

REVISTA Tecnología & Sentido Común



#51

ABRIL
2025

**Estuardo
Castañeda**

NUESTRO INVITADO
A #TYSC

28

El Gubernauta

JAVIER PERIS

12

**Futuro y
Seguridad**

MANUEL SERRAT

16

**Tecnoregulación
en Prospectiva**

NACHO ALAMILLO

20

Radio Security

ALEX ALIAGA

52

Ai Futuro

MARCOS NAVARRO

44

Es tendencia

MARLON MOLINA

36

**La nueva
Administración**

VÍCTOR ALMONACID

48

**Diario de una
tortuga ninja**

JUAN CARLOS MURIA

24

**Mentes
Divergentes**

MARTA MARTÍN

56



REVISTA **Tecnología & Sentido Común**



EQUIPO TYSC

Javier Peris - El Gubernauta
Manuel Serrat - Futuro y Seguridad
Nacho Alamillo - Tecnoregulación en Prospectiva
Juan Carlos Muria - Diario de una Tortuga Ninja
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Marcos Navarro - Ai Futuro
Víctor Almonacid - La Nueva Administracion
Alex Aliaga - Radio Security
Marta Martín - Mentas Divergentes

PUBLICIDAD Y CONTRATACIÓN

Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

GABINETE JURÍDICO

Jesús López Peláz

ATENCIÓN AL LECTOR

soluciones@businessandcompany.com

EDITA

Business, Technology & Best Practices, S.L.
Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
<https://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

9 de Abril
16:00 A 20:00 HS

Las Naves
C/ de Joan Verdeguer 16,
46024 Valencia, España



La Comunidad Global
de **Profesionales** en la
Dirección de Servicios
Comprometidos con la
*Innovación, las Buenas
Prácticas y la Mejora
Continua* presenta:

¿Excelencia?

#SI2025

ORGANIZAN:



COLABORAN:



La Comunidad Global de **Profesionales** en la
Dirección de Servicios Comprometidos con la
Innovación, las Buenas Prácticas y la Mejora
Continua presenta:

¿Excelencia?

PROGRAMA

16:00 A 16:15

Presentación Evento



**Javier
Peris**

SMP - Presidente Global
del Service
Management
Institute



**Alejandro
Blasco**

SMP - Presidente del
Colegio Oficial de
Ingeniería Informática
COIICV

16:15 A 16:45

20000 Leguas de Viaje Tecnológico



**Luis
Morán**

SMP - Chief
Knowledge
Officer del Service
Management
Institute



**Moisés
Robles**

SMP - Vocal del
Subcomité
CTN 71/SC 40
de UNE

16:45 A 17:15

Su excelencia el Servicio Público



**Elena
Ordozgoiti**

Responsable de
Negocio Sector
Servicios de UNE



**Javier
Peris**

SMP - Presidente Global
del Service
Management
Institute

17:15 A 17:45

¿Excelencia?



**Jesús
López Pelaz**

SMP -Presidente del
Consejo Legal
Service Management Institute

17:45 A 18:30

MESA REDONDA

Service Management Professionals



Angie Lopez Gea

SMP - Vocal
Miembro de la Junta
Directiva del Service
Management
Institute



Paula Jovel

SMP - IT Service
Management
Lead en
Equifax Iberia



Juan Darocha

SMP - Director UNE
Ciberseguridad
y Servicios
gestionados en
Nunsys Group



María José Montes Díaz

SMP - Service
Manager, Delivery
Lead & Security
Engineering en
Accenture España

18:30 A 18:45

Proceso de Grandfathering Service Management Professional SMP



Marcos Navarro Alcaraz

SMP - Vocal Miembro de
la Junta Directiva
del Service
Management Institute

18:45 A 19:00

Entrega de insignias y Diplomas



Carlos Manuel Fernández Sánchez

SMP - Vicepresidente Global
del Service Management
Institute

19:00 A 20:00

Degustación de jamón Ibérico a cargo de un Maestro Cortador



**Service
Management
Institute**

9 de Abril

16:00 A 20:00 HS

Las Naves
C/ de Joan Verdeguer 16,
46024 Valencia, España

<https://servicemanagement.institute>

¿Excelencia?

#SI2025

Valencia, España
9 de Abril

ORGANIZAN:



COLABORAN:





SEMANA 2025 INFORMÁTICA

20 años

DEL 8 AL 10 DE ABRIL



Informática y sociedad: disrupciones al servicio de las personas

#SI2025



www.semanainformatica.com

#51

ABRIL 2025



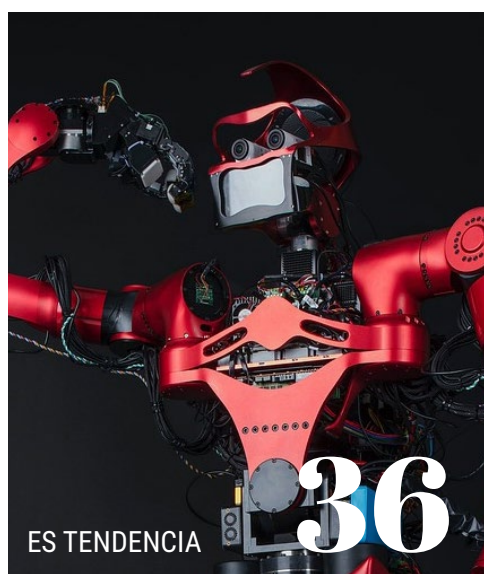
índice

DE CONTENIDOS

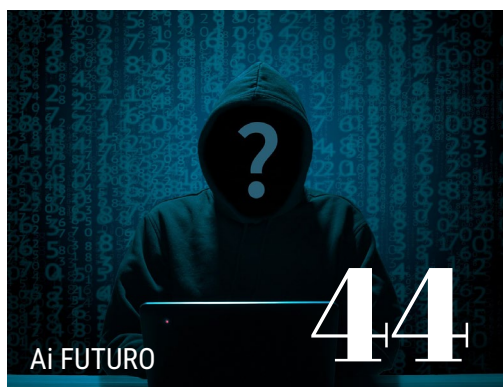
<https://tecnologiaysentidocomun.com>



**Estuardo
Castañeda**



**Los robots humanoides
son tendencia**



**Las CiberAlmenzas
del 2034.
Ciberguardaespaldas**



**Un poco de
atención,
por favor**

Copyright

02

Índice de Contenidos

08

Este mes te recomiendo leer...

por JAVIER PERIS

11

Gestión de Servicios no es (solo) Gestión de Incidencias

EL GOBERNAUTA
JAVIER PERIS

12

Robos de información: ¿evaluamos bien su impacto?

FUTURO Y SEGURIDAD
MANUEL SERRAT OLMO

16

En tiempo de descuento para la implantación de Veri*Factu

TECNOREGULACIÓN
EN PROSPECTIVA
NACHO ALAMILLO

20

¿Por qué un Espacio Europeo de Datos de Salud?

DIARIO DE UNA
TORTUGA NINJA
JUAN CARLOS MURIA

24

Estuardo Castañeda

NUESTRO
INVITADO A TYSC

28

Los robots humanoides son tendencia

ES TENDENCIA
MARLON MOLINA

36

Bring Your Own AI (BYOAI)

OJO AL DATO
RICARD MARTÍNEZ
MARTÍNEZ

40

Las CiberAlmenzas del 2034. Ciberguardaespaldas

AI FUTURO
MARCOS NAVARRO

44

Más vale prevenir que curar

LA NUEVA
ADMINISTRACIÓN
VÍCTOR ALMONACID

48

Amenazas no convencionales en el mundo del IoT

RADIO SECURITY
ALEX ALIAGA

52

Un poco de atención, por favor

MENTES DIVERGENTES
MARTA MARTÍN

56

UNE potencia la innovación en el ámbito de los bioplásticos

NORMALIZACIÓN

60

#51 - ABRIL 2025

Índice

#TYSC

Premios recibidos



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



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

itSMF
ESPAÑA

Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática



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

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

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

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



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



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



Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA



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

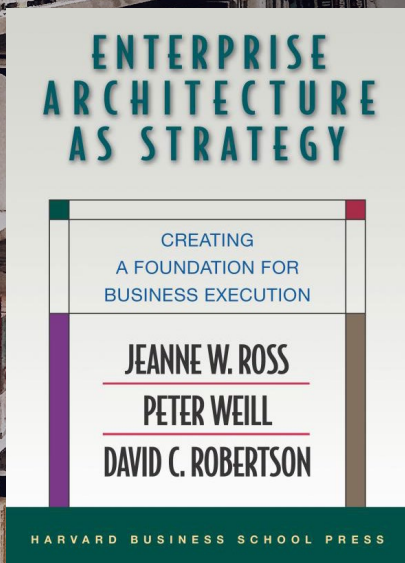


Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



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





Enterprise Architecture As Strategy. Creating a foundation for business execution

Jeanne W. Ross, Peter Weill & David C. Robertson

Publicado por Harvard Business School Press, este libro aborda un tema crucial que a menudo se percibe erróneamente como un asunto puramente técnico: la Arquitectura Empresarial (AE). Los autores, basándose en una extensa investigación en cientos de empresas, argumentan de manera convincente que la AE no es solo cosa del departamento de TI, sino **una estrategia fundamental de negocio** para lograr una ejecución impecable y sostenible.

El corazón del libro late con la idea de construir un "Fundamento para la Ejecución" sólido. Lejos de ser un concepto abstracto, se trata de digitalizar y estandarizar los procesos clave de tu negocio. Imagina poder realizar las operaciones esenciales de forma eficiente y fiable, casi sin pensarlo, liberando así la atención de la gerencia para centrarse en la innovación, el crecimiento y la respuesta ágil a los cambios del mercado. Paradójicamente, esta base estandarizada no genera rigidez, sino que, como demuestran los autores, es la clave para una mayor agilidad empresarial.

Una de las herramientas más valiosas que ofrece el libro es el concepto del "Modelo Operativo". Te ayuda a definir qué nivel de integración (compartir datos entre unidades) y estandarización (hacer las cosas de la misma manera) necesita tu empresa para tener éxito. Presentan cuatro modelos claros (Diversificación,

Coordinación, Replicación y Unificación) que sirven como una hoja de ruta para alinear tu estructura, procesos y tecnología con tu estrategia real de cómo quieres operar y crecer.

A partir de ahí, el libro te guía a través de cómo la Arquitectura Empresarial traduce ese Modelo Operativo en un diseño concreto para tus procesos, datos y sistemas tecnológicos. Explica las etapas de madurez por las que suelen pasar las empresas en este viaje, desde los silos aislados hasta una modularidad que permite flexibilidad y eficiencia. Además, aborda cómo implementar este fundamento proyecto a proyecto, utilizando un "Modelo de Compromiso de TI" que asegura la alineación entre los objetivos locales y los de toda la empresa, e incluso cómo la arquitectura guía decisiones críticas como el outsourcing.

Lo que me ha gustado de este libro destaque es su enfoque práctico y su lenguaje accesible tanto para líderes de negocio como para profesionales de tecnología. Está repleto de ejemplos reales que ilustran cómo empresas líderes han utilizado estos principios para obtener resultados tangibles: mayor rentabilidad, menor tiempo de comercialización, reducción de costos de TI y mayor agilidad estratégica.

Javier Peris



Gestión de Servicios no es (solo) Gestión de Incidencias

La Gestión de Servicios de Tecnología tiene como objetivo alinear los Servicios Tecnológicos con las necesidades del negocio, optimizando la entrega de valor a través de una gestión eficiente y estructurada. Dentro de este marco, la Gestión de Incidencias se erige como el proceso más visible y, a menudo, el punto de contacto inicial entre los usuarios y el departamento de Tecnologías de la Información

Sin embargo, muchas organizaciones caen en el error de implementar exclusivamente la Gestión de Incidencias, relegando a un segundo, tercero o cuarto plano otros procesos críticos como la Gestión de Problemas, Gestión de Cambios, Gestión de Continuidad, Gestión de Disponibilidad, Gestión de Niveles de Servicio. Esta visión miope de la Gestión de Servicios, centrada únicamente en “apagar fuegos”, es en realidad lo que compromete la calidad percibida del servicio, pues impide alcanzar los objetivos estratégicos y limita el verdadero potencial de la tecnología para impulsar el éxito organizacional.

La Gestión de Incidencias se define como el proceso de restaurar el servicio a los usuarios lo más rápido posible tras una interrupción para que la operación de negocio no se detenga, corresponde a los primeros auxilios. Su importancia radica en minimizar el impacto negativo en la productividad y la continuidad del negocio. Este proceso de Gestión de Servicios acapara gran atención debido a su impacto directo y visibilidad en el usuario final.

Sin embargo, la Gestión de Incidencias, por sí sola, es absolutamente insuficiente. Su naturaleza reactiva la limita a “apagar fuegos” constantemente, sin abordar las causas raíz de los problemas subyacentes. Es como un hospital que solo atiende

urgencias: puede salvar vidas en el momento, pero no previene enfermedades ni realiza diagnósticos profundos para evitar futuras crisis. Este enfoque reactivo perpetúa un ciclo de interrupciones y soluciones temporales, impidiendo una mejora continua y una optimización real de los servicios.

La obsesión exclusiva por la **Gestión de Incidencias** a menudo eclipsa otros procesos de Gestión de Servicios igualmente cruciales, cuyo descuido genera consecuencias negativas significativas.

Sin una adecuada **Gestión de Problemas**, los mismos incidentes resurgen una y otra vez, consumiendo recursos valiosos en soluciones temporales. La confianza de los usuarios se erosiona, la productividad disminuye y el equipo de tecnología en su conjunto se ve atrapado en un ciclo interminable de “apagar incendios”. Si solo se solucionan los incidentes individuales sin investigar la causa subyacente, los usuarios seguirán experimentando interrupciones, generando frustración y pérdidas de tiempo y permaneciendo toda la organización en el lodazal.

Sin una adecuada **Gestión de Cambios**, Los cambios mal planificados o ejecutados introducen en la mayoría de las ocasiones nuevos incidentes, generan inestabilidad en los servicios y provocan el caos.

La falta de un proceso de Gestión de Niveles de Servicio conduce a la desalineación entre tecnología y las expectativas del negocio, generando insatisfacción del usuario y ausencia de criterios objetivos para medir el rendimiento.



CONTINÚA EN
PRÓXIMA PÁGINA



Sin una proactiva **Gestión de la Capacidad**, las organizaciones se enfrentan a un rendimiento deficiente de los servicios (lentitud, tiempos de respuesta elevados), interrupciones por agotamiento de recursos y costes elevados por compras reactivas y sobredimensionadas. La falta de planificación impide alinear la infraestructura con el crecimiento del negocio, generando cuellos de botella que inevitablemente se traducen en incidencias y en una mala experiencia de los usuarios.

