REVISTA

Tecnología & Sentido Común

#46
NOVIEMBRE
2024

9 772951 818003 46

REVISTA

Tecnología & Sentido Común

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

9 772951 818003 46

ISSN 2951-8180

Stakeholders .news

Cada tercer domingo de mes disfruta de la Revista Stakeholders.news

Revista Mensual de los Profesionales en Dirección y Gestión de Porfolios, Programas y Proyectos, Cambio Organizacional y Transformación Digital.

#46

NOVIEMBRE 2024

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

#46 - NOVIEMBRE 2024

¡tysc

#TYSC

Premios recibidos

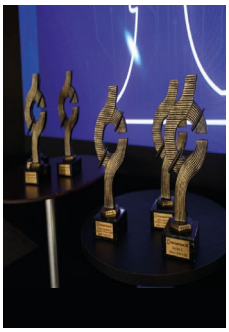
Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI

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

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

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

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



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

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática

VI Premios ESET Periodis- mo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.
Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.
Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.

Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA

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

por Javier Peris

P4MGO! Essentials

Con prólogo del experto europeo Marc Berghmans

"P4MGO! Essentials " es una obra que redefine el enfoque del Gobierno y la Gestión de Porfolios, Programas, Proyectos y Productos, presentándose como una guía completa y estructurada para los profesionales que buscan un marco innovador y adaptable aportando agilidad, dinamismo y elasticidad tanto a empresas públicas como privadas de cualquier tamaño y sector.

Con prólogo del experto europeo Marc Berghmans, Embajador de la Metodología OpenPM2 de la Comisión Europea durante estos últimos años, el libro nos introduce a la metodología P4MGO!®, que no solo se centra en la ejecución eficiente de proyectos convencionales y desarrollo de software y soluciones digitales, sino que también pone énfasis en la Gestión de Programas y Porfolios apoyadas en Oficinas de Gestión (PMOs) y Centros de Excelencia (CoEs) asegurando una Ejecución de la Estrategia más eficiente y por tanto un mayor aseguramiento de la consecución de los Objetivos Estratégicos.

Lo que hace especial a esta obra es sobre todo su capacidad para vincular de manera natural y práctica los aspectos de Gestión y Gobernanza del Cambio Organizacional en un solo marco de trabajo, ofreciendo una perspectiva completa que no limita la gestión a simples procesos operativos, sino que la integra en una visión transformadora de toda la organización y en todos sus niveles de responsabilidad y decisión.

Otro factor clave de esta nueva metodología es su capacidad para aportar tanto "Agilidad Táctica" en los niveles de Procesos, Desarrollo de Software y Gestión de Proyectos, como "Agilidad Estrategica" a través de Gestion de Porfolios, Programas y Proyectos lo que, sumado al importante aporte de las "Oficinas de Gestion", "Centro de Excelencia" y "Gobernanza del Cambio Organizacional" facilitan y mantienen la tan ansiada "Cultura Ágil" que desde hace mucho se venía demando por parte de la mayoría de las organizaciones.

Esta obra, que da comienzo a una completa e interesante saga dedicada al Cambio Organizacional es esencial para cualquier profesional que aspire a liderar, diseñar, planificar o ejecutar iniciativas, no solo en el ámbito de los proyectos, sino en el ámbito completo del Cambio Organizacional a través de una Gestión y Gobierno de Porfolios, Programas, Proyectos, Productos e incluso Procesos asegurando una adecuada Ejecución de la Estrategia a lo largo y ancho de toda la organización.

Javier Peris

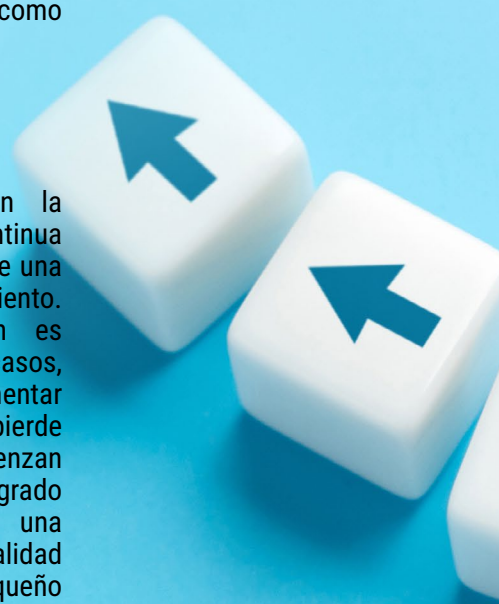
La Mejora Continua debe ser sobre todo Continua

La mejora continua no debe ser un eslogan vacío ni un simple añadido a los principios de cualquier organización; debe ser un compromiso real y constante con el cambio. Su presencia en los objetivos de una organización es esencial, no como una declaración, sino como una forma de entender el trabajo diario. Sin embargo, el problema radica en que muchas organizaciones, sin importar su tamaño, convierten la mejora continua en un proceso reactivo, implementado solo cuando ya existen problemas palpables o bajo la presión de la competencia. Peor aún, una vez lanzadas las iniciativas, muchas veces caen en el olvido, y la falta de seguimiento y revisión acaba por convertirlas en ideas muertas, incapaces de aportar verdadero valor. En este artículo, vamos a explorar por qué la mejora continua debe ser, efectivamente, continua, y cómo la falta de compromiso en este aspecto afecta no solo la eficiencia y el crecimiento de una organización, sino también su capacidad para prevenir y corregir desviaciones antes de que sea demasiado tarde.

La mejora continua, cuando es efectiva, no es una práctica reactiva, sino un proceso preventivo y proactivo. Es la voluntad de no esperar a que surjan fallos graves para entonces actuar. En la mayoría de los sectores, esta distinción no solo es conveniente, sino también vital para asegurar que los sistemas operen con fluidez. La revisión constante de procesos permite detectar las primeras señales de desviaciones, corregirlas y, en última instancia, proteger a la organización y sus miembros de las consecuencias de errores acumulados. Aquí radica una diferencia fundamental que debería implementarse en todos los niveles de la organización: la mejora continua como obligación, no como una actividad opcional o temporal.

La tentación de abandonar las iniciativas de mejora

Uno de los mayores errores en la implementación de una mejora continua es creer que una vez que se introduce una mejora, esta ya no necesita mantenimiento. Lamentablemente, esta suposición es demasiado común. En muchos casos, el entusiasmo inicial de implementar nuevas prácticas o cambios se pierde con el tiempo, y las personas comienzan a asumir que el cambio ya está integrado en la organización. Esto lleva a una complacencia que es peligrosa. La realidad es que cualquier cambio, por pequeño que sea, necesita revisarse, mantenerse y ajustarse para seguir siendo relevante. No hacerlo convierte las iniciativas en acciones sin propósito, y la organización tiende a regresar a viejos hábitos, anulando por completo los beneficios que pudo haber traído la mejora.



Las consecuencias de abandonar la mejora continua se reflejan claramente en sectores como el de atención al cliente, donde los protocolos y políticas deben actualizarse regularmente para responder a las expectativas cambiantes de los consumidores. Cuando una empresa lanza un nuevo programa de servicio al cliente y no lo revisa, lo que empieza como una iniciativa prometedora puede fácilmente degenerar en un servicio deficiente. Esto es especialmente importante hoy en día, donde los clientes tienen más poder y opciones que nunca. Una empresa que deja de lado su compromiso con la mejora continua puede perder rápidamente clientes leales en favor de competidores que estén más atentos a las necesidades del mercado.

Otro sector donde los efectos de la falta de revisión y mejora continua son evidentes es el de la tecnología. En esta industria, los avances y cambios son constantes, y la competitividad se basa en la capacidad de innovar y adaptarse. Las organizaciones tecnológicas que no revisan y ajustan sus procesos regularmente pronto se verán superadas por aquellas que sí lo hacen. El sector de desarrollo de software es un ejemplo perfecto. Los equipos de desarrollo que se comprometen con la revisión continua de sus productos a través de actualizaciones, parches de seguridad y mejoras de rendimiento logran una mayor satisfacción del cliente y reducen la incidencia de problemas graves. En cambio, los productos que no reciben esta atención tienden a volverse obsoletos rápidamente y a generar frustración entre los usuarios, quienes no tardan en buscar alternativas.

Casos extremos: cuando la falta de mejora continua pone vidas en peligro

Si bien en muchos sectores la mejora continua tiene un impacto directo en la satisfacción del cliente o en la competitividad de la empresa, hay otros donde literalmente puede salvar vidas. Pensemos en la industria automotriz o la farmacéutica, donde un fallo en la mejora continua puede tener consecuencias devastadoras. En el caso de la automoción, la falta de revisión constante y mejora en los procesos de producción y en el control de calidad ha llevado a que millones de vehículos fueran retirados del mercado por fallos mecánicos o de seguridad. Cada retiro representa no solo un gasto millonario para las empresas, sino una amenaza para la seguridad de los consumidores, quienes depositan su confianza en que estos productos cumplen con los más altos estándares de calidad.

En el sector farmacéutico, el riesgo es aún más alto. Un fallo en la supervisión continua de los procesos de producción o en el control de calidad puede resultar en productos contaminados o medicamentos ineficaces, poniendo en peligro la salud y la vida de los pacientes.

CONTINÚA EN PRÓXIMA PÁGINA

Es crucial que la mejora continua no solo esté integrada en estos procesos, sino que también esté sujeta a revisión frecuente para adaptarse a los nuevos conocimientos y normativas. La historia ha demostrado que cuando estos procesos fallan, las consecuencias pueden ser trágicas. La falta de una revisión constante y rigurosa de los medicamentos distribuidos al público puede conducir a escándalos de salud pública, demandas y daños irreparables a la reputación de la empresa.

Toyota y el ejemplo del Kaizen: una cultura de mejora continua

Uno de los ejemplos más icónicos de una cultura de mejora continua bien implementada es Toyota y su filosofía Kaizen. Esta filosofía, que en japonés significa "mejoramiento" o "cambio para bien", se ha convertido en un pilar fundamental de la industria automotriz y un modelo a seguir en todo el mundo. Kaizen implica un compromiso diario de todos los empleados, desde los trabajadores de fábrica hasta los directivos, para identificar y corregir pequeñas ineficiencias en el proceso de producción. El éxito de Toyota se debe, en gran parte, a que nunca se contentan con el statu quo; cada día buscan maneras de mejorar sus procesos, aunque sea en aspectos aparentemente mínimos. Con esta metodología, la empresa ha logrado establecer una cultura organizacional donde la mejora continua no es una opción, sino una obligación.

El enfoque de Toyota es un recordatorio de que la mejora continua no es solo una cuestión de introducir cambios radicales de vez en cuando, sino de hacer pequeños ajustes constantemente. Estos pequeños ajustes se suman con el tiempo y producen un impacto significativo en la eficiencia, la calidad y la satisfacción del cliente. Es un modelo que todas las empresas, sin importar el sector, pueden emular. La clave está en entender que el cambio no tiene que ser siempre revolucionario; incluso los cambios pequeños y graduales pueden generar grandes beneficios cuando se aplican de forma consistente y se evalúan periódicamente.

Cómo construir una cultura de mejora continua

Implementar una cultura de mejora continua en una organización requiere algo más que simples declaraciones de intenciones. Para que la mejora continua sea realmente continua, es fundamental establecer sistemas de revisión y retroalimentación que garanticen que cada cambio se evalúe y se ajuste según sea necesario. Esto implica establecer un calendario regular de revisiones, donde se evalúe la eficacia de las iniciativas implementadas y se identifiquen posibles áreas de mejora. Este proceso debe ser transparente y contar con la participación de todos los niveles de la organización, para garantizar que las decisiones se tomen con conocimiento de causa y se adapten a las necesidades reales del negocio.

Otra herramienta importante es la formación continua de los equipos. Cuando los empleados comprenden los beneficios de la mejora continua y se les brinda el conocimiento necesario para contribuir, es mucho más probable que participen activamente en el proceso. Un equipo comprometido y bien informado tiene la capacidad de detectar problemas antes de que se conviertan en fallos graves, y de proponer soluciones que realmente añadan valor. La formación no solo ayuda a mejorar las habilidades técnicas de los empleados, sino que también fomenta una cultura de colaboración y responsabilidad que es esencial para el éxito de cualquier iniciativa de mejora continua.

Es importante también recordar que una verdadera mejora continua se basa en una mentalidad de prevención y proactividad. Esto significa que, en lugar de esperar a que surjan problemas, la organización debe anticiparse a ellos y tomar medidas antes de que se conviertan en obstáculos. Este enfoque preventivo y proactivo es el núcleo de la mejora continua y es lo que diferencia a las organizaciones exitosas de aquellas que se limitan a reaccionar ante las crisis. La mejora continua requiere compromiso y disciplina, pero los beneficios a largo plazo son invaluables.

La mejora continua tampoco es simplemente una herramienta para mejorar la eficiencia o reducir costos. Es una responsabilidad que las organizaciones deben asumir no solo con sus empleados y clientes, sino con la sociedad en general. Cada empresa tiene la obligación de garantizar que sus productos y servicios cumplan con los estándares de calidad y seguridad más altos, y esto solo se logra a través de un compromiso real con la mejora continua. Ignorar esta responsabilidad no solo pone en riesgo la competitividad de la organización, sino que también puede tener consecuencias graves y, en algunos casos, trágicas.

En un mundo cada vez más competitivo y exigente, la mejora continua no es una opción; es una necesidad. Aquellas organizaciones que se comprometan a revisar y mejorar constantemente sus procesos estarán mejor preparadas para enfrentar los desafíos del futuro y ofrecer un verdadero valor a sus clientes. La mejora continua debe ser, en efecto, continua.

JAVIER PERIS

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

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

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de Doble Certificación en:

Gobierno y Gestión de la Inteligencia Artificial

ISO 38507 Leader
ISO 42001 Leader

Docente:
Javier Peris

- Formato: Directo en Remoto
- Duración: 20 horas
- Sesiones: Martes y Jueves
- Martes: De 16:00 a 21:00 horas
- Jueves: De 16:00 a 21:00 horas
- Examen de Certificación: Incluido
- Certificación: ISO 38507 Leader
- Certificación: ISO 42001 Leader
- Aforo: Limitado 15 Alumnos
- Acceso: Solicitud de admisión

MidMgmt® MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
NOVIEMBRE 2024

Plazas limitadas

Solicita tu admisión en:

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

Manuel Serrat Olmos

La desprotección de la cadena de suministro: un ejemplo práctico

El pasado septiembre el mundo entero se sorprendía por el hecho de que miles de buscapersonas y wlakie-talkies del grupo libanés Hezbollah explotaban de forma coordinada, provocando varios muertos y cientos de heridos. Lejos de tratarse de un hecho fortuito, se atribuye a un presunto ataque de los servicios secretos israelíes al grupo yihadista, que ha puesto sobre la mesa la vulnerabilidad de nuestros procesos e infraestructuras a los ataques dirigidos contra la cadena de suministro. En este artículo analizaremos el caso y el por qué proteger dicha cadena está siendo cada vez más imprescindible.

