

REVISTA

Tecnología & Sentido Común



#45

OCTUBRE
2024

**José Manuel
Muñoz Vela**

NUESTRO INVITADO
A #TYSC

24

**¿PMO vs CoE?
that is the question**

JAVIER PERIS

08

**Futuro y
Seguridad**

MANUEL SERRAT

12

**Tecnoregulación
en Prospectiva**

NACHO ALAMILLO

16

**Diario de una
tortuga ninja**

JUAN CARLOS MURIA

20

34 Es tendencia
MARLON MOLINA

42 Ai Futuro
MARCOS NAVARRO

**46 Lanueva
Administración**
VÍCTOR ALMONACID

Radio Security
ALEX ALIAGA

56

**Mentes
Divergentes**

MARTA MARTÍN

60



REVISTA Tecnología & Sentido Común



EQUIPO TYSC

Javier Peris - El Governauta
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://tecnologiaysentidocomun.com>
soluciones@businessandcompany.com



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

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

ISSN 2951-8180



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

Stakeholders.news

PORTFOLIO, PROGRAMME & PROJECT MANAGEMENT
NÚMERO #031 - SEPTIEMBRE 2024

PROYECTOS · GESTIÓN · EXCELENCIA · CALIDAD · PROFESIONALES



STAKEHOLDERS.NEWS
PROTAGONISTA DEL MES
RICARD MARTINEZ

INDIGESTIÓN DE PROYECTOS
CHANGE THE BUSINESS
con Javier Peris

RESILIENCIA Y TRANSFORMACIÓN DIGITAL (I)
ORGANIZACIONES RESILIENTES
con Juan Manuel Domínguez

MÁS ALLÁ DEL PLAN: CÓMO LA GESTIÓN DEL CAMBIO MARCA LA DIFERENCIA EN LOS PROYECTOS EL LADO HUMANO
con Charo Fresneda

SIN CORAJE SOMOS COMO UN TRONCO A LA DERIVA
PERSONAS Y PROCESOS
Luis Morán

LA EMPLEABILIDAD EN DIRECCIÓN DE PROYECTOS: ¿ESTUDIOS, UNA NECESIDAD IMPERIOSA? TRABAJO Y FUTURO
con José Luis Portela

EL PUENTE ENTRE DESASTRE Y PREVENCIÓN: ¿NORMATIVA O PROTOTIPO? TENDIENDO PUENTES
con José Antonio Puentes

PROPÓSITO PARA LA NUEVA TEMPORADA
PROYECTANDO EL FUTURO
con Juan Jesús Urbizu

RESETEO SUPER PMOs
con Ricardo Sastre

FROM COST CENTER TO REVENUE GENERATION (1 DE 2)
EL SALVADOR
con Luis Guardado

PUERTO RICO
PUERTO RICO
con Nesty Delgado

ITERANDO ENTRE EVALUAR Y MEJORAR URUGUAY
con Daniel Sorokins



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.



índice

DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



NUESTRO
INVITADO
A #TYSC

24

**José Manuel
Muñoz Vela**



FUTURO
Y SEGURIDAD

12

**Resiliencia organizacional
versus 40 kilobytes**



ES TENDENCIA

34

**Las telecomunicaciones son
tendencia en época de
alto consumo**



LA NUEVA
ADMINISTRACIÓN

46

**Una inteligencia
artificial que te hace
los informes**

Copyright

02

Índice de Contenidos

04

Este mes te recomiendo leer...

por JAVIER PERIS

07

¿PMO vs CoE? that is the question

EL GOBERNAUTA
JAVIER PERIS

08

Resiliencia organizacional versus 40 kilobytes

FUTURO Y SEGURIDAD
MANUEL SERRAT OLMOS

12

La Directiva NIS2 sigue pendiente de transposición

TECNOREGULACIÓN
EN PROSPECTIVA
NACHO ALAMILLO

16

NIS2 para directivos: claves y desafíos

DIARIO DE UNA
TORTUGA NINJA
JUAN CARLOS MURIA

20

José Manuel Muñoz Vela

NUESTRO INVITADO
A TYSC

24

Las telecomunicaciones son tendencia en época de alto consumo

ES TENDENCIA
MARLON MOLINA

34

¿Es la economía o el GDPR?

OJO AL DATO
RICARD MARTÍNEZ
MARTÍNEZ

38

La evolución de la Logística

AI FUTURO
MARCOS NAVARRO

42

Una inteligencia artificial que te hace los informes

LA NUEVA
ADMINISTRACIÓN
VÍCTOR ALMONACID

46

La guerra invisible contra los sistemas GNSS

RADIO SECURITY
ALEX ALIAGA

50

Desmontando mitos (2)

MENTES DIVERGENTES
MARTA MARTÍN

54

Javier García, director general de UNE, reelegido vicepresidente de ISO

NORMALIZACIÓN

58

#45 - OCTUBRE 2024

TYSC

#TYSC

Premios recibidos



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



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

itSMF
ESPAÑA

Premio 2022 ESET al Periodismo y Divulgación eb 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

a pep | Asociación Profesional Española de Privacidad

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.

 COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

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.

AVIS@
ASOCIACIÓN VALENCIANA DE INGENIERÍA SANITARIA

Smart
Board
Governance
for the AI
Revolution

Tim Glowa

Smart Board Governance for the AI Revolution

Tim Glowa

“*Smart Board Governance for the AI Revolution*” es una obra muy interesante para cualquier líder o directivo que quiera estar preparado para los desafíos de la inteligencia artificial. Tim Glowa logra explicar de manera clara y concisa cómo los consejos de administración deben adaptarse y evolucionar en esta nueva era tecnológica.

Una de las cosas que más me ha gustado es el enfoque práctico del libro. No se queda en la teoría, sino que ofrece herramientas y estrategias concretas que se pueden aplicar en el día a día. Además, utiliza ejemplos reales que hacen que las ideas sean más comprensibles y fáciles de llevar a cabo.

También me ha parecido muy acertado cómo el autor aborda el papel de la IA no como una amenaza, al que estamos sobradamente acostumbrados, sino

como un aliado para mejorar la toma de decisiones. Este enfoque positivo y colaborativo es un soplo de aire fresco en un tema que a veces puede generar resistencia o temor.

En definitiva, “*Smart Board Governance for the AI Revolution*” es una lectura muy valiosa para quienes, como yo, buscan estar al día con las últimas tendencias y quieren asegurarse de que las organizaciones estén preparadas para el futuro. Lo recomiendo sin duda a cualquiera que esté interesado en cómo la tecnología puede transformar el liderazgo y la gobernanza.

¿PMO vs CoE? that is the question

Que las organizaciones están cambiando su enfoque hacia el Cambio Organizacional es un hecho que nos debe alegrar a todos los que defendemos las Buenas Prácticas, pero no debe ocultar que ello es debido a los constantes fracasos y las enormes pérdidas económicas que están suponiendo adaptarse a estos tiempos donde el cambio es constante.

Si ánimo de abusar del “ya os lo decía yo” es evidente que las organizaciones se están dando cuenta que los mantras “falla rápido”, “lo importante es la acción” y “tú ves equivocándote” “si hay que pivotar se pivota” han pasado una factura inmensa tanto en términos de costes de recursos, como de costes de oportunidad lo que ha obligado a un reenfoque mas responsable a la hora de abordar no solo el cambio y la adaptación sino también la innovación.

En este punto es donde emergen de nuevo las estructuras organizativas mas incomprendidas y maltratadas de las que hasta el momento han aparecido en las organizaciones con el fin de aportar Buenas Prácticas, estamos hablando de los Centros de Excelencia CoE.

En relación al Cambio Organizacional y en lo que respecta a Proyectos, Programas y Portfolios, un Centro de Excelencia CoE es una unidad o función dentro de una organización que se encarga de establecer, desarrollar y compartir las mejores prácticas, metodologías y estándares, así como las experiencias, riesgos, lecciones aprendidas, casos de éxito e incluso casos de fracaso, así como la gobernanza asociada a estas áreas.

Seguramente se pensará que realmente estoy hablando de la Oficina de Proyectos PMO, pero no se puede estar más equivocado ya que ambas estructuras organizativas, aunque tienen funciones relacionadas, sus enfoques, alcances y objetivos son tremendamente diferentes.

Una Oficina de Gestión de Proyectos PMO es una estructura operativa cuyo objetivo es supervisar y controlar la gestión de proyectos, programas o portfolios en una organización. Su rol se centra en apoyar la ejecución mediante la estandarización

de procesos, metodologías y la mejora de la eficiencia operativa, pero su enfoque es táctico y operativo, asegurando la consistencia en la entrega de resultados, beneficios o nuevas capacidades y alineando los recursos necesarios para que sobre todo las iniciativas se completen con éxito.

El propósito principal de un Centro de Excelencia es mucho más ambicioso y mucho mas útil para el conjunto de toda la organización, su propósito consiste en proporcionar liderazgo en las mejores prácticas, llevar a cabo investigación y mantenimiento de estándares y metodologías en cada una de las disciplinas que abarca. Su enfoque es estratégico y de largo plazo, con una responsabilidad clave en la innovación, mejora continua y desarrollo de capacidades.

Como habrá podido observar el lector la diferencia más que notable es sobresaliente, estamos hablando de alcances distintos a diferentes niveles jerárquicos de decisión, y en lo que estaremos de acuerdo es que un Centro de Excelencia es lo que usted pensaba que era una PMO. Pero cuidado, no es meramente un cambio de nombre o denominación, no es cuestión de siglas, es algo muchísimo más profundo. Por ejemplo, una PMO no puede albergar todo el conocimiento, experiencias, buenas o mejores prácticas, artefactos y metodologías relacionadas con el Gobierno y la Gestión de la inteligencia Artificial, tampoco con el Gobierno y Gestión del Dato, y mucho menos con el Gobierno y la Gestión de Riesgos o la Gobernanza Corporativa, un Centro de Excelencia CoE por supuesto que sí, aun diría más es incluso su obligación y al hacerlo se convierte definitivamente en la piedra roseta de la organización, el Centro de Sabiduría de la Organización del cual beben las decisiones estratégicas y a través del cual se transmiten el liderazgo y la participación de todas las partes interesadas.



CONTINÚA EN
PRÓXIMA PÁGINA





Con esto no quiero decir que las Oficinas de Portfolios, Programas o Proyectos PMOs no promuevan la innovación y la mejora continua, hasta ahí podíamos llegar, pero a creo que a quedado suficientemente claro que las PMO sea cual sea su alcance, aunque promuevan la mejora, su enfoque principal es estandarizar las metodologías existentes para asegurar la consistencia en la gestión de proyectos, programas o portafolios y no suelen integrar la innovación a nivel estratégico, su ámbito queda circunscrito a mejoras operativas, en cambio son los Centros de Excelencia CoE por definición los que están orientados a la innovación y el desarrollo continuo, fomentando el uso de nuevas metodologías, herramientas, y enfoques para mejorar todos los procesos de la organización, estando a cargo incluso de la exploración de tendencias y la implementación de buenas o mejores prácticas existentes o emergentes en el mercado.

Respecto al horizonte temporal también existen importantes diferencias, un Centro de Excelencia CoE funciona con un horizonte de largo plazo, buscando el desarrollo continuo de capacidades y la optimización estratégica, no está atado a los ciclos de vida de proyectos o programas específicos, sino que busca el desarrollo sostenido del conjunto de la organización, englobando a lo largo y ancho de la organización y en la dimensión del conjunto de todas las disciplinas existentes.

Por el contrario, las PMO suelen operar con un horizonte más a corto o mediano plazo, enfocado en la ejecución y finalización exitosa de proyectos, programas o portafolios dentro de sus plazos específicos.

En resumen, tenga claro que un Centro de Excelencia CoE se enfoca como su nombre indica en la excelencia organizativa y por tanto en desarrollar capacidades estratégicas a largo plazo mientras que una PMO se centra más en la ejecución diaria y la gestión operativa de proyectos, programas o portafolios. Ambos son perfectamente complementarios dentro de una organización que gestiona múltiples proyectos y busca alinear sus resultados con los objetivos estratégicos.

Muy pronto verán la luz nuevos estándares basados en el Gobierno y Gestión de Centros de Excelencia, con especial énfasis en áreas muy concretas que son tendencia y para las que hay que aprovechar las grandes oportunidades que nos presenta esta era digital y donde debemos evitar el retrabajo, el error reiterado, el desperdicio aprovechando las lecciones aprendidas, la experiencia, las oportunidades y el valor ganado y nadie como un Centro de Excelencia CoE para erigirse como exhaustivo elemento afinador de todos y cada uno de los instrumentos que componen esa orquesta sinfónica que es la organización facilitando que se deje definitivamente de hacer ruido y bajo la batuta de la Alta Dirección suene como siempre se ha soñado que debía sonar.

