REVISTA

Tecnología & Sentido Común

TECNOLOGIA Y ENTIDO COMÚN

#49
FEBRERO
2025

49
9 772951 818003

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

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.

#49

FEBRERO 2025

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

#49- FEBRERO 2025

¡tysc

#TYSC

Premios recibidos

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

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

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

Burocrac_IA

Guia para la eliminación de la Burocracia en la era de la IA

de Victor Almonacid

El libro "Burocrac_IA" es una reflexión contundente y bien fundamentada sobre los desafíos y posibilidades de transformar la administración pública a través de la inteligencia artificial. Víctor Almonacid aborda, con una sabia mezcla de rigor y humor, los aspectos más frustrantes de la burocracia tradicional, que describe como un sistema que, si bien necesario, está plagado de ineficiencias, redundancias y dinámicas anacrónicas.

El autor organiza la obra en dos partes complementarias: primero, un diagnóstico crítico de las malas prácticas administrativas, con ejemplos que resuenan en cualquier lector que haya interactuado con una institución pública. Capítulos como "¡Fotocopia del DNI!" o "Reuniones son desilusiones" exponen de manera irónica pero precisa las trabas que obstaculizan el servicio público, desde reuniones improductivas hasta trámites que parecen diseñados para desmoralizar a los ciudadanos.

En la segunda parte, Almonacid pasa de la crítica a la propuesta, destacando soluciones prácticas que combinan simplificación burocrática y transformación digital. Subraya que la verdadera innovación no está en digitalizar la burocracia tal como la conocemos, sino en reinventarla, usando herramientas como la interoperabilidad de datos y la automatización para agilizar procesos y reducir el desperdicio de tiempo y recursos. En este sentido, los capítulos dedicados a la administración proactiva y a las actuaciones automatizadas son una hoja de ruta clara para construir instituciones más eficientes y centradas en el ciudadano.

El anexo, con 100 recomendaciones específicas para la administración pública, es un recurso valioso, demostrando la capacidad del autor para transformar sus ideas en propuestas concretas y aplicables.

Sin embargo, la obra también lanza una advertencia: la tecnología por sí sola no es suficiente. La inteligencia artificial debe ser guiada por una "inteligencia humana" basada en valores como la equidad, el sentido común y el compromiso público. Este enfoque recuerda al lector que la transformación digital no debe convertirse en una nueva capa de burocracia 3.0, sino en un catalizador para eliminar lo superfluo y optimizar lo necesario.

En resumen, "Burocrac_IA" es una lectura imprescindible para responsables públicos y ciudadanos interesados en mejorar las instituciones desde dentro. Con un lenguaje accesible y ejemplos cotidianos, Victor Almonacid logra hacer que un tema tan denso como la burocracia sea comprensible e inspirador, invitando a todos a imaginar una administración pública más eficiente, ágil y justa.

Javier Peris

Service Manager, jamás deshonres el apellido de la familia.

Saludos cordiales al lector y bienvenido a un febrero que se antoja emocionante. En este artículo, abordaré un tema tremendamente grave que me preocupa enormemente y que suelo detectar con muchísima más frecuencia de lo que me gustaría y de lo que considero admisible por el bien de las organizaciones: la deshonra del apellido.

Tenga por seguro el lector que no me estoy refiriendo a un asunto exclusivo de las empresas familiares. Este problema lo veo con tremenda asiduidad tanto en organizaciones grandes, medianas y pequeñas, incluyendo startups, como en Administraciones públicas de cualquier índole.

Vivimos cada vez más en un mundo "as a Service", donde percibimos aquello que necesitamos como servicio, ya sea movilidad, tecnología, o incluso ocio. En el ámbito de las organizaciones, cada vez más los recursos que se nos ofrecen para el cumplimiento de nuestras tareas o el desarrollo de nuestra actividad se presentan como servicio.

Esta cultura "As-a-Service", aparentemente idílica, suele convertirse en una pesadilla cuando el Service Manager deshonra su apellido, "Manager", y lleva a cabo tareas que no le corresponden, asume responsabilidades que no son suyas, toma propiedad de riesgos que no le pertenecen y toma decisiones para las cuales no tiene autoridad.

El rol de Service Manager es un rol de gestión, y en concreto de Gestión del Servicio, al igual que el Project Manager es un rol de Gestión, en concreto de Gestión del Proyecto. Gestionar comienza por medir; no olvidemos que no se puede mejorar lo que no se puede medir, y esto no es una obligación esporádica o puntual. Debe atenerse a ciclos de vida, procesos, roles y responsabilidades basadas en buenas prácticas y/o estándares aplicados de manera adecuada por el Service Manager.

CONTINÚA EN PRÓXIMA PÁGINA

El resultado se traduce en un catálogo interminable de despropósitos en los que, en mayor o menor medida, el lector va a reconocer haberse visto involucrado, seguramente como damnificado. Quiero desarrollar estos despropósitos para luego establecer cuál es su causa principal o raíz:

1.Plazos lentos: De manera inexplicable o injustificable, lo que debería llevar horas lleva días o incluso semanas.

2.Acumulación de peticiones o incidencias: De manera recurrente, existe en la organización un número elevado de solicitudes sin resolver, lo que mina no solo la satisfacción general del servicio sino la operación adecuada de la organización.

3.Problemas en la calidad del servicio: Se sufren altos niveles de entregas de servicios incorrectas, se reiteran las solicitudes, se acentúan los problemas de calidad y se reiteran todos ellos en cada solicitud o petición, lo que evidencia haber entrado en una dinámica en la que los problemas no solo se producen sino que tampoco se resuelven.

4.Ineficiencia en las operaciones: Falta de prioridades bien definidas y no al libre albedrío, repriorización constante, retrasos, desperdicio de recursos y aumento de costes innecesarios son factores que evidencian también una mala o inadecuada gestión cuya causa radica en la pérdida de foco en el apellido de la familia.

5.Aumento de comentarios negativos: Otra evidencia de mala gestión se manifiesta por el incremento de las quejas de usuarios e incluso de proveedores, así como por el feedback negativo de los clientes, lo que en la mayoría de las ocasiones aparece de manera espontánea y al límite, pues no existe un mecanismo de gestión o control adecuado del propio feedback.

6.Presupuestos hinchados: Un adecuado control y gestión de los costes del servicio tiene como consecuencia que estos sigan aumentando sin una adecuada justificación basada en su aportación de valor a la compañía. Ojo, en situaciones de adecuada gestión los presupuestos pueden crecer, pero siempre lo harán de manera justificada en función del crecimiento empresarial y garantizando una adecuada aportación de valor.

La proliferación del uso de la tecnología en el ámbito de las organizaciones obliga a adoptar una Cultura "As-A-Service" que, paralelamente, obliga al establecimiento del rol del Service Manager a suficiente nivel jerárquico como para poder controlar y gestionar todos los aspectos necesarios para prestar un servicio con la calidad deseada por la organización. Jamás un CIO o un CTO podrá prestar un servicio de calidad sin este rol; sus funciones, tareas y responsabilidades son muy diferentes e intentar unirlas llevaría a caer en el cáncer de la microgestión.

Para que las tecnologías, aplicaciones, nuevos desarrollos e incluso nuevos paradigmas aporten valor a la organización, deben prestarse como servicio y jamás cumplirán su cometido sin la figura del Service Manager establecida adecuadamente a nivel ejecutivo, dotado con los recursos, responsabilidad, atribuciones y mando necesarios para que pueda hacer gala de su apellido y que jamás lo deshonre por omisión o dejación.

Cuando un Service Manager deshonra su apellido, la familia no debería permitirlo.

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

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
FEBRERO 2025

Solicita tu admisión en:

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

Manuel Serrat Olmos

La ciberseguridad de los vehículos conectados (II)

En el artículo de junio de 2023 de Tecnología y Sentido Común, nos planteábamos una serie de cuestiones relacionadas con la ciber(in)seguridad de los vehículos conectados, con especial preocupación con lo que pudiera ocurrir con los vehículos autónomos cuando se generalizasen. Un año y medio después, es momento de revisitar la cuestión y analizar si se ha producido algún "avance" en la materia.

A estas alturas de partido, ya todos nuestros lectores estarán al cabo de la calle sobre la cuestión básica que transmitimos siempre que podemos: ningún sistema es seguro al 100% y es sólo cuestión de que a los ciberdelincuentes les merezca la pena la inversión en recursos y riesgo para que un sistema sea violentado. Partiendo de esa idea-fuerza, ya transmitimos en el artículo de esta revista de junio de 2023 una serie de preocupaciones acerca de a qué riesgos se podían enfrentar los vehículos conectados, y los autónomos en particular.

En este tiempo, hemos visto como la Inteligencia Artificial Generativa aparecía en nuestras vidas, manifestando de forma muy visible los avances en el campo de la IA para el común de los mortales, avances, que por otro lado, son sólo un tipo de uso de estas tecnologías. Ya hacía bastante tiempo que se estaban usando sistemas de IA en otro ámbitos, como el diagnóstico médico, el análisis y mejora de imágenes, o los sistemas de decisión en diferentes ámbitos, como los mercados bursátiles o la conducción autónoma de vehículos. En este último ámbito, los sistemas de IA para vehículos autónomos no sólo se enfrentaban a las necesidades de funcionamiento en tiempo real y a altas necesidades de computación, sino también al necesario estudio de sus algoritmos de decisión en un marco ético, ya que las vidas de personas estaban en juego en dichas decisiones. Por ejemplo, en el caso de que una persona se cruzase inesperadamente frente al vehículo autónomo, y el accidente fuese inevitable, el coche deberá decidir en una fracción de segundo si da un volantazo, con el riesgo de que los viajeros del vehículo sufrieran daños o incluso la muerte, dependiendo de las circunstancias del impacto, o si debía reducir todo lo posible la velocidad antes de impactar con la persona que cruza la vía, como mal menor, resultado del análisis de todas la opciones posibles. Y ese mal menor, ¿dependerá de la edad o el sexo del peatón? ¿Será mejor opción el volantazo si quien cruza sin precaución es una mujer embarazada o con un carrito de bebé? ¿Y si es un anciano o un niño?

Observará el lector que existe un evidente riesgo de sesgo en ese algoritmo, por ejemplo, si un desarrollador racista decide (e implementa) que el vehículo tenga en cuenta la raza del peatón para tomar la decisión. O si un fabricante sin escrúpulos dirige el algoritmo hacia decisiones que provoquen daños al vehículo que le reporten más beneficios en su reparación. De ahí la necesidad de que los algoritmos de la IA deban ser analizados desde un punto de vista ético por entidades externas y, a ser posible, públicas, y que la IA tenga una regulación importante para evitar abusos y desmanes varios.

Además de los riesgos que la IA aporta al vehículo autónomo, como sistema de computación y comunicaciones, el vehículo inteligente, sea autónomo o no, está sujeto a los mismos tipos de amenazas que los sistemas IT (Information Technology) y OT (Operational Technology), y especialmente en este último ámbito, hay riesgos específicos en ataques de Denegación de Servicio o de intercepción/manipulación de las órdenes de navegación.

CONTINÚA EN PRÓXIMA PÁGINA

En este tiempo, se han identificado ataques a los sistemas de GPS de buques mercantes, con el supuesto objetivo de desviarlos de las rutas habituales y facilitar su asalto por piratas en el Océano Índico, por ejemplo. A nadie le apetecerá subirse a su coche autónomo si un malhechor es capaz, de forma remota, de controlar el destino del mismo y llevar a sus ocupantes a una zona en la que dicho malhechor pueda tenerlos a su merced.

Dicho todo esto, como resumen o actualización de los ya advertido en nuestro artículo de junio de 2023, merece la pena destacar que las autoridades competentes están tratando de poner coto a estas amenazas, y no puede ser de otro modo que mediante la oportuna legislación para los fabricantes de coches inteligentes. Y en este ámbito el Instituto Nacional de Ciberseguridad de España (INCIBE) publicó una interesante guía el pasado mes de junio, titulada "Nuevas normativas de 2024 de ciberseguridad para vehículos", y en la que se repasan las iniciativas a este respecto, y cómo afectan a la fabricación de las nuevas generaciones de vehículos.

