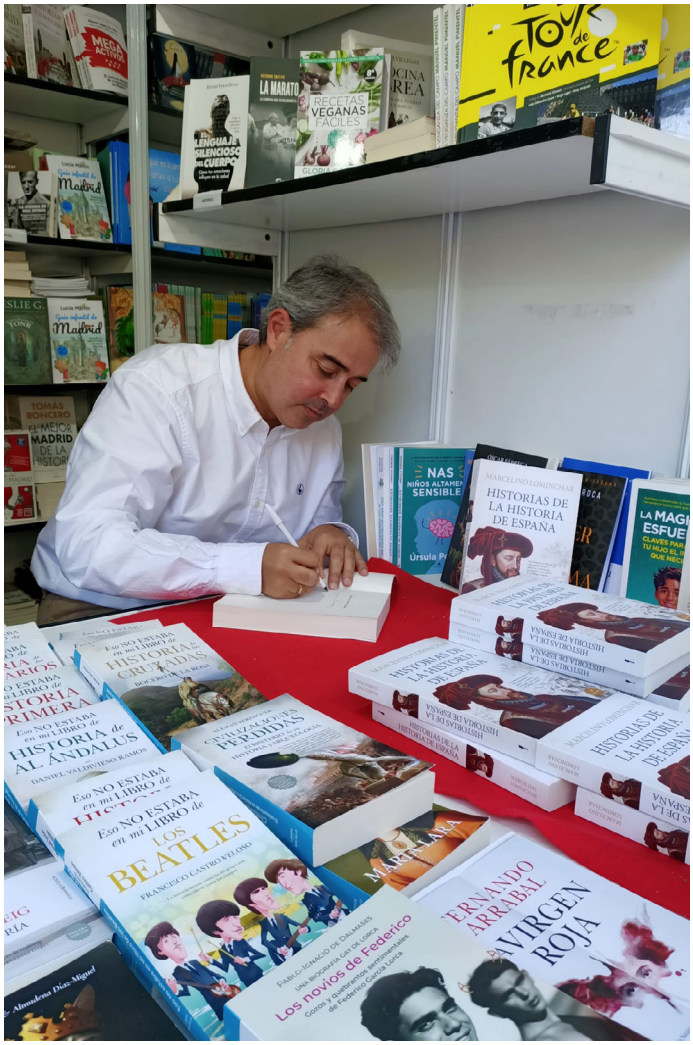
Después llegará la prueba de fuego: saber si a la editorial le gusta y considera que merece ser publicada. En caso afirmativo, ellos decidirán cuándo puede salir. Tampoco hay demasiada prisa: si la pobre lleva esperando desde 2002, puede aguantar un poco más.

Conclusiones.

Si echo la vista atrás, veo una trayectoria que difícilmente habría podido planificar. Estudié Historia, trabajé en sectores muy distintos, llegué a IE y, muchos años después, he terminado liderando un equipo, impartiendo sesiones y publicando libros. Caminos que en un principio parecían separados han acabado encontrándose.
Quizás el hilo conductor haya sido siempre la curiosidad. Me sigue gustando aprender, descubrir historias, conversar con personas interesantes y emprender proyectos sin saber exactamente adónde me llevarán. Siempre es buenos rodearse de gente más inteligente que tú. También he aprendido que las oportunidades rara vez aparecen completamente terminadas: muchas veces hay que reconocerlas, trabajarlas y, sobre todo, atreverse a dar el primer paso.

Me considero afortunado por dedicarme a proyectos que me permiten combinar la educación, la gestión y la historia, pero también soy consciente de que nada se consigue solo. Detrás de cualquier logro hay personas que te ayudan, equipos que te acompañan y familiares y amigos que soportan con paciencia tus obsesiones, tus libros y tus interminables historias.

De cara al futuro, espero mantener intactas las ganas de seguir aprendiendo y contando cosas. Tengo nuevos libros en marcha, proyectos profesionales y unas cuantas ideas más de las que probablemente debería. Pero, mientras siga disfrutando del camino, no parece un mal problema.



Escuela de Gobierno

eGob®

https://escueladegobierno.es



Curso de Certificación en:

Inteligencia Estratégica

ISO 56006 Strategic Intelligence Management Leader

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Incluye BestPractices.Games
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es
https://escueladegobierno.es

ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

Marlon Molina

El contenido basura en Internet es tendencia

La gran amenaza de la inteligencia artificial quizá no sea que terminemos creyéndonos todas las falsificaciones, puede ser algo mucho peor, que dejemos de creer también en las cosas verdaderas.

Llevo pensando mucho en la frase anterior desde que la IA generativa consiguió una adopción masiva. En un principio me alegró ver cómo las personas empezaron a desconfiar del contenido que veían en las redes sociales, con lo cual la ciberseguridad se veía beneficiada con esa dosis de desconfianza. Hoy abordo una nueva perspectiva de esta tendencia, un principio básico de la informática: si entra basura, sale basura.

Lo que ha cambiado es que nunca habíamos tenido máquinas capaces de producir tanta basura, tan rápido y a un coste tan bajo. Textos, fotografías, vídeos, comentarios, respuestas de correos electrónicos, artículos, noticias, y hasta supuestas opiniones pueden generarse ahora de forma prácticamente industrial.

El fenómeno ha adquirido incluso un nombre propio: **AI slop.** Se trata de un término utilizado para referirse a este contenido sintético, repetitivo y de escaso valor que empieza a inundar Internet.

La maquinaria de las redes sociales y los creadores de contenido falso

BBC expuso un ejemplo que resulta especialmente ilustrativo[1]. Una imagen generada mediante inteligencia artificial mostraba a dos niños extremadamente pobres sentados bajo la lluvia en mitad de una carretera, tenían barbas impropias de su edad, a uno le faltaban las manos y estaba frente a una tarta de cumpleaños junto a un cartel pidiendo likes. Lo chapucero de la fotografía hacían bastante evidente su origen artificial, algo que no importó demasiado porque la imagen se hizo viral en Facebook y consiguió cerca de un millón de “me gusta” y corazones.