Este atento porque una vez más España va a ser pionera en estandarización como lo fue en Gestión del Tiempo y de la Productividad, en este caso en un área tan importante como es la Excelencia y un consejo, a partir de ahora cuando le ofrezcan Oficinas de Proyectos, si lo que de verdad quiere es lograr niveles insospechados de rentabilidad y eficacia pida siempre Centros de Excelencia CoE.



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, Kanban, Design Thinking, Scrum & AgileSHIFT® Accredited Trainer ejerce como Business Coach, Business Angel e Interim Manager.

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

Escuela de Gobierno

eGov®

<https://escueladegobierno.es>

Curso de Doble
Certificación en:

Gobierno y Gestión de la Inteligencia Artificial

ISO 38507:2022

ISO 42001:2023

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 42001 Leader
- Certificación ISO 38507 Leader
- Solicita tu admisión

MPPM®

MGEIT®

eGov®

Próxima Convocatoria en Directo

Septiembre 2024

Solicita tu admisión en:



+ 34 96 109 44 44

campus@escueladegobierno.es

Manuel Serrat Olmos

Resiliencia organizacional versus 40 kilobytes

¿Pueden 40 kilobytes poner en riesgo la continuidad de la sociedad digital? ¿Puede un incidente de seguridad afectar tanto como para que nuestras organizaciones tengan que volver al papel y al bolígrafo? ¿Realmente ese es el nivel de resiliencia digital que nuestra sociedad tiene? El incidente con CrowdStrike del 19 de julio de 2024 nos ha de hacer pensar en si realmente no estamos construyendo una sociedad digital con unos cimientos extremadamente débiles.

Llevamos bastantes años escuchando hablar de transformación digital, digitalización de las organizaciones y de la ciudadanía, de mercados digitales, de comercio electrónico, de criptomonedas, etc. En general, de aquello que bien podríamos llamar Sociedad Digital Global, cuyas bondades glosaban los voceros, donde ríos de leche y miel digital iban a inundarnos a todos.

En muchos de nuestros artículos hemos planteado que a esta Sociedad Digital Global la amenazan los cibercriminales de toda índole y nacionalidad, frente a los que las diferentes jurisdicciones tienen dificultades para actuar, por cuestiones de extraterritorialidad, por ejemplo, o por la dificultad en la atribución de los delitos, o porque se tratan de mafias organizadas, y en ocasiones, esponsorizadas por estados. Por todo ello, la necesidad de una adecuada ciberseguridad ha captado la atención por parte de las empresas, los poderes públicos y los ciudadanos, ignorantes de las amenazas a las que están expuestos, e indefensos en la mayoría de los casos, ante este tipo de actividades criminales, y deseosos de que nada destruya la confianza en los mercados digitales.

Una de las más recientes iniciativas europeas al respecto fue la aprobación, en 2022, de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, conocida popularmente como Directiva NIS2, y cuya transposición al derecho español debería hacerse antes de mediados de octubre de 2024. El espíritu de esa norma es lograr algo que, en ocasiones, los expertos en ciberseguridad tendemos a obviar, y es el concepto de **ciberresiliencia**, que podríamos definir como *la capacidad de un sistema de información de resistir frente un determinado evento potencialmente catastrófico, aunque sea de forma degradada*. Por la coyuntura actual, se ha tendido a

reducir la ciberresiliencia a poder enfrentar ataques de tipo ransomware, virus, intrusiones en los sistemas o ciberestafas, por citar algunos, olvidando otras situaciones que pueden suponer un riesgo para los sistemas de información.

Sin embargo, el pasado 19 de julio de 2024 se produjo un evento que demostró con nítida claridad los problemas de ciberresiliencia que aquejan a esa Sociedad Digital Global, afectando a todo tipo de organizaciones por todo el planeta y paralizando sus operaciones. Y ello, con un simple fichero de 40 kilobytes, puesto en el lugar inadecuado en el momento incorrecto.

Poco después de las 6 de la mañana, hora española, AENA informaba de un fallo en sus sistemas que le impedía operar con normalidad. Se presumió rápidamente un posible ciberataque, pero en un muy breve espacio de tiempo, se desechó la teoría del ciberataque y comenzaron las sospechas de que algún componente de una actualización de algún producto ampliamente utilizado estaba provocando que sistemas basados en Microsoft Windows se reiniciaran continuamente. El primer señalado fue el propio sistema operativo Windows, pero pronto se vio que no era ese el origen del incidente, sino una actualización del producto antivirus Falcon, de la compañía estadounidense CrowdStrike, y que provocaba el reinicio de aquellos sistemas donde las actualizaciones de ese producto estaban configuradas para aplicarse automáticamente.

Los sistemas afectados fueron de todo tipo, y en organizaciones de muy variada naturaleza: compañías aéreas, bancos, hoteles, industrias, etc. Su 'cadena del dolor' quedó meridianamente clara poco antes de las 8 de la mañana, y entonces había que investigar cómo resolverlo con carácter urgente.

Los sistemas basados en otros sistemas operativos, o protegidos con otros antivirus, o simplemente, no teniendo activadas las actualizaciones automáticas de Falcon, no se vieron afectados, salvo quizá por el hecho de que dependiesen de sistemas que sí que hubieran resultado afectados por el incidente.



CONTINÚA EN
PRÓXIMA PÁGINA



国际出发 International Departures
 港澳/台出发 HK/Macao/Taiwan Departures
 国内登机 Domestic Boarding

国际出发 International Departures
 港澳/台出发 HK/Macao/Taiwan Departures
 国内登机 Domestic Boarding

国内登机 Domestic Boarding
 国内登机 Domestic Boarding

国内登机 Domestic Boarding
 国内登机 Domestic Boarding





Aviones en tierra, vuelos cancelados, pasajeros teniendo que ser realojados, facturación aeroportuaria haciéndose con papel y bolígrafo, datáfonos desconectados, y un largo etcétera de efectos provocaron un caos internacional de proporciones desconocidas hasta la fecha. Y todo ello debido a un fichero de 40 kilobytes que no debería estar en la actualización. La situación puso de manifiesto la fragilidad de los sistemas sobre los que se basa la Sociedad Digital Global, y la escasa ciberresiliencia que presenta. No fue un ataque orquestado desde el Eje del Mal. Fue una simple actualización mal hecha sobre un producto masivamente usado en sistemas de alta criticidad.

Alrededor de las 10 horas, ya circulaban ciertas 'recetas' para resolver el problema, y durante el resto del día los administradores de los sistemas afectados se centraron en aplicarlas para devolver a la normalidad las operaciones de las organizaciones afectadas. Pero en el mundo real, las personas acababan de experimentar lo que podría haber sido un evento que marcara el fin de nuestra civilización, si se nos permite la exageración.

Resuelto el problema tecnológico y restaurados los servicios, quedaba sacar las oportunas conclusiones. La más obvia es que nuestra Sociedad Digital Global es un sistema complejísimo, por la interdependencia entre sistemas, y la complejidad intrínseca de muchos de ellos, que unido al hecho de las presiones competitivas, hace que se concentre en un puñado de soluciones la oferta en ciertos nichos de mercado, convirtiendo a esa Sociedad Digital Global en un gigante con los pies de barro, en el que una simple actualización mal hecha provoca cientos, si no miles de millones de dólares de impacto económico a nivel mundial. Coincidirán con nosotros en que lo que es confianza, no da precisamente.

Tras el evento, se produjeron tres situaciones que merece la pena resaltar:

1. Los ciberdelincuentes aprovecharon el evento para lanzar campañas maliciosas, con supuestas soluciones al problema de

Crowdstrike, con el efecto final de amplificación del mismo. A rio revuelto, ganancia de pescadores.

2. La compañía, tras pedir disculpas en redes sociales a través de su CEO, publicó un informe preliminar oficial sobre el incidente, y planteó compensar a los afectados con un vale de 10 dólares para pedidos en Uber Eats, cuestión que terminó de indignar a quienes directa o indirectamente, se han visto perjudicados por el incidente. Bastantes días después, publicaron un magnífico informe explicando el incidente con detalle.

3. Microsoft cargó la responsabilidad del incidente en las normas antimonopolio de la Unión Europea, que le obligaron a dar acceso al kernel de Windows a diferentes fabricantes de software.

A partir del momento en que se tranquilizó el sector, comenzó un debate que sí resulta realmente interesante, en torno a la pregunta de cómo podemos mejorar esa resiliencia. Una de las lecciones aprendidas del incidente de Crowdstrike es que nuestros servicios han de disponer de redundancia no sólo numérica o geográfica, como es habitual, sino, a ser posible, en cuanto a sus componentes. La otra lección aprendida es que en el sector de la ciberseguridad hemos desdeñado la ciberresiliencia para centrarnos exclusivamente en los ciberataques activos, lo que nos ha llevado a la especialización del personal en ese ámbito, y ha comportado que en algunas organizaciones se hayan priorizado las inversiones en esa faceta y no en otras relacionadas con la resiliencia. Con ello, perdemos de vista una cuestión fundamental: **las organizaciones actuales dependen totalmente de la tecnología, y por tanto, serán tan resilientes como lo sean sus sistemas tecnológicos.** Cabe, por tanto, optar por la ciberresiliencia, que incluye todos aquellos aspectos de la ciberseguridad 'chic', pero que también tiene en cuenta aspectos como la seguridad física, la redundancia de sistemas y la tolerancia a fallos. En caso contrario, éste incidente del 19 de julio de 2024 puede ser sólo el primero, y cada vez los impactos pueden ser mayores.



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>

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>

Curso de Doble
Certificación en:

Gestión Documental y Gestión del Conocimiento

ISO 30301:2021

ISO 30401:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 30300 Leader
- Certificación ISO 30401 Leader
- Solicita tu admisión

MPPM®

MGEIT®

eGob®



Próxima Convocatoria en Directo

Septiembre 2024

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

La Directiva NIS2 sigue pendiente de transposición

De forma lamentable, el 17 de octubre entrará en vigor la Directiva NIS2 (), que se encuentra pendiente de transposición al ordenamiento jurídico español, generando una innecesaria inseguridad jurídica a las entidades sujetas a su ámbito de aplicación, en especial aquellas que no se encontraban sujetas a la Directiva NIS –Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión–, transpuesta por Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (RDLSRI).

La Directiva NIS2 contiene importantes innovaciones con respecto a la normativa actualmente vigente, al objeto de reforzar la política de la Unión en este ámbito.

En primer lugar, se amplía el ámbito de aplicación con nuevos sectores basados en su grado de digitalización e interconexión y en su importancia para la economía y la sociedad, introduciendo una norma de umbral de tamaño claro, lo que significa que todas las empresas medianas y grandes de los sectores seleccionados quedarán sujetas. Adicionalmente, los Estados miembros pueden identificar entidades más pequeñas con un perfil de alto riesgo para la seguridad, de modo que queden sujetas a las obligaciones legales.

Resulta muy significativa la ampliación de las entidades del sector de infraestructura digital, incluyendo proveedores de redes de servicios de computación en la nube, proveedores de distribución de contenidos, prestadores de servicios de confianza, proveedores de servicios de centro de datos y proveedores de redes públicas de comunicaciones electrónicas, así como servicios de comunicaciones electrónicas disponibles para el público, o la inclusión del sector de gestión de servicios de TIC (de empresa a empresa), con proveedores de servicios gestionados y proveedores de servicios de seguridad gestionados. Otros sectores novedosos incluyen los servicios postales y de mensajería, la gestión de residuos, la fabricación, producción y distribución de sustancias y mezclas químicas, la producción, transformación y distribución de alimentos y determinados subsectores del sector de fabricación, lo que muestra la importancia de que dichas entidades conozcan y puedan cumplir sus obligaciones jurídicas.



CONTINÚA EN
PRÓXIMA PÁGINA





A diferencia de la normativa actual, las entidades sujetas se clasifican en función de su importancia y se dividen en dos categorías: entidades esenciales e importantes, sujetas a diferentes regímenes de supervisión.

Entre otras, son entidades esenciales las grandes empresas de los sectores de alta criticidad; independientemente de su tamaño, los prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel y los proveedores de servicios de DNS; y las medianas empresas proveedoras de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público, en una muestra más de la creciente dependencia en estos servicios. Asistimos, de este modo, a una verdadera convergencia en la política de ciberseguridad.

La normativa fortalece y racionaliza los requisitos de seguridad y presentación de informes por las entidades mediante la imposición de un enfoque de gestión de riesgos, que proporciona una lista mínima de elementos básicos de seguridad que deben aplicarse; así como se introduce disposiciones más precisas sobre el proceso de notificación de incidentes, el contenido de los informes y los plazos.