En el primer párrafo del documento queda meridianamente claro su objetivo: "*El objetivo de esta guía es proporcionar información que ayude a entender la nueva regulación emitida por el Foro mundial para la armonización de la reglamentación sobre vehículos (WP.29), un cuerpo de la Comisión Económica de las Naciones Unidas para Europa (UNECE), referida a la ciberseguridad en vehículos, así como la presentación de consejos que ayuden a su cumplimiento*".

No es un documento normativo, si no informativo, que ayude a facilitar a los fabricantes el entendimiento sobre el proceso de homologación requerido para la fabricación y comercialización de vehículos en Europa. En concreto, respecto de los reglamentos UN R155, que *"concierne a los requisitos para la gestión de la ciberseguridad*" en los vehículos, y UN R156, que "*estipula los requisitos para la gestión de actualizaciones de software*". Ambos reglamentos entraron en vigor en julio de 2024, y por tanto, en la actualidad deberían estar siendo aplicados por los fabricantes de vehículos que se tengan que comercializar en Europa.

Para las personas que estamos habituadas al manejo de la nomenclatura del ámbito de la ciberseguridad, es muy curioso y satisfactorio ver muchos de esos conceptos en una normativa dirigida a fabricantes de vehículos. Por ejemplo, respecto de UN R155, la guía de INCIBE indica que "*El objetivo principal de la regulación R155 es definir los requisitos a cumplir por el vehículo y el fabricante para considerar que presenta un nivel de ciberseguridad adecuado frente a las amenazas de ciberseguridad recogidas en el anexo 5 de la homologación", y un poco más adelante, que "Estos requisitos se centran en el sistema de gestión de la ciberseguridad del vehículo (SGSI), es decir, cómo se organiza y ejecuta la ciberseguridad, no sólo a nivel del vehículo y sus sistemas, también incluye en su alcance la ciberseguridad en los servidores del fabricante, su proceso de diseño y fabricación, sus capacidades para mantenimiento, monitorización y vigilancia, la gestión de vulnerabilidades y la gestión de la cadena de suministros*".

Es decir, se trata el vehículo como un sistema tecnológico de tipo industrial, y como a éstos, se le han de aplicar medidas de seguridad apropiadas a su función. Realmente, merece la pena la lectura de la guía de INCIBE, donde se resumen las 24 medidas a tener en cuenta en el SGSI del fabricante para lograr la homologación, y donde se hace mucho hincapié en la necesaria protección de todos los componentes de la cadena de suministro, aspecto en el que hemos incidido en varias ocasiones en esta revista.

Por lo que respecta a la UN R156, la guía también resume los requisitos que ha de evidenciar el fabricante para mantener actualizado correctamente el software de los vehículos, de forma que éste no se convierta en una fuente de vulnerabilidad del sistema, dado que de él puede depender la vida de los ocupantes del vehículo o de las personas que están alrededor del mismo.

En fin, estamos ante un ámbito en el que los profesionales de la ciberseguridad tienen mucho trabajo por hacer, y con unas peculiaridades que lo convierten en un campo muy interesante. ¿Cuánto tardaremos en conocer algún caso de incidente real con estos vehículos? ¿Estaremos razonablemente seguros en su interior? Veremos….

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

Gov Book

Governance Body of Knowledge

P4MGO!®

P4MGO!

PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Nacho Alamillo

Representación de instrumentos financieros mediante tecnología de registros distribuidos

La Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión, incorporó las reglas necesarias para garantizar la seguridad jurídica en la representación de valores negociables mediante sistemas basados en tecnología de registro distribuido, para permitir la aplicación en España del Reglamento (UE) n.º 2022/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro distribuido y por el que se modifican los Reglamentos (UE) n.º 600/2014 y (UE) n.º 909/2014 y la Directiva 2014/65/UE, en cumplimiento al mandato a los Estados miembros establecido en el artículo 18.2 de dicho Reglamento.

En este sentido, el epígrafe 1 del artículo 6 autorizó la representación de valores negociables por medio de anotaciones en cuenta, títulos o sistemas basados en tecnología de registros distribuidos, ordenándose en el epífrage 5 del propio artículo que, en los casos en que la entidad emisora elija sistemas basados en tecnología de registros distribuidos como forma de representación de los valores negociables, estos sistemas deberán garantizar la integridad e inmutabilidad de las emisiones que en ellos se realicen, identificar de forma directa e indirecta a los titulares de los derechos sobre los valores negociables y determinar la naturaleza, características y número de los mismos, así como que los titulares de los derechos sobre los valores negociables representados mediante sistemas basados en tecnología de registros distribuidos tendrán acceso a la información correspondiente a los mismos, así como a las operaciones sobre los valores por estos realizados.

La entidad emisora deberá disponer de un documento en el que constará la información necesaria para la identificación de la entidad responsable de la administración de la inscripción y registro, así como de los valores negociables integrados en la emisión (artículo 7.1 de la Ley 6/2023), que deberá estar en todo momento a disposición de los titulares y del público interesado en general (artículo 7.3) y que contendrá información suficiente sobre los sistemas en los que se registren los valores, incluyendo entre otros los aspectos principales sobre su funcionamiento y gobierno.

CONTINÚA EN PRÓXIMA PÁGINA

Por su parte, conforme al artículo 8.4 de la citada Ley, la llevanza del registro de valores negociables representados mediante sistemas basados en tecnología de registros distribuidos se llevará a cabo en la forma prevista en el documento de la emisión al que se refiere el artículo 7, debiendo el emisor designar a una o varias entidades que serán responsables de la administración de la inscripción y registro de los valores en el sistema (pudiendo ser el propio emisor o una o varias entidades designadas por este, debidamente autorizadas para la custodia y administración por cuenta de clientes de los instrumentos financieros, incluidos la custodia y servicios conexos como la gestión de tesorería y de garantías y excluido el mantenimiento de cuentas de valores en el nivel más alto). Y añade que, entre otras funciones, estas entidades llevarán la gestión de la identificación de los titulares de los derechos derivados de los valores negociables, así como de los distintos eventos corporativos, inscripciones o gravámenes que afecten a la emisión.

En este contexto, recientemente el Gobierno español ha evacuado el trámite de información pública de la norma reglamentaria propuesta para desarrollar el régimen jurídico de la representación de instrumentos financieros mediante tecnología de registros distribuidos, concretando del régimen jurídico de las entidades responsables de la administración de la inscripción y registro de las emisiones de instrumentos financieros mediante tecnología de registros distribuidos (ERIR).

Además, la propuesta de Real decreto profundiza en el régimen jurídico aplicable a la representación de instrumentos financieros mediante tecnología de registros distribuidos, clarificando elementos fundamentales como el cambio de representación, los documentos informativos, o la práctica de la inscripción en el registro. La forma de transmisión, la característica de fungibilidad o la legitimación registral son otros elementos desarrollados en este capítulo, y finalmente, referencia el régimen jurídico de las ERIR, sus funciones, sus obligaciones o su sustitución o renuncia.

Nótese que las tecnologías de registro distribuido, como las cadenas de bloques, han sido objeto de regulación por el Reglamento (UE) 2024/1182 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital, conocido como Reglamento eIDAS 2, al que me he referido en diversas ocasiones, mediante el nuevo servicio de confianza de libro mayor electrónico, que puede resultar de extraordinaria conveniencia a las entidades responsables de la administración y registro de los valores negociables en el libro mayor electrónico, que en este caso será distribuido.

Dado el rol de la ERIR, asumido por el operador de la infraestructura de mercado que lleve a cabo la liquidación de las operaciones sobre los instrumentos financieros conforme al Reglamento del Régimen Piloto, resulta especialmente conveniente, en términos de responsabilidad, hacer uso de libros mayores electrónicos distribuidos cualificados. Una posibilidad extremadamente interesante, a explorar en el futuro, sin duda alguna.

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 & DLT

ISO 23635 Blockchain & DLT Governance Leader

Docente:
Nacho Alamillo

Coordinación Académica
Javier Peris

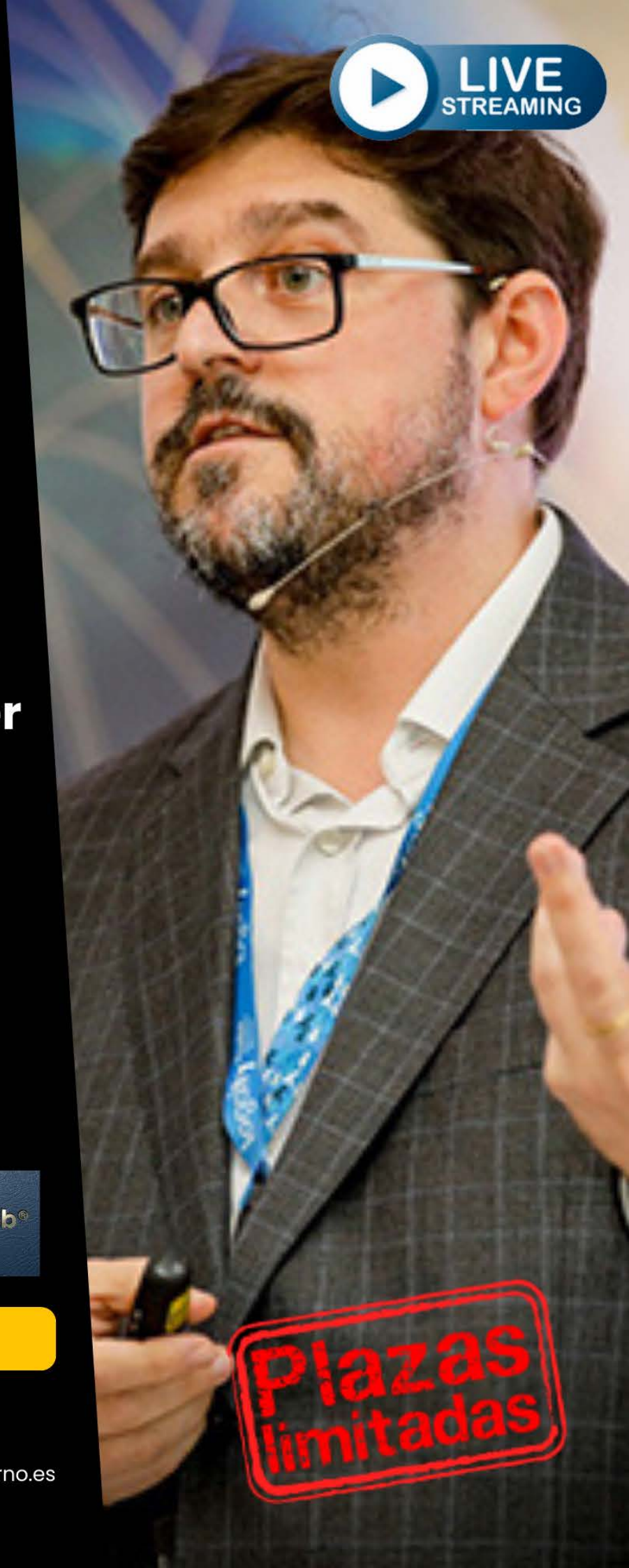
- Formato: Directo en Remoto
- Duración: 20 horas
- Sesiones: Martes y Jueves
- Martes: De 16:00 a 21:00 horas
- Jueves: De 16:00 a 21:00 horas
- Examen de Certificación: Incluido
- Aforo: Limitado 15 Alumnos
- Acceso: Solicitud de admisión

MidMgmt® MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
JUNIO 2025

Solicita tu admisión en:

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



Juan Carlos Muria

Europa y la ciberseguridad de hospitales: protegiendo vidas y datos.