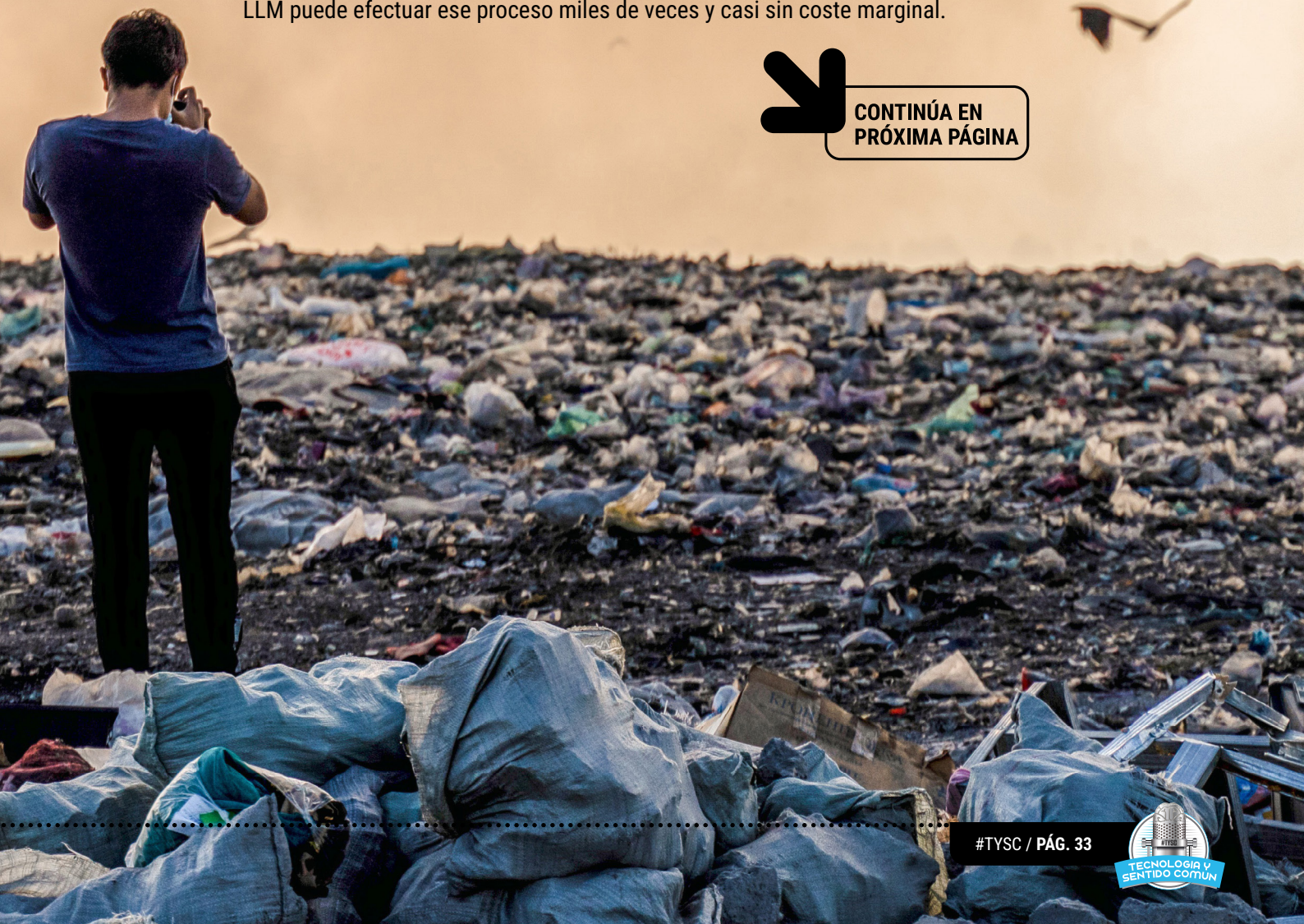


Tal parece que fabricar basura tiene recompensa, así las redes han estado incentivando a sus usuarios para que creen y compartan contenido. Ahora es mucho más fácil, la IA generativa puede hacer que una persona cree contenido de la misma forma que lo hace alguien que invierte miles de euros. Parezca o no contenido real, el hecho es que es fácil y barato.
Este nuevo tipo de contenido no crece solo en las redes sociales, también se traslada a los teléfonos, a las noticias, y en definitiva al contenido profesional.
Como ejemplo profesional, en España ya se han detectado escritos en el sistema judicial presentado por abogados y jueces [(2)], contenido creado con IA generativa y con datos inventados. Algunos abogados han sido "pillados" pero cuántos no. Cuántos libros se han creado con IA y publicado. Cuántas canciones se han hecho con IA generativa y publicada.
Un trabajo académico publicado en 2026 [(3)], basado en una muestra representativa de sitios de Internet Archive, estimó que aproximadamente el 35 % de los nuevos sitios publicados a mediados de 2025 podían clasificarse como generados o asistidos por IA. Antes del lanzamiento de ChatGPT, esa proporción era prácticamente cero en su medición.
El universo de datos digitales ha venido creciendo a un ritmo equivalente a duplicarse aproximadamente cada tres años [(4)]. El contenido se duplica y se construye a partir de contenido existente, pocas veces es contenido 100% original o no inspirado.

En el pasado el contenido se creaba a partir de otro siguiendo un patrón como el siguiente:
•Un periodista leía varias fuentes y escribía otra noticia.
•Un blogger resumía un artículo.
•Un usuario copiaba un texto.
•Una web sindicaba una noticia.

El contenido con "rastros de IA generativa" podría haber superado ya el 50% en algunas categorías
Los grandes modelos de lenguaje (LLM) se alimentan una y otra vez y puede que estén entrando en un modo recursivo casi infinito, y quizá muy difícil de parar. Un LLM puede efectuar ese proceso miles de veces y casi sin coste marginal.

CONTINÚA EN PRÓXIMA PÁGINA



Así, la maquinaria puede estar creando un mar rojo, absolutamente lleno de basura y datos cuya fuente sea difícil de encontrar, y cuya autenticidad sea prácticamente imposible.

Por ejemplo, imaginemos que se crean 100 nuevas unidades de contenido y que 60 de ellas han sido generadas o asistidas por inteligencia artificial. Si, además, suponemos hipotéticamente que el 80 % de ese contenido sintético consiste principalmente en reformular información que ya existía, tendríamos 48 unidades de contenido derivativo (60 multiplicado por 0,8). En términos de volumen, Internet habría crecido en 100 nuevos documentos, pero eso no significa que haya aumentado en 100 unidades equivalentes de conocimiento nuevo.

La preocupación relacionada con el AI slop es que la cantidad de contenido pueda crecer exponencialmente mientras la cantidad de información original no lo haga al mismo ritmo.

Si las redes sociales están preocupadas, quizá todos deberíamos estarlo

La preocupación ha llegado incluso a las propias plataformas que durante años han incentivado la producción de contenido. Snapchat ha decidido dejar de recomendar en Spotlight vídeos generados íntegramente mediante IA y priorizar contenido humano. LinkedIn asegura haber bloqueado miles de millones de intentos de publicar comentarios generados mediante IA y YouTube ha endurecido sus criterios de monetización frente al contenido genérico, repetitivo o producido mediante plantillas. Como es costumbre, Mark Zuckerberg también ha opinado y en resumen asume que hay poco que hacer, aunque sí expresa su preocupación por el futuro de la red si la tendencia continua.

IBM cita una previsión de Gartner según la cual, durante 2026, las organizaciones abandonarán el 60 % de los proyectos de inteligencia artificial que no estén respaldados por datos preparados para IA [5]. La paradoja resulta interesante, nunca había sido tan barato producir información y, al mismo tiempo, disponer de información en la que podamos confiar puede ser cada vez más caro.

Crear contenido nunca había sido tan barato, pero que sea barato producirlo no significa que sea barato para el sistema que tendrá que consumirlo, lo que está ocurriendo es que el coste se desplaza. Lo que ahorramos generando un texto, una imagen o un vídeo en segundos puede aparecer después en forma de tiempo dedicado a comprobar su procedencia, verificar los datos, distinguir lo auténtico de lo sintético y limpiar la información antes de volver a utilizarla. Que yo recuerde, validar datos la mayor parte del tiempo es más caro que el dato. Es algo que las empresas conocen desde mucho antes de la llegada de la IA generativa.

IBM explica que los datos de mala calidad no aparecen espontáneamente, sino que son consecuencia de errores humanos, falta de validación, problemas de integración, una gobernanza deficiente y, cada vez más, bucles de retroalimentación producidos por sistemas de machine learning.

El problema se agrava porque la basura también puede retroalimentar a la máquina. Si utilizamos información de baja calidad para generar nuevo contenido y parte de este contenido vuelve posteriormente a nuestros conjuntos de datos, el ya mencionado principio “si entra basura sale basura” adquiere una dimensión diferente porque la basura que sale puede convertirse en la basura que vuelva a entrar. Cada iteración puede añadir volumen sin necesariamente añadir conocimiento y aumentar, al mismo tiempo, el coste necesario para separar una cosa de la otra.

UNESCO encontró [6] en una encuesta que el 62 % de los creadores de contenido tenía dificultades para evaluar la credibilidad de la información que encontraba en Internet, yo reinterpretaré la afirmación diciendo que o no quieren validar, o no se molestan en validar. Más preocupante todavía es que el 42 % utilizaba como principal indicador de credibilidad el número de “me gusta” y las veces que una publicación había sido compartida.

Cuando quienes construyeron máquinas para distribuir contenido empiezan a tomar medidas porque estamos fabricando demasiado contenido de baja calidad, quizá es el momento en el que deberíamos prestar atención. La inteligencia artificial no es el problema por sí misma ya que puede ayudarnos a escribir, programar, investigar, traducir o crear mejor. El problema es cuando la imprudencia es la guía y una tecnología capaz de producir prácticamente sin coste se conecta con un sistema que recompensa el volumen, la velocidad y la interacción. Así es probable que la gran amenaza no sea que terminemos creyéndonos todo lo falso, ya que el verdadero problema llegará si llenamos Internet de tanta basura que dejemos de creer también en lo verdadero.

1-Tidy, J. (2026). AI ‘slop’ is transforming social media – and a backlash is brewing. BBC News, 4 de febrero de 2026.
2-EFE (2026). El Poder Judicial sanciona a un juez por usar Chat GPT para redactar una sentencia. EL PAÍS, 27 de abril de 2026.
3-Dolezal, J., Alam, S., Graham, M. & Bohacek, M. (2026). The Impact of AI-Generated Text on the Internet. arXiv:2604.26965
4- IDC (2018). The Digitization of the World – From Edge to Core. IDC White Paper, Doc. #US44413318
5- IBM (2025). Dirty data: What it is and how to fix it. IBM Think. Sección: “The impact of dirty data on AI”
6- Naciones Unidas (2024). Un 62% de los influencers no verifica la información que comparte en redes. Noticias ONU, 27 de noviembre de 2024.



MARLON MOLINA

Marlon Molina es ingeniero informático, actualmente vicepresidente internacional de Smart Campus AI, director del Centro para la Ciberseguridad Ciudadana en República Dominicana, y productor de diferentes programas audiovisuales enfocados en la tecnología, incluyendo ALERTA La Serie.