Además, y esta es la segunda gran novedad a la que me voy a referir, la Directiva NIS2 aborda la seguridad de las cadenas de suministro y las relaciones con los proveedores, exigiendo a las empresas que aborden los riesgos de ciberseguridad

en las cadenas de suministro y en las relaciones con sus proveedores.

Precisamente por su importancia, la Directiva exige a la Comisión antes del 17 de octubre de 2024 adoptar actos de ejecución por los que se establezcan los requisitos técnicos y metodológicos de las medidas de seguridad con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, y los prestadores de servicios de confianza.

La ausencia de transposición de la Directiva NIS2 dentro del plazo establecido genera una fuerte inseguridad jurídica, que sólo se ha visto parcialmente mitigada por la publicación, por el CCN-Cert, de la Guía CCN-STIC 892, con un perfil de cumplimiento específico del Esquema Nacional de Seguridad, que con una alta seguridad será adoptado por entidades formalmente no sujetas al mismo.

Confiamos en que, siquiera mediante la criticable técnica del Real Decreto-Ley, veamos cumplida a la mayor brevedad la imprescindible modificación del RDL



NACHO ALAMILLO

Es Doctor en Derecho por la Universidad de Murcia. Licenciado en Derecho por la UNED. Auditor de Sistemas de Información certificado, CISA. Director de Seguridad de la Información certificado, CISM. Ingeniero Certificado en Soluciones de Protección de Datos, CDPSE, por ISACA.

En la actualidad, es Abogado del Ilustre Colegio de Reus, Asesor de Logalty y Director General de Astrea La Infopista Jurídica SL. Asimismo, colabora con el Grupo de Investigación iDerTec de la Universidad de Murcia.

También es miembro del grupo de Infraestructura de Seguridad de Firma Electrónica del Instituto Europeo de Normas de Telecomunicaciones, que normaliza los servicios de confianza, miembro de UNE CTN71/SC307, de CEN-CLC/JTC 19 y de ISO TC 307, relativos a Blockchain.

Dispone de más de 100 publicaciones y ha impartido más de 400 ponencias en identidad digital, servicios de confianza y materias relacionadas.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>

Curso de Doble
Certificación en:

Inteligencia Estratégica y Gestión de la Innovación

ISO 56002:2019
ISO 56006:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 56002 Leader
- Certificación ISO 56006 Leader
- Solicita tu admisión

MPPM®

MGEIT®

eGob®

Próxima Convocatoria en Directo

Septiembre

Solicita tu admisión en:



+ 34 96 109 44 44
campus@escueladegobierno.es



DIARIO DE UNA TORTUGA NINJA

Juan Carlos Muria

“

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



NIS2 para directivos: claves y desafíos

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

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

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

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



**CONTINÚA EN
PRÓXIMA PÁGINA**



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

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

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

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

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

mencionados específicamente en NIS2 por considerar que contienen entidades esenciales o de alta criticidad son: energía, transporte, banca, infraestructuras de mercados financieros, sector sanitario, agua potable, aguas residuales, infraestructura digital, gestión de servicios TI entre empresas, entidades de administración pública (excepto poder judicial, parlamentos y bancos centrales) y el sector espacial.

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

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



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/>

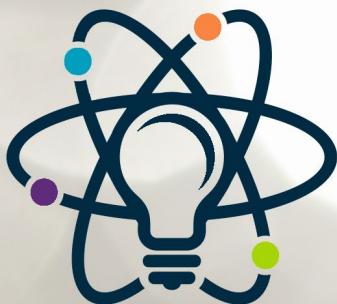
Twitter:
<https://twitter.com/juancarlosmt>

P4MGO! Pfm

**Portfolio Management
Portfolio Governance
Portfolio Offices**

Alcanza tu propósito organizacional y asegura tus objetivos estratégicos de manera ágil, dinámica y elástica con **P4MGO!® Pfm**

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

José Manuel Muñoz Vela

“Uno de los mayores expertos en Derecho de Inteligencia Artificial en Europa y uno de los principales a nivel mundial”. Así fue presentado nuestro protagonista en este número durante la jornada sobre IA que se organizó el pasado 27 de septiembre en la bolsa.

Calificativos que nuestro protagonista agradece desde la modestia y que justifica en el cariño personal de quienes les precedieron en la palabra, pero lo cierto es que José Manuel Muñoz Vela es un abogado valenciano de reconocido prestigio en el ámbito del Derecho Tecnológico y Digital dentro y fuera de nuestras fronteras, con una trayectoria profesional de 25 años de experiencia profesional, y lo es más si cabe en IA, materia sobre la que ha destacado durante los últimos años, no sólo en el ámbito profesional, sino también en el ámbito de la investigación científica y la divulgación.

José Manuel Muñoz es Licenciado y Doctor en Derecho por la Universidad de Valencia con honores Cum Laude y Premio Extraordinario de Doctorado por la misma por su tesis doctoral titulada *“Derecho de la Inteligencia Artificial: Un enfoque global de responsabilidad desde la ética, la seguridad y las nuevas propuestas reguladoras europeas”*, a la que adiona el reconocimiento a su actividad profesional y la prolífica actividad de investigación y divulgación en esta materia, con múltiples monografías y artículos de investigación publicados en materia de IA en editoriales como Aranzadi Thomson Reuters, Wolters Kluwer o Tirant Lo Blanch.

Durante su trayectoria su formación ha sido híbrida, tanto en el ámbito jurídico como tecnológico, habiendo cursado distintos másters y programas especializados en entidades de educación superior nacionales y extranjeras, como el Instituto de Empresa (IE University), el Blockchain Law Institute (BI) o el Massachusetts Institute of Technology (MIT). Asimismo, ostenta las certificaciones profesionales internacionales más prestigiosas en el ámbito

tecnológico en las áreas de gobierno, auditoría, seguridad, gestión de riesgos y privacidad, como CISA, CISM, CGEIT, CRISC o CDPSE, en las que ha dirigido proyectos del más alto nivel nacional e internacional, así como otras nacionales como DPD o ACP.

Del mismo modo, ha sido reconocido con múltiples reconocimientos y premios, entre otros y más recientes, fue reconocido en los Premios Tomás y Valiente 2021 por su investigación sobre IA y seguridad, posteriormente fue nominado al Premio como Mejor Investigador en Derecho Digital 2021, recibió el premio ISACA de investigación 2022 y recibió el 1º Premio Nacional de Investigación Jurídica García Goyena 2023.

José Manuel compagina su actividad profesional, con la docencia y la investigación en materia de Derecho Digital e Inteligencia Artificial, siendo ponente habitual en estas materias en congresos nacionales e internacionales. Del mismo modo, colabora docentemente en múltiples universidades y entidades de formación superior, como la Universidad de Valencia, la Universidad Politécnica de Valencia, la Universidad Internacional de Valencia, la Universidad de Barcelona, la Universidad de Alicante, la Universidad CEU-Cardenal Herrera, la Universidad Europea de Valencia o ESAT, así como en masters y posgrados organizados por entidades como el Ilustre Colegio de Abogados de Valencia, el Ilustre Colegio de Abogados de Barcelona, Cámara de Comercio, la Fundación de Estudios Bursátiles y Financieros o el Blockchain Law Institute.

Una referencia en Derecho Digital e IA, que evidencia el enorme talento que tenemos en nuestro país y en Valencia en particular.



CONTINÚA EN PRÓXIMA PÁGINA





REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Nuestro invitado a #TYSC



TECNOLOGÍA Y SENTIDO COMÚN

#TYSC / PÁG. 26

Pero, ¿quién es José Manuel Muñoz Vela además de profesional, docente e investigador?

Pues verdaderamente un tipo bastante sencillo, que también es padre, marido, hijo, amigo y compañero incondicional, que es de lo que más orgulloso se siente y que intenta ser mejor persona cada día -contesta.

¿Háblanos de tus últimos éxitos o logros profesionales?

Lo cierto es que estos últimos años han sido muy dulces en el ámbito profesional y de investigación, y por supuesto no puedo ocultar mi infinito agradecimiento ante los reconocimientos y premios que han llegado, pero sin duda, la mayor satisfacción para mí es, de un lado, levantarme todos los días con nuevos retos y poder seguir trabajando en estas áreas de especialización que tanto me apasionan y, de otro, los pequeños reconocimientos que mejor saben en forma de palabras de agradecimiento de un cliente, un lector, un alumno o un asistente a una conferencia.

Trabajas intensamente en regulación y en materia digital, háblanos de esto.

Nos hallamos ante un verdadero tsunami regulatorio en la UE en el ámbito digital. Durante los últimos meses estamos escuchando demasiadas veces eso de que "EE.UU. innova, China copia y fabrica, y Europa regula". No puedo compartir esta afirmación, en la medida que China también innova, al igual que Europa, si bien, la carrera por liderar tecnologías como IA o Blockchain está siendo encabezada por EE.UU. y China. En cualquier caso necesitamos regulación y más que nunca.

Es cierto que en tecnología el "ahora" es "antes", el "hoy" es "ayer", a diferencia del Derecho, si bien, en innovación, desarrollo tecnológico y competitividad en los mercados no todo puede valer. Innovar significa romper cosas, pero deben existir unos límites, entre otros, el respecto de los derechos fundamentales.

Eso de "no podemos poner puertas al campo" en el sentido de que no podemos poner límites al despliegue y uso de la tecnología, no lo comparto. Por supuesto que debemos poner líneas rojas a la tecnología, y el Derecho,

esto es, el ordenamiento jurídico, está para eso, para ordenar jurídicamente el desarrollo, despliegue y uso de la tecnología, de modo que se asegure su seguridad, su fiabilidad, su accesibilidad o el respeto de los derechos fundamentales, entre otros aspectos. Un ejemplo lo tenemos claramente en la IA. El único problema es que regular en tecnología requiere nuevas técnicas legislativas e identificar los riesgos que puede suponer una regulación excesiva o, por el contrario, insuficiente, con la correlativa dificultad para el legislador de conseguir el deseable equilibrio dinámico, en constante tensión, entre innovación, desarrollo tecnológico y competitividad, de un lado, y seguridad, fiabilidad, ética, accesibilidad o protección de los derechos fundamentales, de otro.

El reciente informe Draghi destaca que existen más de 100 leyes sobre tecnologías de la información junto con más de 270 reguladores activos en el Mercado Único, significando el posible efecto no deseado de todo ello, entre otros, el efecto disuasorio para que las empresas hagan negocios en la UE a través de filiales, ante los diversos requerimientos, multiplicidad de agencias reguladoras y a la cierta sobrerregulación por parte de las autoridades nacionales.

Llevas a cabo una intensa labor de publicación de documentos, libros, etc. Eres posiblemente el autor con más monografías y artículos de investigación en materia de IA tanto a nivel nacional como europeo en este momento, e incluso me atrevería a decir que a nivel internacional. Hablemos de ella.

Lo cierto es que estos últimos 3 años han sido muy intensos, pero han sido sumamente provechosos en el ámbito profesional y de investigación, en la medida que el análisis y profundización que cada día me exige mi actividad profesional en aspectos de IA, como al abordar cualquier aspecto jurídico relacionado con la misma en el ámbito de la investigación, me enriquece bidireccionalmente en ambas dimensiones y sólo así puedo compaginar las mismas.



**CONTINÚA EN
PRÓXIMA PÁGINA**

Abordar una realidad tan compleja como la IA desde una perspectiva global, jurídica, técnica y de seguridad, me ha permitido tratar con profundidad muchos de sus principales desafíos jurídicos y riesgos, así como como su seguridad, y aspectos relaciones con la confidencialidad, la privacidad, los derechos de propiedad intelectual e industrial o la responsabilidad derivada de su uso y funcionamiento.

Revisando sus últimos libros, monografías y artículos de investigación publicados en el ámbito de la IA en estos últimos años, veo que su actividad ha sido intensa, entre otros, "Cuestiones éticas de la Inteligencia Artificial y repercusiones jurídicas. De lo dispositivo a lo imperativo" (Aranzadi Thomson Reuters), "Inteligencia artificial y responsabilidad penal" (Wolters Kluwer), "Retos, riesgos, responsabilidad y regulación de la inteligencia artificial. Un enfoque de seguridad física, lógica, moral y jurídica" (Aranzadi Thomson Reuters), "Inteligencia artificial y Cuestiones de propiedad intelectual e industrial" (Aranzadi Thomson Reuters), "Avanzando en la regulación de la IA. Hacia un equilibrio entre ética, protección de los derechos fundamentales, seguridad, confianza, innovación, desarrollo y competitividad" (Wolters Kluwer), "IA y responsabilidad civil. Comentarios a las propuestas europeas en materia de derechos de daños por productos defectuosos y adaptación de las normas de responsabilidad civil extracontractual" (Aranzadi Thomson Reuters), "Inteligencia artificial y derecho de autor. Creaciones artificiales y su protección jurídica" (Tirant Lo Blanch), "Inteligencia artificial generativa. Desafíos para la propiedad intelectual" (Premio García Goyena) o "Retos, riesgos y responsabilidad de la inteligencia artificial" (FEBF).

