

REVISTA **Tecnología & Sentido Común**



#52

MAYO
2025

**Ismael
Novo**

NUESTRO INVITADO
A #TYSC

28

El Gubernauta

JAVIER PERIS

08

**Futuro y
Seguridad**

MANUEL SERRAT

12

**Tecnoregulación
en Prospectiva**

NACHO ALAMILLO

16

Radio Security

ALEX ALIAGA

48

Ai Futuro

MARCOS NAVARRO

40

Es tendencia

MARLON MOLINA

32

**La nueva
Administración**

VÍCTOR ALMONACID

44

**Diario de una
tortuga ninja**

JUAN CARLOS MURIA

20

**Mentes
Divergentes**

MARTA MARTÍN

52



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 Administracion
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



índice

DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



**Ismael
Novo**



**Las criptomonedas
vuelven a ser tendencia**



**La creAltividad
del futuro**



**Decálogo para cultivar
el arte de la atención**

Copyright

02

Índice de Contenidos

04

Este mes te recomiendo leer...

por JAVIER PERIS

07

SLA or XLA that is the agreement

EL GOBERNAUTA
JAVIER PERIS

08

Estamos protegidos, seguro

FUTURO Y SEGURIDAD
MANUEL SERRAT OLMOS

12

Caminando hacia la Cartera Europea de Identidad Digital: llega MiDNI

TECNOREGULACIÓN
EN PROSPECTIVA
NACHO ALAMILLO

16

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

DIARIO DE UNA
TORTUGA NINJA
JUAN CARLOS MURIA

20

Ismael Novo

NUESTRO
INVITADO A TYSC

24

Las criptomonedas vuelven a ser tendencia

ES TENDENCIA
MARLON MOLINA

32

Signal leaks tan lejos y a la vez tan cerca

OJO AL DATO
RICARD MARTÍNEZ
MARTÍNEZ

36

La creAltividad del futuro

AI FUTURO
MARCOS NAVARRO

40

CiberseguridadAI

LA NUEVA
ADMINISTRACIÓN
VÍCTOR ALMONACID

44

Desentrañando la Ciberseguridad en Redes Tácticas 6G: Amenazas, Arquitectura e Inteligencia Artificial

RADIO SECURITY
ALEX ALIAGA

48

Decálogo para cultivar el arte de la atención

MENTES DIVERGENTES
MARTA MARTÍN

52

¿Excelencia? Una crónica sobre la transformación del servicio en la era digital

EVENTOS

56

Semana Informática 2025 culmina otra edición con una gran acogida del sector que refuerza su compromiso con la innovación y el desarrollo tecnológico

EVENTOS

68

UNE publica en español el estándar global de IA para las empresas

NORMALIZACIÓN

78

#52 - MAYO 2025

Índice

#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



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.

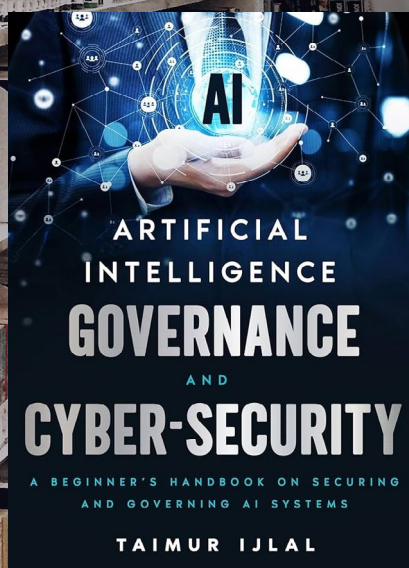


Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA



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.





Artificial Intelligence (AI) Governance and Cyber-Security.

A beginner's handbook on securing and governing AI systems

TAIMUR IJLAL

En un mundo cada vez más impulsado por la Inteligencia Artificial (IA), comprender sus implicaciones y riesgos es crucial, no solo para los expertos técnicos, sino para cualquier profesional en roles de gestión, riesgo o seguridad. El libro de **Taimur Ijlal, *Artificial Intelligence (AI) Governance and Cyber-Security: A beginner's handbook on securing and governing AI systems***, emerge como una guía esencial y accesible para este desafío.

Ijlal, un experimentado profesional de la seguridad de la información, logra desmitificar un campo a menudo intimidante. El libro evita la jerga matemática compleja y la programación, centrándose en cambio en los conceptos fundamentales de la IA y el Machine Learning (ML), explicando su impacto transformador (la "Cuarta Revolución Industrial") y, lo más importante, los riesgos inherentes.

La obra aborda de manera clara y estructurada las preocupaciones clave: desde los riesgos de privacidad y los sesgos algorítmicos hasta la disrupción laboral y el uso malicioso de la IA en ciberataques. Un punto fuerte es su enfoque práctico en la gobernanza y la ciberseguridad específicas para la IA. Ijlal guía al lector en la creación de marcos de gobernanza, destacando principios de confianza como la explicabilidad y la

equidad, y referenciando modelos existentes como el de Singapur.

Particularmente valiosa es la sección dedicada a los riesgos de ciberseguridad únicos de los sistemas de IA, como el envenenamiento de datos y modelos (Data/Model Poisoning), la evasión de modelos (Model Evasion) y la extracción de datos o modelos (Data/Model Extraction). El autor no solo identifica estas amenazas del "aprendizaje automático adversario", sino que propone controles específicos y metodologías como el modelado de amenazas (Threat Modeling) y las pruebas de seguridad adaptadas (referenciando el marco MITRE ATLAS). Además, contextualiza la importancia de la regulación, analizando la pionera Ley de IA de la UE.

En resumen, este libro es una introducción sólida y pragmática para aquellos que necesitan entender y gestionar los riesgos asociados con la IA sin ser científicos de datos. Es una lectura recomendada para profesionales de ciberseguridad, gestores de riesgos, auditores y líderes empresariales que buscan navegar con responsabilidad el complejo panorama de la inteligencia artificial. Ofrece un puente necesario entre la tecnología y su implementación segura y ética.

Javier Peris

SLA or XLA that is the agreement

Como profesionales que llevamos años inmersos en el dinámico mundo de la gestión de servicios, especialmente en el ámbito tecnológico pero extensible a casi cualquier sector, hemos convivido durante mucho tiempo con un acrónimo que ha marcado nuestras operaciones, nuestros contratos y, en gran medida, nuestras conversaciones con clientes y usuarios: el SLA, o Acuerdo de Nivel de Servicio. Hemos dedicado incontables horas a definir métricas precisas, a negociar porcentajes de disponibilidad, tiempos de respuesta y resolución, y a establecer penalizaciones por incumplimiento. Los SLAs han sido, y en muchos casos siguen siendo, la piedra angular sobre la que construimos la confianza contractual con quienes reciben nuestros servicios. Nos han proporcionado un marco tangible, medible y, sobre todo, objetivable para evaluar el rendimiento. Si el servidor estaba disponible el 99,9% del tiempo pactado, si respondíamos a la incidencia en menos de 15 minutos, si resolvíamos el problema en menos de 4 horas, habíamos cumplido. Éxito. O eso creíamos.

Sin embargo, en los últimos años, una nueva corriente ha ido ganando fuerza, introduciendo otro acrónimo en nuestro léxico profesional: el XLA, o Acuerdo de Nivel de Experiencia. La propuesta es atractiva y, a primera vista, parece responder a una evidencia que muchos ya intuíamos o incluso sufríamos en silencio: cumplir rigurosamente con todos los indicadores de un SLA no garantiza en absoluto que el cliente o el usuario final esté satisfecho. ¿De qué sirve una disponibilidad



del 99,9% si el 0,1% restante de caída ocurre precisamente en el momento más crítico para el negocio del cliente? ¿Qué valor tiene responder a una incidencia en 5 minutos si la solución tarda días en llegar o si el trato recibido durante el proceso es impersonal, frustrante o ineficaz? El XLA viene a decirnos que debemos mirar más allá de los fríos números técnicos y empezar a medir lo que realmente importa: la percepción, la satisfacción, la facilidad de uso, el valor aportado desde la perspectiva de quien consume el servicio.

Este cambio de enfoque hacia la experiencia es, sin duda, necesario y bienvenido. Responde a una evolución natural en un mercado cada vez más competitivo, donde la diferenciación ya no reside únicamente en la robustez técnica, sino en la calidad global de la interacción. Los usuarios, acostumbrados a experiencias fluidas y personalizadas en su vida digital personal, esperan lo mismo de los servicios profesionales y corporativos. Quieren sentirse escuchados, comprendidos y valorados. Quieren que la tecnología o el servicio les facilite la vida, no que se la complique. Por tanto, incorporar métricas de experiencia, como el Net Promoter Score (NPS), el Customer Satisfaction (CSAT), el Customer Effort Score (CES), o indicadores más cualitativos obtenidos a través de encuestas, entrevistas o análisis de sentimiento, es un paso lógico y estratégico. Nos obliga a ponernos en la piel del usuario, a entender su viaje (customer journey) y a optimizar cada punto de contacto.

Ahora bien, y aquí es donde me gustaría introducir una reflexión más profunda que va más allá de la simple dicotomía SLA vs. XLA. Creo firmemente que, como profesionales del sector servicios, nuestra aspiración no debería limitarse a cumplir con unas métricas, ya sean técnicas o de experiencia. Deberíamos aspirar a algo más fundamental, algo que debería estar grabado en nuestro ADN profesional: la excelencia en el servicio. La excelencia no es solo cumplir un contrato o satisfacer unas expectativas; es superarlas de forma consistente. Es anticiparse a las necesidades, es resolver problemas de raíz, es ofrecer un trato humano y empático, es buscar la mejora continua de forma proactiva, es entender el contexto del cliente y aportar valor real a sus objetivos.

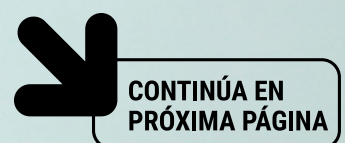
Desde esta perspectiva, el debate no debería ser si reemplazamos los SLAs por los XLAs, sino cómo integramos la medición de la experiencia (XLAs) como un componente más, crucial sin duda, dentro de un marco mucho más amplio de búsqueda de la excelencia. La excelencia debería ser el estándar asumido, la base sobre la que operamos. Los SLAs nos dan el marco técnico mínimo, los XLAs

nos dan el pulso de la percepción del usuario, pero la excelencia es el motor que impulsa la calidad intrínseca y el valor diferencial de lo que hacemos. No deberíamos necesitar un XLA para preocuparnos por si el usuario está contento; esa preocupación debería ser inherente a nuestra ética profesional. El XLA, en este sentido, se convierte en una herramienta valiosísima para *medir y validar* que nuestro compromiso con la excelencia está dando sus frutos en términos de percepción, pero no debería ser la *única* razón para buscarla.

La excelencia implica un compromiso cultural dentro de la organización, desde la alta dirección hasta el último técnico de soporte. Implica invertir en formación, en herramientas adecuadas, en procesos eficientes y, sobre todo, en empoderar a las personas que están en contacto directo con el cliente o usuario para que puedan tomar decisiones orientadas a ofrecer la mejor solución posible. Significa no conformarse con "lo que dice el contrato", sino ir más allá cuando la situación lo requiere. Significa entender que cada interacción es una oportunidad para reforzar la confianza y demostrar nuestro valor.

Y es precisamente en este contexto de búsqueda de una excelencia más estructurada y reconocida donde cobran especial relevancia dos normas ISO que han visto la luz recientemente y que merecen toda nuestra atención. Hablo de **la ISO 23592: Excelencia en el servicio – Principios y modelo** y de **la ISO 11367: Servicios públicos – Excelencia en el servicio público – Principios y modelo**. Estas normas no vienen a reemplazar a los SLAs ni a los XLAs, sino a proporcionar un marco de referencia, unos principios rectores y un modelo para que las organizaciones, tanto del sector privado como del público, puedan abordar la excelencia en el servicio de una manera sistemática y coherente.

Profundicemos un poco en ellas, ya que creo que marcan un hito importante en la formalización de lo que muchos veníamos persiguiendo de forma más intuitiva. La **ISO 23592**, dirigida a cualquier tipo de organización que preste servicios, se basa en la idea de que la excelencia en el servicio es un camino hacia la creación de valor sostenible tanto para la organización como para sus clientes y otras partes interesadas.



CONTINÚA EN
PRÓXIMA PÁGINA

No se trata solo de satisfacer, sino de deleitar y sorprender positivamente al cliente. La norma establece una serie de principios clave que deben guiar a las organizaciones en este camino. Entre ellos, destaca lógicamente el enfoque en el cliente, comprendiendo y anticipando sus necesidades y expectativas, pero va más allá. Habla de liderazgo visionario y comprometido con la cultura de excelencia, de la implicación y desarrollo de las personas como activo fundamental, de la gestión por procesos para asegurar la consistencia y la eficiencia, de la importancia de la innovación y la mejora continua, de la toma de decisiones basada en datos y evidencias (aquí encajarían perfectamente las métricas de SLAs y XLAs), y de la creación de alianzas y relaciones mutuamente beneficiosas. Lo interesante de la ISO 23592 es que propone un modelo flexible que las organizaciones pueden adaptar a su contexto específico, ayudándolas a identificar sus fortalezas y áreas de mejora en el camino hacia la excelencia, fomentando una cultura interna orientada a superar las expectativas.

Por otro lado, tenemos la **ISO 11367**, que aborda la excelencia específicamente en el ámbito de los servicios públicos. Este es un campo con particularidades muy relevantes. Aquí no hablamos solo de clientes, sino de ciudadanos. El objetivo no es únicamente la satisfacción individual o el beneficio económico, sino la creación de valor público, el fortalecimiento de la confianza en las instituciones, la garantía de derechos y el fomento de la cohesión social. La ISO 11367 recoge muchos de los principios de la excelencia en servicios generales, pero los adapta y complementa con aspectos cruciales para el sector público. Pone un énfasis especial en la orientación al ciudadano, asegurando la accesibilidad, la equidad y la inclusión. Destaca la importancia de la ética, la integridad, la transparencia y la rendición de cuentas (accountability) como pilares fundamentales. Subraya la necesidad de eficiencia y sostenibilidad en el uso de los recursos públicos. Además, promueve la colaboración entre distintas entidades públicas y con la sociedad civil para abordar los complejos retos sociales. Esta norma reconoce que la excelencia en los servicios públicos es esencial para el buen funcionamiento de la democracia y el bienestar de la sociedad en su conjunto. Ofrece a las administraciones públicas una guía para modernizarse, para ser más receptivas a las necesidades ciudadanas y para mejorar su desempeño de forma medible y comparable, siempre con el objetivo último de generar un impacto positivo en la vida de las personas.

La aparición de estas dos normas ISO es, a mi juicio, una señal clara de la madurez que está alcanzando la disciplina de la gestión de servicios. Nos invitan a elevar la mirada más allá de los acuerdos contractuales específicos (SLAs) y de la medición de la percepción puntual (XLAs). Nos proponen un marco holístico para integrar la excelencia como un valor estratégico y



operativo fundamental. Implementar los principios de estas normas no es una tarea sencilla, requiere un compromiso profundo y sostenido en el tiempo, pero los beneficios potenciales son enormes: mayor lealtad de los clientes/ciudadanos, mejor reputación, mayor eficiencia operativa, un personal más motivado y comprometido y, en última instancia, organizaciones más resilientes y exitosas.

