

REVISTA **Tecnología & Sentido Común**



#53

JUNIO
2025

**Andoni
Serrano**

NUESTRO INVITADO
A #TYSC

24

El Gubernauta

JAVIER PERIS

08

**Futuro y
Seguridad**

MANUEL SERRAT

12

**Tecnoregulación
en Prospectiva**

NACHO ALAMILLO

16

Radio Security

ALEX ALIAGA

50

Ai Futuro

MARCOS NAVARRO

42

Es tendencia

MARLON MOLINA

34

**La nueva
Administración**

VÍCTOR ALMONACID

46

**Diario de una
tortuga ninja**

JUAN CARLOS MURIA

20

**Mentes
Divergentes**

MARTA MARTÍN

54



REVISTA **Tecnología & Sentido Común**



EQUIPO TYSC

Javier Peris - El Gubernauta

Manuel Serrat - Futuro y Seguridad

Nacho Alamillo - Tecnoregulación en Prospectiva

Juan Carlos Muria - Diario de una Tortuga Ninja

Marlon Molina - Es Tendencia

Ricard Martínez - Ojo Al Dato

Marcos Navarro - Ai Futuro

Víctor Almonacid - La Nueva Administración

Alex Aliaga - Radio Security

Marta Martín - Mentas Divergentes

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://tecnologiasentidocomun.com>

soluciones@businessandcompany.com



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

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

ISSN 2951-8180



Normas al día, solo *on line*

¡Aprovecha todas las ventajas!

- Accesible desde cualquier dispositivo
- Búsqueda sencilla de contenidos
- Facilidad para compartir, imprimir y archivar

Disponible en: revista.une.org

#53

JUNIO 2025



índice

DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



NUESTRO
INVITADO
A #TYSC

24

Andoni Serrano



ES TENDENCIA

34

**Las tabletas son tendencia
y muestran cómo será**



AI FUTURO

42

**El Ecosistema Energético
de 2034**



MENTES
DIVERGENTES

54

**Insomnio, cuando la
mente no se calla**

Copyright

02

Índice de Contenidos

04

Este mes te recomiendo leer...

por JAVIER PERIS

07

¿Es Posible Gobernar la Inteligencia Artificial sin Gobernar el Dato y/o sin Gobernar la Tecnología?

EL GOBERNAUTA
JAVIER PERIS

08

Vivir sin acceso al Oráculo de Delfos: medir para proteger

FUTURO Y SEGURIDAD
MANUEL SERRAT OLMOS

12

Acuerdo sobre algoritmos criptográficos post-cuánticos

TECNOREGULACIÓN
EN PROSPECTIVA
NACHO ALAMILLO

16

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

DIARIO DE UNA
TORTUGA NINJA
JUAN CARLOS MURIA

20

Andoni Serrano

NUESTRO
INVITADO A TYSC

24

Las tabletas son tendencia y muestran cómo será 2030

ES TENDENCIA
MARLON MOLINA

34

¿Y ahora vamos a simplificar o a desregular?

OJO AL DATO
RICARD MARTÍNEZ
MARTÍNEZ

38

El Ecosistema Energético de 2034

AI FUTURO
MARCOS NAVARRO

42

Apagón de inteligencia

LA NUEVA
ADMINISTRACIÓN
VÍCTOR ALMONACID

46

Así se protege una infraestructura 5G frente a ciberataques

RADIO SECURITY
ALEX ALIAGA

50

Insomnio, cuando la mente no se calla

MENTES DIVERGENTES
MARTA MARTÍN

54

La Rioja reflexiona en las Project Sessions 2025 sobre las organizaciones que “cambian el paso” en los ecosistemas empresariales.

EVENTOS

58

X Aniversario de la Asociación de Técnicos de Informática de la Administración Local - ATIAL

EVENTOS

68

UNE aprueba su Estrategia 2030 y refuerza su liderazgo internacional

NORMALIZACIÓN

76

#53 - JUNIO 2025

TYSC

#TYSC

Premios recibidos



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



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

itSMF
ESPAÑA

Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática



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

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

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

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



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



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



Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA



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

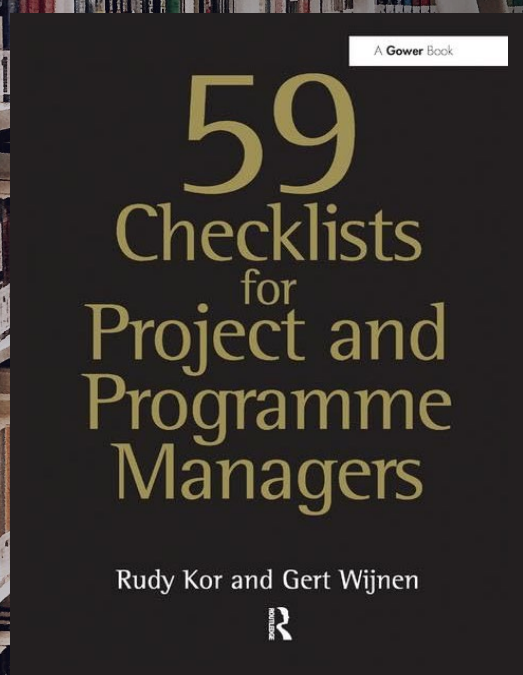


Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



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





59 Checklists for Project and Programme Managers

Rudy Kor y Gert Wijnen

“59 Checklists for Project and Programme Managers”, escrito por Rudy Kor y Gert Wijnen, es un manual dirigido a profesionales de la gestión de proyectos y programas que buscan una herramienta estructurada para asegurar la calidad y el control en cada fase del ciclo de vida de sus iniciativas. A diferencia de textos teóricos o extensos tratados, este libro se centra en la practicidad, ofreciendo 59 listas de verificación que cubren aspectos esenciales como la definición del alcance, la identificación de interesados, la planificación, el seguimiento, la gestión de riesgos y el cierre del programa o del proyecto.

La fortaleza del libro radica en su enfoque sistemático que facilita la aplicación de buenas prácticas alineadas con estándares internacionales. Cada checklist funciona como un recordatorio claro y conciso para evitar omisiones críticas que puedan comprometer el éxito del proyecto o programa. De este modo, el libro se convierte en un recurso indispensable para Programme y Project Managers que requieren una guía rápida, práctica y fiable para la toma de decisiones y el control operativo.

Además, “59 Checklists for Project and Programme Managers” destaca por su orientación hacia la mejora continua y la gestión del conocimiento, promoviendo la documentación de lecciones aprendidas y la evaluación constante de procesos. Esto lo hace especialmente valioso en entornos donde la complejidad y la presión por resultados exigen rigor y disciplina.

En definitiva, el libro “59 Checklists for Project and Programme Managers” de Kor y Wijnen aporta un enfoque profesional y pragmático a la gestión, facilitando a sus lectores la implementación de metodologías robustas sin perder de vista la flexibilidad necesaria para adaptarse a distintos contextos organizacionales. Es un texto que, más allá de ser un simple compendio de listas, se posiciona como un aliado estratégico para quienes lideran proyectos y programas en busca de eficiencia y excelencia.

Javier Peris



¿Es Posible Gobernar la Inteligencia Artificial sin Gobernar el Dato y/o sin Gobernar la Tecnología?

Vivimos tiempos fascinantes con el despegue de la Inteligencia Artificial, una ola tecnológica que está redefiniendo lo posible en múltiples sectores. Es natural que las organizaciones se esfuercen por subirse a esta ola, buscando desde la optimización de sus procesos hasta la creación de productos y servicios radicalmente nuevos, sin olvidar la tan ansiada ventaja competitiva. Pero en medio de esta carrera, a menudo frenética, emerge una reflexión que considero ineludible: ¿estamos prestando la debida atención a cómo vamos a gobernar esta potente herramienta? La norma ISO/IEC 38507 nos ofrece una brújula para navegar las aguas de la gobernanza específica de la IA.

Ahora bien, la IA no es un ente etéreo; se alimenta vorazmente de datos y se asienta sobre las infraestructuras tecnológicas que ya existen en nuestras empresas. Y es aquí donde me surge una pregunta que creo que muchos nos estamos haciendo: ¿Es realista pensar que podemos establecer una gobernanza de IA sólida, como la que nos orienta la ISO/IEC 38507, si no hemos puesto orden primero en casa? Me refiero a tener ya unos cimientos robustos para el Gobierno del Dato (siguiendo la línea de ISO/IEC 38505) y para el Gobierno general de la Información y la Tecnología (como marca la ISO/IEC 38500). Intentar lo contrario sería como empezar a decorar el ático de un edificio sin estar seguros de la solidez de sus cimientos y su estructura principal.

Para desenredar esta madeja, creo que es útil recordar brevemente qué nos aporta cada uno de estos estándares.

Pensemos en la **ISO/IEC 38500** como el gran marco, la piedra angular del Gobierno de TI en cualquier organización. Nos da los principios y ese modelo de “Evaluar, Dirigir y Monitorizar” que la dirección necesita para asegurarse de que la tecnología, hoy y mañana, se usa de forma efectiva, eficiente y aceptable. Toca palos tan importantes como que la TI esté realmente al servicio de la estrategia del negocio, que las inversiones tecnológicas generen valor tangible, que se mida el rendimiento, se cumplan normativas y, algo que a veces olvidamos, cómo influye el factor humano. En definitiva, la ISO 38500 es el esqueleto que articula todo el ecosistema tecnológico, y bajo su paraguas deben cobijarse todas las iniciativas, incluida, por supuesto, la IA. Es el cerebro que conecta la tecnología con los fines y los controles de la empresa.

Luego, reconociendo que los datos son mucho más que un subproducto –son un activo estratégico en toda regla–, apareció la **ISO/IEC 38505**, centrada en el Gobierno del Dato. No es que parta de cero, sino que inteligentemente aplica los principios de la ISO/IEC 38500 al universo específico de los datos. Nos habla de un “Mapa de Rendición de Cuentas del Dato”, que sigue su vida (desde que se recoge hasta que se elimina) y nos alerta sobre tres aspectos que necesitan sí o sí una gobernanza clara: el **Valor** del dato (su calidad, si es oportuno, su contexto), los

Riesgos que lleva asociados (seguridad, privacidad, mal uso) y las **Restricciones** a las que está sujeto (legales, éticas, normativas internas). La ISO/IEC 38505 nos dice: ojo, los datos tienen su propia personalidad y necesitan un gobierno dedicado, aunque siempre integrado en el gobierno general de TI.

Y así llegamos a la **ISO/IEC 38507**, que se mete de lleno con las implicaciones que tiene el uso de la Inteligencia Artificial en la gobernanza. No pretende ser un manual de instrucciones cerrado para gobernar la IA desde cero y de forma aislada. Más bien, es una guía para que quienes toman las decisiones entiendan cómo la IA sacude y reta los mecanismos de gobierno que ya deberíamos tener, sobre todo los que marca la ISO/IEC 38500. La ISO/IEC 38507 pone el foco en lo que hace diferente a la IA: su capacidad para automatizar decisiones, para resolver problemas analizando datos (especialmente el Machine Learning) y esa naturaleza camaleónica de algunos sistemas que aprenden y se adaptan. Nos invita a revisar y, si hace falta, reforzar nuestras políticas en temas como la supervisión directa, cómo se gobierna la toma de decisiones (para que siempre haya una persona responsable), cómo se manejan los datos que usa la IA (un punto crítico), la cultura de la empresa, el cumplimiento de leyes y la gestión de los riesgos propios de la IA.

Viendo el papel de cada una, la conexión entre ellas salta a la vista. Pretender implantar una gobernanza de IA con la sola ayuda de la ISO/IEC 38507, sin haber sentado antes unas bases firmes de Gobierno de TI con la ISO/IEC 38500, me parece un ejercicio condenado a tropezar. La IA, no lo olvidemos, corre sobre sistemas de TI. Se idea, se compra o desarrolla, se pone en marcha y se retira usando los mismos procesos y recursos que el resto de la TI. ¿Cómo vamos a alinear la IA con la estrategia si no tenemos un método claro para alinear toda nuestra tecnología con los objetivos del negocio (Principio 2 de ISO/IEC 38500)? ¿Cómo mediremos lo que la IA aporta si no tenemos forma de medir el retorno de las inversiones en TI en general (Principio 4)? ¿Y cómo gestionaremos los riesgos de seguridad de la IA si no hay un paraguas robusto para los riesgos tecnológicos de toda la organización (Principio 5)? La ISO/IEC 38500 nos da esa estructura vital –quién es responsable de qué, la dirección estratégica, cómo supervisamos y controlamos– sin la cual cualquier intento de gobernar algo tan complejo como la IA se quedaría cojo y, muy probablemente, no serviría de mucho.



CONTINÚA EN
PRÓXIMA PÁGINA



La cosa se pone aún más crítica si pensamos en el tándem Gobierno de IA (ISO/IEC 38507) y Gobierno del Dato (ISO/IEC 38505). La Inteligencia Artificial, y sobre todo ese motor llamado Machine Learning que vemos en tantas aplicaciones punteras, es una gran consumidora y, a la vez, productora de datos. Entrenamos modelos con cantidades ingentes de datos, operan analizando datos en tiempo real y, como resultado, generan aún más datos. La misma ISO/IEC 38507 dedica un buen espacio (sección 6.4) a la gobernanza del uso de datos para la IA, porque sabe de esta simbiosis. Nos dice que hay que estar muy atentos a la calidad, la idoneidad, los posibles sesgos y de dónde vienen los datos con los que alimentamos y operamos los sistemas de IA.