Y acaba de publicar esta misma semana un nuevo libro: "La regulación de la inteligencia artificial. Reto y oportunidad desde una perspectiva global e internacional", con la editorial Aranzadi. ¿Debe regularse la IA?

Este es precisamente el objeto de esta obra, abordar la necesidad de regular la IA, los posibles mecanismos para hacerlo a fin de garantizar una IA segura y fiable, así como las principales iniciativas legislativas a nivel internacional y las claves del nuevo Reglamento

IA de la UE. Los enfoques reguladores son muy distintos a nivel internacional, desde un enfoque tradicionalmente más pro-innovación y basado en la autorregulación como Reino Unido o Israel, a un enfoque más proteccionista de los valores europeos y los derechos fundamentales como el enfoque de la UE.

A lo largo del mismo, abordo los principales desafíos y riesgos jurídicos de la IA, las principales estrategias gubernamentales y supranacionales ante la misma, marcos éticos actuales, su regulación internacional y su estado actual en países como EE.UU. y algunos de sus Estados, Canadá, Chile, Brasil, Colombia, Argentina, México, Perú, Reino Unido, Turquía, África, Israel, Rusia, China, India, Bangladesh, Indonesia, Japón, Singapur, Corea del Sur, Vietnam, Emiratos Árabes Unidos, Arabia Saudita, Australia, Nueva Zelanda o España, pero con especial detalle sobre el Reglamento IA de la UE. También abordo su regulación contractual y sectorial, su normalización y estandarización, y los retos y riesgos de su propia regulación, para concluir con mi posicionamiento sobre la oportunidad y necesidad de regularla y de hacerlo también a nivel global mediante acuerdos y convenios internacionales.

¿Cómo fueron tus comienzos como abogado?

Pues lo cierto es que empecé en estos temas "recién salido del horno". Una vez finalizada mi licenciatura en derecho, realicé el Programa de Práctica Jurídica en la Real Academia de Jurisprudencia y Legislación, durante el cual realicé mi "pasantía" en un despacho de referencia en Valencia, si bien, al año me concedieron una beca de cooperación tecnológica empresarial por parte del IMPIVA (ahora IVACE) que me permitió meterme de lleno a trabajar en proyectos de innovación y cooperación tecnológica transnacionales, y ya entonces empecé a fraguar lo que acabó siendo mi primera firma como boutique legal en Derecho Digital bajo la marca "LegalTech", palabra de moda dos décadas después y hasta la fecha, pero que en los años 1996 y 1997 era novedosa y muy disruptiva.



CONTINÚA EN
PRÓXIMA PÁGINA





REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Nuestro invitado a #TYSC

De hecho, recuerdo anecdóticamente ser invitado por la Universidad de Valencia para presentar mi proyecto profesional como un caso de éxito universitario en un congreso organizado por la misma, si bien, en aquella época, apenas ganaba lo suficiente ni para pagar el alquiler del despacho.

En aquellos años era considerado un “bicho raro” en nuestra profesión, pero empecé ya a trabajar con empresas de informática y sectores como el videojuego.

Nunca he dejado, ni entonces ni ahora, de cuidar mi formación continua jurídica y tecnológica, y de hecho, inicié mi doctorado en Madrid en el primer y único programa entonces en Derecho TIC, realizando mi período de docencia e investigación doctoral con quienes entonces eran la referencia en Derecho Informático en nuestro país, como Javier Cremades, Xavier Ribas, Miguel Ángel Davara o Miguel Ángel Ramos, defendiendo mi tesina sobre Auditoría de Cumplimiento TI y obteniendo el Diploma de Estudios Avanzados doctorales (DEA) previos a mi tesis. Sin embargo, la vida me puso una zancadilla en aquello que más nos puede doler a los que somos padres, y que durante años me obligó a centrarme exclusivamente en mi familia y en mi actividad profesional hasta que las cosas fueron lenta y progresivamente mejorando, lo que me permitió acometer con fuerza mi tesis doctoral con posteridad sobre IA.

Decidí entonces establecer mi sede profesional en esta maravillosa ciudad que es Valencia, mi ciudad, constituyendo la firma actual de la que soy socio fundador junto con mi compañero de fatigas, Ricardo Bonafont. Durante estos años mi actividad profesional ha sido incesante en nuestras áreas de actividad con clientes tanto nacionales como internacionales, y hemos ido creciendo aunque de una manera muy distinta a otras firmas, conformando actualmente una microcorporación con tres sociedades que integran el fantástico equipo de profesionales y mejores personas que constituyen, junto a nuestros clientes, los activos más importantes que tenemos, salvaguardando siempre el rasgo diferenciador de *boutique legal* especializada que nos caracteriza desde un inicio.

¿En qué áreas del derecho te encuentras más cómodo?

Dirijo el área de Derecho Digital y Tecnológico en la corporación, que habitualmente se identifican como sinónimos, pero no lo son, en la medida que no toda la tecnología es digital. Pensemos en la rueda, por ejemplo. Hoy, el área que dirijo incluye aspectos como contratación digital, mercados y servicios digitales, IA, informática, realidad aumentada, virtual y mixta, mundos virtuales, videojuegos, ocio interactivo, audiovisual, influencers, propiedad intelectual e industrial, ciberseguridad o privacidad.

¿De qué te sientes más orgulloso en tu carrera profesional?

De trabajar en aquello que me gusta y me apasiona, a pesar de los distintos y exigentes retos que nos puede plantear cada día.

¿Qué es lo que cambiarías del mundo del derecho?

¿Cuánto tiempo dispongo para responderte?. Muchas cosas. Desde luego considero que debe cambiar en enfoque y las técnicas del legislador, especialmente cuando pretende regular una tecnología en constante evolución y cambio como la IA. Si como decía Stephen Hawking, “la inteligencia es la habilidad de adaptarse a los cambios”, el legislador actual debe ser más inteligente que nunca y hallarse debidamente cualificado para ejercer un poder tan grande. El legislador debe combinar de manera inteligente lo que denominamos el *hard law* (imperativo) con el *soft law* (principalmente con origen en la autorregulación corporativa y sectorial, y de carácter dispositivo), elaborando nuevas normas flexibles que incorporen opciones que les permitan adaptarse con agilidad y rapidez a los sucesivos cambios sin necesidad de pasar por complejos y largos procesos legislativos. Y desde luego, legislar sobre tendencias más que sobre novedades ante la asincronía entre el Derecho y la Tecnología.



CONTINÚA EN
PRÓXIMA PÁGINA





REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



¿Qué es lo que se está haciendo mal y debería cambiarse?

Gobernar, legislar o juzgar no son tareas fáciles, si bien, en el ámbito legislativo, por ejemplo, hemos visto en la tramitación del Reglamento IA de la UE o de la Propuesta de Directiva reguladora de la responsabilidad civil de la misma, como la presión de la industria de la IA ha afectado al objeto y alcance de las normas en contra de las posiciones de expertos y ciudadanía, propiciando múltiples cambios durante su tramitación. Por otra parte, deben legislarse para la diversidad, de modo que no se ahogue a *pymes* y *startups*.

¿Qué es lo que se podría hacer bien y debería potenciarse?

Desde luego escuchar a todas las partes interesadas, potenciar el diálogo internacional y conseguir el compromiso firme de la industria pero también de los sectores público y privado usuarios. En materias como la IA, considero necesaria la creación de una agencia internacional y la promoción de acuerdos y tratados internacionales, al margen del necesario compromiso de la industria.

¿Qué consejos le darías a los directivos o profesionales que se niegan a tomarse en serio la regulación o el derecho?

La regulación legal tiene como principal objetivo ordenar jurídicamente relaciones, garantizando los derechos e intereses de las distintas partes implicadas. La conformidad regulatoria con los marcos legales a los que esté sujeta cualquier organización debe constituir un objetivo estratégico de cualquier organización asociado a la consecución de sus objetivos de negocio, su continuidad, su imagen corporativa, su responsabilidad social empresarial o la sostenibilidad. Somos todos una parte de un todo. Y todo ello, sin entrar en las responsabilidades directivas previstas en los nuevos marcos regulatorios como la Directiva NIS2 en materia de ciberseguridad que será exigible a partir del 17 de octubre.

¿Y a los recién llegados, startups emprendedores que están comenzando?

Los proyectos necesitan recursos para su consecución y todos hemos empezado con recursos limitados en los que hemos tenido que tomar decisiones y priorizar. Ahora bien, la priorización absoluta del negocio por encima de cualquier otra cosa no es factible. Tengo claro que innovar y emprender exige ser disruptivo, comporta riesgos y a veces romper cosas, pero cualquier proyecto empresarial debe ir adecuadamente acompañado desde el área legal desde el inicio para contribuir a tomar las decisiones e implementar las acciones más diligentes y razonables en cada momento. Apoyamos desde un inicio a todo tipo de startups tecnológicas, en lo bueno y en lo malo. No todas superan las primeras fases y alcanzan su consolidación, crecimiento e internacionalización. En ocasiones, las cosas pueden no ir bien y hay que tomar las decisiones adecuadas en el momento preciso, incluyendo la declaración de concurso. Ser empresario y estar en el mercado exige estar preparado y asumir que las cosas pueden ir bien, regular o mal, pero siempre acompañado legalmente en todo momento para tomar las mejores decisiones en cada momento.

Conclusiones

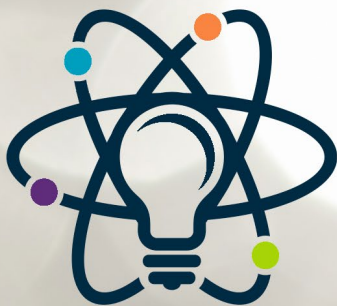
Tecnologías como la IA ya están cambiando el mundo que hoy conocemos y lo hará en mayor medida en los próximos años. La IA es una tecnología estratégica de alto impacto y enorme potencial disruptivo y habilitador incuestionables en todo tipo de sectores y actividades. No obstante, espero que esta no sea la era de la inteligencia artificial sino de la inteligencia humana, para lo que necesitaremos el adecuado ordenamiento y acompañamiento ético y jurídico.

P4MGO! PgM

Programme Management Programme Governance Programme Offices

Alcanza nuevas capacidades organizativas y asegura la obtención de beneficios de manera ágil, dinámica y elástica con **P4MGO!® PgM**

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Las telecomunicaciones son tendencia en época de alto consumo

En los últimos tres años las empresas de telecomunicaciones han invertido 500.000 millones de euros en mejorar y ampliar las redes. El lugar y el rol que juegan las teleoperadoras sigue siendo un enigma, y estas empresas siguen quejándose por proponer las carreteras que son la base de las TIC y no participar del pastel importante de la economía digital.

El consumo de vídeo, las redes sociales, y ahora la inteligencia artificial generativa están haciendo un uso intensivo de las telecomunicaciones, sin que estas empresas se sientan recompensadas.

Los usuarios de empresa y personal pagan cuotas por acceder a la red. Para las telco es como si les dejaran el peaje de la autovía en la que se transporta oro y diamantes, si fuera transporte de carbón o reciclables quizá verían el negocio con otros ojos.

El 10 de septiembre un grupo de CEOs encabezados por Capgemini, Ericsson, SAP, CaixaBank e Iberdrola, entre otros, escribieron una carta abierta en la que enfocan las telecomunicaciones desde la perspectiva de la brecha digital y la competitividad.

Aun cuando la inversión en innovación que se reporta en la Unión Europea es una cifra exageradamente alta, no alcanza a ser ni la mitad de lo que invierte Estados Unidos, de ahí que los CEOs de estas empresas consideren que nos estamos quedando relegados y perdiendo oportunidades futuras. Básicamente Europa se convierte en consumidor.

HIPERREGULACIÓN

Europa vive una disfunción regulatoria que está echando el freno en la innovación y el desarrollo. Los legisladores europeos creen que su función es crear leyes que controlen todo lo que se pueda desarrollar, lo que hace que innovar sea difícil, y que tenga más sentido adquirir los productos en otras geografías.



CONTINÚA EN
PRÓXIMA PÁGINA





Hace años que varias operadoras de telecomunicaciones denuncian que las leyes les han dejado desprotegidos desde la perspectiva de la innovación.