Entonces, volviendo a la pregunta inicial: ¿SLAs o XLAs? Mi respuesta es que necesitamos ambos, pero entendidos no como fines en sí mismos, sino como herramientas dentro de una aspiración mayor: la excelencia en el servicio. Los SLAs nos dan la base técnica y contractual. Los XLAs nos ayudan a medir si estamos conectando emocional y funcionalmente con nuestros usuarios. Pero son las prácticas y la cultura de excelencia, ahora codificadas y guiadas por estándares como la ISO 23592 y la ISO 11367, las que realmente nos permitirán diferenciarnos y cumplir con la responsabilidad que tenemos como profesionales: entregar no solo un servicio que funciona, sino un servicio que aporta valor, que genera confianza y que, idealmente, supera las expectativas. La excelencia ya no es una opción, es el camino que debemos recorrer, y ahora tenemos mejores mapas para guiarnos en él.



JAVIER PERIS

Javier Peris es Socio Director y CKO (Chief Knowledge Officer) de Business Technology & Best Practices (Business&Co.®) especializado en Gestión del Portfolio, Programas y Proyectos, Centros de Excelencia así como Marcos de Gobierno y Gestión de Tecnologías de la Información con más de 20 años de experiencia tanto en empresas como en Organismos Oficiales y Administración Pública. Es Profesor de IE Business School e IE Executive Education y dispone de las Acreditaciones Internacionales CGEIT®, CRISC®, COBIT5® Certified Assessor, ITIL® Expert & Trainer, PRINCE2® MSP® MoP® MoV® MoR® P30® Practitioner & Trainer, Sourcing Governance®, VeriSMTM SIAMTM, OKR, Lean, Kamban, Design Thinking, Scrum & AgileSHIFT® Accredited Trainer ejerce como Business Coach, Business Angel e Interim Manager.

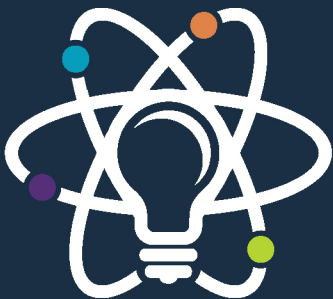
LinkedIn: <https://es.linkedin.com/in/javierperis> **Twitter:** <https://twitter.com/JavierPeris>
Blog: <https://javierperis.com>

Gov Book

Governance

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Estamos protegidos, seguro

Casi tan peligroso que no ser consciente de los riesgos en materia de seguridad de la información es pensar que se está a salvo de cualquier incidente en la materia. La falta de método en la definición de las medidas de seguridad, quizá impulsada por el mercado y a golpe de sobresalto, suele ser habitual en las organizaciones de nuestro entorno. De ahí que se desconozca en muchas ocasiones el nivel de riesgo que se está aceptando de forma inconsciente.

La expresión *"Tranquilo, que nosotros estamos seguros"* (aplicada a los sistemas de información) es una de las frases que muchos responsables de organizaciones escuchan (o han escuchado en el pasado) de ciertos personajes. Si quien la pronuncia es un mando no técnico, probablemente no sea consciente de la realidad de la situación. Pero si quien la pronuncia es un responsable técnico de los sistemas, sólo hay dos opciones: o ha hecho muy bien su trabajo y ha simplificado la frase para que se entienda la situación, o no ha hecho bien su trabajo y desconoce no ya la situación de sus sistemas, sino cómo está el entorno.

En muchas organizaciones, las inversiones tecnológicas se han venido realizando en base a argumentos, digamos, poco objetivos. Hacía falta computación, comprábamos servidores, por ejemplo. Y con la ciberseguridad ha ocurrido algo parecido. Como hace falta tenerla, mucha gente se puso en su día a comprar cortafuegos, antivirus, sistemas de backup, etc., simplemente porque parecía que había una "receta para estar ciberseguro". Sin embargo, la tozuda realidad en esta materia, por mucho que haya quien no quiera verla o interpretarla correctamente, no es tan fácil de resolver simplemente comprando equipos o contratando personal o servicios de terceros.

Lo primero que la Dirección de una organización debe exigir a sus servicios de Tecnologías de la Información es que conozcan las amenazas a las que sus sistemas de información están sometidos, cuál es el posible impacto de dichas amenazas en la organización, y cuál es el nivel de riesgo al que se está expuesto. A continuación, se debe exigir que, a ser posible de forma sistemática y usando algún método contrastado, se proceda a realizar un análisis de las posibles medidas de seguridad que permitan reducir el riesgo hasta niveles aceptables. Y finalmente, aquellos riesgos que no se puedan reducir más, aceptarlos, transferirlos o evitarlos.

Con un **enfoque metódico**, como el propuesto por la norma UNE 71504 "Metodología de análisis y gestión de riesgos para los sistemas de información", o el que se puede encontrar en la metodología MAGERIT 3.0,



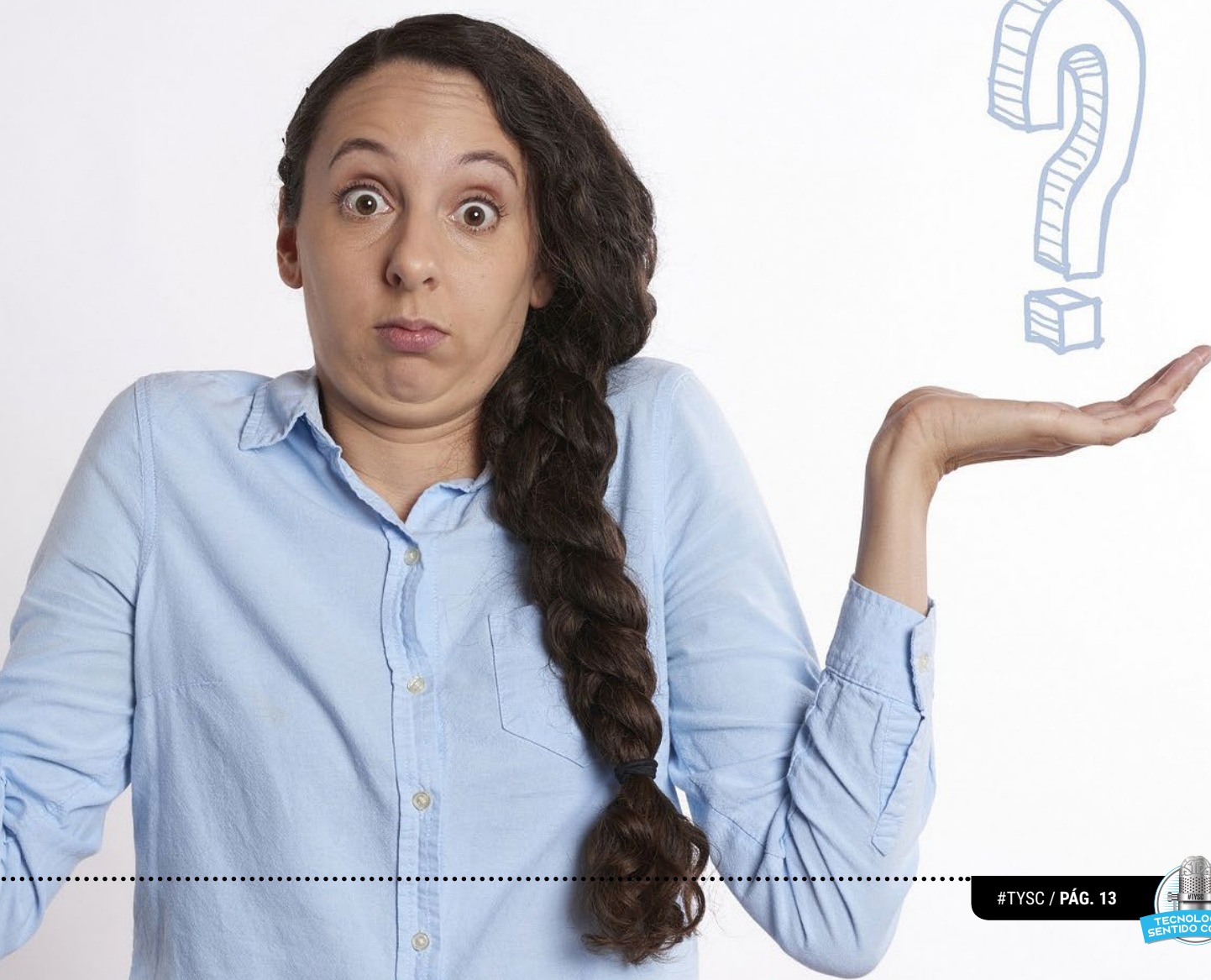
utilizada en las Administraciones Públicas españolas, la organización que desea obtener un adecuado rendimiento de sus inversiones en ciberseguridad dispondrá de una forma adecuada para planificar e implementar las medidas de seguridad apropiadas, evitando sobrecostes o asumiendo riesgos inasumibles.

Sea cual sea la metodología, es muy probable que la organización deba realizar una serie de actividades para lograr un marco de ciberseguridad adecuado a su situación contextual concreta, y que le permita revisarlo con una periodicidad apropiada. Es la aplicación del **ciclo PDCA de Deming a la ciberseguridad** lo que dotará a la organización de un nivel de riesgo lo suficientemente bajo como para que se puedan decir en voz alta expresiones del tipo “*Estamos razonablemente seguros*”, aplicada a los sistemas de información. Porque si algo debe tener claro cualquier responsable de una organización es que el **riesgo cero no existe**. Lo que existe es un nivel de riesgo aceptable. Las actividades que, en general, se deberán acometer en cualquier organización para adecuar su nivel de riesgo son las siguientes:

1. Realizar un inventario de los **activos** relacionados con las tecnologías de la información, no sólo tecnológicos, sino también información, instalaciones, personal, proveedores, etc.

2. Valorar qué supondría para la organización la pérdida (en sentido amplio) de ese activo. Ténganse en cuenta aspectos reputacionales, posibles impactos por pérdidas de confidencialidad en cuestiones de propiedad intelectual, etc. Está claro que valorar los dispositivos tecnológicos es muy fácil. Lo complicado es valorar el resto de componentes. La valoración puede hacerse cuantitativamente (en euros) o cualitativamente (en una escala de Muy valioso a Despreciable).

3. Analizar a qué amenazas está sujeto cada uno de los activos, y cuál es la probabilidad de su ocurrencia. Esta valoración de la probabilidad también puede hacerse de forma cualitativa (en porcentaje en un periodo de tiempo) o cualitativa (en una escala desde Muy alta a Despreciable). Se puede empezar por tres o cuatro amenazas principales, y dejar para ciclos futuros de mejora ir agregando otras. Hay que tener en cuenta que habrá amenazas que no dañen al 100% un activo, por lo que ese factor de daño también hay que tenerlo en cuenta.





4. Conocidos los activos y las amenazas que les circundan, y siendo homogéneos en las escalas de valoración (o cualitativas o cuantitativas ambas) se puede calcular cuál es el daño que cada amenaza haría en caso de materializarse, y a ese valor se le llama **Riesgo**. Se suele escalar en valores de 0 a 10 ó a 100.

5. A continuación, se evalúan las medidas de seguridad existentes en los diferentes activos, y cómo reducen el impacto de la amenaza en el activo, es decir, como reducen el riesgo de esa amenaza y activo. Tras esta evaluación, tenemos un riesgo residual, que es el que debemos tratar (quizá con más medidas de seguridad), transferir (con un seguro, por ejemplo), evitar (retirando activos del uso) o aceptar.

6. Al final, siempre acabaremos teniendo que aceptar algún nivel de riesgo, por lo que es responsabilidad de la Dirección de la organización establecer cuál es **el nivel de riesgo que se acepta (NRA)** en cada ciclo de mejora de la ciberseguridad.

7. Para todos los riesgos que se encuentran por encima del NRA, el personal especializado debe plantear un **Plan de Tratamiento del Riesgo (PTR)**, que, de forma justificada, plantee qué medidas de seguridad pueden ponerse en marcha para reducir esos riesgos por debajo del valor del NRA. Estas medidas pueden ser inversiones, contratar nuevos servicios, o simplemente, cambios organizativos, lo

que incluye también políticas, normas y procedimientos a poner en marcha para lograr nuestro objetivo.

8. Idealmente, tras la finalización del PTR sería conveniente realizar algún tipo de auditoría para verificar la efectividad de las medidas ejecutadas y que realmente el riesgo de los sistemas de información está por debajo del NRA.

9. Pasado un determinado plazo (uno o dos años), o cuando los sistemas de información sufran cambios de calado, se deberá reiniciar el ciclo de mejora de la ciberseguridad, de forma que la Dirección pueda bajar el NRA en cada ciclo, acercándolo cada vez más al cero. Y tampoco estaría de más hacer análisis de riesgos de los nuevos servicios durante la fase de concepción de los mismos.

Como puede ver el lector, esta es una aproximación sistemática, que permite justificar todos los costes que se asumen en la seguridad de los sistemas de información, y que no se ve afectada por “ideas felices” o “presión comercial”.

Y en su organización ¿se analizan los riesgos tecnológicos así, o se gestionan las TIC con el **método ASM (A Salto de Mata)**?



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>

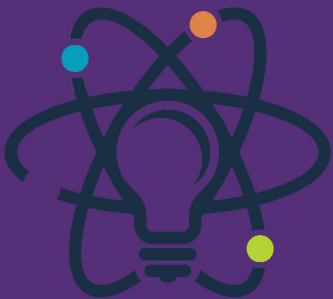
PfM Book

Portfolio

Management

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Nacho Alamillo



Caminando hacia la Cartera Europea de Identidad Digital: llega MiDNI

El 2 de abril se ha publicado en el BOE el Real Decreto 255/2025, de 1 de abril, por el que se regula el Documento Nacional de Identidad, que viene a sustituir al veinteañero Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

Como gran novedad con respecto al régimen jurídico hasta ahora vigente, el Documento Nacional de Identidad consiste en una tarjeta inteligente certificada que permite a la ciudadanía la identificación física mediante la exhibición del documento y la identificación digital, por un procedimiento seguro a través de un dispositivo móvil para acreditar electrónicamente la identidad de las personas, ya sea de manera presencial o remota.

Se trata de una funcionalidad hubiera podido implementarse ya en el antiguo DNI electrónico, dotando al chip de capacidades de autenticación electrónica a distancia, dada la existencia de los estándares al efecto, significativamente UNE-EN 419212 o la colección de especificaciones de BSI para el eIDAS-token, pero que la experiencia ha demostrado de escaso uso en países como Alemania, donde se ha implementado con menor éxito del previsto, sin duda alguna.

Sin embargo, la espera podría haber merecido la pena. Y es que se trata de una iniciativa realmente oportuna, en un momento de verdadera pandemia de fraude en contratación con base en uso de fotocopias de DNIs, así como de lo que parece ser una nueva *jihad* de la Agencia Española de Protección de Datos frente a la exigencia de dichas copias, al menos en aquellos casos en que una ley formal no exija dicha aportación, como sucedería en el caso de las entidades sujetas a la normativa de prevención del blanqueo de capitales.