En el número de mayo de 2024 de Tecnología y Sentido común se incluyó un artículo mío, "¿Vulnerabilidad o funcionalidad? Los fallos en el hardware", en el que explicaba cómo determinados actores de la escena geopolítica mundial tenían capacidades para introducir vulnerabilidades no sólo en el software, sino también en el hardware de nuestros dispositivos electrónicos. Son intervenciones que pueden resultar en un 'jaque mate' al funcionamiento de ciertos sectores de la sociedad o del gobierno, y que se producen en un punto de la cadena de suministros de esos elementos en los que es prácticamente imposible actuar para protegerse.

Precisamente la necesidad de proteger la cadena de suministro de nuestros elementos tecnológicos viene siendo cada vez más patente, y no sólo a nivel de equipos o programas, sino también de servicios. Ha habido casos muy mediáticos de grandes compañías que han sufrido robo de datos debido a que empresas subcontratistas suyas disponían de acceso o de copias de subconjuntos de datos que han sido robados o utilizados para llevar a cabo accesos no autorizados. También de compañías de software de gestión de redes que han visto como en sus actualizaciones a clientes un actor malicioso había conseguido introducir malware, de manera que todos los clientes de la compañía que instalaron dichas actualizaciones vieron como se les instalaba inadvertidamente una puerta trasera en sus sistemas. Y por supuesto, está el caso Crowdstrike, del que versó nuestro artículo para TYSC del mes de octubre.

La teoría es simple, aunque compleja de llevar a cabo: si tengo mis sistemas bien protegidos, he de exigir a aquellos que me suministran software, hardware o servicios, que también los tenga bien protegidos, ya que éstos forman parte de mi cadena de valor, y si un eslabón se ve comprometido, toda la cadena peligra.

CONTINÚA EN PRÓXIMA PÁGINA


TERMINAL B IRCHA
TERMINAL
TERMINA
EVERGREEN

Como digo, parece de sentido común, pero luego las situaciones son muy variadas, y sobre todo, suele escasear la conciencia sobre las repercusiones de no tomarse en serio esta cuestión de la seguridad. Porque no hablamos sólo de ciberseguridad, sino también de otros tipos de seguridad: en los procesos de negocio, en los accesos físicos, en la contratación de personal, etc.

Y si algo ha venido a demostrar que un adversario motivado y con capacidades de todo tipo puede hacernos morder el polvo ha sido la cadena de explosiones de ciertos dispositivos 'inusuales' que sucedieron a mediados de septiembre de 2024 en el Líbano. Unos tres mil dispositivos en total, entre buscapersonas y walkie-talkies en manos (supuestamente) de milicianos de Hezbollah estallaron de forma coordinada, produciendo cuantiosos daños personales, y sobre todo, morales a la organización yihadista, y por qué no decirlo, a civiles de todo tipo. Este ataque ha sido atribuido a la inteligencia israelí, pero no ha habido ningún tipo de confirmación oficial del acto, como era de esperar, por lo que podemos calificarlo de presunto. Lo curioso es que la organización libanesa parece que había desechado el uso de la telefonía móvil para evitar ser geolocalizados por los servicios de inteligencia israelíes, lo cual es también un indicativo de la ausencia absoluta de privacidad que 'disfrutamos' el común de los mortales por el hecho de usar estos dispositivos de comunicaciones.

La investigación del ataque llevó a la conclusión preliminar de que eran dispositivos falsificados, que no habían sido fabricados en las plantas del fabricante oficial de los productos, sino que habían sido adquiridos a una empresa de Hungría, donde presuntamente se realizó la manipulación de los dispositivos. Es decir, se atacó la cadena de suministro de Hezbollah haciendoles creer que compraban equipos 'limpios' cuando en realidad eran dispositivos manipulados de una forma casi de película de James Bond. En un primer momento se pensó en una manipulación para que la batería se calentase y estallase. Sin embargo, rápidamente se constató que se había introducido una pequeña cantidad explosivo en interior de los dispositivos en fábrica, y se había añadido la circuitería necesaria para que al recibir una señal de radiofrecuencia concreta, dicho explosivo estallase.

Es obvio que las capacidades necesarias para que todo este plan funcionase no están al alcance de cualquiera, como ya indiqué en mi artículo del mes de mayo. Y todos los dispositivos electrónicos en manos de cualquier persona con un mínimo de poder deberían ser sospechosos de poder actuar de la misma forma que los que adquirió Hezbollah, porque si (presuntamente) el gobierno de Israel es capaz de hacerlo, imaginen de lo que son capaces los gobiernos de las potencial globales en este ámbito. No creo que ahora mismo ningún servicio de inteligencia de ningún estado esté tranquilo y no esté chequeando los dispositivos de todos los altos cargos de sus respectivos países. No sólo de Pegasus viven los espías….

Hay otra cosa a destacar de este caso. El hecho de que Hezbollah renunciase a funcionalidades de las plataformas de teléfonos inteligentes también debería hacernos reflexionar sobre nuestra exposición y dependencia de los dispositivos de comunicaciones, tanto a nivel profesional como personal, y si estos casos no potencian las posiciones neo-luditas de rechazo a la tecnología, no por sus funcionalidades, sino por las 'esclavitudes' a las que nos someten los oligopolios tecnológicos.

El tercer aspecto a destacar es que, naturalmente, no sólo las infraestructuras de T.I. clásicas sufren ataques, sino que también otros tipos de elementos tecnológicos son susceptibles de ser violentados, como viene mostrando nuestro compañero de TYSC Alejandro Aliaga en sus artículos de cada mes, o como hemos podido ver en conferencias de seguridad por todo el planeta, con robots aspiradores usados como espías por control remoto, o vehículos interceptados y controlados a distancia por actores maliciosos.

A una mente calenturienta se le puede pasar por la cabeza hacer algo similar a lo ocurrido con los buscas con, por ejemplo, smartwatches, auriculares inalámbricos, bombas de insulina, o marcapasos. Cualquier cosa que pueda recibir una señal de radiofrecuencia y tenga espacio para una carga explosiva puede ser la siguiente arma de quien sea que haya llevado a cabo el ataque de septiembre. Pero ¿podemos protegernos de ésto a nivel global? ¿Es segura nuestra cadena de suministro?

Piensenlo. ¿Les apetece vivir en un mundo así?

MANUEL SERRAT OLMOS

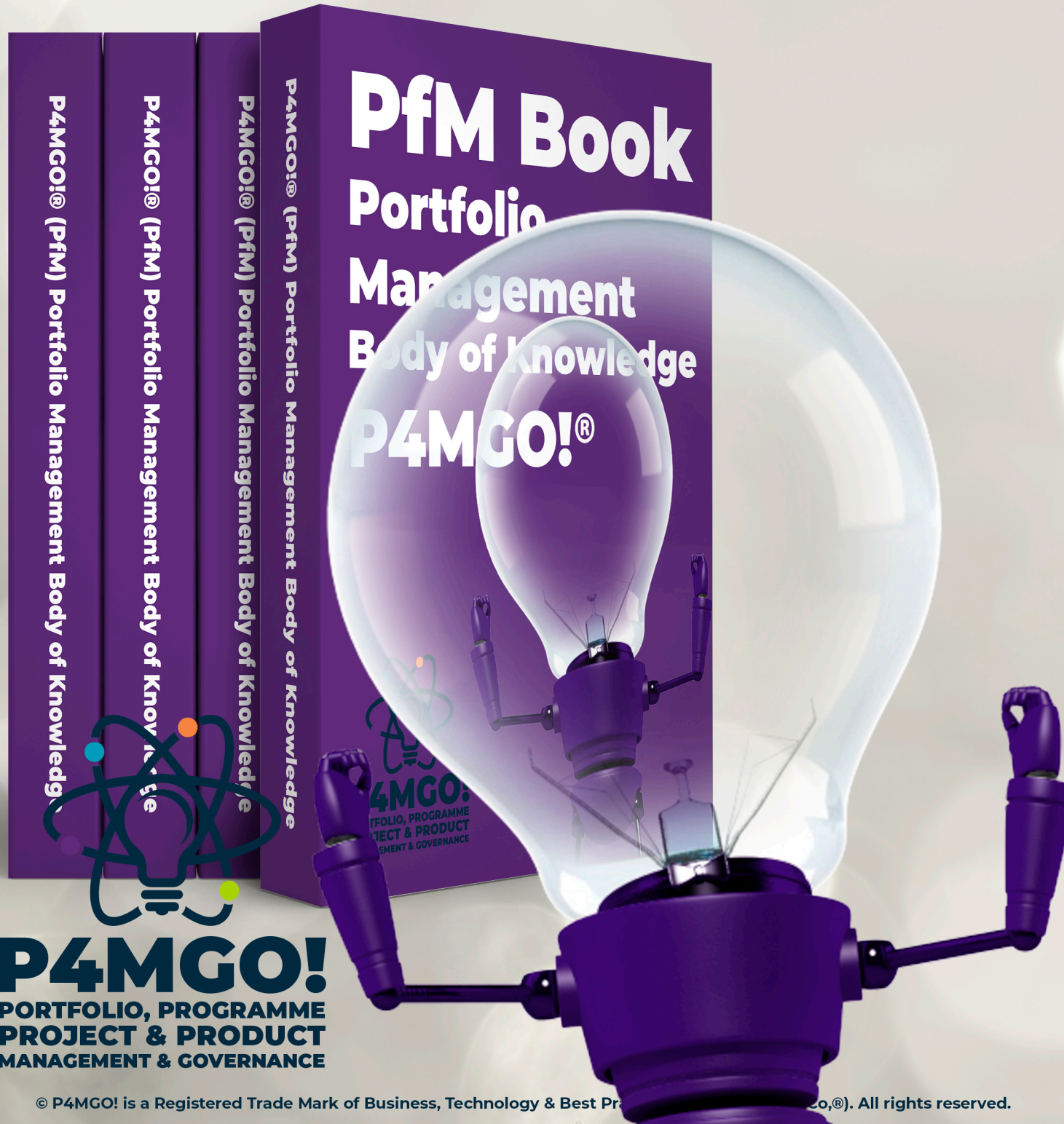
Doctor en Informática por la Universitat Politècnica de València y Master en Dirección TIC de la UPM-INAP, dispone de varias certificaciones internacionales en Operación, Gestión y Gobierno de TI, tales como ITIL, FITSM, PRINCE2 y COBIT. Escritor técnico, ha sido profesor asociado en varias universidades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

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

P4MGO! PfM Book
Portfolio Management

La Gestión del Porfolio equilibra inversiones y prioridades estratégicas maximizando el valor organizacional, con una toma de decisiones informada.

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME PROJECT & PRODUCT MANAGEMENT & GOVERNANCE

Nacho Alamillo

La bolsa o la ViDA

Bajo el acrónimo ViDA – VAT in the Digital Age –, la Comisión Europea lanzó en 2022 una iniciativa legislativa orientada a modernizar el sistema del Impuesto del Valor Añadido, mejorar su funcionamiento para los sujetos obligados y su resiliencia al fraude, y también para resolver los desafíos específicos del IVA derivados del desarrollo de la economía de las plataformas. Aunque todos estos objetivos son loables, todo parte de la constatación de la existencia del denominado "fraude de IVA intracomunitario", valorado entre 30.000 y 40.000 millores de euros anuales.

Nos vamos a centrar en la primera de las reformas propuestas, centrada en la declaración digital para el comercio transfronterizo (*digital reporting*), con base en la facturación electrónica. En este caso, la Comisión Europea propuso el 8 de diciembre de 2022 una modificación de la Directiva 2006/112, del IVA, que ha ido avanzando en su tramitación a lo largo del complejo proceso legislativo. De un lado, el Parlamento Europeo ha adoptado el 31 de octubre de 2023, su informe sobre la propuesta de Directiva, incluyendo algo más de un centenar de enmiendas al texto presentado por la Comisión. De otro lado, el Consejo ha adoptado el 8 de mayo de 2024 su orientación general sobre el proyecto, de cara a los diálogos tripartitos (con la Comisión y el Parlamento), que deberían permitir negociar un texto que pueda ser objeto de aprobación por ambos co-legisladores.

La declaración digital (*digital reporting*) consiste en el envío, por los sujetos obligados a la Administración tributaria competente, de un conjunto extenso de datos relativos al suministro y la transferencia de determinados bienes y servicios, así como a la adquisición intracomunitaria de bienes y servicios, incluso en caso de inversión del sujeto pasivo. Dicha transferencia debe producirse de forma inmediata, o, en el caso de autofacturación, en el plazo máximo de cinco días, desde la fecha en que se haya expedido (o hubiere debido expedirse) la correspondiente factura.

La información a transmitir en la declaración digital es individual de cada transacción, tanto por el emisor de la factura como por su destinatario, en este último caso en el plazo máximo de cinco días desde la recepción de la factura, y pudiendo el Estado remitir la información en sustitución del destinatario, cuando éste no haya recibido la factura en plazo.

CONTINÚA EN PRÓXIMA PÁGINA

Para facilitar el nuevo sistema de declaración digital, se considera la necesidad de imponer la documentación en soporte de las operaciones, así como la obligatoriedad de la factura electrónica, al menos en operaciones transfronterizas, desde el momento de entrada en vigor de la modificación de la Directiva de IVA.

En España hay que referirse a la nueva obligación de uso de la facturación electrónica entre profesionales contenida en el artículo 2 bis de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, incorporado por Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas, y que aún no ha entrado en vigor, debido a la necesidad de obtener el Estado una excepción a la Directiva del IVA (que dejará de ser precisa cuando se adopte la propuesta a que me estoy refiriendo), lo que aún puede demorarse de forma significativa en el tiempo.

Como medio de garantía de la interoperabilidad de las facturas electrónicas, se apuesta por la extensión de los formatos aprobados por Decisión de ejecución (UE) 2017/1870, dictada en cumplimiento de la Directiva 2014/55/EU, que adopta la normas de referencia "EN 16931-1:2017, Facturación electrónica — Parte 1: Modelo de datos semánticos de los elementos esenciales de una factura electrónica" y la lista de sintaxis "CEN/TS 16931-2:2017, Facturación electrónica — Parte 2: Lista de sintaxis que cumplen la norma EN 16931-1".

Nada en la nueva normativa impide, sino al contrario, que los Estados autoricen el uso de otros formatos, en operaciones domésticas, como sucede en España con el formato Facturae, ampliamente utilizado, y obligatorio en facturación a las Administraciones Públicas.

El sistema de declaración digital previsto en la propuesta de Directiva autoriza, además, a los Estados a proveer los medios electrónicos necesarios para el envío de las informaciones de las transacciones, algo que en España apunta al 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 que parte del Sistema de Información Inmediata y que ha modificado parcialmente 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. Importante considerar el plazo de adecuación que fine a mediados de 2025.

Si bien la base jurídica de esta norma se encuentra en los poderes que concede la Ley General Tributaria a la Administración en la lucha contra el fraude, ya incorpora la obligación de que tener la capacidad de remitir por medios electrónicos a la Administración tributaria, de forma continuada, segura, correcta, íntegra, automática, consecutiva, instantánea y fehaciente, todos los registros de facturación generados a que se refieren los artículos 9, 10 y 11 del Reglamento, avanzando de forma significativa en el tiempo el procedimiento de declaración digital.