Ignorar la **Gestión de la Disponibilidad** conduce a interrupciones frecuentes e imprevistas, incumplimiento de los Acuerdos de Niveles de Servicios con clientes y en definitiva a una percepción negativa de TI por parte del negocio y los usuarios. En lugar de diseñar servicios resilientes desde el inicio, el equipo de TI se ve forzado a reaccionar constantemente ante caídas, sin abordar las debilidades arquitectónicas subyacentes, lo que perpetúa la inestabilidad.

La falta de planes de continuidad probados, aprobados y actualizados expone a la organización a riesgos catastróficos. Ante un desastre (incendio, ciberataque masivo, fallo generalizado), la incapacidad para restaurar servicios esenciales puede llevar a pérdidas financieras significativas, daño irreparable a la reputación e incluso al cese de la actividad del negocio. Confiar únicamente en la **Gestión de Incidencias** para eventos de gran magnitud es completamente inadecuado y peligroso.

Una adecuada implementación de los procesos de Gestión del Servicio requiere de una gobernanza sólida y real con un liderazgo efectivo. No se trata solo de una cuestión técnica, sino de una estrategia empresarial sincera que debe ser impulsada desde la alta dirección. El liderazgo debe establecer la **Dirección del Servicio** como una prioridad, asignando los recursos necesarios que por supuesto, como estamos evidenciando, van más allá de la mera **Gestión de Incidencias**.

Lamentablemente con demasiada frecuencia me encuentro en situaciones en las que el rol del *Service Manager* ha sido reducido a un mero supervisor del *Service Desk* o gestor de incidencias. Esta visión limitada impide que el *Service Manager* gestione el ciclo de vida completo del servicio de forma integral. Es necesario empoderar a estos profesionales, brindándoles la autoridad y el mandato para tomar decisiones que impacten positivamente en la calidad del servicio y la satisfacción del cliente. El *Service Manager* debe ser capaz de entender las necesidades del negocio, traducir esas necesidades en requisitos de servicio y trabajar en colaboración con otros equipos de TI para garantizar que esos requisitos se cumplan.

La Gestión de Incidencias, aunque vital, es tan solo una pieza de un puzzle mucho mayor. Descuidar el resto de procesos implicados en la prestación de servicios de tecnología tal como nos muestran las principales Bases de Conocimientos, Metodologías, Estándares y normas internacionales genera graves y costosísimas consecuencias operativas y estratégicas.

Por todo ello, tanto los órganos de gobierno, como los directivos e incluso muchos de los profesionales de tecnologías de la información deberían adoptar un enfoque basado en buenas prácticas, invirtiendo tiempo y esfuerzos en una adecuada formación para lograr determinados niveles de madurez de los procesos implicados en el Gobierno, Dirección, Gestión y Operación de servicios de tecnología. Tenga claro el lector que esta inversión estratégica es una palanca de suma importancia para la calidad, la eficiencia y el logro de los objetivos de negocio.

La **Gestión de Servicios** no es solo apagar fuegos; La **Gestión de Servicios** no es solo **Gestión de Incidencias**; se trata de construir un ecosistema tecnológico robusto que impulse y potencia el éxito organizacional en esta maravillosa era digital que nos ha tocado vivir.



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.

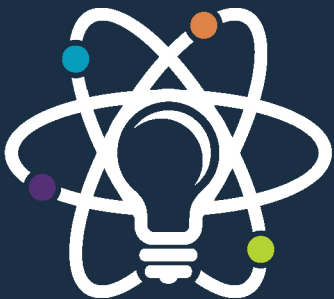
LinkedIn: <https://es.linkedin.com/in/javierperis> **Twitter:** <https://twitter.com/JavierPeris>
Blog: <https://javierperis.com>

Gov Book

Governance

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Manuel Serrat Olmos



Robos de información: ¿evaluamos bien su impacto?

Que en un ataque a una organización o a una persona se produzca un robo de información es casi un clásico en la actualidad. Hasta los ataques de ransomware han evolucionado hacia esa consecuencia. Pero, ¿evaluamos correctamente las organizaciones, o las personas, el riesgo al que nos enfrentamos en caso de sufrir un robo de información?

Una de las preguntas típicas que hago en la primera clase a mis alumnos en materia de ciberseguridad es qué pretendemos proteger cuando establecemos medidas de seguridad en un sistema. Un elevado porcentaje del alumnado se decanta por la respuesta correcta, la información que se trata en dicho sistema, aunque es significativo la porción del alumnado que se decanta por citar la red, o la organización en general, como respuestas.

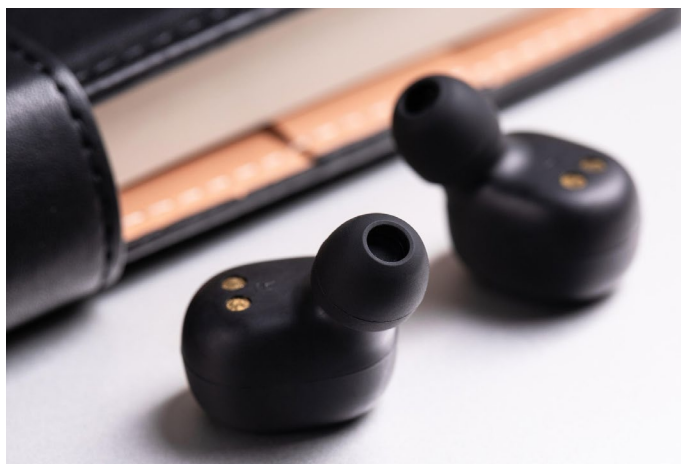
Cuando les confirmo que, efectivamente, es la información el activo más valioso de las organizaciones, planteo dos preguntas relacionadas. La primera es si creen que la protección de su información, la que llevan en su móvil o la que publican en sus redes sociales merece también ser protegida de forma análoga a la información de las organizaciones, y muchos responden que la importancia de esa información es menor. La segunda pregunta que les hago, especialmente a quienes han contestado así la primera pregunta, es si me pueden apuntar en un papel su nombre y su número de tarjeta de crédito, con su fecha de caducidad, el PIN y el CVV. Aquí automáticamente todos responden que no, que con esa información podría hacer compras en Internet.

Este pequeño experimento social con personas jóvenes, nativos digitales, demuestra a mi entender dos cosas: no hay una sensación de que se está desprotegiendo la información personal al publicar en redes sociales, pero sin embargo, en cuanto se toca el tema económico, la actitud cambia. Y ello se debe a que el dinero sí se percibe por este grupo social (y por casi todos los grupos sociales) como un activo valioso, pero la privacidad no.

En las organizaciones, sobre todo en ciertos tipos de ellas, la conciencia de que toda la información que se maneja ha de ser protegida es mucho mayor, aunque los niveles de protección sean dispares y las actitudes reales antes los costes que esa protección requiere también lo sean. Sin embargo, todas las normas de seguridad de la información ponen el acento, precisamente, en la necesidad de que todos seamos conscientes de que esa información es el activo más valioso de nuestros sistemas, y que probablemente sea el único irremplazable (o con un costo enorme de reemplazo).



**CONTINÚA EN
PRÓXIMA PÁGINA**



Es obvio que es así, ya que los sistemas de cómputo se crearon para tratar información, por lo que, por caros que éstos sean, es la información que tratan lo que requiere ser protegido.

En este contexto, merece la pena analizar cada nueva tipología o variante de los ataques que afectan, sobre todo, a los *leaks*, o exfiltración de información. Los ciberdelincuentes saben muy bien el valor de la información en el mercado negro. De hecho, hay incluso estudios que ponen precio a diferentes piezas de información personal o corporativa, aunque en este último caso, al tratarse de ataques dirigidos específicamente a determinadas empresas o organismos públicos, no suelen ser objeto de comercialización aquellos datos confidenciales que se exfiltran. Curiosamente, algunos de los datos más cotizados en ese mercado son los datos de salud de las personas, ya que ello puede permitir campañas de publicidad (legítimas o maliciosas) dirigidas a quienes sufren una determinada enfermedad, tratando de venderles medicamentos o tratamientos específicos (reales o no). Por no hablar de los problemas que pueden generar las suplantaciones de personalidad en transacciones electrónicas en muchos países.

En estos últimos meses se ha conocido un nuevo tipo de ataque de esta clase, al que se ha llamado **bluesnarfing**. Se trata de un ataque cuyo objetivo primordial es la exfiltración de información personal de terminales móviles, gracias al aprovechamiento de ciertas vulnerabilidades del protocolo Bluetooth y al descuido de los usuarios de *smartphones*, por lo que merece la pena darlo a conocer a nuestros lectores con cierto detalle, y sobre todo, aconsejar cómo pueden protegerse del mismo.

El ataque se produce, sobre todo, en zonas concurridas, donde la probabilidad de que el software que han creado los ciberdelincuentes pueda localizar teléfonos vulnerables es mayor. Dicho software analiza cada dispositivo que tenga el interfaz Bluetooth activado, y trata de explotar las

vulnerabilidades conocidas. Dependiendo del software concreto del teléfono atacado, los ciberdelincuentes pueden acceder al almacenamiento del mismo, ya que es uno de las funcionalidades que Bluetooth permite. Una vez accedido el almacenamiento, pueden exfiltrar información, o subir posibles scripts o aplicaciones maliciosas, aunque es cierto que el alcance de esta última amenaza es muy reducido.

Piense el lector sobre toda la información personal que hoy en día acumulamos en nuestros teléfonos: contactos, calendarios, chats, imágenes, documentos, historial de navegación, tarjetas de crédito, etc. Si los ciberdelincuentes son capaces de dejar un dispositivo malicioso en un lugar concurrido haciendo estas tareas de robo de información de forma automatizada, pueden recopilar una ingente cantidad de información de muchas personas, que adecuadamente clasificada y analizada, puede acabar siendo valiosa. Y no será porque no existan mecanismos para hacerlo hoy en día, incluidos los servicios de Inteligencia Artificial al alcance de cualquiera.

Cualquier lector mínimamente avisado ya podrá intuir cómo podemos protegernos de este tipo de ataques, y no, no es evitando ir a lugares concurridos:

1. Como el ataque se produce sobre conexiones Bluetooth activas, basta con llevar el interfaz Bluetooth del teléfono desactivado para que no seamos víctimas propiciatorias de los ciberdelincuentes que usan esta técnica. Sin embargo, hoy en día, con los relojes inteligentes, los auriculares inalámbricos, o los teléfonos integrados en nuestros vehículos, mucha gente lleva el Bluetooth siempre activado para evitar tener que encenderlo y apagarlo cada vez que lo quieran usar. Nuestra recomendación es llevarlo apagado, salvo cuando sea estrictamente necesario.

2. Como el ataque explota determinadas vulnerabilidades conocidas del protocolo Bluetooth y determinadas versiones de su implementación, la medida adecuada es mantener actualizado dicho software, para eliminar esas vulnerabilidades.

3. Es probable que ese ataque, en ciertas versiones de software Bluetooth, solicite permiso para establecer la conexión. Por tanto, debemos rechazar siempre intentos de conexión Bluetooth que no hayamos iniciado nosotros mismos en ese mismo momento. No importa lo atareados que estemos, mejor denegar una conexión legítima por error, que aceptar una conexión maliciosa por prisa.

Como concluirá el lector, para protegernos del *bluesnarfing*, y de otras muchas amenazas, lo principal es el sentido común y la conciencia de qué estamos haciendo cuando hacemos uso de cualquier dispositivo o aplicación informática: tratar información personal o corporativa, que debe ser protegida por se lo más valioso que se tiene entre manos en ese momento.



MANUEL SERRAT OLMOS

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

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

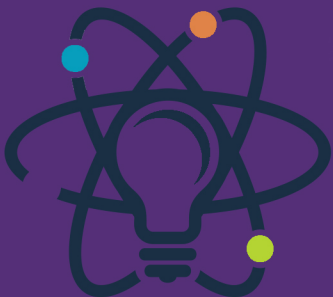
PfM Book

Portfolio

Management

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

En tiempo de descuento para la implantación de Veri*Factu

El 1 de julio de 2025 resultarán exigibles las obligaciones previstas en el Real Decreto 1007/2023, de 5 de diciembre, por el que se aprueba el Reglamento que establece los requisitos que deben adoptar los sistemas y programas informáticos o electrónicos que soporten los procesos de facturación de empresarios y profesionales, y la estandarización de formatos de los registros de facturación, norma dictada al amparo del artículo 29.2.j) de la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT), incorporado por el artículo decimotercero, apartado cuatro, de la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego.

Si bien la obligación prevista en el artículo 29.2.j) de la LGT entró en vigor el 11 de octubre de 2021, ha sido preciso esperar al desarrollo reglamentario de la misma, que como ya se ha avanzado, ha sido producido por Real Decreto 1007/2023, y por el Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación. Ambas normas han sido, a su vez, desarrolladas por la Orden HAC/1177/2024, de 17 de octubre.

Todo lo anterior se traduce en la necesidad de que, antes de 1 de julio de 2025, todos los sistemas de facturación en el tráfico mercantil se hayan adecuado a las obligaciones establecidas en las normas anteriormente indicadas, con independencia de que se refieran a facturas completas o simplificadas (los habituales tiques de caja empleados en los comercios), o a facturas en papel o expedidas electrónicamente.

Y es que, como recuerda el preámbulo del Real decret 1007/2023, el objetivo último es impedir de forma extensiva y general la producción, comercialización, uso o simple tenencia de programas y sistemas informáticos que permitan la manipulación u ocultación de datos contables, de facturación y de gestión; esto es, luchar frente a la coloquialmente conocida como “caja B”.

No será aplicable, como excepción, a las entidades exentas del Impuesto de Sociedades, ni tampoco a aquellas que lleven los libros registros en los términos establecidos en el apartado 6 del artículo 62 del Reglamento del Impuesto sobre el Valor Añadido, que sustenta el conocido como SII o Suministro Inmediato de Información. También existen exclusiones derivadas de la tipología de la operación, como por ejemplo en el régimen especial de la agricultura, ganadería y pesca.

La primera medida estrella de este paquete normativo es la obligación de proceder al encadenamiento de los registros de facturación, de modo que se garantice la trazabilidad de las operaciones (artículos 7 y 12 del Real Decreto 1007/2023), según las especificaciones que se han establecido al amparo de la Orden HAC/1177/2024. Este encadenamiento se produce mediante hashes de los registros, constituyendo un buen ejemplo de libro mayor electrónico centralizado, que podría incluso cualificarse conforme al Reglamento eIDAS modificado, a que me he referido ya en esta sección.