CONTINÚA EN
PRÓXIMA PÁGINA



Si bien en la tarjeta soporte del DNI se mantienen los certificados cualificados, garantizando la identidad del titular de la clave privada de identificación y firma, permitiendo la generación de la firma electrónica avanzada y cualificada, con plazo de validez se establece en dos años, en el caso de la versión digital del DNI, nos encontramos frente a una infraestructura de identificación electrónica con un dispositivo móvil. Para ello, se establecerá una actuación administrativa automatizada para la obtención de la versión digital del Documento Nacional de Identidad, de manera electrónica, telemática o presencial, teniendo de forma alternativa la misma finalidad que el formato físico para la identificación de las personas.

El funcionamiento de la versión digital consiste en virtualizar el Documento Nacional de Identidad en el dispositivo móvil, a través de una comunicación segura, sin que se comprometa la garantía de la identidad segura que la legislación vigente atribuye al Documento Nacional de Identidad, por lo que se trata de una iniciativa que avanza en el camino hacia el enfoque técnico de la futura cartera europea de identidad digital.

Desde la perspectiva de sus efectos jurídicos, la norma establece que la utilización del Documento Nacional de Identidad en su versión digital tendrá la misma eficacia jurídica a efectos de identificación, por lo que permitirá acreditar la identidad ante las autoridades, sus agentes y funcionarios públicos, así como en las relaciones con las Administraciones Públicas y con el sector privado. Este último colectivo es quizá el que mayor necesidad tenga en estos momentos de adoptar el uso de la versión digital del DNI, como hemos avanzado, si bien disponen de un plazo de doce meses para adoptar las medidas necesarias para el buen funcionamiento de la versión digital del Documento Nacional de Identidad.

A pesar de lo que establece la normativa, al menos en esta primera fase, la versión digital del DNI presenta limitaciones, entre las cuales, que no acredita la identidad a través de internet o de manera presencial sin conexión de datos, que no puede presentarse como documento de viaje electrónico para paso de fronteras, que no acredita la identidad en otros países o que no permite hacer gestiones telemáticas de autenticación y/o firma electrónica.

Se trata, todas ellas, de funcionalidades que podrán incorporarse en un futuro, pero que ciertamente conforman el núcleo de valor de la futura cartera europea de identidad digital a expedir, a más tardar a partir de 24 de diciembre de 2026, en plena alineación con el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, modificado por Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024.

¿Evolucionará esta app para convertirse en la cartera de persona física, o será absorbida por esta? Quizá debamos reclamar, una vez más, el necesario debate acerca de una Ley española de identificación electrónica.



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**



Juan Carlos Muria

“

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

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

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

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

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

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

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

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



CONTINÚA EN
PRÓXIMA PÁGINA

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

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

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

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

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

Finalmente, **la sostenibilidad económica y social** también es clave: existen sistemas de IA que, por su propio diseño, requieren un consumo elevado de recursos. También pueden generar desigualdades que podrían acabar generando no solo un sistema de salud de primera y de segunda, sino unos profesionales de primera y de segunda por un doble motivo: en primer lugar al sustituir los junior por los sistemas de IA se “rompe la tubería” que lleva a los junior a convertirse en sénior ya que no tienen oportunidad de adquirir la



experiencia práctica necesaria, siendo cada vez los profesionales sénior más escasos y cotizados, y en segundo lugar puede ocurrir una erosión de las capacidades clínicas conocida por deskilling, provocando el uso de sistemas de IA la pérdida de habilidad manual o cognitiva de los profesionales. Es justo lo que nos ha sucedido a muchos con el GPS y nuestro sentido de la orientación.

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



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>

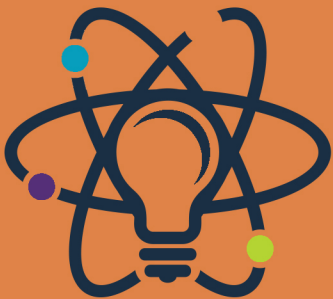
PgM Book

Programme

Management

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE



Ismael Novo

¿Qué debería saber el mundo sobre Ismael Novo antes de seguir leyendo?

Nacionalista Tartesso con raíces Atridas, nací en Ferrol y viví entre Galicia y Murcia hasta los 20 años, cambiando de domicilio por temporadas y sin una cama clara hasta los 33. Siempre fui el gallego en Murcia y el murciano en Galicia. Esa falta de raíces fijas me sirvió para entender pronto que somos personas, no plantas, y que moverse también es una forma de crecer. De dos tierras muy distintas, de contrastes profundos, fue justo en esa dualidad donde encontré la definición de equilibrio.

Crecí en una época sin internet, sin apps, sin chats, sin filtros... De piloto de X-Wing certificado por nadie, a estratega, deportista, detective, príncipe a explorador incansable de castillos y mazmorras resolviendo enigmas con un pollo de goma en el inventario de la vida. Abusé del cine la música y los videojuegos, con sus grandes historias, hasta que mi propia vida se volvió más emocionante que cualquier fantasía que pudiera cargar un dispositivo electrónico.

Lector voraz de Dune y otras fantasías sobre lo que se nos vendría encima, aprendí pronto que la gente más importante del mundo usa software a medida desde hace más de lo que imaginamos. Ahora veo desde un sillón privilegiado que la inteligencia artificial es solo una nueva forma de afilar ese mismo cuchillo.

Una época universitaria demasiado intensa me abrió las puertas de Babson College, la universidad número uno del mundo en emprendimiento. Así que para ganarme la vida terminé integrando lo que parecía imposible: el rigor de la consultoría en una gran empresa con el hambre del emprendedor.

Defensor de una oficina virtual que aún no ha llegado del todo y nómada digital antes de que se popularizara el término; decido asentarme en Murcia por una sencilla cuestión de calidad de vida. Busqué 1001 razones para irme y encontré

1001 para quedarme. Teletrabajo para Europa por las mañanas y las américas por las tardes así que complicado encerrarme en una oficina.

Actual director de #MurciaTIP y del proyecto #PowerUS. Aprendí a tiempo que la realidad puede ser más increíble que cualquier fantasía, si estás dispuesto a ir al fin del mundo en busca de respuestas... Ya fui... Y encontré al final del camino un bonito árbol blanco. También había un mono, pero eso es otra historia.

¿Qué logros han dejado huella real y no solo un titular?

Ganar el premio 'Importantes' de La Opinión en el año 2008 fue el primer aviso de que venían curvas. No entendía como alguien como yo pudiera estar al lado de investigadores o deportistas de élite de mi zona. No sentí que hacía nada especial hasta que tuve por primera vez a cientos de personas delante aplaudiendo de las cuales solo me interesaban dos, las sonrisas de unos padres orgullosos inmortalizadas en el periódico del día siguiente.

El segundo gran hito en mi vida fue conseguir cuatro líneas de texto en la disposición adicional novena de la "Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización": Miniempresa o empresa de estudiantes. Dicen que en la vida hay dos cosas que nunca hay que saber cómo se hacen, las leyes y las salchichas. Pues bien, soy de esos afortunados que ha aprendido como se hacen ambas cosas y confirmo que lo peor, las leyes.

Los años pasaron y llegaron muchos más, he sido de esos pocos afortunados que han podido hablar tanto en el congreso de los diputados como arrancar un aplauso no preparado en un evento político



**CONTINÚA EN
PRÓXIMA PÁGINA**





REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Nuestro invitado a #TYSC



#TYSC / PÁG. 26

delante de mil personas. Ahora bien, la fundación de #MurciaTIP y los proyectos que están saliendo de aquí son la huella más real que está empezando a cambiar todo desde donde realmente importa.

¿Qué errores personales o profesionales te han enseñado más?

A nivel personal, pensar que mucha gente traumada quiere salir de la mierda. Hay muchísima gente que es feliz en su pocilga, revolcándose en sus heces y quejándose del olor cada día sin la más mínima intención de prosperar. Han tirado ya muchos años diciendo que nadie les da una oportunidad, que lo han tenido más difícil que nadie y el universo está en su contra. Campeones de la excusa para todo que el ofrecerles una ducha y un oficio es sacarlos de su zona de confort, así como generar un problema serio en su narrativa.

A nivel profesional, en todo tipo de organizaciones — ya sean sociales, lucrativas o formativas— me costó entender que no todo se puede dividir entre buenos y malos. Cuanto más grande es una organización, más guerras internas se producen: corrientes, egos y bandos que se repiten en todos los entornos. Comprender que estos tejidos cambian de piel sin cambiar de alma fue una de las lecciones más duras. Porque al final, lo que perdura no son los nombres ni los cargos, sino las inercias que debemos aprender a aprovechar... o romper.

¿Cómo empezó tu relación con la tecnología?

Soy orgulloso hijo de un padre militar que arriesgaba su vida cada día para que todos pudiéramos dormir con tranquilidad. Esta paz traía una gran contrapartida, una gran ausencia cubierta por un viejo 286 que desde mi más tierna infancia fue maestro y compañero. Asimov estaba en lo cierto, un joven curioso e incluso únicamente interesado en el ocio, podría aprender matemáticas o letras por accidente sin darse cuenta.

La respuesta a si el exceso de pantallas en un niño es bueno o malo es muy simple: depende de lo que esté haciendo, no del tiempo que pase frente a ellas. Programar a una edad tan temprana modeló mi mente de forma distinta, porque el entrenamiento, en aquel entonces, pasaba muchas veces por editar o modificar cosas sin saber muy bien cómo, solo con curiosidad, prueba y error... y muchas líneas de código a medio entender o tocar hardware muchísimo más que ahora.

Aprendí una gran base de mi esencia de un internet de otro tiempo donde era más puro, cuando la red de

redes explotó sin normas, sin leyes ni villanos, todo era territorio virgen por descubrir. Nadie buscaba tu dinero, no había ni cómo pagar. Nadie perseguía tus clics, porque no existía forma de monetizarlos. Si buscabas algo, lo encontrabas. Y si hablabas con alguien, la ilusión de conectar eclipsaba cualquier mala intención con muy pocas excepciones.

Aunque he conocido sus proezas tarde, la mano invisible de Maria Montessori me empujaba en las sombras, así como recientemente me mandó a una de sus emisarias para avisarme de que todo ha merecido la pena.

¿Qué obsesión guía hoy tu forma de trabajar?

Nunca debemos olvidar que: "Los años que tenemos, son en realidad, los años que ya no tenemos" puesto que los únicos años que realmente tenemos son los que te faltan por vivir. Desde que programar forma parte de mi vida, entendí que, si una empresa gana valor ahorrando tiempo o dinero, yo también podía aplicarlo a nivel personal. Cada minuto que salvamos se puede transformar acumulativamente en años de vida, porque automatizando un minuto, cabe otro minuto encima, el proceso es infinito. Se pueden hacer cada vez más cosas con cada vez menos tiempo si nos tomamos en serio las posibilidades tecnológicas que tiene cualquier ciudadano en su propia mano con un simple teléfono.

Esta obsesión por la productividad me llevó a encontrar poesía en la codificación informática, disfrutando en modelar la métrica, las palabras elegidas o la cantidad de espacios a utilizar... Cada lenguaje aprendido me llevaba a uno más eficiente y optimizado, terminando de asentarme en las últimas tendencias de LowCode y NoCode para hacer mucho más, con mucho menos. Un área complicada, ya que mucho ignorante habla de que solo "arrastramos cajitas" sin entender que la alternativa es repetir las mismas letras una y otra vez, y que eso no aporta valor.

Conozco demasiados técnicos de élite que sufren con la amenaza de "que sale el camión" o que si no hacen algo en el tiempo estipulado "mataremos un gatito". No hay mayor obsesión ahora mismo que ser refugio y conector de personas nobles con ganas de hacer de este mundo un lugar mejor.



**CONTINÚA EN
PRÓXIMA PÁGINA**

¿Qué hábito o forma de pensar te diferencia de los demás?

Soy de la escuela de Larry Bird. El tipo no solo te decía lo que iba a hacer... lo hacía en tu cara justo después. No hay nada tan placentero y que vuelva más loco a tus enemigos que ser transparente con tus planes... ¡Se vuelven locos buscando tus supuestas intenciones reales! Digamos que he aplicado este estilo tanto a la programación como a la ejecución de proyectos y los resultados están siendo muy buenos.

Sumo a lo anterior la constancia de Dashrath Manjhi, "The Mountain Man". Su esposa murió al no poder recibir atención médica por tener que rodear una montaña por un desvío de 50km para llegar al hospital. En 1960 canalizó su rabia con un martillo y cincel durante 22 años para acabar con la montaña y crear un camino directo de 5km. Cambió la vida de generaciones como la cambiará la sede social que queremos construir para nuestra plataforma.

¿Cómo empezó tu historia en los eventos y asociaciones?

En el mundo asociativo siempre fui de los que se apuntaban a todo. Televisión local, fútbol, pintura, teatro, la revista del instituto... hasta el doble salto mortal que supuso el Colegio Mayor Azarbe, mi preparación gracias a un gran director del cual fui mano derecha 4 años que sirvieron como base para liderar la Red Internacional Junior Empresa desde CEJE más tarde.

Lo de los eventos, en cambio, fue más inesperado y divertido. Accedí al primero relevante en una época de mi vida en la que no tenía ni un euro. Un compañero me subió a un avión cuando yo pensaba que era una broma (menos mal que hice la maleta para seguirle el juego). Aterrizamos en Barcelona y yo con un mísero euro en la cartera... Así de tonto fue como viví tres de los días más intensos de mi vida. Al volver, llevaba dos euros encima; me encontré uno en el suelo del parque Güell.

Pero el conocimiento para afrontar todo esto llegó de un viejo heavy del lugar, que me entregó la llave mística de un viejo despacho olvidado. Cientos de papeles cubiertos de polvo guardaban la historia de algo grande. Por el camino, el Embajador Jose Luis Pardos me demostró que con 89 años se puede seguir pensando más rápido que muchos veinteañeros, que la diplomacia también puede ser rebeldía, y que el verdadero legado no está en los títulos, sino en saber encender fuegos en otras mentes.

¿Qué áreas urgentes ves en la Gestión y el Gobierno de organizaciones?

Llegar más allá de la formación y entrar, de una vez, en la educación real. Vivir en el estrato organizacional que he elegido actualmente – ni cerca del cielo ni pegado al infierno– me ha permitido ver con claridad el equilibrio (o el caos) entre quienes más duro trabajan y quienes más duro gestionan.

Del mismo modo que eliminaron la cultura financiera de la enseñanza básica para tenernos esclavizados de por vida, han dejado fuera del sistema educativo todo lo que realmente ayudaría a vivir mejor. Al final, todos tenemos una empresa... o trabajamos para una y conocer gestión y generación de normas, procedimientos y protocolos sirve tanto para el mundo personal como el profesional. Una familia es sin lugar a duda el negocio que mejor debe de funcionar en tu vida.

Más educación global sobre roles, responsabilidades, expectativas, procesos y todas esas cuestiones que nos vendieron tan mal. Estas temáticas que parecen aburridas son, en realidad, las claves para ganar más dinero, tomar mejores decisiones y vivir con más libertad en cualquier aspecto de la vida. Lo que no sabes te puede matar.

¿Qué le dirías a alguien que aún no ve el valor práctico de la automatización o la IA en su día a día?