Europa una vez fue líder en la época de 3G, pero a partir del 4G las leyes no permitieron pruebas y desarrollo, y todo el conocimiento migró a China, desde donde vino el 5G y ahora el 6G. Es decir, volvemos a pagar por el conocimiento, pero esta vez perdiendo el protagonismo.

LEGAL POR DEFECTO

“Las cosas deberían ser legales por defecto, en lugar de ilegales por defecto.” Este es el post con el que Elon Musk respondió a Ursula von der Leyen, la toda poderosa presidenta de la Comisión Europea.

El intercambio de mensajes se dio el pasado 11 de septiembre con razón de un informe presentado por Mario Draghi, economista y anterior primer ministro italiano que básicamente critica la regulación europea y el parón de la innovación.

La reciente regulación para la Inteligencia Artificial es un ejemplo de cómo los residentes políticos de Bruselas frenan la innovación aun cuando los expertos no tienen idea de lo que están creando.

TODO CONFLUYE EN LAS TELECOMUNICACIONES

“La competitividad europea está en juego”, así concluye la carta abierta. En las telecomunicaciones confluye el desarrollo tecnológico y el posible rol que pueda jugar Europa en la economía digital.

La brecha entre el viejo continente comparado con Estados Unidos y China es cada vez mayor, y se basa principalmente en el acceso a la red y los modelos de negocio. Sin el desarrollo apropiado de las telecomunicaciones, las tecnologías de la información y las nuevas tecnologías no se conectarán a la velocidad necesaria para una Europa competitiva, y para unos ciudadanos con igualdad de oportunidades.



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:

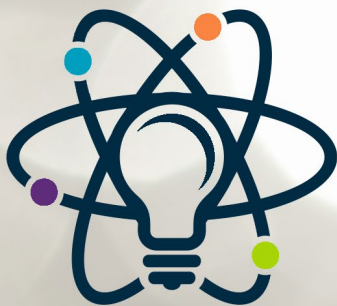
<https://www.linkedin.com/in/marlonmolina/>

P4MGO! PjM

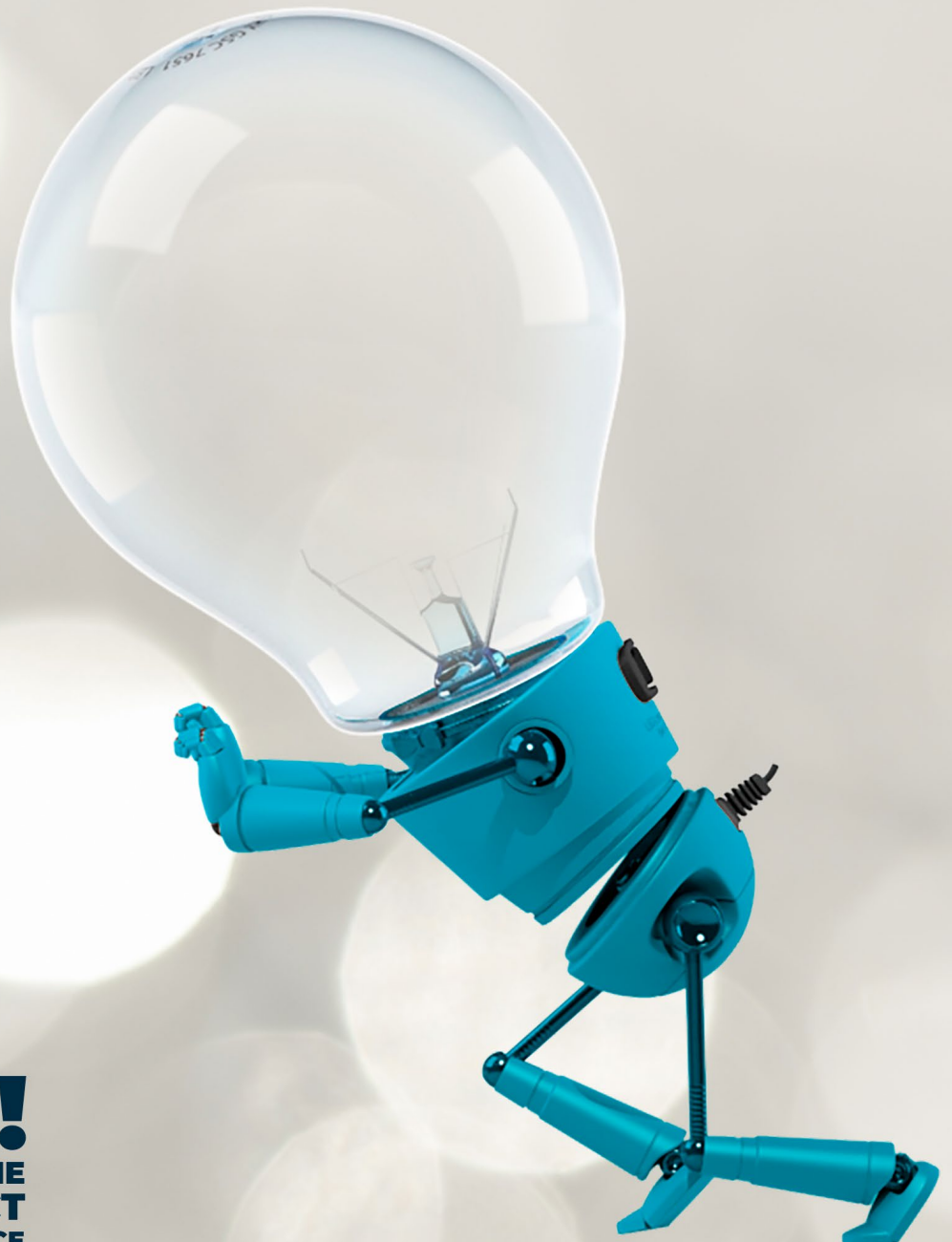
**Project Management
Project Governance
Project Offices**

Alcanza nuevos resultados en tu organización y asegura la creación de entregables de manera ágil, dinámica y elástica con **P4MGO!® PjM**

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE



Ricard Martínez Martínez

¿Es la economía o el GDPR?

El Informe Draghi ([The future of European competitiveness-Part A. A competitiveness strategy for Europe](#)) pone de nuevo sobre la mesa un viejo debate con nuevos enfoques. La tesis que plantea no es otra una descripción de la Unión Europea como gigante regulador que de algún modo anda disparándose en su propio pie. En esencia señala que existen hasta 100 leyes centradas en las empresas tecnológicas y más de 270 reguladores activos en el Mercado Único. A ello se unen las dificultades asociadas a los trámites para el establecimiento de filiales en países de la UE, la gestión de la propiedad intelectual y las patentes. Nuestro sector privado no ha sido capaz, o ha encontrado grandes barreras para la generación de grandes conjuntos de datos, a diferencia de EEUU ni ha aprovechado las posibilidades del sector público mientras que China, ha posido o ha sabido que aprovechar sus instituciones para la agregación de datos. Además, parece que las normas sobre competencia pueden inhibir la cooperación dentro de la industria y las normas nacionales en materia de contratación pública generan elevados costes permanentes para los proveedores de servicios en la nube.

Coincide Draghi con Viktor Mayer-Schönberger y Thomas Ramege en una cuestión paradójica. Los elevados costes operativos que impone la regulación son asumibles para los gigantes tecnológicos e inviables para las PYMEs. Una fuente de problemas deriva, por ejemplo, de la habilitación del Reglamento General de Protección de Datos a los Estados para regular el tratamiento de categorías especiales de datos con fines de investigación. Aunque no se diga expresamente a esa ecuación debemos sumar el soft-law de las autoridades de protección de datos. Ciertamente, existe un solo Reglamento General de Protección de Datos, pero hasta que se llega a un consenso en el seno del Comité Europeo de Protección de Datos se van publicando decenas de guías sobre sectores estratégicos como la biometría, la Inteligencia Artificial o los espacios de datos.

De una parte, debe reconocerse que la Unión Europea intenta paliar la escasez de grandes conjuntos de datos impulsando la compartición mediante la llamada Data Governance Act que contempla servicios de intermediación pública, agregadores privados y altruismo de datos. Y también la Data Act que opera una profunda transformación en el derecho a la portabilidad y debería empoderar a las personas a la hora de disponer de sus datos y compartirlos. Si además los *sandboxes* previstos en el Reglamento Inteligencia Artificial servirán para identificar obstáculos reglamentarios derivados de la legislación de la UE, mejorar la regulación y contribuir al enfoque de las autoridades reguladoras. Si se usan como un corralito para atar en corto la innovación serán un freno más. Draghi es consciente de la significativa importancia de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios.

¿Acierta Draghi? ¿Hay un elefante en la habitación? Andrés Pedreño y Luis Muñoz mantuvieron tesis similares a las del Informe hace años y subrayaron su relevancia en el contexto de una batalla geopolítica por liderar la inteligencia artificial. Lo cierto es que la UE ha diseñado un ecosistema normativo que pretende resolver los problemas evidenciados por el comportamiento de las redes sociales y otras aplicaciones. Negar que existen severos riesgos para nuestros derechos fundamentales y en ocasiones se causan riesgos sistémicos para la democracia sería hipócrita. Sin embargo, es necesario identificar los problemas para la economía ya que no sólo no desaparecerán, sino que podrían incluso agravarse.



CONTINÚA EN
PRÓXIMA PÁGINA





El segundo nivel afecta a la persona delegada de protección de datos. Es tan intenso el impacto de la acción del criterio del regulador que genera una inhibición y transforma sus tareas. La protección de datos desde el diseño y por defecto implica un enfoque de riesgo que hace viable tratar datos garantizando derechos. Pero con frecuencia quienes asesoran en la materia se limitan a emitir juicios binarios y generalmente defensivos que en no pocos casos paralizan los proyectos.

Una tercera cuestión, muy bien entendida en el Informe Draghi, consiste en el coste que implica el marco de funcionamiento actual. Por alguna extraña razón el legislador parece haber creído que el Reglamento General de Protección de Datos se está aplicando y funciona. Nada más lejos de la realidad. Aplicar la norma no se encuentra al alcance de presupuesto de una PYME, que prefiere contratar low-cost aportar por un cumplimiento formal y es epidérmico mediante formularios de copiar-pegar o procesos estandarizados de dudosa calidad. Esto cuando no prefiere acudir a un cáncer llamado LOPD Coste 0, que desvían fondos de formación desde hace un decenio que se transforma en consultoría de protección de datos de baja calidad.

Desde el punto de vista del Reglamento General de Protección de Datos, y de las normas que van surgiendo e incorporan como requisito la gobernanza de datos es necesario plantearse una nueva aproximación al menos en tres frentes.

Desde los reguladores debería renunciarse al enfoque de autoridad a la fijación de criterio desde una aproximación que suele confundir la independencia con el monólogo. Si como sucede la legislación es bastante menos relevante que el soft-law que emana de las autoridades de protección de datos ni es viable que existan tantos criterios como agencias, ni que estos se construyan de un modo autista y de espaldas a la realidad material de los sectores concernidos. Particularmente si tenemos en cuenta que el marco de interpretación y aplicación ha pivotado exclusivamente en torno a la garantía del derecho fundamental como objetivo central y único. Al parecer las referencias a promover el uso, la circulación y la reutilización de datos que se cita expresamente en toda la normativa no es un criterio con el peso suficiente. Porque los conjuntos de datos deben generarse y tratarse conforme a Derecho, pero su generación no puede estar sujeta a requisitos inalcanzables.

Cada uno de estos males tiene un particular remedio. Las autoridades de protección de datos deberían abrirse a procesos de diseño participativo. Deberían apostar por la escucha atenta y por el impulso de consensos operacionalmente viables. Si sus guías integran respuestas consensuadas ganamos todos. La ciudadanía porque se garantizan sus derechos, la economía porque convierte la garantía de la privacidad en una ventaja competitiva. Las personas delegadas de protección de datos deberían entender que su tarea es mucho más complicada que gestionar el riesgo sancionador. En este sentido, el despliegue funcional de este oficio camina por la delgada línea del cómo conseguir los objetivos de negocio lícitos cumpliendo la Ley. Pero no basta con ello. Vivimos en una Unión de Estados con un tamaño de empresa y una fortaleza del talento joven e innovador que según Kjartan Rist en Forbes la Unión Europea está demostrando fortaleza en el despliegue del ecosistema de start-up. Pero necesitan de políticas públicas destinadas a que puedan cumplir con leyes de una complejidad extrema.