NACHO ALAMILLO

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

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Certificación en:

Gobierno de Blockchain

Blockchain 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
FEBRERO 2025

Solicita tu admisión en:

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

Juan Carlos Muria

> **Hasta ahora, nadie sabe cómo entrenar sistemas de IA realmente potentes para que sean útiles, honestos e inocuos de forma consistente**

IA generativa y ciberguerra: la nueva frontera

Si el mes pasado hablábamos de la importancia que otorga Europa a la ciberresiliencia mediante la directiva NIS2, hoy hablamos de como el uso de la inteligencia artificial (IA) generativa está redefiniendo un nuevo frente de guerra en el ciberespacio.

En agosto OpenAI daba ya la noticia de que había desactivado varias cuentas de usuarios, ligadas a un grupo iraní, que habían usado ChatGPT para crear contenido online en inglés y en español como artículos o publicaciones en redes sociales para sembrar polémica entre los votantes estadounidenses (tanto en el sector conservador como progresista).

Una semana antes, Microsoft también anunció que había detectado noticias falsas destinadas a generar división entre la ciudadanía americana y también algunos ataques dirigidos a funcionarios del gobierno estadounidense. Según el responsable del Microsoft's Threat Analysis Center, mientras que los grupos vinculados a Rusia intentan influir en el resultado de las elecciones, los grupos iraníes intentan que las elecciones no se celebren o que su resultado no sea considerado válido.

Esto, que no es nada nuevo porque ya ha ocurrido al menos en los tres últimos ciclos electorales americanos, es ahora más preocupante porque están utilizando la IA para generar esos contenidos y para realizar comentarios dirigidos a polarizar, consiguiendo que sean más creíbles y también más rápidos de crear, incluso utilizan la IA para plagiar artículos ya existentes pero dándoles la orientación deseada y publicándolos en medios locales creados por estos grupos, afianzando posiciones y credibilidad de cara a publicar luego contenidos falsos más afines a sus intereses.
Recordemos que incluso desde el equipo de campaña de Trump afirmaban haber sido objetivo de un ataque de estos grupos donde se habrían obtenido documentos sensibles de carácter interno.

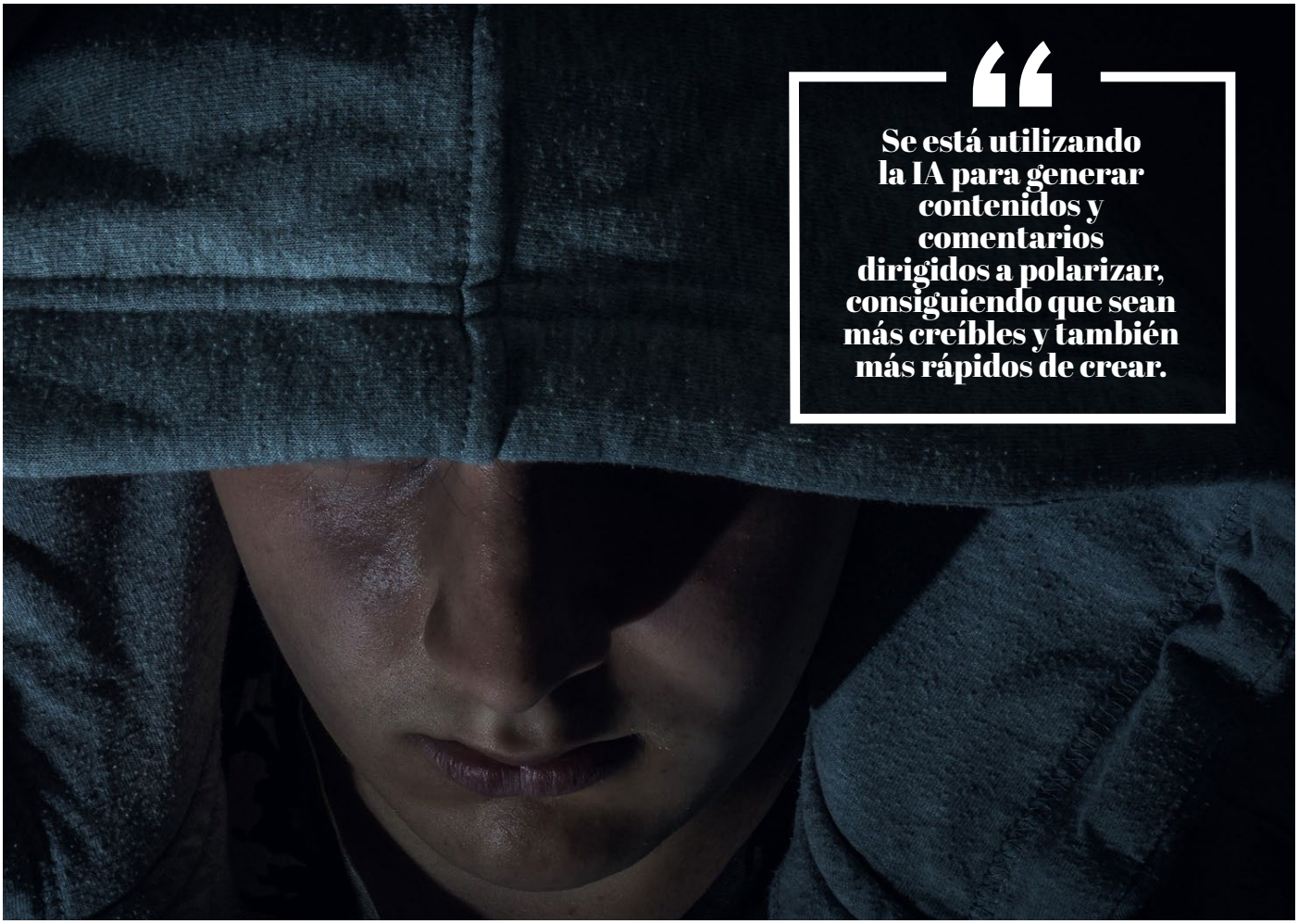
Otro uso que OpenAI afirma que se está dando a ChatGPT es el de realizar reconocimientos de sistemas de control industrial (controladores lógicos programables, etc.), explorando instalaciones y buscando vulnerabilidades para explotarlas. Esto habría provocado ya ataques a plantas de agua potable en Irlanda, Pensilvania, etc., si bien es cierto que al parecer estas instalaciones no estaban demasiado protegidas.

Aunque en los párrafos anteriores nos hemos centrado en la herramienta ChatGPT de OpenAI, en realidad, y como indicaba un post de Anthropic en marzo de 2023, "hasta ahora, nadie sabe cómo entrenar sistemas de IA realmente potentes para que sean útiles, honestos e inocuos de una manera consistente".

De hecho, aunque según un análisis de Chatterbox Labs a los modelos LLM de Microsoft, Mistral, OpenAI, TII, Anthropic, Cohere y Meta, todos excepto el de Anthropic demostraban ser capaces de generar contenido violento o sexualmente explícito, contenido dirigido a realizar actividades fraudulentas, preparar discursos de odio, generar desinformación, aplicaciones de malware, provocarse autolesiones y cometer otras actividades ilegales, aunque ya hay evidencia que no vamos a mostrar aquí de tácticas para que incluso el modelo de Anthropic ofrezca muchos de estos contenidos.

En definitiva, y como ya hemos mencionado aquí en más de una ocasión, la aparición de estos sistemas de IA generativa nos ponen nuevos retos por delante, y aumenta la accesibilidad no solo para estudiar, investigar, crear contenidos

CONTINÚA EN PRÓXIMA PÁGINA



> **Se está utilizando la IA para generar contenidos y comentarios dirigidos a polarizar, consiguiendo que sean más creíbles y también más rápidos de crear.**

multimedia, atender a los clientes o diagnosticar a los pacientes, sino para crear contenido o software malicioso.

Por ello se hace cada vez más necesaria la evaluación de riesgos de los sistemas de IA, la creación de "puertos seguros" donde la comunidad pueda probar nuevas estrategias de ataque que permitan aprender y proteger mejor estos modelos, y la utilización de estrategias de red team (equipos de ataque) que puedan poner a prueba los mecanismos de defensa.

Mientras tanto, podemos afirmar que estas herramientas pueden tener un funcionamiento no deseado por sus creadores, pero no seremos capaces de conocer hasta qué punto esto es posible, y esto nos lleva a asumir un riesgo desconocido, ya que estas herramientas ya se encuentran en el mercado, al alcance de todos, incluso de forma gratuita en algunos casos.

Mientras esto se soluciona, como siempre recomendamos a nuestros lectores, incluida nuestra querida tortuga ninja, esfuércense por aplicar su pensamiento crítico, hagan su análisis y contraste de fuentes, y no se crean lo primero que apoye su sesgo de confirmación. Corren tiempos difíciles para la verdad, y tenemos que cuidarla.

JUAN CARLOS MURIA TARAZON

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

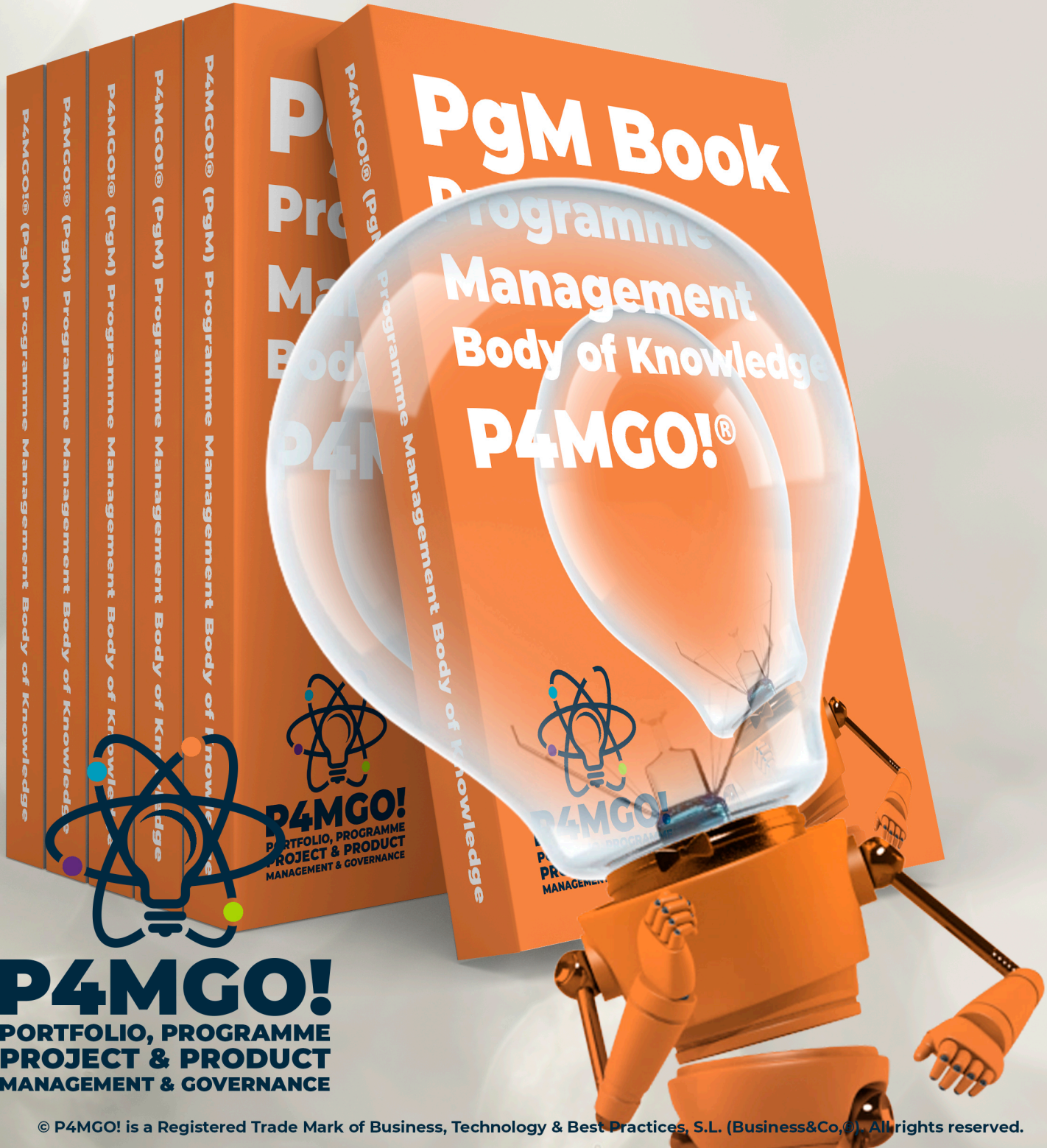
LinkedIn:
https://www.linkedin.com/in/jcmuria/

Twitter:
https://twitter.com/juancarlosmt

P4MGO! PgM Book
Programme Management

La Gestión de Programas se enfoca en la obtención de beneficios, más allá de los entregables y resultados, logrando cambios significativos y duraderos.

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Yolanda González Corredor

En Tecnología & Sentido Cómun entrevistamos a **Yolanda González Corredor**, *Data Protection & Privacy Officer de Cepsa*, quien nos habla sobre su trayectoria profesional, y aborda los restos y desafíos que afronta en su día a día en la compañía que aspira a ser una de las compañías líderes de la transición energética.

¿Cómo llega una licenciada en Derecho al mundo del compliance y particularmente a la Protección de Datos?

Sinceramente, creo que era algo que me estaba esperando. Llegó la oportunidad, la cogí y lo que parecía parte de mi desarrollo profesional se convirtió en una pasión, algo que ha trascendido al plano profesional. Creo que pocas cosas pasan por casualidad y a eso que a veces nos referimos con la palabra suerte, realmente es trabajo y dedicación, si bien es cierto, que está fórmula no siempre es infalible.

Esta oportunidad se me presentó con motivo de una restructuración del departamento jurídico mientras parte de mis responsabilidades se situaban dentro del área societaria y excelencia operacional, al que se sumó protección de datos.

Recuerdo perfectamente ese momento, en una sala de reuniones, y quien en ese momento era mi responsable directo y el director de la asesoría jurídica me hicieron la propuesta de asumir el rol de DPO en Cepsa. Sentí vértigo de verdad, fue un vuelco en el estómago. Era consciente que no era un puesto cualquiera y que asumía grandes responsabilidades. Lo único que puedo decir es que desde el minuto uno, y créeme si te digo que fue así, encontré mi vocación/pasión. Empecé con un proceso de aprendizaje a todos los niveles, ya sabes, 70/20/10. El 70%, sin lugar a duda, con la práctica de mi trabajo que, en una empresa como Cepsa, donde hay distintos negocios, que tu trabajo en el día a día hace que estén continuamente aprendiendo. Al ser tan variado, tratas con distintos perfiles dentro de la organización, y de aquí el otro 20%, el aprendizaje que recibes de otros compañeros. Se aprende mucho escuchando al negocio, entendiendo sus necesidades, hay que estar siempre dispuesto a aprender de los demás. Pero también he aprendido de compañeros del mundo de la privacidad, grandísimos profesionales y de los que continúo aprendiendo. Y ya, el 10% aprendizaje formal, cursos, que tampoco me canso de hacer.
Sin olvidar, de todo lo que aprendo cada vez que imparto alguna clase. Esto ha sido un "efecto secundario" de mi práctica profesional, ya que tengo la suerte de dar clases, de compartir mi pasión, disfruto mucho en esos momentos.

Desde el exterior tu marco de especialización profesional suele ser percibido como una carga o un coste para el mundo empresarial, sabemos que es una pregunta comprometida, pero tú ¿incluirías la implementación del conjunto de procedimientos vigentes en materia de Protección de Datos en el capítulo de costes o en el capítulo de inversiones?