Y yo me pregunto, ¿cómo va una empresa a gestionar bien estas cuestiones de datos en la IA si no tiene ya un sistema de Gobierno del Dato como el que plantea la ISO/IEC 38505? Si no hay políticas claras y controles sobre cómo se recogen los datos, cómo se asegura su calidad y los permisos necesarios (lo que la ISO/IEC 38505 llama Restricciones); si no se clasifican los datos para saber cuán sensibles son y protegerlos como se debe (el aspecto de Riesgo); si no está claro quién responde por cada conjunto de datos y cómo se gestiona su ciclo de vida hasta su eliminación segura... ¿cómo vamos a poder gobernar con garantías los datos que son el combustible de la IA?

Intentar gobernar la IA sin un gobierno de datos robusto es como querer fabricar un producto de primera sin controlar la calidad de la materia prima ni el proceso de fabricación. El resultado es una lotería. Un sistema de IA que ha aprendido de datos malos, sesgados o que no entendemos bien (justo los problemas que un buen gobierno de datos intenta evitar) nos dará respuestas equivocadas, quizás discriminatorias o, simplemente, inútiles, por muy bueno que sea el algoritmo. Una mala gobernanza de los datos que entran y salen de la IA puede llevarnos a problemas de privacidad, a infringir la propiedad intelectual o a tomar decisiones automáticas basadas en información incorrecta, con el consiguiente riesgo legal, financiero y para nuestra reputación. La ISO/

IEC 38507 nos avisa de estos peligros, pero es la ISO/IEC 38505 la que nos da las herramientas para poner los controles básicos a nivel de datos, que son imprescindibles para mitigar esos peligros cuando entra en juego la IA.

Cuando la ISO/IEC 38507 nos habla de los retos propios de la IA –esa dificultad para entender por qué un modelo complejo toma una decisión (la famosa “caja negra”), cómo los sistemas pueden cambiar solos con el tiempo, o la necesidad de que un humano siga siendo el responsable final de las decisiones automatizadas– lo que hace, en mi opinión, es recalcar aún más que necesitamos reforzar, y no saltarnos, las buenas prácticas de gobierno de TI y de datos. Si un modelo de IA es opaco, más rigurosos tendremos que ser con los datos que le damos y con cómo medimos si funciona bien (conceptos de ISO/IEC 38505 y 38500). Si los sistemas se adaptan, necesitamos mecanismos para vigilarlos y validarlos continuamente, integrados en la supervisión general de TI (ISO/IEC 38500). Y si queremos que un humano rinda cuentas por decisiones automáticas, más importante es tener claras las responsabilidades y cómo se delegan en toda el área de TI y en la gestión de datos (principios de ISO/IEC 38500 y 38505).

Así que, para mí, el camino lógico está claro: una buena gobernanza en la empresa necesita un gobierno de TI fuerte (ISO/IEC 38500). Dentro de ese gobierno de TI, tratar los datos como el activo estratégico que son exige un Gobierno del Dato específico (ISO/IEC 38505). Y solo sobre estas dos capas bien asentadas podemos construir una adaptación inteligente de la gobernanza para los desafíos particulares de la Inteligencia Artificial (ISO/IEC 38507). Ir por libre con la gobernanza de la IA, sin esa base sólida de gobierno de TI y de datos, es hacer la vista gorda a dependencias que son críticas y exponerse a riesgos que pueden ser inmanejables.

Esto no quiere decir que haya que ser perfectos en gobierno de TI y de datos antes de dar el primer paso con la IA. La realidad de las empresas es mucho más compleja y mejorar la gobernanza es un camino que se hace al andar, paso a paso. Pero sí creo firmemente que cualquier proyecto serio de IA tiene que ir de la mano de una mirada honesta y un esfuerzo real por mejorar cómo gobernamos nuestra tecnología y nuestros datos. Pensar en la IA debería ser la chispa que nos impulse a fortalecer esos cimientos, no una excusa para olvidarnos de ellos.

En definitiva, a la pregunta de si puede haber Gobierno de IA sin Gobierno del Dato y/o sin Gobierno de TI, me inclino a pensar que la respuesta es un “no” bastante rotundo si lo que buscamos es gestionar bien los riesgos y obtener valor de forma sostenible. La ISO/IEC 38507 es una guía muy valiosa sobre los ajustes y puntos a tener en cuenta con la IA, pero da por hecho que ya existe un sistema de gobierno que funciona para la tecnología y los datos sobre los que opera la IA. Para quienes estamos en posiciones de liderazgo tecnológico y en los órganos de gobierno, esto no hace más que subrayar lo estratégico que es no dejarse llevar solo por el brillo de la IA, sino asegurarse de que la adoptamos sobre bases de gobernanza firmes y bien construidas. Invertir en madurar el gobierno de TI (ISO/IEC 38500) y de datos (ISO/IEC 38505) no es un trámite para cumplir el expediente; es una condición indispensable para navegar con responsabilidad y éxito en esta nueva era de la Inteligencia Artificial.



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 y Trainer, PRINCE2® MSP® MoP® MoV® MoR® P30® Practitioner & Trainer, Sourcing Governance®, VeriSMTM SIAMTM, OKR, Lean, Kanban, 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>

**Curso de
Certificación en:**

Gobierno del Dato

**UNE 0077
Data
Governance
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en la Norma: UNE 0077
- 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>



Vivir sin acceso al Oráculo de Delfos: medir para proteger

En el artículo del mes pasado de Tecnologías y Sentido Común tratamos el tema de cómo valorar si las iniciativas de seguridad de la información estaban correctamente orientadas y podían ser eficientes en la consecución del objetivo de proteger los activos de la organización. El siguiente problema es cómo medir la eficacia de las medidas implantadas a consecuencia del Plan de Tratamiento del Riesgo. Este mes, planteamos una aproximación a cómo hacerlo.

En el contexto actual, donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, como venimos poniendo de manifiesto en esta sección mensual de Tecnología y Sentido Común, es esencial que las organizaciones puedan conocer cuál está siendo la evolución de la eficacia de las medidas de seguridad de la información que implanten. No basta con pensar o decir que tal o cual medida nos protege de tal o cual amenaza, sino que hay que demostrarlo con datos.

Por ello, es necesario que se implementen **métricas e indicadores de ciberseguridad** que permitan a la organización evaluar (y mejorar) su postura de seguridad. Estas métricas permiten a las organizaciones medir la efectividad de sus controles de seguridad, identificar áreas de mejora y comunicar el estado de la seguridad a las partes interesadas, especialmente, a la Dirección General de la misma.



La importancia de establecer métricas e indicadores de ciberseguridad radica en la capacidad de una organización para anticipar, detectar y responder a incidentes de seguridad de manera eficaz. Según las Guías CCN-STIC del Centro Criptológico Nacional de España, la implementación de métricas de ciberseguridad es fundamental para mantener un nivel adecuado de protección y resiliencia frente a las amenazas cibernéticas. Estas guías proporcionan normas, instrucciones y recomendaciones que ayudan a las organizaciones a mejorar su grado de ciberseguridad mediante la adopción de buenas prácticas y la utilización de herramientas adecuadas, y aunque en principio se orientan a las Administraciones Públicas, pueden utilizarse por cualquier organización.

Las **métricas de ciberseguridad** son valores cuantificables que reflejan el rendimiento de los controles de seguridad de una organización. Por otro lado, los **indicadores de ciberseguridad** son medidas específicas que se utilizan para evaluar el estado de la seguridad en áreas concretas de interés para la organización. Para definir métricas e indicadores efectivos, es importante seguir estos pasos:

1. Identificación de Objetivos de Seguridad: Determinar los objetivos de seguridad de la organización, tales como la protección de datos sensibles o confidenciales, la prevención de intrusiones o la respuesta rápida a incidentes.

2. Selección de Métricas Relevantes: Elegir métricas que sean relevantes para los objetivos de seguridad establecidos. Estas métricas deben ser específicas, medibles, alcanzables, relevantes y temporales (SMART: *Specific, Measurable, Achievable, Relevant, y Time-bound*).

3. Establecimiento de Indicadores: Definir indicadores claros que permitan evaluar si las métricas seleccionadas muestran una situación adecuada o no de la organización respecto del objetivo a alcanzar. Los indicadores deben ser precisos y proporcionar información útil para la toma de decisiones.

4. Recopilación de Datos: Implementar procesos para recopilar los datos necesarios para calcular las métricas e indicadores. Esto puede incluir el uso de herramientas de monitorización, logs de eventos y tests o auditorías específicas de seguridad de la información.

5. Análisis y Reporte: Analizar los datos recopilados para evaluar el rendimiento de los controles de seguridad y generar informes que comuniquen los resultados a las partes interesadas.

Tal vez todo esto parezca etéreo o complejo, pero en otros ámbitos de la gestión y el gobierno de las organizaciones la definición de métricas e indicadores es una actividad consolidada y básica, y la ciberseguridad no debe ser una excepción. También es usual que las organizaciones presenten sus indicadores en forma de cuadro de mandos, una herramienta gráfica que muestra la información de forma visual y cómoda, y que suele permitir 'navegar' por los diferentes gráficos del mismo para indagar en la información que presenta.

Sin entrar en excesivo detalle, a continuación se presentan tres ejemplos de métricas de ciberseguridad, junto con sus indicadores asociados, el valor que aportan a la organización y el proceso para recopilar los datos necesarios.



CONTINÚA EN
PRÓXIMA PÁGINA





1. Tiempo Medio de Detección (MTTD)

- Indicador Asociado: Tiempo transcurrido desde la ocurrencia de un incidente de seguridad hasta su detección.

- Valor para la Organización: El MTTD es crucial para evaluar la capacidad de la organización para identificar rápidamente las amenazas. Un MTTD bajo indica una alta eficiencia en la detección de incidentes, lo que permite una respuesta más rápida y reduce el impacto potencial. Este indicador debe asociarse siempre a otro que defina el nivel de falsos positivos de la herramienta de detección, ya que un MTTD bajo asociado a una alta tasa de falsos positivos puede significar una excesiva carga de trabajo para el personal de ciberseguridad y una necesidad de ajuste en dicha herramienta de detección.

- Proceso de Recopilación de Datos: Lo habitual es utilizar herramientas de monitorización de seguridad que registren los eventos de seguridad, tal como un SIEM (*Security Information Event Management*) y sus tiempos de detección. Este tipo de herramientas analizan los registros de los equipos monitorizados a la búsqueda de patrones que indiquen la ocurrencia de los incidentes. Después, se puede calcular el tiempo medio de detección.

2. Tasa de Éxito de los Ataques de Phishing

- Indicador Asociado: Porcentaje de intentos de phishing que resultan en compromisos exitosos.

- Valor para la Organización: Esta métrica ayuda a evaluar la efectividad de las campañas de concienciación y formación en seguridad. Una tasa de éxito baja indica que el personal está bien preparado para identificar y evitar ataques de phishing.

- Proceso de Recopilación de Datos: Realizar pruebas de phishing simuladas y registrar los resultados, para poder analizar los datos y determinar el porcentaje de personal que cayó en los intentos de phishing.

3. Tiempo Medio de Resolución (MTTR)

- Indicador Asociado: Tiempo transcurrido desde la detección de un incidente de seguridad hasta su resolución completa.

- Valor para la Organización: El MTTR es fundamental para evaluar la capacidad de la organización para responder y mitigar incidentes de seguridad. Un MTTR bajo indica una alta eficiencia en la gestión de incidentes, lo que minimiza el impacto y la duración de los mismos.

- Proceso de Recopilación de Datos: Utilizar herramientas de gestión de incidentes que registren los tiempos de resolución y posteriormente, analizar los registros de incidentes para calcular el tiempo medio de resolución.

En conclusión, definir y establecer métricas e indicadores de ciberseguridad es esencial para cualquier organización que desee mejorar su postura de seguridad y proteger sus activos digitales. Al seguir un enfoque estructurado tanto para analizar y mitigar los riesgos, como para la selección de métricas, la definición de indicadores y la recopilación de datos, las organizaciones pueden obtener una visión clara de su rendimiento en ciberseguridad y tomar decisiones informadas para fortalecer sus defensas.

En su organización, ¿siguen este proceso o están suscritos al Oráculo de Delfos?



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/mdserratt>

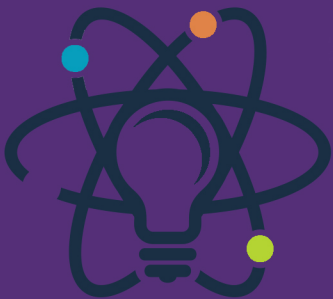
PfM Book

Portfolio

Management

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

[illegible]

Acuerdo sobre algoritmos criptográficos post-cuánticos

El Reglamento sobre la Ciberseguridad ha establecido un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC y los servicios de seguridad gestionados en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión, que se aplicará sin perjuicio de las disposiciones específicas contenidas en otros actos jurídicos de la Unión relativas a la certificación de carácter voluntario u obligatorio.

Los productos, servicios y procesos de TIC y los servicios de seguridad gestionados que hayan sido certificados en virtud de un esquema europeo de certificación de la ciberseguridad adoptado con arreglo al artículo 49 del Reglamento se considerarán conformes con los requisitos de dicho esquema.

La certificación de la ciberseguridad es voluntaria, salvo que se disponga otra cosa en el Derecho de la Unión o de los Estados miembros, lo que ocurre, por ejemplo, en el caso de algunos productos empleados en la prestación de servicios de confianza, como en el caso de los dispositivos cualificados de creación de firma cualificada o de sello electrónico cualificado, conforme a lo establecido en los artículos 30 y 39.2 del Reglamento eIDAS y la Decisión de Ejecución (UE) 2016/650, que se refiere a Common Criteria.

El Reglamento de Ejecución (UE) 2024/482 ha establecido el esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (en adelante, EUCC), aplicable a todos los productos de tecnologías de la información y la comunicación, incluida su documentación, que se presenten para su certificación en virtud del EUCC, y a todos los perfiles de protección que se presenten para su certificación en el marco del proceso de TIC conducente a la certificación de productos de TIC.