La segunda medida relevante, y la que mayor visibilidad tendrá sin duda, es el sistema de emisión de facturas verificables o Veri*Factu, que es el sistema de información de facturación que remite efectivamente por medios electrónicos a la Agencia Estatal de Administración Tributaria de forma continuada, segura, correcta, íntegra, automática, consecutiva, instantánea y fehaciente todos los registros de facturación generados (artículo 16 del Real Decreto 1007/2023), y que se representa mediante un código QR incorporado a la factura, con información parcial de la factura completa (artículo 6.5 del Real Decreto 1619/2012) o simplificada (artículo 7.5 del Real Decreto 1619/2012).



**CONTINÚA EN
PRÓXIMA PÁGINA**



Conforme al artículo 21 de la Orden HAC/1177/2024, el contenido del código QR será la "URL" del servicio de cotejo o remisión de información por parte del receptor de la factura, del cual se informará en la sede electrónica de la Agencia Estatal de Administración Tributaria, y la siguiente información de la factura, que formará parte de la "URL": El NIF del obligado a expedir la factura, el número de serie y número de la factura expedida: la fecha de expedición de la factura y el importe total de la factura.

Y ello para habilitar que los receptores de facturas puedan comprobar su existencia en la sede electrónica de la AEAT, o incluso remitir directamente esta información a la AEAT,

que cabe imaginar adoptará las medidas oportunas frente a la entidad.

En definitiva, hemos entrado en tiempo de descuento para la aplicación efectiva de estas normas. Veri*Factu es posiblemente la opción menos gravosa en cuanto a la implantación, ya que exime de exigencias importantes con respecto a los sistemas independientes, pero ciertamente profundiza en el modelo de suministro inmediato de información, apuesta que ya vimos se encuentra en la reforma de la Directiva de IVA, conocida como ViDA, y que ha sido recientemente aprobada.



NACHO ALAMILLO

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

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

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

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

Curso de Certificación en: Gobierno de Blockchain & DLT

ISO 23635 Blockchain & DLT Governance Leader

Docente:
Nacho Alamillo

Coordinación Académica
Javier Peris

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

MidMgmt®

MPPM®

MGEIT®

eGob®

Próxima Convocatoria en Directo
JUNIO 2025

Solicita tu admisión en:



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

**Plazas
limitadas**



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

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

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

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

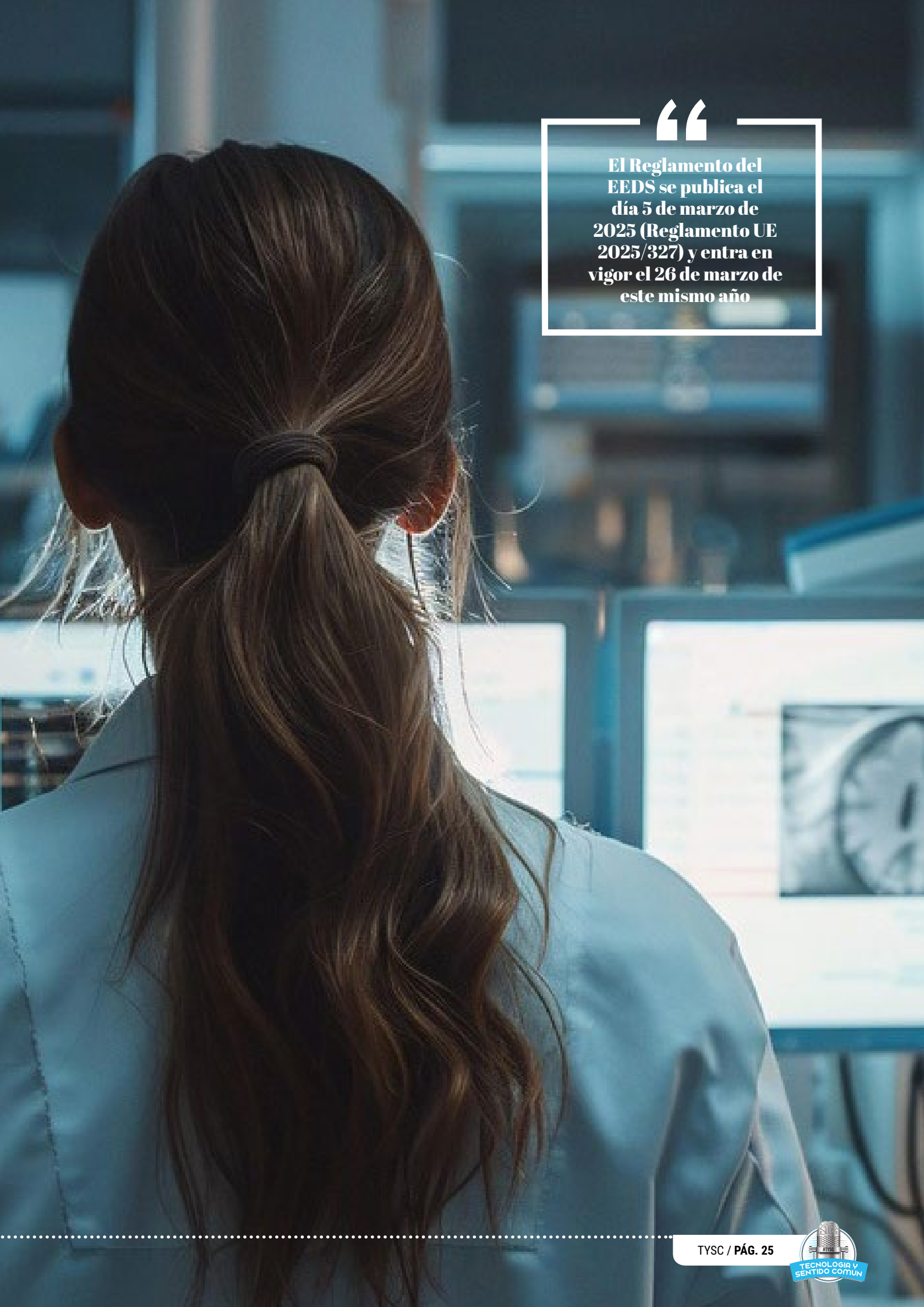
¿Cómo nos afecta esto como **ciudadanos**? Bueno, en principio el EEDS permitirá a los pacientes un acceso más sencillo a sus datos de salud en toda Europa y un mayor control sobre el uso de estos, lo que mejorará la calidad de la atención sanitaria que se les presta, incluso debe permitirse que añadan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

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

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



CONTINÚA EN
PRÓXIMA PÁGINA



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



¿Cómo afecta a las empresas proveedoras de tecnología?

Pues ciertamente son las más afectadas. Aunque se les da de plazo hasta marzo de 2029 para poner a punto sus sistemas informáticos de historia clínica electrónica (HCE), a los que trabajamos en este sector no se nos escapa que el reto es importante: en un sector tradicionalmente "estable" y con clientes "cautivos" esto puede ser una revolución si no se reacciona a tiempo, ya que los sistemas de HCE deben cumplir unas condiciones de interoperabilidad, seguridad y registro indicadas por el Reglamento, además de disponer de una documentación técnica y de usuario para poder certificarse. Si un sistema de HCE no cuenta con dicha certificación, este no se podrá introducir en el mercado ni ponerse en servicio a partir de esa fecha. Algo similar ocurrirá con las aplicaciones de bienestar.

El Reglamento distingue entre uso primario (uso para la asistencia sanitaria propiamente dicha) de los datos de salud, a través de **MiSalud@UE**, y el uso secundario (para investigación, formulación de políticas, salud pública, etc.) de estos mismos datos a través de **DatosSalud@UE**.

Ambas infraestructuras tienen sus características y sus requisitos en dicho Reglamento, pero en definitiva lo que se persigue es dar la importancia que se merece a los datos sanitarios, unos datos que, como suelo recalcar, **pueden compartirse sin deterioro y cuyo valor, aunque disminuye con el tiempo, puede aumentar con el uso y también al combinarlos con otros.**

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



JUAN CARLOS MURIA TARAZON

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

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

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

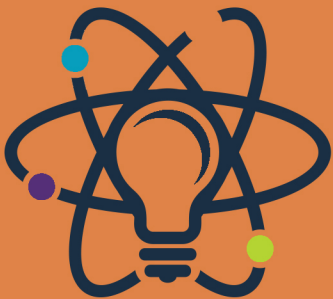
PgM Book

Programme

Management

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE



Estuardo Castañeda

¿Quién es Estuardo?

Estuardo es un hombre con sólidos principios y valores que ha encontrado su vocación en las tecnologías de información y telecomunicaciones, las cuales administra y gestiona desde hace más de 27 años.

Estuardo es un entusiasta, evangelizador y apasionado de la dirección de proyectos, programas, portafolios, quien desde su área de influencia promueve la dignificación de la profesión del director de proyectos.

Estuardo, en un líder de servicio que dedica una cantidad considerable de su tiempo libre para servir a su comunidad.

¿Háblanos de tus éxitos o logros profesionales?

Considero que el éxito se alcanza cuando nos sentimos realizados con quienes somos y con lo que hacemos, y en lo personal me siento realizado por haber dirigido proyectos tecnológicos de alto impacto y valor para la sociedad generando bienestar y particularmente por dirigir uno de los congresos más respetados en mi país. Para mí un factor clave para alcanzar el éxito, ha sido el voluntariado, ya que me ha permitido tener acceso a organizaciones y personas que por ningún otro medio hubiese podido alcanzar.

No podemos separar al profesional de la persona, y el éxito del profesional es el de la persona y viceversa, por ello, para mí uno de los logros más grandes es haber conectado con muchos profesionales en todo el mundo: primero, mediante la tecnología y segundo, mediante el Project Management Institute, el cual ha sido un catalizador que me ha permitido realizar conexiones de manera exponencial y de muy alto valor.

Háblanos de tu experiencia profesional, vivencias incluso anécdotas

Todo comenzó cuando antes de mi intento de ingresar a la Universidad, para lo cual debía someterme a un examen de ubicación que me permitiría elegir una carrera ad hoc a mis expectativas, sin embargo, me topé con la sorpresa que era apto para cursar cualquier carrera de un listado de 16 opciones. Eso me llevó a realizar un análisis sumamente profundo, ya que una decisión tan importante, no debe tomarse a la ligera y fue así como opté por la Ingeniería Electrónica. Esta profesión me permitió laborar en organizaciones que comercializan productos y servicios tecnológicos y a su vez la tecnología me permitió tener acceso a información importante y conocimiento muy valioso, mediante la administración de sistemas de información. Sin saberlo en ese momento, me encontraba laborando en organizaciones basadas en proyectos.

Debo reconocerlo, esto aún no me permitía sentirme realizado, ya que me sueño desde niño era trabajar en la industria de telecomunicaciones. Recuerdo que, a los 9 años, encontré materiales y herramientas que mi padre siempre tenía a mano, y usé mi ingenio e imaginación para elaborar mi primera antena, la cual ni de chiste era funcional, solo era una réplica artística a escala. Con cada día que pasaba y al observar el paisaje urbano en mi ciudad, podía notar una gran variedad de antenas y ¡quería replicarlas todas!



CONTINÚA EN
PRÓXIMA PÁGINA





REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

En mi país contamos con un sistema educativo que divide la secundaria en dos y los primeros años se denominan “ciclo básico” y la segunda mitad “diversificado” porque es acá donde son diversas las opciones para campos de estudio como un bachillerato o un perito en especialidades como contabilidad, mecánica, dibujo técnico y electrónica. Fue de esta manera como llegué a los estudios de un bachillerato industrial y perito en electrónica, sin saber que esta base me permitiría optar a la ingeniería y luego llegar a mi aspiración de trabajar en telecomunicaciones. En su momento no lo sabía, pero esto es aprendizaje basado en proyectos.

Fue en el año 2005 que doy ese salto de fe y logro incorporarme a una organización basada en proyectos de telecomunicaciones, la cual fue el trampolín que me permitió años después integrarme a las organizaciones de telecomunicaciones más grandes e importantes a nivel mundial, desde la organización más relevante de las Américas, pasando por la organización más respetada en España hasta el gigante asiático que hoy día lidera dicha industria. Para esta época, ya sintiéndome realizado y con el niño interior feliz y contento de hacer lo que siempre anhelé, observo a mi alrededor y comprendo que existe una diferencia abismal entre la dirección profesional de proyectos y la gestión empírica, lo cual me inspiró a profesionalizarme en la dirección de proyectos y fue así como en el año 2010, analizando las opciones, encuentro una organización la cual ofrecía formación en Project Management para la industria de telecomunicaciones, y utilizaba como base la guía de proyectos del PMBOK versión 4 y de esta manera fue como conocí al Project Management Institute. De inmediato me pongo manos a la obra y comienza mi búsqueda por este conocimiento, el cual no sabía que desconocía. Logré ponerme en contacto con uno de los líderes del capítulo potencial en Guatemala, y desde ese momento me integre como voluntario y ahora, más de 10 años después, tengo la dicha de presidir la junta directiva.

Me considero un eterno aprendiz y continuo mi travesía de aprendizaje, reuniendo experiencias en transformación digital, transformación ágil, Oficinas de Proyectos (PMO), Centros de Excelencia (CoE), desarrollo de productos y todo aquello que brinde un nuevo nivel de excelencia a todo lo que hago.

Háblanos de PMI Guatemala, su trayectoria sus objetivos y retos

PMI Guatemala, fue reconocido como capítulo formal el 15 de abril de 2014. Para ello, los esfuerzos iniciaron en el año 2010, cuando un grupo de profesionales se organizó para dar vida al capítulo. En la primera sesión se reunieron profesionales

de industrias como: tecnologías de información, telecomunicaciones, banca y servicios. PMI Guatemala tiene como objetivo primordial dignificar la profesión del director de proyectos y a través de los años ha obtenido relevancia e influencia en varias esferas de la sociedad guatemalteca. En el año 2016 se transformó el congreso nacional de proyectos y se renombró como “Project Management Summit” y para fines prácticos hoy día se le conoce como “PM Summit”, el cual se realiza en la ciudad colonial de Santiago de los Caballeros conocida como Antigua Guatemala, reconocida como patrimonio cultural de la humanidad por UNESCO en 1979.

Hoy día PMI Guatemala no solamente es el referente en temas de dirección profesional de proyectos, sino también, es una organización sin ánimo de lucro que promueve la convivencia con otras organizaciones con objetivos similares como IPMA Capítulo Guatemala, IEEE Sección Guatemala, colegios profesionales y ONG’s.