LinkedIn:
https://www.linkedin.com/in/marlonmolina/

Escuela de Gobierno

eGob®

https://escueladegobierno.es

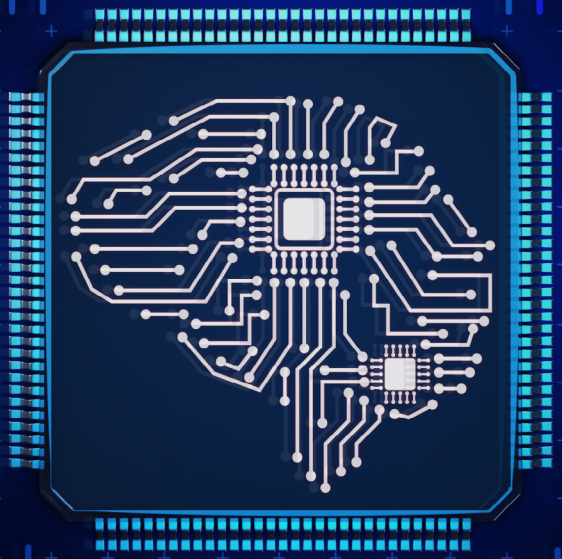
Curso de Certificación en:

Gobierno de la Inteligencia Artificial

ISO 38507 AI Governance Leader

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 15 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- 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

ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

Ricard Martínez Martínez

Las lecciones aprendidas en el caso Meta y el futuro de la inteligencia artificial

A pesar de las significativas expectativas que despertó la demanda presentada por 41 fiscales generales de distintos estados norteamericanos contra Meta, a la compañía la operación de llegar a un acuerdo le ha salido muy bien. El refranero español es sabio, aunque a veces se equivoque: "pleitos tengas y los ganes". No todo el mundo pierde. Cuando una de las partes ocupa una posición asimétrica o existe cualquier tipo de incentivo adicional, como tener un éxito político, negociar y aceptar un acuerdo puede resultar altamente beneficioso. Y eso en el fondo es lo que sucede a los ciudadanos comunes, y al parecer también a los Sres. fiscales, cuando se enfrentan a gigantes tecnológicos y económicos. Y estos han aprendido que tiene premio la ética de maximizar el beneficio a toda costa sacrificando cualquier valor.

A estas alturas nuestros lectores conocen con toda seguridad los pormenores del caso. Gracias a las filtraciones de ingenieros y responsables de desarrollo de producto, y después de muchos años, hemos podido saber que la compañía implantó un diseño sistemático para fomentar la adicción a sus plataformas en redes sociales. Debemos recordar que el valor central para la estrategia de negocio de Meta consiste en moverse rápido y romper cosas. Un correcto entendimiento de esta filosofía podría haber sido asumir que romper con los esquemas mentales establecidos constituye un valor en sí mismo en procesos de desarrollo de tecnologías de la información altamente disruptivos. Quién podía pensar que la ruptura que se nos proponía se refería en esencia a considerar que en la creación, programación y despliegue de una tecnología no se tendría en cuenta el ordenamiento jurídico ni los más elementales principios de la ética.

Dicho en términos coloquiales. La ética del desarrollo de software comparte elementos esenciales con la ética médica que viene prevaleciendo desde Hipócrates y que desde el punto de vista jurídico consagró Ulpiano en la antigua Roma: no hacer daño. En esencia, nos dijo el jurista hay que vivir honradamente (honeste vivere), no hacer daño a otro (alterum non laedere / neminem laedere) y dar a cada uno lo suyo (suum cuique tribuer). Así pues, desde el punto de vista jurídico hasta el último becario del soporte legal de la compañía conocía perfectamente que no era necesaria ninguna ley particularmente sofisticada para garantizar los derechos de las personas.

CONTINÚA EN LA PRÓXIMA PÁGINA



Y, sin embargo, a Meta se la demandó por conocer el carácter adictivo de sus aplicaciones, por estimular esta adicción mediante estrategias como el scroll infinito y las notificaciones hápticas y, sobre todo, por no tener el menor cuidado respecto de la protección de los niños, las niñas y los adolescentes. Por otra parte, y por si lo anterior fuese una mera banalidad, también parece que se conocían los efectos que el diseño gráfico y el brillo de las pantallas causaban en la perturbación del proceso del sueño. Si a ello le sumamos cuarto y mitad de perfilado algorítmico y generación de filtros burbuja que enganchan a personas en pleno desarrollo con contenidos tóxicos y peligrosos de modo recurrente, llegaremos a la conclusión de que el cóctel resultante es explosivo.

Pero no hay ningún problema. Al fin y al cabo, si fuiste rápido y rompiste cosas, es probable que te hayas convertido en un gigante económico. Así que, cuando te demandan para reclamar una cantidad indecente de dinero siempre puedes alcanzar un acuerdo políticamente relevante para las carreras de los fiscales, pero absolutamente inane desde el punto de vista de sus efectos. Al fin y al cabo, si has ingresado 300.000 millones de dólares en los últimos 5 años, si en los últimos dos el beneficio neto por ejercicio rondó los 60.000 millones, pagar hasta 18.000 millones en los próximos 10 años es poco menos que un regalo.

Y esto es así porque con ello has conseguido todos tus objetivos. Sin duda, el primero de ellos consiste en que no se practiquen pruebas en sede judicial y, en consecuencia, que no se someta a verificación la potencial existencia de una relación de causa-efecto entre el uso de tus redes sociales y el repunte de la enfermedad mental, las depresiones y los suicidios en la juventud de todos los países del mundo. El segundo gran objetivo alcanzado consiste en que no has sacrificado un ápice ni de tu diseño tecnológico ni de tu modelo de negocio. Un retoque aquí y allá, controlar las horas de conexión, "cantar el vamos a la cama para descansar" y reservar dos horas al día de enganche para los chicos.

Pero el más relevante es el último. No hace falta ser un gran economista para entender cómo el precio que la compañía ha abonado para hacer frente a la demanda es adecuado habida cuenta de lo ventajoso del acuerdo desde el punto de vista de la gestión del riesgo regulador. De hecho, podríamos afirmar sin temor a equivocarnos que se trata de una inversión prevista y particularmente bien ejecutada. Y esto, consolida materialmente la idea de que sale a cuenta infringir la ley. Y es aquí donde las lecciones aprendidas son particularmente preocupantes.
En el momento de escribir este artículo Mark Zuckerberg acaba de declarar que su compañía no va a implantar



ningún tipo de moratoria en el desarrollo de sus modelos de IA. En concreto ha venido a señalar que los laboratorios de IA tienen un fuerte incentivo para evitar que sus modelos causen daños, ya que de lo contrario podrían enfrentarse a una responsabilidad civil y legal significativa. Esta, que podría parecer una afirmación responsable, no lo es tanto si la juzgamos a la luz de las lecciones aprendidas por Meta Platforms, Inc. En realidad, lo que el señor Zuckerberg nos dice es que el riesgo regulador le sale a cuenta, que no va a parar máquinas. No va a retrasar ni un milisegundo sus objetivos y va a seguir moviéndose rápido, habida cuenta del potencial retorno de su inversión. Si la compañía ya ocupa una posición de práctico dominio de mercado en su nicho de negocio, si los datos que maneja alimentan grandes modelos, si se intuye que esta posición permitirá un despegue multipropósito que podría abrir nuevos escenarios y nichos de negocio: ¿por qué parar? Y, habría que preguntarse, si en esta carrera de nuevo podría estar dispuesto a romper cosas

Meta ha aprendido que el coste indemnizatorio resulta significativamente ridículo en relación con la expectativa de negocio. Por otra parte, no deben olvidar que esto es el mercado amigos, que ustedes son adultos responsables y que si la tecnología que desarrolla una multinacional y pone amable y gratuitamente a su disposición causa algún daño, seguramente sea por su propia culpa. ¿Y quién sabe? Puede que la Inteligencia Artificial acabe pensando lo mismo y obtenga sus propias lecciones. Esperemos que no decida moverse rápido y romper cosas.



RICARD MARTÍNEZ

Profesor en el Departamento de Derecho Constitucional, Ciencia Política y de la Administración y Director de la Cátedra de Privacidad y Transformación Digital. Doctor en Derecho por la Universitat de València. Miembro de la mesa de expertos en datos e Inteligencia Artificial de la Consejería de Innovación y Universi- dades de la Generalitat Valenciana. Miembro del grupo de expertos para la elaboración de una Carta de Derechos Digitales de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. Ha sido Presidente de la Asociación Profesional Española de la Privacidad y responsable del Área de Estudios de la Agencia Española de Protección de Datos.