CONTINÚA EN
PRÓXIMA PÁGINA



El Reglamento sobre la Ciberseguridad también establece el Grupo Europeo de Certificación de la Ciberseguridad (en adelante, GECC), entre cuyas tareas se encuentra la de adoptar dictámenes dirigidos a la Comisión relativos al mantenimiento y revisión de los esquemas europeos de certificación de la ciberseguridad existentes.

Por su parte, el EUCC prevé que la Comisión podrá solicitar al GECC que adopte un dictamen con vistas al mantenimiento del EUCC y que lleve a cabo los trabajos preparatorios necesarios, y autoriza al GECC a adoptar un dictamen para aprobar documentos del estado de la técnica, que serán publicados por ENISA, lo que es muy relevante, dado que los productos TIC se deberán evaluar empleando los documentos del estado de la técnica contenidos en el Anexo I que resulten aplicables.

Hasta el momento, se han venido empleando los mecanismos criptográficos acordados y especificados del SOG-IS, que tiene como misión coordinar la normalización de los perfiles de protección de los Criterios Comunes y las políticas de certificación entre los organismos de certificación europeos con el fin de tener una posición común en el grupo internacional CCRA, en rápido crecimiento, y coordinar el desarrollo de perfiles de protección cada vez que la Comisión Europea lance una directiva que deba aplicarse en las legislaciones nacionales en materia de

seguridad informática, como ha sucedido en el caso del Reglamento eIDAS.

El 15 de mayo de 2024 ENISA remitió al GECC una propuesta de directrices relativas a los mecanismos criptográficos acordados, referida a los SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, en su versión v1.3, que fue discutida por el subgrupo de criptografía del GECC el 6 de junio de 2024 y aprobada por el GECC el 16 de julio de 2024, con vistas a seguir trabajando en un posible documento sobre el estado de la técnica de los mecanismos criptográficos. Posteriormente, el 5 de mayo de 2025, el subgrupo de criptografía del GECC ha aprobado la actualización del documento Agreed Cryptographic Mechanisms a la versión 2.0.

Como gran novedad, el ACM 2 incorpora consideraciones y recomendaciones relativas a la computación cuántica. Como se explica en el documento, el enfoque recomendado es dar prioridad a la mitigación de la amenaza cuántica en aplicaciones en las que la confidencialidad debe protegerse a largo plazo, mediante el despliegue de criptografía segura post-cuántica en modo híbrido junto con la criptografía asimétrica segura clásica existente y/o la codificación simétrica. Estos modos híbridos garantizarán que todos los mecanismos criptográficos pre o post-cuánticos combinados deban romperse simultáneamente para que se rompa el modo híbrido.

Este enfoque ofrece garantías contra la amenaza cuántica, así como garantías contra los problemas de seguridad que podrían afectar a los mecanismos post-cuánticos estandarizados más recientes. Además del despliegue de soluciones híbridas para los mecanismos asimétricos, también se recomienda, como acción mitigadora complementaria, adaptar las longitudes de los parámetros de los mecanismos simétricos, por ejemplo, las longitudes de clave y resumen criptográfico.

Asimismo, el documento presenta varios mecanismos post-cuánticos acordados, como ML-DSA, basado en la primitiva LWE. ¿Empiezan los Juegos del Hambre?



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.

Curso de Certificación en: Gobierno de Blockchain & DLT

ISO 23635 Blockchain & DLT Governance Leader

Docente:
Nacho Alamillo

Coordinación Académica
Javier Peris

- Formato: Directo en Remoto
- Duración: 20 horas
- Sesiones: Martes y Jueves
- Martes: De 16:00 a 21:00 horas
- Jueves: De 16:00 a 21:00 horas
- Examen de Certificación: Incluido
- Aforo: Limitado 15 Alumnos
- Acceso: Solicitud de admisión

MidMgmt®

MPPM®

MGEIT®

eGob®

Próxima Convocatoria en Directo
JUNIO 2025

Solicita tu admisión en:



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

**Plazas
limitadas**



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

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

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

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

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

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

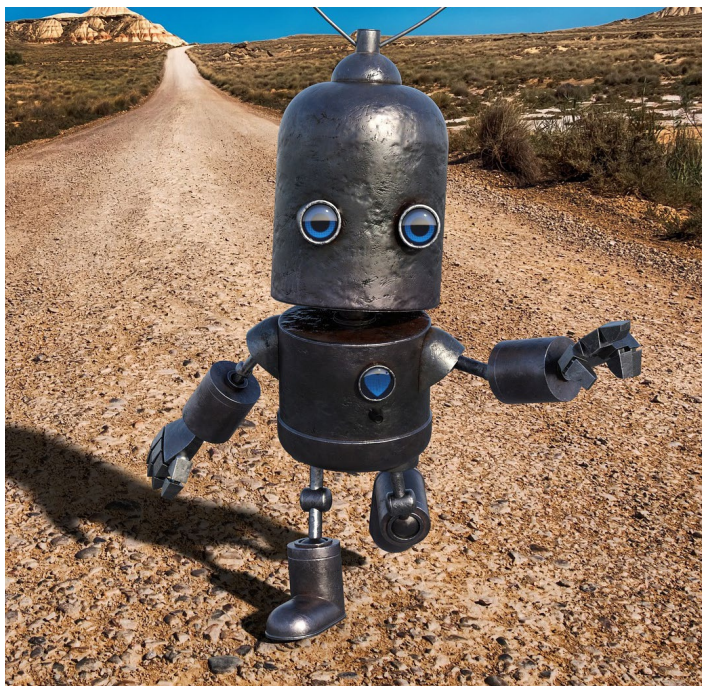


CONTINÚA EN
PRÓXIMA PÁGINA



“

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



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

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

La organización, las personas, los procesos, los datos de entrenamiento o la configuración del propio sistema de IA, entre otros, pueden ser orígenes de estos riesgos.

La realidad es que hay estudios que indican que más del 50% de interacciones de los usuarios con chatbots basados en IA incluyen información personal sensible, y que más del 11% de empleados en las organizaciones comparte información confidencial de su empleador con estos chatbots.

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

Además, están los ataques tradicionales que se ven potenciados por la IA, como los ataques de denegación de servicio, los ataques de phishing o los deep fakes. Ya hemos

visto que la IA tiene una facilidad enorme para imitar nuestra voz y nuestra cara, incluso nuestra forma de escribir.

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

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

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

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

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

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



JUAN CARLOS MURIA TARAZON

Licenciado en Informática y Doctor Cum Laude en Organización de Empresas por la Universidad Politécnica de Valencia (UPV). Con acreditación en Gestión de Datos para Investigación Clínica, es miembro de la Junta Directiva de la Asociación Valenciana de Informáticos de Sanidad, auditor CISA, CGEIT y está certificado en ITIL, COBIT 5 y PRINCE 2. Con más de 20 años de experiencia en el sector de la salud, ha dirigido proyectos de interoperabilidad, seguridad y big data, y ha sido profesor de marketing digital, big data e inteligencia de negocio. Actualmente es profesor de Organización de Empresas en la UPV y consultor independiente.

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

Twitter:
<https://twitter.com/juancarlosmt>

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>



Andoni Serrano

¿Quién es Andoni Serrano?

Soy arquitecto de sistemas informáticos especializado en entornos críticos, con más de 30 años de experiencia liderando la implantación, asesoramiento y soporte de infraestructuras tecnológicas de alta disponibilidad para empresas del IBEX 35, organismos gubernamentales y consorcios internacionales. A lo largo de mi trayectoria, he contribuido a garantizar la continuidad operativa en sectores estratégicos donde la fiabilidad tecnológica es clave. Pero esa es solo una parte de mi historia. La otra mitad de mi vida profesional y personal está profundamente ligada a un compromiso social: acompañar a niños con cáncer a través de una tecnología muy especial. Como fundador de la Fundación The Pink Force estoy dirigiendo una red internacional que emplea nuestros 35 droides R2-KT como "herramienta" de acompañamiento hospitalario en 17 países. Lidero la promoción de un proyecto STEAM muy especial con impacto social real que hemos denominado Pink Force Factory, que busca transformar las aulas en talleres donde se unen ciencia y esperanza.



CONTINÚA EN
PRÓXIMA PÁGINA

Nuestro invitado a #TYSC

Háblanos de tus éxitos o logros profesionales

En el plano técnico, he tenido la fortuna de liderar el diseño de sistemas de infraestructura crítica para autopistas, empresas energéticas y consorcios de transporte público, donde la continuidad operativa es esencial. Esta experiencia me ha permitido participar en proyectos estratégicos a nivel multinacional, siempre buscando soluciones que integren estabilidad, innovación y resiliencia. Sin embargo, quizás lo más valioso ha sido aplicar todo ese conocimiento técnico en beneficio de un propósito social. La Fundación The Pink Force ha sido reconocida por su modelo de innovación humanista y actualmente está firmando convenios de colaboración con instituciones educativas de gran prestigio, como la Universidad de Navarra y la U-tad.

Estas alianzas están permitiendo mejorar significativamente la capacidad de interacción hospitalaria de nuestros robots, al incorporar nuestros proyectos a programas de robótica e ingeniería. Hemos conseguido algo poco habitual: tender puentes entre mundos que tradicionalmente no se cruzaban, como el de la ingeniería de sistemas y el de la atención pediátrica emocional.

¿Qué es la Fundación ThePinkForce?

Es una organización internacional sin ánimo de lucro dedicada a mejorar la vida de los niños con cáncer a través de la robótica emocional y educativa. Utilizamos el droide R2-KT, nacido en 2005 para acompañar a Katie Johnson, como símbolo de esperanza, valentía y ternura. La fundación coordina la construcción, adaptación y despliegue de unidades funcionales de este droide, integrándolas en programas hospitalarios y escolares. The Pink Force es también una plataforma de colaboración. Trabajamos con makers, ingenieros, pedagogos, psicólogos, creativos y voluntarios en todo el mundo. Nuestra misión es crear momentos mágicos en entornos de alta vulnerabilidad emocional. Hacer que los niños y niñas enfermos sientan que alguien piensa en ellos de una forma muy especial.



CONTINÚA EN
PRÓXIMA PÁGINA





SPANOGI

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Nuestro invitado a #TYSC

¿Cómo fueron vuestros comienzos?

Empezamos con mucha ilusión, pero sin recursos. Lo que teníamos eran ganas, muchos conocimientos técnicos, creatividad y una conexión personal con la historia original de R2-KT. Construir nuestra primera unidad funcional fue un desafío lleno de desafíos técnicos y aprendizajes constantes. Recuerdo perfectamente nuestra primera visita al hospital universitario de San Sebastián de la mano de Aspanogi donde se generó tal emoción entre los pequeños pacientes, que una madre nos dijo: "Es la primera vez que mi hijo sonríe desde que fue diagnosticado". Ese fue el punto de no retorno. Otra anécdota imborrable sucedió en el hospital Virgen del Camino de Pamplona donde no puedo olvidar las lágrimas de un niño al recibir una foto suya entregada por nuestra droide.

¿Cuál es la respuesta de los niños a vuestra iniciativa?

Desbordante. Los niños no ven a R2-KT como una máquina, sino como algo mágico. La abrazan, le hablan, pronuncian su nombre. Lo integran en su mundo emocional como un elemento positivo, y eso tiene un efecto terapéutico real. En algunos hospitales nos han reportado que la presencia del droide reduce la ansiedad previa a tratamientos invasivos o ayuda a mejorar la comunicación con pacientes más introvertidos. Un caso que siempre recordamos con cariño es el de Oier, un niño que desde el primer momento adoptó a R2-KT como una amiguita más y esperaba cada nueva visita con gran ilusión. Hoy Oier es una de nuestras historias de éxito habiendo dejado atrás la enfermedad.

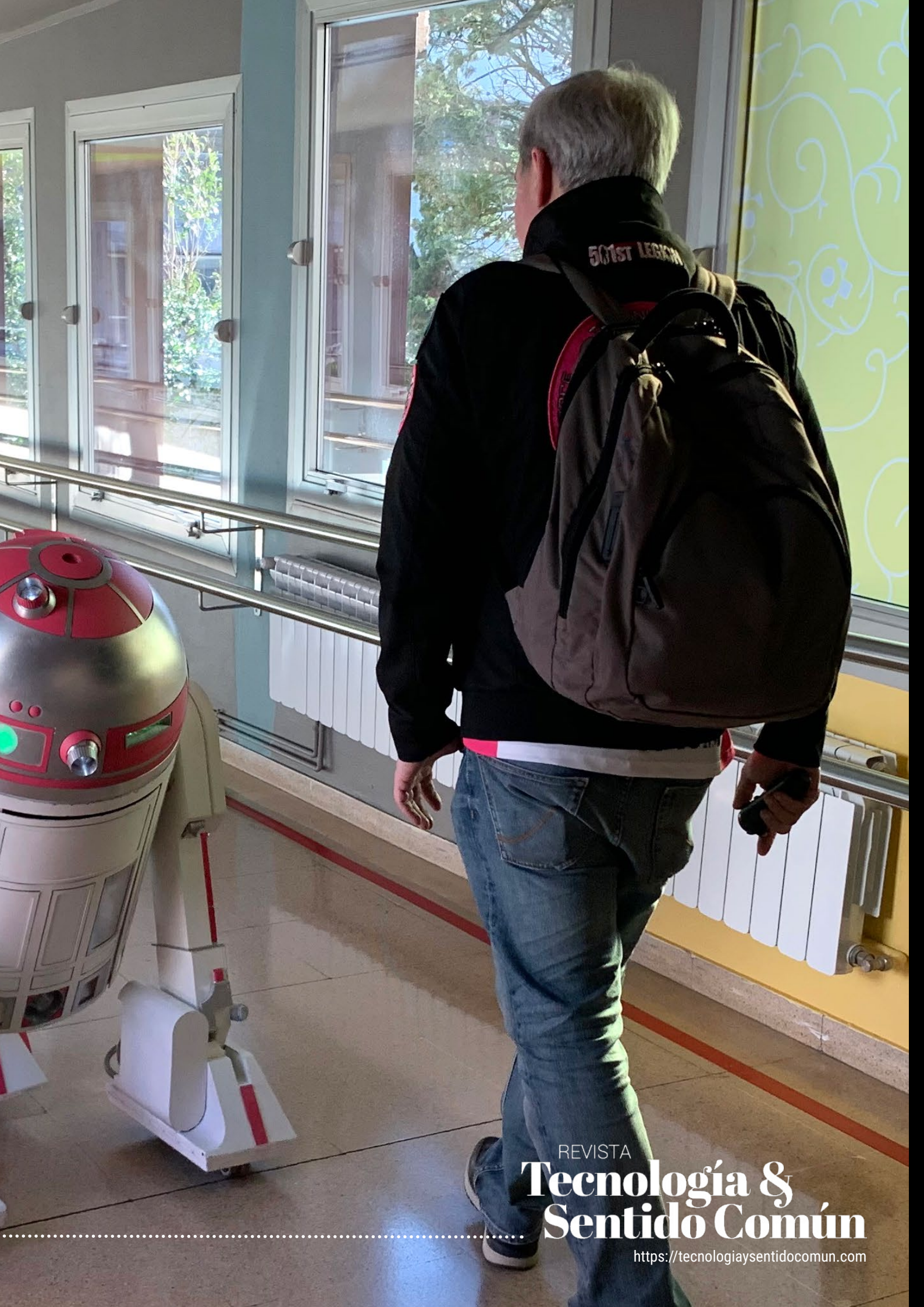
¿Y la de la sociedad en su conjunto médicos, instituciones?