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:

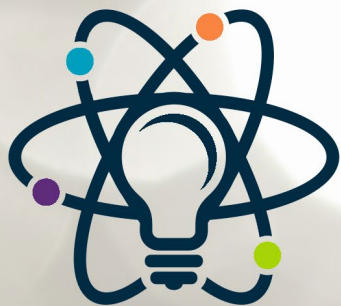
<https://www.linkedin.com/in/ricardmartinezmartinez/> Twitter: <https://twitter.com/ricardmm>

P4MGO! PdM

**Product Management
Product Governance
Product Offices**

Alcanza la digitalización en tu organización y asegura la creación de productos digitales ágil, dinámica y elástica con **P4MGO!® PdM**

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE



Marcos Navarro



La evolución de la Logística

En este 2034 el transporte y la logística han experimentado una transformación absoluta debido a la aplicación combinada de la inteligencia artificial, vehículos autónomos y nuevas infraestructuras diseñadas para maximizar la calidad de servicio y la eficiencia, así como, para reducir el impacto ambiental. Los drones guiados por IA, que forman parte del paisaje de nuestros cielos, han sustituido a los carteros y repartidores. Este nuevo paradigma ha redefinido cómo las mercancías llegan a su destino, desde los centros de producción a las grandes ciudades, y hasta las zonas rurales más remotas.

LA LOGÍSTICA AUTÓNOMA

Si bien los drones comenzaron a aparecer en la década de 2020 como una solución emergente para la entrega de paquetes, en 2034 se han convertido en un pilar fundamental de la logística aérea. Empresas como Amazon, Wing y Zipline, que a principios de siglo experimentaban con la entrega de productos pequeños y medicinas en áreas remotas, ahora operan redes de drones masivas cubriendo tanto áreas urbanas como rurales.

En las ciudades, los drones de reparto operan en pasillos aéreos diferentes, utilizando corredores especiales que están regulados y monitorizados por sistemas de gestión de tráfico aéreo autónomos. Estos drones son capaces de entregar paquetes en cuestión de minutos, aterrizando en plataformas específicas, contenedores de entregas colectivos en las azoteas de los edificios o directamente en los balcones de los pisos equipados con zonas de aterrizaje.

Mientras que los drones han transformado las entregas aéreas, los robots terrestres autónomos se han convertido en una solución esencial para las entregas en zonas urbanas, donde el espacio aéreo puede estar más congestionado o los drones no son adecuados por regulaciones o limitaciones del espacio aéreo.

Soluciones como las de Starship Technologies y Nuro han evolucionado para convertirse en actores principales en la logística urbana de 2034. Estos robots están equipados con sensores de visión artificial, cámaras 360° y tecnología LiDAR que les permiten navegar de manera autónoma por entornos complejos, evitando peatones, ciclistas y otros obstáculos.

LOGÍSTICA SUBTERRÁNEA Y ULTRARRÁPIDA

Además del uso del aire, en 2034 también hemos asistido a la expansión de los sistemas logísticos subterráneos. Esta tecnología, como MagWay, comenzó a probarse a finales de la década de 2020, y ha sido de aplicación en ciudades densamente pobladas o zonas con restricciones especiales en el

espacio aéreo. Las tuberías de transporte subterráneo conectan almacenes automatizados con los centros de distribución y las zonas residenciales de las ciudades. Estas tuberías utilizan cápsulas electromagnéticas que pueden transportar paquetes a altísimas velocidades. Este tráfico es gestionado por un sistema de IA que garantiza que las entregas se realizan en minutos y evitando las colisiones entre cápsulas.

Por otro lado, y extendiendo el concepto de tuberías, el Hyperloop se ha convertido en una realidad operativa para el transporte de mercancías de larga distancia. En lugar de camiones o trenes, los contenedores viajan a más de 1.200 km/h a través de tubos de vacío que conectan ciudades en cuestión de minutos. Esto ha transformado el transporte intercontinental, permitiendo que productos perecederos se muevan a largas distancias en tiempo récord.

TRANSPORTE MARÍTIMO Y PUERTOS AUTÓNOMOS

Una de las innovaciones más revolucionarias en 2034 es la generalización de los buques autónomos. Estos barcos, controlados por sistemas de inteligencia artificial (IA), navegan sin tripulación humana o con una tripulación mínima, suponiendo una reducción de costes operativos y riesgos sin precedentes.

Empresas como Rolls-Royce, Kongsberg y Yara ahora gestionan flotas enteras de barcos completamente automatizadas. Estos buques son capaces de tomar decisiones en tiempo real basándose en datos de navegación, clima y tráfico marítimo. Además, están interconectados a través de redes globales de sensores marinos, lo que les permite evitar colisiones, optimizar sus rutas y maximizar la eficiencia del combustible, e incluso evitar hábitats o especies protegidas.

El transporte marítimo en 2034 no es solo cuestión de los barcos; también ha habido avances significativos en los puertos y la logística intermodal, que permiten una transición más fluida entre los diferentes medios de transporte (marítimo, aéreo, hyperloop, terrestre). Los puertos inteligentes son ahora centros completamente automatizados donde la IA y los robots autónomos juegan un papel crucial en la descarga, clasificación, almacenamiento y distribución de mercancías.

ALMACENES

Los almacenes automatizados y gestionados por IA...



CONTINÚA EN
PRÓXIMA PÁGINA



Utilizan una combinación de visión artificial, LiDAR y sensores para moverse de manera eficiente por el espacio, evitando obstáculos y colaborando entre ellos para optimizar el flujo de trabajo. Compañías como Boston Dynamics, GreyOrange, ASTI-ABB y Kiva Systems han desarrollado robots inteligentes que ahora pueden realizar casi cualquier tarea de almacenamiento sin necesidad de intervención humana.

Estos almacenes operan 24/7 sin intervención humana, lo que maximiza la eficiencia y permite manejar grandes volúmenes de mercancías con precisión milimétrica.

La IA no solo se encarga de la operación física del almacén, sino que también gestiona los niveles de inventario de manera predictiva. Los algoritmos de aprendizaje automático analizan patrones de compra, datos históricos y tendencias de mercado para anticipar qué productos serán más demandados y cuándo. Esto permite a los almacenes ajustar automáticamente los pedidos de reabastecimiento, reduciendo los costos de almacenamiento excesivo o la falta de stock.

La preparación de pedidos (*picking*) y el empaquetado (*packing*) están completamente automatizados. Los sistemas de IA que gestionan el almacén calculan el mejor camino para los robots de *picking*, reduciendo los tiempos de desplazamiento y asegurando que los pedidos se completen en el menor tiempo posible. De igual manera, los robots de empaquetado ajustan el tamaño y tipo de empaques de acuerdo con el contenido del pedido, reduciendo el uso de materiales innecesarios y optimizando el espacio. Además, los sistemas permiten la personalización del empaquetado, agregando detalles como etiquetas personalizadas o mensajes según las preferencias del cliente.

Los centros de microdistribución se han convertido en una parte clave de la logística urbana. Estos *hubs* locales son pequeños

almacenes automatizados situados cerca de las áreas de alta demanda, que permiten realizar entregas rápidas, generalmente en menos de una hora. Los *hubs* están diseñados para recibir productos desde los almacenes principales y organizar las entregas de última milla mediante robots autónomos, drones o vehículos eléctricos. Los sistemas de IA optimizan el flujo de productos entre los almacenes y los *hubs*, asegurando que siempre haya suficiente stock disponible sin sobrecargar los pequeños almacenes urbanos.

IMPACTO EN EL MEDIOAMBIENTE

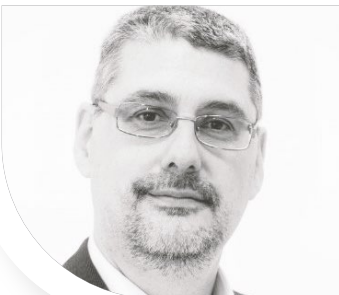
La combinación de tecnologías avanzadas, regulaciones estrictas y diseño ecológico han permitido minimizar el daño a la biodiversidad, tanto en tierra como en el aire y el mar. Estas soluciones no solo buscan reducir las emisiones de carbono, sino también proteger los hábitats naturales, prevenir la contaminación y garantizar la coexistencia armónica entre las actividades humanas y los ecosistemas.

Los gobiernos y las empresas de infraestructura han diseñado corredores ecológicos y pasos de fauna que permiten a los animales cruzar líneas de transporte sin riesgo de colisión. Estos pasos, integrados en los entornos naturales (terrestre, aéreo y marinos), se encuentran equipados con sensores y cámaras de visión artificial para monitorizar el comportamiento de los animales y garantizar que las rutas migratorias no se vean interrumpidas.

El transporte aéreo, y particularmente el uso de drones, ha requerido un enfoque cuidadoso para evitar impactos negativos en las poblaciones de aves. Los drones autónomos están equipados con sensores avanzados de visión artificial, radares y sonar para detectar aves u otros animales en su ruta de vuelo. Los drones son capaces de modificar su trayectoria en tiempo real para evitar colisiones. Además, los sistemas de comunicación entre drones y los gestores de tráfico aéreo urbano permiten coordinar las operaciones en áreas donde se ha identificado fauna sensible. En áreas urbanas, donde la actividad de aves es alta, se han creado zonas de vuelo bajo regulado (*sky layers*). En estas zonas, los drones deben volar a altitudes específicas y seguir rutas que minimicen la interferencia con la fauna local.

De igual manera, los buques están equipados con sensores submarinos y sonar que detectan la presencia de vida marina en sus rutas. En caso de detectar grandes mamíferos marinos, como ballenas o delfines, los sistemas automáticos ajustan la velocidad y el rumbo del barco para evitar colisiones. Además, gran parte de estos buques autónomos están equipados con sistemas de recolección de desechos marinos, que limpian los océanos de plásticos y otros residuos mientras transportan mercancías. Estos residuos se gestionan en los puertos de destino, y supone un ahorro considerable en impuestos para las empresas que los implementan.

La diversidad de medios de transporte no solo hace que existan diferentes alternativas para cada necesidad, sino que permite adaptarse a los requerimientos de los consumidores, de una manera eficiente y segura.



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/>

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



Curso de
Doble Certificación

Gobierno de la Externalización

**SGF +
ISO 37500**

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación SGF Executive
- Certificación ISO 37500 Leader
- Módulo 9: MasterPPM[®]



Del 18 al 26 de octubre



+ 34 96 109 44 44
campus@escueladegobierno.es



Una inteligencia artificial que te hace los informes

"- Los humanos tienen sueños. Hasta los perros tienen sueños, pero no tú. Tú eres solo una máquina. Una imitación de la vida. ¿Puede un robot escribir una sinfonía? ¿Puede un robot convertir... un lienzo en una obra maestra?

- ¿Podría usted?" (Conversación entre el detective humano Del Spooner y el robot Sonny, en la película "Yo, robot").

La inteligencia artificial generativa (IAG) es una rama de la IA que tiene la capacidad de crear diversos tipos de contenido, imitando en cierta medida la creatividad humana. Su potencial es vasto y, en el ámbito del sector público, podría representar un avance significativo en el cumplimiento de los principios de legalidad, transparencia, eficiencia e integridad. Actualmente, la IAG ya puede desempeñar un papel clave en la redacción de borradores de documentos legales, como informes y contratos, aunque también sería deseable un mayor desarrollo normativo y la creación de soluciones técnicas específicas para aprovechar plenamente esta herramienta en la Administración. Casi todo el mundo conoce ChatGPT. Bien. En este caso no hablamos de cualquier IAG, sino de una especializada en Derecho, porque si a un modelo de lenguaje genérico se le pide en ese estado básico la elaboración de un informe jurídico, el resultado va a ser claramente deficiente si lo medimos con un estándar profesional, aunque sí podría servir como apoyo a un estudiante o para resolver una consulta sencilla a cualquier usuario.

La redacción de documentos jurídicos de todo tipo es una aplicación concreta de la IAG al Derecho en general, que va más allá de la "clásica" automatización algorítmica de las tareas repetitivas del trabajo de

oficina. Se trata de una funcionalidad totalmente utilizable en la redacción de documentos basados en modelos, tales como contratos (mercantiles, laborales, administrativos) o escrituras; y en un nivel más avanzado, otros escritos de mayor complejidad, como informes legales e incluso demandas y contestaciones a las demandas, para lo que esta IA debe ser capaz de alcanzar un alto grado de comprensión de la realidad, precisión, coherencia y manejo de la terminología técnica y los formalismos legales.