LinkedIn:
https://www.linkedin.com/in/ricardmartinezmartinez/ Twitter: https://twitter.com/ricardmm

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Certificación en:

Gestión de la Inteligencia Artificial

ISO 42001 AI Management 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: 695,00 €
- 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

ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

Marcos Navarro

La empresa del Siglo XX y los trabajadores digitales

La empresa del siglo XX no está preparada para los trabajadores digitales del siglo XXI

Durante décadas hemos diseñado las empresas para coordinar personas y sistemas de información. La llegada de los agentes de inteligencia artificial introduce un tercer recurso: entidades digitales capaces de razonar, decidir y actuar. El reto ya no consiste únicamente en saber qué puede hacer la IA, sino en determinar cómo se controla a estos nuevos "trabajadores virtuales", qué permisos tienen, quién responde por sus decisiones y cómo se mide el valor que generan. Introducir agentes en una organización del siglo XX sin modificar su modelo operativo supone gestionar una realidad nueva con reglas antiguas.

Un nuevo activo empresarial

Las estructuras, procesos y mecanismos de control de las empresas parten de una premisa: el trabajo lo realizan personas apoyadas por sistemas. Una persona solicita una compra y otra la autoriza; un comercial registra una oportunidad en el CRM; Finanzas aprueba un pago; Recursos Humanos define responsabilidades; Sistemas concede accesos; y Auditoría y Compliance revisan lo ocurrido.

La tecnología tradicional ejecutaba aquello para lo que había sido programada. Un ERP no buscaba por iniciativa propia un proveedor alternativo ni un CRM negociaba con un cliente. Los agentes de IA empiezan a romper esa frontera: pueden recibir un objetivo, elaborar un plan, consultar información, utilizar herramientas, interactuar con otros agentes y actuar sobre sistemas corporativos con distintos grados de autonomía.

La diferencia también modifica el riesgo. Un asistente que redacta mal un correo genera un problema limitado; un agente conectado al ERP puede modificar datos, crear pedidos, conceder descuentos o comunicar información incorrecta a clientes. Estamos incorporando esta capacidad a procesos que nunca fueron diseñados para ella.

Agentes del siglo XXI en empresas del siglo XX

Durante años, la transformación digital consistió en digitalizar procesos existentes: primero se informatizaron los departamentos, después se conectaron las aplicaciones y, finalmente, se automatizaron tareas mediante BPM, workflows y RPA. Sin embargo, el modelo de operación permaneció estable: personas, procesos (cuando estaban definidos) y sistemas. La IA generativa introdujo asistentes que ayudan a las personas; los agentes añaden algo distinto porque pueden incorporarse al flujo de ejecución.

En un proceso de compras, un empleado detecta una necesidad, consulta proveedores, solicita ofertas, compara propuestas, negocia condiciones, introduce el pedido en el ERP y pide las aprobaciones correspondientes. Un agente podría consultar la demanda prevista, identificar necesidades, solicitar propuestas, comparar ofertas, preparar una recomendación, crear el pedido e incluso enviarlo si dispone de permisos suficientes.

La pregunta deja entonces de ser qué productividad proporciona la IA. Hay que saber quién autoriza al agente, con qué límites económicos opera, a qué información accede, qué decisiones requieren supervisión humana, cómo se revocan sus permisos y quién responde cuando se equivoca. Muchas organizaciones despliegan agentes sobre procesos concebidos bajo la hipótesis de que detrás de cada acción relevante existe una persona identificable. Ese supuesto empieza a dejar de ser cierto.

Alta Adopción y retorno incierto

El entusiasmo empresarial es considerable. KPMG señalaba en abril de 2026 que el 81 % de las organizaciones españolas estaba invirtiendo en incorporar agentes de IA, pero solo un 23 % había alcanzado el máximo nivel de madurez contemplado en su estudio y únicamente el 22 % se encontraba en una situación en la que la IA formaba parte del trabajo cotidiano. Además, solo una minoría declaraba haber establecido claramente el retorno de la inversión. Las empresas con buena visibilidad sobre los costes tenían cinco veces más probabilidades de conseguirlo.

El dato relevante es la distancia entre experimentar y obtener resultados económicos. Crear agentes resulta cada vez más sencillo; integrarlos en procesos, gobernarlos y conseguir un retorno sostenido es mucho más difícil. Antes de aprobar un proyecto, el comité de dirección debería preguntar qué indicador empresarial mejorará: coste por transacción, tiempo de resolución, conversión comercial, tasa de error, nivel de servicio o capacidad de trabajo reasignable.

Automatizar un proceso mediocre solo consigue que la mediocridad funcione más deprisa. Por eso el enfoque debe parecerse a la gestión de inversiones: valor esperado, coste total, riesgo, complejidad y plazo de retorno.

Gobierno, identidad y soberanía de los datos

La autonomía de los agentes introduce un cambio cualitativo en el riesgo. Un agente conectado al correo, al CRM, al ERP, a la banca, a plataformas cloud o a bases de datos puede convertirse en una identidad digital capaz de actuar en nombre de la organización. Por ello hay que definir quién es, quién responde por él, qué función desempeña, qué información consulta, qué acciones ejecuta, durante cuánto tiempo mantiene sus permisos y cuándo es obligatoria la aprobación humana.

A la gestión de identidades, permisos y actividad se añade la soberanía de los datos. La organización debe saber dónde se procesan, qué proveedor los recibe, qué información conserva, si puede emplearla para mejorar modelos, dónde se almacenan los registros de actividad y qué ocurriría si fuera necesario cambiar de proveedor.

CONTINÚA EN PRÓXIMA PÁGINA



> **La autonomía nunca debe crecer más deprisa que la capacidad de controlarla.**

En Europa, esta cuestión empieza a tener consecuencias regulatorias. Las obligaciones del AI Act para proveedores de modelos de propósito general incluyen documentación técnica, políticas relacionadas con copyright y transparencia sobre los contenidos utilizados para entrenamiento. Los modelos considerados de riesgo sistémico incorporan exigencias adicionales sobre evaluación de riesgos, incidentes y ciberseguridad. No obstante, cumplir la regulación debe considerarse el mínimo, no el objetivo: la cuestión empresarial es conservar el control cuando parte del trabajo la ejecutan entidades digitales autónomas.

Una función para gobernarlos a todos

Las personas requieren selección, contratación, definición de funciones, formación, evaluación y desvinculación. Los activos tecnológicos necesitan arquitectura, operación, seguridad y mantenimiento, mientras que Compliance establece normas, controles y evidencias. La incorporación de agentes plantea quién debe ocuparse de ellos.

Una posible respuesta es crear una función de Gestión de Recursos Digitales, AI Workforce Management, Oficina de Agentes o Digital Workforce Office. El nombre es secundario. Su misión no debería ser bloquear proyectos, sino permitir que la empresa utilice trabajadores virtuales de forma rentable, segura y controlada.

Sus responsabilidades incluirían el inventario corporativo de agentes, la asignación de un propietario humano, la definición de permisos y límites de autonomía, los criterios de supervisión, la trazabilidad, la seguridad, privacidad y propiedad de los datos, el código ético, la gestión de proveedores, los mecanismos de desconexión y los indicadores económicos. Esta función debe conectar Operaciones, Tecnología, Ciberseguridad, Riesgos, Compliance, Recursos Humanos y negocio, porque afecta simultáneamente a la tecnología, la organización del trabajo y la responsabilidad empresarial.

La ISO/IEC 42001 ofrece una referencia al plantear un sistema para establecer políticas, responsabilidades, procesos, evaluación y mejora continua alrededor de la IA. No resuelve por sí sola el problema, pero confirma que la inteligencia artificial empieza a necesitar un sistema de gestión empresarial propio.

Humanos y agentes en los mismos procesos

El futuro no debe plantearse como una competición entre personas y máquinas. La pregunta útil para un CEO es qué combinación de personas, sistemas tradicionales, automatización e IA produce el mejor resultado económico con un riesgo aceptable.

Algunas tareas seguirán siendo humanas porque requieren responsabilidad, empatía, negociación o criterio. Otras serán adecuadas para la automatización determinista mediante RPA, ya que sus reglas son estables. Algunas necesitarán IA como apoyo a profesionales y otras podrán ser ejecutadas por agentes con autonomía limitada. El modelo de operación deberá diseñar conscientemente esas fronteras.

La evolución puede organizarse en cuatro niveles: asistentes individuales, automatización de tareas, agentes conectados a sistemas y procesos autónomos de extremo a extremo. Cuanto mayor sea la autonomía, mayores deben ser las exigencias de gobierno, resiliencia y responsabilidad.

La autonomía nunca debe crecer más deprisa que la capacidad de controlarla.

Los riesgos de esperar y de avanzar sin control

Esperar puede parecer prudente, ya que la tecnología y la regulación evolucionan con rapidez. Sin embargo, no actuar también tiene un coste. Las organizaciones demasiado cautas pueden competir con empresas capaces de operar a menores costes, atender 24 horas al día, acortar tiempos administrativos o escalar sin incrementar proporcionalmente sus estructuras.