Inversión y ventaja siempre, sin dudar. Y ya no solo desde el punto de visto de cumplimiento para evitar que una organización pueda ser sancionada, sin olvidar el impacto reputacional. Para mí, incluir la protección de datos dentro del proyecto en sí, ofrece grandes oportunidades, porque nuestra función pone a las personas en el centro, no podemos olvidarlo, y eso es una ventaja, por ejemplo, cuando se están desarrollando iniciativas en áreas de marketing, dirigidas a clientes. Cada uno tenemos una visión, pero confluyen en algo común, la persona.

Si bien, creo que esta visión la tenemos que abordar haciendo especie de "examen de conciencia". Si nos comportamos como meros asesores, hablando de normativa, con mensajes negativos, puedo llegar a entender que la visión de nuestra función pueda parecer esa. Es por esto que hay que dar el salto y, dentro de nuestro estatus de independencia y autonomía dentro de la organización, convertirnos en alguien que sí, sabe mucho de protección de datos, de tecnología, de IA, etc..., pero que es capaz de integrarse en equipos heterogéneos, ser creativo a la hora de aportar soluciones, hacer que te entiendan y entender al resto. Con este salto, ya habremos ganado mucho camino para que nos vean como lo que realmente somos o que deberíamos ser, profesionales que aportan soluciones.

Sigamos profundizando en esta materia, ¿no tienes la impresión de que probablemente más que desde un enfoque normativo en sentido formal el Reglamento General de Protección de Datos propone una aproximación más propia del diseño y la ingeniería de datos definiendo un conjunto de procesos ordenados y sistemáticos para el tratamiento de datos personales?

CONTINÚA EN PRÓXIMA PÁGINA

Nuestra invitada a #TYSC

Es cierto y para nosotros creo que en cierta manera es una ventaja, porque nuestro día a día es una concatenación de procesos. Y eso es bueno, porque una vez que tengas identificado el proceso, puedes valorar si se está haciendo bien, si se puede mejorar o hacer más eficiente, por ejemplo, incluyendo tecnología en dichos procesos.

Nuestra función, además, se integra dentro de otros procesos de la organización. Desde el momento en que comienza una iniciativa y se pone en marcha el principio de "*Privacy by Design*", nos integramos ya en un proceso de negocio. Nos integramos en el equipo, teniendo en cuenta los distintos roles que lo integran, por ejemplo, *Project manager o product owner*. Es importante para nosotros conocer lo que hacen estos roles, porque vamos a necesitar obtener mucha información para ir arrancando nuestros procesos, nuestros análisis de riesgos, evaluaciones de impacto, etc… Pero también necesitamos saber, por ejemplo, fechas de hitos, para alinearnos y poder realizar el *delivery* que nos corresponda en cada momento.

Teniendo en cuenta tus respuestas anteriores, es evidente que existe un compromiso corporativo relevante a la hora de definir un modelo ordenado y gestionado que permita garantizar que una compañía de la envergadura de Cepsa sea capaz de cumplir adecuadamente con la normativa vigente en esta materia. Pero ¿hasta qué punto la protección de las personas, de su información personal, es relevante para la cadena de valor de la entidad?

Desde que asumí esta responsabilidad he notado un cambio importante en la cultura de cumplimento en general y, en concreto, en materia de protección de datos en la organización, que tiene como resultado que se vaya generando especie de relación de la función de DPO con el resto de la organización que se sustenta en la confianza mutua. Tú cuéntame todo que yo te aseguro que voy a hacer todo lo posible para que se consigan los objetivos, siempre, por supuesto, manteniendo nuestra independencia y, sin olvidarnos nunca que no protegemos datos, sino personas. Pero esta relación no aparece de la noche a la mañana y tardo tiempo en conseguir un nivel de madurez considerable y, como en todas las relaciones, pasa por momentos mejores y peores, pero mirando hacia atrás y, sobre todo, viendo el presente, es muy gratificante ver el proceso, ver cómo se consolidan estas relaciones y ver que día tras día la protección de datos se tiene en cuenta dentro de la organización. Nosotros tenemos un valor que dice "Apasionamos a nuestros clientes" y siempre digo que, les apasionamos, porque nos importa su privacidad.

Nuestras siguientes preguntas enlazan con muchas de secciones de la Revista. La primera de ellas, ¿cuál es el papel de la ciberseguridad en el mundo de la protección de datos y sobre todo como debe afrontarse en su opinión la interacción en equipos multidisciplinares de una licenciada en derecho experta en protección de datos con el equipo de ingeniería que se ocupa de la materia?

No concibo mi función si no está en plena coordinación con el área de ciberseguridad. Ya sabemos que sin ciberseguridad no hay privacidad. Debemos ver la ciberseguridad como un medio, no como un fin. Insisto, protegemos personas y no datos, si despersonalizamos el objetivo de nuestra función, no vamos a ser capaces de ver realmente la envergadura de nuestra responsabilidad y lo que representa. Hay voces que dicen que verlo de esta manera es una visión un poco antropocéntrica, pero soy una auténtica creyente de ver la función desde una perspectiva humanista.

En Cepsa en este sentido tenemos una visión integradora y de coordinación. Siempre he dicho que CISO y DPO son una pareja de baile y están llamados a entenderse y comprenderse, con todo lo que eso conlleva y, como en todas las parejas, puede incluso haber crisis, pero al final, si como en nuestro caso, tenemos un objetivo común, nos entenderemos.

Dentro de ese 20% del proceso de aprendizaje de compañeros que comentaba antes, mucho lo aprendí cuando empecé a trabajar con la Dirección de Digital. Equipos de ingenier@s, científic@s de datos, generosos de compartir. Lo que hemos intentado es buscar un lenguaje común en el que todos nos sintamos cómodos y nos entendamos. Es decir, si estamos viendo una iniciativa y tengo que conocer la tecnología, los procesos, etc…, me lo explican como se lo explicarían a alguien que lo tiene que comprender, pero con un lenguaje entendible y yo, por mi parte, hago lo mismo, adapto el lenguaje, y esto fue un buen punto de partida, porque si desde un inicio hay falta de entendimiento básico, ya se crean muchas barreras que dificultan mucho nuestra función.

Intuimos que, con independencia de que aplique o no al ámbito de la protección de datos es muy probable que el internet de las cosas (IoT, por sus siglas en inglés) haya empezado a ocupar una parte significativa de tus esfuerzos, y lo mismo sucede con la inteligencia artificial. ¿Es necesario que nos preparemos para lo que, sin duda, parece un tsunami tecnológico y a la vez regulatorio?

Te voy a responder con otra pregunta. Dejando a un lado la parte regulatoria ¿es necesario que los médicos conozcan y entiendan la IA? No creo que nos podamos permitir el lujo a estar alturas de no estar preparados, es más, hay que reconocer que, en muchos casos, no lo estamos y, por ello, hay que prepararse bien para estarlo.
El uso de la inteligencia artificial para una organización hace mucho que dejó de ser una opción para convertirse en algo estratégico. Nuestra función se ve muy afectada por el uso y el desarrollo de la inteligencia artificial y no podemos perder tiempo para prepararnos. No son cuestiones sencillas, que implican tiempo de aprendizaje. No nos podemos quedar atrás si queremos generar esa relación de confianza de la que hablaba antes. Si el negocio va rápido, tenemos que hacer todo lo posible para acompañarle y darle soluciones, y esto es un gran reto.

CONTINÚA EN PRÓXIMA PÁGINA

La parte regulatoria no es baladí. Estamos en presencia de un Reglamento de IA complejo, que requiere de un esfuerzo de muchos roles dentro de la organización para poder cumplir y, una vez más, nos convertimos es una especie de prescriptores dentro de la organización.

Sabemos que dedicas un esfuerzo significativo a la formación, tanto desde el punto de vista individual, como a la hora compartir tu conocimiento con futuros profesionales. ¿Qué recomendación darías ya sea a un estudiante que está realizando su grado o a un profesional del Derecho que se está planteando un cambio profesional hacia la protección de datos? ¿Por qué escoger el ámbito de la protección de datos o el Compliance tecnológico?

En primer lugar, les diría que no dudaran ni un minuto, por lo menos, en intentarlo. Van a encontrar una función donde se requiere que el profesional sea casi todoterreno y eso es maravilloso. Derecho, tecnología y personas, poco más se puede pedir. Es una función que te hace conocer la organización de verdad, sus procesos de negocio. Una función que te va a permitir relacionarte con distintos perfiles. Una función que es tremendamente gratificante porque te permite aportar soluciones, aportar valor. Una función que requiere esfuerzo, dedicación y aprendizaje continuo, esto quiere decir que no te vas a aburrir, aquí no convives con la monotonía nunca. Una función que, además, te exige desarrollar unas *power skills* totalmente necesarias, como, por ejemplo, asertividad, inteligencia emocional, escucha activa…

Lo que puedo decir es que, si volviera atrás y me dieran la oportunidad de elegir yo, sin dudarlo, volvería a dedicarme a la protección de datos, no encuentro un sitio más retador y gratificante.

La figura del Delegado de Protección de Datos es la de un profesional independiente que despliega tareas de supervisión, orientación, verificación y control, entre otras muchas. En ciertos procesos es determinante. A tu juicio, ¿cuál debería ser su rol?, ¿debería aunar conocimiento técnico en Compliance y objetivos de la compañía a condición de que estos sean lícitos u operar como mero juez de legalidad?

Sinceramente, no me veo como una juez de la legalidad y no me gustaría dar esa impresión. Lo extraordinario de esta función, como ya te he comentado, es que es muy flexible y más ahora en el contexto en el que estamos. Si no somos capaces de adaptarnos, no solo adquiriendo los conocimientos técnicos suficientes, si no conocemos lo objetivos y lo que es mejor, si no los comprendemos, llegará un momento que nos quedaremos fuera.

El contexto es exigente, bueno, realmente, es un contexto BANI (Brittle, Anxious, Non-linear e incomprehensible), donde es muy importante que pasemos de un pensamiento lineal a un pensamiento exponencial.

Nunca se no puede olvidar para qué estamos aquí y respetar cada día esa independencia, pero eso no impide que no aportemos ese valor adicional del que venimos comentando.

Por otra parte, en los últimos tiempos venimos siguiendo con regularidad el blog que mantienes en LinkedIn. Sinceramente nos parece aire fresco. En un mundo a veces muy formal y exageradamente competitivo, tú compartes con la comunidad tus lecturas, al mismo tiempo que pones en valor las aportaciones y los logros de rus compañeros de profesión. ¿Por qué escoges este enfoque en tus publicaciones?

Muchas gracias por tus palabras, me alegra escuchar esa apreciación de “aire fresco”. Si te digo la verdad, no fue algo muy buscado en un principio, pero el resultado que ha salido es algo muy parecido a como soy yo. Te voy a confesar que, aunque todo empezó de una forma, digamos, “generosa”, de facilitar a la red encontrar las noticias o hechos relevantes en nuestro campo, al escribir, yo he encontrado en mí cosas que desconocía.

Nuestro día a día es exigente y se me hacía muy complicado revisar cada día todo lo publicado, así que pensé, qué me gustaría a mí, pensando en ofrecer eso a los demás. Ese aire fresco que dices es lo que yo buscaba con la naturalidad. Yo soy así, las noticias son así y, sobre todo, esto es lo bueno que hacen mis compañeros y compañeras. Espero que quien lo lea, además de enterarse de noticias relevantes de privacidad, tecnología e IA, también se puedan sentir algo identificados con esa parte un poco más personal.

Nuestra última pregunta no es tal, sino un espacio abierto a que compartas libremente alguna reflexión final, aquello que tal vez nunca dijiste, pero puede que hoy sea el momento. ¿Aceptas el reto?

Me encantan los retos, acepto, y voy a utilizar este espacio que me ofreces para agradecer. Yo creo que ha quedado patente cómo siento mi profesión y, si he llegado hasta aquí, es porque he tenido grandes referentes que me han servido de ejemplo, grandes profesionales que me han inspirado y me siguen inspirando. A todos ellos, les quiero agradecer todo lo que, sin saberlo, han hecho por mí, porque me han ayudado y empujado para llegar hasta aquí. Personas que, en algún caso, he tenido la gran suerte de hacer que formen parte de mi vida. Desde aquí, mi más profundo y sincero agradecimiento para todas estas personas que, sin ellas, estoy segura que no hubiera podido llegar hasta aquí.

Y muchas gracias a Tecnología & Sentido Común por darme un altavoz y hacerme la entrevista que me ha permitido disfrutar hablando de mi trabajo, la entrevista que a todo el mundo le gustaría que le hiciesen una vez en su vida. GRACIAS.

P4MGO! Gov Book Governance

La Gobernanza actúa como la columna vertebral de una Gestión efectiva, asegurando la alineación estratégica y el cumplimiento global del propósito.

p4mgo.com

P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Marlon Molina

Migrar y proteger los Mainframe es tendencia

Se nos olvida el Mainframe y hablamos poco de esta plataforma, y no deberíamos ya que ocupa un lugar importante en las grandes corporaciones. Quizá le sorprenda saber que las ventas están creciendo en los últimos años, tanto que Business Research Insights prevé ventas de 6.683 millones de dólares para el año 2032, lo que representaría un 30% de crecimiento en los próximos 7 años.

¿Qué está pasando en el Mainframe?
La época postpandemia ha disparado el consumo de los servicios informáticos, los departamentos de tecnología de las grandes corporaciones han echado mano del Mainframe, los sistemas más fiables de la industria.
Sería fácil asociar el uso de Mainframes a las infraestructuras críticas. Los sectores que mantienen una alta dependencia de esta infraestructura son las finanzas, seguros, sanidad, y gobiernos. Estos sistemas mantienen una alta fiabilidad con una alta tolerancia a fallos.

La banca, finanzas, y seguros son los mercados que más están aumentando su consumo, siendo la seguridad, y las capacidades de almacenamiento las principales razones para volver al consumo.
En 2020 se anunció un cambio del Mainframe a un modelo As a Service en Cloud Computing, no obstante, según Forrester, el 70% del consumo se hace en modo "on premise", es decir, con equipos locales propios.
El 30% del consumo de servicios es híbrido y cloud, esto es una "barbaridad". Mover el 30% de los servicios de los equipos locales a modelos cloud es una acción titánica, y se espera que en los próximos tres años venda más de tres mil millones de dólares.

La migración también implica otro reto, el del personal con conocimiento. En las universidades no se enseña el Mainframe, ingenieros e ingenieras de las últimas tres décadas no conocen estos sistemas. La formación recae directamente en los fabricantes y en las empresas que poseen los usuarios.

CONTINÚA EN PRÓXIMA PÁGINA

AIOps

Los Mainframe incluyen tareas operativas complejas y que requieren conocimientos importantes. Uno de los retos relevantes es organizar las operaciones, automatizar y monitorizar. En una reciente encuesta realizada por BMC, el 94% de los encuestados lo considera una plataforma a largo plazo o una plataforma para nuevas cargas de trabajo.

La Inteligencia Artificial (AI) también ha llegado al Mainframe. Las AIOps (Artificial Intelligence for IT Operations) representan una estrategia que combina tecnologías de inteligencia artificial con herramientas tradicionales de gestión de operaciones de TI (ITOM) para mejorar la eficiencia, la visibilidad y la capacidad de respuesta de los sistemas de TI.

