REVISTA

Tecnología & Sentido Común

#43
JULIO 2024

9 772951 818003 43

REVISTA

Tecnología & Sentido Común

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

9 772951 818003 43

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.

#43

JULIO 2024

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

#43 - JULIO 2024

¡tysc

#TYSC

Premios recibidos

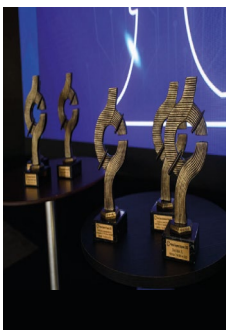
Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI

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

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

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

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



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

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática

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

Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA

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

ESTE MES TE RECOMIENDO LEER...

por Javier Peris

Corporate Governance

Christine A. Mallin

"Corporate Governance" de Christine A. Mallin se ha convertido en una referencia esencial para comprender la gobernanza corporativa en el entorno empresarial actual. Este libro combina teoría y práctica, proporcionando una guía accesible y detallada sobre cómo las organizaciones deben ser dirigidas y controladas para asegurar su integridad y eficiencia.

El libro comienza con una sólida introducción a los conceptos clave de la gobernanza corporativa, destacando su importancia para el funcionamiento ético y efectivo de las empresas. Define la gobernanza corporativa y explora las estructuras y mecanismos de control necesarios para alinear las acciones de la empresa con los intereses de sus accionistas y otras partes interesadas.

Uno de los aspectos más destacados del libro es su análisis del papel del consejo de administración. La autora examina en detalle las responsabilidades de los directores, como la supervisión de la gestión, la formulación de estrategias y la rendición de cuentas. También discute las cualidades y habilidades necesarias para ser un director efectivo, así como la importancia de la independencia y la diversidad en el consejo.

El libro además proporciona recomendaciones prácticas para mejorar la efectividad del consejo, explorando las dinámicas internas y la relación con la gerencia y los accionistas. La autora subraya la importancia de la comunicación y la transparencia en una gobernanza exitosa.

"Corporate Governance" de Christine A. Mallin es una obra integral que se ha ganado su lugar como un recurso indispensable para estudiantes, académicos y profesionales interesados en mejorar las prácticas de gobernanza en sus organizaciones. La combinación de teoría y ejemplos prácticos la convierte en una lectura obligatoria para aquellos que buscan entender y aplicar los principios de una buena gobernanza corporativa.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión Documental y Gestión del Conocimiento

ISO 30301:2021
ISO 30401:2021

Dirección Académica:
Javier Peris

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

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

19 de julio 2024

11:00 a 15:00

C/Génova 6
28004 Madrid
España

Evento
CIERRE DE TEMPORADA
Revistas "Tecnología y Sentido Común" y "Stakeholders.news"

Ven a Celebrarlo!

ORGANIZA:

Business&Co®
Business, Technology & Best Practices, S.L.

COLABORADORES:

UNE Normalización Española

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

MGEIT®

MPPM®

Managers.Institute
Knowledge to Grow

AGENDA

11:30 a 11:45


Presentación Evento

PALOMA GARCÍA LOPEZ
Directora de Programas de Normalización y Grupos de Interés de UNE, Asociación Española de Normalización

JAVIER PERIS
Director revistas Tecnología y Sentido Común y Stakeholders.news

11:45 a 12:00

Bienvenida de UNE, Asociación Española de Normalización

PALOMA GARCÍA LOPEZ
Directora de Programas de Normalización y Grupos de Interés de UNE, Asociación Española de Normalización

12:00 a 12:30

De Gestionar a Gobernar... con 'G' de Ganar

RAMSÉS GALLEGO
ISACA Hall of Fame 2024

12:30 a 13:00

Mesa Redonda "Stakeholders.news"

modera Javier Peris

Juan Manuel Dominguez

Sección: Organizaciones Reslientes

Luis Morán

Sección: Personas y Procesos

Jose Antonio Puentes

Sección: Tendiendo Puentes

Juan Jesús Urbizu

Sección: Tecno-transformación

13:00 a 13:30

Mesa Redonda "Tecnología y Sentido Común"

modera Javier Peris

Alejandro Aliaga

Sección: Radio Security

Renato Aquilino

Sección: Marcos y Normas

Marlon Molina

Sección: Es Tendencia

Marcos Navarro

Sección: Ai Robot

Manuel Serrat

Sección: Futuro y Seguridad

13:30 a 13:45

Nombramiento Embajadores de Stakeholders.news

El Salvador

Puerto Rico

Uruguay

13:45 a 14:00

Entrega de Premios

PREMIO REVISTA
Tecnología & Sentido Común
2024

PREMIO REVISTA
Stakeholders .news 2024

14:00 a 15:00 Degustación de Exclusivo Catering y Networking

Evento
CIERRE DE TEMPORADA

Revistas "Tecnología y Sentido Común" y "Stakeholders.news"

ORGANIZA:

Business&Co®
Business, Technology & Best Practices, S.L.

COLABORADORES:

UNE Normalización Española

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

MGEIT®

MPPM®

Managers.Institute
Knowledge to Grow

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Inteligencia Estratégica y Gestión de la Innovación

ISO 56002:2019
ISO 56006:2021

Dirección Académica:
Javier Peris

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

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre

Solicita tu admisión en:

+ 34 96 109 44 44
campus@escueladegobierno.es

EL GOBERNAUTA

Javier Peris

De indocumentables e indocumentados

Cada vez con mayor frecuencia me encuentro situaciones donde las organizaciones no pueden afrontar adecuadamente los retos y oportunidades que nos brinda esta era digital por culpa del llamado legacy, termino amistoso para definir aquello que deberia haber sido cambiado, pero nunca se ha encontrado el momento, el dinero, los recursos, la actitud o incluso la paz espiritual suficiente para hacerlo.

En la mayoría de estas situaciones la causa raíz es un poco más profunda, no hay que rascar mucho para darse cuenta que de ninguna manera el problema es el propio legacy, sino que lo que la verdad esconde, y es al foco del problema, la absoluta falta de documentación.

> **Si quieres ir rápido ves solo, si quieres llegar lejos ves documentado.**

Se confunde con demasiada frecuencia rapidez con fugacidad y agilidad con precipitación creyendo de esa manera contentar en el plazo minimo de tiempo las necesidades de nuestros clientes sin pararnos a pensar si de verdad atendemos sus necesidades o nos estamos labrando un futuro mucho peor.

Frecuentemente veo directivos que deberían estar documentando que huyen hacia delante incorporando aquellas metodologías que menos le comprometen a documentar para meter debajo de la alfombra incapacidades y carencias que ponen en grave riesgo el futuro inmediato de la compañía.

Recuerdo una ocasión en la que escuché decir a un responsable, mejor dicho a un Mando Intermedio porque de responsable tiene bien poco, que un determinado aplicativo de gestion crítico para el negocio se documentaria cuando tuviera más tiempo o cuando se incorporaran más personas en el equipo. Le pregunté si él tambien a sus hijos esperaba a que tuvieran la mayoría de edad, o que hubieran encontrado pareja, para educarlos.

> **Si una tarea no vale la pena hacerla como es debido, es que no vale la pena hacerla en absoluto.**

Lamentablemente en el mundo de las organizaciones se otorga responsabilidad a quien no es responsable y esto nunca acaba bien. Y digo que no se es responsable por pura naturaleza, es decir, hay ámbitos que pertenecen más al mono que al sapiens, venimos todos con una carga genética difícil de modificar y en base a esto se han definido distintos modelos o "Persotipos" que identifican claramente para que está preparado y para que no un determinado ser humano.

Si el lector quiere ahondar en la de los "Persotipos" cuestión le invito lea atentamente mis dos artículos de mayo y junio en la seccion "El Goberanuta" de la revista "Tecnología y Sentido Comun" donde trato con profundidad este asunto.

Entonces el problema no está tanto en la persona que no demuestra estar a la altura de las circunstancias sino de aquel que ha tenido los arrestos suficientes para darle una responsabilidad para la cual no estaba adecuadamente dotado.

Afirmar que cualquier ser humano puede ser lo quiera llegar a ser es una soberana incongruencia que además fomenta y propicia el fracaso personal y profesional de manera irresponsable. Le puedo asegurar al lector que yo hace muchos, muchos años tomé consciencia que jamás sería ni un baloncestista de élite, entrenara las horas que entrenara, un saxofonista de éxito ensayara las horas que ensayara.

CONTINÚA EN PRÓXIMA PÁGINA

> **Si no conoces de qué color es cada miembro de tu equipo y donde puede desarrollarse con mayor eficacia estáis perdidos.**

El lector pensará que puede haber muchos otros factores que pueden tener un impacto en el problema raíz del legacy o de desarrollos heredados que como hemos visto es la falta documentación, y tiene toda la razón. Pero en esos casos en los que la carga genética es la adecuada para la responsabilidad asumida la predisposición del individuo es radicalmente distinta. No huye de la documentación, se enfrenta a ella, no huye de sus responsabilidades, sino que busca ayuda bien de manera autodidacta o bien a través de colegas de profesión, o de centros especializados, es decir se enfrenta al problema y no lo esquiva porque lo hace suyo.

Este tipo de profesionales involucrados en encontrar soluciones confiables que garanticen un futuro mejor necesariamente tienen mayor visión a medio y largo plazo, aportan mayor valor a la organización y no se dejan embaucar por el ahora, tienen mayor perspectiva y altura de miras y por tanto son más confiables a la hora de desempeñar sus funciones, son más estratégicos y no tan tácticos permitiendo el crecimiento a largo de la organización.
Y permítame el lector incidir en que este tipo de "Persotipo" no es ni mejor ni peor que el anteriormente descrito más táctico, fugaz, oportunista y dicharachero, siempre y cando cada uno estén en su ligar adecuado. Tan malo es poner a aluien con capacidades y habilidades de "Dirección General" como "Desarrollador de Software" como poner a alguien con habilidades y capacidades de "Desarrollador de Software" como "Director General" de la organización.

Prueba de ello es la enorme lista de casos de fracaso en ascensos o promociones de "Desarrolladores de Software" a "Project Managers"; de "Project Managers" a "Programme Managers"; de "Mandos Intermedios" a "Alta Dirección"; llevándose la palma últimamente con el mayor número de despropósitos la promoción de "Projects Managers" a "lideres de PMOs", "Persotipos" en la mayoría de los casos absoluta y radicalmente distintos.

Recapitulemos pues, en el hipotético caso que la Dirección haya otorgado la responsabilidad a una persona con las habilidades y capacidades necesarias para ello ¿Qué podría estar impidiendo el adecuado desarrollo de esta importante tarea? Y la respuesta viene rápidamente en formato de otra pregunta, a la gallega. ¿Eso es todo lo que tiene que hacer la Dirección? ¿Asignar al responsable?

Con toda seguridad esa falta de documentación vendrá motivada por una sensación de pérdida de tiempo por parte de los directivos respecto de la documentación en la gestion de sus iniciativas, ya sean productos, proyectos, programas o porfolios, el jefe quiere más y lo quiere rapido, aunque sea sin especificar, detallar y pararse a pensar.
Es probable también que nuestro flamante Responsable de Documentar aunque tenga las capacidades aún no tenga las habilidades, deberíamos formarlo tanto en habilidades específicas como transversales o Soft Skils e incluso en Sistemas de Gestion del Conocimiento que le permitan lograr el fin previsto y todo ello pasa necesariamente por recursos que en la mayoría de los casos parten de la pertinente y oportuna aprobación de la dirección.
Seamos sinceros y metamos el dedo en la llaga ¿Existe en la organización una adecuada cultura enfocada a hacer las cosas correctas de la manera correcta o seguimos ofreciendo culto a la precipitación con el uso de la metodología como ASM (Al Salto la Mata) corriendo como pollo sin cabeza de manera habitual y constante?
Decía el gran William Edwards Deming que la culpa del fracaso empresarial podíamos achacarlo a muchas y muy diversas circunstancias pero que en cualquiera de los casos y siempre el motivo era el mismo: Mala Gestion. Yo desde mi mayor humildad me permito complementarlo añadiendo que esa Mala Gestion es síntoma de Desgobierno.