Uno de los mayores retos que enfrenta, es el desconocimiento de las organizaciones sobre el valor y la importancia de la dirección profesional de proyectos, por ello nuestro mayor compromiso es promover el valor de las certificaciones y el de los profesionales que las ostentan.

Nuestra estrategia en una sola frase es: “Dignificar la profesión del Director de Proyectos”, con ello realizamos y promovemos todo aquello que nos permita dignificar a nuestros asociados, voluntarios y todas las personas que laboren ejerciendo dicho rol.

¿Cómo fueron tus comienzos en el mundo de los Proyectos?

Sin saberlo, desde mi primera experiencia laboral, me encontraba trabajando en organizaciones basadas en proyectos, programas y portafolios. Como lo menciono en una pregunta anterior, conocí una certificación, la cual tenía como base la guía del PMBOK de PMI.

Conservo vivo el recuerdo de que en ese momento de iluminación me encontraba supervisando actividades clave para un proyecto y fue en ese momento que decidí conocer a PMI, ¡y eso me cambió la vida para siempre!

Conocí la dirección profesional de proyectos y esto tuvo un impacto positivo de manera inmediata en la manera en la que trabajaba. Los proyectos a mi cargo tenían una alta probabilidad de éxito, porque lo primero que puse por obra fue la adecuada gestión de Stakeholders.



**CONTINÚA EN
PRÓXIMA PÁGINA**

Nuestro invitado a #TYS



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

A lo largo de los años establecí la manera en la que trabajo: primero, me enfoco en las personas, segundo, me enfoco en los procesos y tercero, me enfoco que los resultados. Porque para dar resultados, debemos conocer los procesos y colaborar con las personas. Para mí es muy importante la gestión de Stakeholders y sus expectativas. En los proyectos no solamente existe un tema contractual o de compromiso, sino también de expectativas, ya que se espera que los proyectos beneficien a una organización, una comunidad o un país o región y que el producto resultante de ese esfuerzo genere un impacto positivo y de buena imagen y reputación.

En cierta ocasión me encontraba en una reunión de planificación y en ella, quien lideraba la sesión resalto la importancia de gestionar adecuadamente a los **"Steak Holders"** porque ellos tenían la "carne" y nosotros debíamos ir a por ella. Eso me dejó en perplejo ya que estaba tergiversando por completo el significado de "Stakeholders". Este fue el detonante que me llevó a adquirir todo el conocimiento posible para no cometer esa clase de errores y de esa cuenta llegue a conocer los enfoques de PMI, IPMA, Prince2, Scrum, Kanban, normas ISO, XP, Crystal, etc., para apoyar a personas y organizaciones a encontrar el modelo de dirección y/o gestión de proyectos que más se adecuara a sus necesidades.

¿Cómo según tú aportan valor los Proyectos a las organizaciones?

Los proyectos traen consigo mejoras a la organización, siempre y cuando se capitalicen de manera oportuna las lecciones aprendidas y el failure management. Muchos proyectos requieren de sistemas específicos y en muchos casos, los sistemas imperantes no tienen la capacidad de soportar el ciclo de vida del proyecto ni el ciclo de vida del producto, es acá donde se requiere de pensamiento sistémico para dar vida a la innovación, la cual es clave para ampliar la capacidad de las organizaciones ya que les permite robustecer su operación mediante las adquisiciones de los recursos adecuados para poder llevar a cabo proyectos. Esto a su vez les permite diversificar su cartera de servicios y obtener una mayor cantidad de clientes.

Los proyectos permiten a las organizaciones pasar de un estado actual a un estado futuro con mayor capacidad e influencia.

Los proyectos tienen el potencial de mejorar considerablemente la imagen y reputación de las organizaciones y de los profesionales que los dirigen.

¿Cuáles crees que son los factores a corregir o mejorar respecto del Cambio Organizacional por parte de las organizaciones?

Las organizaciones más añejas y grandes se vuelven paquidérmicas para implementar cambios en sus formas de trabajo, y hoy día, en un mundo tan cambiante, más que nunca antes. La agilidad organizacional nos recomienda romper silos para que organicemos equipos auto organizados o células ágiles integrando áreas de las organizaciones que permitan la generación de productos lo más pronto posible. Pero ¿qué sucede en la alta dirección? Es acá donde vemos la necesidad de enfatizar la diferencia entre agilidad estratégica y agilidad táctica.

¿Qué áreas de mejora te parecen más importantes o relevantes en el Gobierno y la Gestión de las organizaciones?

A lo largo de los años he podido observar de cerca como las organizaciones contratan profesionales de la dirección de proyectos, programas y portafolios y los nombres de los cargos suenan muy atractivos, sin embargo, los tratan como gestores de proyectos y las áreas operativas consideran al project management como una actividad sin valor. Por lo tanto, considero que una mejora importante y urgente es que las organizaciones empoderen a los profesionales de la dirección de proyectos. Para este objetivo es clave mejorar la cultura organizacional y la gestión del cambio humano y adecuarlas para que el director de proyectos cuente con la autoridad necesaria para hacer que las cosas pasen en cada proyecto, programa o portafolio.

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

Tuve mi primer contacto con una computadora personal cuando tenía 8 años de edad y desde entonces he tenido la oportunidad de tener acceso a tecnología de punta, lo cual he logrado gracias a mi profesión y en los últimos años gracias al project management. Me siento orgulloso de ser pionero en muchas áreas y esto lo he conseguido gracias a la tecnología, las telecomunicaciones y el project management.



**CONTINÚA EN
PRÓXIMA PÁGINA**





PM Summit

By PM Guatemala

mala,

26 de Julio de 2024

Nuestro invitado a #TYS

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



La única constante en mi vida ha sido el cambio y en cada etapa, no solamente me adapto, sino que también me transformo para mantenerme relevante. Hoy día uno de los logros más importantes de mi vida es presidir una junta directiva, liderar una comunidad y representar a un país, desde mi rol de presidente de PMI Guatemala.

¿Qué consejos le darías a los directivos que no conocen las ventajas de la Gestión de Proyectos?

La gestión de proyectos es posible que parezca un gasto, sin embargo, es una inversión, porque no contar con la gestión profesional de proyectos en una organización, puede que sea mucho más caro que tenerla. Ya que la gestión profesional de proyectos nos permite incrementar las probabilidades de éxito en los proyectos y reduce el re trabajo y el sobrecosto.

Mi consejo es: si tu organización aun no gestiona proyectos de manera profesional, contrata un consultor experto en temas de proyectos y asígnale un proyecto estratégico. Al finalizar el proyecto evalúa los resultados. Con ello podrás comparar un proyecto gestionado profesionalmente y otro gestionado como habitualmente se realiza en tu organización. Ahí podrás ver la diferencia y estoy seguro que optarás por la dirección profesional y esto transformará tu organización y la experiencia de tus clientes se verá supremamente beneficiada y te darán más trabajo, más proyectos.

¿Qué les dirías a las organizaciones que no conocen lo que hace el PMI en Guatemala?

Los invito cordialmente a que nos acompañen en nuestros eventos presenciales y virtuales y en especial, los invito a la decimoprimer edición del PM Summit, el cual se realizara el 25 de julio en Santo Domingo del Cerro, Antigua Guatemala. Este evento es la muestra más completa de todo lo que somos y hacemos, ya que el despliegue logístico es importante y la calidad de los conferencistas es sin igual.

Somos una comunidad de profesionales, donde nos apoyamos mutuamente para que juntos conozcamos buenas prácticas de dirección de proyectos que se pueden adaptar a cualquier proyecto de cualquier industria.

¿Cómo sería el futuro de una sociedad sin Proyectos?

Todo lo que nos rodea es un proyecto, y sin proyectos no tendríamos más expresiones artísticas, innovación e incluso una vida más cómoda, la ciencia y la tecnología se estancarían y recordemos que lo que no crece, ¡decrece!

Conclusiones

Dependiendo del enfoque la dirección de proyectos, puede ser un arte, una disciplina y/o una ciencia. Pero por el impacto que esta puede tener, es más considerada un arte, porque hacer que las cosas sucedan en el momento oportuno, que las personas se comuniquen adecuadamente mediante en canal correcto y que se gestionen expectativas, requiere no solamente de management, sino también de leadership.

Las organizaciones quieren evolucionar de un estado actual hacia uno mejor y para ello tienen dos caminos, el de la profesionalización de los servicios que ofrecen o el de continuar de manera empírica esperando que el universo conspira a su favor. La dirección profesional de proyectos, no es barata, ¡pero es más caro no tenerla!

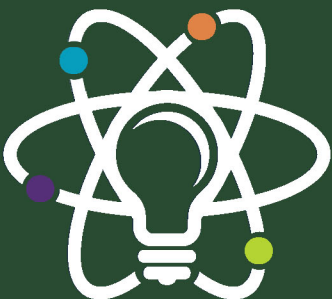
La dirección profesional de proyectos incrementa las probabilidades de éxito de los proyectos y los proyectos exitosos traen prestigio y buena reputación a las organizaciones y esto lleva a las empresas a ser reconocidas por la calidad de sus productos y formas de trabajo.

S&O Book

Services & Operations

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Marlon Molina

Los robots humanoides son tendencia

La creación de robots humanoides es tendencia y emerge como un resultado natural con el desarrollo acelerado de la Inteligencia Artificial. Boston Dynamics lleva décadas desarrollando sus modelos, muy populares en los congresos, ferias, y en las universidades. Actualmente en propiedad de Hyundai Motor, desarrolla productos para ayuda en fábricas y el transporte de todo tipo de mercancías. Pick es un modelo humanoide que trabaja incansablemente moviendo cajas en los almacenes de distribución. Según explica Aya Durbin, "la razón para hacer robots humanoides es ayudar a los humanos".

ENTORNOS HUMANOS

El desarrollo de robots humanoides no parece tener sentido desde un punto de vista mecánico. Hacer que un robot se desplace dando pasos sobre dos pies es más difícil que hacerlo con uno de cuatro patas, o uno con ruedas.

La razón principal para crear robots humanoides con pies y manos, es para que trabajen en entornos creados para los humanos. Es un enfoque curioso si se piensa que los entornos creados para humanos no son los óptimos en distribución, seguridad, y accesibilidad. Un enfoque humanoide adapta el robot al entorno y no el entorno a una solución más eficaz.

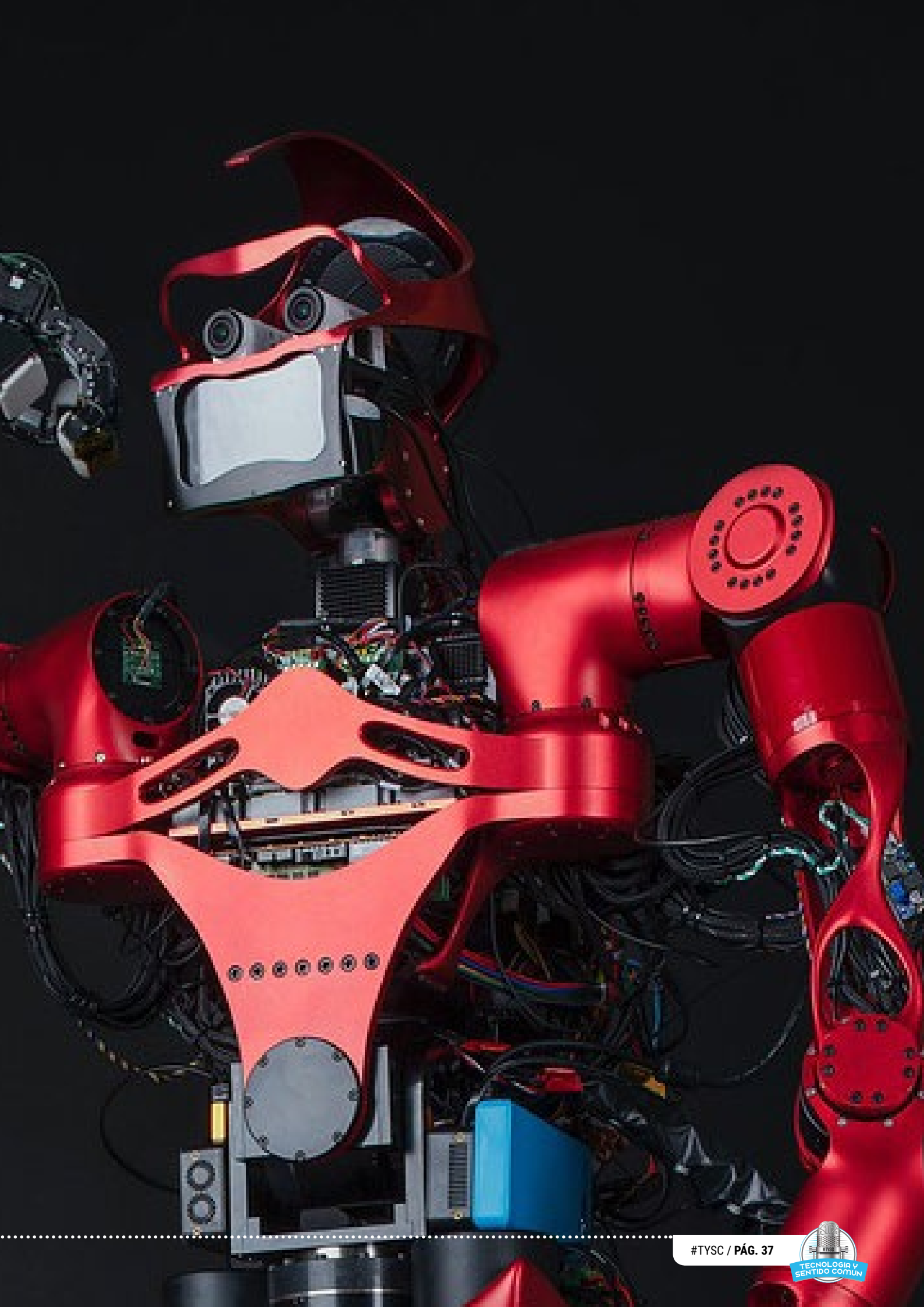
Atlas de Boston Dynamics requiere operar en un espacio iluminado, donde las piezas que manipula están a la altura de una persona, cuando un robot podría diseñarse para mover piezas a alturas más bajas o más altas, y desde luego sin necesidad de iluminar, o acondicionar el espacio tal como lo exige un trabajador humano.