Que busquen a la persona más mayor de su familia y se sienten con ella una única tarde a escuchar. Que asimilen como hace 50 años casi era necesario ser mecánico para conducir o como era el mundo del campo en aquellos tiempos. Que hablen de como el tractor reemplazó al burro y de cómo la lavadora cambió la vida de millones de familias. Que investiguen sobre serenos, vendedores callejeros de hielo, afinadores de piano ambulantes y muchas más profesiones perdidas.



**CONTINÚA EN
PRÓXIMA PÁGINA**





Nuestro invitado a #TYS

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



Que nuestra historia viva les cuente de primera mano, lo que significó ya no el agua caliente sino el agua “corriente” en un domicilio. Estamos en continua evolución y así como los consultores existimos desde que el oráculo de Delfos estaba en pie; seguimos aquí. Desciframos el presente y preparamos a quien quiera escuchar para un futuro que muchos aún no son conscientes de que ha llegado. Cualquier tecnología suficientemente avanzada es indistinguible de la magia y para demasiada gente la tecnología empieza a ser brujería heráldica.

¿Qué está por venir en tu Asociación?

Desde #MurciaTIP y mediante el proyecto #PowerUS, a parte de un festival tecnológico y cultural anual vamos a construir en paralelo y como sede “El palacio de congresos más épico del universo”. Hemos elegido la forma de un castillo que vive dentro de la imaginación de todo niño de los 80 y reconocible por siempre para cualquier generación por lo característico que es. Alrededor de él estamos formando una familia que viajará unida a lo Charli y los Argonautas en un “Barco de Colegas” con una misión épica y toda la ilusión del mundo. Como solemos decir: Estaba escrito, en el molonito. Un molonito del Mar Menor que siendo una laguna privilegiada a nivel mundial es donde ejecutaremos nuestra RSC lo antes posible.

En las asociaciones es MUY importante un gran evento anual, este tiene que servir tanto de escaparte del trabajo realizado como de punto de evaluación y decisión sobre el futuro de la organización. Así como es una herramienta profundamente motivadora para los voluntarios implicados, más aún cuando dicho evento tiene un impacto real en el tejido de nuestra sociedad.

¿Qué se perdería alguien que no asista a vuestro evento anual?

Simple. La fusión perfecta entre formación, ocio y negocio. Habrá quien solo vendrá por la parte cultural que es bien diferente y entretenida. Otros simplemente aprovecharán el tener tan cerca

a técnicos premiados por Microsoft del más alto nivel. Por supuesto, dispuestos a compartir sin filtros lo que normalmente se puede tardar más de una vida en aprender. ¿Negocio? Claro que sí. ¿Acaso no surgirán cientos de nuevas locuras de concentrar en un único punto a tanto talento? Eso tiene que traducirse en oportunidades para todos los niveles.

¿Uno habla igual cuando le graban que cuando no? ¡NO! La única forma tener charlas auténticas es no grabarlas y eso es marca de la casa. Antiguamente usábamos los ordenadores para huir del mundo real... Ahora queremos usar el mundo real para huir del virtual puesto que, tecnología no siempre significa pantallas.

¿Cuál es tu última frase de guerra?

Fabricamos tiempo... ¡Se acabaron las excusas! Si de verdad no quieres que te moleste o cuente contigo por favor, dímelo sin rodeos, no me pongas como excusa a ese hijo al que no haces caso o dejes mal a tu pareja diciendo que no te deja hacer lo que supuestamente te hace feliz. Di directamente que no quieres, di que eres más feliz sin hacer nada, di que cuando seas viejo te sentirás orgulloso de todas esas tardes perdidas.

El sentido de la vida, esa pregunta mágica, de donde venimos y a donde vamos tiene una respuesta difícil PERO una certeza clara: La vida va de aprender a morir.

Es importante compartir ese camino con una persona mágica, de esas que usan capa invisible, te miran como si fueras su hechizo favorito, y te mandan señales rojas cuando menos lo esperas, aunque sea con una lechuza azul en plena noche. Porque al final, la verdadera magia no está en los libros, está en quien camina a tu lado cuando el castillo tiembla.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de Doble
Certificación en:**

Gobierno y Gestión de la Inteligencia Artificial

**ISO 38507 Leader
ISO 42001 Leader**

Docente:

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
- Certificación: ISO 38507 Leader
- Certificación: ISO 42001 Leader
- Aforo: Limitado 15 Alumnos
- Acceso: Solicitud de admisión

MidMgmt®

MPPM®

MGEIT®

eGob®

Próxima Convocatoria en Directo

MAYO 2025

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>

**Plazas
limitadas**



Marlon Molina



Las criptomonedas vuelven a ser tendencia

Las criptomonedas vuelven a ocupar un porcentaje de las noticias principalmente motivados por el anuncio del euro digital, y robos que se han hecho famosos. Es inevitable que las criptomonedas sigan haciendo hueco en el mercado. Probablemente en cinco años más del 90% de la ciudadanía tenga un wallet crypto instalado en el móvil, lo quiera o no.

En este momento las plataformas y la tecnología enfrenta al menos cuatro retos: nuevos modelos para la tecnología, el euro digital, robos en wallets, y futuros robos que se están planificando actualmente.

Nuevos modelos para la tecnología

Blockchain enfrentó desde su inicio una fuerte resistencia debida al enorme consumo energético, y enfrentará cada vez más la crítica por los costes de las transacciones. Cuando El Salvador adoptó Bitcoin como moneda, la transacción para comprar una fruta en el mercado podía resultar más cara que la fruta puesta en manos del consumidor, aunque lo peor podría estar en el tiempo, ya que el vendedor de la fruta necesitaría hasta veinte minutos para validar el pago.

Por suerte se trata de tecnología, y puede rediseñarse. Actualmente se experimenta y se investigan nuevos desarrollos de modelos en criptomonedas, como las Layer 2 solutions, cadenas laterales (sidechains) y protocolos de consenso alternativos como Proof of Stake (PoS) y Proof of History (PoH). Estas innovaciones buscan resolver los problemas de escalabilidad, eficiencia energética y tiempos de transacción que afectan a redes tradicionales como Bitcoin y Ethereum. A nivel de ciberseguridad, estos modelos presentan nuevos desafíos ya que cada nueva capa tecnológica puede introducir vulnerabilidades que aún no han sido plenamente auditadas ni comprendidas por la comunidad.

La descentralización también está encontrando nuevas formas con los ecosistemas DeFi (Finanzas Descentralizadas), las DAO (Organizaciones Autónomas Descentralizadas) y los contratos inteligentes más complejos. Estas herramientas brindan mayor flexibilidad y autonomía, también amplían la superficie de ataque. Un error en el código de un contrato inteligente o una mala implementación de un protocolo puede permitir ataques muy caros, como los que ya se han visto en varias plataformas DeFi.

El Euro digital

Para mí como si se tratara de un mal sueño, una pesadilla para la privacidad. Dicho en versión cinematográfica: de los creadores del fallido reglamento de protección de datos, próximamente en la pantalla “el euro digital”, la herramienta final para el control de la privacidad y las voluntades.

Debemos recordar que la economía y el pago es herramienta para motivar la voluntad, así funciona un descuento persuadiendo al comprador, y así mismo trabaja un impuesto, alejando al comprador.

El euro digital pretende crear una versión digital de la moneda fiduciaria europea con el objetivo de facilitar pagos más rápidos, seguros y controlados, tanto dentro como fuera de la eurozona.



CONTINÚA EN
PRÓXIMA PÁGINA

Desde una perspectiva de ciberseguridad, el reto es monumental: asegurar que esta nueva forma de dinero no pueda ser falsificada, robada o manipulada, al mismo tiempo que se protegen los datos personales de millones de ciudadanos europeos, mientras se evita que políticos sin escrúpulos espíen a sus anchas.

No tengo dudas en que el euro digital traerá una nueva ola de ataques por parte de grupos criminales y estados hostiles. Al tratarse de una infraestructura crítica, los posibles vectores de ataque incluyen desde intentos de suplantación de identidad hasta sabotajes en la cadena de bloques o ataques coordinados a wallets digitales de los ciudadanos. El desconocimiento de una herramienta tan sofisticada empezará con una cantidad nunca vista de estafas a personas poco conocedoras, víctimas no solo de los ciberdelincuentes, también de los gobiernos que cambien la moneda física. Este contexto exige no solo tecnologías de cifrado avanzadas, sino también una gobernanza robusta y una arquitectura descentralizada que limite los puntos únicos de fallo, algo poco conciliable con los modelos centralizados de los bancos centrales.

Robos actuales en las wallets

En los últimos meses se han conocido un número de atracos a conocidos magnates de las criptomonedas. Cada uno de los robos podría inspirar el guion de una película. También se han conocido asesinatos de personas para robar el teléfono, es decir, la llave de sus gordas wallets digitales.

La historia de la humanidad no había registrado ricos que salieran de paseo o de viaje cargando toda su fortuna, hasta ahora. En el teléfono móvil algunos tienen la llave a una cantidad ingente de criptomonedas, todo en un solo dispositivo, y un dispositivo con poco misterio. En los meses que lleva 2025, hemos podido leer historias donde los delincuentes van mucho más allá del phishing o la instalación de software espía, han irrumpido en las viviendas de personas que se conoce tienen cantidades de criptomonedas, y les obligan a transferirlas, ya os podéis imaginar que después del traspaso no hay nada que hacer. En un entorno sin intermediarios, como el de las criptomonedas, la seguridad del wallet es equivalente a la seguridad del banco personal. Este es también un punto a considerar en el euro digital.

Ataques futuros

Algunos gobiernos a nivel institucional están almacenando las cadenas de bloques, cifradas con la esperanza de poder abrirlas en un futuro no muy lejano con la ayuda de



la computación cuántica. Es una gran estrategia por parte de estos países, y una clara falta de visión por occidente, que permite sacar nodos y replicarlos fuera de las fronteras de confianza. Quizá la plataforma de Bitcoin o Ethereum no hayan tenido alternativas, pero iniciativas como LACChain son un ejemplo de que el buenismo (falta de visión, o sobrada ambición en el presente) nos puede dejar en manos de los atacantes.

Hoy es monitorización, hoy es un problema geopolítico, mañana será un problema económico y social. Esta práctica por parte de gobiernos no tan amigos les permite estudiar patrones de comportamiento económico, realizar análisis forenses y, en el peor de los casos, identificar puntos débiles para explotar en el futuro. En una situación de conflicto cibernético, acceder a registros históricos de transacciones podría ser una forma de identificar objetivos críticos o incluso sabotear infraestructuras relacionadas con criptomonedas.

El almacenamiento masivo de bloques es una herramienta de inteligencia a largo plazo. Se estima que en los últimos 10 años, entre un 60% y 70% de los bitcoins en circulación han cambiado de manos, visto desde otro ángulo, al menos el 30% no se ha "movido", lo cual también permite pensar que descifrar la cadena en los próximos 10 años podría dar acceso digamos al 20% de los bitcoins, al precio actual representa unos 293 mil millones.



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/>

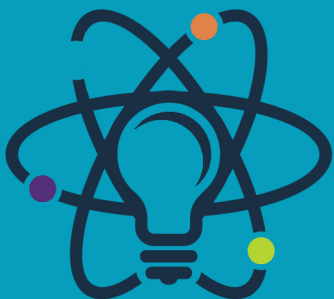
PjM Book

Project

Management

Body of Knowledge

P4MGO!®



P4MGO!

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



Ricard Martínez Martínez

Signal leaks tan lejos y a la vez tan cerca

El caso conocido como Signalgate o Signal leaks supone una de las crisis de seguridad nacional más graves para el Gobierno de EE. UU. De acuerdo con la información publicada entre el 11 y el 15 de marzo de 2025, altos funcionarios de seguridad nacional, incluyendo al vicepresidente, el secretario de Defensa, la directora de Inteligencia Nacional y el director de la CIA, mantuvieron conversaciones en un grupo de Signal para coordinar ataques militares contra los hutíes en Yemen. Por error, el asesor de seguridad nacional Michael Waltz añadió a Jeffrey Goldberg, editor jefe de The Atlantic, al grupo. Goldberg tuvo acceso a detalles sensibles y posteriormente publicó parte de las conversaciones.

Posteriormente se reveló por The New York Times que el secretario de Defensa compartió información militar altamente sensible sobre los bombardeos a los hutíes en Yemen en un chat privado de Signal que incluía a su esposa, su hermano y su abogado personal, además de otros asesores y colaboradores del Pentágono. Se ha conocido que además utilizó su teléfono personal para crear y gestionar un grupo de Signal donde compartió los horarios de vuelo y detalles operativos de los ataques del 15 de marzo, repitiendo así la conducta que ya había provocado el escándalo original del Signalgate. Este grupo privado no estaba limitado a personal autorizado para manejar información clasificada, lo que incrementaba el riesgo de filtraciones accidentales o deliberadas.

Signal es una app cifrada pero no autorizada para compartir material clasificado en EE. UU. cuyo funcionamiento presenta además problemas de auditabilidad ya que la función de autodestrucción de mensajes dificultó la preservación de registros oficiales y generó sospechas de destrucción ilegal de documentos federales. Por otra parte, su uso en dispositivos no gubernamentales y sin las protecciones adecuadas abre la puerta a posibles interceptaciones por parte de actores hostiles.

El incidente evidencia una cultura de informalidad y ausencia de protocolos claros para el manejo de información sensible en la Administración, así como una posible falta de respeto a las obligaciones de seguridad.



CONTINÚA EN
PRÓXIMA PÁGINA



Por otra parte, la inclusión de familiares y asesores sin justificación clara en la cadena de información sensible multiplica las posibilidades de filtración y pone en duda los criterios de seguridad interna del Departamento de Defensa. Por si fuera poco, el uso de dispositivos personales y apps no seguras al margen de los canales oficiales y sin las protecciones requeridas para información clasificada, expone a vulnerabilidades técnicas y a posibles hackeos.

Vistos los hechos, parece bastante evidente que las políticas de seguridad del Gobierno norteamericano en esta materia dejan bastante que desear y podría presumirse que las directrices de seguridad que se imponen a cada uno de los funcionarios públicos no aplican a los niveles de alta responsabilidad política o al menos no se han comunicado de manera eficiente y clara.

Esta no parece ser una cuestión exclusiva de los EE. UU. Basta con consultar la hemeroteca española para verificar que no existe ni un solo asunto judicializado y relacionado con la política en la que no exista alguna referencia a un chat en WhatsApp. Y esto es ciertamente sorprendente, ya que de acuerdo con el vigente esquema Nacional de Seguridad y las directrices que el centro criptológico nacional pública en materia de seguridad en el uso de terminales móviles, las administraciones y los órganos de gobierno de alto nivel deberían excluir de raíz el uso de este tipo de mensajerías.

En primer lugar, porque de una parte es necesario tener una relación contractual con el proveedor del servicio y asegurarse de que no exista ningún riesgo para la seguridad nacional y los derechos de las personas. No es ocioso recordar que la compañía META se encuentra sujeta a la ley norteamericana Foreign Intelligence Surveillance Act (FISA) y en la investigación penal ordinaria a la Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

En segundo lugar, porque en no pocas ocasiones se utiliza un terminal privado o susceptible de ser utilizado fuera de las instalaciones propias de la Administración, lo que los hace particularmente

vulnerables. En el primer caso, usar smartphones o números telefónicos privados en este tipo de contextos puede vulnerar el derecho fundamental a la protección de datos del titular del terminal cuando se le impone este tipo de uso. En ambos casos, el empleo de mensajerías privadas para usos propios de dirección pública profesional, o para tareas propias de la Administración puede suponer incumplimientos graves de los principios del RGPD, del Esquema Nacional de Seguridad o de directrices de seguridad nacional.