> **La Mala Gestión es Desgobierno.**

¿Cuánta prioridad real le da la dirección a la documentación? ¿Se trata de un nuevo calentón o de verdad va a tomaren serio el asunto? ¿Sabe que es una actitud duradera y perecedera en el tiempo? ¿Está decidida a invertir no solo esfuerzo, recursos y tiempo sino a priorizar tareas y responsabilidades frente a otras que el día a día nos ofrece o la propuesta es que hagamos esto fuera de horas de trabajo?

Respuestas que deben encontrarse en el Gobierno Corporativo y que a través de la Gobernanza deben comunicarse efectiva y eficazmente a los distintos niveles de responsabilidad y vigilar su adecuado comportamiento.
No lo olvides, la mala gestion es desgobierno y o se establecen desde la Alta Dirección las políticas, principios, marcos y normas necesarios para documentar o lo contrario y muy lamentablemente la organización seguirá desgobernada, los nuevos desarrollos seguirán siendo indocumentables y el legacy muy en contra de lo que se pretendía seguirá indocumentado.

JAVIER PERIS

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

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

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

LIVE STREAMING

Curso de
Doble Certificación

Gobierno del Tiempo y Gestión de la Productividad

Director Académico:
Javier Peris

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

MPPM® MGEIT® eGob®

Del 15 al 23 de marzo

+ 34 96 109 44 44
campus@escueladegobierno.es

Manuel Serrat Olmos

Brechas de datos: el Titanic de nuestra Seguridad y Privacidad

La segunda mitad del mes de mayo de 2024 ha sido desastrosa por lo que a las brechas de datos de personas españolas se refiere. Grandes corporaciones del IBEX 35, alguna que otra multinacional, e incluso agencias gubernamentales han reportado incidentes de este tipo, en los que datos identificativos más o menos sensibles de clientes y ciudadanos se han visto filtrados masivamente. ¿Qué hacemos ahora?

Quizá se deba a cuestiones geopolíticas, debido a la postura del Estado español frente a la invasión rusa de Ucrania, o el genocidio en Gaza. Quizá sea una simple coincidencia y varios grupos de ciberdelincuentes han materializado filtraciones casi simultáneamente, tal vez en una especie de 'pique' a ver quienes son más audaces o efectistas. Pero lo que es una realidad es que en la segunda quincena del mes de mayo diferentes organizaciones han sufrido brechas de seguridad que han supuesto la filtración de datos de, supuestamente, millones de españoles.

Empresas como Ayesa, Iberdrola, Santander o Telefónica han denunciado haber sido violentadas, o que datos de sus clientes han sido robados, generalmente, a través de otras empresas que les prestan servicios. Hablamos de filtraciones de casi un millón de personas, al parecer, la mayor de ellas, aunque el hecho de que algunas de estas empresas sean multinacionales implica que también pueden haberse filtrado datos de empresas y ciudadanos de otros países, sin estar del todo calro el alacnce de los datos sustraídos. También Ticketmaster ha denunciado el robo de datos de más de 500 millones de clientes a nivel global, y en este caso, se sabe que entre la información sustraída se encuentran datos de tarjetas de crédito. Y Decathlon también ha sufrido un ataque de este tipo en el que ya se puede considerar un mayo negro en lo que a la ciberseguridad y privacidad se refiere.

Siendo muy graves estas filtraciones, el mes terminó con la denuncia de la Dirección General de Tráfico, que investiga la Guardia Civil, de que en la Dark Web se venden los datos de 34 millones de conductores españoles y de sus vehículos, supuestamente robados a la DGT. Y no sólo se vende la base de datos completa, sino que también se venden consultas puntuales a la misma.

Como ya he explicado en artículos previos, el gran problema de estas filtraciones no es, en si mismo, el robo de los datos, sino todo lo que los delincuentes pueden hacer con ellos. Teniendo acceso a todas esas fuentes de datos, y con un trabajo de minería de datos, o alimentando una inteligencia artificial, las bandas de ciberdelincuentes pueden armar potentes campañas de suplantación de identidad o de phishing extremadamente perfeccionadas, y por tanto, con una alta probabilidad de éxito. El elevado volumen de datos sustraidos parece apuntar a que uno de los objetivos es precisamente, entrenar con ellos a inteligencias artificiales desarrolladas por esos grupo de ciberdelincuentes.

CONTINÚA EN PRÓXIMA PÁGINA

Sin ánimo de ser alarmista, con los datos filtrados en casi cualquiera de esas filtraciones de mayo, y con un poco de investigación en redes sociales, se puede fabricar un DNI español falso sin demasiados problemas. Y con ese DNI se pueden cometer muchos tipos de fraudes, sólo hace falta un poco de imaginación, sobre todo, si se combina con datos de tarjetas de crédito.

Bien es cierto que en filtraciones anteriores ya había muchos datos nuestros circulando por lugares nada recomendables, pero éstas últimas vienen a demostrar que nadie está a salvo de un ataque informático dirigido por parte de un grupo criminal adecuadamente motivado, y que el mercado de los datos robados está siempre hambriento de nuevas capturas con las que alimentar sus actividades ilegales.

Los expertos en la materia auguran una oleada de correos, SMS o llamadas fraudulentas, tratando de hacer 'picar' a las personas cuyos datos han sido recientemente filtrados, ya que la probabilidad de que esos datos sean de calidad es alta. En este asunto, los ciudadanos estamos a bordo de nuestro propio Titanic, y va a ser trabajoso esquivar al iceberg (o a legiones de icebergs) que van a ponerse en nuestro camino a partir de ahora debido a estas filtraciones.

Lo más importante es qué podemos hacer al respecto. Por supuesto, no podemos hacer desaparecer esa información del mercado negro, eso está descartado. Como ciudadanos de a pie, sólo podemos estar mucho más alerta aún, y no hacer caso a mensajes de correo electrónico que aleguen ser de compañías de las que somos clientes y en las que se alegue cualquier motivo para que rellenemos algún tipo de formulario con datos, claves, etc. Sobre todo, si se aduce algún tipo de urgencia en ello. Es decir, debemos ser mucho más vigilantes ante correos de phishing, que ahora serán mucho mejores que los que hemos venido viendo en el pasado, o mensajes en Whatsapp o Telegram o SMS con enlaces, o incluso llamadas telefónicas sospechosas.

Desde el punto de vista de los Estados democráticos, en este caso, el español, se desconoce si tienen algún tipo de plan o estrategia, no sólo para mejorar la protección de los sistemas de información, más allá del Esquema Nacional de Seguridad o la Directiva Europea NIS2. Me estoy refiriendo a que, quizá, ha llegado el momento de que no sólo nos defendamos, y que comencemos a atacar, no sólo a los grupos de ciberdelicuentes 'normales', sino también a los grupos auspiciados por gobiernos de países que están demostrando sernos hostiles. Y quizá ha llegado también el momento en que lo que ha sido una especie de ciberguerra más o menos encubierta en estos pasados años se convierta en un conjunto de acciones coordinadas con decisiones a nivel comercial y/o diplomático. Quizá ha llegado el momento de desconectar a ciertos países de Internet, y que sus empresas no puedan comerciar con las de los países que sí respetan las reglas internacionales de respeto a la legalidad y soberanía de los demás. Y por supuesto, debemos potenciar las unidades policiales que tratan con la ciberdelincuencia, de manera que, en coordinación con otros países de nuestro entorno, puedan actuar con rapidez y contundencia, incluso, a través del ataque a las infraestructuras que usen los grupos de ciberdelicuentes para sus actividades.

Por otro lado, también es urgente que nosotros, los ciudadanos, tomemos conciencia de qué es lo que está en juego cuando nuestros datos se filtran o son usados para entrenar una inteligencia artificial, y tomemos medida. Debemos responsabilizarnos más de lo que publicamos en redes sociales, publicando sólo lo imprescindible, o incluso, no publicando nada. Debemos responsabilizarnos de saber manejar enlaces recibidos por cualquier medio, y verificarlos antes de clicar en ellos. Debemos tomar conciencia como empleados de que manejamos datos de otras personas, y que de nuestra falta de profesionalidad o precauciones pueden verse negativamente afectados.

Debemos, en resumen, tomar el timón de nuestro Titanic personal y poner atención en la singladura del mundo digital. Y quien no quiera hacerlo, se hundirá en cuanto colisione con los icebergs.

Para terminar este último artículo de la temporada, me permito desearle al lector unas felices y merecidas vacaciones, y esperando que continúen siguiéndonos en la 10ª temporada de Tecnología y Sentido Común.

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

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Análisis de Negocio y Gestión por Procesos

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BPA Leader
- Certificación BPM Executive
- Módulo 2: MasterGEIT®
- Módulo 2 MasterPPM®

MPPM® MGEIT® eGob®

Del 5 al 13 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Nacho Alamillo

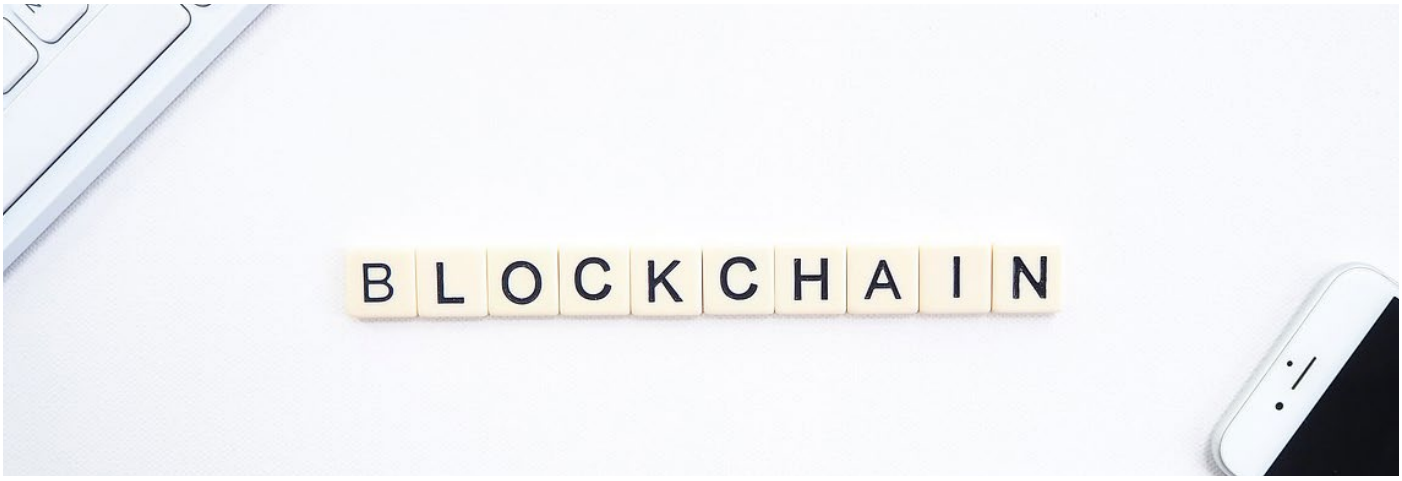
La Comisión Europea crea el consorcio para el blockchain europeo

El recientemente aprobado Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS 2), regula el nuevo servicio de confianza que denomina "libro mayor electrónico", que supone el primer reconocimiento jurídico general de las tecnologías de registro distribuido, como las cadenas de bloques (blockchains), innovación a la que ya me he referido en esta sección.

Esta novedad legislativa nació para dar cobertura jurídica al proyecto de cadena de bloques liderado por la Comisión Europea, veintiún Estados miembros de la Unión Europea y Noruega, a partir de la firma de la European Blockchain Partnership el 10 de abril de 2018, al que posteriormente se unirían otros ocho Estados, conocido como European Blockchain Services Infrastructure (EBSI).

Desde su inicio, el proyecto EBSI se ha centrado tanto en el despliegue de la infraestructura como en el desarrollo de casos de uso de la misma. EBSI ha desplegado una red piloto con más de 40 nodos repartidos por toda Europa para proyectos piloto, en particular en lo que respecta al intercambio y la verificación de credenciales relativas a ciudadanos u organizaciones en diversos sectores o áreas como la educación, el aprendizaje permanente y la seguridad social, de forma alineada con el marco europeo de identidad digital regulado en el propio Reglamento eIDAS 2, y que sustenta el Piloto de Gran Escala DC4EU. La Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) también utiliza EBSI para poner a prueba acciones de lucha contra la falsificación, junto con otros casos de uso de trazabilidad.