Ha sido muy positiva. En el ámbito hospitalario hemos sido acogidos con respeto y admiración. Los profesionales sanitarios ven en R2-KT una herramienta complementaria de humanización. Además, contamos con el apoyo de fundaciones oncológicas de referencia, que valoran nuestra capacidad para conectar con las emociones de los pacientes sin invadir su espacio clínico. La combinación de rigor técnico y sensibilidad emocional es nuestra seña de identidad.



CONTINÚA EN
PRÓXIMA PÁGINA





REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Nuestro invitado a #TYSC

¿Lideráis alguna iniciativa adicional?

Sí, nuestra actividad principal es el acompañamiento hospitalario emocional, pero la imagen del droide tiene tal fuerza simbólica que sentimos una gran responsabilidad de aprovecharla también en iniciativas orientadas a la prevención del cáncer infantil. Por ello, estamos estableciendo alianzas con asociaciones de referencia en el ámbito culinario, con el objetivo de que puedan diseñar platos saludables inspirados en la figura de R2-KT. Asimismo, colaboramos con organizaciones que promueven hábitos de vida activos entre los más pequeños, como la carrera infantil Behobia Txiki, para que la imagen de nuestra simpática droide motive a la infancia a participar en actividades deportivas y saludables. Y para cerrar el círculo, estamos en conversaciones con el CNIO, con la posibilidad de que R2-KT participe este año en la Noche Europea de los Investigadores e Investigadoras, reforzando así el vínculo entre ciencia, salud y compromiso social.

¿Cuáles son vuestros planes de futuro que se puedan conocer?

Queremos, en primer lugar, consolidar durante este año 2025 la implantación de las Pink Force Factory en España. De cara al próximo año, nuestro objetivo es crear una red internacional de "Pink Force Factory Labs", pequeños espacios de innovación gestionados por la fundación, que al igual que en España, colaboren con los colegios de sus respectivos países para construir nuestras pequeñas droides y entregarlas a niños con cáncer ingresados en hospitales locales. Paralelamente, estamos desarrollando una versión de R2-KT en realidad aumentada, para que los droides puedan seguir acompañando a los niños incluso después de nuestras visitas presenciales a los centros hospitalarios. Y, por supuesto, queremos continuar ampliando la presencia de The Pink Force en Asia. Además, estamos trabajando en la publicación de una guía metodológica que permita a cualquier hospital o institución educativa replicar nuestro modelo. Nuestro deseo es que el impacto no dependa exclusivamente de nosotros, sino que florezca allí donde exista vocación y compromiso.



CONTINÚA EN
PRÓXIMA PÁGINA



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

¿Habéis viajado recientemente a Japón, ¿Cómo ha sido la acogida de la iniciativa?

La acogida fue increíblemente respetuosa y entusiasta. En Tokio tuvimos el honor de entregar la primera unidad Mini-R2-KT en Asia a la CCAJ (Childhood Cancer Association of Japan), una de las asociaciones contra el cáncer infantil más respetadas y longevas del continente. Fue un momento histórico y profundamente emotivo, ya que se trataba de una unidad construida por niños españoles durante un taller STEAM promovido por el Ayuntamiento de Bilbao, con ideas aportadas por niños con cáncer pertenecientes a la asociación La Cuadri del Hospi, que lleva más de diez años apoyando a familias oncológicas. La conexión fue inmediata. La CCAJ mostró un gran interés por cada detalle de nuestro proyecto, valorando tanto el aspecto tecnológico como el emocional. Podemos regresar a España con la alegría de anunciar que, antes de que finalice el año, Asia contará con su primera unidad R2-KT de tamaño real. Además, un pequeño documental sobre la historia de R2-KT fue transmitido a nivel nacional en la televisión japonesa, dentro del programa Warakora, lo que refuerza aún más el impacto y la proyección de nuestra iniciativa.

¿Hay mucho cambio cultural con la sociedad de Japón?

Sí, pero también muchas coincidencias. Los japoneses valoran profundamente el respeto, la empática silenciosa y la belleza funcional. R2-KT conecta muy bien con ese imaginario de ternura contenida. Allí, la tecnología no se ve como frialdad, sino como puente entre almas. Creo que ese paralelismo con nuestros objetivos hizo que la acogida fuera tan especial. Además, en Japón hay una larga tradición de robótica aplicada al bienestar. Eso hizo que nuestro enfoque emocional y simbólico fuera muy bien comprendido. Sentimos que habíamos encontrado un segundo hogar.

¿Qué necesidades no cubiertas tiene la fundación y cómo podrían cubrirse?

Necesitamos apoyo estructural: financiación estable, capacidad de contratar a tiempo completo, medios para escalar nuestra logística y llegar a más hospitales. Hasta ahora hemos hecho milagros con muy poco, pero si queremos llevar una unidad mini-R2-KT a cada niño que lo necesite, necesitamos el compromiso de empresas, administraciones y ciudadanos. Buscamos patrocinadores con visión social, alianzas con fabricantes de componentes, acceso a espacios para talleres, y sobre todo, una red de voluntarios cualificados que compartan nuestros valores. Cada gota de ayuda cuenta, y el retorno

¿Te apetece pedir un deseo, cuál?

Que podamos atender todas las peticiones que recibimos de colegios y asociaciones de padres de niños con cáncer. No hay centro educativo o entidad a la que hayamos presentado el proyecto y que no haya mostrado entusiasmo y deseo de participar. Eso representa una gran responsabilidad, porque estamos convencidos de que la sociedad necesita iniciativas como esta, especialmente en un momento en el que los estímulos superficiales nos invaden por todas partes. Que el futuro no sea solo inteligente, sino también profundamente compasivo.

Conclusiones.

La historia de The Pink Force demuestra que un droide nacido de una tragedia puede convertirse en un embajador de vida. Y que, al final, la tecnología cobra un significado muy especial cuando se pone al servicio de lo más humano: el cuidado, la compasión y la infancia. Hoy sabemos que no estamos solos. Que somos muchos los que creemos en una tecnología que cura, que acompaña y que emociona. Que el color rosa no es solo un símbolo de lucha contra el cáncer, sino también de ternura con propósito. Seguiremos adelante, con cada nueva sonrisa como combustible. **Porque mientras haya un niño que necesite compañía, la Fuerza Rosa estará allí.**



**Curso de
Certificación en:**

Gobierno Corporativo

**ISO 37000
Corporate
Governance
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 37000
- 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>

Marlon Molina

Las tabletas son tendencia y muestran cómo será 2030

Vemos cientos de tecnologías luchando entre ellas por hacerse un hueco en el mercado, y mientras tanto, hay un hardware que se posiciona en la empresa y en el consumo particular: las tabletas.

Al cierre de 2024 la venta de tabletas había crecido un 20,4% interanual según lo había comunicado IDC, en el último cuatrimestre del año pasado se vendieron 39,6 millones de tabletas, una cantidad impresionante. El crecimiento siguió en 2024, el primer cuatrimestre siguió creciendo, esta vez un 8,5% interanual lo que ha representado 36,8 millones de estos dispositivos.

Apple es el fabricante que más tabletas vende, lleva años manteniendo su liderazgo con una impresionante cuota de mercado del 37,3%. Para Apple, el iPad representa un 6,83% de sus ingresos, aunque muy por debajo del iPhone que tiene el 51,45% de los ingresos, pero visto desde otra perspectiva, la empresa que sigue siendo la mejor valorada en todo el mundo, dependen de dos dispositivos muy similares que juntos suman el 58,28% de sus ingresos. Detrás de Apple están las marcas chinas como Huawei y HONOR, seguidas por la coreana Samsung. Sin embargo, la tendencia más importante está en las marcas nacionales, pequeños fabricantes que personalizan un dispositivo y lo nacionalizan para hacerse con un porcentaje del mercado, que según IDC, es un muy buen porcentaje.

¿Qué trae este repunte de la venta de tabletas y por qué es importante?

Es importante mantener en el radar todas las tendencias del mercado, al fin y al cabo, como tendencia no pueden estar todas las tecnologías, normalmente se pueden contar con los dedos de la mano. Las tendencias nos dan señales de lo que interesa a la mayoría de los consumidores, ya sean consumidores corporativos o particulares.

La consultora Canalys apunta a que la principal razón de este crecimiento en los últimos ocho meses se debe a renovaciones de los dispositivos comprados en la época de la pandemia sanitaria, e IDC complementa la información explicando que durante la pandemia las aulas y los estudiantes remotos se hicieron con un número importante de tabletas, las que hoy renuevan. En segundo lugar, estos dispositivos se compran para ocio, ya sea video juegos o para la lectura.

El Ministerio de Educación Español anunció en mayo de 2025 que el 92,3% de centros públicos de Secundaria y FP contaban en ese momento con un entorno virtual de aprendizaje, un cambio radical en la educación.



CONTINÚA EN
PRÓXIMA PÁGINA





Consecuencia o no de la pandemia, o bien acelerado por las circunstancias que vivió el planeta entre los años 2019 y 2021, el mundo se acostumbró al aprendizaje en línea, y en el año 2025 renueva la forma de estudio favorita: la tableta.

Un cambio en la infraestructura educativa

Como es bien sabido, una tableta a diferencia de un PC o un portátil no tiene suficiente almacenamiento para videos o archivos en general. De hecho, una situación poco conocida es que los teléfonos móviles suelen tener más espacio de almacenamiento que las tabletas. Con esta información, es posible entender que la educación ocurre completamente en línea.

Las telecomunicaciones parecen servicios invisibles, al igual que la electricidad que solo la valoramos cuando hay un apagón, las telecomunicaciones están creando un nivel muy alto de dependencia en los modelos de negocio, y en este caso, en los modelos de estudio y ocio.

Los centros educativos que hace unas décadas se publicitaban en sus ciudades, hoy lo hacen en un mundo global. Estados Unidos vende en España, pero España también vende en Estados Unidos. Para el estudiante de un máster o una especialización en 2025 no le resulta extraño valorar opciones entre centros de diferentes países, e incluso distintos continentes. Una escuela de negocios de Australia compite de tú a tú con una escuela de negocios en Francia, donde el idioma ya no es un problema gracias a una combinación fascinante de tecnologías como la IA generativa.

El estudiante tampoco tiene miedo de enfrentarse a un modelo internacional, porque es el entorno que ya conoce, y porque no se diferencia del que ofrece su propio país.

La lección para la próxima década

Si los estudiantes del mundo son globales, estudian conectados, y se basan en herramientas automatizadas para comunicarse, podemos asumir que los servicios en general serán cada vez más globales.

Hay algunas evidencias en el mercado, servicios como Uber, mercados como Amazon, o plataformas de entretenimiento como Netflix no solo son globales, sino que además los consumidores las reconocen de forma normal y asumen su existencia. En las conversaciones internacionales no es necesario pararse a explicar qué es Netflix, o usar una frase como "lo compras en Amazon", o "he reservado un AirBnB".

El crecimiento en la venta de las tabletas es una señal clara de hacia dónde se dirige el mundo. En estos dispositivos convergen movilidad, conectividad y accesibilidad, características que definen tanto la educación como el trabajo y el ocio del futuro. Quizá los reglamentos que está creando la Unión Europea alrededor de la economía circular marquen un camino diferente para los fabricantes, pero desde luego, el consumo tiene una visión clara, y por lo tanto es una oportunidad para adelantarse y posicionarse en el futuro próximo.



MARLON MOLINA

Marlon Molina es ingeniero en informática, es certification officer en Computerworld University desde donde lidera la certificación Business IT, también dirige el laboratorio de ciberseguridad para los Parlamentos de las Américas en la OEA, es profesor en varias Escuelas de Negocio, y es asesor de varios Consejos de empresa en España e Internacionales. En 2019 Cherwell le incluyó en el TOP 5 de los líderes técnicos de la transformación digital en EMEA.

LinkedIn:

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

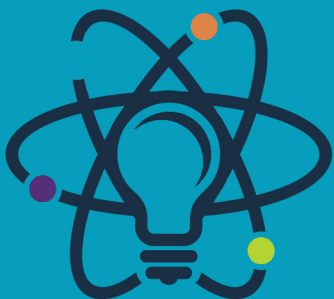
PjM Book

Project

Management

Body of Knowledge

P4MGO!®



P4MGO!