Desde el punto de vista técnico, es innegable que los modelos actuales de IAG ya pueden ser entrenados utilizando conjuntos de datos compuestos por informaciones y documentos jurídicos previamente redactados y revisados por expertos en Derecho, o incluso perfeccionados por la propia herramienta a través de su capacidad de aprendizaje. De hecho, estos modelos aprenden los patrones lingüísticos y estructurales presentes en estos documentos, así como los convencionalismos y formalidades propias del lenguaje jurídico. Una vez entrenados, los modelos de IAG pueden generar documentos jurídicos completos y coherentes a partir del *prompt*, una breve descripción o un conjunto de datos de entrada proporcionados por el usuario (antecedentes, hechos). Matiz: mejor hablemos de "borradores" de documentos jurídicos, reservando esa última revisión al ojo (profesional) humano.



CONTINÚA EN
PRÓXIMA PÁGINA



OLWHIE'S
HISTORY
OF
DEVONSHIRE

MANNERS
CUSTOMS &
OF THE
RUSSIANS

TRAVELS
IN
EGYPT

AND
NUBIA

BY
NORDEN

LONDON 1727

LONDON 1719

PRINTS

PRINTS





Y si la IAG trabaja con datos, esta IAG lo hace con datos que proceden de una doble entrada: por un lado, los datos precargados, literalmente la “base de datos” de legislación y jurisprudencia, en continua actualización, y por otro lado los datos incorporados al caso concreto, básicamente los hechos del caso en cuestión y otras circunstancias relevantes que concurran. Esta herramienta, como buena IA, funcionará mejor a medida que se vaya utilizando, pudiendo al cabo de un tiempo incluso identificar el estilo propio de las personas que “rematan” los documentos e imitarlo, del mismo modo que podemos pedir a ChatGPT que escriba una poesía con el estilo de Lorca (no vamos a entrar en la polémica de si lo consigue o no, pero es indudable que reproduce pautas).

Lo importante es que, a partir de los datos del caso concreto, la funcionalidad será capaz de redactar como un letrado, uno muy torpe al principio, aunque aprenderá. Finalmente generará un texto, que evidentemente siempre tendrá que ser supervisado y validado por un jurista real, un ser humano. Y no ya solo por el famoso “sesgo del algoritmo”, sino porque nunca sabemos dónde puede aparecer un gazapo. Hablamos de documentos

importantes, hay que revisar. Hagámoslo, teniendo también en cuenta la falta de empatía del algoritmo con las circunstancias de cada persona, ya que el Derecho aborda en ocasiones situaciones personales francamente dramáticas.

Sea como fuere, la IAG es y, sobre todo, será capaz de generar diferentes tipos de textos jurídicos de gran calidad y precisión. Y además el resultado será legible y entendible para los no expertos, pues incluso se podrá presentar en forma de extractos o resúmenes más breves y comprensibles. Y todo ello sin renunciar al rigor, porque también podrá generar varias versiones, al menos una impecablemente jurídica y otra en lenguaje accesible, incluso en su versión extensa. Además, podrá traducir el texto a otros idiomas, lo cual es muy útil en las Comunidades Autónomas con dos lenguas oficiales, y también para informar de los procedimientos a los ciudadanos extranjeros con asuntos pendientes en España.



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/>

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

Curso de
Doble Certificación

**Gobierno
Corporativo**

**COSO +
ISO 37000**

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COSO Executive
- Certificación ISO 37000 Executive
- Módulo 10: MasterGEIT®
- Módulo 1:0 MasterPPM®

MPPM®

MGEIT®

eGob®

Del 22 al 30 de noviembre



+ 34 96 109 44 44
campus@escueladegobierno.es



Alex Aliaga

La guerra invisible contra los sistemas GNSS

Hoy en día, los sistemas de posicionamiento global por satélite (**GNSS**) constituyen una infraestructura clave que proporciona información precisa y fiable sobre la posición y el tiempo. Son parte fundamental de nuestras vidas cotidianas; los utilizamos en vehículos, aplicaciones de smartphones, y en operaciones críticas como el tráfico aéreo, transacciones bancarias y la sincronización de redes eléctricas. Sin embargo, la seguridad de estos sistemas se enfrenta a amenazas cada vez mayores debido a la creciente dependencia global de esta tecnología.

El sistema de posicionamiento más conocido es el **GPS** (Global Positioning System), desarrollado por Estados Unidos, pero existen otros como el europeo **Galileo**, el ruso **GLONASS** y el chino **BeiDou**. Todos estos sistemas son vulnerables a ciberataques y manipulación, lo que pone en riesgo no solo su operación, sino también los sectores que dependen de ellos.

GEOPOLÍTICA DEL POSICIONAMIENTO Y SUS RIESGOS

La seguridad de los sistemas GNSS ha cobrado relevancia como una de las amenazas más serias en los últimos años, sobre todo por su uso intensivo en operaciones civiles y militares. Se estima que más del 90% de las infraestructuras críticas dependen de la precisión y sincronización que ofrecen estos sistemas. Sin embargo, esta dependencia también los convierte en objetivos atractivos para actores maliciosos, desde estados-nación hasta grupos hacktivistas y delincuentes comunes.

Uno de los principales riesgos es el **spoofing**, que consiste en enviar señales GPS falsas para que los receptores de un objetivo perciban una ubicación equivocada. Este tipo de ataque puede tener graves consecuencias: desde desorientar aviones y barcos, hasta alterar rutas de transporte y afectar operaciones militares. Por ejemplo, antes de la invasión rusa a Ucrania en 2021, se registraron casos de spoofing que afectaron a buques de guerra de la OTAN en el puerto de Odesa, Ucrania, lo que interrumpió sus operaciones en la región.

Otra amenaza importante es el **jamming**, que implica bloquear las señales de GPS mediante la emisión de señales de radio potentes en la misma frecuencia. Los dispositivos utilizados para este fin son relativamente baratos y fáciles de conseguir, lo que amplía su potencial de uso tanto por actores estatales como no estatales. En el conflicto en Ucrania, se ha observado que las fuerzas rusas emplean jamming para deshabilitar los sistemas de navegación de aeronaves y vehículos, lo que ha provocado disrupciones en toda Europa.

Estos ataques no solo afectan operaciones militares o logísticas; su impacto puede extenderse a la economía y a infraestructuras críticas como la red eléctrica o los sistemas de telecomunicaciones. La capacidad de interrumpir estas redes es motivo de gran preocupación, especialmente porque, a medida que avanzamos hacia una mayor automatización, el riesgo de sufrir ciberataques aumenta considerablemente.

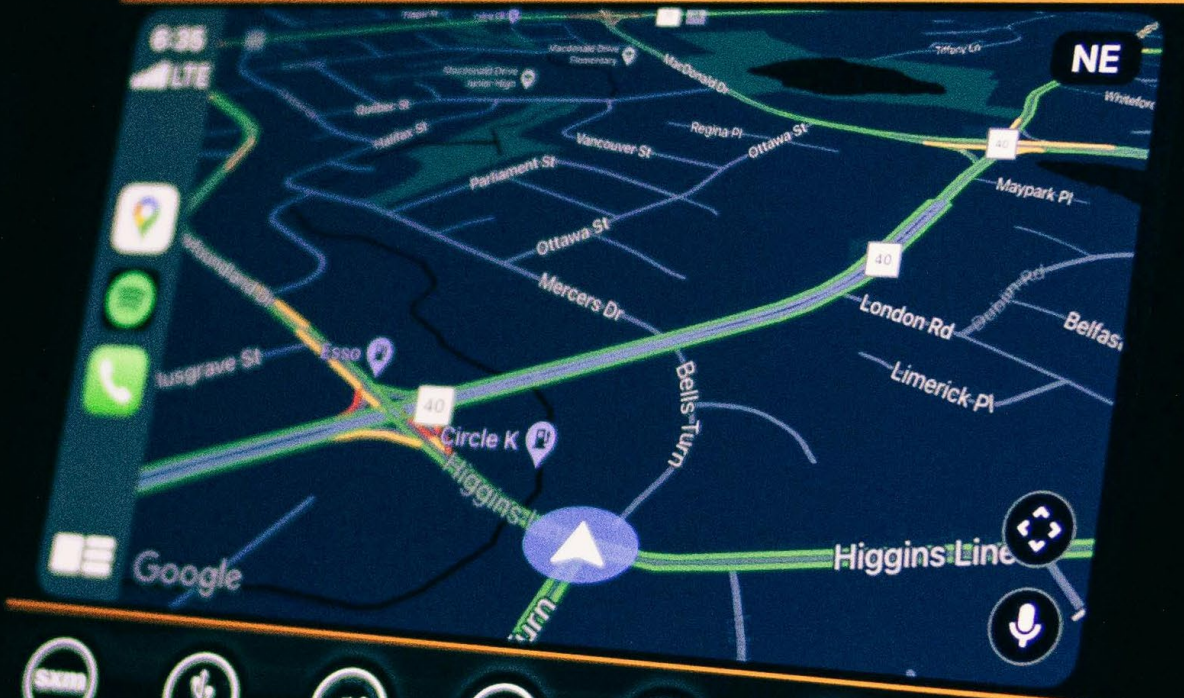









CONTINÚA EN
PRÓXIMA PÁGINA

19.5°

11°out.

19.5°



- 
Radio
- 
Media
- 
Climate
- 
Apps
- 
Controls
- 
Nav
- 
CarPlay

VOLUME



MUTE



SCREEN OFF



A/C



OFF



AUTO

TUNE

BROWSE

ENTER

SCROLL



FRONT



REAR



OFF



OFF



eco



SPORT





HACKTIVISMO Y ATAQUES A INFRAESTRUCTURAS CRÍTICAS

En los últimos años, grupos hacktivistas han incrementado sus ataques contra sistemas GNSS. Un ejemplo es **GhostSec**, un colectivo que afirmó haber comprometido equipos GPS utilizados en instalaciones industriales críticas. Estos ataques pueden generar consecuencias catastróficas si se ejecutan con éxito. Los GNSS no solo proporcionan posicionamiento; también sincronizan redes eléctricas y soportan transacciones bancarias, entre otros servicios vitales.

El problema se agrava debido a la cantidad de sistemas GNSS conectados a internet sin medidas de seguridad adecuadas. Algunos estudios han encontrado que muchas de estas infraestructuras exponen públicamente sus interfaces de control, lo que las hace vulnerables a ataques remotos. Incluso, se han identificado módems satelitales en sectores como la energía, telecomunicaciones y transporte que no han cambiado las credenciales predeterminadas, lo que facilita la entrada de actores malintencionados.

Un ataque reciente, denominado **Operación Cataclysm**, dirigido por el grupo **One Fist**, mostró cómo los hacktivistas pueden desactivar módems satelitales utilizados en sectores clave como la aviación y el transporte marítimo. Durante esta operación, los atacantes eliminaron configuraciones críticas de los módems, causando interrupciones en la conectividad satelital. Este tipo de ataques no solo comprometen la integridad de los datos, sino que también pueden causar interrupciones en el suministro de servicios esenciales.

Por otro lado, los ciberataques más sofisticados, como el ransomware, también están afectando al sector espacial. Empresas que proveen servicios y componentes para satélites, como **Viasat**, han sido objeto de ataques que han interrumpido operaciones globales. En 2022, un ataque al sistema KA-SAT de Viasat afectó a 5800 turbinas eólicas en Alemania, lo que demuestra el impacto devastador que pueden tener los ataques a sistemas GNSS y satelitales.

ESTRATEGIAS CLAVE PARA PROTEGER LOS SISTEMAS GNSS DE CIBERATAQUES

A la luz de estas amenazas, diversas agencias de seguridad, como el **Departamento de Seguridad Nacional** de EE. UU. y la **CISA** (Agencia de Seguridad de Infraestructura y Ciberseguridad), han emitido directrices para mitigar los riesgos. Entre las recomendaciones se incluyen medidas para detectar y contrarrestar ataques de spoofing y jamming, además de la implementación de sistemas de **PNT resiliente** (Posicionamiento, Navegación y Temporización). Estos sistemas proporcionan una capa adicional de protección al complementar el GPS con tecnologías terrestres o alternativas satelitales, lo que ayuda a mantener la precisión y disponibilidad de los servicios, incluso en caso de interferencias.

En la **Unión Europea**, se han lanzado iniciativas para fortalecer la seguridad de **Galileo**, su sistema de navegación por satélite. La Agencia Espacial Europea trabaja en mejorar las capacidades de detección de interferencias y el desarrollo de nuevas técnicas criptográficas para proteger las comunicaciones entre los satélites y las estaciones terrestres.



CONCLUSIÓN

A medida que los sistemas GNSS se integran más en la vida moderna y en nuestras rutinas, aumenta la amenaza y el riesgo de sufrir ciberataques en estos activos críticos. Los satélites, sus estaciones terrestres, los enlaces de comunicación, el software que se ejecuta en todos sus sistemas pueden ser vulnerables a ciberataques; no por estar en el espacio están exentos de sufrir un ciberataque.