CONTINÚA EN PRÓXIMA PÁGINA



Como parte del Programa Europa Digital, la Comisión ha financiado también la iniciativa EBSI Nodes Expansion (EBSI-NE), una iniciativa de colaboración entre 24 organizaciones de 14 Estados europeos, todas ellas reconocidas por su experiencia en tecnologías de registro distribuido y por iniciativas anteriores de EBSI. La misión principal de EBSI-NE es fortalecer la red EBSI mediante la adición de 18 nuevos nodos validadores a la red de producción y la prestación de servicios de soporte integrales a todas las partes interesadas relevantes de EBSI; con el objetivo de acelerar la adopción de la tecnología blockchain en toda Europa.

Precisamente en EBSI-NE se están realizando los trabajos preparatorios para la eventual cualificación de la red EBSI como servicio de confianza de libro mayor electrónico, lo que permitirá la aplicación de la presunción legal prevista en el Reglamento eIDAS 2; esto es, que los registros de datos contenidos en un libro mayor electrónico cualificado gozarán de la presunción de unicidad y exactitud de su orden cronológico secuencial y de su integridad.

Una de las dificultades identificadas en su momento para poder iniciar la prestación de servicios con base en EBSI fue la ausencia de un vehículo jurídico que pudiera obligarse contractualmente con los nodos, con los usuarios del servicio y responder frente a terceros. Ello es preciso, además, para disponer de una entidad con personalidad jurídica que pueda actuar como prestador de servicios de confianza, a los efectos del Reglamento eIDAS.

La solución a dicha dificultad ha venido de la mano de la creación, mediante la Decisión de Ejecución (UE) 2024/1432 de la Comisión, de 21 de mayo de 2024, por la que se crea el Consorcio Europeo de Infraestructuras Digitales para la Asociación Europea de Cadenas de Bloques y la Infraestructura Europea de Cadena de Bloques para los Servicios (EUROPEUM-EDIC).

El Consorcio Europeo de Infraestructuras Digitales (EDIC, en inglés) es un nuevo tipo de persona jurídica prevista en la Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030, que forma parte de los instrumentos de ejecución de proyectos plurianuales por parte de los Estados miembros.

El EDIC adquiere personalidad jurídica desde la entrada en vigor de la Decisión de la Comisión que los crea y tiene, en cada Estado miembro, la capacidad jurídica más amplia reconocida a las personas jurídicas por la legislación de dicho Estado miembro.

En el EUROPEUM-EDIC, acogido por Bélgica, participan Croacia, Chipre, Grecia, Italia, Luxemburgo, Portugal, Rumania y Eslovenia, mientras que Polonia ha manifestado su interés, y se ocupará de establecer y gestionar EBSI para prestar servicios transfronterizos a escala de la Unión, en particular servicios públicos, deapoyar la cooperación transfronteriza entre autoridades públicas en materia de tecnologías descentralizadas y de facilitar la interoperabilidad de las soluciones basadas en dichas tecnologías descentralizadas.

Cabe felicitarse por el éxito que supone este hito, que por fin ha de permitir disponer en Europa de cadenas de bloques fiables, resilientes y con valor jurídico pleno.

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

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Proyectos

OpenPM² (PjM) + ISO 21502

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PjM) Executive
- Certificación ISO 21502 Leader
- Módulo 3: MasterGEIT®
- Módulo 3 MasterPPM®

MPPM® MGEIT® eGob®

Del 19 al 27 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Miguel Angel Arroyo

Analizando los comportamientos de nuestros adversarios

En artículos anteriores de esta sección ya hemos mencionado la importancia de contar con un programa de inteligencia en amenazas dentro de la organización ya que es la única forma de poder hacer una evaluación eficaz del riesgo e implantar medidas de seguridad que reduzcan la probabilidad de que una amenaza se materialice o que, en caso de materializarse, reducir su posible impacto. El objetivo siempre es el mismo; reducir el riesgo.

A través de artículos o informes de fabricantes especialistas en inteligencia en amenazas podemos aprender a identificar los comportamientos de los adversarios, analizarlos y extraer conclusiones interesantes en relación a las tácticas, técnicas y procedimientos (TTP) utilizados por estos adversarios, una información que resultará muy útil a la hora de elaborar un programa de seguridad o plan de tratamiento para dar respuesta a las técnicas ofensivas usadas, ya que incluirán técnicas defensivas más eficaces en base a la información de valor (inteligencia) obtenida durante el proceso.

CONTINÚA EN PRÓXIMA PÁGINA

El enfoque aquí propuesto es basándonos en los comportamientos, que serán las tácticas utilizadas por los adversarios. MITRE ATT&CK, del cual ya hemos hablado en esta sección, cuenta con diferentes matrices para agrupar las tácticas y técnicas ofensivas utilizadas.

Tomaremos como ejemplo la matriz ENTERPRISE, y las 12 tácticas que van desde el "*Acceso inicial*" (INITIAL ACCESS) hasta el "*Impacto*" (IMPACT).

La idea es que, a través de la información facilitada por los analistas en los diferentes artículos e informes que comparten podamos ir identificando las diferentes fases que han ido ejecutando durante su ataque, intentando plasmarlas en un orden cronológico y alineándolo con el famoso CYBER KILL CHAIN (*ciber cadena de la muerte*).

Veamos un pequeño ejemplo para entender el enfoque y cómo extraer la información de valor que nos permita identificar tácticas y técnicas. Centrémonos en el siguiente extracto de un informe:

The vector of the infection, similarly to other APT28 / FancyBear attack, is a spear phishing email delivering a Word Office document with a significant name, often related to International Conferences or other events involving several countries. As expected, the document triggers a MACRO function able to extract a Microsoft Dynamic Link Library (DLL) which acts as downloader of a SkinnyBoy dropper (tdp1.exe) from a first dropurl.

En el extracto anterior se puede observar el nombre del grupo APT que estamos analizando, en este caso el APT28 o FancyBear. Como se puede ver, el acceso inicial se produce a través del envío de un *phishing* dirigido (*spear phishing*) con un documento adjunto. En las dos primeras frases del párrafo se puede extraer que para la táctica de INITIAL ACCESS, el grupo APT28 utilizaba *spear phishing*.

El phishing está etiquetado como la técnica T1566 (dentro de MITRE ATT&CK) y el *spear phishing* concretamente es una subtécnica, que dependiendo de si el correo incluye un adjunto o un enlace, se identifica de una manera diferente. En este caso, se trata de un *spear phishing* con adjunto, por lo tanto, estaríamos hablando de la subtécnica T1566.001.

El fichero adjunto incluye una macro capaz de extraer una librería DLL que actúa como herramienta para la descarga de otros ficheros maliciosos necesarios para continuar el ataque.

Esto es solo un pequeño ejemplo como, a partir de informes compartidos por fabricantes y analistas independientes, podemos extraer información muy valiosa que, tras ser debidamente procesada, nos puede ayudar a tomar las mejores decisiones a la hora de implantar medidas eficaces de seguridad.

En este sentido, el propio MITRE ATT&CK nos propone, por cada técnica, diferentes mecanismos para la detección de la técnica y su mitigación. Información que puede ser completada si además de MITRE ATT&CK utilizamos MITRE D3FEND para identificar técnicas ofensivas para contrarrestar las técnicas ofensivas identificadas.

En el ejemplo que acabamos de ver, y para la subtécnica de *spear phishing* con adjunto, algunas medidas de seguridad recomendadas puede ser la capacitación y concienciación de usuarios para identificar correos maliciosos, bloquear correos entrantes con adjuntos que puedan contener macros, aplicar el principio de mínimo privilegio para los usuarios o la segmentación de las redes para minimizar el impacto en caso de que se llegue a ejecutar el código malicioso.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

MIGUEL ANGEL ARROYO

Miguel Ángel Arroyo es consultor de seguridad de la información, con certificación CISA de ISACA y 15 años de experiencia en el mundo de la ciberseguridad. Experiencia en auditorías de seguridad e implantación de SGSI (ISO/IEC 27001). Desempeña la labor de Director de Ciberseguridad, liderando la estrategia de seguridad para la gestión de riesgos IT. Es Responsable del Comité de Cordoba y Co-Líder del Grupo de Expertos de Seguridad en la Asociación itSMF España. Profesor en varios másteres de ciberseguridad (UCLM, Universidad de Sevilla y Universidad de Córdoba). Es autor del blog hacking-etico.com, fundador de Hack&Beers y ponente en congresos de ciberseguridad de ámbito nacional.

LinkedIn:
https://www.linkedin.com/in/miguel-angel-arroyo-moreno

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

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Programas

OpenPM² (PgM) + ISO 21503

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PgM) Executive
- Certificación ISO 21503 Leader
- Módulo 4: MasterGEIT®
- Módulo 4 MasterPPM®

MPPM® MGEIT® eGob®

Del 3 al 11 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Juan Carlos Muria

2024. El verano de los riesgos de la IA

En nuestra sección Diario de una tortuga ninja hemos hablado en anteriores ocasiones sobre los riesgos de la inteligencia artificial (IA) y su impacto social, pero hoy nos detendremos en las nuevas ciberamenazas que surgen en el uso de sistemas de IA.

Y es que con la resaca de los recientes ciberataques a grandes empresas, ahora debemos prepararnos para una segunda mitad del año que puede ser "caliente" en lo que a ciberataques se refiere, y no solo hablamos de ciberataques "tradicionales" sino que con la inteligencia artificial se abren nuevos escenarios para los que debemos estar preparados.

Organizaciones como MITRE u OWASP, desde sus diferentes perspectivas, tienen ya unas taxonomías definidas de nuevas estrategias de ataque sobre los sistemas de aprendizaje automático o inteligencia artificial y esto es lo que abordaremos a continuación, así como las mejores prácticas para evitarlos.

En primer lugar, tenemos que ser conscientes de que los ataques que pueden realizarse son de cuatro tipos: ataques durante la fase de desarrollo, ataques durante la fase de entrenamiento, ataques de caso de uso y ataques al sistema.
En la fase de desarrollo los ataques pueden ir dirigidos a alterar el comportamiento del modelo de IA o a vulnerar la confidencialidad del propio modelo o incluso de los datos de prueba. En definitiva, son variantes de ataque de tipo cadena de suministro que debemos conocer y tomar medidas para evitar que ocurran.
En la fase de entrenamiento el foco debe estar en los datos, en evitar que ocurran brechas de datos que pongan en riesgo la privacidad o la confidencialidad de estos datos, o bien que una alteración de estos datos de entrenamiento produzca un comportamiento erróneo del modelo, algo que se conoce como envenenamiento de datos.

En cuanto a casos de uso (o de mal uso, para ser más precisos), pueden producirse ataques adversarios, robos de modelos, ingeniería inversa del modelo, ataques para que el modelo revele datos confidenciales de personas o de organizaciones, inyecciones de código, o inferirse la identidad de una persona o una organización a partir de la interacción con el sistema de IA, entre otros tipos de ataque.

CONTINÚA EN PRÓXIMA PÁGINA

> Con la inteligencia artificial se abren nuevos escenarios de ataques para los que debemos estar preparados

> Seamos activistas de la IA, defendamos su desarrollo rápido y sencillo pero también responsable y seguro

Para finalizar, sobre el sistema de IA en ejecución pueden hacerse otro tipo de ataques más tradicionales, como saltarse los controles de acceso al modelo, comprometer plugins de terceros, ataques de denegación de servicio, etc.

En los tiempos actuales, donde hay un ambiente bélico con gobiernos que piden "dañar la economía, las instituciones y gobernantes, el bienestar de los ciudadanos y su confianza en el futuro", y afirman que "hay que encontrar problemas en sus tecnologías críticas y golpearlas sin piedad", es obvio que debemos proteger especialmente estos sistemas de IA que cada vez están más presentes en el día a día de sectores como la salud o la seguridad.