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



Ricard Martínez Martínez



¿Y ahora vamos a simplificar o a desregular?

En la Unión Europea soplan vientos de desregulación. Medios de comunicación especializados en la UE, como Politico, citando fuentes de la UE señalan desde abril que la Comisión Europea se está preparando para proponer cambios significativos al Reglamento General de Protección de Datos (RGPD) en un futuro próximo. La Comisión tendría previsto presentar una propuesta para «recortar» el RGPD, con el objetivo de reducir la carga normativa que pesa sobre las empresas y mejorar la competitividad frente a rivales globales como Estados Unidos y China. Esta iniciativa forma parte de una estrategia más amplia de la UE para simplificar las normas y reducir los costes de cumplimiento para las empresas, que ya incluye medidas en ámbitos como la información sobre sostenibilidad y el acceso a la inversión. Las medidas de simplificación normativa pretenden ser proporcionadas y mantener objetivos fundamentales como la estabilidad financiera y la protección de los inversores, al tiempo que se reduce la complejidad y el coste del cumplimiento. Todo ello sin dismantlar los principios fundamentales de la protección de datos. De alguna manera, puede deducirse que se trata de una primera respuesta al Informe Draghi (The future of European competitiveness-Part A. A competitiveness strategy for Europe) que afirmaba que la falta de competitividad de la industria digital europea puede tener su origen en la existencia de un marco de hiperregulación.

Michael McGrath, Comisario de la UE para Democracia, Justicia, Estado de Derecho y Protección del Consumidor, señaló en una actividad del Center for Strategic & International Studies (The Future of Transatlantic Digital Collaboration) que se está preparando un paquete Omnibus que incluirá reformas al RGPD, especialmente para reducir la carga administrativa sobre pymes y organizaciones con menos de 500 empleados, particularmente en lo relativo al registro de actividades de tratamiento. En este sentido, se rebajaría el nivel de detalle exigido para determinadas actividades de tratamiento consideradas de menor riesgo. Se plantearían procedimientos de evaluación de riesgos simplificados que proporcionan orientaciones más claras y metodologías menos complejas para que las pymes evalúen sus actividades de tratamiento de datos. Asimismo, se trabajaría en plantillas y herramientas estandarizadas que facilitan el cumplimiento sin necesidad de conocimientos jurídicos o técnicos especializados.

Llegados a este punto conviene reflexionar en voz alta respecto de las circunstancias que de alguna manera pueden habernos conducido a este estado de cosas. En primer lugar, no hay que descartar que una parte de este efecto Bruselas resida en una cierta soberbia del legislador europeo convencido de estar creando las mejores piezas legislativas de la historia de la humanidad y en una suerte de concepción genesíaca de la ley. Históricamente el desarrollo de la legislación digital se ha basado en estudios de una altísima calidad académica, pero de una extraordinaria lejanía respecto de la realidad material que se planteaba regular. Y así, cuando se utiliza la ley para fijar estándares y condiciones de cumplimiento normativo lejanos o imposibles de alcanzar confiar en el valor performativo de las normas es algo más bien ilusorio. Las leyes no crean la realidad. Esta nace de una definición estratégica de políticas públicas que requieren de un diseño adecuado, de plazos razonables para su ejecución y de un marco inversión coherente con los objetivos que se persiguen.



CONTINÚA EN
PRÓXIMA PÁGINA



Por otra parte, se ha producido un efecto perverso a la hora de interpretar tanto la Directiva de Protección de Datos de 1995 cómo su sucesor el RGPD. La base legal que alimentaba la primera y se mantuvo en el segundo no era otra que la construcción del Mercado Interior. El funcionamiento de este Mercado requiere ineludiblemente garantizar un adecuado flujo de datos entre los distintos Estados miembros incluidos los datos de carácter personal. Por otra parte, la consecución de los objetivos económicos de los Tratados de la Unión Europea implica el fomento de condiciones adecuadas de tratamiento de los datos personales al servicio de la investigación, la innovación, y el emprendimiento y en última instancia al servicio del bien común. Obviamente, ese tratamiento de información personal debía modularse a través de un conjunto de principios, valores y procesos cuyo objetivo esencial no era otro que garantizar nuestros derechos fundamentales.

Sin embargo, en la realidad práctica la garantía del derecho fundamental se impuso frente a cualquier otra consideración transmutando lo que debería haber consistido en un delicado esfuerzo de equilibrio para crear un ecosistema favorable al tratamiento de datos en un esquema de prevalencia absoluta del derecho fundamental. Y basta con ver los posicionamientos de las autoridades de protección de datos durante COVID en relación con la trazabilidad de contactos basada en geolocalización para entender hasta qué punto el enfoque europeo resultó catastrófico.

No ha sido ajena a ello la extraña posición constitucional que han alcanzado estas autoridades. En la práctica, existen dos regulaciones en esta materia: el RGPD y las directrices e informes de las autoridades. Curiosamente, los aspectos fundamentales para orientar el cumplimiento normativo en esta materia se fijan en documentos que no permiten el control jurisdiccional hasta que se dicte una resolución sancionadora. Incluso en este caso acaban consolidando cuándo los distintos operadores no están dispuestos asumir los costes procesales y los riesgos asociados a la interposición de un recurso.

De otro lado, ha crecido un mercado de asesoramiento especializado que sin duda es de una enorme calidad, pero no es ajeno a dos riesgos sistémicos. El primero de ellos consiste en situar a la persona delegada de Protección de Datos en una posición de preeminencia que en la práctica determina las decisiones de las organizaciones en aspectos cruciales para sus modelos de negocio operando como un freno a la innovación y pervirtiendo el Estatuto de independencia que les otorga la ley y el deber de contribuir a desplegar metodologías de protección de datos desde el diseño y por defecto. El segundo y no menos grave ha consistido en promover modelos de cumplimiento normativo basados en plantillas de copiar pegar. Estos han favorecido la corrupción en el empleo de poco fondos públicos de formación y trasladado a las pymes la idea de que la protección de datos es una especie de peaje que hay que pagar, aunque no sepamos para qué sirve.

En la práctica, puede afirmarse que no ha existido una política pública orientada a la integración armónica de la regulación en los procesos de las organizaciones públicas y privadas capaz de favorecer condiciones efectivas de cumplimiento que promovieran la competitividad de la industria digital europea. Este estado de cosas ha favorecido la acumulación de grandes volúmenes de datos por parte de aquellas grandes empresas foráneas a las que se quería disciplinar, cuyo músculo financiero les ha permitido desplegar modelos de compliance formalmente adecuados y soportar los procesos de *enforcement* y las batallas jurídicas que comportan.

Es evidente por qué la Unión Europea se ha visto obligada a apostar por la desregulación. Con independencia del punto de llegada de esta nueva política, lo cierto es que la experiencia demuestra que la única manera de reconducir este estado de cosas pasa por definir marcos legales accesibles y rediseñar en la medida de lo posible las tareas de autoridades que sin duda manifestarán en este proceso una significativa resistencia al cambio.



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 Universidades 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>

Curso de Certificación en:

Estrategias de Cumplimiento para Inteligencia Artificial

IA Compliance Strategist

Docente:
Ricard Martínez

Coordinación Académica
Javier Peris

- Formato: Directo en Remoto
- Duración: 20 horas
- Sesiones: Martes y Jueves
- Martes: De 16:00 a 21:00 horas
- Jueves: De 16:00 a 21:00 horas
- Examen de Certificación: Incluido
- Aforo: Limitado 15 Alumnos
- Acceso: Solicitud de admisión

MidMgmt®

MPPM®

MGEIT®

eGob®

Próxima Convocatoria en Directo
JULIO 2025

Solicita tu admisión en:



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

**Plazas
limitadas**



Marcos Navarro



El Ecosistema Energético de 2034

Un sector Impulsado por la Tecnología, Centrado en el Ciudadano y Resiliente

El sector energético ha experimentado una transformación radical en 2034. La convergencia de avances en generación, inteligencia artificial, robótica, ciberseguridad y drones ha creado un ecosistema descentralizado donde la resiliencia es primordial. La estrategia energética favorece la autogeneración, subrayando la necesidad de redes seguras capaces de gestionar miles de minicentrales.

LA REVOLUCIÓN SOLAR: EFICIENCIA, ACCESIBILIDAD E INTEGRACIÓN

En 2034, parques solares flotantes dominan el paisaje junto a aerogeneradores modulares. Entre 2025 y 2034, la energía solar experimentó un crecimiento anual compuesto (CAGR) del 9,5%, impulsado por inversores inteligentes que optimizan la conversión incluso con baja luminosidad.

Los materiales de cuarta generación, como nanopartículas combinadas con polímeros, han creado células más eficientes que aprovechan tanto el espectro visible como el infrarrojo. Las perovskitas han superado récords de eficiencia, estableciéndose como alternativa viable en el mercado. Los paneles solares auto reparables utilizan nano capas capaces de regenerar su estructura ante microgrietas, revolucionando durabilidad y mantenimiento.

La optimización de procesos ha reducido costes, haciendo la energía solar más accesible. El autoconsumo se ha generalizado, y la venta de excedentes mediante blockchain ha permitido a hogares reducir su factura energética en un 40% así como una suficiencia energética.

Desde 2030, la normativa europea exige paneles solares en edificios nuevos, impulsando soluciones fotovoltaicas integradas en los edificios (BIPV) que combinan eficiencia con estética arquitectónica. Las películas fotovoltaicas ultrafinas pueden cubrir hasta el 60% de la superficie de un edificio, produciendo hasta el 30% de sus necesidades eléctricas.

El desarrollo de baterías avanzadas y sistemas de gestión inteligente ha optimizado uso y almacenamiento, gestionando la variabilidad de producción y asegurando continuidad del suministro.

LA POTENCIA EÓLICA: INNOVACIÓN Y GESTIÓN INTELIGENTE

Los aerogeneradores terrestres superan los 25 MW, evolucionando desde modelos anteriores como el Sany SI-270150 (15 MW) y el Nordex N175/6.X. Las turbinas con palas biomiméticas, inspiradas en albatros, reducen resistencia y aumentan captación en vientos bajos.

La IA analiza datos en tiempo real para ajustar orientación y ángulo de palas, maximizando producción incluso ante cambios meteorológicos. El mantenimiento predictivo identifica patrones que preceden a fallos, permitiendo

intervenciones preventivas que reducen inactividad y costes operativos hasta un 10%.

Los drones realizan inspecciones detalladas con cámaras de alta resolución y sensores térmicos, detectando daños sin detener turbinas por largos periodos. Una inspección que antes requería días ahora se completa en menos de una hora. Además, los parques cuentan con sistemas de parada automática cuando se detectan aves en trayectorias de riesgo.

LA ENERGÍA HIDRÁULICA: GENERACIÓN Y ALMACENAMIENTO

En 2034, la energía hidroeléctrica se ha transformado en pilar fundamental de la transición energética global pero muy limitada debido a que se produce con un recurso cada vez más escaso como es el agua. Con eficiencia del 90%, las centrales modernas integran gemelos digitales y la IA gestiona flujos hídricos en tiempo real, mientras algoritmos predictivos optimizan la generación durante sequías, reduciendo pérdidas energéticas en un 25%. Robots submarinos y drones equipados con LiDAR revolucionan el mantenimiento, detectando micro fisuras y optimizando cuencas hidrográficas, recortando costes operativos en 40%. Además, las estaciones de bombeo hidroeléctricas sirven como sistemas de almacenamiento de energía a gran escala mediante un proceso sencillo y eficiente. Durante los periodos de baja demanda eléctrica o cuando hay un exceso de generación renovable (como la solar o eólica), se utiliza la energía sobrante para accionar bombas que elevan el agua desde el embalse inferior hasta el superior. De este modo, la energía eléctrica se convierte en energía potencial almacenada en forma de agua en altura.

LA ENERGÍA NUCLEAR: MODULARIDAD Y FUSIÓN HÍBRIDA

La energía nuclear ha duplicado su capacidad global desde 2024 gracias a reactores modulares pequeños (SMR) y diseños de fusión-fisión híbrida. Esta última tecnología combina estabilidad de fisión con eficiencia de fusión, reduciendo residuos radiactivos en un 90%. Los SMR portátiles abastecen regiones remotas con huella de carbono 50% menor que plantas tradicionales. Las centrales submarinas suministran energía a archipiélagos y plataformas marinas, protegidas contra tsunamis mediante contención geodésica. Los gemelos digitales para plantas nucleares simulan fallos y entrenan operarios en entornos virtuales, reduciendo accidentes en un 85%.



**CONTINÚA EN
PRÓXIMA PÁGINA**

LA INTELIGENCIA ARTIFICIAL: EL CEREBRO COORDINADOR

La IA gestiona flujos bidireccionales en redes descentralizadas. Mientras en 2024 los centros de datos consumían 945 TWh, algoritmos de deep learning han limitado el crecimiento a 1,2% anual.

Aplicaciones disruptivas incluyen gemelos digitales para plantas nucleares, robots humanoides en mantenimiento con bajo coste operativo, y sistemas de gestión para optimizar rendimiento en instalaciones solares y eólicas.

La IA no solo aumenta eficiencia operativa, sino que es fundamental para la resiliencia del sistema, permitiendo gestión dinámica frente a cambios en demanda, condiciones meteorológicas adversas o amenazas a la seguridad.

CIBERSEGURIDAD: EL ESCUDO IMPRESCINDIBLE

En un mundo donde la energía está cada vez más digitalizada y descentralizada, la ciberseguridad se ha convertido en una defensa vital. Incidentes del pasado, como el ciberataque a redes solares, sirvieron como lecciones cruciales que llevaron a la implementación de protocolos de defensa en profundidad.