Por otra parte, existe una cuestión evidente ya que este tipo de aplicaciones móviles se ha diseñado y programado para funcionar en sistemas operativos propietarios, cuyas políticas de actualización dependen de terceros. Además, ocupan una posición de dominio de mercado que implica el control de corporaciones muy específicas. Por tanto, no parece una buena decisión utilizar productos de mercado en entornos de alta seguridad que los hace altamente vulnerables a variables no sólo tecnológicas, sino también a un escenario geopolítico cambiante como demuestran cada día los titulares de prensa.

Algo parece estar fallando en el diseño e implementación de la seguridad en los niveles de alta dirección. Que se invoque el borrado de conversaciones como una directriz de seguridad y buenas prácticas definida por la persona delegada de protección de datos y las directrices internas no es ninguna buena noticia. Sencillamente, porque esta es una medida que mitiga el riesgo. Y hay algo de sentido común: hay que preguntarse si es posible reducirlo o eliminarlo. Y uno tiene la impresión de que esa reducción o eliminación pasa por perder el temor reverencial, formar a los altos cargos y exigirles responsabilidad. Implica plantearse la posibilidad de disponer de terminales seguros con sistemas operativos propietarios del propio Gobierno o la Administración. Y finalmente supone que el recurso a mensajerías privadas debería limitarse a desarrollos propios con un alto nivel de seguridad. Bueno, a esto y a mirar quien se sienta detrás del usuario en el vagón de tren del AVE.



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**



La creAltividad del futuro

En el año 2034, el panorama de la creatividad ha experimentado una transformación radical debido a los avances tecnológicos nunca antes empelados en la creación artística. La inteligencia artificial, la realidad virtual y aumentada, el metaverso, los BCE y otras innovaciones han redefinido la forma en que creamos, consumimos y experimentamos el arte, la música, el cine y la literatura.

LA INTELIGENCIA ARTIFICIAL COMO MUSA Y COLABORADORA

La inteligencia artificial (IA) se ha convertido en una herramienta fundamental para artistas, músicos, cineastas y escritores. Los sistemas de IA generativa, que comenzaron a ganar prominencia en la década de 2020 con herramientas como DALL-E, Sora y GPT, han evolucionado hasta convertirse en colaboradores creativos sofisticados.

Otro de los cambios radicales ha sido el canal por el que se disfruta del arte, la música, el cine y la literatura. Tradicionalmente el oído y la vista eran los canales o sensores que permitían a nuestro cerebro disfrutar de ellos. Gracias a los BCE (Interface cerebro computadora), ya no es necesario usar dispositivos para oír o disfrutar una canción, un video o una obra pictórica. Mediante los dispositivos BCE accedemos directamente a la información, que está conectada a nuestro cerebro, pudiendo así oír y ver con una calidad antes desconocida.

EL NUEVO ARTE VISUAL

En el ámbito de las artes visuales, la IA ha revolucionado el proceso creativo. Los artistas utilizan algoritmos avanzados para generar obras originales, explorar nuevos estilos y experimentar con formas que desafían la imaginación humana.

Herramientas de IA como "NeuralCanvas" permiten a los artistas describir conceptos abstractos y ver cómo la IA los interpreta visualmente, creando obras que fusionan la visión humana con la capacidad de procesamiento de la máquina.

La galería virtual *tokenizada* "MetArtistry", lanzada en 2029, se ha convertido en un espacio de exhibición de renombre para obras creadas en colaboración entre humanos e IA. Estas exposiciones desafían las nociones tradicionales de autoría y creatividad, generando debates sobre la naturaleza del arte en la era digital.

LA MÚSICA Y EL VIDEO

En la industria musical, la IA ha transformado tanto la composición como la producción. Los compositores utilizan algoritmos para generar melodías, armonías y ritmos, que luego refinan y adaptan a sus visiones artísticas. El álbum "Synthetic Symphony", lanzado en 2031 por el artista conocido como NeuroBeats, fue el primer álbum en alcanzar el número uno en las listas de música en streaming compuesto enteramente por una IA y masterizado por humano.

Los sistemas de IA también han revolucionado la personalización musical. Plataformas de streaming como "MoodMelody" utilizan algoritmos avanzados para crear listas de reproducción dinámicas que se adaptan en tiempo real al estado de ánimo y las actividades del oyente, basándose en datos biométricos recolectados por el BCE y ambientales.

EN la industria cinematográfica los guionistas utilizan asistentes de IA para desarrollar tramas dinámicas, diálogos y personajes, mientras que los directores emplean simulaciones de IA para visualizar



escenas complejas antes de crearlas. Ya no se filma, las imágenes se generan mediante complejos sistemas CGI (Imágenes Generadas por Computadora) combinados con IA. La película "Quantum Dreams", estrenada en 2033, fue pionera en utilizar escenarios y actores completamente generados por IA, marcando un hito en la integración de IA en la producción cinematográfica.

Incluso existe todo un catálogo digital de actores de todos los tiempos que pueden ser empleados en las producciones de video. Los actores y sus herederos reciben royalties por el uso de su imagen. Incluso ya existen estrellas de cine totalmente digitales que atraen a gran número de seguidores.

Uno de los aspectos que ha permitido la tecnología ha sido la generación de producciones de video dinámicas, adaptadas a la persona, a sus sentimientos. Son películas o series "vivas". Al interactuar con nuestro BCE las películas tienen un algoritmo embebido que identifica nuestros sentimientos y preferencias y adaptan la trama en tiempo real. Así la misma película o serie se desarrolla de manera diferente según las preferencias o sentimientos de la persona que la está disfrutando.

LA LITERATURA INTERACTIVA

En el mundo literario, los autores utilizan sistemas de IA para generar ideas, desarrollar personajes y hasta escribir borradores iniciales de capítulos. La novela "The Algorithm's Muse", publicada en 2032, fue escrita íntegramente por un sistema de IA, convirtiéndose en un best-seller y generando debates sobre la autenticidad y la creatividad en la era digital.

Las editoriales emplean IA para analizar tendencias del mercado, predecir el éxito potencial de manuscritos y personalizar recomendaciones para lectores, e incluso para hacer que sus escritores virtuales basados en AI generen contenidos que sean tendencia. La plataforma "NeuralNarrative" permite a los lectores interactuar con historias dinámicas que se adaptan a sus preferencias y elecciones en tiempo real, difuminando las líneas entre literatura y juego interactivo.



**CONTINÚA EN
PRÓXIMA PÁGINA**



EL METAVERSO: UN NUEVO LIENZO PARA LA CREATIVIDAD

El metaverso, un concepto que ganó tracción en la década de 2020, se ha convertido en una plataforma crucial para la expresión artística y el consumo de contenido cultural en 2034. Este espacio virtual inmersivo e integrado con nuestro BCE ha redefinido cómo experimentamos el arte, la música, el cine y la literatura.

GALERÍAS Y MUSEOS VIRTUALES

Los museos y galerías virtuales en el metaverso ofrecen experiencias inmersivas que trascienden las limitaciones físicas. La Galería Infinita, inaugurada en 2030, presenta exposiciones que desafían las leyes de la física, permitiendo a los visitantes interactuar con obras de arte tridimensionales y dinámicas. Los artistas humanos o basados en IA crean piezas específicamente para este medio, explorando conceptos que serían imposibles de realizar en el mundo físico.

CONCIERTOS Y PERFORMANCES VIRTUALES

Los conciertos en el metaverso se han convertido en eventos espectaculares que fusionan música, arte visual y experiencias interactivas. Podemos estar a la vez en nuestro salón de casa disfrutando de un concierto en una sala virtual con miles de personas disfrutando experiencias únicas y personalizadas para cada concierto.

LA BIBLIOTECA DE AI-LEJANDRÍA

La biblioteca de AI-lejandria, se creó para recoger en una gran biblioteca virtual todo el conocimiento disponible, y va siendo alimentada en tiempo real por los millones de publicaciones que se realizan diariamente. Los contenidos son escudriñados por diferentes IA que lo clasifican en opiniones, realidades

contrastadas, novelas de ficción, ensayos, etc. Su objetivo es rechazar contenidos, argumentos o citas falsas. Por otro lado, los idiomas ya no son un problema ya que directamente se genera la traducción según nuestra necesidad. Nuestro BCE es capaz de identificar qué información o lectura se necesita y como se quiere consumir, en modelo lectura, audio o visual.

EL FUTURO DE LA CREATIVIDAD

En 2034, la creatividad se encuentra en un punto de inflexión, donde la tecnología no solo facilita la creación y distribución de arte, música, cine y literatura, sino que también redefine fundamentalmente lo que significa ser creativo. La fusión de la inteligencia humana con la artificial está dando lugar a formas de expresión previamente inimaginables, mientras que el metaverso conectado a nuestros BCE ofrece nuevos espacios para la experimentación y la experiencia artística.

A medida que avanzamos, el desafío será equilibrar la innovación tecnológica con los valores humanos fundamentales que han impulsado la creatividad a lo largo de la historia. La autenticidad, la emoción y la conexión humana seguirán siendo cruciales, incluso cuando exploramos nuevas fronteras digitales. Será crucial navegar cuidadosamente los desafíos éticos y sociales que surgen, asegurando que la tecnología amplíe y enriquezca la creatividad humana en lugar de reemplazarla.

En última instancia, el arte, la música, el cine y la literatura del 2034 reflejan una sociedad en la encrucijada entre lo humano y lo digital, desafiándonos a redefinir nuestra comprensión de la creatividad, la autenticidad y la experiencia artística en la era de la inteligencia artificial y los mundos virtuales.



MARCOS NAVARRO ALCARAZ

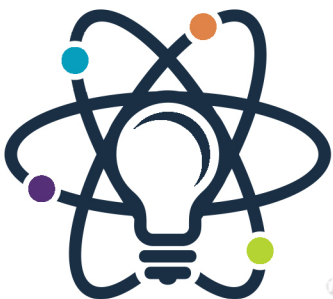
Consultor experto en Tecnologías de la información y ha sido ejecutivo de TI en varias compañías multinacionales. Ahora es experto en Outsourcing de TI, Robots y Autoamización y es profesor universitario y en escuelas de negocio.

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



CiberseguridadAI

La seguridad siempre ha sido importante, y no es en vano que llevamos años hablando del Esquema Nacional de Seguridad (ENS). *Next level*. En la era de la inteligencia artificial (IA, AI en inglés, de ahí la palabra que da título), la ciberseguridad se ha convertido en un pilar fundamental para garantizar el funcionamiento eficiente y seguro de un nuevo funcionamiento que se basa sobre todo en los datos, y en el que estos se pueden ver comprometidos. Ni que decir tiene que las instituciones públicas manejan grandes volúmenes de datos sensibles, desde información personal de los ciudadanos hasta documentos estratégicos o simplemente protegidos o *protegibles* por su carácter confidencial. Por ello, la protección contra amenazas cibernéticas no es solo una necesidad técnica, sino una responsabilidad ética y política que impacta directamente en la confianza de la sociedad respecto a lo público. Esta necesidad se ha visto multiplicada por nuestra dependencia de los datos y, muy pronto, de la propia IA.

Es un hecho que las administraciones públicas son objetivos atractivos para los ciberdelincuentes debido a la naturaleza crítica de la información que custodian. Datos como registros fiscales, historiales médicos, información electoral o los datos de los usuarios de servicios públicos de todo tipo son un botín codiciado tanto para actores maliciosos individuales como para organizaciones criminales, e incluso son objeto de ataques patrocinados por otros estados en esta nueva “guerra fría”. Un solo incidente puede tener consecuencias devastadoras: desde la interrupción de servicios esenciales hasta la pérdida de credibilidad institucional. Y esto no es una advertencia, es un hecho. En los últimos años, hemos sido testigos de ataques *ransomware* que han paralizado ayuntamientos, filtraciones de datos que han expuesto a millones de ciudadanos y sofisticados intentos de manipulación electoral a través de campañas de desinformación digital. Estos eventos subrayan la urgencia de fortalecer las defensas cibernéticas en el sector público.

Ante tal amenaza, animamos a adoptar un rol activo. La implementación de medidas de ciberseguridad en la administración enfrenta retos únicos. En primer lugar, muchas instituciones operan con sistemas heredados (*legacy systems*) que, aunque funcionales en su momento, no fueron diseñados para resistir las amenazas actuales. Incluso el propio ENS ha debido ser revisado varias veces.



CONTINÚA EN
PRÓXIMA PÁGINA

“

**Los amateurs
hackean sistemas,
los profesionales
hackean personas**

Bruce Shneier



Actualizar estos sistemas implica costes elevados y una coordinación compleja entre administraciones y diferentes servicios de una misma administración, lo que a menudo dificulta esta labor. Además, la burocracia inherente a las estructuras públicas puede ralentizar la adopción de las tecnologías más modernas y la respuesta ante incidentes como los descritos, dos procesos que deberían abordarse simultáneamente. La falta de personal especializado en ciberseguridad es otro obstáculo: mientras el sector privado compite agresivamente por talento, las administraciones suelen ofrecer salarios menos competitivos y pocas posibilidades de promoción profesional, lo que dificulta atraer y retener expertos.

Por último, un teórico punto fuerte de la administración electrónica como es la interoperabilidad, por fin llegó, pero en este caso no es más que una nueva brecha que deriva de la interconexión de sistemas y datos entre diferentes niveles de gobierno (local, regional, nacional, institucional), a los que hay que añadir la colaboración con entidades privadas, todo lo cual amplía el espectro del ataque. Un agujero de seguridad en un solo punto puede comprometer toda la red.

Por todo ello, no podemos terminar sin proponer al menos unas cuantas estrategias o medidas clave que las administraciones pueden adoptar para protegerse de estas amenazas:

1. Inversión en nuevas infraestructuras. Reemplazar sistemas obsoletos por soluciones seguras y escalables es esencial. Esto incluye la adopción de tecnologías en la nube con cifrado robusto y sistemas de autenticación multifactor.

2. Capacitación continua. Según detectamos en su momento, este ya era un factor a mejorar en la “era del ENS”. Sin embargo, los empleados son a menudo el eslabón más débil en la cadena de seguridad. Programas regulares de formación sobre *phishing*, manejo seguro de datos, buenas prácticas digitales y la mera “concienciación” pueden reducir significativamente el riesgo por errores humanos.

3. Sistemas de respuesta rápida y coordinada. Esta medida pasa por establecer equipos especializados de respuesta ante incidentes cibernéticos (CERT) y protocolos claros para actuar ante brechas de seguridad, lo cual garantiza una mitigación efectiva del daño.

4. Colaboración Público-Privada (CPP). El sector privado tiene, sin duda, más experiencia en estas cuestiones. Contratar a empresas tecnológicas permite acceder a herramientas y conocimientos avanzados que llevan años siendo testados en situaciones reales. Además, los estándares compartidos entre sectores pueden fortalecer la resiliencia global.