Por otro lado la Ley de Inteligencia Artificial de la UE pide para los sistemas de IA de alto riesgo que exista un sistema de gestión de riesgos, una gobernanza de datos, una documentación técnica que demuestre que el sistema de IA cumple los requisitos de la ley y que proporcione información para que las autoridades comprueben su cumplimiento, un registro automático de eventos (log) con unas características determinadas, que sea transparente y explicable (Considerando 27), que cuente con una supervisión humana que permita incluso detener su funcionamiento, y que sea robusto, preciso y ciberseguro.

Por ello, y para evitar en la medida de lo posible todas estas amenazas, la clave está en poner en marcha una buena gobernanza de IA, implantando procesos de gobierno para los riesgos que introduce el uso de sistemas de IA, así como considerar estos nuevos sistemas dentro de los procesos de seguridad de la información y el ciclo de vida del software.

También debemos aplicar controles de seguridad tradicionales sobre el sistema de IA, ya que no deja de ser un sistema de información, aplicando estos controles también a la cadena de suministro y seleccionando, eso sí, los activos a monitorizar del sistema de IA que estamos utilizando.

Es fundamental también que en los entornos donde se desarrolla la ciencia de datos adoptemos también medidas de seguridad, tanto sobre los datos con los que se trabaja como sobre los algoritmos que se aplican para analizar estos datos: la calidad de los datos de entrada, la representatividad, filtrado, etc. deben ser evaluados continuamente para evitar manipulaciones que corrompan los resultados.

Así pues, si en el artículo anterior explicábamos que la aparición de normas y regulación sobre la IA era un síntoma de que esta tecnología comenzaba a estar madura para aplicarla, la aparición de nuevas estrategias de ataque sobre estos sistemas de IA es también un síntoma de esa madurez, pero si no adoptamos de forma exhaustiva y metódica medidas y controles de protección de estos sistemas podemos ser muy vulnerables.

Nos espera un futuro prometedor, lleno de riesgos, pero también repleto de oportunidades para la sociedad de la que forman parte ustedes lectores, y nuestra tortuga ninja. Seamos activistas de la IA, defendamos su desarrollo rápido y sencillo pero también responsable y seguro.

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

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Service Management FitSM + ISO 20000

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación FitSM Executive
- Certificación ISO 20000 Leader
- Módulo 5 MasterGEIT®
- Módulo 5 MasterPPM®

MPPM® MGEIT® eGob®

Del 17 al 25 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Elena Liria Fernández

Elena Liria es desde 2019 consejera delegada de Madrid Digital (Agencia para la Administración Digital de la Comunidad de Madrid). Nació en Bilbao y se enamoró de la capital desde que se afincó en ella en 1997. Estudió Ingeniería Informática en la Universidad de Deusto, donde empezó la carrera en el año 1991 y el último curso lo hizo en Francia en la École National Supérieure des Telécommunications (ENST), Telecom Bretagne, donde también realizó un Máster ISIC (Ingénierie des Systêmes Informatiques Communicants). Cuenta con más de 27 años de experiencia en el sector tecnológico en los ámbitos público y privado. Es madre de dos niñas de 15 y 13, de un niño de 10 y líder indiscutible de su sector. En 2021, Elena Liria recibió el premio CIONET de Líderes Digitales Europeos a la Mejor Líder Digital de España.

En 2024 recibió el Premio Profesional Ingeniera Informática en los II Premios Nacionales de Ingeniería Informática 2024. Tiene formación en liderazgo para la Innovación por el MIT y el programa del IESE de Consejos de Administración.

CONTINÚA EN PRÓXIMA PÁGINA

REVISTA
Tecnología & Sentido Común
https://tecnologiaysentidocomun.com

Elena, háblanos de tu trayectoria profesional

Empecé mi carrera profesional en Madrid, en 1997, en el sector de la consultoría, primero en IECISA y después en DMR Consulting, actual NTT Data, donde fui gerente de Telecom y de Administraciones públicas.

En consultoría, pude crecer como profesional y obtener experiencia multinacional en la dirección de proyectos de tecnología de grandes clientes. Como gerente, me ocupaba del desarrollo de negocio de los clientes asignados y la dirección global de proyectos, sobre todo en el sector de Telecom. Siempre pienso que la consultoría es la mejor formación para nuestra profesión y una gran oportunidad de aprendizaje constante.

Tras nueve años en el sector privado, en septiembre de 2005 me incorporé a la Agencia de Informática y Comunicaciones de la Comunidad de Madrid (actualmente Madrid Digital), como personal laboral fijo. Desde entonces he desempeñado distintos puestos directivos, gestionando actuaciones y proyectos estratégicos para varias consejerías de la Comunidad de Madrid. Destacaría especialmente los años en los que fui responsable de la Dirección de Innovación y Transformación Digital, posición que me permitió conocer en profundidad el estado del arte en cuanto a la transformación digital y su aplicación en beneficio de los ciudadanos. Tras cuatro años al frente de esta Dirección, en noviembre de 2019 fui nombrada consejera delegada de Madrid Digital.

Como consejera delegada de Madrid Digital, desde hace cinco años, gestiono y dirijo una empresa pública de 650 personas, con un presupuesto de 439M€ (incluido Fondos UE), que gestiona a diario más de 1.600 aplicaciones para trámites administrativos, toda la red de comunicaciones de la Comunidad de Madrid que conforman más de 4.600 sedes: edificios públicos; centros educativos; centros de salud, hospitales y todos los puestos de trabajo digitales para los más de 180.000 empleados públicos. Todo un reto.

¿Cómo fueron tus comienzos en el mundo de la Administración Pública?

En septiembre 2005, decidí dar un cambio profesional al sector público, inicialmente, buscando conciliar mejor mi vida personal con la profesional. Preparé un concurso oposición y saqué una plaza de personal laboral en la Agencia que hoy dirijo.

Desde el momento que empiezas a trabajar en el sector público, te das cuenta del impacto que tiene para la sociedad y para mejorar la vida de las personas. El servicio público es algo que engancha, la dimensión e impacto social de los proyectos a los que nos enfrentamos no tiene comparación.

CONTINÚA EN PRÓXIMA PÁGINA


ECONOMÍA
TRANSPORTE
HACIENDA
JUSTICIA
SANIDAD
DEPORTES
INF
AS

En la Comunidad de Madrid, desde el inicio, tuve la oportunidad de asumir puestos de responsabilidad y participar en proyectos muy relevantes. Como directora de servicios, fui responsable de las actuaciones y proyectos de Madrid Digital ante las Consejerías de varios ámbitos (Economía y Hacienda; Educación; Políticas Sociales; Sanidad; Empleo; Turismo y Cultura; Transportes; Vivienda; Medio Ambiente), participando en proyectos tan relevantes como la Plataforma Integral de Atención a la Dependencia o la Modernización de los Sistemas de Información e Infraestructuras de Centros Educativos. En 2015, asumí la dirección de innovación y transformación digital, donde pude elaborar la estrategia digital de la agencia y de la Comunidad de Madrid y desarrollar las líneas de negocio de innovación y digitalización que hoy están consolidadas (CX; omnicanalidad; datos e inteligencia artificial; cloud; blockchain; etc.).

En cuanto a la conciliación, tengo que reconocer que no siempre lo consigo, y desde que soy CEO mucho menos. En Madrid Digital, dedicamos mucho tiempo y esfuerzo para conseguir dar un buen servicio a la Comunidad de Madrid y lograr los objetivos marcados.

¿Cuáles son los retos más importantes a los que te has enfrentado al frente de Madrid Digital?

Agradezco mucho a la Comunidad de Madrid la oportunidad que me ha dado de liderar Madrid Digital durante tres legislaturas, en ellas he podido enfrentarme a grandes retos y trabajar en entornos muy diversos desde entonces.
La primera legislatura estuvo marcada por la crisis del COVID, con los retos que supuso en materia de infraestructuras y Comunicaciones de Hospitales y Centros Sanitarios, y en la dotación y gestión de infraestructuras y soluciones para el trabajo en remoto de los empleados públicos de la Comunidad de Madrid y todos los proyectos TIC derivados de la crisis: Línea de Ayudas COVID-19; ERTEs; Desempleo; Conciliación Telemática; Mesas virtuales de contratación; Vistas Judiciales; etc.

A partir del 2021, nos enfocamos en el liderazgo de la transformación digital y en la digitalización de la Administración de la Comunidad de Madrid, un proyecto apasionante, de larga duración, que va a suponer un antes y un después en la interacción del ciudadano con la administración y en la propia gestión pública. Tenemos el objetivo de lograr una administración digital 100% y para ello estamos lanzando grandes proyectos que precisan transformar, personas, culturas, procedimientos administrativos, procesos, etc.

Este proyecto se afianzó en junio de 2023 con la creación de la Consejería de Digitalización que dirige nuestro consejero, Miguel López-Valverde y que es la primera consejería en España que dirige y gestiona todos los activos digitales para la digitalización de la región (economía, sociedad y administración) y aquí nuestra agencia tiene un papel clave en todo lo que atañe a la digitalización de la administración de la Comunidad de Madrid.

CONTINÚA EN PRÓXIMA PÁGINA


adriddigital

¿Qué logros destacarías de tu carrera profesional?

A lo largo de los años, he tenido la suerte de participar en proyectos muy relevantes y asumir grandes retos, tanto en el ámbito privado, como en el público.
Dentro de la Comunidad de Madrid, si tuviera que destacar uno, sería la gestión de la crisis del COVID. En marzo 2020, nos enfrentamos a una crisis sin precedentes, yo estaba recién nombrada consejera delegada de Madrid Digital, y los retos a los que nos enfrentamos fueron enormes: dotar de infraestructuras y puestos a nuevos hospitales, hoteles medicalizados, IFEMA; montar en tiempo récord el teletrabajo para todos los empleados público de servicios críticos, seguir manteniendo el servicio y crear servicios con sus sistemas de soporte de la noche a la mañana. El equipo de Madrid Digital trabajó 24x7 durante más de 2 meses. De esa etapa aprendí, la generosidad, la solidaridad, la capacidad infinita que tenemos las personas para trabajar y colaborar cuando nos une y nos supera una motivación tan grande. Sin duda, dirigir la Agencia en aquellos momentos y conseguir unos resultados satisfactorios de aquella gestión creo que es uno de los logros de los que más me siento orgullosa.

¿Qué es lo que más te gusta de tu profesión?

La capacidad de crear y poder cambiar las cosas. En el ámbito público sobre todo es ver cómo tu trabajo ayuda a crear servicios públicos para ciudadanos y empresas y cómo con tu trabajo puedes ayudar a mejorar la vida de las personas. Hay experiencias de trabajo vividas que me han aportado mucho como persona y que nunca las olvidaré.

Háblanos de Madrid Digital, sus objetivos y retos

El gobierno de la Comunidad de Madrid, con la creación de la Consejería de Digitalización, está haciendo una gran apuesta por la digitalización, tanto de la región como en clave interna de la Administración. Nuestro objetivo es que Madrid sea la región más digitalizada de Europa y alcanzar una administración digital 100%. Para ello en 2022 desarrollamos un plan estratégico con 5 ejes de actuación: Innovación para una Administración Digital; Gestor y Empleado Público Digital; Infraestructuras, Soluciones y Arquitecturas Digitales; Ciberseguridad y Seguridad de la Información; Transformación de Madrid Digital.

CONTINÚA EN PRÓXIMA PÁGINA

¿Cómo se gestiona Madrid Digital? ¿Cuáles son sus órganos de gobierno?

Madrid Digital es la entidad pública que provee y administra los recursos de informática y comunicaciones en la Comunidad de Madrid. Dispone de un Consejo de Administración, presidido por el Consejero de Digitalización que cuenta con la representación de todas las Consejerías de la Comunidad de Madrid a través de sus Secretarios Generales Técnicos, y de las Direcciones Generales que tienen competencias transversales relevantes para la digitalización.

Madrid Digital tiene la misión de impulsar la transformación digital de la Comunidad de Madrid mediante la innovación tecnológica y la gestión eficiente de los recursos que la administración pone a nuestra disposición. Nuestros valores se centran en la orientación al ciudadano y al empleado público, en la inquietud constante por la innovación y simplificación y en principios éticos y de transparencia.

Nuestro modelo de trabajo está estrechamente relacionado con las necesidades de las distintas Consejerías que conforman la Comunidad de Madrid. La organización dispone de un modelo matricial en el que toda la cadena de valor se orienta hacia la gestión y prestación de servicios a las consejerías. Los equipos de Madrid Digital gestionan la demanda que las distintas Subdirecciones Generales de la organización ejecutan y operan.