La Comisión Europea ha publicado en 2025 un plan de acción para proteger el sector salud a nivel europeo. Según la rueda de prensa de presentación del plan, en 2023 se registraron 309 incidentes significativos de ciberseguridad en el sector sanitario. Esta cifra es superior a la de cualquier otro sector crítico, según indicaron también. El reto de proteger al sector sanitario de ciberataques es pues importante, especialmente si consideramos que pronto se pondrá en marcha el Espacio Europeo de Datos de Salud.

En dicho plan se recopilan iniciativas que ya venían tiempo planteándose y que parece que ahora al fin se van a hacer realidad, como el apoyo de la Unión Europea a sus socios a través de un Centro de Ciberseguridad para Hospitales y otros Proveedores Sanitarios de la mano de ENISA, la Agencia de Ciberseguridad de la Unión Europea, o las iniciativas de formación y concienciación para profesionales sanitarios. También se va a activar un servicio de alerta temprana a nivel europeo y un catálogo de vulnerabilidades conocidas en dispositivos médicos.

Otra de las iniciativas a tener en cuenta es un servicio de respuesta rápida a incidentes, específico para el sector salud, que complementará a los servicios nacionales existentes en incidentes a gran escala.

Hemos de tener en cuenta que el sector de la salud, especialmente en el caso de los hospitales, tiene diferencias significativas en comparación con otros sectores: tiene un horario de 24x7x365 en muchos casos, maneja una información altamente sensible y persistente (como siempre digo, uno no puede cambiar de enfermedad aunque se haga público que la padece, a diferencia del número de tarjeta de crédito o la contraseña de un servicio), y tiene una superficie de ataque enorme, debido sobre todo a la conexión de equipamiento médico raramente actualizado a la misma red que las aplicaciones que manejan la información clínica de los pacientes, y a que estas mismas aplicaciones tienen un ciclo de vida extraordinariamente largo y un soporte normalmente escaso.

CONTINÚA EN PRÓXIMA PÁGINA

> El reto de proteger al sector sanitario de ciberataques es importante, y más si consideramos que pronto se pondrá en marcha el Espacio Europeo de Datos de Salud

Es de esperar que iniciativas como el catálogo de vulnerabilidades conocidas, los requisitos de ciberseguridad para dispositivos médicos que exige la certificación europea MDR (Medical Device Regulation), las directrices para la adquisición de equipamiento médico, y el diálogo con los fabricantes pueda mejorar esta situación.

El plan busca en resumen fortalecer la ciberseguridad del sector salud aumentando su madurez en ciberseguridad, fortaleciendo las cadenas de suministro, y ofreciendo los servicios mencionados anteriormente de alerta y respuesta rápida.

Sin embargo, como suele pasar en estos casos, se pide también el compromiso de cada uno de los Estados miembros, como el establecimiento de centros de apoyo de ciberseguridad nacionales específicos para hospitales y otros proveedores sanitarios, planes de actuación nacionales con el foco en el sector de la salud, y el análisis y la compartición de información sobre los incidentes a través, por ejemplo, de centros de análisis y compartición de información (ISACs). También se les pide la realización de ejercicios de ciberseguridad nacional para probar sus protocolos de respuesta y reforzarlos si fuera necesario, entre otras cosas. Para esto también se plantea que existan presupuestos finalistas que no se detraigan de los presupuestos para la atención sanitaria.

Por otro lado, la visión europea del plan, con sistemas sanitarios a menudo centrados en hospitales y pequeñas clínicas, hace que en ningún momento se mencione a la Atención Primaria (bueno, solo una vez: para explicar que el 79% de ciudadanos de la UE tiene acceso a su historia clínica electrónica de Primaria), aunque sí habla de pequeños centros de atención sanitaria. Es cierto que la superficie de ataque en un centro de Atención Primaria es menor en términos de variedad y número de puestos de trabajo en relación con un hospital, pero el impacto de un ciberataque sobre sistemas de información centralizados de Atención Primaria sería notorio y podría interrumpir servicios esenciales o provocar la pérdida de confianza de los ciudadanos, además de colapsar los hospitales de manera indirecta, así que esperemos que los Estados miembros con un sistema de Atención Primaria semejante al español tomen nota y presten atención también a este nivel asistencial en términos de ciberseguridad.

Tampoco tiene en especial consideración actividades de concienciación a los pacientes, algo que tendrá que acompañar estas iniciativas, porque los atacantes siempre van a ir al eslabón más débil, y prefiero no desgranar aquí el interés y las posibles maneras en que pueden hacerlo.

En definitiva, para que este plan realmente tenga éxito hace falta un compromiso mutuo como es habitual entre la Unión Europea y sus Estados miembros, y presupuesto para financiarlo, algo que tradicionalmente ha sido escaso ya que había que decidir entre el gasto de farmacia, de hospitalización y de bloque quirúrgico y el gasto en medidas de ciberseguridad, algo que se busca evitar con este plan.

Ojalá tenga un resultado muy positivo este conjunto de iniciativas, y que tanto ustedes, lectores, como este mismo que escribe, y la tortuga ninja, podamos disfrutar por muchos años de la confianza en nuestro sistema sanitario.

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

PfM Book

Portfolio Management Body of Knowledge

P4MGO!®

P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Angie Lopez Gea

¿Quién es Angie Lopez Gea?

Creo que sin duda esa es siempre la pregunta más complicada y difícil de responder. Una persona es siempre "uno y sus circunstancias" y a largo del tiempo siempre se cambia. Asi que, como hacerlo con unas palabras que definan la esencia, complicado pero bueno, me encantan los retos. Y eso, es precisamente lo que me define, alguien que va buscando el siguiente reto para encontrar la mejor versión de lo que puedo llegar a ser.
Desde que tengo uso de razón siempre he sido alguien muy analítica, buscando los pros y contras de cualquier situación a la que me he encontrado y teniendo el aliciente de conseguir cosas que van contra pronóstico o simplemente parecen muy complicadas o difíciles de conseguir. Y aunque la vida me ha enseñado que no todas las batallas merecen ser luchadas ni hago alusión a imposibles, siempre me ha encantado conseguir cosas que nadie hubiese podido o simplemente ni se ha intentado.

¿Háblanos de tus éxitos o logros profesionales?
La verdad que cada paso que he dado para mi es un logro personal, pero si cierro en el ámbito profesional, el primero sin duda sería hace la carrera de ingeniería informática. Dando un poco de contexto, cuando era pequeña, la gente particular no podía tener un ordenador, no era como ahora, era solo para algunos privilegiados, no existían móviles y aunque parezco joven he nacido en los 80. Tuve la gran suerte de tener un ordenador en casa desde los cinco años y desde ese día dije que quería estudiar eso, sin más. Asi que cuando llegué a la universidad no había cambiado de opinión y seguí mi camino. Para mí, mi mayor logro profesional es ese, siempre he tenido claro mi foco profesionalmente y lo he seguido.
Luego por supuesto, han venido muchos tantos, he ampliando el foco, hice un par de máster lo que me permitió especializarme, trabajé para una empresa en Malta reconocida internacionalmente en el sector del juego online, de la cual tengo muchas experiencias y anécdotas; llegué a ser la CIO de una organización en alimentación que hace productos para el ejército americano, la cual me enseñó mucho sobre negocios en el ámbito de las TI.
Durante todo mi recorrido profesional, siempre me he encontrado incertidumbre en ciertas áreas de conocimiento, por lo que lo he suplido con certificaciones y estudiando, que sigo a día de hoy.

CONTINÚA EN PRÓXIMA PÁGINA

> **Los servicios son el tejido que une a nuestra sociedad, facilitando la colaboración, el bienestar y el progreso en cada rincón de nuestras vidas**

Nuestra invitada #TYSC

Háblanos de tu experiencia profesional en seguridad y/o ciberseguridad
Tras varios años como responsable de TI y después de un máster en ciberseguridad sentí que era "lo mío" y decidí cambiar y centrarme solo a ciberseguridad. Aunque tengo mucha base técnica y además me gusta esa parte, decidí cambiar mi estresante vida como CIO, llevando de todo en mi cabeza y comenzar como Consultora Senior de Ciberseguridad en el área de GRC.

¿Qué he ganado con ello? Mucho, había que empezar desde un escalón más abajo para poder tener experiencia y mejorar mi conocimiento en esa área. Esto me ha aportado el poder conocer muchas organizaciones privadas y entidades públicas de diferentes sectores, pudiendo ver sus sistemas y buscando como aportarles valor en su negocio. Actualmente lidero el área de GRC dentro de una consultora que está muy ligada a organismos públicos, lo que me permite entender los sistemas de la administración pública.

El área de GRC es un poco la olvidada dentro de ciberseguridad, pero a mi sin duda, me parece la más interesante. No solo por el tema legal, sino por el de gobierno y riesgos. Al final poner el foco en los riesgos que tiene la organización y conseguir que la capa de gobierno se implique son componentes que hacen que la ciberseguridad funcione.

Dentro de esta área he podido analizar sistemas ferroviarios desde el punto de continuidad de negocio, sistemas de banca analizando sus transacciones en bolsa, sistemas de otro país extranjero, viendo sus conexiones con el resto de sistemas públicos de dicho país, sistemas de otras consultoras en materia de seguridad e incluso sistemas clasificados como secreto.

¿Como fueron tus comienzos en el mundo de la Gestión?
Estaba como técnico informático y se fue el responsable, asi que decidieron darme la oportunidad de ser la responsable del departamento de informática. Casualmente, era la última en llegar al departamento, la más joven y la única mujer. No sé cual de los componentes tuvo que ver, pero no fue fácil. Allí estaba yo, delante de un departamento al que gestionar dentro de una organización que lo único que le interesaba era que entrase dinero.

CONTINÚA EN PRÓXIMA PÁGINA

Nuestra invitada a #TYSC

El comienzo fue adaptarme a mi nuevo rol, el tener que transformar las decisiones de dirección en acciones viables dentro del departamento haciéndoles sentir útiles. Reconozco que cuando te enfrentas a la parte de gestión, te vuelves más humano, porque eres el traductor entre el negocio y sus empleados y también mas paciente, antes solo buscaba resultados a corto plazo, desde entonces aprendí a tomar decisiones de fondo.

¿Cuáles crees que son los factores a corregir o mejorar respecto de la Cultura as a Service en Seguridad y Ciberseguridad por parte de las organizaciones?
Creo que siempre me he encontrado con los mismos impedimentos, falta de patrocinio, la seguridad como un gasto, falta de tiempo de las organizaciones para la seguridad, poco valor…
Todo esto creo que debe ser un ejercicio tanto del personal de seguridad de la organización como de la alta dirección. Muchas veces no hay entendimiento entre ellos, unos hablan de negocio y los otros de su día a día y se les olvida esa capa de gestión, que une ambas partes y hace que la comunicación fluya. Asique como mejora, poner una persona/departamento que impulse la seguridad y permitirle hacer de la seguridad un proceso trasversal más de la organización, analizando su retorno de inversión.

¿Como según tú aportan valor los Servicios a las organizaciones?
Sin servicios, desde luego no hay sinergias y es complicado que una organización funcione de forma eficiente. El cometido de un servicio es ese, "servir", es complicado que una organización sea autosuficiente en todos sus aspectos y además que lo sea de forma óptima. Por ello muchas veces es mejor contratar un servicio que hacerlo uno mismo, incluso aunque se puede hacer, porque a veces es mejor contar con un profesional con años de experiencia en diferentes materias, que te puede aportar lo mismo que ibas a realizar, pero en menor tiempo y con más calidad.

¿Qué áreas de mejora te parecen más importantes o relevantes en Gestión de la Seguridad y/o Ciberseguridad?
Sin duda el área donde me encuentro, Gobierno, Riesgo y Cumplimiento. La ciberseguridad debe ser vista por el gobierno, desde tener un patrocinio y debe ser un proceso integral de la organización, además se debe ser en base a los riesgos que tiene la organización, incluyendo el cumplimiento legal como otro riesgo más. Sin está área, poner firewalls, parches y hacer hacking está muy bien, pero hace falta recursos, motivación y compromiso por todos lo implicados y eso recae sobre nuestra área.