5. Regulación y cumplimiento. Por último, cabe recordar la normativa de la cual sabemos que disponemos pero que no siempre cumplimos y hacemos cumplir. Implementar normativas estrictas sobre seguridad y ciberseguridad, como el Reglamento General de Protección de Datos (GDPR) o el propio Reglamento de Inteligencia Artificial, obligan a los empleados de las instituciones a vigilar los sistemas de riesgo, a priorizar la protección de datos y a establecer sanciones por negligencia, entre otras medidas preventivas y reactivas.



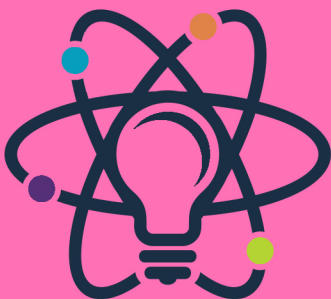
VÍCTOR ALMONACID

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

Desentrañando la Ciberseguridad en Redes Tácticas 6G: Amenazas, Arquitectura e Inteligencia Artificial

La evolución de las comunicaciones móviles hacia la sexta generación (6G) ha abierto un abanico de posibilidades en entornos críticos y tácticos, donde la seguridad y la disponibilidad se convierten en pilares fundamentales para la operatividad. En un contexto donde las redes deben ser resilientes y seguras en situaciones de emergencia, el desarrollo de infraestructuras tácticas se convierte en una necesidad imperiosa para organismos de seguridad pública, defensa y emergencias. Esta transformación no solo implica una mejora en las capacidades de transmisión y procesamiento de datos, sino también la integración de tecnologías emergentes que permitan una respuesta ágil y adaptativa ante amenazas cibernéticas. La integración de redes terrestres y no terrestres, la computación en el borde (edge computing) y la inteligencia artificial (IA) son algunos de los conceptos revolucionarios que configuran el nuevo ecosistema de las comunicaciones 6G.

Estas tecnologías permiten la creación de **“burbujas tácticas”**, redes privadas de despliegue rápido que garantizan conectividad en zonas de desastre, áreas remotas o escenarios de alta incertidumbre. La combinación de estas soluciones tecnológicas posibilita la entrega de servicios críticos como videoconferencias de alta definición, supervisión en tiempo real y control remoto de dispositivos, pero sin olvidar una parte muy importante la seguridad de la información.

Evolución y Relevancia de las Redes Tácticas en 6G

La transición de las tecnologías de comunicación tradicionales a soluciones basadas en 6G se fundamenta en la necesidad de satisfacer exigencias cada vez más complejas en entornos críticos. Durante décadas, las comunicaciones de seguridad pública se han apoyado en infraestructuras específicas, como la TETRA, pero el avance hacia redes basadas en estándares 3GPP ha permitido la convergencia de servicios y la optimización de recursos. Esta evolución no solo mejora la eficiencia operativa, sino que también reduce los costes al aprovechar infraestructuras comerciales que se extienden con soluciones privadas y de despliegue rápido.

El concepto de **"burbuja táctica"** surge como respuesta a escenarios en los que la infraestructura convencional no está disponible o ha sido comprometida, como en catástrofes naturales o ciberataques a gran escala. Estas burbujas permiten la implementación inmediata de una red autónoma, capaz de operar de forma aislada y de gestionar aplicaciones críticas como la comunicación en grupo, la vigilancia en tiempo real y el control remoto de vehículos y robots. La integración de capacidades de IA y análisis de datos en el borde (edge computing) de la red añade una capa adicional de inteligencia, permitiendo una orquestación rápida y flexible de los recursos disponibles.

Arquitectura de Seguridad para Redes Tácticas

El diseño de una arquitectura de seguridad para redes tácticas 6G requiere un enfoque que abarque desde la protección del acceso a la red hasta la seguridad de las aplicaciones y servicios desplegados. Los estándares 3GPP han establecido una base sólida en cuanto a procedimientos de autenticación, autorización y encriptación, los cuales se extienden a la integración de redes no terrestres mediante protocolos específicos para garantizar la protección de los enlaces de backhaul.

El diseño de la arquitectura de seguridad se fundamenta en principios como la exposición controlada de capacidades, la automatización a través de inteligencia artificial y la escalabilidad para adaptarse a distintas topologías y volúmenes de tráfico. En las **burbujas tácticas**, es fundamental que los dispositivos y sistemas se autenticuen mutuamente antes de intercambiar información, lo que se logra mediante el uso de certificados digitales, credenciales específicas y protocolos de seguridad reforzados. La separación de funciones y la segmentación de la red permiten limitar el alcance de un posible compromiso, reduciendo el riesgo de que un ataque se propague de manera incontrolada.



CONTINÚA EN
PRÓXIMA PÁGINA

La arquitectura también incorpora mecanismos para la gestión dinámica y la orquestación de servicios de seguridad, apoyados en tecnologías de virtualización y en redes definidas por software (SDN). Estas soluciones posibilitan la implementación de políticas de seguridad que se adaptan en tiempo real a los cambios en el entorno operativo. La integración de sistemas de detección de intrusiones y de respuesta automática a incidentes permite no solo identificar amenazas en etapas tempranas, sino también activar medidas de mitigación que protejan la continuidad del servicio. La resiliencia operativa se refuerza mediante el uso de redundancia y la capacidad de aislamiento de segmentos comprometidos, garantizando que incluso en el peor de los escenarios, la red pueda seguir funcionando en la medida de lo posible.

Desafíos y Perspectivas Futuras en la Ciberseguridad Táctica 6G

A pesar de los avances tecnológicos, la implementación de soluciones de ciberseguridad en entornos tácticos 6G enfrenta desafíos significativos que requieren una atención continua por parte de investigadores y profesionales. Uno de los principales retos reside en la interoperabilidad de sistemas heterogéneos, donde dispositivos de distintos fabricantes y protocolos diversos deben operar de manera coordinada. Esta diversidad complica la integración de mecanismos de seguridad unificados y obliga a diseñar soluciones que sean lo suficientemente flexibles para adaptarse a distintos escenarios operativos sin sacrificar la robustez de las medidas de protección.

Otro desafío relevante es el equilibrio entre el rendimiento y la seguridad. Las aplicaciones de misión crítica, que requieren latencias extremadamente bajas y un alto ancho de banda, imponen restricciones que pueden entrar en conflicto con la implementación de capas adicionales de encriptación y autenticación.

Este escenario demanda innovaciones en algoritmos de seguridad que sean eficientes y que, al mismo tiempo, ofrezcan un nivel de protección acorde a los estándares de resiliencia necesarios para la operatividad en situaciones de alta tensión. La investigación en criptografía post-cuántica y en técnicas de encriptación es fundamental para superar estas barreras y asegurar que las redes 6G puedan mantener la integridad y

confidencialidad de los datos sin comprometer la velocidad de procesamiento.

La colaboración entre organismos de investigación, industrias y entidades gubernamentales se vislumbra como una necesidad imperiosa para avanzar en este campo. La estandarización de protocolos y la elaboración de marcos regulatorios adaptados a las nuevas realidades tecnológicas permitirán crear un ecosistema de seguridad robusto y adaptable. En este sentido, en España hemos avanzado algunos pasos, ya que disponemos del ENS5G (Esquema Nacional de Seguridad 5G), lo que permite regular y definir una línea base para la seguridad de las redes 5G.

Conclusiones

La transformación digital en el ámbito de las **comunicaciones tácticas** ha alcanzado un punto de inflexión crucial con la llegada del 6G. Las nuevas capacidades tecnológicas, la integración de redes terrestres y no terrestres y el uso intensivo de inteligencia artificial están redefiniendo la forma en que se protege la información y se aseguran los servicios críticos en entornos operativos.

La arquitectura de seguridad propuesta para redes tácticas 6G se fundamenta en principios sólidos que abarcan desde la autenticación y la autorización hasta la encriptación y la gestión dinámica de recursos. La implementación de soluciones basadas en SDN, NFV y otras tecnologías de virtualización garantiza la flexibilidad necesaria para operar en entornos heterogéneos y en condiciones adversas.

En conclusión, la ciberseguridad en redes tácticas 6G representa un desafío de gran envergadura, pero también una oportunidad única para transformar el paradigma de la protección en entornos críticos.

El camino hacia un ecosistema seguro exige la convergencia de tecnologías de vanguardia, la colaboración estrecha entre sectores y el compromiso continuo con la innovación. Solo a través de una estrategia integral y adaptativa será posible garantizar que, en el futuro, las comunicaciones en situaciones de emergencia sean no solo eficientes, sino también inviolables.



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.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gestión de Centros
de Operaciones
de Seguridad (SOC)**

**SOC
Management
Leader**

Docente:

Alejandro Aliaga

Coordinación Académica:

Javier Peris

- Formato: Directo en Remoto
- Duración: 20 horas
- Sesiones: Viernes y Sábados
- Viernes: De 16:00 a 21:00 horas
- Sábados: De 9:00 a 14:00 horas
- Examen de Certificación: Incluido
- Aforo: Limitado 15 Alumnos
- Acceso: Solicitud de admisión

MidMgmt®

MPPM®

MGEIT®

eGob®

Próxima Convocatoria en Directo
MAYO 2025



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



**Plazas
limitadas**

Marta Martín

Decálogo para cultivar el arte de la atención

Uno de los aspectos más preocupantes del TDAH tiene que ver con la forma en la que el cerebro maneja la atención y la concentración. Sin duda, vivir con TDAH supone un reto para Mantenerlas de forma sostenida y optimizarlas, supone un reto para las personas con TDAH a la vez que genera altos niveles de frustración y agotamiento. Por ello, es fundamental tener a mano algunas estrategias que pueden ayudarnos.

No todas las técnicas funcionan para todo el mundo. Cada persona tiene una manifestación y combinación de síntomas de TDAH características. Pero, entre todas las pautas que vamos a ver, alguna puede ser de utilidad para mejorar tu capacidad de concentración.

1. Crea una rutina estructurada

Los cerebros con TDAH no se llevan bien con la incertidumbre. Por eso, una rutina diaria y constante

nos prepara para saber qué esperar, para reducir la ansiedad y favorecer nuestra concentración. Crea un horario de estudio regular y elige un lugar para trabajar. Encuentra una rutina que funcione para ti y cíñete a ella. Esta constancia facilitará tu concentración y mejorará tu productividad.

2. Organiza el entorno

Una vez elegido el espacio de trabajo conviértelo en un lugar tranquilo donde puedas concentrarte, mantenlo ordenado y libre de distracciones, con todos los materiales que necesites organizados y a tu alcance.

3. Desarrolla habilidades de gestión del tiempo

Imprescindibles para manejar el tiempo con precisión y evitar la ceguera temporal tan característica del TDAH. Los cronómetros y planificadores son muy útiles para realizar un seguimiento de las tareas y los plazos. A

P L A N



algunas personas les funcionan bien estrategias como la técnica Pomodoro, es decir, trabajar concentrado por un intervalo de tiempo definido seguido de pausas breves. Sin embargo, a otras les va mejor dejarse llevar cuando están concentradas. Sea como sea, siempre viene bien programar pequeños descansos que te ayuden a procesar la información en lugar de sobrecargarte.

Y no olvides establecer plazos concretos. Las fechas u horas límite proporcionan un objetivo sólido y crean una sensación de urgencia que nos ayuda a gestionar nuestro tiempo con eficacia.

4. Elimina las distracciones

Busca un lugar tranquilo para trabajar o estudiar y apaga las notificaciones de los dispositivos electrónicos. Puedes instalar un bloqueador de aplicaciones y sitios web para reducir tu exposición a contenidos no deseados.

5. Divide las tareas en partes

A veces, las tareas grandes pueden resultar abrumadoras. Dividir las en pasos más sencillos y manejables las hace menos intimidantes. Por ejemplo, si tienes un objetivo importante, divídelo en pasos más pequeños. Termina un paso, tómate un breve descanso y luego pasa al siguiente.

6. Utiliza herramientas organizativas

Encuentra herramientas que te ayuden a mantener tus tareas y fechas de entrega organizadas. Quizás te sean útiles agendas, calendarios, notas adhesivas, pestañas de colores o aplicaciones. Puede que necesites probar y equivocarte, pero lo importante es que encuentres el sistema que mejor funcione para ti.

Y por supuesto, ten una libreta de notas cerca para anotar tareas, mensajes, citas y pensamientos importantes que podrás abordar más tarde.

El auténtico arte de la memoria es el arte de la atención

**Samuel Johnson
(1709-1784)**

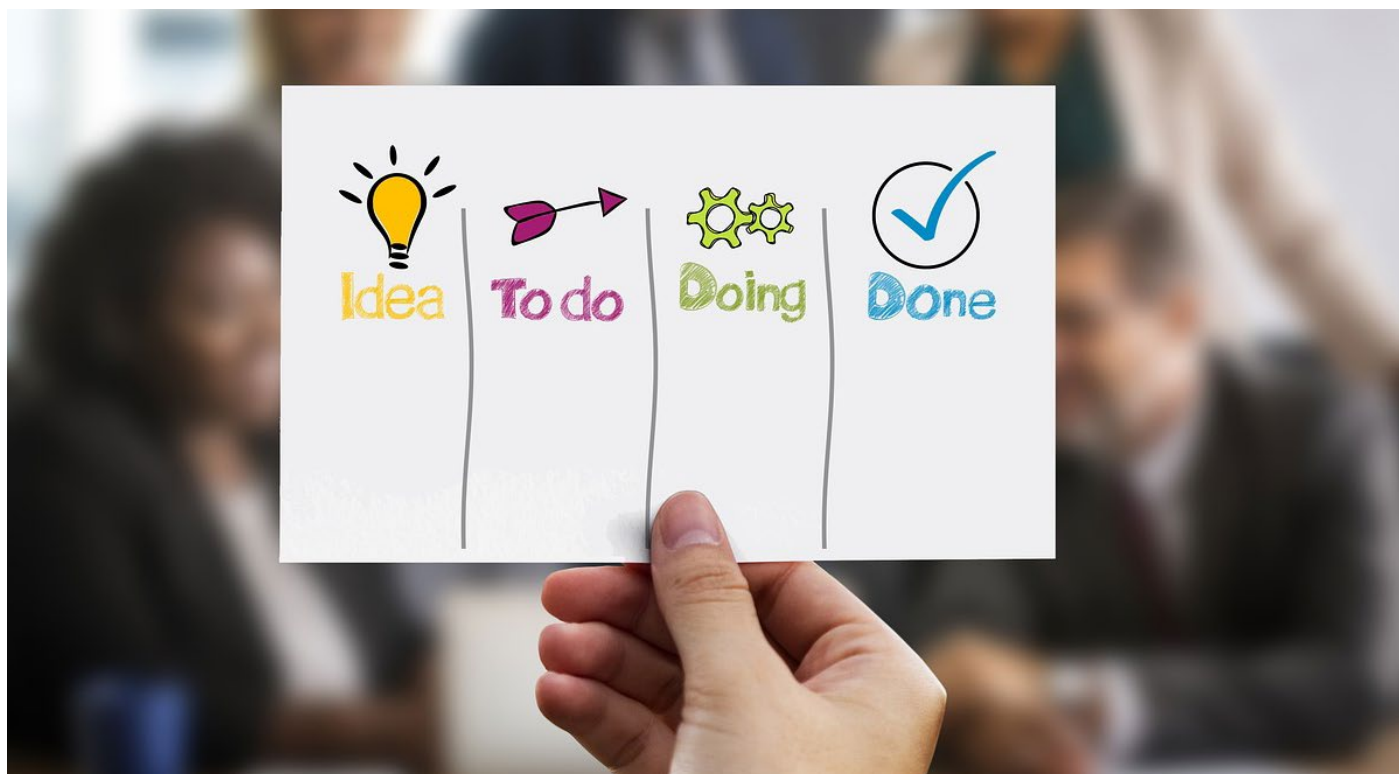
7. Enfócate en una sola tarea a la vez

Ser multitarea está muy valorado pero lo cierto es que los estudios demuestran que no es tan productivo como parece. Y desde luego, para nosotros funciona mucho mejor centrarnos en una sola tarea. Pasito a pasito, nuestra concentración es mucho más eficaz. Para ello, realiza una lista de las tareas pendientes y ordénalas según su importancia y urgencia. Empieza por la más relevante y dedícala toda tu atención con los descansos que necesites para finalizarla. Cuando la taches de la lista, te sentirás motivado para seguir con la siguiente.