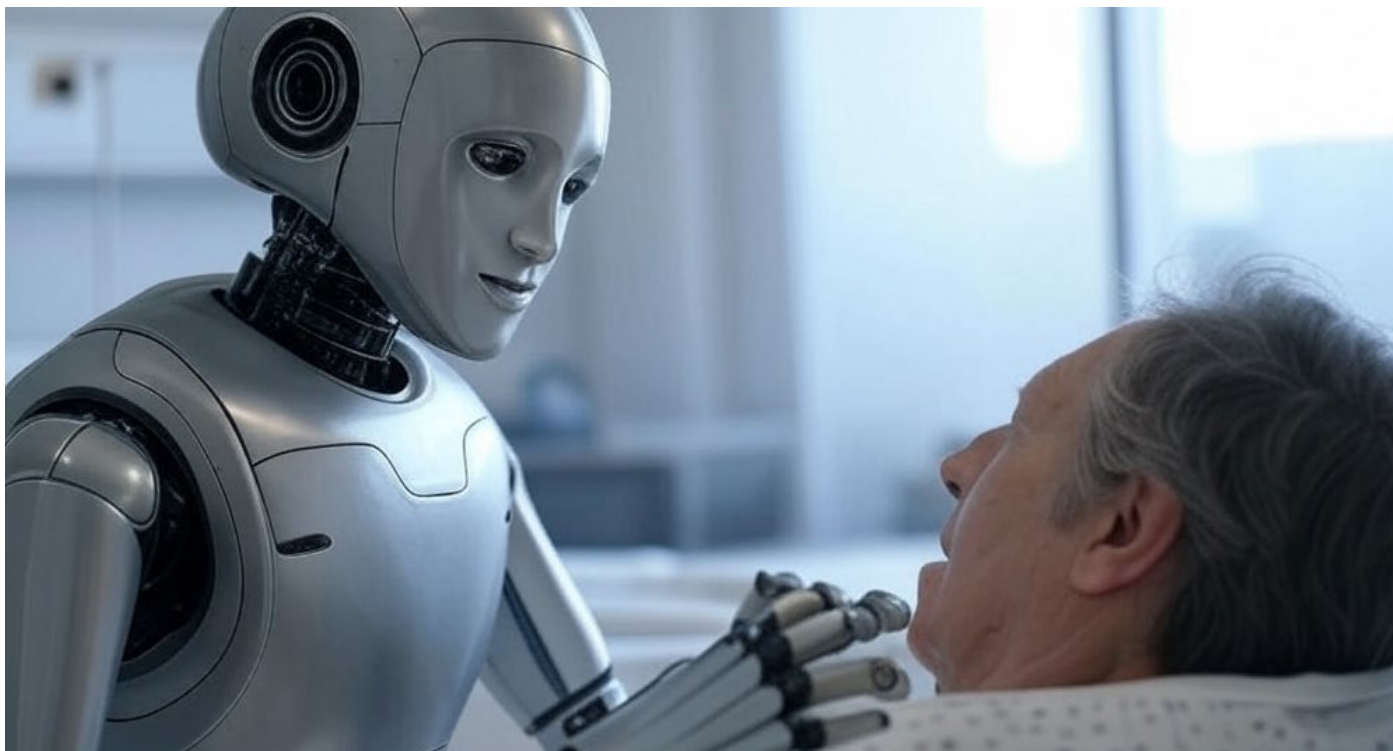
"Económicamente es absurdo sustituir los brazos robóticos por robots humanoides, pero los humanos que financian proyectos prefieren las fotos de una moda porque no entienden la optimización"

Es probable que Elon Musk haya sido el impulsor de la moda y la tendencia de los robots humanoides. Optimus Tesla tiene tres años desde su creación, y un año escaso de su presentación en sociedad. El robot ha hecho sus actuaciones rompiendo un huevo, haciendo ejercicio, y conduciendo un coche Tesla autónomo, el cual ya es un robot. El robot tiene un precio de mercado superior a los 25.000€, para realizar tareas que hace un robot de cocina de tan solo 100€. Pero ahí está la magia de Elon Musk y Tesla, el diseño es impresionante, y es el primer robot humanoide que exhibe la marca en el pecho, y se le ha visto bailando en una disco.



CONTINÚA EN
PRÓXIMA PÁGINA





La apuesta más reciente e interesante podría ser la propuesta de la empresa Agility Robotics, que presenta el robot medio humanoide con el nombre “Digit”, que hace todo lo que es capaz de hacer Optimus o Atlas, pero sin la necesidad de una cabeza, o unos dedos articulados. Los creadores de la empresa dicen del robot que “es un robot pragmático”, algo así como “sin tonterías” para que realice los trabajos que se quiere que haga, no para bailar o dar paseos en coche. Pero es feo, algo que seguramente es más fácil de trabajar una vez logrado un dispositivo eficiente.

UNA VISIÓN DE LAS TECNOLOGÍAS PARA EL AHORRO DE TRABAJO (LABOR-SAVING-TECH)

La propuesta de Agility Robotics no se basa en que los humanos tengan un “esclavo”, o sustituir el trabajo que hace un humano, sino en potenciarlo. Este concepto se está expandiendo la tendencia para crear tecnologías que ahorren **esfuerzo** en el trabajo y las tareas que desempeñan los humanos.

Algunos ejemplos:

- En vez de sustituir a una enfermera con sus tareas con un paciente con movilidad reducida, el robot humanoide le ayudan a levantar el paciente, a movilizarlo, a mantenerlo

en una posición mientras se realizan algunas tareas como puede ser el aseo.

- En vez de sustituir a un empleado en un almacén quien tiene que descargar materiales pesados y peligrosos, lo hace un humanoide para evitar lesiones y accidentes al humano.

- En vez de sustituir a un empleado en un restaurante de comida rápida que está en la cocina friendo patatas, ahora lo haría un humanoide sin miedo a quemarse con los aceites o a dañarse los pulmones por respirar el vapor que produce el aceite mientras se quema.

Este último ejemplo es el que anunció Yum Brands, el dueño de cadenas de comida rápida como Taco Bell, Pizza Hut, y KFC. La empresa ha anunciado una inversión superior a los mil millones de dólares en tecnología “labor saving”, que además de mejorar el rendimiento cuida a sus empleados.

En una entrevista, Rene Hass actual CEO de ARM, ha manifestado que el año 2025 es el momento ideal para aprovechar la ola de creación de robots, que en resumen es, poner motores de IA en dispositivos.



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 Parla-mentos de las Américas en la OEA, es profesor en varias Escuelas de Negocio, y es asesor de varios Consejos de empresa en España e Internacionales. En 2019 Cherwell le incluyó en el TOP 5 de los líderes técnicos de la transformación digital en EMEA.

LinkedIn:

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

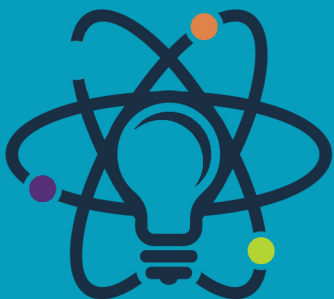
PjM Book

Project

Management

Body of Knowledge

P4MGO!®



P4MGO!

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



Ricard Martínez Martínez

IA

Bring Your Own AI (BYOAI)

Lo confieso, soy incapaz de dedicar una sola línea a loar las virtudes de **deepseek**. Tampoco soy muy ducho en muchas otras herramientas y no es por incapacidad. Me permito usar IA en la medida en la que la generación de recursos de investigación me lo permiten ya que la política universitaria de compras en este campo sigue por definir. Existen servicios gratuitos como **NotebookLM** que me puedo usar para el análisis y síntesis de textos y avanzar en establecer su relevancia y utilidad. Ahora bien, deben ser exclusivamente textos de fuentes abiertas como artículos doctrinales, jurisprudencia, guías etc. Un servicio que cada vez me produce mayor satisfacción es **Consensus: AI-powered Academic Search Engine**, como herramienta asociada a la búsqueda bibliográfica y la localización de trabajos relevantes. Pero todas ellas tienen algo en común: utilizo la versión free, y en esta versión las garantías que recibo son razonables, aunque no parece claro que no vayan a aprovechar toda la información que les proporciono.

Uso, previo religioso pago la integración de Copilot con Microsoft, Perplexity AI y DeepL. De hecho, trato de utilizar estas herramientas con cargo a recursos de investigación de modo que en la medida de lo posible exista una vinculación clara y una obligación jurídica con la institución de modo que pueda asegurar una eventual demanda o reclamación ante cualquier práctica indebida. Pero les aseguro que esta circunstancia deriva de un ejercicio de diligencia autoimpuesta. No proviene de una circular o instrucción precisa.

Y esta es precisamente mi mayor preocupación. Al parecer lo que yo hago se llama BYOAI que en mi caso podría calificarse BYOAI responsable. Esta práctica consiste en la tendencia de los empleados a utilizar sus propias herramientas de inteligencia artificial para realizar tareas

diarias sin necesariamente contar con la aprobación explícita de la organización. Así que de repente si nota que sus empleados son más eficientes, han cambiado el modo de emitir sus informes y parecen tener mucho tiempo libre, sospeche.

Si Perplexity no ha alucinado y ha leído bien los estudios como el **Índice de Tendencias del Trabajo 2024 sobre el Estado de la Inteligencia Artificial en el Trabajo** y los informes de **T-Systems e InfoJobs** un 78% de los trabajadores en España ya utilizan sus propias herramientas de IA en el trabajo, una cifra que aumenta al 80% en empresas de tamaño mediano. Además 1 de cada 3 trabajadores (32%) en España emplea herramientas de IA en su día a día laboral, un incremento significativo respecto al 18% reportado en 2023.

El 75% de los trabajadores del conocimiento utiliza herramientas de IA generativa, y casi la mitad comenzó a hacerlo en los últimos seis meses. La brecha generacional es sorprendente ya que el 85% de los empleados de la Generación Z (18 a 28 años) utilizan IA personalizada y más del 70% de los baby boomers (mayores de 58 años) también emplean estas herramientas. Y esto está ocurriendo sin que existan directrices empresariales precisas.

Permítanme proponerles tres escenarios: a) una empresa solicita a un técnico una evaluación de las tendencias en mercados de futuros; b) se encarga a expertos en prevención de riesgos laborales la elaboración de un plan de contingencia para una determinada situación productiva; c) un médico en formación utiliza una IA para realizar diagnósticos diferenciales.



CONTINÚA EN
PRÓXIMA PÁGINA



Obviamente son supuestos puramente teóricos cuya coincidencia con la realidad sería una pura especulación. Evidentemente se trata de una pura ficción del articulista con fines pedagógicos y es imposible que esté sucediendo. Porque, si sucediera, resultaría que su universidad existe personal investigador vinculado por obligaciones de confidencialidad, -Non Disclosure Agreements (NDA)-, subiendo documentos confidenciales a entornos radicados en una potencia extranjera que ejerce un control férreo sobre sus empresas con particular atención a todo aquello que pueda explotar. Podría suceder, que se afectase al derecho fundamental a la protección de datos de sus clientes ya que al fin y al cabo se usan recursos “free” sin el compromiso propio de un encargado del tratamiento. Es más, en el corto plazo podría incumplirse el Reglamento de la Unión Europea sobre Inteligencia Artificial.

Por otra parte, ante una oferta que crece de manera exponencial nadie nos asegura que no se trate de una herramienta maliciosa, que se produzcan robos o filtraciones de información incluido ese código de programación que subimos para depurarlo más rápidamente. Y podemos añadir un elemento adicional ya que en un mismo contexto de trabajo vamos a generar un ecosistema que no va a ser disruptivo sino fragmentado. Una parte de la plantilla trabajará de acuerdo con procedimientos y estándares tradicionales mientras que la otra va a incorporar una nueva cultura. Y no sólo se trata de que usen IA sino del marco de referencia epistemológica que genere cada prompt. Al fin y al cabo, las metodologías de análisis de la información y su output dependerán de las fuentes que maneje el LLM, del idioma, del enfoque y profundidad del modelo y de la propia cultura del empleado. Y ello implica el empleo de

procesos que la organización no sólo no ha solicitado, sino que puede ser contraria a su propio modelo de gestión. Y todo esto puede ser desplegado por un empleado prudente, responsable y con formación o por su opuesto.

El despliegue de la inteligencia artificial en cualquier organización debe responder a decisiones conscientes y debidamente planificadas. La herramienta debe ser funcional a los intereses y objetivos de la organización, útil para el despliegue de sus tareas y ofrecer garantías de seguridad y robustez. Además, el personal debería ser formado adecuadamente. En los tres ejemplos ofrecidos más arriba se plantean situaciones en las que pueden generarse riesgos muy graves. Por ello es esencial integrar las herramientas de inteligencia artificial en sus sistemas y procesos para aprovechar sus beneficios sin comprometer la seguridad y considerando el impacto en el conjunto de la organización en todas sus dimensiones.

Habida cuenta de nuestro perfil de lector es muy improbable que Vd. no haya usado al menos un LLM. La experiencia es particular. En primer lugar, es inevitable humanizar a la máquina cuando se le habla en lenguaje natural. Por otra parte, salvo que se realicen preguntas exploratorias e intencionales, los resultados que devuelve suelen ser coherentes en su contexto. Sólo una atenta revisión experta permite identificar inconsistencias o alucinaciones. Además, estas herramientas acaban resultando adictivas y ocupan cada vez un mayor espacio como instrumento profesional.

El uso de la IA puede revolucionar la eficiencia y productividad, pero el BYOAI puede tener efectos perniciosos. En primer lugar, desde el punto de vista del entorno profesional y la evaluación del desempeño puede introducir asimetrías e inducir a error sobre las capacidades de nuestros colaboradores. Llevado al extremo puede atribuir virtudes a personas no capacitadas y el engaño funcionará hasta que éstas sean incapaces de gestionar un error o alucinación de la IA. O cuando no sean conscientes, por ejemplo, de estar liberando secretos empresariales. O en el caso de que el diagnóstico diferencial falle y una persona muera.

Si en lugar de invertir en formación y de rediseñar el enfoque de procesos de su organización desde la IA permite o alienta el BYOAI está apostando por promover un entorno de trabajo que corre el riesgo de acabar siendo disfuncional, irresponsable e imprevisible. Y ésta debería ser la menor de sus preocupaciones. En caso de producirse algún evento dañoso aprenderá un concepto latino muy interesante: la culpa o negligencia in vigilando. Incluso un juez de la era analógica transportado en el tiempo sabría que los dueños o directores de un establecimiento o empresa responden respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones. Vd. no debería olvidarlo.