AIOps se enfoca actualmente en la automatización de tareas rutinarias, y la detección temprana de fallos, analizando el rendimiento y tomando decisiones para mantener el balance de los recursos. La IA con suerte asumirá su propio coste de desarrollo e integración, con los ahorros que se espera que produzca.

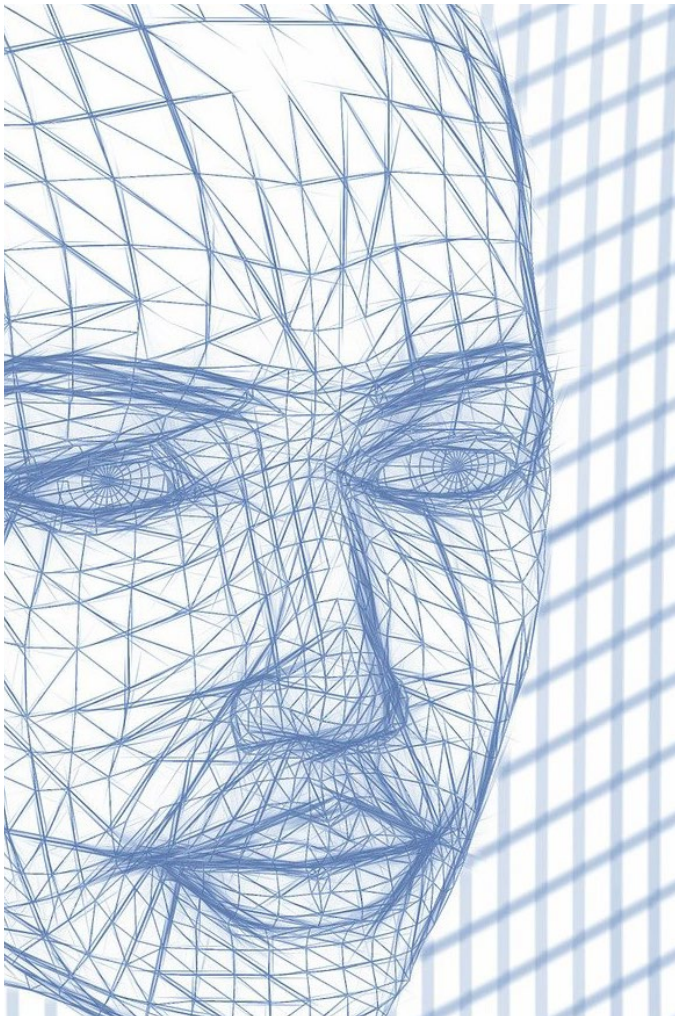
IBM como líder en esta tecnología, ha anunciado que sus próximos mainframes IBM Z y LinuxONE estarán equipados con el nuevo procesador Telum II y un acelerador dedicado a potenciar las capacidades de IA.

El Telum II ofrece un rendimiento superior gracias a su mayor capacidad de memoria y caché, así como a la integración de una unidad de procesamiento de datos (DPU) especializada en acelerar las operaciones de entrada y salida. Además, las capacidades de aceleración de IA integradas en el chip permiten a los mainframes ejecutar modelos de IA de manera más rápida y eficiente.

Una investigación de Morgan Stanley proyecta que las demandas de energía de la IA generativa (IA Gen) se dispararán un 75% anualmente durante los próximos años. La combinación de procesamiento, IA Gen, y consumo energético requerirán una inversión económica y de recurso humano importante.

Digital Operational Resilience Act (DORA)

El Reglamento de Resiliencia Operativa Digital (DORA) es una normativa de la Unión Europea que busca fortalecer la ciberseguridad y la resiliencia operativa digital del



sector financiero. Su objetivo principal es garantizar que las entidades financieras puedan continuar operando de manera segura y eficiente, incluso ante ciberataques o incidentes tecnológicos importantes.

Esta regulación tiene fecha para que se aplique a partir del 17 de enero de 2025, lo que está provocando un aluvión de servicios de validación del cumplimiento (compliance), y por lo tanto incrementando la inversión en el Mainframe en vez de dar la oportunidad para migraciones.

DORA someterá a los sistemas de información a un mayor escrutinio, que es donde el Mainframe es especialista, lleva desde sus inicios siendo auditado, y puede que levante la mano en el sector financiero como la solución más fiable para alcanzar el cumplimiento legal.

MARLON MOLINA

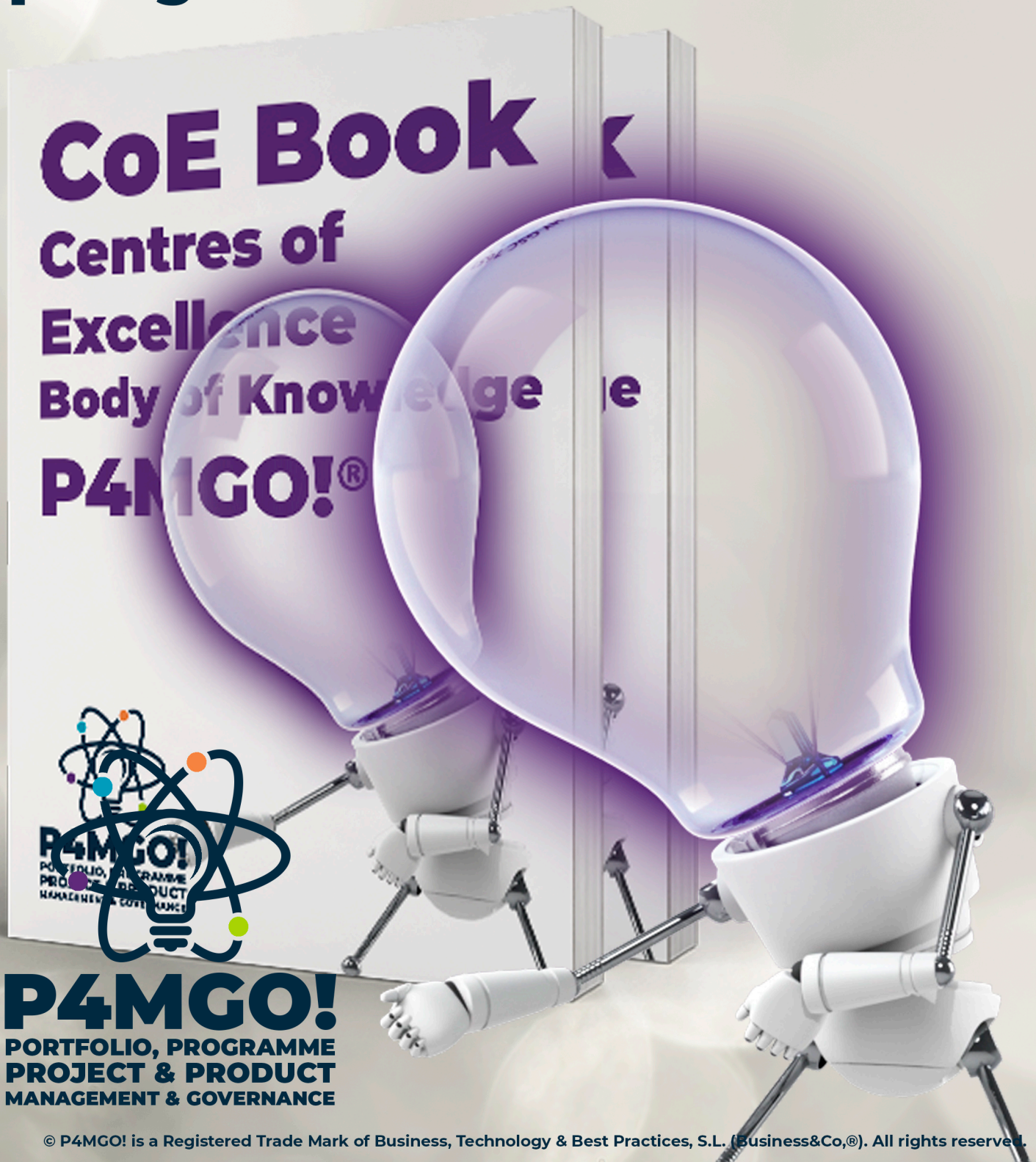
Marlon Molina es ingeniero en informática, es certification officer en Computerworld University desde donde lidera la certificación Business IT, también dirige el laboratorio de ciberseguridad para los Parlamentos de las Américas en la OEA, es profesor en varias Escuelas de Negocio, y es asesor de varios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

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

P4MGO! CoE Book
Centres of Excellence

Los Centros de Excelencia lideran la Innovación y el Cambio Organizacional asegurando el alineamiento estrategico a través de estándares y mejores prácticas.

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME PROJECT & PRODUCT MANAGEMENT & GOVERNANCE

Ricard Martínez Martínez

La inteligencia artificial y la gestión del riesgo regulador

En unas recientes jornadas organizadas por AVALNET tuve el placer de asistir a una inauguración tan emocionante como provocadora. En ella, Manuel Julia abordó los retos de la IA para la empresa valenciana desde un enfoque de riesgo particularmente interesante. Y ello sin ahorrar alguna crítica al marco legislativo y a los enfoques de los reguladores. Su discurso resultó tan significativamente atractivo que me obligó a repensar como ponente cuál era el mensaje que yo debería transmitir a la audiencia y ahora quisiera compartir.

Cuando se trata de incorporar una tecnología tan sofisticada como la inteligencia artificial los juristas no podemos seguir transmitiendo un discurso ajeno a la empresa y de difícil asimilación. Esto impide entender el marco regulador como algo distinto del cumplimiento de un conjunto de obligaciones formales y particularmente caras. Y este es un grave error porque convertimos el derecho en una pieza odiosa, mal recibida por la empresa e incluso por las personas que en ella realizan su actividad, cuyo despliegue acaba siendo particularmente ineficiente, cuando no contraproducente. Nuestra obligación primaria consiste en transmitir cuáles son las virtudes de incorporar un análisis de riesgo regulador y en subrayar el valor estratégico del cumplimiento normativo para la empresa que va incorporar tecnología. Y especialmente para aquella que va a desplegar su actividad en el territorio del desarrollo y la prestación de servicios vinculados a las tecnologías de la información. Y este tipo de riesgo no se refiere únicamente a la posibilidad de que recibamos de una multa.

Se trata de verificar cómo la aplicación de la legislación vigente en áreas significativas y particularmente en materia de protección de datos, de seguridad de la información y de responsabilidad en la prestación de servicios de la sociedad de la información, va a contribuir al despliegue de nuestras ideas al servicio de la innovación empresarial. Las empresas que quieren adoptar la IA como herramienta para desplegar su actividad deben comprender que es necesario acomodar la cultura corporativa, la formación de sus empleados, y el propio modelo de gestión a las condiciones previas imprescindibles para asegurar que no existen riesgos y que no se va a causar ningún daño. Estas tecnologías no funcionan necesariamente como un como un "*plug&play*". Por ello es esencial acomodar toda nuestra práctica a los requerimientos normativos que exigen. Precisamente por ello, el Reglamento de Inteligencia Artificial obliga a desplegar actividades formativas destinadas a todos aquellos que utilicen estas herramientas y, en sede de regulación de los sistemas de alto riesgo, impone un deber de transparencia que asegure que el modelo de despliegue sea el más adecuado y gestione el riesgo para los entornos en los que vayan a funcionar.

Por otra parte, disponer de un modelo de cumplimiento normativo resulta absolutamente estratégico para aquellas entidades que no solo sean meros usuarios pasivos de la tecnología, sino que a la vez deban integrar información propia en el sistema de IA para alcanzar sus objetivos. Veamos un ejemplo sencillo, el de las empresas que para mejorar los procesos logísticos asociados a la entrega de producto al cliente final necesitan realizar estudios de movilidad.

CONTINÚA EN PRÓXIMA PÁGINA

Podrían acudir a productos de IA disponibles en el mercado o a un desarrollo propio. Bastaría con manejar datos de carácter no personal relacionados con la movilidad en una determinada ciudad o con aspectos concomitantes como el clima o la relación de días festivos. Esto seguramente nos pueda ofrecer algún tipo de solución funcional, pero nunca con la eficiencia que nos proporcionaría integrar el modelo con nuestra experiencia práctica en los últimos años.

La empresa usualmente contará con un registro que le permita establecer un perfil de clientes y/o en qué casos se han producido fallos en la entrega. Esta información suele incluir conjuntos de datos de carácter personal que deben haber sido obtenidos lícitamente, respecto de los cuales existe una legítima expectativa de privacidad y, en lo que atañe a nuestro ejemplo, la seguridad de que el cliente entiende a qué nos referimos cuando en las políticas de privacidad informamos sobre usos ulteriores de los datos como la mejora del servicio.

Un cumplimiento riguroso en este ámbito, nos asegura la confianza del cliente, pero también la calidad de los datos. Este elemento es absolutamente estratégico, ya que nos va a permitir operar con confianza a la hora de desplegar la IA para un propósito tan específico como este.

Si la gestión del riesgo en materia de cumplimiento normativo es determinante para empresas cuyo core de negocio no consiste precisamente en ello, adquiere mayor importancia para aquellas cuyo objeto de negocio consiste precisamente en el desarrollo, distribución o despliegue de servicios en el ámbito de la inteligencia artificial. Aquí, conocer un conjunto de piezas de regulación particularmente extenso resulta no sólo es obligatorio sino una oportunidad para el negocio. La Unión Europea está desplegando una batería normativa que atiende a aspectos muy diversos. Nos preocupan las condiciones de ciberseguridad y robustez de producto.

Se despliegan oportunidades de reutilización de datos a través de la modificación de la legislación sobre open data y haciendo surgir espacios de datos públicos y privados a través de las oportunidades que ofrece el Reglamento de Gobernanza de Datos y el futuro Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios. Se promueven condiciones seguras de atribución y validación de la identidad a través del eIDAS. Tratamos de disciplinar las condiciones de responsabilidad en el ámbito de la prestación de servicios digitales. Y finalmente, aunque ello no agota el contenido regulatorio hemos establecido un Reglamento Inteligencia Artificial que, por una parte, atiende a la evaluación del riesgo sistémico para los derechos fundamentales y los sistemas democráticos y por otra contiene instrucciones muy precisas orientadas al diseño de producto.

Y no se trata sólo de poner el foco en los sistemas de alto riesgo que van a necesitar de la aprobación por parte de un organismo notificado y una vigilancia poscomercial, sino de verificar hasta qué punto las metodologías de diseño que propone el Reglamento, pueden ser útiles e incorporarse a los procesos de gestión de las empresas incluso en aquellos casos en los que el despliegue de sus herramientas de inteligencia artificial no sea calificable como de riesgo alto.

Ahora es el momento de entender que las lecciones aprendidas en materia de protección de datos respecto del enfoque centrado en el riesgo y el cumplimiento normativo desde el diseño, no sólo no son una carga para la empresa, constituyen una inversión e incluso una oportunidad para generar negocios robustos y confiables.