**CONTINÚA EN
PRÓXIMA PÁGINA**





8. Alterna entre tareas

De todas formas, si te agobias o te aburres con un trabajo concreto y no logras avanzar, cambia a otro. Ese bloqueo no es nada productivo así que, aparta aquello que no te permita avanzar y retómalo más adelante.

9. Fomenta la atención plena y la relajación

Hay multitud de técnicas para reducir la inquietud y mejorar la concentración como la atención plena o la relajación. La atención plena o mindfulness consiste en hacer que nuestro cerebro se centre en el momento presente, en el aquí y en el ahora, dejando al margen lo que nos pueda distraer.

Los ejercicios de respiración profunda practicados con regularidad tienen efectos positivos sobre nuestra función cerebral, capacidad de atención y relajación. Prueba a respirar profundamente unas cuantas veces y a notar cómo se siente tu cuerpo. También puedes cerrar los ojos durante unos segundos y escuchar los sonidos que te rodean. Puedes dar un paseo tranquilo, beber algo o sentir un aroma relajante.

10. Mantén hábitos saludables

Hábitos recomendables para todo el mundo, pero mucho más si necesitas controlar tu TDAH. El triunvirato perfecto es ejercicio, alimentación y sueño.

No hace falta que recuerde los múltiples beneficios del ejercicio,

pero por si acaso, ahí van algunas de sus ventajas: reduce la ansiedad, mejora la concentración y la memoria; suaviza el carácter; mejora nuestra disciplina; la imagen que tenemos de nosotros mismos, por lo que sube nuestra autoestima; nos ayuda a dormir mejor; y nos oxigena mejorando nuestras funciones cerebrales.

Presta atención a tu alimentación y no olvides beber agua. Y, por supuesto, cuida tu sueño porque un cuerpo y una mente bien descansados proporcionan una base sólida para la concentración y la productividad sostenidas.

Dicho todo lo anterior, no hay duda de que controlar estos aspectos del TDAH no es sencillo. Pero conocernos mejor para saber cuáles son nuestras mayores dificultades nos ayudará a aprender cómo afrontarlas y a ser más comprensivos con nosotros mismos. Así que, establece metas claras y utiliza las herramientas que consideres más adecuadas para mantenerte organizado y minimizar las distracciones. Si probamos una técnica y no funciona, pasemos a la siguiente, lo importante es descubrir qué funciona mejor para cada uno de nosotros.



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

¿Excelencia? Una crónica sobre la transformación del servicio en la era digital

A las puertas de un mundo cada vez más interconectado, la inteligencia artificial ya no es una promesa futurista: es una realidad presente que exige reflexión, responsabilidad y, sobre todo, excelencia. Bajo esta premisa, el Service Management Institute (SMI) convocó a profesionales, expertos y líderes del sector en una jornada que, más que una conferencia, se transformó en una llamada a la acción: redefinir la gestión y dirección de servicios en tiempos de transformación acelerada.

La jornada, titulada "¿Excelencia?", no solo jugó con el acrónimo de la inteligencia artificial sino también insinuó una pregunta profunda: ¿cómo garantizar la excelencia cuando la tecnología avanza más rápido que las estructuras organizativas y los marcos regulatorios? La respuesta se desplegó a lo largo de una intensa agenda que combinó análisis normativo, debate ético, inspiración profesional y visión estratégica.



CONTINÚA EN
PRÓXIMA PÁGINA



NA 2025
MÁTICA

20^o

O DE ABRIL

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Desde los primeros compases del evento, quedó claro que la gestión de servicios ha dejado de ser un asunto meramente técnico. Nacida de las entrañas del modelo ITIL, esta disciplina ha evolucionado hacia un rol estratégico. Hoy, casi todos los servicios –públicos o privados– descansan sobre pilares digitales. Y en ese entorno, gobernar y gestionar ya no es una opción: es una obligación estructural.

Javier Peris, presidente del SMI, lo dijo sin rodeos: *"Gobernar y gestionar los servicios no es una opción, es nuestra obligación."*

Alejandro Blasco, presidente del Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana, fue aún más enfático al recordar que la excelencia de servicio es el camino para fidelizar y destacar:

"La excelencia de servicio es fundamental para cualquier organización que aspire a destacarse y fidelizar a los clientes."

Tras una destacada introducción por parte de dos reconocidos profesionales, llegó el turno de Luis Morán y Moisés Robles, que forman parte de varios Comités Técnicos de Normalización UNE, quienes ofrecieron una charla en formato conversacional y relajada centrada en las certificaciones más relevantes en el ámbito de los servicios de TI. Durante su intervención, abordaron los principales marcos de referencia en gestión de servicios (ITSM) y analizaron su evolución y tendencias desde 2005 hasta la actualidad. Entre los enfoques discutidos se incluyeron ITIL, ISO/IEC 20000, FitSM, VeriSM, COBIT e IT4IT, proporcionando una visión comparativa y actualizada del panorama de certificaciones y buenas prácticas en el sector.

El interés por esta excelencia no es nuevo, pero lo novedoso es la forma en que se intenta medirla, fomentarla y certificarla. En este sentido, la normalización se convierte en protagonista, con la ISO 20000 aún vigente, y la reciente UNE 11367:2025 aportando una visión renovada y centrada en el ciudadano para el servicio público.



CONTINÚA EN
PRÓXIMA PÁGINA



Pocas veces una norma técnica despierta tanto entusiasmo como lo hizo la UNE 11367:2025, desarrollada en el seno del comité CTN 309-SC1. Inspirada en un modelo alemán, esta norma no solo detalla buenas prácticas; dibuja un horizonte ambicioso: ofrecer servicios públicos capaces de sorprender y deleitar. Todo esto nos lo contó Elena Ordozgoiti, responsable de Negocio de UNE, mostrando los modelos de calidad que existen dentro de las normas.

Javier Peris explicó con entusiasmo el espíritu de esta nueva guía:

"Es una norma para todas las compañías que quieren prestar servicios Wow. Servicios que entusiasman, que no se quedan en la gestión."

La pirámide de excelencia que propone la UNE 11367 y presentada por Elena y Javier empieza con el cumplimiento del servicio prometido, pero escala hasta la creación de experiencias extraordinarias. Y lo hace sobre cuatro pilares fundamentales: liderazgo, cultura organizativa, enfoque en el ciudadano y mejora continua. Un marco que trasciende lo técnico para abrazar lo humano.

Pero si hay un protagonista que atraviesa transversalmente todos los temas del evento, ese es la inteligencia artificial. Lejos de celebrarla acríticamente, los ponentes coincidieron en subrayar su potencia y, al mismo tiempo, la necesidad de un uso ético, responsable y legalmente sostenible.

Los casos de uso son muchos: categorización de incidencias, automatización de tareas repetitivas, análisis predictivo de fallos, personalización de la experiencia del usuario. Sin embargo, junto a estos beneficios emergen riesgos elevados, desde la manipulación de emociones hasta la identificación biométrica remota.

Jesús López, presidente del Consejo Legal del SMI, hizo una presentación magistral hablando de IA y destacó:

"No nos vale con cumplir la ley porque lo dice la ley. Tenemos que convertir el cumplimiento de la ley en satisfacción para el cliente."

Esa afirmación resume un cambio de paradigma: la legalidad como base, pero no como techo. La excelencia exige ir más allá del reglamento y abrazar una ética del servicio que inspire confianza y promueva la transparencia.



CONTINÚA EN
PRÓXIMA PÁGINA



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Uno de los espacios más emotivos e inspiradores de la jornada fue, sin duda, la mesa redonda moderada por Angie López, Vocal de la Junta Directiva del SMI con profesionales certificados SMP.

Aquí, lejos de las definiciones académicas, se habló de personas, de emociones, de clientes reales con expectativas reales. Se habló de cómo la tecnología debe ser una aliada, no un sustituto, y de cómo la excelencia solo se alcanza cuando hay humanidad detrás del servicio.

Paula Jovel, líder de gestión de servicios Equifax, lo expresó con claridad:

"Tenemos que estar en constante cambio, superándonos, formándonos... siempre de la

mano del tacto humano y la empatía. Porque al final, son claves para la calidad del servicio."

María José Montes, de Accenture, fue aún más tajante:

"La excelencia del servicio no se trata solo de cumplir, sino de generar confianza y ser un socio estratégico, no solo un proveedor."

A lo que Juan Darocha, director de servicios de Nunsys añadió *"Me ha gustado mucho el concepto de XLA, que va más allá del SLA... buscar ese poquito más allá mediante escucha activa y personalización a los clientes."*

Esa confianza no se construye únicamente con métricas ni se resume en SLA cumplidos. Se cultiva con escucha activa, con personalización sin improvisación, con



celebraciones de los éxitos y aprendizajes de los errores.

Porque en un mundo cada vez más automatizado, la empatía sigue siendo el diferencial más difícil de replicar.

La jornada también dedicó espacio a reflexionar sobre los factores globales que inciden en la prestación de servicios. La posible imposición de aranceles por parte de potencias como Estados Unidos podría modificar la dinámica de los proveedores internacionales, impulsando a muchas empresas a reconsiderar sus cadenas de suministro y apostar por la proximidad o por la autosuficiencia regulatoria.

Este escenario geopolítico añade una capa más de complejidad a la gestión del servicio, recordando que la excelencia no es solo técnica

ni interna, sino también estratégica. Se trata de anticipar riesgos, garantizar la continuidad y construir organizaciones resilientes, incluso en entornos volátiles.

Siguiendo el evento de mediante la excelencia de los servicios, Marcos Navarro, Vocal de la Junta Directiva del SMI, nos enseñó que, en un escenario en constante cambio, donde la inteligencia artificial redefine lo posible, la necesidad de contar con un lenguaje común para la dirección de servicios se vuelve crítica.



CONTINÚA EN
PRÓXIMA PÁGINA





Por eso, el anuncio del Service Management Body of Knowledge (SMBOK) marcó uno de los momentos más esperanzadores de la jornada.

Este compendio de conocimiento, impulsado por el SMI, busca convertirse en la base estructural del saber en gestión y dirección de servicios, sin limitarse a un sector o tecnología específica. Su aparición no solo marcará un hito en la disciplina, sino que también pondrá fin al llamado "grandfathering" de la certificación Service Management Professional (SMP).

El broche de oro, lo puso Carlos Manuel Fernández Sánchez, vicepresidente del SMI, con una petición clara a los profesionales del sector:

"Si eres un buen profesional en dirección de servicios, certifícate y que todo el mundo te pueda medir por esa excelencia."

La certificación SMP no es solo un reconocimiento formal. Es un compromiso ético, una declaración de principios y una apuesta por la mejora continua. Basada en valores como la honestidad, la responsabilidad y el respeto, esta certificación busca identificar a aquellos que, más allá del conocimiento técnico, lideran con propósito.



CONTINÚA EN
PRÓXIMA PÁGINA

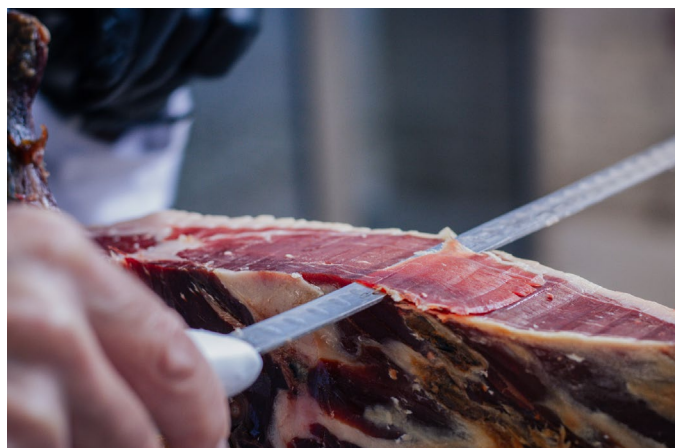


La jornada “¿Excelencia?” no ofreció soluciones mágicas, pero sí algo mucho más valioso: una brújula ética y profesional para navegar el futuro. En un momento en que la tecnología avanza sin pedir permiso, y la inteligencia artificial se infiltra en todos los procesos, la verdadera pregunta no es si podemos usarla, sino cómo la usaremos.

Y esa respuesta requiere una nueva generación de líderes del servicio: profesionales con visión estratégica, compromiso ético, sensibilidad humana y formación continua.

Profesionales que entienden que la excelencia no es un estado, sino un camino sin fin, impulsado por la mejora constante y la pasión por servir.

El evento cerró con una invitación directa a la acción: conocer el SMBOK, certificarse como SMP y, sobre todo, liderar el cambio con rigor, humildad y valentía. Porque la excelencia en la inteligencia artificial no comienza en los algoritmos, sino en las personas que los diseñan, los aplican y los regulan.

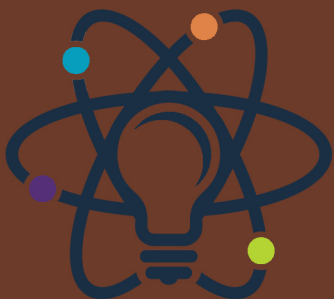


PMO Book

Management Offices

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE



Semana Informática 2025 culmina otra edición con una gran acogida del sector que refuerza su compromiso con la innovación y el desarrollo tecnológico

Semana Informática 2025, el evento de referencia para profesionales de las tecnologías de la información (TI), celebró su 20ª edición del 8 al 10 de abril. Bajo el lema '**Informática y sociedad: disrupciones al servicio de las personas**', este encuentro, organizado por el Colegio Oficial de Ingeniería Informática de la Comunitat Valenciana (COIICV), reunió a profesionales del sector que debatieron sobre los últimos avances y desafíos tecnológicos, explorando cómo la tecnología impacta en la sociedad y mejora la vida de las personas.

Esta edición contó como parte del comité organizador con la Cátedra de Ciberseguridad INCIBE-UPV, financiada por los Fondos Next Generation de la Unión Europea (UE) e impulsada por el Plan de Recuperación, Transformación y Resiliencia, a través de Incibe, y con la colaboración del Ajuntament de València, a través de la Valencia Innovation Capital.