El extremo contrario es igualmente peligroso. Desplegar agentes sin gobierno puede generar costes difíciles de explicar, procesos fuera de control, accesos excesivos, fuga de información, incumplimientos y decisiones cuya responsabilidad nadie sabe dónde situar. El problema actual es que la autonomía aumenta antes de que las organizaciones dominen por completo su economía y su gobierno.

La agenda del comité de dirección

El CEO y el comité de dirección deben patrocinar la iniciativa de manera activa, no para crear un gran número de agentes ni para añadir burocracia, sino para rediseñar el modelo de operación (AI-Human Production System?). Esto exige definir el gobierno, integrar talento humano e IA, gestionar los datos y los riesgos y establecer una cartera de inversión centrada en procesos concretos.

Antes de entrar en producción, cada agente debería tener un propietario, un perímetro de actuación y un resultado económico esperado. Conforme avancen las iniciativas, una función corporativa debería mantener el inventario de agentes, modelos y proveedores; gestionar identidades y permisos; definir guardarraíles y supuestos de intervención humana; supervisar la privacidad, la propiedad intelectual y la soberanía de los datos; registrar incidentes; y medir el coste, la productividad, la calidad y el retorno.

La decisión final debe seguir perteneciendo a una persona cuando afecte al dinero, al empleo, a compromisos contractuales, a información sensible, a la seguridad o a cuestiones con consecuencias relevantes para clientes y ciudadanos. Además, cada agente debería contar con una ficha de puesto digital que recoja su misión, propietario, sistemas accesibles, datos autorizados, acciones permitidas, límites económicos, nivel de autonomía, indicadores, mecanismos de auditoría y procedimiento de desconexión.

La pregunta no es cuántos agentes tendremos

Durante los próximos años veremos miles de agentes incorporarse a las empresas. Algunos trabajarán junto a empleados; otros interactuarán con clientes y proveedores; y también habrá agentes que supervisen a otros agentes o sistemas multiagente que ejecuten procesos hoy repartidos entre varios departamentos.

Sin embargo, disponer de muchos agentes no hará que una empresa sea avanzada, del mismo modo que tener más empleados no garantiza mayor productividad. La ventaja competitiva estará en diseñar mejor el sistema completo: personas donde el juicio humano aporte valor; sistemas donde las reglas sean suficientes; IA donde ayude a interpretar y decidir; y agentes donde la autonomía produzca una ventaja económica demostrable. Todo ello debe operar bajo un modelo común de responsabilidad, seguridad, datos y gobierno.

Durante el siglo XX aprendimos a gestionar organizaciones formadas por personas y sistemas, y en las primeras décadas del XXI digitalizamos buena parte de ellas. Ahora debemos aprender a dirigir empresas en las que no todos los que trabajan son personas. La pregunta ya no es si una empresa necesita agentes de inteligencia artificial, sino si está preparada para gobernarlos cuando lleguen.



MARCOS NAVARRO ALCARAZ

Consultor experto en Tecnologias de la información y ha sido ejecutivo de TI en varias compañias multinacionales. Ahora es experto en Outsourcing de TI, Robots y Autoamtizacion y es profesor universitario y en escuelas de negocio.

Twitter:
https://twitter.com/mnalcaraz

LinkedIn:
https://www.linkedin.com/in/mnalcaraz/

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Certificación en:

Excelencia en el Servicio

ISO 23592 Service Excellence Leader

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 23592
- 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



Víctor Almonacid



En el término medio está la virtud

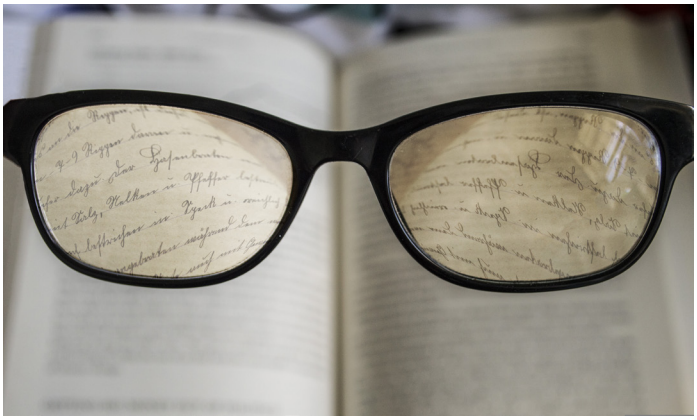


La inteligencia artificial ya trabaja dentro de las organizaciones públicas: redacta borradores, resume expedientes, ordena datos, prepara respuestas y sugiere caminos. La pregunta ya no es si conviviremos con ella, sino cómo dirigir cuando una parte relevante del trabajo intelectual puede hacerse con una rapidez desconocida.

El término medio no consiste en repartir cautelas y entusiasmos por igual, sino en situar cada cosa en su lugar. La IA puede reducir carga burocrática, detectar patrones y liberar tiempo; pero no sabe por sí misma qué merece protección, qué excepción importa o quién debe responder por una decisión. Su utilidad depende del juicio que la encuadra. Sin dirección, una herramienta potente puede acabar automatizando inercias. El riesgo no está solo en el error técnico, sino también en la apariencia de certeza. Un texto bien construido puede parecer más verdadero de lo que es; una recomendación rápida puede ocultar supuestos discutibles. La delegación silenciosa del criterio empieza cuando la respuesta llega antes, suena razonable y nadie reserva tiempo para comprobarla.

Por eso algunas capacidades humanas vuelven al centro: preguntar bien, distinguir lo automatizable de lo indelegable, escuchar lo que no cabe en un dato y sostener una decisión ante quienes resultan afectados. Cuanto más eficaz sea la máquina en ciertas tareas, más visible será lo que no puede hacer en nombre nuestro.

CONTINÚA EN PRÓXIMA PÁGINA



Ese juicio, además, no se ejerce en abstracto. Lo ejerce alguien sometido a prisa, cansancio, presión política, hábitos adquiridos y una determinada manera de tratarse a sí mismo. Una persona agotada puede usar la tecnología para ocultar su falta de presencia; un equipo saturado puede convertir una herramienta de ayuda en otra fuente de exigencia.

También aquí conviene el término medio: ni convertir el autocuidado en retórica blanda ni despreciarlo como asunto privado. La atención, el descanso, la escucha y el autocontrol forman parte de la responsabilidad institucional, porque quien decide desde la fatiga o desde el piloto automático deja huella en la organización.

La transformación no será solo digital, ni se resolverá con discursos genéricos sobre liderazgo humano. Harán falta reglas, trazabilidad, formación técnica y controles; pero también culturas capaces de preguntar para qué se automatiza, qué se pierde al hacerlo y quién responde si algo falla. Esa tarea puede llamarse **Gobernanza de la Inteligencia Combinada** —GIC—: un enfoque directivo que ordena la relación entre inteligencia humana, sistemas de IA, datos, normas, valores, procesos y responsabilidades.

La GIC no se limita a incorporar herramientas. Determina qué tareas debe realizar cada tipo de inteligencia, con qué finalidad, límites y controles, y bajo qué régimen de supervisión y rendición de cuentas. Para la función directiva, implica evitar tanto la fascinación tecnológica como la resistencia estéril: aprovechar la capacidad de cálculo, análisis y generación de la máquina sin abdicar del juicio humano.

Un recorrido práctico empieza por revisar tareas: cuáles conviene automatizar, cuáles solo apoyar y cuáles deben permanecer bajo deliberación humana. Después habrá que mirar el modo de dirigir, cuánto espacio real existe para pensar, qué conversaciones se evitan y qué uso de la tecnología aumenta —o reduce— la responsabilidad. Solo entonces tienen sentido los protocolos, porque sin cultura acaban siendo papeles de cumplimiento.
La finalidad no es poner máquinas a producir más sobre organizaciones exhaustas, sino retirar carga inútil, mejorar el análisis y devolver tiempo a lo que requiere criterio: comprender un caso, hablar con quien discrepa, explicar una decisión, corregir un error y aprender de la experiencia. Una administración más automática no será necesariamente mejor; lo será si la automatización la hace más atenta, responsable y clara.

Dirigir cuando la máquina responde exige una virtud antigua, la prudencia. La mesura, el sentido común de toda la vida. Pero no para frenar por sistema, ni para acelerar sin criterio, sino para poner cada inteligencia en su sitio. La máquina puede ayudar mucho si no sirve para esconder decisiones, acelerar errores o empobrecer la conversación pública. La inteligencia emocional, los valores públicos y el sentido común siguen siendo esenciales. Gobernar la inteligencia combinada significa, en síntesis, gobernar la inteligencia con inteligencia.