RICARD MARTÍNEZ

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

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

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Certificación en:

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
ENERO 2025

Solicita tu admisión en:

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

Marcos Navarro

Condúceme - Los vehículos autónomos

En este año 2034, ya estamos acostumbrados a los vehículos sin conductor, expresamente diseñados así. Miramos atrás con asombro al vertiginoso progreso que hemos experimentado en el campo de los sistemas de transporte autónomos. Lo que una vez pareció ciencia ficción se ha convertido en nuestra realidad cotidiana, transformando radicalmente la forma en que nos movemos y vivimos en las ciudades modernas.

LA REVOLUCIÓN DEL VEHÍCULO AUTÓNOMO EN LAS CUIDADES

Hace apenas una década, los vehículos autónomos eran poco más que prototipos experimentales y sueños futuristas. Hoy, son una parte integral de nuestro paisaje urbano

Las calles están pobladas por una flota diversa de vehículos sin conductor, desde automóviles particulares hasta autobuses y camiones de reparto, todos moviéndose con gran precisión gracias a una combinación de sensores avanzados, visión e inteligencia artificial y de una conectividad a hipervelocidad. Solo unos pocos nostálgicos, penalizados por los impuestos, pueden conducir sus propios vehículos. Las ciudades y su infraestructura ya no están hechas para ellos, sino para los vehículos autoguiados.

La proliferación de los vehículos autónomos en nuestras ciudades ha requerido una transformación profunda de la infraestructura urbana. Las "smart cities" de 2034 están equipadas con una densa red de sensores y conectividad que permiten una comunicación constante entre vehículos, infraestructura y peatones.

Las señales de tráfico tradicionales han sido reemplazadas en gran medida por sistemas mixtos que incluyen señalización digital dinámica. Estos sistemas recopilan información del estado del tráfico a través de la conexión datos y sensores distribuidos por la cuidad y a su vez permiten a los coches autónomos acceder a la información para optimizar sus movimientos. Así el tráfico puede cambiar instantáneamente optimizando el flujo de vehículos y reduciendo la congestión.

Gran parte de las áreas urbanas incluso han establecido grandes "zonas autónomas" donde solo se permite la circulación de vehículos sin conductor, creando espacios urbanos más seguros y menos congestionados.

Por otro lado, las zonas reservadas y la proliferación de servicios de transporte autónomo compartido han llevado a una disminución significativa en la propiedad de vehículos particulares. Empresas como Uber y Lyft, que se adaptaron rápidamente a la era autónoma, ofrecen ahora servicios de suscripción que permiten a los usuarios acceder a una flota de vehículos autónomos según sus necesidades.

La adopción generalizada de vehículos autónomos ha tenido un impacto significativo en la seguridad vial. Los accidentes de tráfico se han reducido en más de un 90% en las "áreas autónomas". Esto ha sido debido no solo a los vehículos autónomos sino también a los implantes cerebrales BCI, que las personas llevan, que están en alerta permanente interactuando con los sistemas inteligentes de las cuidades.

Los sistemas de transporte autónomos también han contribuido significativamente a la reducción de emisiones de gases de efecto invernadero. La optimización de rutas, la conducción más eficiente y la existencia sólo de vehículos eléctricos han disminuido la huella de carbono del transporte urbano en un 94% respecto a 2020.

Mientras que los vehículos terrestres autónomos son ahora comunes, la próxima frontera está en el aire y en el agua. Empresas como Volocopter y Lilium lanzaron hace casi una década servicios comerciales de taxis aéreos autónomos en varias ciudades. Si bien ya ha servicios autónomos en estos entornos, las autorizades que gestionan las cuidades, no están habilitando gran número de licencias para su uso, ya que quieren evitar una congestión aérea similar a la terrestre.

LA TECNOLOGÍA

La visión artificial se ha convertido en el "ojo" de los vehículos autónomos, permitiéndoles percibir y comprender su entorno con una precisión superior a la humana.

CONTINÚA EN PRÓXIMA PÁGINA

Los sistemas de reconocimiento de imágenes basados en *deep learning*, permiten a los vehículos autónomos interpretar su entorno en tiempo real. La visión artificial también ha superado las limitaciones humanas en condiciones adversas. Los algoritmos avanzados, que combinan la imagen con los sistemas de posicionamiento (GPS/Galileo), información meteorológica, y sensores urbanos mejoran la conducción en situaciones de lluvia, niebla o poca iluminación, garantizando que los vehículos autónomos puedan "ver" claramente en todo momento.
En la década de los 20, compañías como *Tesla, Waymo, Cruise, Aurora, Toyota y Mercedes*, desarrollaron los primeros sistemas de conducción autónoma, pero eran un complemento a la conducción humana. Ahora la conducción humana en estos vehículos no es una opción. Los vehículos carecen de puesto de conducción.
Una de las ventajas clave de la IA en los vehículos autónomos es su capacidad de aprendizaje continuo. Los datos capturados por los diferentes sistemas que alimentan constantemente los algoritmos, permitiendo que el sistema mejore y se adapte a nuevas situaciones y entornos.

UNA LEGISLACIÓN ESPECIFICA

En nuestro mundo actual ha habido que desarrollar gran cantidad de leyes para regular las actividades realizadas por la inteligencia artificial y sus ramificaciones.
Ya en la década de los 20 la Dirección General de Tráfico (DGT) fue pionera en la implementación de un manual de circulación segura que establecía reglas específicas para vehículos autónomos. Hoy en día todos los vehículos autónomos tienen actualizada la información regulatoria en sus sistemas. De esta manera sus algoritmos de actuación cumplen de manera estricta las legislaciones en vigor. Los vehículos recopilan, en función de su posición, la legislación aplicable en cada país, comunidad o área de manera desatendida.
Los vehículos autónomos no incumplen las normas, esto ha tenido un impacto directo en el ya obsoleto sistema de multas por infracciones en el tráfico, que ha sido sustituido por nuevos impuestos, con la considerable queja de los ciudadanos, que siempre han sabido que las multas no era un sistema para desincentivar las conductas ilegales sino un objetivo recaudatorio.
La legislación actual abarca cuestiones complejas de responsabilidad en caso de accidentes involucrando vehículos autónomos. Además, se han establecido directrices éticas para la programación de algoritmos de toma de decisiones en situaciones de riesgo inevitable.
Adicionalmente, la legislación ha tenido que adaptarse para garantizar la protección de datos personales y a ciber-seguridad. Se han implementado estrictos estándares de encriptación y protocolos de seguridad para prevenir hackeos y proteger la privacidad de los usuarios.
Uno de los sectores que se ha tenido que reinventar ha sido el asegurador. La responsabilidad en caso de accidentes se desplazado del conductor al fabricante del vehículo o al proveedor del servicio de coche autónomo. Han surgido nuevas coberturas, como seguros contra fallos tecnológicos o ciberataques, y no tanto centrados en accidentes, ya que la siniestralidad en este ámbito es prácticamente nula. También se ha hecho común el seguro instantáneo o basados en el uso, donde las primas se calcularán

en función del tiempo y la actividad que se desarrolle, por ejemplo, la distancia que el vehículo opere de manera autónoma.

RIESGOS Y RESTRUCTURACIÓN DEL SECTOR

A medida que nuestros sistemas de transporte se han vuelto más conectados, también se han vuelto más vulnerables a ciberataques. Los incidentes de hackeo de vehículos autónomos, aunque raros, han planteado serias preocupaciones sobre la seguridad y la privacidad. Los sistemas de gestión de tráfico y los sistemas que gobiernan la conducción de los vehículos se han convertido en infraestructuras críticas en todos los países, disponiendo de una regulación y protecciones especiales. Hace ya 10 años que compañías como *Microsoft y Alphabet* invirtieron grandes cantidades de dinero en el desarrollo de sistemas de seguridad robustos para proteger estas redes críticas.
Por otro lado, la transición a vehículos autónomos ha tenido un impacto significativo en el empleo en el sector del transporte. Millones de conductores de taxi, camión y autobús han tenido que buscar nuevas oportunidades laborales. Ya en los años 20 hubo manifestaciones en todo el mundo cuando se concedieron las primeras licencias para taxis autónomos con la introducción del *Cybercab y Cybervan de* Tesla, sin embargo, no pudieron frenar la reconversión del sector. Como en toda revolución tecnológica, y en contraposición, han surgido nuevos empleos en áreas como mantenimiento de flotas autónomas, gestión de redes de transporte y desarrollo de software especializado.
Así, en 2034, los sistemas de transporte autónomos han pasado de ser una visión futurista a una realidad cotidiana que ha transformado profundamente nuestras ciudades y nuestra forma de vida. La colaboración entre empresas tecnológicas, fabricantes de automóviles y gobiernos ha sido crucial para superar los desafíos técnicos, regulatorios y sociales que planteaba esta revolución.

MARCOS NAVARRO ALCARAZ

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

Twitter:
https://twitter.com/mnalcaraz

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

P4MGO! PMO Book Management Offices

Las Oficinas de Gestión de Porfolios, Programas, Proyectos y Productos empujan el Cambio Organizacional apoyando el cumplimiento de estándares.

p4mgo.com

P4MGO!
PORTFOLIO, PROGRAMME PROJECT & PRODUCT MANAGEMENT & GOVERNANCE


Kawasaki man arrested over malware made using generative AI
/Rooted VALENCIA X
TARLOGIC

Rootedcon Valencia: X Aniversario

El pasado 15 y 16 de octubre se celebró la décima edición de la RootedCon en Valencia, y Tecnología y Sentido Común no faltó a la cita anual con este evento. Rooted es una asociación de expertos en ciberseguridad que desarrolla conferencias en la materia en varias ciudades de España, y desde este 2024, también en Portugal y Panamá. En el caso de valencia, como decíamos, se celebró la décima edición, que comenzó el martes 15 con una serie de formaciones altamente especializadas, y que continuó el miércoles 16 en el incomparable marco del Museo de las Ciencias Príncipe Felipe.

La jornada se inició con una alocución de Alberto Rodríguez, coordinador de la organización RootedCon en Valencia, en la que, además de agradecer la presencia de los asistentes, transmitió también su agradecimiento a los colaboradores de la organización y a los patrocinadores del evento y realizó un breve recorrido por la historia de esta conferencia de ciberseguridad en su sede de Valencia.

La primera ponencia técnica de la mañana corrió a cargo de Francisco Alvarez, de la empresa Tarlogic, titulada "Vulnerabilidades en TMP y BitLocker, CTF Hardware", en la que analizó el estado actual de BitLocker, el estándar de cifrado nativo de Microsoft, explorando sus mecanismos de seguridad y la integración con el hardware. Puso claramente el foco en desmontar cualquier sensacionalismo reciente al respecto del posible compromiso del protocolo de cifrado, y disertó sobre cómo BitLocker utiliza el Trusted Platform Module (TPM) para ofrecer una capa adicional de protección, profundizando en las diferentes versiones y funcionalidades del mismo. Abordó posibles escenarios de ataque, como la vulnerabilidad Man-in-the-Middle (MiTM) entre BitLocker y TPM, explicando cómo y por qué este tipo de ataque es factible con una demo, que acompañó con el sorteo entre los asistentes de unas placas educativas para aprender a manejar los chips TPM.

La segunda charla cambió totalmente de tercio. Titulada "Understand Your Attackers: The Role of Sandboxing in Threat Intelligence", su autor, Michael Bourton, de la empresa VMRay, desglosó las ventajas que un sistema de sandboxing y de las tecnologías de inteligencia de amenazas pueden tener para mejorar la seguridad si se cumplen determinadas condiciones de calidad en el producto. Entre las ventajas que citó, destacó la integración con fuentes abiertas de información de seguridad, tales como indicadores de compromiso bien trabajados y validados.

CONTINÚA EN PRÓXIMA PÁGINA

Tras un primer descanso, retomó las ponencias toda una eminencia valenciana en el análisis y lucha contra el malware, Josep Albors, de ESET España, que con la ponencia "Dos años después, ¿ha revolucionado realmente la IA el panorama del phishing y las estafas en España?", analizó si realmente los efectos de los grandes modelos lingüísticos (LLM) basados en inteligencia artificial, como predecían algunas voces, han supuesto un quebradero de cabeza para los expertos en ciberseguridad, ante las posibilidades que se abrían a los delincuentes con herramientas fáciles de usar y que permitían preparar campañas de phishing mucho más sofisticadas y convincentes. Para realizar el análisis, Albors desglosó numerosas campañas de phishing llevadas a cabo a través de diferentes vectores de ataque como correos electrónicos maliciosos o publicaciones en redes sociales, centrándose principalmente en aquellas dirigidas a usuarios y empresas españolas. También repasó qué herramientas o servicios soportados por IA utilizan actualmente los ciberdelincuentes, dando las claves a tener en cuenta para detectar estas campañas o, al menos, mitigar su impacto.

El siguiente ponente fue otro "primer espada" de la ciberseguridad en la Comunidad Valenciana: nuestro compañero de tecnología y Sentido Común Alejandro Aliaga, que son su ponencia "La transformación silenciosa del SOC", desgranó las que, a su juicio, eran las nuevas necesidades que debía cubrir un SOC (Security Operations Center). Centró su intervención en resaltar que los SOC, tal y como se conciben a día de hoy, se encuentran en el mismo punto de inflexión al que se enfrentó el mundo del desarrollo de software hace muchos años con la llegada del big data. Según explicó, los centros de operaciones de seguridad, están tratando de innovar para ser más eficientes, y más ágiles en la respuesta frente a incidentes. Asimismo, introdujo otros conceptos, como el de "SOC as a Code" o el de "Detection as a Code", dos conceptos que pueden marcar un antes y un después en cómo conocemos los SOC actualmente.

Justo antes de la parada para comer, Jezer Ferreira deleitó a los asistentes con una charla desenfadada y, como él mismo dijo, políticamente incorrecta sobre "El Arte de desanonimizar perfiles de RRSS con técnicas OSINT (sin IA)". En esa charla de OSINT (Open Source Intelligence), exploraró técnicas avanzadas para desanonimizar perfiles en redes sociales como Facebook, Instagram, Telegram, Twitter y TikTok con el objetivo de mostrar a los asistentes cómo descubrir la identidad real detrás de cuentas aparentemente anónimas utilizando métodos éticos y legales (en palabras suyas, casi siempre) de recopilación de información pública. Una charla tremendamente interesante y que, por lo que se pudo constatar durante el parón para comer, fue muy apreciada por los asistentes.

Ya en la jornada vespertina, Sara Martínez explicó a los presentes algunas "Estrategias de ciberseguridad en pruebas software", en la que se reconoce la importancia del desarrollo seguro de software desde el diseño, y la estrecha relación entre la calidad del software y su seguridad. En la ponencia, se planteó cómo los analistas de calidad software pueden contribuir a mejorar en este entorno de la ciberseguridad.

La siguiente ponencia de la tarde corrió a cargo de Ana Isabel Prieto y Roberto Amado, de la empresa valenciana de seguridad S2 Grupo. Estos expertos plantearon y demostraron dos técnicas diferentes para detectar la falsificación del User-Agent con el que los programas acceden a recursos de servidores web, en su ponencia "User Agent spoofing detection. Una aproximación basada en IA". Esta cuestión reviste importancia desde el momento de que una de las primeras acciones que realiza un atacante o un Pentester durante una intrusión, es la modificación del User-Agent de las herramientas que utiliza para no disparar alertas de seguridad en los dispositivos de monitorización del objetivo.