La Comunidad de Madrid, cuenta con un Consejo Asesor de Transformación Digital, iniciativa pionera dentro de la administración, al que solicitamos asesoramiento sobre modelos de provisión o gestión de servicios tecnológicos. Su colaboración nos brinda información sobre las tendencias, riesgos y oportunidades que se plantean, lo que nos facilita adecuar mejor nuestras necesidades a las capacidades del mercado.

¿Cuáles son los Programas y Proyectos más relevantes que estáis llevando a cabo?

Desde Madrid digital trabajamos con más de 300 proyectos, de los que estratégicos son unos 80 en distintos ámbitos de la Comunidad de Madrid. Destacamos los financiados por el Mecanismo de Recuperación y Resiliencia. Algunos de los proyectos más relevantes son la Cuenta Digital del Ciudadano, Justicia Digital e Historia Social Única, además de la Estrategia de Inteligencia Artificial y Ciberseguridad.

El proyecto INNOVA, en el ámbito de innovación, se ocupa del rediseño de los servicios públicos digitales que se irán incorporando al nuevo canal de interacción con el ciudadano que conforma la Cuenta Digital. En Justicia Digital se agrupan todos los proyectos dirigidos a la transformación digital de la Justicia como son el Expediente Judicial, Inteligencia Artificial a plicada a l a gilización de la justicia o el escritorio judicial. También hay que destacar el proyecto de Historia Social Única y Teleasistencia Avanzada, que proporcionará mayor coordinación y seguimiento en la atención a las personas usuarias de los servicios sociales.
En Inteligencia Artificial tenemos más de 16 casos de uso en ámbitos como Justicia, Economía o Vivienda, y la Estrategia de Inteligencia Artificial se ha desarrollado para disponer de un Hub de Servicios Analíticos que nos permita extrapolar las soluciones desarrolladas de forma ágil a distintos ámbitos.

Elena, muchas gracias por habernos concedido esta entrevista y enhorabuena por la labor que realizáis desde Madrid Digital. Estáis siendo un referente en las Administraciones Públicas.

Muchas gracias a vosotros, Javier, por la oportunidad de brindarme este espacio en vuestra revista. Aprovecho para daros la enhorabuena por la labor divulgativa que realizáis.

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

LIVE STREAMING

Sesión de Formación y Certificación en:

Sistema de Gestión de la Inteligencia Artificial

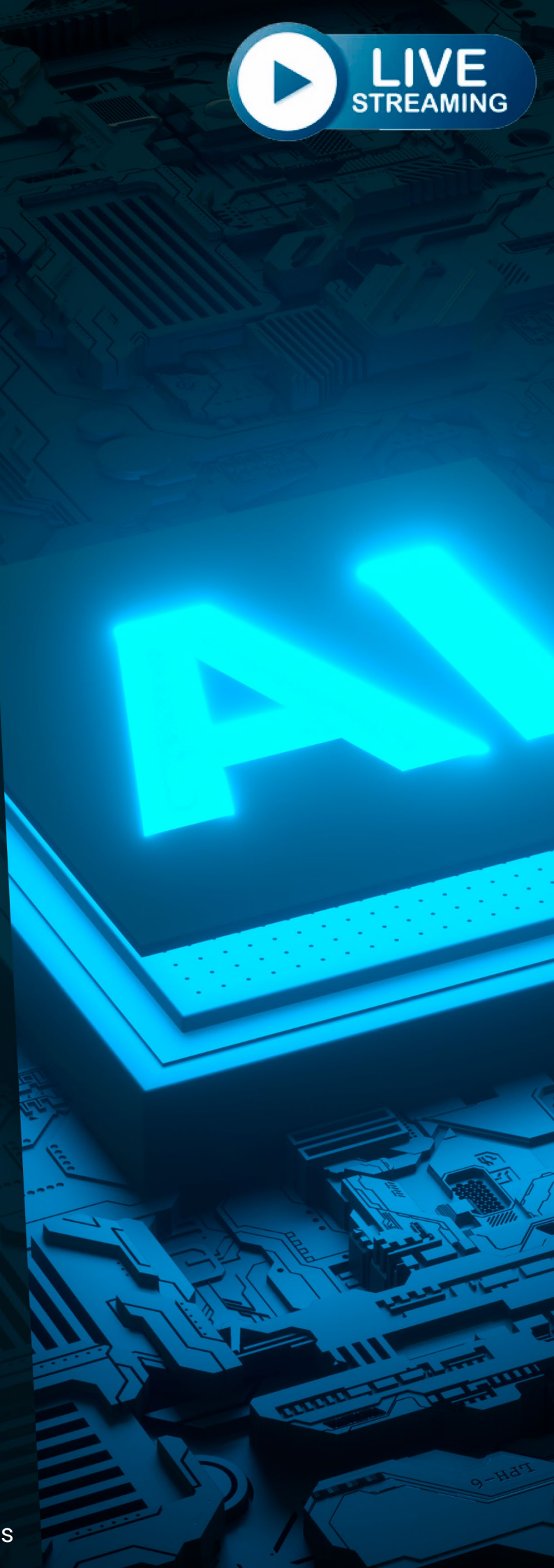
Director Académico:
Javier Peris

- Duración 5 horas
- Sesión única
- Miércoles de 16:00 a 21:00 horas
- En Directo y en Remoto
- Basado en la norma ISO 42001:2023
- Examen de Certificación Incluido
- Certificación ISO 42001 Leader
- Plazas limitadas

MPPM® MGEIT® eGob®

Miércoles 10 de Abril

+ 34 96 109 44 44
campus@escueladegobierno.es



Marlon Molina

El freno a la Inteligencia Artificial es tendencia

La Inteligencia Artificial es el tema de moda en cualquier conversación, en la prensa, y en los congresos tecnológicos y los no tecnológicos. Uno de los principales temas es la preocupación por lo que los humanos no puedan controlar, básicamente la cuestión ética.

Actualmente existe más de una visión, que podría resumirse en dos grupos: quienes no entienden la IA y por lo tanto tienen miedo y tienden a pensar que la solución a su falta de conocimiento es crear leyes; y los grupos que conocen la IA porque han escrito código y creado sistemas, y creen que debería acelerarse la adopción aunque de forma estratégica.

Creo que el punto intermedio está en la prudencia antes de conectar cualquier sistema. No parece irracional pedir que se piense antes de actuar. El estrés lo crea la competencia que tiene cualquier empresa, si su competidor no frena y por el contrario acelera, entonces la empresa entra en pánico entendiendo que se quedará fuera de la ola de la tecnología, pero también deben pensar que su competidor probablemente "meta la pata" y sufra un problema de seguridad, o deje los sistemas inestables, lo cual le daría una ventaja competitiva.

Mi propia opinión es la misma que llevo exponiendo desde hace mucho tiempo, la cual se divide en dos: anticiparse, y aprender a nadar para no morir en la piscina.
Para la mayoría de las empresas que no llevan al menos cinco años investigando con la IA y haciendo pequeñas integraciones, este momento les deber parecer un poco mágico, pero lo que les debería parecer es peligroso (no porque quiera conquistar el mundo, peligroso porque la ciberseguriad). Por otro lado, el consejo que debe recibir es que llegado el verano todo el mundo quiere darse un chapuzón en la piscina, y la mejor forma de proteger a los más jóvenes es enseñándoles a nadar, dominar el agua, y ser prudentes.

CONTINÚA EN PRÓXIMA PÁGINA

Hace un año Steve Wozniak y Elon Musk pidieron poner una pausa general a la tecnología generativa para que la sociedad tuviera la oportunidad de pensar y planificar. Desde luego no hubo eco en la petición, así que nadie paró las máquinas.
Expertos como Geoff Schaefer quien asesora al gobierno de los Estados Unidos, llaman a ser cuidadosos con lo que se conecta a los sistemas de producción, y especialmente prudentes con los datos que se usan para entrenar y generar patrones. Schaefer dice ser "un optimista de la IA, pero cree que controlarla no es posible ni deseable".

Crecimiento de los proveedores
Mientras los proveedores están creciendo en ventas, los reguladores y creadores de leyes aceleran los mecanismos para parar el desarrollo, al menos en Europa.
En junio, Oracle anunció un incremento del 6% de sus ingresos anuales gracias a la IA, Nvidia ha escalado puestos entre las empresas más valoradas, y Apple anunció la "tontería" de poner IA debajo de iOS y con esto consiguió recuperar el primer puesto como la empresa más valorada, después de todo no son los expertos quienes comprar sus valores en bolsa, sino el público en general, y en general los gestores de carteras que analizan gráficos.
Desde luego quien está liderando las ventas es Microsoft, que está creciendo en sus ingresos a un ritmo de 15% trimestral. Compró casi el 50% de OpenAI, la empresa desarrolladora y dueña de ChatGPT, el modelo más famoso de IA Generativa.

Meta acelera, frena, acelera y desacelera
Meta envió un mensaje a sus usuarios que muchos mal interpretaron, la mayoría cree que Meta le está preguntando si puede o no usar todos los datos que le ha dado hasta hoy para entrenar sus sistemas de IA. No era una pregunta, sino un aviso. Como si fuera poca cosa, el aviso era solo condicionante para futuros datos, ya que los previos se dan por sentado que se podrán usar, en caso de que el usuario manualmente cambie la configuración, servirá para evitar que se usen sus datos a partir de la fecha en la que se haga dicho cambio en la configuración.
Meta anunció en junio que retrasaría el lanzamiento de sus modelos de inteligencia artificial en Europa después de que los reguladores de privacidad irlandeses le ordenaran retrasar su plan para utilizar datos de los usuarios de Facebook e Instagram.

Regulación excesiva
Todos los países y regiones se proponen a sí mismos como líderes del desarrollo y avance de la Inteligencia Artificial, sin embargo, en una carta abierta firmada por miembros de Digital Europe, el grupo advirtió que la regulación excesiva de la industria de la IA podría afectar negativamente la capacidad de la región para convertirse en un líder mundial en la tecnología.
La Comisión Europea ha hecho los cálculos mal. Se siente muy orgullosa de poder decir que es pionera en legislar para la IA, algo que en realidad debería causarnos una gran vergüenza. Primero porque ser pioneros en legislación no indica ningún avance,

segundo porque el objetivo debería ser liderar el desarrollo y la investigación, y finalmente porque sin ninguna duda, los reguladores de la Unión Europea se han esforzado para detener el desarrollo y seguir dependiendo de lo que se hace fuera de la UE.

Digital Europe también afirma que la carga financiera que podría suponer para las empresas que quieran llevar al mercado productos basados en IA podría ser insostenible para las pequeñas empresas, y reducir la competitividad de las empresas desarrolladoras europeas.

En junio, 163 destacados ejecutivos que representaban a algunas de las mayores empresas tecnológicas y empresariales de Europa, como Airbus, ARM, Capgemini, Schneider Electric y Siemens, firmaron una carta abierta en la que instaban a la UE a adoptar un enfoque más de no intervención en la regulación de la IA, preocupados de que el proyecto de Ley de IA hiciera que el continente fuera menos competitivo en este campo de rápido crecimiento.

Así volvemos al principio del artículo. En los próximos meses veremos principalmente a las personas que no han estudiado inteligencia artificial y que no programan pedir regulación, y ser estrictos con la regulación, y a quienes sí son técnicos pedir bajar las revoluciones.

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/

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de
Doble Certificación

Seguridad de la Información

CSX + ISO 27001

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación CSX Executive
- Certificación ISO 27001 Leader
- Módulo 6: MasterGEIT®

MGEIT® eGob®

Del 7 al 15 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

Ricard Martínez Martínez

Innovar es cosa de todos: lecciones aprendidas en WAIQ Summer Course 2024

Por segundo año el Real Colegio Complutense en la Universidad de Harvard ha acogido el curso Web3, AI and Quantum Computing (WAIQ) se trata de una iniciativa en la que profesionales de muy distintas procedencias y estudiantes en formación hemos tenido la oportunidad de abordar el futuro inmediato de estas tecnologías. Las aulas de la Harvard Law School han acogido un debate con un alto nivel en el que ponentes y participantes han creado un marco de diálogo altamente creativo y no exento de intensidad emocional. Quiera finalizar el curso de Tecnología y Sentido Común alguna de las significativas lecciones aprendidas.