Volviendo a ti ¿De qué te sientes más orgullosa en tu carrera profesional?
De que mi nombre suene y suene para bien. Nada me hace mas sentir orgullosa que alguien me comenté que ha hablado con otra persona y le haya dicho "pues la conozco, nos llevó tal servicio y conseguimos buenos resultados". Al final el ser un referente positivo en lo que hago y tener una imagen de marca dentro de ciberseguridad, es y será de lo que más orgullosa de siento profesionalmente. Esto hace que quiera seguir mejorando y aportando más valor a las empresas.

¿Qué consejos le darías a los directivos que no conocen las ventajas de una adecuada Gestión de Servicios?
La Gestión de Servicios no es solo una función operativa, sino una estrategia integral que puede transformar la manera en que una organización opera y se relaciona con sus clientes.
Gestionar servicios es un proceso de planificar, organizar y supervisar la entrega de servicios para asegurarse de que se cumplan las expectativas de los clientes y se alcancen los objetivos de la organización que es todo lo que se hace para que un servicio funcione de la mejor manera posible.
La gestión, para mí, es la columna vertebral de un servicio, que une la toma de decisiones de la cabeza con la parte ejecutora de las extremidades. He visto grandes servicios, con buenas ideas, abocados al fracaso pese a una gran dirección y un equipo humano excepcional porque la parte de gestión fue descuidada y lo que podía ser un beneficio acabó siendo un servicio cerrado a perdidas, malestar entre los empleados y clientes descontentos.
Como consejo, que pongan el foco en la gestión, tener una buena gestión puede mejorar la experiencia del cliente, optimizar procesos, reducir costes, mejorar la eficiencia, evolucionar los servicios o crear unos nuevos, evaluar el rendimiento, ayudar al cambio y promover la colaboración entre departamentos, lo que hace una cultura organizacional.

CONTINÚA EN PRÓXIMA PÁGINA

¿Qué les dirías a las profesionales que aún no son miembros del Service Management Institute?
Sin duda le diría que unirse a nuestra asociación es una excelente oportunidad para crecer y desarrollarse en el campo de la dirección de servicios. Ser parte del Service Management Institute es poder compartir espacio y momento con grandes profesionales de diferentes sectores, lo que ofrece una red de contactos de gran valor además de poder disfrutar de ventajas como la formación y eventos.

Estas sinergias me han permitido aprender de las mejores prácticas y mantenerme al día con las tendencias del sector en cuanto a servicios, algo que mejora mi visión en mi día a día en ciberseguridad y me permite ayudar a la organización que pertenezco en cuanto estrategia y visión.

Además, ser parte de esta una comunidad significa tener la oportunidad de contribuir a la evolución de la dirección de servicios, algo que me hace no solo crecer profesionalmente sino personalmente.

Que representa para ti ostentar la Certificación SMP
Es un gran honor, ¿a quien no le gusta que le reconozcan méritos? Es sabido que me encanta certificarme de cualquier certificación de diferentes ámbitos que aporte valor, que me haga adquirir nuevos conocimientos y me suponga un reto intelectual. En el caso del SMP, yo la adquirí mediante el proceso de Grandfathering, el cual significa que tienes que demostrar ciertos conocimientos y experiencia en la dirección de servicios, ser miembro de la asociación y enviar una solicitud que se ha de aprobar por el comité evaluador. Cuando me dijeron que estaba aprobada, fue la misma sensación que cuando acabas una carrera de fondo y llegas a la meta, muy satisfactoria. Además, durante los eventos del SMI he podido relacionarme y conectar con personas que durante tiempo he seguido sus carreras profesionalmente y hemos podido hablar de tú a tú, teniendo esa gran oportunidad gracias a que la certificación nos ha unido.

¿Como sería el futuro de una sociedad sin servicios?
Imaginar una sociedad sin servicios es un ejercicio interesante y, a la vez, un poco inquietante. Los servicios son fundamentales para el funcionamiento de nuestra sociedad, ya que facilitan la vida cotidiana y permiten que las comunidades evolucionen. Sin ellos, desde luego existen grandes retos.

No tener servicios básicos como la atención médica, la educación, el transporte y la seguridad podría implicar al individuo depender completamente de sus propios recursos y habilidades, lo que aumentaría la desigualdad y la vulnerabilidad en la sociedad. Además, muchas industrias no podrían operar de manera efectiva, lo que se traduce en poca productividad y bajo empleo.

Desde mi punto de vista profesional en ciberseguridad y tecnologías de la información, la innovación sería complicada, ya que los servicios son a menudo el motor que impulsa el desarrollo de nuevas ideas y tecnologías.

En resumen, un futuro sin servicios podría ser un lugar más difícil y menos cohesionado, donde la vida cotidiana se volvería más complicada y las oportunidades de crecimiento personal y profesional se verían limitadas. Los servicios son, sin duda, una parte esencial de lo que hace que nuestra sociedad funcione de manera efectiva y armoniosa.

Algún mensaje, conclusiones o Despedida.
“Los servicios son el tejido que une a nuestra sociedad, facilitando la colaboración, el bienestar y el progreso en cada rincón de nuestras vidas”.

PgM Book

Programme Management Body of Knowledge

P4MGO!®

P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Marlon Molina

Debatir la libertad de expresión en las redes sociales es tendencia

Elon Musk abrió el debate en el año 2021, el mayor hito ocurrió el 8 de enero de ese año cuando Twitter decidió bloquear de forma permanente la cuenta de Donald Trump, usando así su poder para la censura. Como bien sabemos, Musk inició su campaña para comprar la red social con un lema principal "la libertad de expresión, que cada persona se exprese en libertad".

Independientemente de si está consiguiendo el objetivo o no, el caso es que el debate de la libertad de expresión se trasladó a las redes sociales, y en particular a Twitter, en vez de debatirse en los parlamentos y en los foros de la ciudadanía.

Twitter ya rebautizado como X, lanzó Grok en 2023, un chatbot de Inteligencia Artificial Generativa, al estilo de ChatGPT, Gemini, y Perplexity. A finales de 2024 dejó abierta la puerta a todos los usuarios de X sin ningún tipo de restricción para acceder a la herramienta y pedir básicamente cualquier tipo de imagen, siendo la única restricción la generación de imágenes de tipo sexual.

Grok ganó (o ahorró) millones en publicidad creando imágenes realistas de personajes famosos en las condiciones que el usuario quisiera. En España fueron populares algunos memes que cerraron el año 2024 en los que era posible ver besándose a Pedro Sánchez y a Alberto Núñez Feijó, supuestos contrincantes políticos. Las imágenes con un gran realismo las puede pedir cualquier usuario de la red.

Desde la perspectiva del líder de X, pedir las imágenes es parte de la libertad de expresión, y la difusión podría serlo siempre que no se use para ofender. Una posición bastante extremista.

CONTINÚA EN PRÓXIMA PÁGINA

Mark Zuckerberg copia a Elon Musk
El martes 7 de enero de este año, Mark Zuckerberg se desdijo a sí mismo, o dicho de otra manera, cambió de opinión respecto del control de las noticias falsas y la libertad de expresión de los usuarios de los productos de Meta entre los que están Instagram y Facebook.

Zuckerberg no solo copió el enfoque de Musk, copió el discurso completo. El líder de Meta ha explicado que una vez que elimine la validación de contenidos y las restricciones de los algoritmos, la libertad de expresión se beneficiará en las redes sociales. El mismo discurso de Elon Musk.

"Hola a todos. Hoy quiero hablar de algo importante, porque es hora de volver a nuestras raíces en torno a la libertad de expresión en Facebook e Instagram", fueron las palabras exactas de Mark Zuckerberg, quien posteriormente ha aclarado que los gobiernos de Obama y Biden le presionaron para filtrar los mensajes en las redes y controlar el contenido.

El péndulo en el extremo
¿Abierto? ¿filtrado? ¿cerrado?
La influencia de las redes sociales ha sobrepasado por mucho a los medios de comunicación. El fenómeno está en tal extremo que la prensa misma contribuye a la creación de contenido en las redes, y los usuarios se fían más de lo que leen en X que lo que se publica en un periódico digital. En el otro lado de la mesa, es común ver a los telediarios publicando y comentando publicaciones de X para presentar las noticias, atrás quedaron los días en los que una periodista enviada a la zona cero de la noticia narra los hechos.

El péndulo se mueve al extremo. Desde luego es un tema difícil y quizá imposible de resolver en la era en la que vivimos. Lo cierto es que al levantar el filtro (sea lo que sea que filtre) queda del lado del usuario el 100% de la responsabilidad.
Esta situación trae a la mesa un segundo asunto: el usuario. En todo momento se habla de los usuarios, pero la realidad es otra, en las redes sociales lo que hay son perfiles, y muchos usuarios tienen perfiles "anónimos" que usan para abusar de la libertad.

Ciberseguridad
El 9 de enero se publicaron desde Venezuela imágenes falsas de las protestas de la población. Los medios no sabían qué filtrar, el gobierno publicó bulos, pero también lo hicieron otros usuarios para acusar al gobierno.
Las noticias falsas tomaron sus posiciones, en la izquierda, en la derecha, y de lado. En un telediario español los presentadores que daban cobertura a la protesta leían mensajes en X y advertían al mismo tiempo a los espectadores que era información no verificada.
Al mismo tiempo, el 9 de enero, llegaban a Los Ángeles las llamas de uno de los peores incendios de la historia de California. Personas sin validar sus almas publicaron vídeos e imágenes falsos, tratando de ganar posición y popularidad en X. también había imágenes reales, pero parecía increíble que alguien quiera falsificar este tipo de contenido.
Como resultado la ciudadanía empieza a entender una de las mejores reglas para mejorar la posición en la ciberseguridad: Todo es falso. Esta podría ser una ventaja para la ciberseguridad, y un beneficio para todos al enviar el péndulo al extremo de la libertad de expresión.

MARLON MOLINA

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

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

PjM Book

Project Management Body of Knowledge

P4MGO!®

P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Ricard Martínez Martínez

Netaholics ¿Hacía donde nos lleva la dependencia de las redes sociales?

En los últimos tiempos varias compañías dedicadas a las redes sociales han sido objeto de investigación o demanda en Estados Unidos y la Unión Europea con motivo de prácticas lesivas para los derechos de los menores o de sus usuarios. En un interesante y extenso artículo en el que Michal Lavi sustenta la exigibilidad de responsabilidad civil describe cómo funciona el uso de algoritmos en este contexto.

Como es sabido se ofrece contenido personalizado a partir del seguimiento integral de todas las acciones de los usuarios y su comportamiento. Además, los sistemas de recomendación personalizada gestionada por algoritmos pueden llevar a que los usuarios queden atrapados en "burbujas" donde solo están expuestos a información que refuerza sus puntos de vista existentes, a menudo repitiendo ideas y buscando generar conflicto. Al personalizar el contenido, las compañías crean un contexto donde los usuarios son más susceptibles de ser influenciados. Esto incluye el uso de técnicas como la repetición de mensajes y la manipulación de la dinámica social

Se recopila información sobre el estado de ánimo y las emociones de los usuarios para dirigirlos con mayor precisión explotando sus emociones. Mediante el "*framing*" (encuadre) se influye en la dinámica social en las redes y se puede alterar la percepción de la realidad y empujar a los usuarios a consumir contenido o adoptar comportamientos específicos. Ciertos algoritmos opacos pueden influir en el pensamiento intuitivo, emocional e instintivo, evitando así el modo de pensamiento deliberativo. Esto significa que pueden manipular las reacciones emocionales de los usuarios sin que estos sean plenamente conscientes de ello.

En este sentido, los modelos de manipulación se basan en la explotación de sesgos, heurísticas, y limitaciones cognitivas de los individuos. Esto permite personalizar la manipulación a un nivel individual, más allá de las limitaciones colectivas.