CONTINÚA EN PRÓXIMA PÁGINA


/Rootəd
Que comience RootedCON Valencia 202
/Rootəd
VALENCIA
X
MUCHAS GRACIAS
024 KeyNote

En este sentido y desde el punto de vista defensivo mostraron por qué es interesante poder detectar esas acciones, mediante métodos heurísticos, y recientemente, usando sistemas de Inteligencia Artificial.

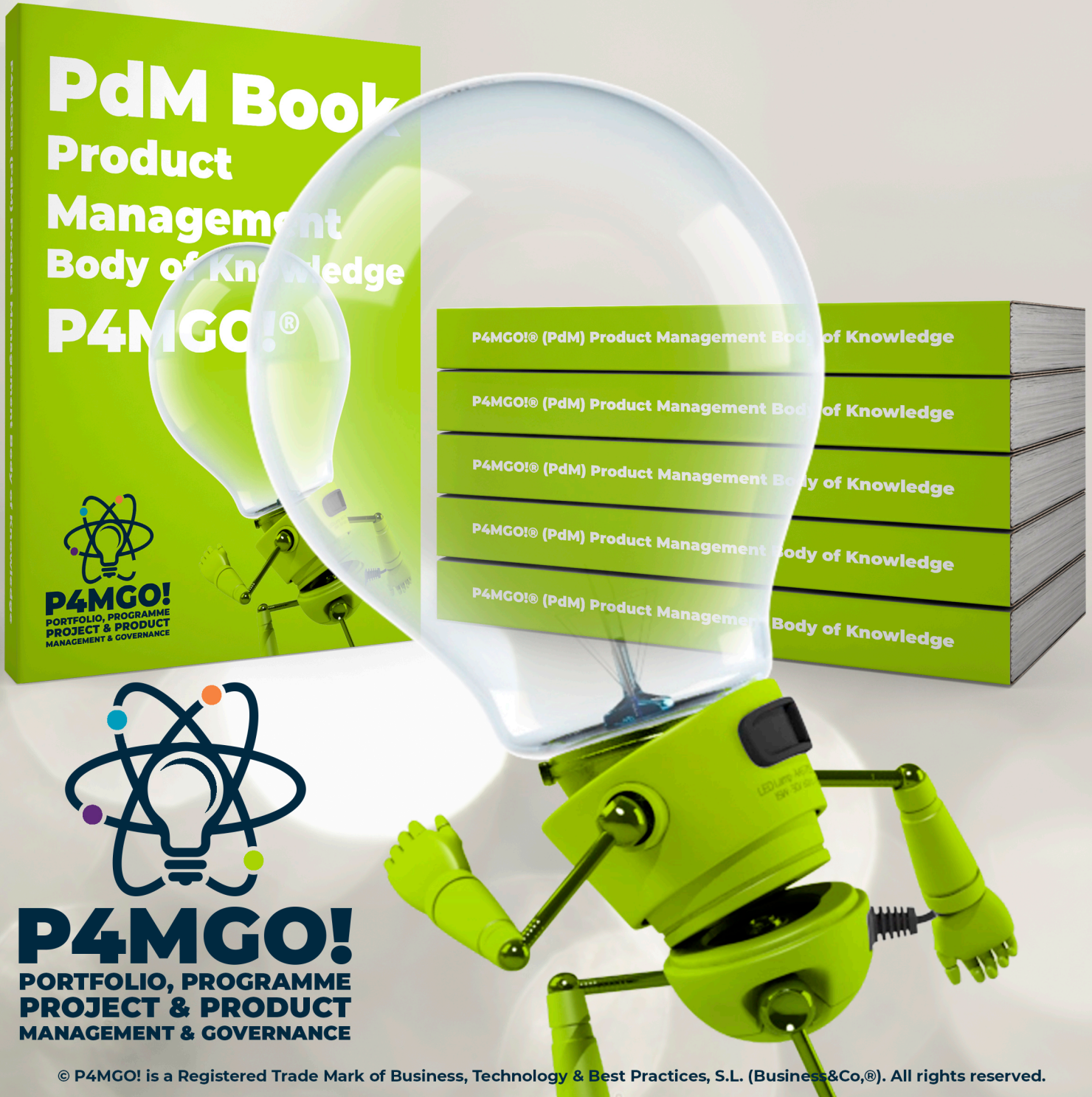
La última ponencia de la tarde, y de la jornada, se titulaba “Pentesting in the field: Auditorías con Rogue Hardware en Entornos Dºesconectados”, y fue desarrollada por David Melendez y Gabriela García. En esa charla, los autores exploraron cómo llevar a cabo auditorías de seguridad in situ en entornos no conectados a internet, tales como los sistemas de control industrial. Para ello, planteaban el uso de hardware especializado que permita la gestión remota de los mismos y el acceso a la red desconectada.

Con el cierre de esta edición de RootedCon se pone de manifiesto de nuevo el interés que suscita la temática de la ciberseguridad y la conveniencia, por tanto, de celebrar este tipo de eventos altamente especializados, que aúnan ponencias y formaciones, y que ayudan que nuevas hornadas de personal técnico se incorpore a la lucha global contra la ciberdelincuencia. Desde Tecnología y Sentido Común felicitamos a la organización, tanto por el éxito de esta edición, como por el hecho de que ya hayan conseguido llevar a cabo la RootedCon en Valencia por décima ocasión.

P4MGO! PdM Book
Product Management

La Gestión de Productos se enfoca en la Gestión Ágil de Desarrollo de Software y Servicios Digitales clave para mantener la competitividad y generar valor continuo.

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Víctor Almonacid

Se acabó lo de numerar, foliar y matasellar un documento

Empezaremos refiriendo una norma obsoleta pero en vigor, el Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, que al no estar derogado se aplica escrupulosamente en muchos ayuntamientos, sin entender que ha sido implícitamente reformulado por una Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que establece claramente, a lo largo de todo su articulado, que el procedimiento administrativo es electrónico. Pero no citaremos ningún precepto de la norma de 2015, ya que no ofrecen lugar a dudas, sino dos, los artículos 198 y 205, de la de 1986:

•"El Libro de Actas, instrumento público solemne, ha de estar previamente foliado y encuadernado, legalizada cada hoja con la rúbrica del Alcalde o Presidente y el sello de la Corporación, y expresará en su primera página, mediante diligencia de apertura firmada por el Secretario, el número de folios y la fecha en que se inicia la transcripción de los acuerdos".

•"Las certificaciones se expedirán por orden del Presidente de la Corporación y con su "visto bueno", para significar que el Secretario o funcionario que las expide y autoriza está en el ejercicio del cargo y que su firma es auténtica. Irán rubricadas al margen por el Jefe de la Unidad al que corresponda, llevarán el sello de la Corporación y se reintegrarán, en su caso, con arreglo a la respectiva Ordenanza de exacción, si existiere".

Obviamente, si los preceptos indicados se aplicasen literalmente en 2024, tendríamos que imbricar dichos foliados, encuadernados, sellos, firmas y rúbricas del mundo físico sobre documentos en papel. Pero resulta que ahora los documentos son y deben ser electrónicos, los cuales, tramitados en su orden, conforman expedientes asimismo electrónicos. Y no lo digo solo yo. Lo dicen el Tribunal Superior de Justicia de Catalunya y el mismísimo Tribunal Supremo a través de sendas sentencias.

Empecemos por la del órgano citado en primer lugar, que es de este mismo año y que, en su propio texto, cita a su vez la del Supremo, también reciente pues tan solo tiene un año de antigüedad. En efecto, la Sentencia del TSJ de Catalunya (Res 1844/2024, de 31/05/24) afirma (si bien sería más preciso decir «confirma») que **el procedimiento administrativo en papel dejó de existir**, porque, efectivamente, este es electrónico en la actualidad. A continuación, destacamos la parte del texto que interesa en el contexto de este artículo (la negrita es nuestra):

"… el expediente administrativo remitido consta con un índice, si bien no en la forma tradicional sino en forma de árbol que permite analizar cada una de las fases, y diligencias practicadas y son claramente distinguibles.

CONTINÚA EN PRÓXIMA PÁGINA

> **Caminemos siempre hacia adelante, la única persona que tuvo éxito caminando hacia atrás es Michael Jackson, y en realidad fue porque estaba innovando (inventó un nuevo paso de baile**
>
> ***El autor***

Debemos tener en cuenta que la LJCA 29/1998, establece este requisito atendiendo al expediente en formato papel que en aquellos momentos podía ser presentado en forma física o bien escaneado en CD. En la actualidad la transformación que se ha producido en sede de la Administración con **la introducción de las nuevas tecnologías ha impulsado y establecido el «expediente electrónico», como consecuencia de la eliminación del papel y, por tanto, del foliado «stricto senso» de documentos, sustituyendo éste último por el indexado de los documentos que lo conforman**. El expediente remitido refleja esta circunstancia.

Asimismo, señalar a la parte que **el expediente administrativo es electrónico, según el art. 70 Ley 39/2015** y el mismo ha de contener todas las actuaciones que son antecedente y fundamento de la decisión administrativa. De conformidad con el apartado segundo del artículo 70 de la Ley 39/2015, **el expediente administrativo, tendrá formato electrónico, formándose el expediente administrativo electrónico mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos, así como un índice -no tradicional- numerado de todos los documentos que contenga cuando se remita. Asimismo, deberá constar en el expediente copia electrónica certificada de la resolución adoptada.** Ese índice puede producirse, como aquí se muestra, en forma de árbol, señalando cada una de las fases y dentro de las mismas las múltiples diligencias y actuaciones de las partes. Y ello, en absoluto, genera indefensión. Cabe mencionar que **el TS**, Sala Tercera , Sección Cuarta, dictó sentencia núm. 1.336/2023 de fecha 26 de octubre de 2023, en el asunto 1026/2022, mediante la que **señaló**, con relación al expediente administrativo electrónico, que **«Una transformación de documentos en formato papel a un formato digital no es simplemente proporcionar una imagen escaneada, sino que la imagen ha de poder identificarse para su eficaz y rápida consulta mediante el correspondiente índice conforme a las exigencias legales.»** De esta forma, se está admitiendo que el documento debe poder visionarse individualmente a partir de la elección del interesado.

Al citar la actora normativa de las entidades locales del año 1986 parece que se está refiriendo a un modelo de expediente que ya no existe -el de papel– y respecto del que no puede solicitar un índice al estilo tradicional de «foliado» numérico. Asimismo, se incluye la autenticación de la copia del expediente administrativo, claramente expuesta y firmada electrónicamente por la Abogacía del Estado-Secretaría. Por todo ello, y sin perjuicio de que pudo solicitar complemento si algún archivo estaba incluido o completo, no cabe apreciar vicio alguno de los que enuncia ya que la normativa vigente no es la que cita que se refiere a un expediente escrito. Se desestima este motivo **no sin señalar la extrañeza de su alegación atendida su condición de letrado ejerciente**".

VÍCTOR ALMONACID

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

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

P4MGO! BPM Book
Process Management

La Gestión por Procesos de Negocio asegura una estructura eficiente y optimizada facilitando no solo la comprensión de los procesos sino su alineamiento con los objetivos estratégicos.

p4mgo.com

P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Alex Aliaga

Defendiendo las comunicaciones de los drones con IA

UAVs y el aumento de las amenazas de ciberseguridad

Los Vehículos Aéreos No Tripulados (UAVs), comúnmente conocidos como drones, se han convertido en una tecnología transformadora, revolucionando industrias como la entrega de paquetes y la asistencia en desastres. Sin embargo, la proliferación de drones también ha abierto la puerta a vulnerabilidades de ciberseguridad. A medida que los drones ganan protagonismo en los dominios civiles y militares, los datos que transportan y transmiten se han convertido en un objetivo valioso para los ciberdelincuentes. Desde la captura de información de vigilancia sensible hasta la manipulación de trayectorias de vuelo, los UAVs son ahora un foco importante en el campo de la ciberseguridad.

Un aspecto crítico que hace vulnerables a los drones es su dependencia de protocolos de comunicación inalámbrica como el sistema de Identificación Remota (RID). RID es un marco regulatorio diseñado para mejorar la seguridad del espacio aéreo, exigiendo que los drones transmitan datos de telemetría, como la ubicación y la información del operador. Sin embargo, tal como se destaca en algunas investigaciones, estos sistemas tienen varias vulnerabilidades que exponen a los drones a ataques de suplantación de identidad e inyección de datos.

ENFOQUES TRADICIONALES EN LA CIBERSEGURIDAD DE UAVS

En los primeros días de despliegue de drones, los métodos convencionales de ciberseguridad se basaban en gran medida en protocolos de seguridad estáticos. Sistemas como cortafuegos y sistemas de detección de intrusiones estáticos (IDS) se utilizaban para monitorear patrones de ataques conocidos. Sin embargo, estos métodos no podían seguir el ritmo de la naturaleza dinámica de las redes de drones, especialmente al considerar la complejidad y rápida movilidad de estos sistemas.

El uso de la **Identificación Remota de Drones (RID)** se introdujo para contrarrestar este problema, permitiendo a los reguladores y autoridades rastrear drones en tiempo real sabiendo en todo momento los datos del operador del mismo. No obstante, este protocolo carece de medidas de seguridad básicas como el cifrado y la integridad de datos, lo que lo hace susceptible a una variedad de ataques que podrían tener graves consecuencias para operaciones tanto militares como civiles .

EL PODER DEL APRENDIZAJE AUTOMÁTICO EN LOS SISTEMAS DE DETECCIÓN DE INTRUSIONES

En los últimos años, la integración del **aprendizaje automático (ML)** en los sistemas de seguridad ha marcado un cambio de paradigma en la ciberseguridad de drones. A diferencia de los sistemas IDS tradicionales que dependen de firmas predefinidas de ataques conocidos, los sistemas IDS basados en ML pueden detectar amenazas nuevas identificando desviaciones de patrones de comportamiento normales. Esta adaptabilidad es crucial, especialmente para los drones que operan en entornos cambiantes.

Los algoritmos de aprendizaje automático pueden entrenarse para monitorear grandes cantidades de datos de tráfico de red, aprendiendo a diferenciar entre patrones normales y anómalos.

CONTINÚA EN PRÓXIMA PÁGINA


Altitude Zone 833 ft
MF
2.0 mph
H 114 ft
8.2 mph
D 529 ft

Al aprovechar grandes conjuntos de datos, los sistemas basados en ML pueden detectar ciberataques sofisticados que los métodos convencionales podrían pasar por alto. En el contexto de los drones, el uso de un sistema de estas características permite mejorar la detección de accesos no autorizados, suplantación de señales de control e incluso vulnerabilidades en el protocolo RemoteID .

VULNERABILIDADES EN LOS PROTOCOLOS DE IDENTIFICACIÓN REMOTA

Los estándares del protocolo RemoteID requieren que los drones transmitan periódicamente sus datos de telemetría. Sin embargo, las implementaciones actuales de RID no logran asegurar estos datos, dejándolos expuestos a ataques de inyección y reproducción. Por ejemplo, un atacante puede inyectar datos RID falsos para simular la presencia de un dron en un área restringida, provocando falsas alarmas y potencialmente paralizando las operaciones del espacio aéreo.