VÍCTOR ALMONACID

Secretario de la Administración Local, categoría superior. Director de Prevención, Formación y Documentación en la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana. Directivo Público. Máster en Nuevas Tecnologías aplicadas a la Administración Pública. Máster en Planificación estratégica. Tiene o ha tenido presencia activa en las siguientes asociaciones: ADPP, COSITAL, RECI, UDITE, ADPP, AENOR y equipo técnico de la FEMP. Autor de numerosas publicaciones, especialmente en el ámbito de la administración electrónica práctica (procesos, organización, planificación, procedimiento...). Responsable de la implantación de diversos proyectos reales en dicho ámbito, dentro de varias Adminis- traciones Públicas. Entre otros reconocimientos: Medalla de la Vila del municipio de Picanya, Premio CNIS al innovador público del año 2015, Premio NovaGob Excelencia 2015 al mejor Blog, Premio internacional al mejor innovador en las Administraciones Públicas en el año 2020.

LinkedIn:
https://www.linkedin.com/in/victoralmonacid/
Twitter:
https://twitter.com/nuevadmon
Blog:
http://nosoloaytos.wordpress.com/

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Certificación en:

Diseño de Servicios Excelentes

ISO 24082 Service Excellence Designer

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 24082
- 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



Marta Martín

Del caos a la oportunidad: emprender con TDAH

Creatividad, impulsividad, entusiasmo y búsqueda constante de nuevos retos. El perfil de algunas personas con TDAH puede encajar con determinados aspectos del emprendimiento. La clave reside en conocer las fortalezas y gestionar las dificultades.

No hay duda de que la relación entre TDAH y emprendimiento despierta un interés considerable en diversos foros. Las redes sociales, los medios de comunicación y las comunidades empresariales son cada vez más conscientes de que el perfil emprendedor y el TDAH están estrechamente relacionados.
Una asociación que tiene sentido si tenemos en cuenta que emprender suele asociarse con asumir riesgos, detectar oportunidades donde otros no las ven y tener la capacidad de convertir una idea en un proyecto. Pero también implica hacer presupuestos, responder correos, cumplir plazos, organizar reuniones, revisar documentos y repetir tareas poco estimulantes sobre todo para los cerebros neurodivergentes.

PROS Y CONTRAS

Es decir, hablar del perfil emprendedor del TDAH puede resultar engañoso. Pero vayamos por partes. Estos son algunos de los rasgos que se presentan como posibles fortalezas.

- **Creatividad y generación de ideas:** la capacidad de establecer conexiones rápidas entre conceptos y encontrar soluciones alternativas a los problemas.
- **Curiosidad y novedad: l**os entornos cambiantes y los nuevos proyectos suelen resultar estimulantes.
- **Capacidad para asumir retos** o la facultad de convertir los desafíos en una motivación.
- **Hiperfoco**, es decir, una concentración intensa cuando un tema despierta un interés.
- **Adaptabilidad** ya que la necesidad de enfrentarse a situaciones nuevas favorece la capacidad de reaccionar ante cambios y problemas inesperados.
- **Iniciativa:** el impulso de poner en marcha nuevas ideas puede facilitar que una persona pase rápidamente de detectar una oportunidad a intentar desarrollarla.
- **Pensamiento poco convencional:** cuestionar las formas establecidas de hacer las cosas ayuda a identificar productos, servicios o modelos de negocio diferentes.

CONTINÚA EN PRÓXIMA PÁGINA



Pero hay una cara B. Estas características también pueden generar dificultades como empezar muchos proyectos y no terminarlos, tomar decisiones impulsivas, procrastinar, tener problemas para organizar el tiempo o perder interés cuando desaparece la novedad.

•**El impulso de empezar.** Tener una idea puede llevar unos minutos. Desarrollarla requiere meses o incluso años de trabajo. Y es en ese recorrido donde pueden aparecer algunas de las mayores dificultades ya que la novedad proporciona estímulo, pero la rutina resulta mucho más difícil de sostener. De ahí que una de las habilidades más importantes no sea aprender a generar más ideas, sino a decidir cuáles merecen convertirse en proyectos.

•**Organización.** Detrás de una presentación atractiva o de una idea innovadora existe una enorme cantidad de trabajo administrativo, tareas especialmente difíciles cuando no despiertan interés inmediato. No porque no sepan hacerlas, sino por la dificultad en iniciarlas, priorizarlas o mantener la atención hasta terminarlas.

•**Ceguera temporal o la dificultad para percibir,** calcular y gestionar correctamente el paso del tiempo, lo que se traduce en problemas para saber cuánto tiempo ha pasado, cuánto se necesita para realizar una tarea o cuánto falta para un plazo.

•**Dificultad para delegar.** La autoexigencia o el perfeccionismo de algunos cerebros neurodivergentes pueden llevar a un emprendedor a querer abarcar todos los aspectos del negocio y evitar delegar.

•**La impulsividad tan oportuna** en determinadas circunstancias, pero tan peligrosa en el entorno empresarial. Por ello, es necesario introducir pequeñas barreras antes de tomar decisiones importantes. La idea no es frenar la iniciativa, sino ponerle un marco.

Llegados a este punto, ¿es el TDAH una ventaja para emprender?

LA RESPUESTA ES: NO NECESARIAMENTE.

Hay que ser especialmente cuidadosos con la idea de que el TDAH es un superpoder. No hay duda de que, en muchas ocasiones, puede estar asociado a determinadas fortalezas, pero también puede generar dificultades que afectan seriamente a la vida profesional.

Cada emprendedor tiene una combinación diferente de habilidades, experiencias, intereses y complicaciones. El TDAH es solo uno de los elementos de ese conjunto. Y no todas las personas con TDAH son especialmente creativas. No todas disfrutan asumiendo riesgos. No todas quieren emprender. Y tener TDAH no garantiza una mayor capacidad empresarial.



Pero sin duda, el emprendimiento ofrece ventajas para los neurodivergentes que les permite desarrollar todo su potencial. Por ejemplo, la capacidad y la autonomía para diseñar el trabajo alrededor de sus fortalezas. De esta forma, tiene libertad para trabajar en los momentos del día en los que se concentre mejor, ocuparse de las tareas más estimulantes y estructurar aquello que le resulte más abrumador.

Sin olvidar que, lo más importante es conocer cómo funciona su TDAH y cómo debe gestionar los aspectos más inconvenientes. Así que, es fundamental identificar qué situaciones provocan más distracción, qué tareas suelen posponerse, cuándo aparece la impulsividad o qué condiciones favorecen la concentración.

En lugar de interpretar cada dificultad como un defecto personal, puede convertirse en información para diseñar el entorno de trabajo. Se trata de reducir la distancia entre lo que quiere conseguir y la manera en que realmente funciona.

EMPRENDER SIN ROMANTIZAR EL TDAH

La conversación sobre TDAH y emprendimiento puede ser positiva siempre que se aleje de los extremos y de la visión romántica de esta condición como un superpoder. Las personas con TDAH no son buenas emprendedoras simplemente por su condición. Algunas pueden encontrar en el emprendimiento un entorno en el que determinadas características de su forma de funcionar —como la creatividad, la curiosidad o la búsqueda de nuevos retos— encajan especialmente bien. El éxito, sin embargo, depende también de desarrollar estrategias para compensar las dificultades de organización, planificación y constancia.



MARTA MARTÍN

Mujer diagnosticada con TDAH en su madurez, como tantas otras, en una de las revisiones de TDAH de su hijo. Licenciada en Periodismo y Derecho, actualmente cursa sus estudios de Doctorado en Ciencias de la Información y está escribiendo su primera novela. Trabaja en el sector audiovisual y es profesora en la Escuela de Artes Escénicas de Madrid (TAI). Consciente de que el día a día de una mujer adulta con TDAH no es fácil pero tampoco es imposible, ha creado un canal de youtube, Mujeres al borde del TDAH, y una cuenta de instagram con el mismo nombre, para divulgar y ayudar a los adultos que lo padecen.

LinkedIn:
https://www.linkedin.com/in/marta-mart%C3%ADn-garc%C3%ADa-463a5a2a
Youtube:
https://www.youtube.com/channel/UCn02bjVXA3q9GP0_23DRwIw
Instagram:
https://www.instagram.com/mujeresalbordedeltdah/

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Certificación en:

Gestión de Centros de Operaciones de Seguridad (SOC)

SOC Management Leader

Docente:
Alejandro Aliaga

- Formato: Grabado con Tutorías
- Tutorías en directo: Lunes Tardes
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Importe del Curso: 995€
- Tasas Examen: Incluidas
- En tu horario, a tu ritmo.
- Con toda comodidad
- Solicita tu admisión

MidMgmt® MPPM® MGEIT® eGob®

Tutorías en Directo

+ 34 96 109 44 44
admisiones@escueladegobierno.es
https://escueladegobierno.es



ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

Crónica de la XI edición de la RootedCon Valencia

Como ya es tradición en Valencia, a la vuelta de las vacaciones se celebra en el Museo de las Ciencias Príncipe Felipe de la Ciudad de las Artes y las Ciencias la que es probablemente mejor conferencia en materia de ciberseguridad y tecnología que disfruta la ciudad: la RootedCon Valencia. En esta ocasión, se celebró el pasado 18 de septiembre, y al contrario que en las últimas ediciones, ésta no vino precedida de una jornada de formación adicional.