RICARD MARTÍNEZ

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

LinkedIn:

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

Curso de Certificación en:

Estrategias de Cumplimiento para Inteligencia Artificial

IA Compliance Strategist

Docente:
Ricard Martínez

Coordinación Académica
Javier Peris

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

MidMgmt®

MPPM®

MGEIT®

eGob®

Próxima Convocatoria en Directo
MARZO 2025

Solicita tu admisión en:



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

**Plazas
limitadas**



Las CiberAlmenzas del 2034. Ciberguardaespaldas

En el año 2034, el ciberespacio se ha convertido en un campo de batalla, donde ciberdelincuentes, terroristas y ejércitos están en permanente conflicto. Todos ellos tienen a su disposición armas basadas en la Inteligencia Artificial para identificar vectores de ataque y mecanismos de penetración en todos los sistemas. Las empresas, los sectores estratégicos, los sistemas de salud, justicia, los servicios de inteligencia y las fuerzas armadas de todos los países, combaten 24/7 por el control de la información. Incluso los ciudadanos contratan servicios de guardaespaldas digitales que protegen su identidad real y virtual para evitar intrusiones en sus sistemas BCI y en sus entornos virtuales.

LA INTELIGENCIA ARTIFICIAL EN EL CORAZÓN DE LA CIBERSEGURIDAD

Gianluca comienza su jornada a las 5:30 a.m. en su apartamento de Málaga. Mientras prepara su café, revisa las alertas generadas por "AiSecSis", su sistema de inteligencia artificial personalizado. AiSecSis no es un simple programa; es una entidad digital avanzada que ha evolucionado a partir de los primeros sistemas de detección de amenazas desarrollados en la década de 2020.

"Buenos días, Gianluca," comunica AiSecSis a través del implante auditivo de Gianluca. "He detectado tres anomalías críticas durante la noche. La más urgente afecta a Ana Gómez."

Ana Gómez es una influyente empresaria tecnológica especializada en interfaces cerebro-computadora, una tecnología que en 2034 permite a millones de personas conectar sus cerebros directamente a sistemas digitales para mejorar sus capacidades cognitivas y controlar dispositivos con el pensamiento.

Caso: Ataque a Sistemas BCI

Gianluca accede a su estación de trabajo holográfica y examina los datos. AiSecSis ha detectado un intento de intrusión en los sistemas BCI de Ana, utilizando un malware generado por IA que evoluciona dinámicamente para evadir detección.

"El patrón de ataque muestra similitudes con operaciones previas de 'Black Phoenix'," informa AiSecSis, mostrando un análisis comparativo de vectores de ataque. "Probabilidad de coincidencia: 87.3%."

Black Phoenix es un grupo criminal internacional especializado en el robo y manipulación de datos neuronales, una evolución de los grupos de ransomware que operaban en la década de 2020. Su objetivo: acceder a los datos y información de Ana para manipular sus decisiones empresariales y extraer información confidencial sobre tecnologías emergentes.

Gianluca activa su interfaz neural y se sumerge en una representación tridimensional del ataque. Lo que ve es preocupante: el malware está utilizando algoritmos de aprendizaje profundo para adaptarse a las defensas del sistema BCI de Ana.

"AiSecSis, implementa contramedidas adaptativas y activa el protocolo Escudo Neuronal," ordena Gianluca.

El sistema despliega instantáneamente una serie de defensas:

•**Respuesta Autónoma:** AiSecSis implementa contramedidas automáticas que bloquean temporalmente el acceso no autorizado mientras Gianluca analiza el origen del ataque.

•**Análisis Predictivo:** Utilizando datos históricos de ataques similares, AiSecSis predice los próximos movimientos de los atacantes y refuerza preventivamente las áreas vulnerables

•**Aislamiento Neural:** El sistema BCI de Ana es temporalmente aislado de la red global para prevenir la extracción de datos sensibles.

"Ataque contenido temporalmente," informa AiSecSis. "Sin embargo, la firma digital sugiere que este es solo un ataque de distracción. Detecto actividad sospechosa en los nodos secundarios."

Gianluca comprende inmediatamente la estrategia: mientras todos los recursos se concentran en defender el sistema principal, los atacantes intentan infiltrarse por sistemas aparentemente menos importantes. Esta táctica, conocida como "Maniobra Fantasma", se ha vuelto común en los últimos años.

"Contacta con la Agencia Nacional de Ciberseguridad (ANC)," ordena Gianluca. "Necesitamos coordinar una respuesta conjunta."

ROBOTS Y DRONES VIRTUALES: GUARDIANES DEL MUNDO DIGITAL

Mientras la ANC moviliza sus recursos para ayudar con el caso de Ana Gómez, Gianluca recibe otra alerta urgente: un grupo criminal ha hackeado drones autónomos para atacar físicamente los centros de datos de Quantum Dynamics, una empresa cliente especializada en computación cuántica.

Caso: Hackeo a Drones Autónomos

"Los drones han sido comprometidos a través de una vulnerabilidad en su sistema de navegación," informa AiSecSis. "Están programados para impactar contra el centro de datos principal en aproximadamente 18 minutos."

Gianluca activa inmediatamente el protocolo de respuesta híbrida, que combina defensas físicas y digitales: "Despliega los drones defensivos y activa los robots de perímetro".

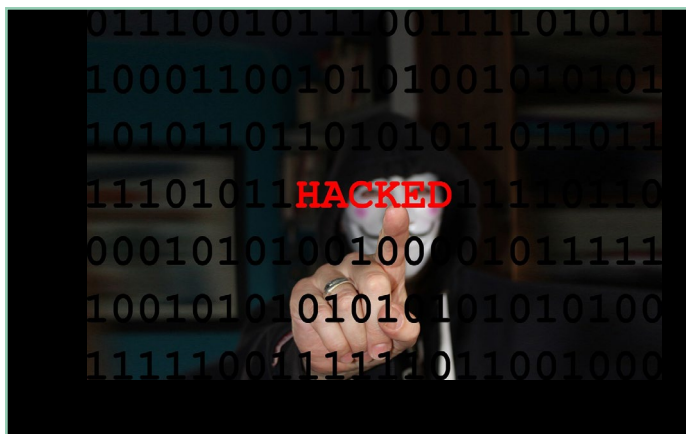
En cuestión de segundos, desde una base cercana a las oficinas de Quantum Dynamics, se lanzan drones defensivos equipados con contramedidas electrónicas. Estos drones, desarrollados inicialmente para aplicaciones militares, pero ahora disponibles para seguridad civil, utilizan tecnología de interferencia dirigida para interrumpir las comunicaciones de los drones hostiles.

Simultáneamente, robots terrestres autónomos comienzan a patrullar el perímetro del edificio, equipados con sensores avanzados y capacidades defensivas no letales.

"Los drones defensivos han interceptado 70% de las amenazas," informa AiSecSis mientras Gianluca empleando su BCI está monitorizando el perímetro de la empresa gracias a las cámaras de vigilancia y la información que proporcionan los satélites destinados a la Ciber protección de infraestructuras estratégicas. "Los robots de perímetro están en posición."



CONTINÚA EN
PRÓXIMA PÁGINA



Gianluca observa a través de su visor de realidad aumentada cómo los drones defensivos neutralizan las amenazas restantes. Los drones hostiles, ahora bajo control, son dirigidos a una zona segura para su posterior análisis forense.

"AiSecSis, ejecuta un análisis profundo del código malicioso utilizado para hackear los drones," ordena Gianluca.

La IA comienza a desensamblar el código, revelando una firma digital asociada con "Crimson Veil", un grupo terrorista digital conocido por sus ataques contra infraestructuras críticas.

"El código contiene elementos avanzados de IA autónoma," informa AiSecSis. "Sugiere colaboración con un actor estatal. Recomendando informar al Comando Cibernético Nacional."

Gianluca asiente. La línea entre ciberdelinquentes y actores estatales se ha vuelto cada vez más difusa en los últimos años, con naciones utilizando grupos criminales como proxies para sus operaciones cibernéticas.

INGENIERÍA DEL COMPORTAMIENTO: EL FACTOR HUMANO

Al día siguiente, Gianluca enfrenta un caso que ilustra cómo la ingeniería social ha evolucionado hasta convertirse en una ciencia precisa. Una campaña masiva de desinformación está causando pánico entre los ciudadanos mediante deepfakes ultrarrealistas que simulan declaraciones falsas de líderes gubernamentales anunciando una crisis económica inminente.

Caso: Desinformación Masiva

"Los deepfakes están siendo distribuidos a través de redes neuronales descentralizadas," informa AiSecSis. "Análisis preliminar indica que están diseñados específicamente para provocar respuestas emocionales basadas en perfiles psicográficos individuales."

Esta es la evolución de las campañas de desinformación que comenzaron a principios de siglo. En 2034, los atacantes no solo

crean contenido falso convincente, sino que lo personalizan para cada receptor basándose en sus vulnerabilidades psicológicas específicas.

Gianluca trabaja junto a expertos en psicología digital e ingeniería conductual para contrarrestar esta amenaza:

"Necesitamos implementar una campaña de contraprogramación conductual," explica a su equipo. "AiSecSis, analiza los patrones emocionales que estos deepfakes están diseñados para activar." La IA identifica rápidamente que los deepfakes están calibrados para explotar miedos específicos relacionados con la estabilidad económica, utilizando microexpresiones y tonos vocales diseñados para eludir los filtros racionales del cerebro.

Gianluca coordina con la Agencia Nacional de Ciberseguridad una respuesta en tres niveles:

1. Neutralización Técnica: Implementación de filtros avanzados de autenticación de contenido en las principales plataformas de comunicación.

2. Contraprogramación Psicológica: Difusión de mensajes diseñados específicamente para contrarrestar las respuestas emocionales provocadas por los deepfakes.

3. Educación Inmersiva: Despliegue de programas educativos en entornos virtuales que enseñan a los ciudadanos a identificar manipulación emocional digital.

"Hemos identificado el origen de la campaña," informa AiSecSis después de varias horas de análisis. "Los servidores principales están ubicados en un país conocido por sus operaciones de guerra informativa."

Gianluca contacta inmediatamente con el Comando Cibernético Nacional, que tiene autoridad para implementar contramedidas ofensivas contra amenazas extranjeras.

"Esto ya no es un simple caso de ciberdelincuencia," explica Gianluca al comandante de la unidad. "Es una operación de desestabilización nacional."

"Un día más en la oficina", se dice Gianluca cuando llega la noche. Su trabajo puede ser extenuante, pero es consciente de la importancia del mismo para la sociedad en su conjunto.

En 2034, la ciberseguridad no es solo una prioridad técnica; es un pilar fundamental para garantizar la estabilidad económica, política y social en un mundo hiperconectado. Las tecnologías emergentes ofrecen oportunidades sin precedentes, pero también presentan desafíos formidables que requieren una vigilancia constante e innovación continua.



MARCOS NAVARRO ALCARAZ

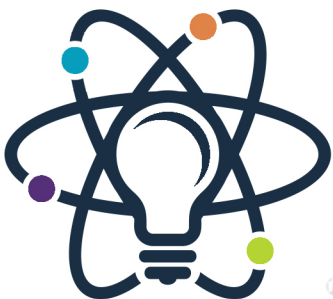
Consultor experto en Tecnologías de la información y ha sido ejecutivo de TI en varias compañías multinacionales. Ahora es experto en Outsourcing de TI, Robots y Autoamplificación y es profesor universitario y en escuelas de negocio.

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

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

CoE Book

Centres of Excellence Body of Knowledge P4MGO!®



P4MGO!

PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE



Más vale prevenir que curar

Habrán visto que no coinciden el título y la frase de Erasmo de Rotterdam. No tienen por qué. Curiosamente, la expresión que finalmente se ha consolidado en el uso coloquial, «Más vale prevenir que curar», es en realidad una mezcla entre la cita de Erasmo y el refrán castellano «Más vale prevenir que lamentar». Pero fue la televisión, y de forma concreta el famoso programa de Ramón Sánchez Ocaña, el que impuso su influencia en la sociedad. Entonces adoptamos el «Más vale prevenir», algo que todos sabemos por otra parte. Pero nuestro fuerte en la práctica no es prevenir.

Lo cierto es que las políticas preventivas funcionan bastante bien en materia de salud, seguridad vial o servicios sociales. Y podrían haber funcionado mejor en cuestiones de capital importancia como violencia de género y medio ambiente si se hubieran implantado de manera más efectiva. Y no funcionaron, ni bien ni mal, a la hora de prever el desastre de la DANA... Sabemos que no es tarea fácil enfrentarse a estos problemas, de modo que no se entienda el comentario como una crítica a las medidas que se han venido tomando al respecto, ni mucho menos como una crítica política, pero sí que parece evidente que dichas medidas tienen que replantearse cuando los problemas y situaciones a que se aplican acaban produciendo consecuencias negativas, en ocasiones desastrosas, para la sociedad.

Hablando de este tema, queremos introducir un inciso sobre determinado tipo de prevención. Como bien es sabido, desempeñé la responsabilidad del cargo de *Director de Prevención de la Agencia Antifraude de la Comunitat Valenciana*. Lo ideal, desde luego, es que la corrupción ni siquiera llegue a producirse. No hay mejor fraude que el que nunca ocurrió porque, antes de hacerlo, la idea de infringir el Derecho o la ética en beneficio propio desapareció de la cabeza de quien se lo estaba planteando.



CONTINÚA EN
PRÓXIMA PÁGINA

“

**Mejor es
prevenir
que curar**

Erasmus de Rotterdam





Se suele utilizar la expresión «lucha contra la corrupción», pero contra la corrupción y el fraude inexistentes ni siquiera hay que luchar, del mismo modo que la batalla contra el cáncer de pulmón se gana incluso antes de empezar simplemente dejando de fumar. También a través de la quimioterapia, claro está, pero en este caso ya tenemos que actuar a posteriori, con mucho sufrimiento y muchas menos posibilidades de éxito.

Por supuesto, el sistema debe establecer mecanismos reactivos contra los ilícitos que ya se han producido y, por desgracia, se seguirán produciendo, pero la mejor arma contra el fraude es precisamente la prevención. Y ahí destaca el fomento de una cultura de integridad y ética pública.

La formación y educación de toda la sociedad (no solo los responsables públicos), es la que permite desarrollar esta ética. La diferencia entre el simple fraude y la infracción legal grave (particularmente el delito), es que una actuación fraudulenta puede ser formalmente legal, pero en el ánimo, en la voluntad del infractor, aparece en ambos casos la desviación de poder, por lo que, en su fuero interno, el pensamiento del corrupto es tan reprochable como el del delincuente.