En el metaverso, se espera que la tecnología permita monitorear las respuestas psicológicas y los datos biométricos de los usuarios, como las expresiones faciales, lo que proporcionaría nuevas oportunidades para la manipulación. Desde un punto de vista del riesgo, debemos entender que estas técnicas pueden influir en la toma de decisiones de los usuarios, a menudo a través de sistemas de recomendación personalizados. Esto incluye empujar a los individuos a pensar de manera diferente a como lo harían de otra manera.

Por otra parte, en el caso de los menores se ha demandado civilmente a redes sociales en EE.UU. al considerar que existe un diseño intencional para atraer, implicar y, en última instancia, atrapar a jóvenes y adolescentes. La cuestión es que para conseguir este objetivo se pueden causar daños en la salud mental al promover un uso compulsivo y prolongado de la plataforma. Existiría un diseño intencional orientado a estimular los mecanismos cerebrales de recompensa. En este sentido la generación de dopamina que producen los likes seguiría los mismos circuitos que producen adicción a las drogas o el juego.

CONTINÚA EN PRÓXIMA PÁGINA

La dependencia se vería acrecentada al favorecer una suerte de scrolling infinito en los que los contenidos nunca acaban y siempre hay que seguir. Por otra parte, la estructura visual y lumínica de la pantalla estimularía la vigilia afectando a los ciclos del sueño. Finalmente, las herramientas para la generación de contenidos favorecerían la dismorfia en la concepción del propio cuerpo con resultados previsibles en términos de trastornos alimentarios.

De ser ciertas las afirmaciones anteriores, y debo decir que en las aulas estos efectos se perciben a simple vista, enfrentamos un contexto social de dependencia de redes sociales generalistas, escasamente productivas, altamente adictivas e intensivas en tiempo y cuyo algoritmo podría promocionar discursos de odio, debates polarizadores y el negacionismo de la ciencia. Poco importaría entonces su contribución al tejido productivo y las ventas publicitarias de sus clientes ya que podrían erigirse en heraldos de los cuatro jinetes.

El impacto desde hace tres lustros en las futuras generaciones de profesionales puede ser demoledor. Los procesos de aprendizaje tradicionales se han visto profundamente afectados. Algunos de nuestros jóvenes presentarán trastornos de atención. Otros se verán afectados por la constante interrupción de sus tareas debido a la ansiedad de consultar la pantalla. Este proceso altera las mecánicas de trabajo que consolidan mediante la repetición y la concentración la memoria a largo plazo. Por otra parte, altera el ritmo de las tareas impidiendo una adecuada ejecución en el periodo planificado.

Pero no se trata de una cuestión de futuro sino también de presente. Toda la población consume masivamente redes sociales generalistas. Y ello puede tener profundas implicaciones empresariales. La primera y la más obvia tiene que ver con el rendimiento laboral. Pero no es la única. No hace falta ni ser psicólogo, ni ser un lince para entender que la prohibición de uso del teléfono móvil privado debería incorporarse a la prevención de riesgos laborales en muchos oficios en los que un pequeño despiste puede conducirnos a un accidente mortal.

Por último, existe un riesgo sistémico para la democracia y se apunta que incluso geopolítico. De una parte, la capacidad de manipulación emocional puede ser utilizada para desestabilizar países enteros o para atacar a sus sectores críticos. De otra, el rastro de “miguitas” que van dejando nuestros colaboradores puede hacerlos vulnerables

e incluso poner en riesgo de manera inadvertida secretos empresariales. Además, el ataque del problema presenta serios problemas políticos ya que la población no será capaz de entender o admitir medidas contundentes porque ahora su bar, su salón de reuniones y su patio de recreo está en una red social que les engancha como cualquier otra dependencia.

La Unión Europea se ha provisto de herramientas normativas generales que completan el RGPD con prohibiciones de desarrollo de algoritmos de manipulación en el Reglamento de Inteligencia Artificial y limites a los grandes operadores en el Reglamento de Servicios Digitales. España y la UE estudian el desarrollo adicional de normas de protección de los menores. No es suficiente, desde la educación en valores el conjunto de la sociedad debería comprometerse en la gestión de los riesgos que provocan entornos aparentemente dedicados al ocio y la socialización que, sin embargo, en las manos adecuadas nos hacen altamente vulnerables y podrían amenazar nuestra democracia y nuestra economía.

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 responsa- ble 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
MARZO 2025

Solicita tu admisión en:

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

Marcos Navarro

AI-ngeniería 2034: El Futuro de la Construcción ya está aquí

En 2034, la ingeniería y la construcción han alcanzado niveles sin precedentes de innovación y sostenibilidad. Las ciudades han dejado de ser simples conglomerados de edificios y carreteras; se han transformado en organismos vivos e interconectados que respiran, se adaptan y crecen con sus habitantes. Esta evolución ha sido impulsada por avances tecnológicos que han revolucionado la forma en que diseñamos, construimos y gestionamos las infraestructuras urbanas. Desde edificios inteligentes y carreteras que cargan vehículos eléctricos en movimiento, hasta campos fotovoltaicos ultramodernos y gemelos digitales que predicen el futuro de nuestras ciudades, la tecnología ha cambiado el rostro de la ingeniería.

Es una mañana de primavera en Madrid Nuevo Norte, el nuevo distrito tecnológico construido en tiempo récord gracias a las últimas innovaciones en construcción e ingeniería. María Moreno, ingeniera jefa del proyecto de expansión urbana, observa desde su oficina holográfica cómo los robots constructores y las impresoras 3D gigantes trabajan en perfecta sincronía. Lo que antes habría llevado una década, ahora se materializa en meses. Bienvenidos al 2034, donde la construcción y la ingeniería han experimentado una transformación radical que ha cambiado para siempre la forma en que diseñamos, planificamos y construimos nuestro entorno.

Planificación Urbana: El Cerebro Digital de las Ciudades

El diseño y la planificación de las ciudades en 2034 se basan en una sinergia perfecta entre la inteligencia artificial (IA) y el Building Information Modeling (BIM). La planificación urbana se apoya en sistemas de Inteligencia Artificial Urbanística (IAU) que evolucionaron de los primeros gemelos digitales desarrollados en la década de 2020. Cada ciudad cuenta con su “cerebro digital”, un sistema que integra datos en tiempo real de millones de sensores, cámaras y dispositivos IoT. Este sistema no solo modela el presente, sino que predice necesidades futuras con una precisión del 98%.

Las ciudades han evolucionado hasta convertirse en verdaderos organismos vivos, donde cada elemento arquitectónico y estructural contribuye activamente al uso eficiente y a la generación y distribución de energía.

Las calles y carreteras, antaño meras vías de comunicación para el transporte, se han convertido en centrales energéticas lineales. Los sistemas piezoeléctricos avanzados, herederos de aquellos primitivos prototipos de 2024, aprovechan cada pisada y cada vehículo que transita sobre ellos. La eficiencia ha alcanzado niveles sorprendentes: un solo kilómetro de estas carreteras inteligentes genera energía suficiente para alimentar cincuenta hogares promedio.

La integración de células fotovoltaicas transparentes en el asfalto y las barreras de seguridad representa otro salto cualitativo. Con una eficiencia del 35%, estos sistemas han superado todas las expectativas iniciales de los primeros paneles transparentes desarrollados en 2024. Complementando estas tecnologías, los vehículos que transitan sobre estas vías de comunicación son capaces de abastecerse en movimiento gracias a los sistemas de transmisión de energía sin cables evitando así las esperas en la recarga eléctrica de antaño.
Los edificios modernos han evolucionado de su función tradicional para convertirse en verdaderas centrales energéticas. Sus fachadas inteligentes son obras maestras de la ingeniería, donde convergen paneles solares transparentes, películas termoeléctricas y sistemas de captación eólica en una simbiosis perfecta. El almacenamiento energético distribuido, mediante baterías de estado sólido y sistemas de hidrógeno, garantiza un suministro constante y confiable.

En el corazón de esta revolución energética se encuentra la inteligencia artificial, que orquesta una danza perfecta entre producción y consumo. Los algoritmos avanzados analizan patrones de uso, condiciones climáticas y demanda energética en tiempo real, optimizando cada aspecto del sistema con una precisión que supera la capacidad humana.

Esta transformación representa más que un simple avance tecnológico; es un cambio de paradigma en nuestra relación con la energía. Las ciudades de 2034 no solo consumen energía, la generan, la almacenan y la distribuyen con una eficiencia que habría parecido ciencia ficción hace apenas una década. El futuro energético ya no es una promesa lejana; es nuestra realidad cotidiana

Construcción Robotizada: La Nueva Fuerza Laboral

En esta década también se ha transformado como se acometen las obras de construcción. Los RCA (Robots Constructores Autónomos) han revolucionado esta industria. Estos robots, evolución de los primeros prototipos de 2024 como Hadrian X, trabajan 24/7 en condiciones que serían peligrosas para humanos. Equipados con IA avanzada y sistemas de visión 3D, pueden realizar tareas desde la colocación precisa de componentes y materiales hasta soldaduras complejas en estructuras de gran altura. Utilizan algoritmos de IA para adaptar sus métodos de construcción en tiempo real, optimizando el uso de materiales y energía. Los sistemas de impresión 3D gigantes de 2034 pueden construir un edificio de 20 pisos en apenas 2 semanas. Utilizan materiales compuestos que son más fuertes, ligeros y sostenibles que el hormigón tradicional. Estos materiales fueron desarrollados a partir de los primeros hormigones con nanotecnología de 2025. Ahora los edificios no solo son más resistentes que los tradicionales, sino que además son 100% reciclables. Los residuos de construcción se procesan in situ mediante robots especializados que los convierten en nuevos materiales utilizables.

CONTINÚA EN PRÓXIMA PÁGINA

La construcción moderna se ha convertido en una sinfonía perfectamente orquestada de datos, sensores y sistemas interconectados. Cada construcción es ahora un organismo vivo digital, constantemente monitorizado y optimizado a través de una red IoT ultraconectada que procesa millones de datos por segundo.
La revolución digital en la construcción no solo ha transformado cómo construimos, sino que ha redefinido fundamentalmente nuestra relación con el entorno construido. Los edificios del 2034 son testimonio de esta transformación, marcando el camino hacia un futuro donde la tecnología y la construcción se fusionan de manera perfecta para crear espacios que verdaderamente mejoran nuestras vidas. Los nanosensores integrados en los materiales de construcción han revolucionado la forma en que monitorizamos la integridad estructural. Estos diminutos dispositivos, no más grandes que un grano de arena, están embebidos en el hormigón compuesto, el acero y otros materiales estructurales. Su capacidad para detectar tensiones, compresiones, microfisuras y fatiga de materiales ha transformado como se gestiona el comportamiento estructural en tiempo real. El mantenimiento predictivo ha revolucionado la gestión de cualquier tipo de construcción. Los algoritmos avanzados pueden predecir con asombrosa precisión cuándo y dónde se necesitará mantenimiento, eliminando prácticamente los fallos imprevistos. Esta capacidad predictiva ha extendido significativamente la vida útil de las infraestructuras mientras reduce los costes operativos.

La digitalización completa ha transformado todos los aspectos de la construcción. La eficiencia ha aumentado exponencialmente, con reducciones dramáticas en tiempos de construcción y costes operativos. La sostenibilidad ha dejado de ser una aspiración para convertirse en una realidad medible y optimizable.

La inteligencia artificial se ha convertido en el cerebro central de cada proyecto de construcción. Mediante análisis predictivo y aprendizaje continuo, estos sistemas gestionan desde el inventario hasta la programación de tareas con una precisión nunca antes vista. La optimización de recursos y la reducción de desperdicios han alcanzado niveles que antes parecían imposibles.