La jornada comenzó con una apertura a cargo de Alberto Rodríguez, coordinador de Rooted en Valencia, en la que, tras los pertinentes agradecimientos a patrocinadores y personas presentes, realizó un rápido repaso a las actividades de la organización este año, en la que han celebrado eventos en Madrid, Lisboa, Panamá, y por supuesto, Valencia. También anunció en primicia que para 2027 van a extender su foco para lanzar un evento RootedCon en Dublín. También aprovechó la ocasión para rendir un pequeño homenaje a Jose Manuel Vera, miembro de la Revista SIC, colaborador de

la asociación, y que falleció antes del verano. Para terminar, Alberto Rodríguez repasó las acciones de lucha contra los bloqueos de La Liga, actualmente ante el Tribunal Constitucional, y contra el mecanismo Chat Control que la UE trata de imponer, y que supone un riesgo para todos los ciudadanos europeos.

Tras la keynote de apertura, comenzó la primera ponencia, a cargo de Roger Sanz, titulada *"AgenticAI Rebellion: Rogue Agents Behaviour. Detecting, Explaining and Killing Runtime"*. Inició la ponencia con una definición del significado que la expresión "agente de IA" tenía en el contexto de la charla, y con un detalle de las funciones que suelen realizar estos elementos tecnológicos. Para poder ser útiles, los agentes tiene diferentes componentes: las habilidades (o *skills*), que son las que definen las acciones que el agente de IA va a realizar y que pueden adquirirse en *markerplaces* específicos; y el manifiesto del agente, donde se publica qué se supone que puede hacer dicho agente y sus *skills*. Obviamente, una de las razones por las que se mencionaron estos conceptos en este tipo de conferencia es porque puede haber maliciosidad en esos mercados para inyectar skills maliciosas en los equipos de los clientes.

CONTINÚA EN PRÓXIMA PÁGINA


STAFF

Para demostrarlo, el ponente explicó un caso de laboratorio en el que un agente trabajó como se esperaba de él durante 37 días, pero realizó una acción inesperada 38º día. Puso de relieve que no se dispone de elementos de control sobre los agentes, ya que salvo determinados agentes muy concretos, todos trabajan de forma no determinista, y por tanto, pueden arrojar resultados inesperados o no deseados. Continuó el ponente comentando algunos incidentes en los que agentes de IA borraron bases de datos en producción, por ejemplo, poniendo el foco en la dificultad de asignar la culpa de ese incidente, ya que en realidad la raíz del problema, en su opinión, generalmente es una deficiencia en la arquitectura de despliegue de los agentes.

Curiosamente, el ponente también comentó el caso de Hugging Face - OpenAI, manifestando que no se creía mucho las explicaciones oficiales de las compañías implicadas. La inexistencia de mecanismos de control sobre lo que están haciendo los agentes de IA (observabilidad), es lo que, a juicio del ponente, hace que cualquier desviación sobre el resultado esperado por el ser humano se considera una rebelión de los agentes. Y esa categoría incluye también las *skills* envenenadas que realizan acciones maliciosas, aprovechando que no hay un estudio serio del funcionamiento interno del agente antes de su puest en producción. Súmese a eso el uso de credenciales de los usuarios humanos, y se obtienen incidentes casi imposibles de investigar en la realidad.

Roger Sanz puso de manifiesto la enorme dificultad de poder desarrollar el proceso clásico de respuesta a este tipo de incidentes, por la rapidez en que se va produciendo y la necesidad de investigarlo, por lo que es necesario disponer de un *kill switch* para detener el proceso agéntico, algo que no es tan fácil de implementar. También existe una dificultad intrínseca en la detección de cuándo se produce un incidente generado por un agente de IA, ya que hay que relacionar el manifiesto, con las acciones realizadas, y definir unos umbrales de confianza, dado el carácter no determinista de esta tecnología. Terminó la primera ponencia con una demo de este tipo de situaciones de “rebelión” de agentes de IA y la dificultad de detenerlos.

CONTINÚA EN PRÓXIMA PÁGINA


/Roota



Tras el descanso para el café, Daniel Haro y Carles Cano continuaron la jornada con la charla *"Grappling with new technologies: Supabase common pitfalls"*, en la que explicaron, en una charla muy técnica y especializada, su metodología para el uso de Supabase y los consejos para no cometer errores habituales con la misma al evaluar nuevas tecnologías de integración de software.

Supabase es una plataforma SaaS para el despliegue de aplicaciones en la Nube. Por tanto, es necesario poder hacer pentesting sobre esas aplicaciones, y que en realidad, pasa por hacer *pentesting* de la propia plataforma. La ponencia centró buena parte de su duración en ejemplificar los errores de desarrollo que los ponentes han detectado en sus *pentesting* y que son fáciles de evitar. Como conclusión final, recalcaron la necesidad de hacer buenas configuraciones para evitar determinados tipos de incidentes de seguridad.

La tercera ponencia, y última de la mañana, corrió a cargo de un clásico en los eventos de Rooted, Tomás Isasia, en el que, bajo el título de "*Prompt Injection en el Buzón: Evadiendo defensas de correo basadas en ML y cómo construir un contra-agente local con SLMs*", el ponente describió, con su habitual sentido del humor, un caso de enfrentamiento entre una IA ofensiva y una IA defensiva, mediante una prueba de concepto.

La motivación de la charla nació al detectar el ponente que no hay soluciones de seguridad adaptadas a microPYMES o usuarios domésticos, que están abandonados por las compañías del sector. Como ya indicó el primer ponente, Tomás recalcó la obsolescencia del proceso de gestión de ciberincidentes ante los ataques potenciados por IA, e indicó que, en su opinión, la única estrategia de defensa posible es asegurar el *endpoint* del usuario con nuevas técnicas que le protejan ante estos ataques. Más si cabe, cuando existen modelos de LLM descargables de forma abierta en los que no hay guardarailes éticos o técnicos, y que son utilizados por los ciberdelincuentes. Lo que provoca una asimetría clara entre atacantes y defensores.

Por eso la ponencia continuó planteando la conveniencia de instalar en los PC de los usuarios de LLM ligeros, que ayuden a éstos ante determinados tipos de ciberincidentes, como el *phishing*. Por ello, el ponente hizo una demo tanto de un componente ofensivo potenciado con IA para generar correos de *phishing* hiper-personalizados, y que supera los filtros tradicionales anti-spam y anti-phishing, como de otro componente defensivo que en pocos segundos analiza esos correos para descartarlos como maliciosos.

CONTINÚA EN PRÓXIMA PÁGINA

La idea del componente defensivo es utilizar una especie de detección semántica, en base al comportamiento percibido por el receptor respecto del emisor. Es algo similar a cómo los seres humanos reconocemos a nuestro conocidos incluso sin verles la cara, por otras características como la forma de andar y similares.

Tras el descanso para comer, se llevó a cabo la cuarta ponencia, a cargo de Alejandro López, CEO de la compañía Slimbook, que bajo el título de "Exhibición de la placa al token: montamos todo el hardware de una estación multi-GPU para IA local" en la que presentó una sesión totalmente práctica sobre qué hace falta realmente para ejecutar inteligencia artificial moderna en un equipo local, más allá del marketing habitual. La charla recorrió desde los fundamentos hasta la elección de CPU, GPU, plataforma y software para desplegar modelos de lenguaje en infraestructura propia.

A partir de dos equipos de la compañía equipades con dos GPU diferentes de NVIDIA, se compararó el comportamiento del mismo modelo de lenguaje, analizando rendimiento, consumo, memoria y límites reales de cada configuración. También se abordaron otras arquitecturas como Ryzen, Threadripper y DGX Spark, y en qué escenarios tiene sentido cada enfoque.
Durante la charla se hicieron demostraciones en directo de *benchmarking e indirect prompt injection*. También se abordaron cuestiones como la soberanía del dato y su jurisdicción, cuando código, logs, credenciales o prompts abandonan la infraestructura propia y pasan por servicios cloud.