En primer lugar, resulta altamente enriquecedor poder sentar a una misma mesa investigación, innovación, tecnología y derecho. Surgen muchos puntos de encuentro que demuestran la importancia de incorporar la cultura del cumplimiento desde el diseño al ADN de las organizaciones. Sin embargo, por favor absténganse juristas tradicionales, profetas del moverse rápido y romper cosas y científicos descreídos. Porque ninguna de estas actitudes tradicionales conduce a buen puerto. En WAIQ la descripción del marco jurídico que nace era considerado desde un enfoque de código, de requerimiento para el diseño. Y otro tanto sucedió con los valores éticos. A un tiempo, desde el punto de vista jurídico se hizo indispensable un esfuerzo de entendimiento de la realidad.

La falsa dicotomía entre derecho e innovación debería ser rechazada y descartada. En realidad, es muy probable que el mantra de la Unión Europea como paraíso regulador que limita la innovación deba ser revisado desde otros puntos de vista. A mi juicio, el problema no reside en la disciplina del llamado paquete digital de Reglamentos y Directivas. Estas normas tienen de una parte una enorme componente reactiva. Es muy probable que sin el problema del "olvido", el dumping normativo y el establecimiento en jurisdicciones "débiles", o la monetización de nuestros datos personales, el Reglamento General de Protección de Datos hubiera sido innecesario.

Pero es indiscutible que todos estos hechos han sucedido. Y es posible que sin Cambridge Analytica y el lanzamiento masivo de ChatGPT el Reglamento de Inteligencia Artificial fuera otra cosa.

Por otra parte, todas estas normas son funcionales a proyectos muy precisos de la la Unión Europea en el Programa de Década Digital y en la ejecución de políticas instrumentales en el ámbito de los espacios de datos o la inteligencia artificial. Puede que se apunte un cierto repunte proteccionista, pero debemos entender que la UE trata de definir su propio espacio de desarrollo público y privado en un entrono muy fluido y cambiante. Sea cual fuere la razón para ello, el marco jurídico deviene un requerimiento indispensable para el desarrollo de las tecnologías digitales.

Respecto de estas últimas resulta fascinante apreciar su estado de desarrollo y madurez y los mundos que anuncian. La probablemente mal llamada inteligencia artificial está cada vez más presente, al punto de ser una herramienta cotidiana para una parte significativa de la población se sea consciente o no. En WAIQ tuvimos ocasión de departir con cierta profundidad los compromisos empresariales que supone, las oportunidades para el país y las condiciones de despliegue y adopción. Desde el punto de vista del jurista, al margen de una lógica preocupación por el futuro de la criptografía, resultó de altísimo interés apreciar las potenciales interacciones de futuro entre la computación cuántica y la inteligencia artificial. Particularmente como la altísima capacidad de cálculo puede acelerar los procesos y, al mismo tiempo, los algoritmos pueden empujar la programación y la eficiencia en la computación cuántica. Ello sin contar con el fascinante mundo de las arquitecturas de hardware cuyas distintas opciones causan una sensación similar a la contemplación de la Sagrada Familia o la Gran Pirámide.

CONTINÚA EN PRÓXIMA PÁGINA

Por otro lado, el mundo WEB 3 ofrece tantas formas de concebir lo digital como escenarios seamos capaces de imaginar. Desde el mundo financiero y la contratación, a los entornos de juego y socialización pasando por casi cualquier mundo que se pueda imaginar. Y además, en algunas presentaciones con un sustrato libre y libertario y un compromiso social que te devuelve a aquella Internet que parecía haberse ido para siempre.

Finalmente, resulto emocionante apreciar como organizaciones de todo el orbe y de cualquier tamaño imaginable, muchas de ellas de nuestro país, han integrado distintas estrategias de innovación de diverso tipo buscando ser mejores y más comprometidas con su entorno. No parece un camino sencillo, cada uno debe recorrerlo desde su cultura interna, o a fuerza de cambiarla, abordando un escenario de avance científico y tecnológico acelerado. Y ello obliga a reclamar políticas públicas y estrategias empresariales en España que consoliden nuestro talento y aseguren un despliegue que alcance a todos los segmentos.

Y la lección final es propia. Las organizaciones no pueden desplegar la innovación tecnológica desde la asunción de que al no haberse regulado su "gadget" no hay límites. El marco de los derechos fundamentales, la responsabilidad de no hacer daño y responder por el que se causara, y el marco normativo sectorial previo del segmento en el que se despliegue la actividad "aplican". Lo mismo que lo hace una mínima ética corporativa. Y estos valores deben integrar el ADN de nuestras organizaciones. También debemos asumir un nuevo rol para los juristas: el de facilitador. No se confundan, el facilitador no te lo pone fácil ni te dice a todo que sí. Es quien desde la legalidad puede trabajar en equipos multi y/o transdisciplinares contribuyendo a que las cosas pasen.

Y, esta no es una responsabilidad menor. El principio que debe guiar nuestros pasos es el de la legalidad, pero desde un entendimiento operacional en el que nuestra labor no se aleja de la ingeniería de procesos como una barrera final, se integra en ella y evoluciona en cada iteración. En cada oficio hay valores, principios y metodologías imprescindibles. Los de los juristas crecen y se enriquecen en su contacto con la investigación, la innovación y el desarrollo de la tecnología. Nuestro reto es asegurar no sólo la legalidad sino también que la tecnología sea inclusiva, democrática y garante de los derechos fundamentales. No es precisamente una tarea menor.

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

LIVE STREAMING

Curso de
Doble Certificación

Continuidad de Negocio

BCI + ISO 22301

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BCI Executive
- Certificación ISO 22301 Leader
- Módulo 7: MasterGEIT®

MGEIT® eGob®

Del 5 al 13 de julio

+ 34 96 109 44 44
campus@escueladegobierno.es

ECOSISTEMA EMPRENDEDOR

Catalina Valencia Z.

Evolución de las empresas innovadoras y tecnológicas en España

En esta columna, por lo general, suelo hablar de startups, pero en menos ocasiones me refiero a las scaleups. Una scaleup es una empresa que ha superado la fase inicial de arranque (startup) y se encuentra en una etapa de crecimiento acelerado y sostenido. Estas empresas han logrado una validación inicial de su producto o servicio en el mercado y ahora se enfocan en escalar sus operaciones para expandir su alcance y aumentar sus ingresos.

A diferencia de las startups, que se centran en encontrar un modelo de negocio viable, las scaleups ya han encontrado un modelo rentable y están en proceso de maximizar su impacto y presencia en el mercado. Este crecimiento suele implicar la ampliación de su base de clientes, el incremento de su capacidad de producción o servicio, y la expansión a nuevos mercados geográficos o segmentos de clientes.

Durante mucho tiempo en España nos estuvimos enfocando en apoyar a las startups, pero lo que ocurría era que cuando estas empresas crecían, necesitaban seguir teniendo inversión y otro tipo de apoyos, y ya no era tan fácil conseguirlo. Por eso desde hace unos años los esfuerzos se han ido ampliando también hacia las scaleups, pues al final, son empresas que ya están demostrando un modelo de negocio y necesitan seguir siendo atractivas para clientes, inversores y potenciales empleados.

El crecimiento de una scaleup se mide generalmente en términos de incremento significativo en ingresos, personal, y/o presencia en el mercado durante un período sostenido. Como decía antes, estas empresas suelen necesitar importantes inversiones de capital para financiar su expansión, ya que deben invertir en infraestructura, marketing, desarrollo de productos y talento.
Las scaleups son vistas como un motor importante para la economía, ya que no solo generan empleos, sino que también pueden influir positivamente en sus sectores industriales a través de la innovación y la competencia. Además, tienen un potencial elevado para convertirse en líderes de mercado y transformar industrias enteras.

CONTINÚA EN PRÓXIMA PÁGINA

Resultados del informe Ecosistema Startup

El Referente presentó recientemente el primer Informe de Scaleups de España del año 2024, que está incluido dentro del informe sobre el ecosistema de empresas tecnológicas e innovadoras en España. Dicho informe confirma que existen en la región más de 7.000 compañías tecnológicas activas, de las cuales 1.185 son scaleups. Las 1.185 scaleups generan más de 64.000 empleos y un impacto económico anual de 9.762M€.

Si se mira la evolución del ecosistema startup y emprendedor en España desde el 2010 hasta la actualidad, el 2015 fue el año que más scaleups españolas concentró, con un total de 137. Desde entonces, la cifra ha sido inferior, situándose en 96 en 2019, en 83 en 2020, y en 44 en 2021.

Este descenso del número de scaleups no significa que haya descendido el número de startups exitosas, de hecho, en ese periodo comprendido entre 2010 y 2024 algunas scaleups se han convertido en empresas consagradas o incluso en unicornios. Lo que ha descendido es la disponibilidad de capital.

Según el informe Ecosistema Startup, el sector tecnológico en España cuenta con 7.028 empresas y genera un impacto económico de 11.541 millones de euros.
La suma de estas empresas incluye a las de nueva creación o startup (3.640 compañías), a las de nueva creación e innovadoras o scaleup (1.185) y a las pymes (2.203), que entre todas generan 99.919 empleos, de ellos 69.035 corresponden al primer grupo. El informe contabiliza este tipo de empresas creadas desde 2010, con un mayor pico de 927 empresas nuevas en 2021, mayoritariamente startup.

Cataluña es la comunidad autónoma que reúne a un mayor número de empresas del sector tecnológico, con 2.064 compañías y más de 34.000 empleados, seguida por Madrid (1.677), Comunitat Valenciana (773) y País Vasco (698).

En cuanto a inversión acumulada por comunidades autónomas, hay cinco regiones a la cabeza por mayores inversiones encabezadas por Cataluña, con un acumulado de 4.510 millones a través de 599 operaciones desde 2019, y Madrid, con 5.105 millones (528 operaciones). Les siguen Comunitat Valenciana, con 747,5 millones (208 operaciones), País Vasco, con 319,6 millones (223 operaciones) y Andalucía (290,3 millones, 121 operaciones).

Por vertical, las dedicadas al sector de la salud suman 559 compañías, seguido por el sector biotech con 382 empresas. En el último lugar de la lista figuran las empresas dedicadas al estudio y asesoramiento sobre el cambio climático (44 empresas).

Análisis de scaleups

Si se analiza la concentración de **scaleups por ciudades,** Barcelona y Madrid tienen el mayor número de scaleups en España, superando ambas comunidades autónomas las 300 compañías. Valencia es la tercera ciudad con 67 scaleups, seguidas de Bilbao y San Sebastián con 24 scaleups cada una; y las ciudades andaluzas de Málaga y Sevilla con 19 y 18 scaleups respectivamente.

El informe sobre el ecosistema de empresas tecnológicas e innovadoras también ha analizado a las scaleups según sectores y tecnologías. El sector que más scaleups acumula es el de la **energía**, con 76 empresas tech con alta escalabilidad y/o facturación. Le sigue ehealth (68), fintech (61), biotech (60), foodtech (59), ecommerce (55), marketing, media (46), SaaS (45), proptech (45) y movilidad (45). Los que menos acumulan son: arte (6), talento, laboral (5) y sostenibilidad (4).

CATALINA VALENCIA Z

Catalina Valencia Zuluaga es Community Lead en KM ZERO Food Innovation Hub y además mentora en Interacpedia, EIT Food, Demium, etc. Responsable de StartUp Europe Awards de la Comisión Europea y la Fundación Finnova hasta 2019. Elegida la persona que más promueve el ecosistema emprendedor en los VLC Startup Awards del Ayuntamiento de Valencia.