Los nuevos arquitectos e ingenieros

En los estudios de arquitectura e ingeniería modernos, el espacio físico se ha transformado en un portal hacia dimensiones virtuales infinitas. Los arquitectos e ingenieros ya no están limitados por las paredes de sus oficinas; ahora se sumergen en espacios de trabajo virtuales donde las ideas cobran vida instantáneamente. Un arquitecto en Madrid puede caminar junto a su colega de Tokio a través de un edificio virtual, señalando detalles y compartiendo enfoques en tiempo real. La tecnología de colaboración inmersiva ha eliminado las barreras geográficas y temporales. Las reuniones de diseño son ahora experiencias multisensoriales donde los participantes pueden tocar, modificar y experimentar cada aspecto del proyecto. Los clientes pueden "habitar" sus futuros espacios antes de que se coloque el primer cimiento, tomando decisiones informadas basadas en experiencias virtuales casi indistinguibles de la realidad.

Los hologramas interactivos han revolucionado la visualización arquitectónica. En el mismo sitio de construcción, los modelos tridimensionales a escala real se superponen sobre el terreno real, permitiendo a los equipos de construcción visualizar con precisión milimétrica cada detalle del proyecto. Esta tecnología ha reducido drásticamente los errores de interpretación y ha acelerado los procesos de construcción.

Los hologramas no son simples proyecciones estáticas; son entidades interactivas que responden al tacto y a los comandos de voz. Los arquitectos pueden "esculpir" espacios en tiempo real, ajustando alturas, modificando acabados y experimentando con la luz natural, todo ello mientras camina por el sitio de construcción real.

La capacidad de simular condiciones ambientales ha transformado fundamentalmente el proceso de diseño sostenible. Los arquitectos pueden ahora someter sus diseños a décadas de condiciones climáticas en cuestión de minutos. Pueden observar cómo el edificio responde a tormentas severas, olas de calor extremo o terremotos, todo ello antes de finalizar el diseño.

Esta capacidad predictiva ha llevado a una nueva era de arquitectura resiliente. Los edificios ya no son diseñados solo para el clima actual, sino que se adaptan proactivamente a los escenarios climáticos futuros proyectados. La sostenibilidad ha dejado de ser un objetivo abstracto para convertirse en una variable cuantificable y optimizable en tiempo real.

La gestión de las obras

La integración de drones equipados con realidad aumentada ha revolucionado la supervisión de obras. Estos sistemas de control aéreos no solo capturan imágenes de alta resolución, sino que también proporcionan datos en tiempo real sobre el progreso de la construcción, la calidad de los materiales y el cumplimiento de las especificaciones técnicas.

El control gestual avanzado ha eliminado las barreras entre la intención y la acción. Los jefes de obra pueden controlar múltiples sistemas con simples movimientos de manos o incluso con comandos mentales, gracias a interfaces neuronales de última generación. Esta integración perfecta entre humano y máquina ha llevado la precisión en la obra a niveles sin precedentes.

La transformación digital ha redefinido el papel del arquitecto y de los responsables de las obras. Los profesionales de hoy deben ser tanto artistas como tecnólogos, capaces de navegar entre mundos virtuales y reales con igual destreza. La formación continua se ha convertido en una necesidad, ya que las herramientas y tecnologías evolucionan constantemente.
El horizonte que nos espera promete ciudades no solo más habitables, sino también profundamente adaptativas. Lugares donde la innovación tecnológica será sinónimo de bienestar humano y equilibrio ambiental. Desde la planificación de metrópolis inteligentes hasta la construcción de infraestructuras que desafían los límites de lo posible, la ingeniería del futuro está creando un mundo que antes solo podíamos imaginar en la ciencia ficción.

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/

PdM Book

Product Management Body of Knowledge

P4MGO!®

P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Víctor Almonacid

¿Cómo financiar la transformación digital?

¿Cómo financiar todo un proyecto de transformación digital en un Ayuntamiento, bien empezando de cero, o bien innovando en los servicios existentes ahora ya con la incorporación de nuevos sistemas de IA? Arrojaremos luz sobre este asunto a partir de nuestra experiencia.

Ayuntamiento de Picanya, primera década del siglo. Nuestro proyecto fue financiado con el plan Avanza, el cual en aquella época pocos estaban en disposición de aprovechar, porque las inversiones iban por otro lado. Para nosotros, el proyecto supuso un coste de 85.000 euros en total, todo financiado por el Estado, y además se produjo un retorno casi inmediato de la inversión debido al consiguiente ahorro por la eliminación de papeles, trámites y cargas burocráticas. Aquel Plan Avanza, aprobado en 2005, fue seguido por el Plan Avanza 2, y por su Estrategia 2011-2015, con el fin de continuar la senda hacia la Sociedad de Conocimiento. Años más tarde, la Agenda Digital para España, aprobada en 2013, dio continuidad a esta estrategia de desarrollo fijando "el marco de referencia para establecer una hoja de ruta en materia TIC y de administración electrónica" y la "estrategia de España para alcanzar los objetivos de la Agenda Digital para Europa". Aquel era el tren al que subirse.

Cambiamos de década y de municipio. En el Ayuntamiento de Alzira, el proyecto fue mucho más ambicioso, y se plasmó en tres planes estratégicos:

- Plan de Mejora e Innovación del Ayuntamiento de Alzira (2012).
- 1ª Revisión del Plan de Mejora e Innovación (rebautizado a PMI) 2013-2015.
- 2ª Revisión del PMI: "Proyectos Alzira Inteligente y Alzira Avanza", 2014-2019.

En este caso fue imprescindible apostar por estos proyectos comprometiendo la parte necesaria del Presupuesto, algo que demuestra la alineación del impulso técnico con la estrategia política. Si usted está gestionando un plan de actuación y no tiene asignada una buena partida presupuestaria, sepa que está destinado a pasar dificultades en su ejecución.

CONTINÚA EN PRÓXIMA PÁGINA

> **Bienaventurado el que tiene talento y dinero, porque empleará bien este último**
>
> Menandro de Atenas

Dicho lo cual, nuevamente se hace necesaria la ayuda externa, normalmente en forma de convocatorias para el reparto de los fondos estratégicos de otras instancias, empezando por Europa.

De hecho, en 2018 nos concedieron una buena cantidad dentro del llamado EDUSI para financiar nuestro proyecto Alzira Avanza, de acuerdo con la Orden HFP/888/2017, de 19 de septiembre, por la que se aprobó la tercera convocatoria para la selección de Estrategias de Desarrollo Urbano Sostenible e Integrado (EDUSI).

Más tarde desarrollamos un proyecto en la misma línea, pero incorporando la participación de otros actores de lo público.

Así vio la luz el Plan Urbano de Actuación Municipal de Alzira (PUAM), en este caso financiado por la Diputación de València, que través de su Área de Cooperación Municipal y Cohesión Territorial, destinó parte de su Plan de Inversiones 2020-2021, al impulso de los llamados planes urbanos de actuación municipal (PUAM), con el fin de que las actuaciones incluidas en estos planes pudieran ser elegidas como subvencionables en el Plan de Inversiones de la Diputación. De forma concreta, el PUAM de Alzira se planteó con una vocación transformadora de los espacios y áreas municipales y para su desarrollo activó los procesos de participación, debate e interlocución entre la ciudadanía y los agentes sociales para concretar un diseño municipal de futuro basado en la sostenibilidad en sentido amplio, no solo tecnológica.

Obviaremos esta vez los fondos Next Generation, por ser muy probablemente la línea de subvenciones para la transformación más conocida. Por su parte, las convocatorias más recientes las encontramos en resoluciones como la Orden HAC/1072/2024, de 2 de octubre, por la que se aprueban las bases reguladoras para la asignación de senda financiera FEDER a Planes de actuación integrados de entidades locales, en el marco del Desarrollo Urbano Sostenible, con cargo al Fondo Europeo de Desarrollo Regional en el periodo de programación 2021-2027, y otras de carácter similar.

Por último, nuevamente desde nuestra experiencia, compartimos los siguientes consejos para aumentar las posibilidades de acceder a estas ayudas:

- Alineación con los ODS y políticas públicas europeas.
- Tener en marcha proyectos reales relacionados con la convocatoria.
- Aunque no se opte a una ayuda “Next Generation”, apostar por la recuperación, transformación y resiliencia, aún en el contexto post-pandemia.
- Proponer el destino de los fondos a las áreas afectadas por la DANA.
- Por supuesto, leer bien la convocatoria y ajustarse a sus parámetros
- Si no tenemos los recursos para elaborar el proyecto, contratar técnica asistencia externa.

Suerte.

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/

BPM Book

Business Process Management Body of Knowledge

P4MGO!®

P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Alex Aliaga

Security Operations Center

Introducción: El Panorama del SOC Moderno

Con un escenario donde el perímetro es totalmente difuso debido a la movilidad de los trabajadores, la migración de las aplicaciones al cloud y las consecuencias de la adopción de proyectos de transformación digital dentro de las organizaciones. Hace que la superficie de exposición, y las vulnerabilidades hayan incrementado de forma exponencial en los últimos años.

Poco a poco, las organizaciones de todos los tamaños se han dado cuenta de sus limitaciones en cuanto a personal y experiencia para abordar adecuadamente esta creciente necesidad de proteger su negocio de las constantes amenzas de los cibercriminales.

La enorme inversión que se tiene que realizar para poder disponer de un SOC (Security Operations Center), es algo que muy pocas organizaciones pueden permitirse. No sólo debemos pensar en la inversión tecnológica, sino también en la inversión de talento y capital humano necesario para abordar el conocimiento de todas las plataformas tecnológicas existentes alrededor de un SOC

Selección y Recolección de los Datos Adecuados

La selección y recolección de los datos correctos es vital para el funcionamiento eficaz de cualquier SOC. Esta estrategia implica la cuidadosa consideración del valor relativo de diferentes tipos de datos, como la información proveniente de sensores y los datos de registro recolectados por sistemas de red y del endpoint, recursos en cloud, aplicaciones, etc. Lo primero que se suele plantear en un proyecto de SOC para recopilar toda esta información, es instalar un SIEM.
A pesar de que, por lo general, existe una clara conciencia de que las soluciones SIEM son complejas de instalar, muchas organizaciones se aventuran a la instalación de este tipo de soluciones sin definir claramente objetivos, requisitos y estimaciones de crecimiento. Incluso se aventuran a pensar que hay soluciones que *"out of the box"* ya pueden cumplir sus requisitos. Una mala planificación hace que, por lo general, el proyecto no se implemente de forma adecuada, obteniendo unos resultados que no son los esperados o que no cumplen las expectativas generadas

Otro de los errores que más se cometen a la hora de implantar un SIEM, es no definir claramente un alcance. Es habitual encontrarse con dos extremos, los que no definen un alcance y aquellos que su alcance es "**monitorizarlo todo**".

Evidentemente, ambos extremos son perjudiciales, y como se suele decir en el equilibrio está la clave. Querer abarcarlo todo desde un principio es complicado, sobre todo porque este tipo de herramientas requieren de la coordinación con muchas otras áreas de TI (sistemas, redes, etc.) y no sólo eso, sino que también hay que tener en cuenta que no basta con integrar las fuentes de información directamente en un SIEM, sino que hay que diseñar previamente qué información queremos recopilar de cada fuente, el formato y la retención que queremos tener.

Estos factores condicionaran tanto la elección de la herramienta, el hardware elegido, la arquitectura del sistema, las licencias y por supuesto tendrá un impacto en el presupuesto. Por tanto, son claves para el éxito de un proyecto de estas características. Algunos de los puntos clave a tener en cuenta para la instalación de un SIEM son, entre otros:

•Evaluar las necesidades, recursos disponibles y el nivel de madurez de la organización para determinar si una herramienta SIEM puede sernos de utilidad

•Hacer una pequeña lista de proveedores de SIEM, y estudiar con detenimiento si las propuestas se ajustan a las necesidades de tu organización

•Siempre que sea posible, es interesante hacer una prueba de concepto (PoC) para conocer el producto en detalle y saber si se ajusta a nuestras necesidades

•Definir el alcance del proyecto, si fuese necesario repartirlo en varias fases

•Conocer las dependencias tecnológicas del alcance definido

•Definir un set inicial de reglas que cubra las necesidades de detección. Este set de reglas podrá ampliarse en fases posteriores del proyecto, incluso combinarlo con trabajos de "caracterización de amenazas" para conocer qué gaps tenemos.