Obviamente, no podemos ser tan ingenuos de pensar que la ética se puede introducir de la noche a la mañana en el

ADN de algunos sujetos con determinada trayectoria e intenciones, pero sí que puede ser muy eficaz recordar continuamente los principios y valores de lo público. Esto es lo que algunos llaman «principios generales del Derecho», otros «vocación de servicio público», y otros «Código ético». No hay mejor prevención contra el fraude que la interiorización de la ética.

No podemos finalizar si realizar una mención especial a la Inteligencia Artificial (IA), cuya capacidad predictiva supera en fiabilidad y eficacia a cualquier técnica anterior de prevención o planificación. En efecto, la capacidad de predicción de la IA no solo ayuda a anticiparse a los problemas mejorando la calidad de los servicios, sino también la de la toma de decisiones.

Esta predicción viene de los datos, debidamente obtenidos, procesados e interpretados. Además, el carácter incuestionablemente objetivo de los datos encaja por completo en el interés general, frente a las opiniones y ocurrencias subjetivas que en el mejor de los casos podían ser erróneas, pero, cuando eran intencionadas, también incurrían en desviación de poder. La IA tiene la capacidad de analizar grandes cantidades de datos (*big data*) de manera rápida y eficiente. La predicción es la nueva planificación.

En el sector público, esto se traduce en la capacidad de procesar vastos conjuntos de información de interés público, como datos demográficos, económicos y de salud. Los algoritmos de aprendizaje automático pueden identificar patrones y tendencias que podrían pasar desapercibidos en análisis manuales o más superficiales, proporcionando una visión más completa para respaldar decisiones con un fundamento sólido.

En una frase: la Administración se rige por el principio de objetividad, y no hay nada más objetivo y veraz que los datos ciertos.



VÍCTOR ALMONACID

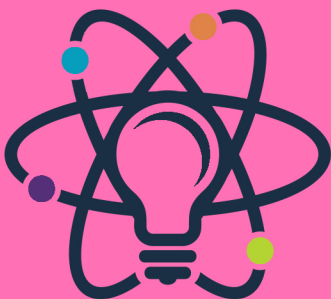
Secretario de la Administración Local, categoría superior. Director de Prevención, Formación y Documentación en la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana. Directivo Público. Máster en Nuevas Tecnologías aplicadas a la Administración Pública. Máster en 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/nuevadmno>
Blog:
<http://nosoloaytos.wordpress.com/>

BPM Book

Business Process Management Body of Knowledge

P4MGO!®



P4MGO!

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



Alex Aliaga

Amenazas no convencionales en el mundo del IoTM

A medida que las nuevas tecnologías se expanden, también lo hacen los desafíos de seguridad asociados. Es normal ver como muchas organizaciones disponen de controles de seguridad basados en red, como el control de acceso (NAC), Firewalls, IDS, IPS, EDR, XDR, registros de todos los movimientos de los usuarios, etc.

Estas soluciones de seguridad cubren una gran parte de las amenazas a las que se enfrentan las organizaciones, pero existen entornos críticos que, con el aumento de las tecnologías de comunicaciones inalámbricas y la rápida adopción de estas, se hace necesario implantar nuevos controles de seguridad que tengan en consideración también el espacio radioeléctrico: es el claro ejemplo del mundo del IoTM (Internet de las cosas médicas).

El IoTM es la aplicación de la tecnología de internet de las cosas en el sector sanitario, siendo una de las áreas donde sus beneficios son más importantes y evidentes.

¿POR QUÉ ES IMPORTANTE PROTEGER EL MUNDO DEL IOTM?

Las empresas de tecnología médica fabrican una amplia variedad de dispositivos médicos (se cifra en más de medio millón), una cantidad nada despreciable, que puede ser considerada una superficie de exposición notable.

Entre estos dispositivos se incluyen marcapasos, monitores de glucosa en sangre, bombas de insulina, dispositivos de imagenología portátiles, wearables para el seguimiento de signos vitales, y equipos de telemedicina, entre muchos otros.

La adopción del IoTM conlleva beneficios significativos, como la mejora en la atención al paciente, mayor eficiencia de los profesionales sanitarios, diagnósticos más precisos y una mejor prevención de enfermedades. Sin embargo, también presenta desafíos, como garantizar la seguridad y privacidad de los datos.



CONTINÚA EN
PRÓXIMA PÁGINA



A 1.25

En definitiva, la capacidad de estos dispositivos médicos de conectarse a internet, en muchos casos, de forma inalámbrica, para transmitir información en tiempo real está revolucionando la medicina, pero también estamos abriendo la puerta a ataques y amenazas más complejas que pueden explotar estos protocolos de comunicación inalámbricos.

LA NECESIDAD DE IMPLANTAR SISTEMAS DE DEFENSA DEL ESPACIO RADIOELÉCTRICO

Un ataque mediante RF es un tipo de ataque que no requiere encontrarse próximo al dispositivo objetivo, lo cual lo hace más difícil de detectar y proteger. Estos ataques, como el lector ya podrá imaginar, pueden llegar a tener consecuencias desastrosas, ya que pueden causar que estos dispositivos interrumpan sus funciones, o puedan acabar dañados por el atacante, poniendo en peligro la salud del usuario.

En muchas ocasiones, los fabricantes, en la fase de diseño, no consideraron una amenaza que estos dispositivos fuesen atacados usando comunicaciones inalámbricas, por lo que durante su concepción no aplicaron controles de seguridad. Pero hoy en día, con el abaratamiento de los sistemas SDR (radios definidas por software) y la gran cantidad de información accesible en internet, hace que sea más factible que un atacante quiera usar las comunicaciones inalámbricas como vector de ataque.

Sin embargo, y ante la gravedad del problema, hemos de afirmar que abordar el problema no es sencillo; si bien existen soluciones de seguridad muy enfocadas al mundo del IoT, estas no contemplan las amenazas que tienen como vector de ataque los sistemas de radiofrecuencia, y en otras ocasiones, los protocolos de comunicaciones usados no son seguros desde su concepción.

Para poder abordar este tipo de amenazas, es necesario un enfoque totalmente distinto al que venimos acostumbrados en la protección de otros activos. Evidentemente, hay que seguir prestando atención a los ataques que vienen a través de la red, pero también hay que buscar otro enfoque, que contemple el análisis del espectro radioeléctrico, analizando las señales electromagnéticas emitidas por los diversos dispositivos IoT para poder determinar anomalías y desviaciones del comportamiento normal del dispositivo, lo que ayudaría a identificar actividades maliciosas, acceso no autorizados y filtraciones de datos, entre otros ataques.

Para resolver el problema mencionado, existen diversos grupos de investigadores y empresas privadas que buscan, mediante el análisis de las señales radio, distinguir entre transmisiones legítimas y no autorizadas, para poder detectar estos tipos de ataques. Para ello, utilizan técnicas de sensado de espectro radioeléctrico, usando para ello equipos de radio definida por software (SDR).

Son técnicas que ahora nos parecen excesivamente complicadas pero ya existen empresas y entornos donde estas medidas forman parte ya de su plan de seguridad. Y es que, la tecnología avanza hacia un mundo sin cables.



¿POR QUÉ ES ESENCIAL PROTEGER LOS DISPOSITIVOS DE LAS AMENAS DE RF?

Para comprender más en detalle a qué riesgos nos enfrentamos, veamos a modo resumen algunas razones por las que es importante protegernos de las amenazas de RF:

•**Superficie de ataque en expansión:** a medida que más dispositivos dependen de la conectividad inalámbrica, el nivel de riesgo aumenta en proporción. Y, aunque no es muy popular, existen grupos especializados en atacar sistemas usando como vector de ataque los sistemas RF.

•**Detección de ataques "invisibles":** los atacantes suelen explotar vulnerabilidades en protocolos de comunicaciones que, normalmente, las organizaciones no tienen en cuenta. Convirtiéndose en puertas de entrada silenciosas donde no se han implementado controles de seguridad.

•**Monitorización y sensado del espectro:** los dispositivos IoT e IoTM usan distintas frecuencias y protocolos para sus comunicaciones, por lo tanto es importante disponer de sistemas de sensado de RF y detección de actividad no convencional en una gran variedad de frecuencias

Conclusión

Dado que los sistemas de comunicaciones inalámbricos cada vez son más comunes en estos entornos, debemos incorporar en nuestros planes de protección, planes directores de seguridad, y mapas de riesgos que incluyan los sistemas de comunicaciones inalámbricos como un riesgo más y darles todo el cariño necesario para implementar los controles de seguridad que nos permitan disminuir la probabilidad de que estos ataques puedan materializarse.



ALEX ALIAGA

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

**Curso de
Certificación en:**
**Gestión de Centros
de Operaciones
de Seguridad (SOC)**
**SOC
Management
Leader**

Docente:
Alejandro Aliaga

Coordinación Académica:
Javier Peris

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

MidMgmt®

MPPM®

MGEIT®

eGob®

Próxima Convocatoria en Directo
MARZO 2025

Solicita tu admisión en:

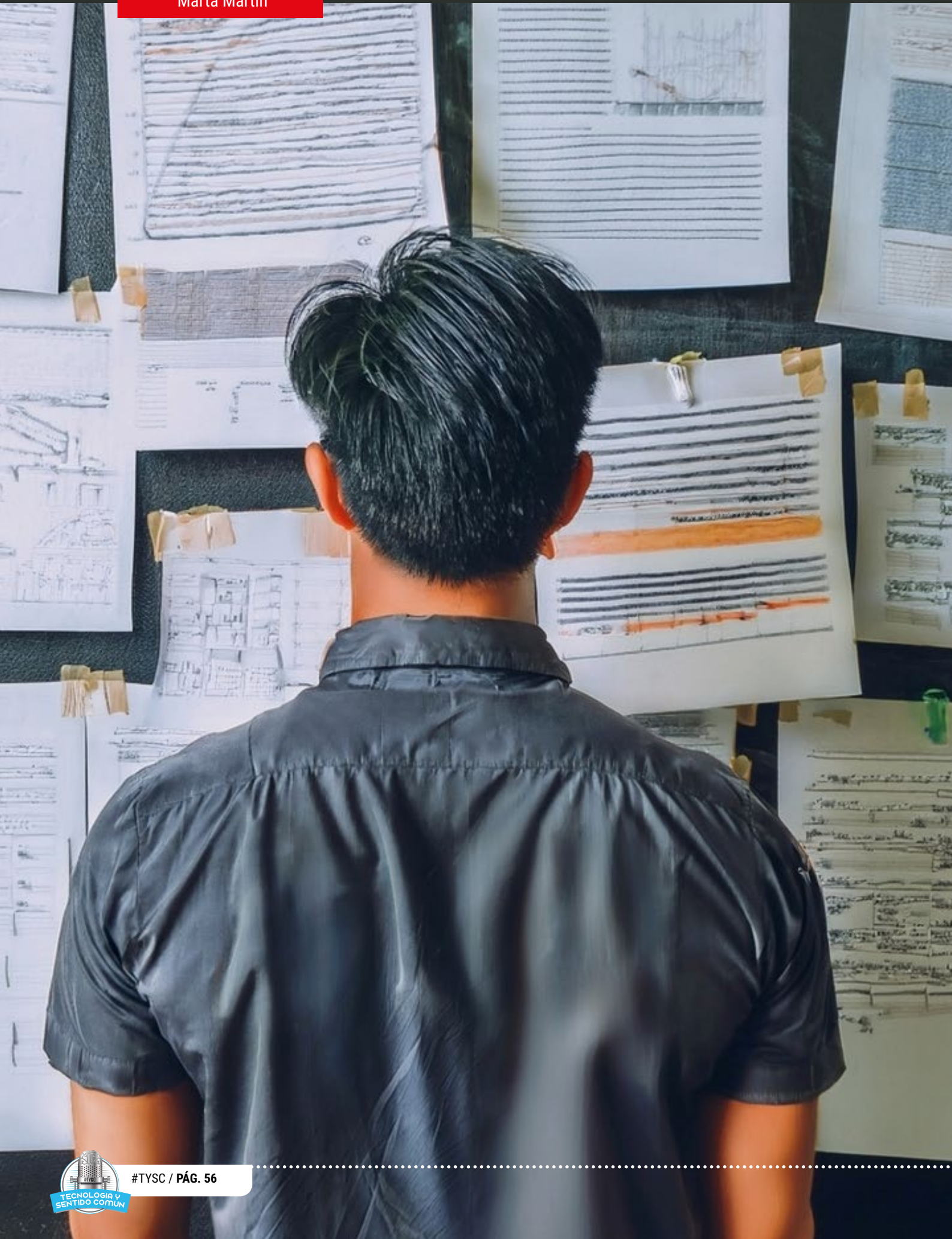


+ 34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>



**Plazas
limitadas**

Marta Martín



Un poco de atención, por favor

Prestar atención puede parecer un acto mecánico e involuntario, pero en realidad se trata de un complejo sistema de circuitos neuronales fundamental en nuestro día a día.

La atención es la capacidad de generar, dirigir y mantener un estado de activación adecuado para procesar correctamente la información y para enfocarnos en los datos relevantes discriminando el resto. Gracias a la atención, seleccionamos solo algunos estímulos de todos los posibles, selección que dependerá, entre otros factores, de la indemnidad de varios circuitos cerebrales. Lo que significa que, aunque parezca que prestar atención a un solo estímulo durante un tiempo sostenido es algo intuitivo o involuntario, en realidad requiere un cierto control en el que tienen un papel protagonista algunas funciones superiores de nuestra mente, las funciones cognitivas.

Sí, esas funciones cerebrales que nos ayudan en nuestra planificación, organización, memoria de trabajo y velocidad de procesamiento entre tantas otras cosas y que las personas con TDAH tenemos afectadas dificultando nuestra capacidad para discriminar la información. Por lo tanto, nuestra atención queda comprometida y más aún cuando los estímulos son poco motivadores o gratificantes ya que afecta a nuestra motivación por la atención.

Todo lo dicho nos indica que sí, que tenemos un problema. Y más, teniendo en cuenta que el sistema atencional no es sencillo ni unitario. De forma resumida, las personas con TDAH tenemos afectados varios circuitos neuronales. En primer lugar, los circuitos de la atención selectiva que nos permiten focalizarnos en un estímulo relevante; los de la atención sostenida, que nos permiten mantener la atención sobre ese estímulo por un periodo prolongado; y los de la atención dividida que nos permiten atender a dos estímulos simultáneos. Todos estos circuitos neuronales junto con la motivación y la memoria constituyen los procesos cognitivos básicos con los que trabaja el sistema ejecutivo central.