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

Twitter:
https://twitter.com/catavalencia

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

LIVE STREAMING

Curso de
Doble Certificación

Gobierno de I&T

COBIT + ISO 38500

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COBIT Executive
- Certificación ISO 38500 Leader
- Módulo 8: MasterGEIT®

MGEIT® eGob®

Del 6 al 14 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Marcos Navarro

Robots ayudando en el cambio climático

Uno de los objetivos de la humanidad es preservar el mundo para las generaciones venideras. Las nuevas tecnologías están teniendo una contribución ambivalente en la lucha contra el cambio climático. Por un lado los centros de datos y todos los dispositivos tecnológicos son consumidores de energía en mayor o menor medida. Sin embargo, la automatización y la inteligencia artificial pueden optimizar la eficiencia energética, mejorar la gestión de recursos y reducir las emisiones de carbono, contribuyendo significativamente a mitigar el impacto del cambio climático. Este artículo de TYSC exploro cómo la automatización de procesos y la IA pueden ser implementadas para combatir el cambio climático y su potencial uso en el futuro.

El cambio climático es una de las amenazas más urgentes y extremas a las que se enfrenta la humanidad, que no el planeta. El planeta ha sufrido muchos cambios climáticos a lo largo de su existencia. El problema, es que en esos cambios la vida existente acaba casi por extinguirse. Los efectos de este cambio están siendo papables en todo el mundo, desde el aumento del nivel del mar hasta los eventos climáticos extremos. Para combatir este desafío, necesitamos soluciones innovadoras y efectivas que actúan a nivel local,pero que se extiendan a nivel global.

Casi 4000 millones de personas viven en zonas muy vulnerables al cambio climático, según la Organización Mundial de la Salud y se espera que esto provoque unas 250000 muertes adicionales entre 2030 y 2050 sólo por desnutrición, malaria, diarrea y estrés térmico.

En este contexto, la automatización, la analítica de datos y la Inteligencia Artificial pueden ser herramientas muy efectivas en la lucha contra el cambio climático. Estas tecnologías pueden ayudarnos a reducir las emisiones de gases de efecto invernadero y optimizar el uso de recursos de cara crear un futuro más sostenible.

Optimización y mejor gestión de recursos

Seguro que estamos de ver edificios de oficinas totalmente iluminados por la noche, incluso con grandes pantallas que se emplean para marketing de la empresa o para presentaciones encendidas sin que haya nadie presente.

La automatización del consumo de energía en edificios es una de las aplicaciones más directas y efectivas. Los sistemas pueden programarse para regular la iluminación, la calefacción y la refrigeración en función de la ocupación y las condiciones climáticas, lo que permite un uso más eficiente de los recursos energéticos. Por ejemplo, en un edificio de oficinas, se puede ajustar automáticamente la iluminación y la temperatura según la cantidad de personas presentes, la iluminación y la temperatura exterior, reduciendo así el consumo de energía, sobre todo, cuando las áreas no están ocupadas. Además, estos sistemas pueden integrarse con otros sistemas de gestión de edificios inteligentes para monitorizar continuamente el uso de energía y ajustar los sistemas en tiempo real. Esta capacidad de respuesta inmediata no solo mejora la eficiencia energética, sino que también contribuye a reducir los costes operativos y las emisiones de carbono.

CONTINÚA EN PRÓXIMA PÁGINA

En el sector industrial, la analítica de datos junto con la IA puede desempeñar un papel crucial en la identificación y reparación de fugas de agua y de energía, así como en la optimización de procesos industriales. Las fábricas y plantas de producción deben ser muy eficientes en el uso de recursos, por los costes y por sostenibilidad,. Monitorizando equipos y procesos, es posible detectar rápidamente cualquier anomalía que indique una fuga de recursos. Por ejemplo, los sistemas automatizados pueden utilizar sensores y algoritmos para identificar puntos de pérdida de calor en una planta industrial y activar las alarmas correspondientes y realizar la reparación inmediata. Además, se pueden optimizar los horarios de funcionamiento de las máquinas y los procesos de producción para minimizar el consumo de energía durante las horas pico, o aprovechar el sol en instalaciones fotovoltaicas, contribuyendo así a una operación más sostenible y económica.

El sector del transporte es otro ámbito en el que la automatización de la planificación de rutas y la gestión de flotas permite reducir el consumo de combustible y las emisiones de gases de efecto invernadero. Mediante el uso de algoritmos avanzados, se puede analizar datos en tiempo real sobre el tráfico, las condiciones meteorológicas, información de la carga y su estado, para determinar las rutas más eficientes para los vehículos. También se puede optimizar la gestión del mantenimiento de las flotas, programando revisiones y reparaciones preventivas basadas en la información recopilada de los sensores instalados en los camiones y remolques y su historial de uso. Esto no solo prolonga la vida útil de los vehículos, sino que también asegura que operen de manera más eficiente, reduciendo su impacto ambiental.

Mejoras en la generación de energía limpia

Una de las aplicaciones de la IA es la optimización de la gestión de las fuentes de energía renovable como la eólica y la solar. La IA puede analizar datos meteorológicos históricos y en tiempo real para predecir la producción de energía y optimizar la ubicación y el diseño de parques eólicos y solares, maximizando la captación de energía renovable. Otros de los aspectos importantes es adecuar la demanda de energía a la producción de energías mas sostenibles. La IA puede gestionar de manera eficiente la integración de las fuentes de energía en la red eléctrica, ajustando la producción hacia energías menos contaminantes, activando estaciones de bombeo para un uso mas eficiente del agua y almacenar energía, en función de la demanda y las condiciones climáticas. Esto no solo aumenta la eficiencia de las fuentes de energía renovable, sino que también ayuda a estabilizar la red eléctrica y reducir la dependencia de fuentes de energía no renovable.

Evitar la degradación del medio ambiente

Las zonas verdes del planeta, como los bosques y los parques, desempeñan un papel crucial en la lucha contra el cambio climático. Por una parte los árboles y las plantas absorben dióxido de carbono (CO_2), uno de los principales gases de efecto invernadero, a través de la fotosíntesis, reducen la contaminación del aire, mitigan las islas de calor, son una protección contra inundaciones y la degradación de suelos, y producen un incremento de la biodiversidad. Por lo tanto, aumentar nuestras zonas verdes es una estrategia clave para combatir el cambio climático.

Mediante el uso de tecnologías de monitorización y análisis de datos, la IA puede ayudar a detectar y prevenir la deforestación, vertidos contaminantes y otros problemas ambientales. Los sistemas de IA pueden analizar imágenes de satélite o captadas por drones para identificar áreas de deforestación ilegal en tiempo real, permitiendo tomar medidas inmediatas para detener estas actividades destructivas. También la IA puede utilizarse para una gestión sostenible de recursos en la agricultura. Los algoritmos de IA pueden analizar datos sobre el clima, el suelo, el color de los cultivos para optimizar el uso de agua, fertilizantes y otros productos fitosanitarios, reduciendo el impacto ambiental y mejorando la productividad de los cultivos.

Ademas, mediante el analisis de la información recogida por satelite y drones, se pueden identificar cultivos sonlosmas indicados para reforestar determinadas areas. Así se puede planficar la dispersión de semillas mediante drones a una velocidad 100 veces más rápida que si se hiciera manualmente.

Otras acciones que ayudan a combatir el cambio climático es hacer más eficiente la gestión de los residuos. Los residuos son grandes productores de metano y responsables del 16% de las emisiones mundiales de gases de efecto invernadero (GEI), según la Agencia de Protección del Medio Ambiente de Estados Unidos. Ya existen sistemas de IA que analizan las instalaciones de tratamiento y reciclaje de residuos para ayudar a recuperar y reciclar más material de desecho. Se identifican un conjunto de características en los residuos y se reducen las toneladas de residuos que se envía a los vertederos o incineradoras.

Otro área de aplicación es la reducción de la contaminación de los océanos.

La IA está ayudando a luchar contra el cambio climático en sistemas como los que identifican la contaminación por plásticos en el océano. Mediante sistemas de IA se detectan objetos flotantes o en suspensión mediante el análisis de imágenes y permite crear mapas detallados de basura oceánica. Esta información permite definir campañas de recogida y retirada de estos residuos.

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/

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

LIVE STREAMING

Curso de Cuadruple Certificación

Gobierno, Gestión y Calidad del Dato

UNE 0077, 0078 0079 y 0080

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación UNE 0077 Leader
- Certificación UNE 0078 Leader
- Certificación UNE 0079 Leader
- Certificación UNE 0080 Leader
- Módulo 9: MasterGEIT®

MGEIT® eGob®

Del 6 al 14 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Valladolid se convierte en la capital mundial de Blockchain y las tecnologías DLT

Del 3 al 7 de junio, Valladolid acoge la reunión de la Organización Internacional de Normalización (ISO) a cargo de elaborar estándares globales sobre Blockchain y DLT (Tecnologías de Registro Distribuido). Asisten más de 90 expertos de 30 países.

CONTINÚA EN PRÓXIMA PÁGINA

REVISTA
Tecnología & Sentido Común
https://tecnologiaysentidocomun.com

Esta reunión internacional, organizada por la Asociación Española de Normalización, UNE, cuenta con el patrocinio de la Universidad de Valladolid, el Ayuntamiento de Valladolid, la Agencia de Innovación y Desarrollo Económico del Ayuntamiento de Valladolid (IdeVa), la International Association for Trusted Blockchain Applications (INATBA) y KRON WORLD, así como con la colaboración del Banco de España.

España es un referente internacional en estándares de Blockchain y tecnologías DLT (Tecnologías de Registro Distribuido). UNE ha estado involucrada desde el inicio en el Comité internacional ISO/TC307 desempeñando un papel significativo en su dirección y desarrollo estratégico.

Evento Protagonista

La Asociación Española de Normalización, UNE, miembro nacional de la Organización Internacional de Normalización (ISO), organiza, del 3 al 7 de junio en Valladolid, la reunión de ISO a cargo de elaborar estándares globales con las mejores prácticas sobre Blockchain y DLT (Tecnologías de Registro Distribuido). De esta forma, Valladolid se convierte esta semana en el epicentro mundial de los estándares ISO en estos ámbitos, poniendo en valor el liderazgo español en esta materia.

CONTINÚA EN PRÓXIMA PÁGINA

REVISTA
Tecnología & Sentido Común
https://tecnologiaysentidocomun.com

Esta reunión cuenta con el patrocinio de la Universidad de Valladolid, el Ayuntamiento de Valladolid, la Agencia de Innovación y Desarrollo Económico del Ayuntamiento de Valladolid (IdeVa), la International Association for Trusted Blockchain Applications (INATBA) y KRON WORLD, así como con la colaboración del Banco de España.

Durante toda la semana, Valladolid acoge la reunión plenaria del Comité Técnico de Normalización internacional ISO/TC 307 "Blockchain and other Distributed Ledgers Technologies", responsable de elaborar estos estándares, así como otras sesiones.

El acto de apertura ha tenido lugar hoy, 3 de junio, en el que han participado Susana Álvarez, vicerrectora de Innovación Docente y Transformación Digital de la Universidad de Valladolid; Luis Carro, vicedecano de la Facultad de Educación y Trabajo Social de la Universidad de Valladolid; Mónica Sanzo, directora de Cooperación y Relaciones Internacionales de UNE; Scott Farrell, Presidente del Comité de Normalización ISO/TC 307; y Amy Howie, secretaria del ISO TC/307.

A continuación, se ha mantenido la reunión Plenaria, en la que han participado expertos de numerosos países.
A la reunión asisten más de 90 expertos de 30 países, entre ellos, representantes de entidades públicas, gobiernos, asociaciones sectoriales, organizaciones internacionales, organismos de normalización, empresas privadas, centros de investigación y universidades. Valladolid, se convierte así en la capital mundial de Blockchain y las tecnologías DLT (Tecnologías de Registro Distribuido).

El Comité de Normalización internacional ISO/TC 307 "Blockchain and other Distributed Ledgers Technologies" de ISO es responsable de desarrollar los estándares globales de numerosos aspectos de estas tecnologías, como vocabulario y terminología, seguridad, privacidad y gestión de identidad, smart contracts, gobernanza, interoperabilidad, Non-Fungible Tokens (NFTs) y monedas digitales. Está estructurado en 7 Grupos de Trabajo y 5 Grupos Asesores, que han publicado 12 estándares y están desarrollando 16 actualmente.

Liderazgo español

España es un referente internacional en estándares de Blockchain y tecnologías DLT. UNE ha estado involucrada desde el inicio en este Comité internacional, desempeñando un papel significativo en su dirección y desarrollo estratégico. Un logro destacado es la Norma UNE 71307-1 *Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de Referencia Genérico*, la primera norma mundial para la gestión de identidades digitales descentralizadas basada en Blockchain y tecnologías DLT.