•Evaluar regularmente el funcionamiento del SIEM, incluir nuevas reglas de detección (casos de uso) lo cual redundará en una mejor postura de defensa de la organización

Priorizar la Respuesta a Incidentes

Un aspecto esencial en la operación de un SOC es la respuesta a incidentes. Esta debe ser priorizada de forma organizada y sistemática. Para esto, el uso de **manuales de procedimientos (playbooks) es vital, pues permite estandarizar la respuesta a incidentes de forma efectiva**. Un manual de procedimientos generalmente incluye: título, intención, alcance, condiciones estimulantes (circunstancias en las que se debe usar el manual), procedimientos, pasos y expectativas a seguir, y varios metadatos (quién lo aprobó, historia de revisión). Aunque el SOC no siga con frecuencia un escenario de respuesta a incidentes, puede ser útil codificar ese tipo de incidente en un procedimiento operativo estándar (SOP) para que la próxima persona no tenga que reaprender el proceso.

El arte de escribir manuales de procedimientos efectivos reside en balancear la cantidad de detalle y especificidad, y al mismo tiempo entender que algunos detalles cambiarán con cada incidente. Es necesario capturar aquellos aspectos que son consistentes entre un tipo específico de tecnología y un incidente de alta prioridad para el constituyente. Si un manual es muy general, los respondientes cibernéticos experimentados lo complementarán con su propio conocimiento, lo que puede ser bueno, pero también puede llevar a inconsistencias y a que otros queden sin información. Igualmente, si dejan la organización, su conocimiento se irá con ellos.

CONTINÚA EN PRÓXIMA PÁGINA

Es necesario capturar suficiente detalle para que los respondientes cibernéticos menos experimentados entiendan cómo responder a un incidente y que los respondientes más experimentados sean consistentes en su enfoque.

Por otro lado, un exceso de detalle puede hacer que el manual se vuelva obsoleto rápidamente y puede sofocar la capacidad de los analistas para actuar por intuición y adaptarse al incidente. Finalmente, cuando el SOC explica un incidente a las partes interesadas y a la alta dirección, el mensaje debe ser claro y conciso. **La explicación no debe enfocarse en bits y bytes sino en la misión, los costos y a veces las vidas**. Las cuatro preguntas que se deben responder son: (1) qué (y/o quién) fue el objetivo, (2) si el adversario tuvo éxito, (3) quién es el adversario y cuál es su motivación, y (4) cómo continuar la misión.

Contratar y Desarrollar Personal de Calidad

La tecnología sin personas que la operen, no sirve de nada. Por tanto, a la hora de planificar un SOC, el personal es el aspecto más importante. Numerosas encuestas indican que la contratación de personal es la principal preocupación para aquellos que trabajan en el campo de la ciberseguridad y que la escasez de habilidades tiene un impacto significativo en sus organizaciones.

No solo se trata de contratar talento, también es necesario crear un ambiente que anime al personal a quedarse ("fidelización del talento"), mientras se planifica para la eventual rotación que , queramos o no, ocurrirá. A la hora de hacer las contrataciones ya no vale guiarse por la "titulitis" en este sector, hay aspectos que marcan mucho la diferencia entre los profesionales de ciberseguridad:

•**Pasión por la ciberseguridad:** Es quizás la principal cualidad a buscar en cualquier posible contratación al SOC, independientemente de la posición o el nivel de experiencia.
•**Entusiasmo, curiosidad y sed de conocimiento:** Un especialista en ciberseguridad debe ser entusiasta, curioso y siempre querer aprender más.
•**Habilidades blandas y trabajo en equipo:** El candidato ideal debe demostrar habilidades en el manejo de personas y debe tener una disposición al trabajo en equipo.
•**Conocimientos técnicos:** Un candidato debe demostrar conocimientos generales de TI y ciberseguridad, así como un conocimiento profundo en al menos una o dos áreas relacionadas con las operaciones de ciberseguridad.

Ahora bien, una vez tenemos a nuestro personal, como si de un gimnasio se tratase, hay que proveerles de un entrenamiento para mejorar su capacidades y sacir su ansiedad por nuevos conocimientos.

El entrenamiento formal del personal es esencial para asegurar una base de conocimientos técnicos y la adhesión a procesos relevantes del SOC. Esto puede incluir un proceso de calificación técnica o "check-ride" que cada nueva contratación debe pasar dentro de un período de tiempo específico después de la contratación. Este tipo de procesos asegura que todos los empleados puedan operar con un nivel base de capacidades técnicas y una adhesión consistente a los procesos relevantes del SOC, dependiendo de su función laboral. El programa también debe incluir actividades de enriquecimiento, tales como asistencia a congresos de seguridad, simulacros, asistencia a foros donde se comparten procesos y procedimientos que ayudan a una mejor gestión del SOC.
Por esta razón, es necesario que tengamos en consideración la formación de los líderes que van a gestionar el SOC, prepararles para trabajar en ambientes de mucha presión, y con skills que no sólo van a ser técnicos, hay que trabajar mucho su faceta de comunicación con la alta dirección, y con actores externos, como pueda ser la prensa, por ejemplo.
Y si entramos en la formación, también debemos considererar formar a nuestra alta dirección en el entendimiento de qué es un SOC, y de cómo actuar ante un ciberincidente. Que todas las partes impilcadas en un incidente de seguridad estén bien formadas, es la clave para restaurar en el menor tiempo posible la normalidad sin que para ello exista un grave impacto en la continuidad de negocio, y en la reputación e imagen de la organización.

Conclusión: El Camino hacia la Excelencia en Ciberseguridad

El establecimiento de un centro de operaciones de seguridad requiere de un entendimiento profundo de los datos, la tecnología y, sobre todo, el factor humano. La selección y la recolección de los datos correctos, el uso de herramientas, el desarrollo tanto del personal como la alta dirección, así como la priorización de la respuesta a incidentes son los pilares fundamentales de un SOC eficaz.

Para garantizar un buen funcionamiento del SOC, es crucial **mantener una comunicación clara y una colaboración fluida con todas las partes interesadas.** Esto incluye a la alta dirección, los responsables de IT y los usuarios. La capacidad de traducir jerga técnica en lenguaje de negocios, la elaboración de informes claros y concisos, y el establecimiento de métricas y KPIs relevantes son elementos clave para la eficacia del SOC.

Además, con un servicio de seguridad gestionada adecuado, las organizaciones tendrán la tranquilidad de saber que hay un equipo de expertos cualificados que supervisan constantemente su empresa, buscan amenazas, investigan actividades sospechosas y responden a posibles incidentes.
Con el panorama de amenazas a la ciberseguridad en permanente evolución, trabajar con un equipo cuyo único objetivo es la ciberseguridad aporta tranquilidad a su empresa para que pueda centrarse en su negocio.

Hashtags: #Ciberseguridad #SOC #SecurityOperations #ThreatIntelligence #IncidentResponse #SIEM #SOAR #Cybersecurity #RedTeam #BlueTeam #CyberDefense #SecurityAnalyst #ThreatHunting

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®

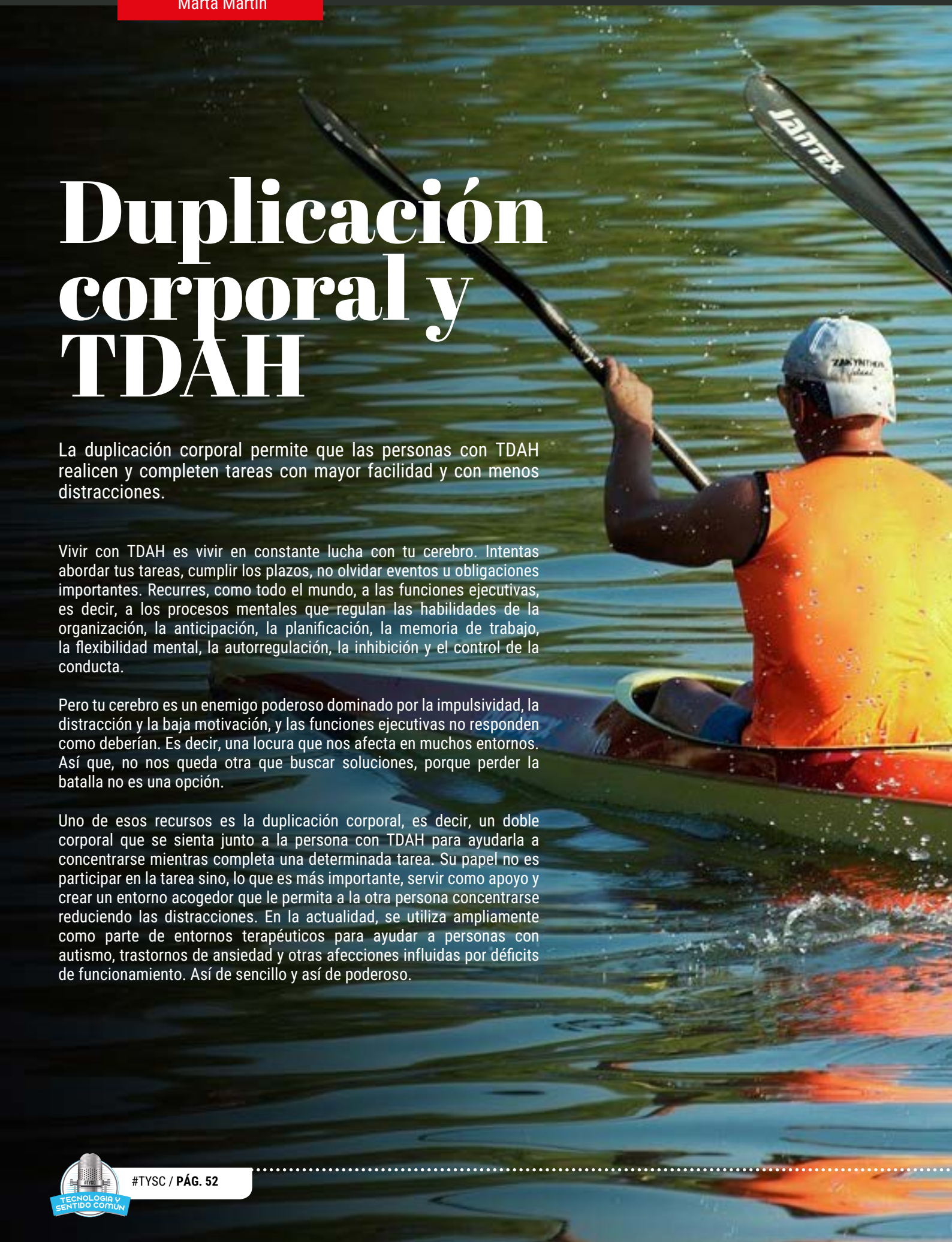
Próxima Convocatoria en Directo
MARZO 2025

Solicita tu admisión en:

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

Marta Martín

Duplicación corporal y TDAH



La duplicación corporal permite que las personas con TDAH realicen y completen tareas con mayor facilidad y con menos distracciones.

Vivir con TDAH es vivir en constante lucha con tu cerebro. Intentas abordar tus tareas, cumplir los plazos, no olvidar eventos u obligaciones importantes. Recurres, como todo el mundo, a las funciones ejecutivas, es decir, a los procesos mentales que regulan las habilidades de la organización, la anticipación, la planificación, la memoria de trabajo, la flexibilidad mental, la autorregulación, la inhibición y el control de la conducta.

Pero tu cerebro es un enemigo poderoso dominado por la impulsividad, la distracción y la baja motivación, y las funciones ejecutivas no responden como deberían. Es decir, una locura que nos afecta en muchos entornos. Así que, no nos queda otra que buscar soluciones, porque perder la batalla no es una opción.