EN 2034, la seguridad se integra a nivel de componente. Cada panel solar, por ejemplo, incorpora tecnología avanzada de ciberseguridad:

- Encriptación cuántica: Se utiliza para bloquear intrusiones en los inversores, protegiendo la comunicación y la gestión de la energía.
- Sensores de integridad física: Estos sensores son capaces de detectar manipulaciones no autorizadas en el equipo y desconectarlo automáticamente para prevenir daños o accesos maliciosos.

A nivel de red, la iniciativa CyberEurope 2024 sentó las bases para el desarrollo de firewalls autónomos. Estos sistemas aprenden de cada intento de ataque, mejorando continuamente su capacidad de defensa y reduciendo las brechas de seguridad en un estimado del 95%. Una ciberseguridad robusta es esencial para garantizar la continuidad de los servicios en este ecosistema interconectado.

DRONES Y METAVERSO: VIGILANCIA Y PLANIFICACIÓN

El papel de los drones en el sector energético se ha expandido enormemente. Si en 2024 gestionaban alrededor de 10.000 operaciones al año, en 2034 son herramientas indispensables para la inspección técnica, el mantenimiento predictivo, la mejora de la seguridad laboral, la eficiencia operativa y la monitorización ambiental.

Empresas integran estos datos en el metaverso, donde ingenieros y ciudadanos co-diseñan redes de distribución utilizando avatares de IA que asesoran en tiempo real sobre eficiencia energética y simulaciones climáticas extremas.

CONTINUIDAD DE SERVICIOS: RESILIENCIA ANTE AMENAZAS

La resiliencia de la infraestructura energética es una lección aprendida de experiencias pasadas. En una sociedad tan dependiente de la energía es clave el empleo de tecnologías que aseguran la continuidad del suministro.

Una de estas tecnologías son las baterías de gravedad, que almacenan excedentes de energía renovable bajando y subiendo pesas en pozos de hasta 1.000 metros de profundidad, con una notable eficiencia del 82%. Además de las soluciones técnicas de almacenamiento y gestión inteligente (IA, baterías avanzadas), han surgido modelos contractuales innovadores, como los contratos de resiliencia, mediante los cuales las empresas pagan primas para asegurarse acceso prioritario a microgrids durante apagones de red.

EL CIUDADANO Y LA EMPRESA EN EL CENTRO

El hilo conductor de todas estas transformaciones tecnológicas es cómo sirven al ciudadano y a las empresas en el mundo de 2034. Las empresas han adoptado microrredes híbridas solar-eólicas que les proporcionan autonomía energética, reduciendo su dependencia de la red principal y aumentando su resiliencia. Los hogares, por su parte, se han convertido en prosumidores, capaces no solo de auto consumir su energía solar generada, sino también de comercializar sus excedentes a través de tecnología blockchain, logrando reducciones significativas en sus facturas energéticas, así como una independencia energética.

La descentralización, facilitada por la autogeneración y las microrredes, se gestiona de manera eficiente gracias a la IA y los sistemas de gestión inteligente.

Este modelo circular, donde cada usuario es productor y consumidor, refleja las lecciones aprendidas de décadas pasadas. El objetivo principal es asegurar un suministro energético fiable, asequible y sostenible que impulse la economía y mejore la calidad de vida de ciudadanos y empresas.

UN PARADIGMA CENTRADO EN LA GESTIÓN INTELIGENTE

En 2034, el sector energético es casi irreconocible comparado con décadas anteriores. La convergencia tecnológica ha creado infraestructuras resilientes y gestionadas inteligentemente. La energía hidráulica, solar y eólica, con innovaciones en materiales, diseño y gestión, lideran la transición, apoyadas por una energía nuclear más segura.

La inteligencia artificial optimiza producción, distribución y mantenimiento. Los drones y el metaverso aportan capacidades de inspección y planificación colaborativa. La ciberseguridad protege infraestructura vital. Y la resiliencia, incorporada a través de almacenamiento avanzado y políticas adaptativas, asegura continuidad frente a cualquier amenaza.

El reto ya no es generar más, sino gestionar mejor, un principio que guía cada innovación en este nuevo paradigma energético centrado en el ciudadano y sostenible para el planeta.



MARCOS NAVARRO ALCARAZ

Consultor experto en Tecnologías de la información y ha sido ejecutivo de TI en varias compañías multinacionales. Ahora es experto en Outsourcing de TI, Robots y Autoamización y es profesor universitario y en escuelas de negocio.

Twitter:
<https://twitter.com/mnalcaraz>

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

CoE Book

Centres of Excellence

Body of Knowledge

P4MGO!®



P4MGO!

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



Apagón de inteligencia

El apagón del pasado 28 de abril de 2025, que dejó sin electricidad a gran parte de la península ibérica durante varias horas, ha revelado con crudeza una realidad incómoda: la fragilidad de nuestras infraestructuras tecnológicas en una sociedad que de forma ingenua y vanidosa presume de estar digitalmente avanzada. Semáforos apagados, trenes detenidos, redes de comunicación caídas, servicios administrativos paralizados... Todo colapsó en cuestión de minutos, y con ello, se desmoronó momentáneamente la ilusión de control que rodea a nuestras ciudades ¿inteligentes? Ahora de repente recordamos que la tecnología funciona con electricidad. Y yo recuerdo aquel chiste en el que están hablando, de forma metafórica, algunas plataformas y tecnologías entre sí:

- Wikipedia: "Yo lo sé todo".
- Google: "Yo lo tengo todo".
- Facebook: "Yo conozco a todos".
- Internet: "Sin mí, no son nada".
- Electricidad: "Je, je, je..."

Pues eso. En pleno auge de la Inteligencia Artificial (IA), la automatización de tareas y los servicios digitales de última generación, este suceso ha servido como inquietante recordatorio de que toda esta innovación depende absolutamente de una base muy tangible: la energía eléctrica y la conectividad. Sin electricidad no hay datos, no hay procesamiento, no hay algoritmos funcionando ni decisiones automatizadas. Sin electricidad no hay nada, salvo que renunciemos al modelo propio del mundo moderno, un debate interesante y que no podemos abordar en esta ocasión.



CONTINÚA EN
PRÓXIMA PÁGINA

“

**En realidad, la
electricidad no es
más que un rayo
organizado**

George Carlin



Esta vulnerabilidad no es solo técnica, sino también estratégica, incluso psicológica. A medida que delegamos cada vez más decisiones y procesos en sistemas complejos interconectados, la sociedad se vuelve vulnerable y queda más expuesta a disrupciones imprevistas. Una avería, un fenómeno natural o una simple sobrecarga pueden desencadenar efectos en cadena que paralizan no solo el innecesario WhatsApp, que es lo que parece importarles a la gente, sino la mayoría de los servicios esenciales.

En el apagón del 28 de abril, las islas Baleares y Canarias, gracias a su red eléctrica independiente, no sufrieron el corte, lo que evidencia la importancia de modelos descentralizados y resilientes en el diseño de infraestructuras críticas.

Más allá del susto puntual, el episodio obliga a repensar la forma en que planificamos nuestras políticas tecnológicas. No basta con incorporar IA o digitalizar servicios públicos si no se garantiza antes la estabilidad de los sistemas que la sostienen. La sostenibilidad energética, la ciberseguridad, la redundancia operativa y la preparación ante contingencias deben formar parte de cualquier hoja de ruta tecnológica.

Además, el incidente pone sobre la mesa una cuestión más profunda: la confianza ciudadana. Cuando los servicios fallan, incluso por causas excepcionales, la población experimenta una sensación de desprotección que erosiona la credibilidad de las instituciones y los avances prometidos. La modernidad tecnológica debe ir acompañada de una filosofía que podríamos llamar “de la robustez”: si algo puede fallar, debe estar previsto; si algo es imprescindible, debe poder mantenerse y seguir funcionando en condiciones adversas. La propia IA puede ayudar mucho a elaborar planes de contingencias.

En definitiva, el apagón del 28 de abril no solo oscureció nuestras calles, sino también muchas certezas. No habrá IA ni nueva tecnología posible si falla lo elemental. Quizá falle la propia inteligencia enfocada a la prevención, y no hablamos de la artificial. Es un hecho que todas las catástrofes nos cogen con los pantalones bajados. En un mundo que corre hacia la digitalización total, resulta más urgente que nunca detenerse a consolidar los cimientos de la sociedad moderna. Porque sin energía, sin infraestructuras robustas, sin previsión, la innovación no es más que una promesa vacía. Menuda decepción.



VÍCTOR ALMONACID

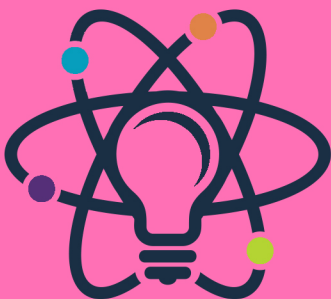
Secretario de la Administración Local, categoría superior. Director de Prevención, Formación y Documentación en la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana. Directivo Público. Máster en Nuevas Tecnologías aplicadas a la Administración Pública. Máster en 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 Administraciones 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/>

BPM Book

Business Process Management Body of Knowledge

P4MGO!®



P4MGO!

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



Alex Aliaga



Así se protege una infraestructura 5G frente a ciberataques

La quinta generación de redes de comunicaciones móviles (5G) ya es una realidad en muchos países, y millones de usuarios hacen uso diario de esta tecnología. Por sus características técnicas, 5G permite conexiones permanentes, ubicuas, de gran capacidad y, sobre todo, de muy alta velocidad.

Con la llegada de esta tecnología, se abre un enorme potencial de transformación, con un impacto multiplicador en la productividad empresarial, la automatización industrial, los servicios críticos y la conectividad de dispositivos, etc. Sin embargo, como toda innovación disruptiva, su adopción conlleva nuevos retos y ciberriesgos que deben ser cuidadosamente analizados y gestionados. La tecnología 5G no solo representa un salto cuantitativo en velocidad y capacidad de conexión, sino también un cambio cualitativo en la forma en que se diseñan y operan las redes móviles. Este nuevo paradigma trae consigo oportunidades sin precedentes, pero también introduce desafíos significativos en materia de ciberseguridad. En este artículo, profundizaremos en los elementos arquitectónicos clave de 5G, las amenazas emergentes y las estrategias para mitigar los riesgos asociados.

ARQUITECTURA DE 5G: UN ECOSISTEMA COMPLEJO Y DINÁMICO

La arquitectura de las redes 5G representa una evolución significativa respecto a las generaciones anteriores, caracterizándose por su flexibilidad, escalabilidad y capacidad para adaptarse a una amplia variedad de casos de uso. Esta transformación es posible gracias a la integración de tecnologías avanzadas que permiten una gestión más

eficiente y dinámica de los recursos de red. En particular, las redes 5G adoptan un enfoque basado en servicios (Service-Based Architecture, SBA), donde las funciones de red se implementan como componentes modulares y virtualizados, usando muchas de las tecnologías que conocemos en el ámbito del mundo IT.

Esta modularidad facilita la implementación de servicios personalizados y la adaptación rápida ante las demandas cambiantes del mercado. Además, la separación entre el plano de control y el plano de usuario permite una gestión más granular y eficiente del tráfico de red.

Como comentábamos, muchas de las tecnologías son conocidas y vienen del mundo IT, a continuación nombramos algunas detallando sus funciones dentro del ecosistema del 5G:

•**Virtualización de Funciones de Red (NFV):** NFV transforma funciones de red que tradicionalmente requerían hardware especializado en aplicaciones que se ejecutan sobre infraestructura de propósito general. Esto reduce la dependencia de hardware propietario y permite una implementación más ágil de nuevos servicios. No obstante, la virtualización también amplía la superficie de ataque, ya que las funciones virtualizadas pueden ser susceptibles a vulnerabilidades del sistema operativo o del hipervisor.



CONTINÚA EN
PRÓXIMA PÁGINA

•**Computación en el Borde (Edge Computing):** La computación en el borde acerca el procesamiento de datos al usuario final, reduciendo la latencia y mejorando la eficiencia en aplicaciones sensibles al tiempo, como vehículos autónomos o realidad aumentada. Esta proximidad también plantea retos de seguridad, ya que los nodos de borde pueden ser más vulnerables a ataques físicos o cibernéticos.

•**Segmentación de Red (Network Slicing):** La segmentación de red permite crear múltiples redes virtuales independientes sobre una misma infraestructura física, cada una optimizada para diferentes casos de uso y con políticas de seguridad específicas.

Esta capacidad es esencial para atender las diversas necesidades de aplicaciones como IoT, comunicaciones críticas o servicios de alta velocidad. Sin embargo, la gestión de múltiples segmentos introduce complejidad adicional en términos de orquestación y aislamiento de seguridad.

AMENAZAS EMERGENTES EN 5G

Tal y como comentábamos en la sección anterior, la adopción de tecnologías como la virtualización de funciones de red (NFV), las redes definidas por software (SDN) y la computación en el borde (edge computing) ha introducido vulnerabilidades que los atacantes pueden explotar. Además, la implementación de la segmentación de red (network slicing) y la proliferación de dispositivos IoT han multiplicado los vectores de ataque, requiriendo una revisión exhaustiva de las estrategias de seguridad existentes.

En este contexto, es fundamental identificar y comprender las amenazas emergentes que afectan a las redes 5G. Estas amenazas no solo comprometen la integridad y disponibilidad de los servicios, sino que también ponen en riesgo la privacidad de los usuarios y la confidencialidad de los datos transmitidos. La creciente dependencia de proveedores externos y la complejidad de las cadenas de suministro tecnológicas añaden capas adicionales de riesgo que deben ser gestionadas de manera proactiva.

A continuación, se detallan algunas de las principales amenazas que enfrentan las redes 5G:

•**Ataques a la Identidad y Privacidad del Usuario:** Aunque 5G implementa mecanismos como el SUCI para proteger la identidad del usuario, estudios han revelado que el protocolo de 5G-AKA aún presenta vulnerabilidades. Estas incluyen ataques de vinculación que permiten rastrear a un usuario a lo largo del tiempo y capturas de IMSI (International Mobile Subscriber Identity), especialmente cuando se emplean

esquemas de cifrado nulos o configuraciones inseguras por parte de los operadores.