CONTINÚA EN PRÓXIMA PÁGINA




CONGRESO DE CIBERSEGURIDAD & TECNOLOGÍA
Rooted°
VALENCIA
DIAMANTE
TARLOGIC
CYBERSECURITY EXPERTS
VARGROUP
INSTITUCIONAL
ccn-cert
ANY RUN


The entry point
/Rooted
A poisoned skill can be a silent entry point.
/Rooted VALENCIA
TARLOGIC
VARGROUP



Como conclusión, se plantearon criterios prácticos para decidir qué cargas puede merecer la pena ejecutar en local, con qué hardware y bajo qué modelo de seguridad, mostrando de forma transparente tanto las ventajas como las limitaciones de una arquitectura de IA privada.

La quinta ponencia corrió a cargo de Jorge Martínez, responsable del proyecto Hack the Music de Rooted, con un título provocativo: "Hack(ing) the Music - Robando propiedad intelectual". Jorge comenzó la ponencia con varios ejemplos de incidentes de ciberseguridad a la industria musical en los últimos 10 años, con afectados como Madonna, U2, Lady Gaga, Ed Sheeran o Elton John, en los que se robaron demos de esos artistas e informaciones contractuales o datos personales.
A continuación, el ponente revisó algunos aplicativos utilizados en los proyectos musicales de Hack the Music y varios conceptos de tratamiento de audio con esos aplicativos. Finalmente, disertó acerca de las capacidades de inyección de código malicioso en algunas de dichas aplicaciones musicales, y las respuestas poco halagüeñas de los fabricantes ante los informes de los expertos en ciberseguridad sobre las vulnerabilidades de sus productos.

Tras una pausa para estirar las piernas, la sexta ponencia de la jornada fue realizada por Mario Lobo, con el título de "*AIMARU C2: The New Era of LotL (MCP AI-Driven C2)*". La charla comenzó con una introducción de los conceptos y datos necesarios para entender el resto de la misma. Como por ejemplo, que el 85% de los incidentes no provienen de ningún malware, o el actual florecimiento de la economía del Ransomware-as-a-Service. Un dato remarcable que aportó el ponente es la tendencia actual en la que los agentes maliciosos utilizan las herramientas legítimas presentes en los sistemas atacados siempre que sea posible, formando parte de una estrategia de minimizar o evitar que los archivos maliciosos toquen el disco del equipo atacado, a la que se ha venido a dar el nombre de "*Living-of-the-Land*" (LotL). Si todo esto se une a la potencia de los sistemas de IA, el panorama se complica extraordinariamente para los defensores.

CONTINÚA EN PRÓXIMA PÁGINA



El ponente continuó la charla con la presentación de un *framework d*e mando y control (o C2), al que han bautizado como AIMARU, y que han desarrollado como prueba de concepto de lo que se puede hacer combinando tecnologías legítimas como Powershell, LLMs y el protocolo MCP. Con un entorno de este tipo, cualquier atacante sin conocimientos de ciberserguridad ofensiva podría lanzar ataques de toma de control de *endpoints* sin esfuerzo, sin conocimientos previos, y de forma indetectable para la seguridad de los equipos Windows.

Finalmente, en sus conclusiones el ponente explicó las ventajas de usar este tipo de herramientas por parte de los equipos de Red Team, de manera que puedan testear las capacidades defensivas de las organizaciones auditadas, y el impacto en el Blue Team, debido a los desafíos que las conclusiones del uso de este *framework* plantea para las reglas de detección, la respuesta a incidentes y el *Threat Hunting proactivo* en entornos donde los binarios del sistema y la IA actúan en conjunto.

La séptima y última ponencia del congreso corrió a cargo de Mar Llambí, con el título “Cierra los ojos y verifica: zk-Auth para agentes que no puedes (ni debes) ver”, en la que la ponente comenzó explicando la gran diferencia existente entre la autorización de aplicaciones deterministas y de las no deterministas, como los agentes de IA. Y la pregunta que planteó (y trató de resolver como investigadora pre-doctoral) fue cómo validar a los agentes de IA en entornos corporativos, de manera que tanto el agente como en sistema de validación conozcan el conjunto de información que realmente han de conocer, para lo cual usó una analogía con un portero de discoteca. Esta persona debe asegurarse de que quien quiera acceder a la misma tiene al menos 18 años, y para eso, pide que le enseñen el carnet de identidad. Pero al hacerlo, el portero tiene acceso a mucha otra información que no necesita para esa función.

Para resolver esa cuestión, la ponente propuso un *framework (zk-Auth)* que sea capaz de validar cual es la intención del agente para alcanzar sus objetivos en un contexto determinado con la mínima cantidad de intercambio de información. La ponencia, de una elevada complejidad técnica, continuó con las premisas criptográficas que permitirían que un agente pueda realizar su misión de forma autorizada sin que se pueda filtrar excesiva información del mismo. Es decir, que se pueda autorizar a un agente sin exponer datos, prompts ni pesos en ese proceso, en un nuevo paradigma de las transacciones entre sistemas autónomos.

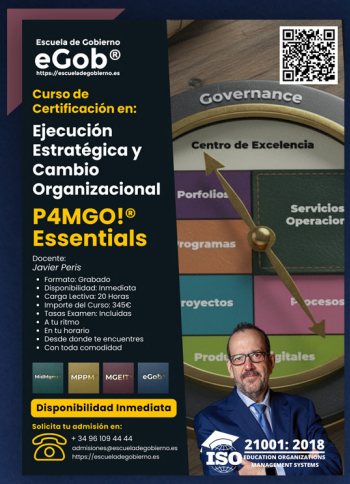
La demo que la ponente realizó se basó en requerir a un agente hacer un merge GitOps y una rotación de credenciales, pero solo si demostraba, sin revelar datos sensibles, que cumplía ciertas políticas definidas.

Con esta ponencia se dio por terminada la jornada, que una vez más reunió a un nutrido grupo de asistentes, deseosos de disfrutar no sólo de un elenco de ponentes de alto nivel, sino también de ese contacto personal con otros profesionales y empresas del sector.

Escuela de Gobierno eGob®

https://escueladegobierno.es

Competencias Directivas en **Ejecución Estratégica** y **Cambio Organizacional**





















ISO 21001: 2018
EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

IMQ CERTIFIED
QUALITY MANAGEMENT SYSTEM
ISO 9001:2015

IMQ CERTIFIED
MANAGEMENT SYSTEM FOR EDUCATIONAL ORGANIZATIONS
ISO 21001:2018

UNE celebra sus 40 años de apoyo a la industria y la sociedad

El Grupo UNE (liderado por la Asociación Española de Normalización junto a sus sociedades participadas: AENOR y CEISLAB) ha conmemorado los 40 años de su creación en el Museo del Prado. Cuatro décadas en las que un equipo constituido por más de 1.600 personas ha contribuido, a través de las normas, al progreso compartido de la sociedad y a reforzar la competitividad de las empresas, tanto en el ámbito nacional como en los mercados internacionales.

Con motivo de esta ocasión tan especial, Grupo UNE estuvo acompañado por el subsecretario de Industria y Turismo, Pablo Garde; el presidente de CEOE, Antonio Garamendi; y el presidente de la Cámara de Madrid, Ángel Asensio; junto a más de 150 personas, representantes de la vida empresarial y social del país.

CONTINÚA EN PRÓXIMA PÁGINA





El presidente del Grupo UNE, Alfredo Berges, rememoró el origen de la organización: "unos sectores industriales y la administración coincidimos en que era imprescindible dar a las empresas españolas herramientas para competir en igualdad de condiciones dentro y fuera de nuestras fronteras. En el Grupo UNE se respiran parámetros de seguridad, calidad, innovación, competitividad, sostenibilidad y tecnología. Todo ello nos lleva a fijar objetivos ligados al crecimiento de las empresas y al progreso de la sociedad, creando mercados más seguros, competitivos, sostenibles, innovadores y conectados".

Por su parte, el presidente de CEOE, Antonio Garamendi, destacó que: "40 años es una cifra importante y significa un bagaje, porque la normalización es la clave para ganar la globalización y el futuro".
El subsecretario de Industria y Turismo, Pablo Garde, reconoció que: "estos años han sido un compromiso con la calidad y la excelencia, además la normalización es un instrumento de confianza para el país y para sus sectores, acompañando a España en una verdadera modernización e internacionalización del país, junto a un desarrollo tecnológico e industrial inédito".

Cuarenta años en el que se ha conformado un ecosistema formado por sectores empresariales, representantes de la administración central y autonómica, universidades y centros de investigación, unidos para celebrar todo lo construido y hacer historia del grupo.



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.

UNE Normalización Española

Progreso compartido

une.org

Deja de perder el tiempo intentando Gestionarlo
y aprende definitivamente a Gobernarlo.



Time Slot Governance TSG4 White Belt

Porque lo que no es Método es Improvisación

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

amazon