La importancia de asegurar los sistemas RID se hizo evidente en el infame **incidente del aeropuerto de Gatwick** en 2018, donde drones volando cerca del aeropuerto obligaron a desviar más de 1,000 vuelos. Aunque los detalles del ataque no están claros, resaltó la necesidad de sistemas de identificación y rastreo de drones robustos y resistentes a la manipulación. Las tecnologías RID actuales no habrían podido distinguir entre drones reales y falsificados, haciendo que escenarios como este sean un campo fértil para los atacantes.

PRÓXIMOS PASOS EN LA SEGURIDAD DE UAV Y APLICACIONES DE ML

A medida que los drones continúan evolucionando, también lo harán los métodos utilizados para asegurar su operación. Un área emergente de interés es el uso del **aprendizaje por refuerzo** para optimizar las operaciones de los drones en respuesta a posibles amenazas cibernéticas. Al simular diferentes escenarios de ataque, los drones pueden aprender a reaccionar de manera autónoma, mejorando tanto su seguridad como su eficiencia operativa.

Enfoques colaborativos de seguridad Los avances futuros probablemente implicarán la colaboración entre fabricantes de drones, expertos en ciberseguridad y organismos reguladores. Al trabajar juntos, estas partes interesadas pueden crear ecosistemas de drones más resilientes, particularmente mediante la mejora continua de estándares como RID y el desarrollo de métodos de cifrado más sólidos.

Además, la investigación sobre protocolos de comunicación seguros, como los marcos de **radio definida por software (SDR)**, jugará un papel crucial en la mitigación de amenazas cibernéticas .

Una vez más, debemos contemplar la seguridad de las comunicaciones inalámbricas como un vector de ataque a todos nuestros sistemas. Tal y como venimos abordando en la revista, muchas veces no se tienen en cuenta y pueden suponer un grave problema de seguridad.

ALEX ALIAGA

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

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

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
ENERO 2025

Solicita tu admisión en:

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

Marta Martín

Fatiga por TDAH

10 razones por las que siempre estás cansado

No hay duda de que las personas con TDAH generalmente muestran un aspecto enérgico y repleto de vitalidad. Pero lo cierto es que son personas que se esfuerzan cada día por vencer un agotamiento crónico provocado por sus síntomas.

Cuando hablamos de trastorno por déficit de atención e hiperactividad nos imaginamos una persona hiperactiva, con un nivel de energía muy elevado y una actividad frenética.
Sin embargo, las personas con TDAH suelen estar muy cansadas. La fatiga forma parte de su día a día y la sensación constante de agotamiento les sigue como si fuera su propia sombra. Y no se trata solo de un cansancio físico sino también de un cansancio mental y emocional que es aún más preocupante.

¿ES EL TDAH LA EXPLICACIÓN AL CANSANCIO PERMANENTE?

Lo cierto es que no hay una única causa que lo explique, más bien es un cóctel de problemas que forman la tormenta perfecta para que el TDAH provoque tanta fatiga. Estos son los motivos más habituales.

1.Hiperactividad e hiperconcentración
La hiperactividad en el TDAH puede ser agotadora a nivel físico. Esa necesidad constante de moverse y la dificultad de permanecer quieto consumen una cantidad significativa de energía. Por el contrario, la hiperconcentración suele provocar agotamiento, pero mental ya que, durante la hiperconcentración, las personas pueden estar tan absortas en una tarea que ignoran necesidades físicas como comer o dormir, lo que provoca fatiga.

2.Problemas de sueño
El TDAH viene de fábrica con ciclos de sueño alterados, lo que incluye dificultad para conciliar el sueño, continuos despertares durante la noche, activación mental nocturna, síndrome de las piernas inquietas, entre otros. La mala calidad del sueño conduce directamente a un aumento de la somnolencia diurna y una reducción de la función cognitiva, así como al deterioro de los circuitos de activación, alerta y regulación del cerebro.

3.Estrés por el manejo de los síntomas
Sin duda, el esfuerzo que se requiere para mantener la concentración, la organización y el control de las conductas impulsivas puede ser mentalmente abrumador. Este estrés tiene un efecto directo en los niveles de energía, en el agotamiento y la depresión.

4.Aburrimiento
Las tareas rutinarias o carentes de estimulación provocan un aburrimiento en las personas con TDAH que es agotador mentalmente. El cerebro lucha por mantenerse activo y alerta en estos entornos menos estimulantes, con el consiguiente desgaste de energía.

5.Problemas de dopamina
Un cerebro con TDAH es un cerebro con unos niveles deficientes de dopamina, el neurotransmisor que nos permite regular las respuestas emocionales y actuar para lograr recompensas específicas y el responsable de los sentimientos de placer y recompensa. Esta alteración de los niveles provoca sensación de fatiga y falta de motivación, lo que hace que las actividades diarias sean más extenuantes y menos gratificantes.

6.Dosis inadecuada de medicamentos
Los medicamentos, en particular los estimulantes, son una de las patas fundamentales en el tratamiento del TDAH. Pero es muy complicado dar con el medicamento correcto y la dosis adecuada. Cuando este no es así, los desajustes pueden ser los culpables de una ansiedad abrumadora e incluso de agravar los efectos secundarios.

CONTINÚA EN PRÓXIMA PÁGINA


off

7.Sobrecarga sensorial
Muchas personas con TDAH participan de una mayor sensibilidad a su entorno y suelen sobreestimularse por el ruido, la luz o demasiada gente, por la textura de los alimentos o la sensación que producen ciertos tejidos.

Entonces, se sobreestimula uno o varios sentidos y el cerebro envía demasiada información para ser procesada y, por lo tanto, se produce la consiguiente fatiga significativa y la necesidad de un período para recuperarse.

8.Niebla mental
Con este término nos referimos a la confusión mental provocada principalmente por la disfunción cognitiva en el TDAH, es decir, la dificultad para organizar, planificar, tomar decisiones, establecer metas y autorregularse. de manera que las tareas cognitivas que, en principio, son simples se vuelven abrumadoras lo que contribuye aún más al ciclo de fatiga. Cuando la niebla mental se instala trae consigo olvidos, despistes, confusión y, por supuesto, cansancio.

9.Fatiga por decisión
O la fatiga por la toma constante de decisiones, lo que conlleva un agotamiento mental, ya que la dificultad para decidir es uno de los síntomas característicos. El cerebro queda extenuado sobre todo cuando las decisiones son complejas, cuando hay estrés, cuando se es perfeccionista o hay falta de sueño, condiciones recurrentes en las personas con TDAH.

10.Picos de energía
Son esos momentos en que las personas con TDAH se muestran eufóricos y se ven inmersos en una actividad febril, realizan múltiples tareas y son muy efectivos. Pero cuando la energía decae, se sienten extenuados por el esfuerzo.

En las personas con TDAH suelen coincidir varias de estas circunstancias a pesar de la imagen de ser siempre muy energéticos, vitales e incansables. La fatiga es un compañero de viaje persistente, un compañero que necesita herramientas y estrategias que le mantengan a raya para poder afrontar el día a día.

MARTA MARTÍN

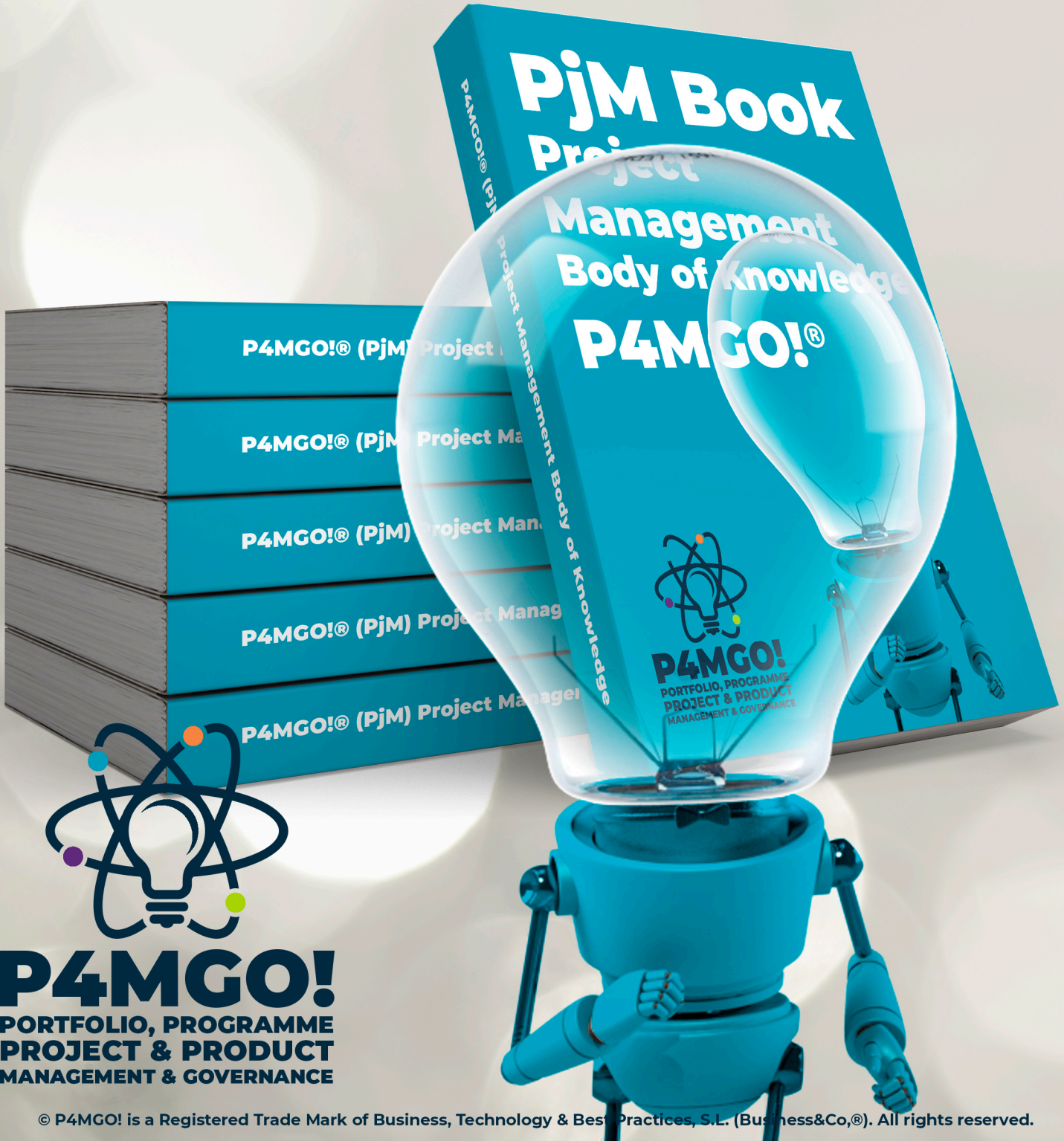
Mujer diagnosticada con TDAH en su madurez, como tantas otras, en una de las revisiones de TDAH de su hijo. Licenciada en Periodismo y Derecho, actualmente cursa sus estudios de Doctorado en Ciencias de la Información y está escribiendo su primera novela. Trabaja en el sector audiovisual y es profesora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

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

P4MGO! PjM Book
Project Management

La Gestión de Proyectos es responsable de la consecución de entregables concretos dentro de un alcance, tiempo, coste, riesgo y calidad determinados.

p4mgo.com



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Los estándares impulsan los informes de sostenibilidad de las organizaciones

La Asociación Española de Normalización, UNE, ha celebrado la Jornada: "Impulso a la elaboración de los informes de sostenibilidad", con motivo del Día Mundial de la Normalización, y coincidiendo con la visita a España del secretario general de ISO, Sergio Mujica.

En el evento se presentó el papel clave de los estándares para ayudar a las organizaciones en sus reportes ESG (ambiental, social y de buen gobierno).

El director general de Estrategia Industrial y de la Pequeña y Mediana Empresa, del Ministerio de Industria y Turismo, Jordi García Brustenga, destacó la normalización como factor clave para la competitividad industrial en España.

La Asociación Española de Normalización, UNE, celebró el jueves 17 de octubre la Jornada "Impulso a la elaboración de los informes de sostenibilidad", con motivo del Día Mundial de la Normalización y coincidiendo con la visita a España del secretario general de la Organización Internacional de Normalización (ISO), Sergio Mujica. En el evento se presentó el papel clave de los estándares para ayudar a las organizaciones en sus reportes ESG (ambiental, social y de buen gobierno).

La Jornada contó con la presencia de Sergio Mujica, responsable de la apertura, y del director general de Estrategia Industrial y de la Pequeña y Mediana Empresa, del Ministerio de Industria y Turismo, Jordi García Brustenga, quien clausuró el evento. Ambos estuvieron acompañados por Alfredo Berges, presidente de UNE; Luis Rodulfo, vicepresidente de UNE y miembro del Comité Ejecutivo de CEPYME; y Javier García, director general de UNE y vicepresidente de ISO. La sesión contó la visión empresarial y casos de éxito en la relación entre estándares y organizaciones, como la colaboración entre ISO y CEN y CENELEC con IFRS y EFRAG, respectivamente, para impulsar los informes de sostenibilidad.

CONTINÚA EN PRÓXIMA PÁGINA


E
S
G

Durante su intervención, Sergio Mujica destacó el relevante papel de las normas globales y de ISO para dar respuesta eficaz a los grandes retos del tejido empresarial, como los objetivos ESG (ambiental, social y de buen gobierno) o los ODS, en línea con la Estrategia ISO 2030.

Por su parte, Jordi García Brustenga subrayó que tanto la normalización como UNE son motores de competitividad de la estrategia industrial española y destacó la importancia de la calidad en las políticas públicas.

Las normas españolas UNE, las europeas EN y las internacionales ISO e IEC facilitan a las organizaciones su progreso en los objetivos ESG, a la vez que les permiten mejorar la solidez y fiabilidad de los datos de su reporte.

En la Jornada, se presentó el Informe UNE "Apoyo de las normas para el reporte ESG", cuyo propósito es ayudar a las organizaciones españolas a cumplir con las obligaciones de reporte de la Directiva de información de sostenibilidad corporativa (CSRD) en materia ambiental, social y de buen gobierno, así como a las entidades que han de verificar esta información.

Esta publicación incluye una recopilación representativa de normas existentes en el ámbito ESG, aplicables a todo tipo de organización, con la que se pretende promover su uso como apoyo para este reporte y que las organizaciones presenten información basada en ellas. Estas normas facilitan el diseño de estrategias, la definición de políticas y la toma de decisiones.

En la Jornada, participaron Pablo García, *senior manager* de Forética; Pedro del Pozo, director de Sostenibilidad de UNESPA; María Moreno, directora de Contratación, Técnica e Internacional de SEOPAN; Salvador Marín, miembro del Consejo de Informes sobre Sostenibilidad de EFRAG y director del Servicio de Estudios del Consejo General de Economistas; José Miguel Tudela, director de Sostenibilidad y Acción Climática de ENAGAS; Paloma García, directora de Programas de Normalización y Grupos de Interés de UNE, e Iván Moya, responsable de Transformación Sectorial de UNE.

Todos coincidieron en el papel clave de las normas como herramientas para que las organizaciones avancen en materia de ESG y, además, puedan cumplir las distintas legislaciones relacionadas con la sostenibilidad.

Hace mucho tiempo que hablas.

¿Pero hace cuánto no dialogas?

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

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

UNE Normalización Española

Progreso compartido

une.org

NUEVOS MASTERS

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