•**Vulnerabilidades en APIs y Gestión de IoT:** El uso intensivo de APIs para la gestión de dispositivos IoT en redes 5G ha introducido nuevos vectores de ataque. Investigaciones han identificado fallos en la autenticación y control de acceso en estas interfaces, permitiendo potencialmente el acceso no autorizado a datos y funciones críticas.

•**Ataques de Denegación de Servicio (DoS) y Desincronización:** El protocolo 5G-AKA también ha mostrado vulnerabilidades ante ataques de denegación de servicio y desincronización. Estos ataques pueden explotar la gestión de números de secuencia o mensajes de error para causar fallos persistentes en la autenticación del usuario.

REFLEXIÓN FINAL

Para garantizar la seguridad y resiliencia de las redes 5G frente a las amenazas emergentes, es esencial que los operadores de redes móviles, proveedores de servicios y organismos reguladores colaboren estrechamente en el desarrollo e implementación de medidas de seguridad integrales. En España, este compromiso se ha materializado con la aprobación del Esquema Nacional de Seguridad de redes y servicios 5G (ENS 5G), mediante el Real Decreto 443/2024, de 30 de abril.

El ENS 5G establece un marco normativo específico para abordar los riesgos asociados a la tecnología 5G, considerando las aportaciones de cada agente de la cadena de valor. Sus objetivos incluyen reforzar la protección de la seguridad nacional, garantizar un funcionamiento continuado y seguro de las redes y servicios 5G, y promover un mercado de suministradores diversificado para evitar la dependencia de proveedores de alto riesgo.

Además, el esquema contempla la creación de un Centro de Operaciones de Seguridad 5G de referencia, dependiente del Ministerio para la Transformación Digital y de la Función Pública, encargado de apoyar en la prevención, protección, detección y respuesta frente a amenazas, incidentes y ciberataques en las redes y servicios 5G. Este centro contribuirá a la certificación y normalización de los sistemas, fortaleciendo así la ciberseguridad en el ecosistema 5G nacional.

Asegurar las redes 5G implica ir más allá de las medidas tradicionales: exige el diseño de arquitecturas seguras por defecto, la actualización continua de los protocolos, la cooperación y la capacidad de respuesta ante ciberamenazas complejas y persistentes.



ALEX ALIAGA

Profesional Especializado en la Gestión de la seguridad, tanto desde el punto de vista tecnológico como desde el punto de vista estratégico. Con más de 20 años de experiencia en el sector, ha trabajado tanto en España como en otros países ayudando a las empresas en la gestión, y mitigación de los riesgos TIC, aplicando siempre las mejores prácticas y controles para aportar siempre la protección adecuada. Es colaborador habitual en diversos congresos de seguridad, así como, medios de comunicación, radio y prensa escrita, a nivel internacional donde sus publicaciones técnicas y estratégicas son muy apreciadas. Puede hablarte de ciberseguridad en 3 idiomas.

**Curso de
Certificación en:**

Gestión del Dato

UNE 0078

**Data
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
- Basado en la Norma: UNE 0078
- 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



Insomnio, cuando la mente no se calla

El insomnio es el trastorno del sueño más frecuente. Afecta a uno de cada tres adultos, mientras que esta cifra se duplica en personas con TDAH.

“Dormir es distraerse del mundo”, o así debería ser según Borges. Pero en general, las personas con TDAH tenemos una relación complicada con el sueño, una especie de amor-odio ya que, por un lado, necesitamos dormir y descansar como todo el mundo, pero, por otro lado, la hora de ir a la cama puede convertirse en un momento de estrés ya que nos resulta difícil echar el freno a nuestro cerebro y ponerlo a descansar.

Lo cierto es que el trastorno por déficit de atención e hiperactividad afecta con frecuencia a los patrones de sueño. Las personas con TDAH suelen manifestar dificultades para conciliar el sueño y también para mantenerlo. De hecho, se calcula que entre el 25 y el 50 por ciento tienen problemas para dormir, lo que agrava los síntomas propios de su condición. Provoca un peor funcionamiento cognitivo, mayor somnolencia diurna, inquietud e impulsividad. Y lo que es más grave, un mayor riesgo de presentar otros trastornos asociados como ansiedad o depresión.

¿Qué ocurre cuando dormimos?

El tiempo que pasamos en la cama, si es de calidad, tiene efectos muy positivos en nuestro organismo. Estos son algunos de los más importantes.

Incrementa la creatividad y la productividad. Cuando el cerebro está descansado, la producción de hormonas se equilibra y eso hace que la memoria funcione correctamente y que la imaginación y la creatividad se potencien.

Reduce la depresión. Mientras descansamos se liberan melanina y serotonina, las hormonas que nos ayudan a ser más felices y emocionalmente más fuertes porque contrarrestan los efectos de las hormonas del estrés, la adrenalina y el cortisol.

Consolida la memoria y el aprendizaje, lo que resulta imprescindible para las capacidades cognitivas. Nuestro hipocampo, esa parte de nuestro cerebro donde almacenamos la memoria, se restaura y transforma la memoria a corto plazo en memoria a largo plazo.

Mejora nuestro sistema inmunitario. Se fortalece nuestra respuesta inmune necesaria para defendernos de todos los agresores externos y no enfermarnos.

Ayuda a perder peso. La falta de sueño no solo hace que las células grasas liberen menos leptina que es la hormona supresora del apetito, sino que además provoca que el estómago libere más grelina, que es la hormona del apetito. Así que, dormir ocho horas, nos ayuda a mantener un peso saludable y, por tanto, también mejora nuestra autoestima.

Protege el corazón, ya que la falta de sueño eleva los niveles en sangre de las hormonas del estrés y sube la tensión arterial y la frecuencia cardíaca.

Equilibra nuestro sistema nervioso lo que nos permite tener una buena salud emocional. A pesar de todas las ventajas de un buen descanso, un alto porcentaje de personas con TDAH no encuentran el botón de apagado cuando llega la hora de dormir.



**CONTINÚA EN
PRÓXIMA PÁGINA**



El cerebro con TDAH, acelerado ya de por sí con la hiperactividad mental y con los pensamientos intrusivos, es incapaz de frenar y llega a toda velocidad a la cama. Incluso, cuando consigue dormir, no es un sueño relajante o reparador. Así que, durante el día pueden sentirse muy somnolientos o mostrar alteraciones del estado del ánimo con sensación de irritabilidad, fatiga, cansancio o con escasa capacidad para prestar atención a sus tareas. Es decir, síntomas parecidos a los que presentan personas con patologías del sueño. Estos son algunos de los más frecuentes:

Insomnio: algunas personas muestran más energía durante las horas cercanas a la noche que durante el día y eso puede conducir a un mal descanso y a alterar el ciclo sueño-vigilia. De ahí las dificultades para levantarse por la mañana y la excesiva somnolencia durante el día.

Alteraciones circadianas, lo que implica que se muestren más alerta durante las horas previas a dormir y se retrase el momento de ir a dormir se retrase mucho.

Apneas. Aproximadamente un tercio de las personas con TDAH tienen apneas. Es necesario descartar esta patología que puede ser concomitante con un TDAH y mostrar síntomas diurnos parecidos en ambos casos.

Síndrome de piernas inquietas, que puede estar asociado a otra afección más común que es el movimiento periódico de las piernas durante el sueño.

Narcolepsia. Con frecuencia, los adultos diagnosticados de narcolepsia refieren haber tenido en la infancia síntomas de TDAH.

Es fundamental identificar y tratar estas alteraciones del sueño concomitantes ya que repercuten directamente en los síntomas del TDAH. No son problemas menores porque afectan a nuestro desempeño diario y, lo que es más grave, a nuestra salud física y emocional. Es indudable que el trastorno del sueño agrava la sintomatología de las personas con TDAH ya que causa un empeoramiento del funcionamiento cognitivo e incrementa la inquietud y la impulsividad.

Son muchos los estudios que demuestran esta relación entre los trastornos del sueño y el TDAH, así como que la mejora en la calidad del sueño se asocia con una disminución de los síntomas más molestos. De ahí la necesidad de un diagnóstico temprano y de un tratamiento basado en pautas de higiene del sueño y, en caso de que fuera necesario, tratamiento farmacológico como melatonina, benzodiacepinas o antidepresivos en los casos más extremos.



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_23DRwlw

Instagram:

<https://www.instagram.com/mujeresalbordedeltdah/>

PdM Book

Product Management Body of Knowledge

P4MGO!®



P4MGO!

PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE



La Rioja reflexiona en las Project Sessions 2025 sobre las organizaciones que “cambian el paso” en los ecosistemas empresariales

Las Project Sessions 2025, bajo el título *“Organizaciones que cambian el paso. Diferentes etapas, diferentes formas de avanzar”*, celebradas a comienzos de mayo en Logroño, llenaron el salón de actos de la Consejería de Economía, Innovación, Empresa y Trabajo Autónomo en el Centro Tecnológico de la Rioja, de líderes empresariales, emprendedores y profesionales en una jornada diseñada para discutir los desafíos de las organizaciones en crecimiento.

Organizadas por la Dirección General de Empresa, Energías e Internacionalización del Gobierno de La Rioja, en colaboración con la Asociación de Profesionales de Gestión de Proyectos (APGP), las Project Sessions se enmarcan en el proyecto TECH FABLAB, que es parte del Programa de Redes Territoriales de Especialización Tecnológica (RETECH) y financiado por la UE (Next Generation EU).



CONTINÚA EN
PRÓXIMA PÁGINA



El evento, que cuenta ya con ocho ediciones, se enfocó esta vez en las distintas etapas del ciclo de vida de las empresas, abordando temas como la evolución de las startups hacia corporaciones maduras y los diferentes estilos de gestión. Todo ello desde la visión complementaria de dos ponentes de lujo: Javier Peris y Daniel Alonso.

Apertura de la Jornada: Tecnología y Transformación Empresarial

La jornada fue inaugurada por Amadeo Lázaro, Director General de Empresa, Energías e Internacionalización, quien destacó la importancia de crear espacios de encuentro donde emprendedores, expertos en tecnología y líderes empresariales puedan intercambiar experiencias y conocimientos. Lázaro explicó que el proyecto TechFabLab, desarrollado en colaboración con seis comunidades autónomas, tiene como objetivo generar un ecosistema de emprendimiento conectado, tanto físicamente como virtualmente, para facilitar el intercambio de ideas y oportunidades de negocio entre las regiones. “En La Rioja, este proyecto nos va a permitir lanzar la fase de emprendimiento y escalado de emprendedores en el nuevo parque científico tecnológico denominado TechRioja, que es tremendamente importante, estratégico para la comunidad autónoma”, comentó, subrayando la importancia de preparar a las empresas para adaptarse a un entorno cambiante.



**CONTINÚA EN
PRÓXIMA PÁGINA**



La Rioja

JAVIER PERIS

Director Académico Escuela de Gobierno eGov
Director Tecnología & Sentido Común y
Stakeholders.news



De Macondo a Corporate: El Viaje de la Startup

Javier Peris, Senior Business Strategist y especialista en mejores prácticas, abrió las sesiones con su ponencia “Cien Años de Startup. De Macondo a Corporate”. Inspirándose en la narrativa de Gabriel García Márquez, Peris trazó un paralelismo entre la evolución de las startups y la mítica ciudad de Macondo, explorando cómo las organizaciones pasan de unas etapas iniciales en las que prima el dinamismo y la organización informal a la estabilidad operativa y gobernanza formal. Durante su intervención, Peris indicó que no hay que caer en el error de implementar estructuras corporativas demasiado pronto pero tampoco de desarrollarse al margen de marcos de trabajo que permitan adaptar las estructuras a las nuevas realidades. “Tenemos que cambiar la forma en la que venimos cambiando. Estas oportunidades van a permitir que las empresas logren nuevos objetivos, pero tienen que hacer cosas nuevas”, reflexionó, enfatizando que la gestión de programas, portafolios y servicios es fundamental para aprovechar las oportunidades de la era digital.



CONTINÚA EN
PRÓXIMA PÁGINA

Conducir vs. Pilotar: Diferentes Estilos de Liderazgo

A continuación, Daniel Alonso, Digital & Venture Executive, presentó “Conducir vs. Pilotar”, una reflexión sobre cómo varía el estilo de gestión según el tamaño y la madurez de la organización. Alonso comparó la gestión de startups con la de grandes corporaciones, describiendo cómo cada tipo de empresa exige un enfoque diferenciando para navegar sus desafíos internos y externos. “El cambio es parte de la vida y no hay que tenerle miedo. Hay que coger el toro por los cuernos, entender qué es lo que necesitamos e ir a por ello”, afirmó, resaltando la importancia de frenar y tomarse el tiempo para pensar y, a continuación, actuar.



**CONTINÚA EN
PRÓXIMA PÁGINA**



ZA
OS

Formación Digital
para el futuro
del mundo
del trabajo
del futuro

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



Mesa Coloquio: Liderar en Movimiento

El evento culminó con una mesa coloquio titulada “Liderar en Movimiento: Proyectos, Personas y Dirección en Empresas que Cambian”, moderada por Juan Manuel Domínguez, Presidente de APGP que introdujo el debate con una metáfora sobre el cambio en las organizaciones: “Pues, como el propio título de la jornada, estamos hablando de cambiar el paso y nosotros como personas nos cambiamos los zapatos cuando vamos creciendo, cuando nos rozan”, animando a las organizaciones a ajustar sus estructuras y modelos de gestión para responder a un mercado en constante evolución.