Las posibles consecuencias si un ataque de estas características se materializase serían significativas y potencialmente peligrosas, que no sólo afectarían al activo en sí, sino que se verían afectados gran cantidad de sistemas y sectores que dependen de estos activos, así como de la ciudadanía que hacen uso de los sistemas GNSS.

Defenderse de los ciberataques en el espacio es un desafío complejo que requiere cooperación internacional, en primer lugar es importante conocer la gravedad del riesgo que supondrían un ataque de estas dimensiones. Y, aunque ya existen, muchas iniciativas es complejo atajar de raíz los problemas existentes. Mientras tanto, es importante divulgar y conocer cuáles son los riesgos para que, en aquellas infraestructuras o sistemas informáticos donde se puedan aplicar controles de seguridad y medidas adicionales a las ya existentes, se puedan aplicar de inmediato.



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
Doble Certificación

Gobierno del Tiempo y Gestión de la Productividad

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación TSG4® Yellow Belt
- Certificación UNE 71404 Executive
- Módulo 1: MasterGEIT®
- Módulo 1: MasterPPM®

MPPM®

MGEIT®

eGob®

Del 15 al 23 de marzo



+ 34 96 109 44 44
campus@escueladegobierno.es



Marta Martín

Desmontando mitos (2)

Los estigmas en torno al TDAH no solo no son ciertos, sino que son inabarcables. Lo que no es óbice para no luchar contra las falsas informaciones que etiquetan injustamente a una condición neurobiológica

El trastorno por déficit de atención e hiperactividad es una condición neurobiológica que afecta a millones de personas en todo el mundo. A pesar de estar más extendido de lo que se piensa y de los avances en la investigación, la lista de mitos que le rodea es infinita.

Hemos abordado los más habituales, pero sin duda, hay muchos otros pendientes de desmontar, porque solo a través del conocimiento y la educación se podrá construir una sociedad más inclusiva y colocar al TDAH en el lugar que realmente merece. Estos son algunos de los más habituales:

- **Las personas con TDAH no pueden tener éxito.** De hecho, es habitual que cuando se busca el diagnóstico muchos médicos lo desestiman porque los pacientes tienen estudios superiores, o un buen trabajo, o gestionan sus familias y sus hogares. No hay que olvidar que, con el apoyo adecuado, estrategias de manejo y adaptaciones, y mucho trabajo, se pueden alcanzar muchos objetivos personales y profesionales.

- **Las personas con TDAH son todas hiperactivas.** Es muy frecuente pensar que si alguien es muy tranquilo o introvertido no puede tener TDAH. No hay que olvidar, que el TDAH se manifiesta de tres formas: el subtipo inatento, el hiperactivo y el combinado. Muchas personas con TDAH participan del subtipo inatento y no muestran una hiperactividad e impulsividad muy marcada, por lo que pasan desapercibidas, principalmente las niñas. Además, en la madurez la hiperactividad física suele moderarse, aunque la hiperactividad

mental permanece o incluso, se agrava. Lo que no significa que se hayan curado o que no tengan TDAH.

- **El TDAH es una cuestión de fuerza de voluntad.** Lo cierto es que es una condición neurobiológica crónica que no se desaparece con más esfuerzo o con cambios en el estilo de vida. Por lo tanto, pedir a una persona con TDAH que se esfuerce es ignorar la naturaleza neurobiológica del trastorno y solo genera frustración y daños en la autoestima. La mejor manera de superarlo es implementando estrategias como la medicación, la terapia cognitivo-conductual o las técnicas de organización.

- **El TDAH es sólo un problema de falta de atención.** No hay duda de que este es uno de los síntomas nucleares, pero el TDAH va mucho más allá. De hecho, las dificultades más complicadas de gestionar son las relacionadas con las funciones ejecutivas, es decir, las habilidades mentales que se encargan de ayudarnos a conseguir nuestros objetivos y que controlan el procesamiento general del cerebro, tanto de la organización como de la regulación.

- **El TDAH afecta a la inteligencia.** Con frecuencia se relaciona el bajo rendimiento de las personas con TDAH con el aburrimiento, el descuido o la pereza, es decir se asocia a defectos de personalidad, en lugar de reconocer las dificultades del trastorno. De nuevo aquí, entran en juego las funciones ejecutivas que son las responsables de poder mantener una acción en el tiempo, resolver problemas y persistir hasta llegar a un objetivo.



CONTINÚA EN PRÓXIMA PÁGINA





Es más, no es extraño que confluyan el TDAH y las altas capacidades, lo que se conoce como doble excepcionalidad. Es decir, muchas personas con TDAH son altamente inteligentes y creativas, aunque se enfrenten a dificultades en áreas como la organización y la concentración, lo que puede imposibilitar la manifestación completa de su potencial.

• **El TDAH no es preocupante si no provoca fracaso escolar.** Sin embargo, son numerosos los casos en los que el niño no presenta fracaso escolar porque su nivel de inteligencia está compensando las dificultades que provoca el trastorno. Los problemas pueden presentarse en el ámbito familiar o social debido a la inatención o la impulsividad, lo que repercute en su relación con el entorno y su autoestima.

• **La medicación del TDAH provoca adicción.** Los fármacos cubren el déficit de neurotransmisores de los cerebros con TDAH. No alteran el funcionamiento cerebral, solo normalizan los niveles deficitarios de dopamina y noradrenalina en las áreas cerebrales implicadas en el TDAH. Y cuando el tratamiento se suspende, lo único que ocurre es que el cerebro vuelve a su estado inicial, es decir, a ser deficitario en estos neurotransmisores y sufrir las dificultades iniciales. La prueba más evidente de que la medicación no es adictiva es que a las personas con TDAH a menudo se les olvida tomársela.

• **Hay que descansar de la medicación en las vacaciones y los fines de semana.** Lo cierto es que la medicación no se prescribe solo para mejorar la atención o la impulsividad, sino también para mitigar otros síntomas que afectan a las relaciones sociales, a la hiperactividad mental o a la mala gestión de las funciones ejecutivas. Y para todos estos problemas, no hay vacaciones ni festivos.

La lista de mitos es infinita y, sin duda, todos estos estigmas tienen consecuencias negativas y reales en las personas con TDAH que son señaladas y etiquetadas injustamente y, lo que es más preocupante, retrasan o evitan el diagnóstico y su consecuente tratamiento. Las dificultades diarias del TDAH son realmente significativas y si a éstas les sumamos estas creencias erróneas, vivir con TDAH se hace aún más costoso.

No hay una forma más efectiva de formentar una sociedad inclusiva que desmontar los estigmas a través de la concienciación y la educación. Y entender que, en un mundo neurodiverso en el que cada persona posee una configuración única de habilidades y talentos, es esencial reconocer que ni el diagnóstico de TDAH, ni los síntomas, definen la capacidad de una persona ni la limitan en ningún sentido.



MARTA MARTÍN

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

LinkedIn:

<https://www.linkedin.com/in/marta-mart%C3%ADn-garc%C3%ADa-463a5a2a>

Youtube:

https://www.youtube.com/channel/UCn02bjVXA3q9GP0_23DRwIw

Instagram:

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

Escuela de Gobierno

eGov®

<https://escueladegobierno.es>

Curso de Doble
Certificación en:

Gestión de Beneficios y Gestión de Portafolios

P4MGO!® BfM Leader

P4MGO!® PfM Leader

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Metodología P4MGO!®
- Exámenes de Certificación Incluidos
- Certificación P4MGO!® BfM Leader
- Certificación P4MGO!® PfM Leader
- Solicita tu admisión

MPPM®

MGEIT®

eGov®

Próxima Convocatoria en Directo

Octubre 2024

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es



P4MGO!

Javier García, director general de UNE, reelegido vicepresidente de ISO

Javier García ha sido reelegido por dos años más como vicepresidente de ISO durante la Asamblea General celebrada esta semana en Colombia. De esta forma, el director general de UNE completará un mandato de cuatro años que comenzó en 2023, convirtiéndose en el primer español elegido para desempeñar esta responsabilidad.

Su nombramiento refleja la destacada influencia y reputación de la normalización española en el mundo y proporciona al tejido empresarial español la oportunidad de seguir liderando las normas globales que les ayudarán a superar con éxito sus grandes desafíos.

ISO ha publicado el primer estándar global que ayudará a las organizaciones a la consecución de los ODS de Naciones Unidas. De libre acceso en el marco de colaboración entre ISO y ONU, estará disponible en español esta semana como UNE-ISO/UNDP PAS 53002. UNE ha liderado su traducción oficial al español.

Javier García, director general de la Asociación Española de Normalización, UNE, ha sido reelegido por dos años más como vicepresidente de Gestión Técnica de la Organización Internacional de Normalización (ISO), con lo que completará un mandato de cuatro años. Javier García

se convirtió en 2021 en el primer español elegido para desempeñar este cargo en ISO para el período 2023-2024; ahora, ha sido nombrado para el período 2025-2026.

El nombramiento ha sido ratificado durante la Asamblea General de ISO celebrada la semana pasada en Cartagena de Indias, Colombia, en la que Javier García ha estado presente, acompañado por la directora de Cooperación y Relaciones Internacionales de UNE, Mónica Sanzo. UNE es el representante español en ISO, la responsable de crear los estándares globales con las mejores prácticas en gestión empresarial. Está formada por 172 países.

En palabras de Javier García: "Me siento profundamente honrado y agradecido por la confianza que de nuevo han depositado en mí los miembros de ISO. Continuar mi labor al frente de la Vicepresidencia Técnica supone una oportunidad para que el tejido productivo español siga liderando los estándares globales que les ayudarán a superar con éxito sus grandes desafíos. El que escribe la norma define el mercado".



**CONTINÚA EN
PRÓXIMA PÁGINA**





Este nombramiento es también un reconocimiento a la extraordinaria influencia y reputación de la normalización española en el mundo, así como a la labor de UNE que permite que España disponga de uno de los organismos de normalización más potentes del mundo y sea un referente internacional en estandarización; actualmente, los expertos de nuestro país lideran más de 150 presidencias y secretarías de órganos técnicos en los organismos internacionales y europeos de normalización (ISO, IEC, CEN y CENELEC y ETSI) y cada vez más normas españolas son la base para elaborar estándares globales.

El director general de UNE cuenta con un destacado reconocimiento internacional que se materializa en sus diversos cargos de responsabilidad en los organismos mundiales y europeos de normalización. Actualmente es miembro del Consejo de Administración del Comité Europeo de Normalización (CEN). Durante su carrera profesional, ha sido Vicepresidente Técnico del Comité Europeo de Normalización Electrotécnico (CENELEC). También formó parte del Consejo Técnico de Normalización de la Comisión Electrotécnica Internacional (IEC).

Javier García trabaja desde hace más 25 años en el Organismo español de normalización, cuya Dirección General ocupa desde 2017. Es licenciado en Ciencias Químicas, máster en Gestión de la Innovación y posgrado en Administración de Empresas y Dirección de Marketing.

Desde su posición en ISO, Javier García asume la responsabilidad de asegurar que las nuevas normas técnicas internacionales se alinean con la Estrategia trazada por ISO para 2030, enfocada a impulsar, entre otros ámbitos, la transición ecológica y energética, la transformación digital, los objetivos ESG (ambiental, social y de buen gobierno) o el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS).

Primer estándar global para los ODS de Naciones Unidas

El último punto cobra especial relevancia pues en la Asamblea General, ISO ha publicado el primer estándar global que ayudará a las organizaciones de todo el mundo a la consecución de los ODS de Naciones Unidas: el ISO/UNDP PAS 53002 "Directrices para contribuir a los Objetivos de Desarrollo Sostenible (ODS) de



las Naciones Unidas". Este estándar es fruto del acuerdo de cooperación firmado entre ISO y el Programa de las Naciones Unidas para el Desarrollo (PNUD).

En su desarrollo han participado 66 países, entre ellos España, a través de UNE, que ha liderado la traducción de la versión oficial al español, permitiendo así agilizar su llegada a un mercado de más de 600 millones de hispanohablantes, impulsando una aplicación homogénea.

Este documento es de libre acceso de forma totalmente excepcional en el marco del acuerdo entre ISO y Naciones Unidas. La próxima semana estará disponible en español en la web de UNE como UNE-ISO/UNDP PAS 53002.

Además, ISO está desarrollando la futura Norma ISO/UNDP 53001 que establecerá los requisitos para desarrollar un sistema de gestión de los Objetivos de Desarrollo Sostenible.

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



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 convalidable 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>

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 FISM 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 DAIMA 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 asignaturas del Master en Gobierno y Gestión de Información y Tecnología MasterGEIT®.

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



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