Semana Informática 2025, que este año se centró en la ciberseguridad, la inteligencia artificial, la innovación y la economía digital, fue inaugurada por **Alejandro Blasco**, presidente del COIICV. Durante la primera jornada, que tuvo lugar en el centro de innovación social y urbana Las Naves de Valencia, Blasco destacó que "las tecnologías están revolucionando sectores clave como la salud, la educación y los servicios públicos, mejorando su eficiencia y accesibilidad".



CONTINÚA EN
PRÓXIMA PÁGINA

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



SEMANA 2025
INFORMÁTICA

Informática y sociedad:
disrupciones al servicio
de las personas

Administración
digital al servicio de
las personas

Martes 8 de abril



www.semanainformatica.com



#S2025



Además, el presidente del COIICV hizo hincapié en que “estas innovaciones no solo facilitan la vida cotidiana, sino que también promueven la inclusión social al ofrecer soluciones adaptadas a personas con discapacidades y a comunidades marginadas”. Sin embargo, “también plantean desafíos éticos y de privacidad que debemos abordar con responsabilidad”, señaló.

La bienvenida también contó con la presencia de **Javier Balfagón**, director general de Tecnologías de la Información y las Comunicaciones (DGTIC) de la Generalitat Valenciana, y **David Rosa**, director de Valencia Innovation Capital. Por su parte, Balfagón puso el foco en cómo la DANA “aceleró la planificación para introducir tecnologías disruptivas”, por lo que “hubo que usarlas para dar soluciones rápidas y servicio a las personas afectadas”; mientras que David Rosa abogó por seguir con “una colaboración público-privada en el marco de la estrategia impulsada desde el Ajuntament de València para lograr una ciudad realmente innovadora”.

Durante esta primera sesión, titulada ‘**Administración digital al servicio de las personas**’, se reflexionó sobre el impacto de la robótica en la agilización judicial, así como sobre los beneficios y desafíos de la adopción de la nube pública en la administración. Asimismo, se abordó el reto de hacer que las administraciones resulten más atractivas para los nuevos egresados TIC, con estrategias para atraer talento.

La clausura de la jornada corrió a cargo del vicepresidente segundo y conseller para la Recuperación Económica y Social de la Comunitat Valenciana, **Francisco José Gan Pampols**, quien destacó que “los informáticos son la muestra palpable del potencial de la región de la Comunitat Valenciana”. “Los profesionales de la ingeniería informática son las soluciones de los problemas y llevan sobre sus hombros una gran responsabilidad”, puntualizó.

La tarde de la primera jornada comenzó con un **seminario online** sobre la automatización de pruebas en proyectos web. En un contexto en el que la calidad del software es un factor clave para el éxito de cualquier proyecto tecnológico, el encuentro destacó cómo la automatización de pruebas contribuye a optimizar tiempos y aumentar la eficiencia en el desarrollo.



CONTINÚA EN
PRÓXIMA PÁGINA

NA 2025
MÁTICA

20 años

10 DE ABRIL



#SI2025



#TYSC / PÁG. 72

El segundo encuentro de Semana Informática estuvo marcado por la sesión '**Seguridad informática: adaptación y respuesta ante nuevas amenazas**', que versó sobre la ciberseguridad y tuvo lugar también en Las Naves. Esta sesión la inauguró el **presidente del COIICV**, quien aseguró que "en un mundo sin fronteras digitales, la seguridad informática es esencial para proteger a las personas y organizaciones ante nuevas amenazas".

La apertura también contó con **Jerónimo Mora**, secretario autonómico de Innovación, que destacó que "la ciberseguridad debe integrarse en el diseño, en nuestra estructura". Además, agradeció al COIICV "su compromiso con la sociedad" y ha invitado a sumar esfuerzos "a las administraciones, a los colegios y a las empresas para mejorar la ciberseguridad".

Durante la jornada se abordaron temas clave como el papel de las Fuerzas Armadas en el ciberespacio, la protección digital en los puertos valencianos y los desafíos en la seguridad de entornos de trabajo distribuidos. Además, **Santiago Escobar**, director de la Cátedra de Ciberseguridad INCIBE-UPV, presentó los objetivos y acciones desarrolladas por la misma, y, por otro lado, se analizó la problemática específica en entornos industriales.

La sesión también contó con la presencia de **Román Ramírez**, fundador de la RootedCon, una de los eventos de seguridad informática más destacados en el ámbito hispanohablante. Asimismo, se puso de relieve la necesidad de fortalecer la seguridad digital en sectores estratégicos, adaptándose a un panorama de amenazas en constante evolución para garantizar así la protección de infraestructuras y datos críticos.

Esa misma tarde, el **Service Management Institute (SMI)** celebró su jornada '**Excelencia**', donde se compartieron las novedades sobre las normas fundamentales para una dirección excelente de servicios y se valoró el impacto de la inteligencia artificial en la prestación y evolución de los servicios. Además, se destacó la importancia de estar certificado en SMP (Service Management Professional) como garantía de excelencia, conocimiento y compromiso.

La tercera y última sesión de la Semana Informática estuvo marcada por el **XX Congreso de Ingeniería Informática de la Comunitat Valenciana**, que también tuvo lugar en Las Naves.



CONTINÚA EN
PRÓXIMA PÁGINA



SEMANA 2025
INFORMÁTICA

DEL 8 AL 10 DE ABRIL



Información y sociedad:
disponibles al servicio
de las personas



#TYSC / PÁG. 74

Este encuentro anual de profesionales del sector lo inauguró **Alejandro Blasco**, quien habló del “empeño personal” y del colectivo que representa “para que la Comunitat Valenciana tenga un sector empresarial TIC, visible como industria y con el peso específico que los números le acreditan”.

La apertura del congreso también contó con **Fernando Suárez**, presidente del Consejo General de Colegios de Ingeniería Informática (CCII), quien indicó que en la ingeniería informática “es necesario reconocer el papel de las mujeres”. “Necesitamos una informática más diversa, más justa y con más representación. Por eso, la educación es la base para adaptarse a los retos del futuro”, señaló.

La jornada comenzó con un análisis del Instituto Valenciano de Investigaciones Económicas (IVIE) sobre la **economía digital en España**, explorando las oportunidades y desafíos que la nueva realidad nos presenta como sociedad. Además, también se contó con la visión de empresas tecnológicas referentes en el ecosistema local, que reflexionaron sobre los primeros pasos a realizar para la **creación de un clúster TIC en la Comunitat Valenciana**.

La Fundación ONCE focalizó su intervención en la necesidad de la **inclusión de la accesibilidad en el diseño de productos y servicios basados en TIC**. En el ámbito de la salud, se exploró cómo la **IA generativa puede humanizar la medicina**, ayudando a tomar decisiones clínicas más precisas y eficaces. También se trataron las distintas opciones de compra de TIC que permite la Ley de Contratos del Sector Público, y se reflexionó sobre el “síndrome del algoritmo”, analizando los posibles sesgos de la inteligencia artificial en el sistema sanitario, así como la IA puede contribuir a acabar con las desigualdades.

Durante la tarde del jueves se impartió el seminario online **‘Resolución de Problemas Complejos en el Desarrollo Software’**, que tuvo como propósito enseñar a identificar este tipo de problemas y a enfocar su resolución mediante métodos experimentales.

El colofón de Semana Informática 2025 lo puso la entrega de los **Premios Sapiens**, cuya gala tuvo lugar en el edificio de Veles e Vents de Valencia la noche del 10 de abril ante más de 200 personas. Estos galardones, que desde 2006 concede anualmente el COICV, tienen como objetivo distinguir a profesionales, empresas y administraciones públicas que sobresalen en el uso ético y social de las Tecnologías de la Información y las Comunicaciones (TIC).



CONTINÚA EN
PRÓXIMA PÁGINA



La gala de estos Premios fue conducida por la periodista **Susana Ollero**, y comenzó con la bienvenida del presidente del COIICV, **Alejandro Blasco**. En su intervención, recordó que este evento “no es solo una entrega de premios; es una celebración de la excelencia, la innovación y el compromiso inquebrantable con el avance de nuestra disciplina, pero también de toda la sociedad. Nos inspira para seguir adelante, a seguir innovando, aprendiendo y compartiendo nuestro conocimiento con el mundo”.

Además, hizo hincapié en su interés “por lograr un sector TIC fuerte y vibrante en la Comunitat Valenciana”. “El beneficio de unos serán los logros de otros y viceversa. Subamos el nivel de intensidad de las alianzas. Nos harán más fuertes, más robustos, más diferenciales, más relevantes”, puntualizó.

El comité de los Premios Sapiens otorgó la distinción ‘**Sapiens Empresa**’ a **Kio España**, una compañía que refuerza su apuesta con la innovación mediante la construcción de un nuevo Centro de Datos en Valencia. **Javier Jarilla**, CEO de KIO España, fue el encargado de recoger el galardón entregado por **Manuel Herrero Mas**, jefe de Área de Innovación y Agenda Digital del Ayuntamiento de Valencia.

El galardón ‘**Sapiens Proyecto**’ recayó en la iniciativa ‘Cajero Autoservicio con Reconocimiento Facial’, desarrollada por el Ayuntamiento de Paiporta. Una idea que transforma el acceso ciudadano a los servicios públicos electrónicos, haciéndolo más ágil y seguro. **María Sanchis Valero**, técnica de informática en el Ayuntamiento de Paiporta, recogió el galardón en nombre del consistorio de manos de **Juan Pablo Peñarrubia**, vicepresidente del COIICV.

La distinción ‘**Sapiens Humanismo y Compromiso Social**’ fue para la Fundación ONCE por su labor en favor de la accesibilidad y la innovación social. **Antonio J. Ingelmo**, técnico experto del departamento de Accesibilidad Tecnológica, Dirección de Accesibilidad e Innovación de Fundación ONCE, fue el encargado de recogerlo. El premio fue entregado por **Silvia Rueda**, vicepresidenta 2ª del COIICV.

El ‘**Premio Sapiens Divulgación Digital**’ reconoció la labor de la iniciativa **eFormación**, un servicio online de formación en abierto de la Generalitat Valenciana que facilita la capacitación de la ciudadanía en áreas como las tecnologías digitales y la ciberseguridad. **Jorge Belenguer**, jefe del Servicio de Tecnología y Calidad de las TIC de la Generalitat Valenciana, recogió el galardón entregado por **Ricardo Jorge**, presidente del Consejo General de Colegios Oficiales de Ingeniería Técnica en Informática (CONCITI).

Por otro lado, el ‘**Premio Sapiens Académico**’ fue entregado a **Cristina Campos Sancho**, doctora en Informática y profesora del Grado de Ingeniería Informática en la Universitat Jaume I, por su compromiso con la educación y el avance de la informática.

El galardón lo entregó **Javier Balfagón**, director general TIC de la Generalitat Valenciana.

El ‘**Sapiens Profesional**’ recayó en **Julián del Valle**, licenciado en Informática y especialista en Gestión de Sistemas y Tecnologías de la Información, por su trayectoria, por su impacto en la profesión y por ser un referente para el sector. Este galardón fue entregado por **Alejandro Blasco**, presidente del COIICV.

Este año, el COIICV entregó también, de manera extraordinaria, un **premio a la trayectoria en ciberseguridad a S2 Grupo**, empresa que se ha consolidado como la compañía de referencia en Europa y Latinoamérica en ciberseguridad y en operaciones de sistemas de misión crítica.

José Miguel Rosell y Miguel Juan, socios directores de S2 Grupo, fueron quienes recogieron la distinción, entregada por **Santiago Escobar**, director de la Cátedra de Ciberseguridad INCIBE-UPV.

Tras la entrega de premios, la cena de gala puso el broche de oro a otra edición exitosa.

El evento reunió a más de 40 ponentes y contó con una destacada participación de profesionales y empresas, reflejo del creciente dinamismo y solidez del sector tecnológico en la Comunitat Valenciana.

Una vez más, Semana Informática se mostró como un encuentro imprescindible, donde se fomenta la colaboración activa y el intercambio de ideas, proyectos, inquietudes y desafíos entre expertos del ámbito tecnológico profesional, empresas y administraciones.

A lo largo de sus tres jornadas, el evento no solo ayudó a cohesionar y dar visibilidad a un sector en plena expansión, sino que también reforzó su papel clave en el crecimiento económico de España, demostrando su resiliencia e impulsando su proyección de futuro.



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 publica en español el estándar global de IA para las empresas

La Asociación Española de Normalización, UNE, ha publicado, en español, el primer estándar global ISO/IEC sobre sistemas de gestión de la inteligencia artificial (IA). La Norma UNE-ISO/IEC 42001 está disponible en la web del Organismo español de normalización.

El estándar especifica los requisitos para establecer, implementar y mejorar de forma continua un sistema de gestión de la inteligencia artificial en las organizaciones, de acuerdo con los principios de gobernanza, transparencia, ética y seguridad.

Está dirigido a todas las organizaciones, independientemente de su tamaño, tipo y naturaleza, que provean o usen productos o servicios que utilicen sistemas de IA.



CONTINÚA EN
PRÓXIMA PÁGINA



La Asociación Española de Normalización, UNE, representante nacional de la Organización Internacional de Normalización (ISO) y de la Comisión Electrotécnica Internacional (IEC), ha publicado la versión en español del primer estándar global sobre sistemas de gestión de la inteligencia artificial (IA), dirigido a todo tipo de organizaciones.

Este estándar especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la IA en el contexto de una organización, proporcionando una respuesta integral que garantiza que los sistemas de IA están diseñados y operan de acuerdo con los principios de gobernanza, transparencia, ética y seguridad.

La Norma está disponible en la web del Organismo español de normalización como UNE-ISO/IEC 42001:2025 Tecnología de la información. Inteligencia artificial.

Sistema de gestión. Su principal objetivo es facilitar un enfoque sistemático y coherente para la gestión de la inteligencia artificial, cubriendo aspectos esenciales como equidad, rendición de cuentas, transparencia, seguridad informática y privacidad, seguridad y salud, consecuencias financieras, accesibilidad y derechos humanos.

Para Javier García, director general de UNE y vicepresidente de ISO: “La inteligencia artificial está transformando el mundo a una velocidad sin

precedentes, lo que hace imprescindible establecer marcos de referencia robustos, fiables y medibles, basados en valores como la transparencia, la ética y la seguridad. Con la publicación en español del estándar global de IA, desde UNE, como organización global, damos respuesta eficaz a los desafíos de transformación digital de las organizaciones españolas, contribuyendo así al progreso compartido de la sociedad”.

La Norma UNE ISO/IEC 42001 es aplicable a cualquier organización, independientemente de su tamaño, tipo y naturaleza, que provea o use productos o servicios que utilicen sistemas de IA.

Implementar un sistema de gestión de la IA según este estándar ofrece numerosos beneficios, entre ellos: permite identificar y mitigar los riesgos asociados; refuerza la confianza de clientes, empleados y otras partes interesadas; facilita el cumplimiento normativo y mejora la toma de decisiones. La norma es certificable por tercera parte independiente, una forma de asegurar que se aplica eficazmente.

En la elaboración de la norma internacional participaron los expertos del Comité UNE de Inteligencia artificial y big data (CTN-UNE 71/SC 42), donde están representados 136 expertos de 58 entidades de todos los sectores.



**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>