La conversación abierta entre los ponentes también contó con la activa participación del público presente. Durante una hora se abordaron temas como los retos de liderar organizaciones en transformación, el momento adecuado para profesionalizar la gestión y las diferencias en la toma

de decisiones entre startups y grandes corporaciones. También hubo referencias a las pymes y al reto que supone adaptarse rápidamente al cambio tecnológico y crecer sin perder su esencia.

Lecciones para el Futuro Empresarial

El mensaje central de las Project Sessions 2025 fue claro: el éxito empresarial no solo se mide por resultados, sino por la capacidad de evolucionar, adaptarse y seguir compitiendo. Las organizaciones que entienden esto estarán mejor preparadas para enfrentar los desafíos que vendrán.

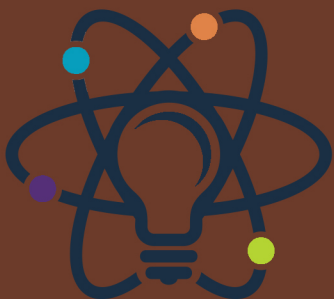
Con eventos como este, TechFabLab continúa consolidándose como un espacio vital para el intercambio de ideas y experiencias en el ámbito de la innovación y el emprendimiento.

PMO Book

Management Offices

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

X Aniversario de la Asociación de Técnicos de Informática de la Administración Local - ATIAL

Siempre es una gran satisfacción cuando una entidad asociativa de las que vertebran el tejido social español alcanza un hito temporal

significativo o un logro de sus fines de relevancia. Y este es el caso de la Asociación de Técnicos de Informática de la Administración



Local - ATIAL, que el pasado 23 de mayo de 2025 celebró su décimo aniversario. Tecnología y Sentido Común estuvo allí.

En el ya lejano 2008, un grupo de personas, dedicadas a las TIC en varios ayuntamientos valencianos se plantearon que era el momento de que ese colectivo, afectado por múltiples carencias,

se organizara para, sobre todo, compartir ayuda mutua y conocimiento útil para su día a día. De aquella idea primigenia, en mayo 2015 un grupo de más de 30 de estos profesionales constituyeron formalmente la



**CONTINÚA EN
PRÓXIMA PÁGINA**



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Asociación de Técnicos de Informática de la Administración Local – ATIAL, y comenzaron su andadura con unos fines asociativos en los que prima la solidaridad entre profesionales, y la puesta en valor del trabajo que este colectivo realiza en los ayuntamientos, diputaciones, cabildos y mancomunidades de España.

El pasado 23 de mayo, ATIAL celebró diez años de existencia, con una serie de actividades, que en este ejercicio, han virado desde las jornadas de marcado carácter profesional y formativo que se realizan cada año, a una jornada eminentemente lúdica y de reencuentros.



**CONTINÚA EN
PRÓXIMA PÁGINA**



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>





La jornada comenzó con una Asamblea General, en la que se renovó la Junta Directiva, bajo la presidencia de Fernando Torregrosa, y que gestionará ATIAL durante los próximos dos años. En dicha reunión también se aprobaron la memoria de actividades y las cuentas anuales de 2024, y el presupuesto para 2025.

Un rato más tarde, los asistentes al evento se trasladaron a la ciudad de Catarroja, uno de los pueblos afectados por la DANA, para comenzar la parte más lúdica de la jornada.

La Junta Directiva había decidido en su momento que esta celebración se realizara en uno de los pueblos afectados por la DANA del pasado mes de octubre de 2024, y así se hizo, con el ánimo de aportar su pequeño grano de arena a la recuperación de la zona.

Cabe decir que son bastantes los socios de ATIAL que prestan sus servicios en ayuntamientos de la zona afectada o que residen en la misma, por lo que la asociación ha estado siempre dispuesta a apoyar en lo que hiciese falta, tanto a estos socios, como a sus entidades locales o a los ciudadanos en general, a través de sus iniciativas de voluntariado.



CONTINÚA EN
PRÓXIMA PÁGINA



La parte lúdica de la jornada comenzó con la actuación del cómico Pablo de los Reyes, que con su humor consiguió que durante toda su actuación los asistentes al evento no pararan de reír, actividad muy sana y útil en el contexto actual. Tras la actuación, se sirvió una estupenda comida de hermandad en el restaurante donde se celebraba el evento.

Finalizado el ágape, ATIAL reconoció el apoyo y colaboración de personas o entidades que, durante estos diez años de andadura, han estado al lado de la asociación, participando de sus actividades o facilitándolas en grado sumo.

En este contexto, ATIAL reconoció al centro Alzira/ Valencia de la Universidad Nacional de Educación a Distancia, al Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana, y D. César Herrero Pombo, secretario general del Ayuntamiento de Tavernes de la Valldigna.

La jornada se cerró con un discurso del presidente de ATIAL, en el que se destacó que la asociación llevaba *"una década dedicada a potenciar el intercambio de experiencias, a concretar sinergias y a dignificar la labor fundamental de los profesionales TIC en el corazón de nuestras administraciones locales"*.

Asimismo, el Sr. Torregrosa incidió en la *"función casi terapéutica de la asociación frente a las situaciones que todos los TIC locales viven en sus administraciones"*.

No en vano ATIAL ha venido reivindicando en estos años el reconocimiento profesional de este personal y el valor que pueden aportar a sus ayuntamientos y diputaciones, si les dejan hacerlo.

Y en esta ocasión, en su discurso el presidente de la asociación recordó alguno de los retos a los que sus socios habían hecho frente en estos años, como la llegada de la Ley 39/2015, la pandemia del COVID19, y finalmente, la funesta DANA de 2024, en las que los servicios y el buen hacer de sus asociados han sido clave para mantener en funcionamiento a sus administraciones locales.

Para finalizar, el presidente de ATIAL agradeció a las entidades colaboradoras, patrocinadores, socios y miembros actuales y pasados de la Junta Directiva de la asociación su apoyo, ayuda y dedicación en estos diez años, y manifestó su convencimiento de que ATIAL continuará creciendo y mantendrá sus fines y actividades mucho más allá de otros diez años.

Stakeholders

.news

Cada tercer domingo de mes disfruta de la Revista Stakeholders.news
Revista Mensual de los Profesionales en Dirección y Gestión de Porfolios, Programas y Proyectos, Cambio Organizacional y Transformación Digital.



UNE aprueba su Estrategia 2030 y refuerza su liderazgo internacional

•La Asamblea General de UNE aprueba la Estrategia 2030, que tiene tres objetivos: poner el conocimiento de las normas técnicas al servicio del progreso compartido de España, impulsar la comunicación sobre los beneficios de las normas, y asegurar la sostenibilidad de UNE.

•En 2024, UNE publicó estándares que ayudan a las empresas españolas a superar sus grandes desafíos, en ámbitos como la doble transformación digital y ecológica, el acceso a los mercados, la innovación o los retos sociales, como el primer estándar global para lograr los Objetivos de Desarrollo Sostenible.



D. Edmundo Fernández
Tesorero UNE

D. Javier García
Secretario

UNE

Normalización Española

• **España reforzó su liderazgo internacional en normalización, incrementando hasta 161 las responsabilidades de los expertos españoles en los organismos globales de estandarización. El director general de UNE, Javier García, fue reelegido vicepresidente de ISO para un nuevo mandato de dos años.**

• **Las normas técnicas son herramientas estratégicas para el crecimiento económico y la competitividad empresarial: aportan el 1 % del PIB español y suponen el 5 % de los ingresos por ventas de las empresas que las aplican, según varios estudios.**

La Asociación Española de Normalización, UNE, ha celebrado hoy su Asamblea General, en la que se ha aprobado la Estrategia UNE 2030, que guiará los pasos de la Entidad durante los próximos años, y se ha presentado el Informe Anual 2024, que recoge las principales actividades desarrolladas por el Organismo español de normalización el pasado ejercicio. El director general de Estrategia Industrial y de la Pyme del Ministerio de Industria y Turismo, Jordi García Brustenga, ha clausurado la

Asamblea, en la que se han entregado los Premios UNE de Normalización 2025.

El director general de UNE y vicepresidente de ISO, Javier García, ha señalado: "La Estrategia UNE 2030 marca con un adecuado nivel de detalle los pasos hacia dónde debemos dirigir todos nuestros esfuerzos los próximos años para lograr nuestro propósito: contribuir al progreso compartido de la sociedad y a la creación de un mundo más seguro, sostenible y competitivo a través del desarrollo de estándares".

La Estrategia UNE 2030, que coge el relevo de la Estrategia 2025, se basa en tres objetivos: poner el conocimiento recogido en las normas al servicio del progreso compartido de España, impulsar la comunicación sobre los beneficios de las normas y asegurar la sostenibilidad de UNE.



**CONTINÚA EN
PRÓXIMA PÁGINA**





En línea con su Estrategia, en 2024 UNE publicó nuevos estándares que ayudan a las empresas españolas a superar sus grandes desafíos, en ámbitos como la doble transformación digital y ecológica, el acceso a los mercados y las exportaciones, la innovación o la capacitación de los profesionales.

Además, el Organismo español de normalización desarrolló normas que contribuyen a hacer de España un país más resiliente, en campos como la protección de las infraestructuras críticas, solidez de la gobernanza, prestación de servicios de asesorías, gestorías y despachos profesionales o prevención del fraude alimentario.

Beneficios económicos

Las normas son herramientas estratégicas para el tejido productivo y empresarial y tienen beneficios económicos. En este sentido, aportan al crecimiento económico español el 1 % del PIB y suponen el 5 % de los ingresos por ventas de las empresas que las aplican, según estudios del Instituto de Estudios Económicos (IEE) y la Organización Internacional de Normalización (ISO). Además, reducen un 7 % los costes empresariales y mejoran un 13 % la productividad, según dichos estudios.

En una dimensión social, el año pasado se publicó el primer estándar global para lograr los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de Naciones Unidas. UNE participó activamente y lideró su traducción al español.

Liderazgo internacional

Otro de los hitos en 2024 fue el impulso a la internacionalización del liderazgo español en la normalización; de hecho, las responsabilidades de los expertos españoles en los organismos internacionales y europeos de estandarización se incrementaron hasta

las 161. Entre ellas, la de Javier García, director general de UNE, que fue reelegido vicepresidente de ISO para dos años más, con lo que completará un mandato de cuatro años. Cada vez más normas españolas son la base para elaborar estándares europeos o internacionales. Un ejemplo ilustrativo: España lideró a nivel europeo iniciativas de estandarización relacionadas con el uso ético de la inteligencia artificial (IA) en 2024.

Nuevos miembros UNE

En 2024 se incorporaron 26 nuevos miembros a la base asociativa de UNE, compuesta por 548 entidades, que representan a la práctica totalidad del tejido productivo y económico español. Entre ellas, se encuentran las 200 principales asociaciones empresariales españolas, grandes empresas, Administraciones públicas, universidades y centros tecnológicos. Los miembros de UNE son el motor y pilar del sistema de normalización español.

El año pasado UNE publicó su cuarto informe anual del Observatorio de Vigilancia de Mercado, para fortalecer la colaboración público-privada en esta materia y contribuir a la comercialización de productos y servicios conformes y seguros.

Premios UNE 2025

Durante la Asamblea General, se entregaron los Premios UNE de Normalización 2025 con los que distingue el compromiso y la profesionalidad de los Comités de Normalización y las personas que los conforman. Los premiados de esta edición han sido:

- Premio López Agüí al CTN-UNE más destacado: CTN-UNE 60 Combustibles gaseosos e instalaciones y aparatos de gas, cuya secretaría lidera SEDIGAS; y CTN-UNE 321 Ascensores, escaleras mecánicas y andenes móviles, cuya secretaría desempeña FEEDA.

- Premio UNE a la Presidencia más destacada de CTN-UNE o SC-UNE: Antonio Valladolid, presidente del CTN-UNE 205 Lámparas y equipos asociados.

- Premio UNE a la Vocalía más destacada de CTN-UNE o SC-UNE: Ismael Caballero, socio-director de DQTeam (CTN-UNE 71/SC 7 Ingeniería de software y sistemas de información).

- Premio UNE a la Integración de la Estandarización y la Innovación: centro tecnológico AIMPLAS.

**Hace mucho
tiempo que
hablas.**

**¿Pero hace
cuánto no
dialogas?**



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

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

NUEVOS MASTERS



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

MasterGEIT®
Gobierno y Gestión de
Información y Tecnología

TITULACIÓN
MasterGEIT®

CONTENIDO DEL MASTER

Módulo 01: Gestión del Tiempo
Curso de Doble Certificación TSG4® Yellow Belt + TSG4® Green Belt

Módulo 02: Gestión de Procesos de Negocio
Curso de Doble Certificación BPM Executive + ISO 19510 Leader

Módulo 03: Dirección y Gestión de Proyectos
Curso de Doble Certificación OpenPM® (PgM) Executive + ISO 21502 Leader

Módulo 04: Dirección y Gestión de Programas
Curso de Doble Certificación OpenPM® (PgM) Executive + ISO 21503 Leader

Módulo 05: Gestión de Servicios de Tecnología
Curso de Doble Certificación FITSM Executive + ISO 2000 Leader

Módulo 06: Gestión de Seguridad de la Información
Curso de Doble Certificación CSX Executive + ISO 27000 Leader

Módulo 07: Gestión de la Continuidad del Negocio
Curso de Doble Certificación CBC Executive + ISO 22301 Leader

Módulo 08: Gobierno de Información y Tecnología
Curso de Doble Certificación COBIT 2019 Executive + ISO 38500 Leader

Módulo 09: Gobierno del Dato
Curso de Doble Certificación DANA Executive + ISO 38505 Leader

Módulo 10: Gobierno Corporativo
Curso de Doble Certificación COSO Executive + ISO 37000 Leader

MISIÓN
Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- ✓ Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- ✓ Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- ✓ Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- ✓ Cursos de Doble Certificación convalidables por asignatura del Master en Gobierno, Dirección, Gestión y Ejecución de Portfolios, Programas y Proyectos MasterPPM®.

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

eGob®

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