Uno de esos recursos es la duplicación corporal, es decir, un doble corporal que se sienta junto a la persona con TDAH para ayudarla a concentrarse mientras completa una determinada tarea. Su papel no es participar en la tarea sino, lo que es más importante, servir como apoyo y crear un entorno acogedor que le permita a la otra persona concentrarse reduciendo las distracciones. En la actualidad, se utiliza ampliamente como parte de entornos terapéuticos para ayudar a personas con autismo, trastornos de ansiedad y otras afecciones influidas por déficits de funcionamiento. Así de sencillo y así de poderoso.

El trabajo en paralelo se hizo popular durante la pandemia. Los estudios de investigación sobre su efectividad son escasos pero hay multitud de pruebas anecdóticas que sugieren que puede cambiar las reglas del juego. Eso sí, para obtener buenos resultados es fundamental tener las expectativas claras, elegir el entorno adecuado y hacer pausas regulares. De esta manera, el doble corporal nos ayudará a lidiar con las manifestaciones más incómodas de nuestra condición como, por ejemplo:

•**Las dificultades para iniciar y finalizar tareas que no nos motivan o gratificantes.** Al tener un compañero, de manera inconsciente la persona se reconduce mejor y crea un sentido de la responsabilidad.

•**La percepción del tiempo.** Ayuda a una correcta gestión del mismo como por ejemplo ser consciente de las fechas de entrega o de las pausas que tenemos que hacer.

•**La autorregulación de la conducta**, que mejora con la sensación de que alguien está vigilando.

•**La regulación emocional,** ya que a veces es difícil lidiar con las emociones, sobre todo con las cosas que no nos aportan una gratificación inmediata o las que nos frustran. El doble puede proporcionarnos apoyo social y emocional, ayudarnos a controlar nuestras emociones y a hacer que las tareas sean menos desalentadoras.

•**La excitación,** estamos más alerta y comprometidos cuando hay alguien cerca y como las personas con TDAH suelen tener niveles de excitación más bajos tienen también más dificultades para el inicio y la concentración.

CONTINÚA EN PRÓXIMA PÁGINA

Sin embargo, este método no es efectivo para todos ya que una mala elección del doble corporal puede suponer una distracción o generar una relación de dependiencia que nos impida desarrollar estrategias individuales de trabajo.
Y si ese compañero no contribuye a un entorno cómodo y seguro, interferirá en la percepción de los propios síntomas, y nos hará sentirnos aún más criticados y frutrados. A esto hay que suamarle otros factores que pueden condicionar su eficacia como las distintas personalidades, las preferencias individuales o los tipos de tareas.

Para los casos en los que no funcione siempre tenemos alternativas.

•**Listas y aplicaciones:** en su versión analógica pero también a través de aplicaciones diseñadas para ayudar a gestionar las tareas, controlar el tiempo y concentrarse.

•**Cambio de tarea:** si tenemos dificultades para concentrarnos en una tarea, es mejor cambiar y retomarla más adelante. Eso puede restablecer nuestra concentración y mantener nuestro cerebro ocupado.

•**Rutinas diarias rígidas:** nos proporcionan la estructura que muchas personas con TDAH necesitamos. Muy recomendable para reducir la fatiga por decisiones, con lo que tendremos más energía mental para tareas más importantes.

•**Entornos tranquilos y silenciosos:** no todas las personas con TDAH prosperan en ambientes ajetreados, otras se desenvuelven mejor en espacios tranquilos y silenciosos donde rebajar la sobreestimulación sensorial.

Cada persona debe encontrar cuál es la estrategia con la que mejor funciona. Sea cual sea, lo más importante es recordar que el TDAH, al igual que el resto de las neurodivergencias, no es un defecto ni un fallo, tan solo una forma diferente de estar en el mundo. Así que, tanto si utilizas el doble corporal o si prefieres otras herramientas alternativas, el objetivo no es ser como los demás, sino encontrar formas de prosperar con tu condición.

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/

CoE Book

Centres of Excellence Body of Knowledge

P4MGO!®

P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Estándares para la inteligencia artificial

por José Antonio Jiménez Caballero
Coordinador de Digitalización
UNE

Tanto en el ámbito europeo como en el nacional se están desarrollando estándares que contribuyan a un uso seguro, ético y responsable de la inteligencia artificial (IA). Aquí explicamos qué trabajos están actualmente en marcha.

En los últimos años se ha producido una explosión de actividad relacionada con la inteligencia artificial (IA). Por un lado, cantidades ingentes de aplicaciones de la IA en todos los ámbitos, con el consiguiente impacto socioeconómico. Por otro lado, se han visto los peligros de la IA, que surgen cuando no se hace un uso seguro, ético y responsable de la misma.

Como se ha hecho con muchas otras tecnologías anteriormente, en la Unión Europea se ha elaborado una legislación común que regula la IA, y los países miembros por su parte tienen sus propias estrategias nacionales específicas en la materia, que en su conjunto permitirán disfrutar de las ventajas de la IA a la vez que se mitigan sus riesgos.

El Reglamento Europeo de Inteligencia Artificial

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial tiene como objetivo mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de

inteligencia artificial, de conformidad con los valores de la Unión. El objetivo es promover la adopción de una inteligencia artificial centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, seguridad y derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la UE.

Dada la enorme variedad de campos de aplicación de la IA, conseguir los objetivos del Reglamento europeo de IA requiere imponer requisitos distintos según la aplicación de la que se trate. Para establecer un conjunto proporcionado y eficaz de normas para los sistemas de IA, el Reglamento aplica un enfoque basado en los riesgos claramente definido, que adapta el tipo y contenido de las reglas que exige a la intensidad y el alcance de los riesgos que puedan generar los sistemas de IA considerados. La clasificación por riesgo se muestra en la Figura 1.

El papel de la normalización

Como muchas otras regulaciones europeas, bajo el modelo del Nuevo marco legislativo o "nuevo enfoque" (New Legislative Framework, NLF), el Reglamento (UE) 2024/1689 se apoyará en estándares europeos para demostrar la conformidad de los sistemas de IA con respecto a ciertos requisitos técnicos. El uso de estándares ya establecido o por venir aplicará a las siguientes categorías:

- sistemas de IA de alto riesgo;
- modelos de IA de uso general;
- presentación de información y documentación a fin de mejorar el funcionamiento de los de los sistemas de IA desde el punto de vista de los recursos, como la reducción del consumo de energía y de otros recursos.

De momento, la Comisión Europea ha solicitado el desarrollo de estándares para cubrir los siguientes aspectos de los sistemas de IA de alto riesgo:

1. Sistema de gestión de riesgos

Debe concebirse como un proceso continuo e iterativo que se desarrolla a lo largo de todo el ciclo de vida del sistema de IA y que tiene por objeto prevenir o minimizar los riesgos pertinentes para la salud, la seguridad o los derechos fundamentales. Debe ser compatible con los sistemas de gestión de riesgos propios de la aplicación específica del sistema de IA cuando forme parte de un componente de seguridad de un producto determinado.

2. Gobernanza y calidad de los conjuntos de datos utilizados

Los proveedores de sistemas de IA deben aplicar los procedimientos adecuados de gobernanza y gestión de datos, y cubrir los aspectos de calidad de los conjuntos de datos utilizados para entrenar, validar y probar los sistemas de IA.

3. Registro automático de eventos

Este registro automático de eventos permitirá la trazabilidad de dichos sistemas a lo largo de su ciclo de vida, así como el seguimiento de sus operaciones, y facilitará el seguimiento posterior a la comercialización por parte de los proveedores.

CONTINÚA EN PRÓXIMA PÁGINA

4. Transparencia e información para los usuarios
Los sistemas de IA deben diseñarse de forma que garanticen la transparencia del funcionamiento para que los usuarios puedan comprender los resultados del sistema y utilizarlos adecuadamente. Deben ir acompañados de instrucciones de uso detalladas como capacidades y limitaciones del sistema, instrucciones de mantenimiento, información para perfiles de usuarios profesionales o no profesionales.

5. Supervisión humana
Los sistemas de IA deben contener medidas y procedimientos que garanticen la supervisión humana de su funcionamiento, que permitan que los usuarios comprendan, supervisen, interpreten, evalúen e intervengan en su comportamiento.

6. Especificaciones de precisión
Los proveedores de sistemas de IA deben declarar los parámetros y niveles de precisión pertinentes, incluyendo, cuando esté justificado, un conjunto de herramientas y parámetros adecuados para medir la precisión con respecto a niveles definidos.

7. Especificaciones de robustez
Los sistemas de IA deben contemplar medidas para garantizar su robustez, teniendo en cuenta las fuentes pertinentes de errores, fallos e incoherencias, así como las interacciones del sistema de IA con el entorno, incluidos los que siguen aprendiendo después de su comercialización o puesta en servicio, en particular en lo que respecta a los circuitos de retroalimentación.

8. Ciberseguridad
Deben proporcionarse soluciones organizativas y técnicas adecuadas para garantizar que los sistemas de IA sean resistentes a los intentos de alterar su uso, comportamiento y funcionamiento o de comprometer sus propiedades de seguridad por parte de terceros malintencionados que exploten las vulnerabilidades de estos sistemas.

9. Sistema de gestión de la calidad para proveedores
Los proveedores de sistemas de IA deben implantar un sistema de gestión de la calidad que asegure el cumplimiento continuo de los aspectos descritos en los puntos 2 al 8.

10. Evaluación de la conformidad
Deben establecerse procedimientos de verificación y validación de los sistemas de IA que garanticen que son adecuados para su uso y el sistema de gestión de la calidad se ha implantado de forma correcta. Estos procedimientos deben contemplar la posibilidad de una autoevaluación o una evaluación por un tercero independiente.

Los estándares que se van a utilizar para demostrar la conformidad con estos requisitos se están elaborando en el Comité europeo CEN/CENELEC JTC 21 Artificial Intelligence, utilizando en su mayor parte los estándares desarrollados en el Comité internacional ISO/IEC JTC 1/SC 42 Artificial Intelligence, para alinear los requisitos europeos con los internacionales. En el ámbito nacional, estos estándares se desarrollan en el Comité CTN-UNE 71/SC 42 Inteligencia artificial y big data de UNE.

La Estrategia de Inteligencia Artificial 2024 de España
La Estrategia de Inteligencia Artificial 2024 del Gobierno de España pretende aprovechar la oportunidad que proporciona la IA como palanca de transformación económica de nuestro país, reforzando la Estrategia Nacional de Inteligencia Artificial (ENIA), que se publicó en 2020. La Estrategia de Inteligencia Artificial 2024 contiene iniciativas que pretenden generar impacto económico y social a través de la IA, en las que la normalización tiene especial relevancia. Reflejo de esa relevancia es la creación de un sello de calidad en materia de IA sostenible y el desarrollo de un ecosistema de colaboración público-privada, que se desarrolla a través del Programa Nacional de Algoritmos Verdes (PNAV).

Así, la creación de un sello de Calidad Green Tech instaurará un programa de reconocimiento de modelos de inteligencia artificial medioambientalmente sostenibles, que proporcione una ventaja competitiva a los modelos desarrollados en España. La aportación de información sobre consumo energético de los sistemas de IA de propósito general está prevista en el Reglamento (UE) 2024/1689.

En este contexto, la Secretaría de Estado de Digitalización e Inteligencia Artificial ha tomado la iniciativa de desarrollar, con el apoyo de la Asociación Española de Normalización, las Especificaciones UNE necesarias para evaluar el impacto medioambiental de los sistemas IA, sustentando con ello la concesión de dicho sello de calidad. Además, este trabajo puede servir como base al futuro proceso de estandarización europeo en esta materia, permitiendo a las empresas españolas que ya posean el sello nacional una transición más sencilla hacia los requisitos de información futuros derivados del Reglamento Europeo de IA.

Las Especificaciones UNE se están desarrollando en el Grupo de Trabajo CTN-UNE 71/SC 42/GT 1 Evaluación de la eficiencia energética de los sistemas de inteligencia artificial, liderado por la Secretaría de Estado de Digitalización e Inteligencia Artificial y en el que colaboran 63 expertos de 29 entidades.

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

eGob®

Escuela de Gobierno eGob®

admisiones@escueladegobierno.es

https://escueladegobierno.es