Lo dicho, tenemos un problema. Porque, como bien sabemos, recurrimos a la atención para todo en nuestro día a día. La necesitamos para asimilar todo tipo de datos sobre el mundo que nos rodea, para aprender cosas, realizar tareas y crear nuevos recuerdos. Nos ayuda a aprender en el colegio, a progresar en el trabajo y a tener buenas relaciones personales. Imprescindible pero imperfecta. Es muy sensible a las distracciones ya que interfieren en nuestra capacidad de concentración, problema que se agrava con el TDAH.



CONTINÚA EN
PRÓXIMA PÁGINA



LOS PROCESOS ATENCIONALES

¿Qué procesos atencionales entran en juego a la hora de leer este artículo? Todo dependerá del interés que genere en nosotros el título o el tema. Si tenemos TDAH o alguien cercano que lo tenga, si el tema de la atención nos provoca curiosidad, o hemos leído anteriormente otro artículo de esta sección y nos ha gustado, entrará en juego la motivación, un mecanismo clave a la hora de iniciar cualquier acción humana.

Decidimos, entonces, leer este texto y focalizamos nuestra atención en él ignorando el resto de los estímulos que nos bombardean, tanto externos como internos, gracias a nuestro control inhibitorio y a los procesos de atención sostenida necesarios para no perder esa motivación que nos hizo empezar a leer. Si la atención no se sostiene a lo largo de la lectura, probablemente no llegaremos al final del texto.

Mientras leemos, nuestro cerebro lleva a cabo procesos cognitivos complejos de comprensión a la vez que tiramos de concentración para llevar a cabo razonamientos complejos que nos permitan generar aprendizajes. Para ello es imprescindible planificar, organizar y monitorizar nuestro pensamiento haciendo uso de la memoria de trabajo en colaboración con el sistema ejecutivo central y con las funciones de orden superior, las denominadas funciones ejecutivas. Pero, si con este artículo, consigo generar tu interés y que mantengas un estado de alerta

óptimo, la puesta en marcha de los procesos cognitivos superiores será más sencilla y el aprendizaje más eficaz. No hay duda de que, para las personas con TDAH, la lectura de este artículo será más difícil porque nos cuesta más mantener la concentración y el enfoque en una tarea mientras lidiamos con multitud de pensamientos dispersos. Estos problemas constituyen todo un desafío ya que influyen negativamente en muchos ámbitos de la vida que, si bien, no son el reflejo de una actitud perezosa o maleducada, generan una imagen negativa en el resto e impactan significativamente en nuestro día a día.

Por ello es importante conocernos y saber si nuestras distracciones son las normales, o reflejan un trastorno subyacente como el TDAH. La clave para identificarlas está en la duración y la persistencia. La falta de atención común es muy habitual y normalmente responde a factores temporales como el cansancio, el estrés o la falta de interés. Es temporal y variable. Por el contrario, en el TDAH las dificultades de atención, al igual que el resto de síntomas, persisten durante un período prolongado e interfieren negativamente la vida diaria.

LA PARADOJA DE LA HIPERCONCENTRACIÓN

A pesar de todo lo dicho, algunas personas con TDAH viven la paradoja de la hiperconcentración, episodios de concentración de forma intensa y prolongada en contextos y situaciones concretos.

La hiperconcentración en el TDAH se manifiesta cuando nos sumergimos en una actividad que nos resulta particularmente estimulante o atractiva. En esos momentos, mostramos una atención enfocada y sostenida, ignorando la mayoría de las distracciones externas y manteniendo una inusual capacidad para concentrarnos. El detonante para esta habilidad se halla en las tareas que ofrecen una gratificación inmediata, hecho que aumenta la liberación de neurotransmisores como la dopamina, el neurotransmisor relacionado con la recompensa y el placer, que tiene la virtud de mejorar la función ejecutiva y, por lo tanto, nuestra capacidad de concentración.

Esta cualidad, sin duda puede resultar muy útil en determinadas situaciones, pero también puede ser problemática cuando nos absorbe de tal manera que descuidamos otras responsabilidades.

Para poder gestionar todas estas dificultades, sin duda, lo más importante es comprender cómo nos afectan estos problemas atencionales e incorporar estrategias efectivas para lidiar con los aspectos más negativos de este síntoma.



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_23DRlwIw

Instagram:

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

PdM Book

Product Management Body of Knowledge

P4MGO!®



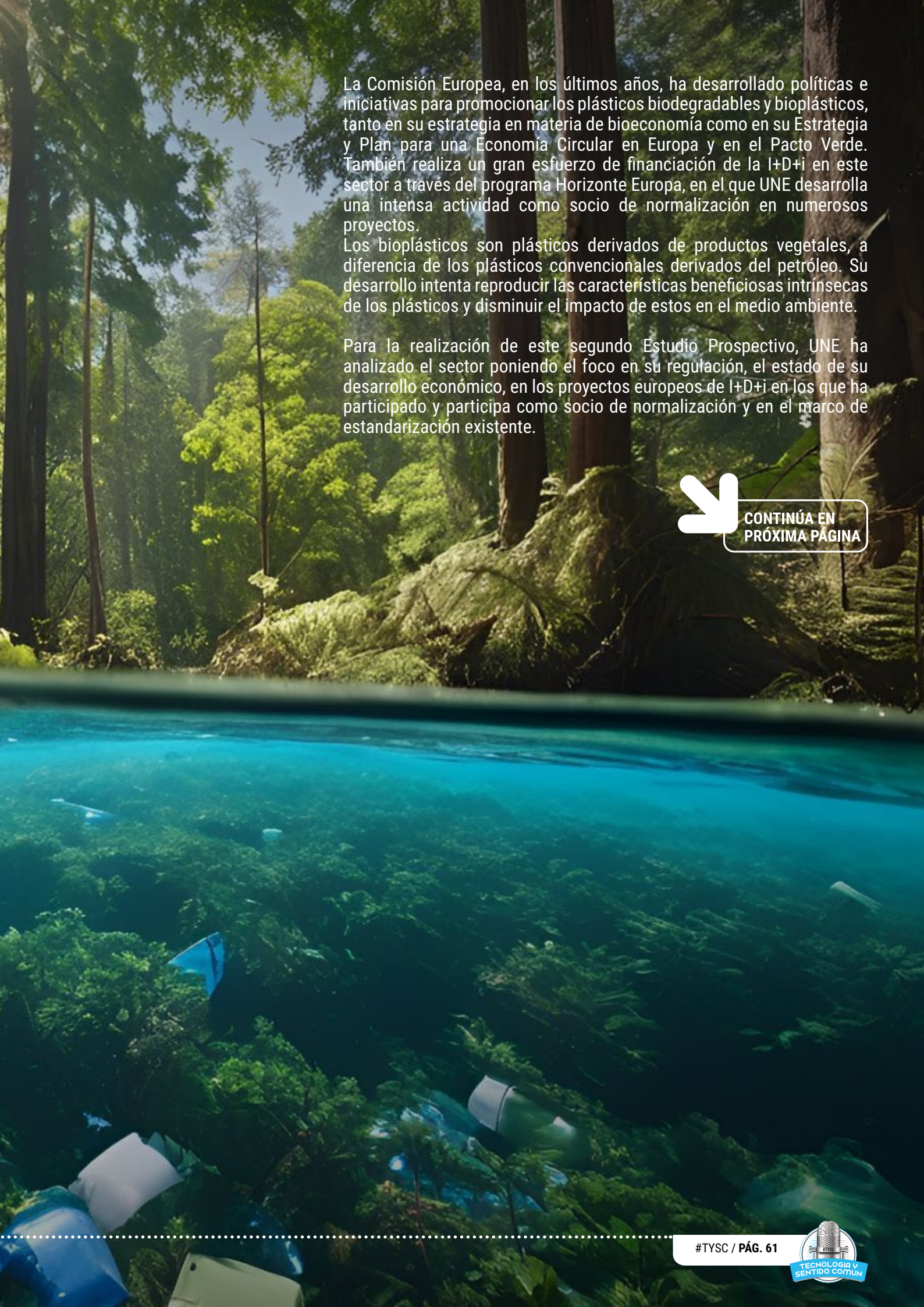
P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

UNE potencia la innovación en el ámbito de los bioplásticos

- La Asociación Española de Normalización, UNE, siguiendo su compromiso con la innovación, publica su segundo Estudio Prospectivo, enfocado en los bioplásticos.
- En ellos analiza información de varias fuentes contrastándola con socios relevantes de los sectores implicados. Pretende crear nuevas actividades de normalización lideradas por organizaciones españolas que apoyen el desarrollo de nuevas tecnologías y soluciones innovadoras.
- La normalización es una herramienta para introducir y consolidar el uso de los bioplásticos en el mercado.

La Asociación Española de Normalización, UNE, ha publicado el segundo documento de su serie de Estudios Prospectivos, centrado en la innovación en los bioplásticos. Con estos estudios pretende apoyar la implantación industrial de nuevas tecnologías y soluciones innovadoras mediante la elaboración de normas técnicas, que las entidades españolas lideren a nivel europeo e internacional.

Fernando Utrilla, responsable de I+D+i de UNE, destaca: "Con este nuevo tipo de Estudios Prospectivos invitamos a reflexionar sobre el papel que la normalización puede jugar para facilitar la innovación en sectores estratégicos. En UNE innovamos constantemente, pues entendemos la estandarización como una herramienta estratégica al servicio de la capacidad innovadora de las empresas, que acelera el acceso al mercado de sus productos o servicios".



La Comisión Europea, en los últimos años, ha desarrollado políticas e iniciativas para promocionar los plásticos biodegradables y bioplásticos, tanto en su estrategia en materia de bioeconomía como en su Estrategia y Plan para una Economía Circular en Europa y en el Pacto Verde. También realiza un gran esfuerzo de financiación de la I+D+i en este sector a través del programa Horizonte Europa, en el que UNE desarrolla una intensa actividad como socio de normalización en numerosos proyectos.

Los bioplásticos son plásticos derivados de productos vegetales, a diferencia de los plásticos convencionales derivados del petróleo. Su desarrollo intenta reproducir las características beneficiosas intrínsecas de los plásticos y disminuir el impacto de estos en el medio ambiente.

Para la realización de este segundo Estudio Prospectivo, UNE ha analizado el sector poniendo el foco en su regulación, el estado de su desarrollo económico, en los proyectos europeos de I+D+i en los que ha participado y participa como socio de normalización y en el marco de estandarización existente.



CONTINÚA EN
PRÓXIMA PÁGINA

PRINCIPALES CONCLUSIONES DEL ESTUDIO

La normalización es una herramienta para introducir y consolidar el uso de los bioplásticos en el mercado. Entre las temáticas susceptibles de estandarización se encuentran la definición de conceptos, los parámetros y especificaciones de los productos para su caracterización, la correlación de los ensayos con el producto final, su uso específico según aplicaciones, la trazabilidad de los materiales y su producción, así como las condiciones de operación de las unidades productivas.

Otra de las conclusiones que destaca el Estudio es la necesidad de involucrar a Administraciones públicas, centros de investigación, fabricantes de productos, asociaciones de estas empresas y grupos de interés relacionados, así como gestores de residuos, para el desarrollo sectorial y la elaboración de las normas. Los bioplásticos tienen un futuro prometedor y transformador en el sector de la industria del plástico.

El Estudio Prospectivo "Bioplásticos" ha recabado la opinión y el conocimiento de agentes representativos de la cadena de valor del sector de los plásticos: CEISLAB, Asociación Española de Industriales de Plásticos (ANAIP), Instituto Tecnológico del Plástico (AIMPLAS), Centro tecnológico del calzado y del plástico (CETEC), Instituto Tecnológico del Embalaje, Transporte y Logística (ITENE), Asociación Nacional de

Recicladores de Plásticos (ANARPLA) y Asociación Española de Plásticos Biodegradables Compostables (ASOBIOCOM).

Más información: <https://www.une.org/normalizacion/estudios-prospectivos-une/>

SOBRE LA ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN, UNE

La Asociación Española de Normalización, UNE, es una organización global cuyo propósito es desarrollar normas técnicas o estándares que contribuyan al progreso compartido de la sociedad y a la creación de un mundo más seguro, sostenible y competitivo.

Las normas recogen el consenso del mercado sobre las mejores prácticas en aspectos clave para la competitividad de las organizaciones y para los intereses de toda la sociedad, siendo el resultado del diálogo y la colaboración conjunta de los sectores económicos y las Administraciones públicas.

Con la participación de más de 14.000 profesionales en sus mesas de trabajo, UNE es el representante español en los organismos de normalización internacionales (ISO e IEC), europeos (CEN-CENELEC y ETSI) y americanos (COPANT). Actualmente, el vicepresidente de ISO es el español Javier García, director general de UNE.



**Hace mucho
tiempo que
hablas.**

**¿Pero hace
cuánto no
dialogas?**



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

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

NUEVOS MASTERS



TITULACIÓN MasterGEIT®

CONTENIDO DEL MASTER

- Módulo 01: Gestión del Tiempo**
Curso de Doble Certificación TSG4® Yellow Belt + TSG4® Green Belt
- Módulo 02: Gestión de Procesos de Negocio**
Curso de Doble Certificación BPM Executive + ISO 19510 Leader
- Módulo 03: Dirección y Gestión de Proyectos**
Curso de Doble Certificación OpenPM® (PgM) Executive + ISO 21502 Leader
- Módulo 04: Dirección y Gestión de Programas**
Curso de Doble Certificación OpenPM® (PgM) Executive + ISO 21503 Leader
- Módulo 05: Gestión de Servicios de Tecnología**
Curso de Doble Certificación FITSM Executive + ISO 2000 Leader
- Módulo 06: Gestión de Seguridad de la Información**
Curso de Doble Certificación CSX Executive + ISO 27000 Leader
- Módulo 07: Gestión de la Continuidad del Negocio**
Curso de Doble Certificación CBC Executive + ISO 22301 Leader
- Módulo 08: Gobierno de Información y Tecnología**
Curso de Doble Certificación COBIT 2019 Executive + ISO 38500 Leader
- Módulo 09: Gobierno del Dato**
Curso de Doble Certificación DAMA Executive + ISO 38505 Leader
- Módulo 10: Gobierno Corporativo**
Curso de Doble Certificación COSO Executive + ISO 37000 Leader

Los cursos de Doble Certificación se basan en los Programas de la Escuela de Gobierno eGob® y cuentan con la acreditación de la EFMD EQUIS, AACSB y AMBA. Los cursos de Doble Certificación se basan en los Programas de la Escuela de Gobierno eGob® y cuentan con la acreditación de la EFMD EQUIS, AACSB y AMBA.

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



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

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



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

eGob®

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