Esta norma proporciona un marco para la emisión, gestión y uso descentralizados de atributos que caracterizan e identifican a individuos u organizaciones, permitiendo a las entidades crear y controlar su identidad digital de manera autónoma. Tras su éxito nacional, fue elevada a norma europea y ha servido de base para el desarrollo de dos normas ISO.

El programa de la reunión contempla varias sesiones de los Grupos de Trabajo del Comité. Además, bajo el impulso del Banco de España, el martes 4 de junio se celebrará un Side-Event junto con el Grupo Asesor TC307/AG3 "Digital currencies" y el Comité ISO/TC 68 "Financial services" en la sucursal del Banco de España en Valladolid; se hablará del uso potencial de las tecnologías DLT en la implementación y distribución de las monedas digitales de los bancos centrales.

También como parte de la agenda, el miércoles 5 de junio se celebrará el Social-Event abierto, patrocinado por INATBA, en el que presentará su papel en los desarrollos de alto nivel relacionados con la tecnología Blockchain y sus aplicaciones. Participarán representantes de INATBA, la Junta de Castilla y León, UNE y la Comisión Europea.

La semana se completa con el cierre de la reunión plenaria del Comité Técnico de Normalización internacional ISO/TC 307, a la que asistirá una nutrida delegación española, incluyendo representantes de KRON WORLD, AIRBUS, CSIC, Banco de España, Asociación Reacción Económica y Halborn, entre otros, demostrando así la firme apuesta de España por la estandarización en el ámbito de Blockchain y DLT.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Sesión de Formación y Certificación en:

Principios y Modelo para la Excelencia en el Servicio

Director Académico:

Javier Peris

- Duración 5 horas
- Sesión única
- Miércoles de 16:00 a 21:00 horas
- En Directo y en Remoto
- Basado en la norma ISO 23592:2021
- Examen de Certificación Incluido
- Certificación ISO 23592 Leader
- Plazas limitadas

MPPM® MGEIT® eGob®

Miércoles 8 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Víctor Almonacid

Algoritmos malvados

Me asombra la creciente preocupación por la supuesta falta de ética de los algoritmos, preocupaciones que parecen más basadas en influencias de la ciencia ficción que en la realidad. La inteligencia artificial (IA) es una herramienta poderosa, pero la "conciencia artificial" aún no ha sido alcanzada y no deberíamos temer las supuestas malas intenciones de una máquina que carece de intenciones.

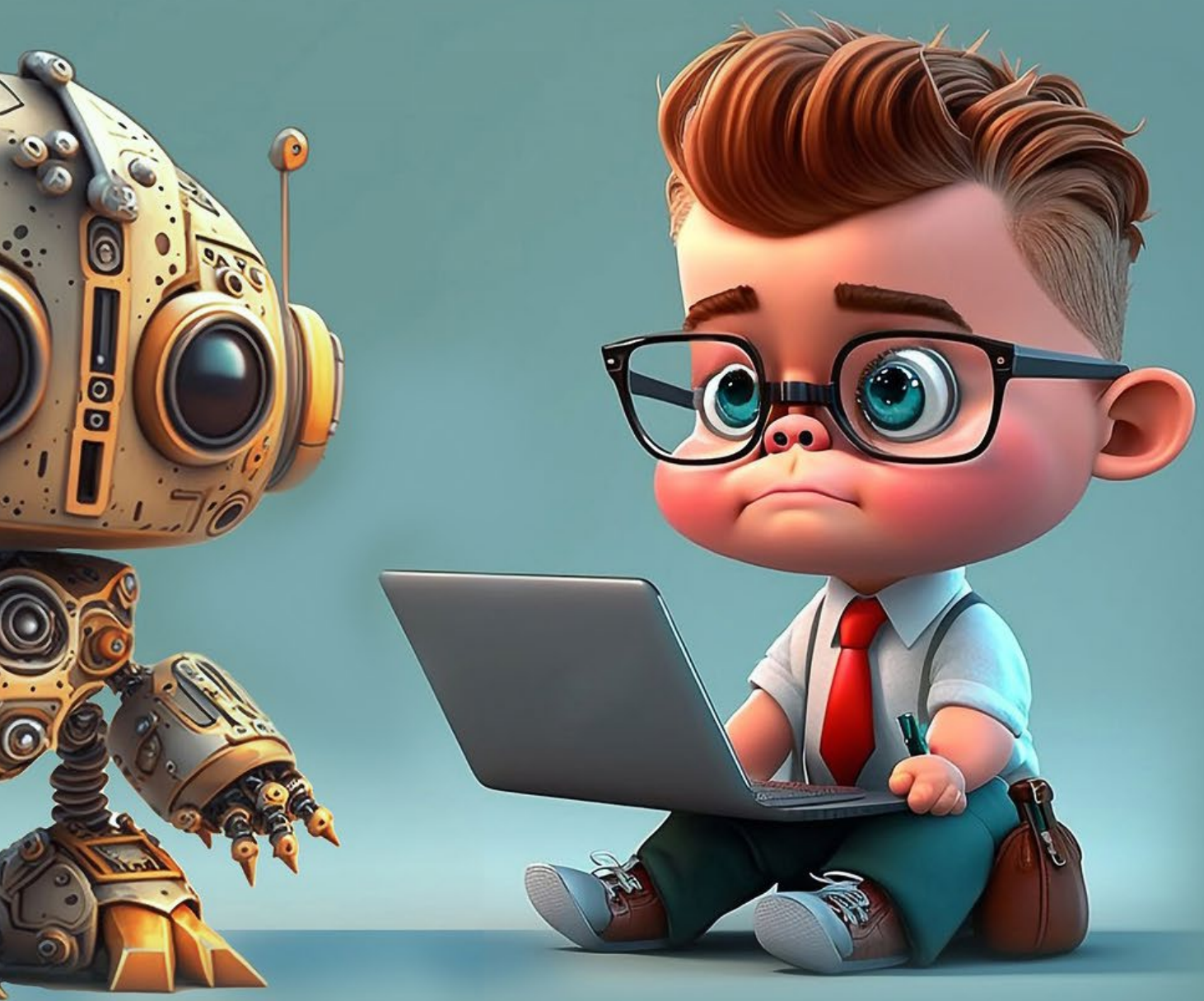
Por el contrario, su carácter instrumental nos puede ayudar, y mucho. De hecho ya lo hace. La IA ya juega un papel importante, especialmente en grandes organizaciones que manejan enormes volúmenes de datos. La automatización facilita el procesamiento, medición y análisis de estos datos, ayudando a tomar decisiones más objetivas y fundamentadas. La Administración se rige por los principios de objetividad, eficacia y eficiencia, donde los algoritmos encajan como anillo al dedo. Sin embargo, es crucial recordar que los algoritmos, aunque aportan valiosos elementos de juicio, no toman ni pueden tomar decisiones finales en asuntos críticos sin supervisión humana.

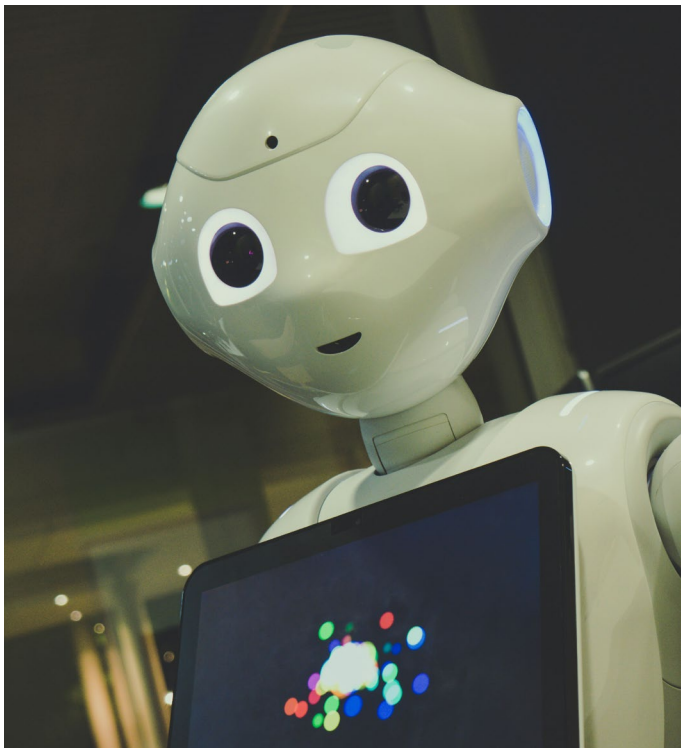
Las decisiones importantes siempre tienen algún grado de supervisión o verificación humana para asegurar su legitimidad. En realidad ya lo dice la ley: en la Administración, las decisiones las toma "el órgano competente", y este siempre está compuesto por una o varias personas.

Por otra parte, la efectividad de los algoritmos depende en gran medida de su correcta programación, y en este sentido resulta esencial configurar estos sistemas incorporando los principios de legalidad y ética de forma que estén integrados desde el diseño.

CONTINÚA EN PRÓXIMA PÁGINA

> **Se puede confiar en las malas personas, no cambian jamás.**
>
> *William Faulkne*





Esto implica cumplir con las normativas de privacidad y protección de datos, así como asegurarse de que los algoritmos no perpetúen injusticias o sesgos que en realidad no son propios, sino "heredados" del proceso que automatizan. Por supuesto, estamos a favor de humanizar las decisiones, y es cierto que aunque los algoritmos pueden aprender y adaptarse (*mediante machine learning y deep learning*), no pueden desarrollar empatía. Pero esto puede ser visto tanto como una limitación como una ventaja, ya que asegura la objetividad y la ausencia de preferencias personales.

Lo que sí debe quedar claro es que los algoritmos no son inherentemente buenos ni malos; son herramientas diseñadas para seguir un conjunto específico de instrucciones. En terminología administrativa, un algoritmo actúa dentro de un sistema reglado, carece de discrecionalidad. Si una aplicación automatizada produce resultados injustos, generalmente es debido a fallos en la programación subyacente, no en el algoritmo en sí. El llamado "sesgo algorítmico" a menudo se debe a datos de entrenamiento sesgados o a normas defectuosas que los algoritmos no obstante aplican de manera uniforme.

Por eso la decisión última es competencia y responsabilidad de un ser humano. Legalmente, los algoritmos no pueden tomar decisiones que afecten a los derechos de las personas, conforme al artículo 22 del Reglamento General de Protección de Datos (RGPD). Esta norma establece que "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". Asimismo, la Ley 15/2022 de igualdad de trato y no discriminación establece en su artículo 23 ("Inteligencia Artificial y mecanismos de toma de decisión automatizados") una serie de normas éticas y de control.

En conclusión, aunque nuestra dependencia de los algoritmos va en aumento, es importante abordar su implementación sin prejuicios ni temores infundados, porque estos, al igual que la sobre regulación, frenan el progreso. Los algoritmos son, en última instancia, herramientas basadas en las matemáticas y no poseen características humanas como la corrupción, que por desgracia es un mal exclusivamente humano. Aún así resulta crucial trabajar en la mejora continua de estos sistemas, en cuanto a su programación y regulación, asegurando su uso ético y eficaz tanto en la administración pública como en otros sectores.

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/

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno Corporativo COSO + ISO 37000

Director Académico:

Javier Peris

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

MPPM® MGEIT® eGob®

Del 22 al 30 de noviembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Jesús López Peláz

Proteger una marca comercial en los Estados Unidos

El sistema de protección de las marcas comerciales en Estados Unidos presenta notables diferencias con otros sistemas en el mundo, como, por ejemplo, España, Italia o el resto de países europeos.

A diferencia de lo que sucede en Europa, donde la tutela de la marca suele ser una medida preventiva y previa a su uso en el mercado, en Estados Unidos una marca sólo puede registrarse a nivel federal después de haber sido utilizada en el comercio estadounidense.

Formas de protección de la marca

Siguiendo la subdivisión administrativa a tres niveles en EE. UU., que va desde el nivel local (condado), pasando por el nivel estatal, hasta el nivel federal, en EE. UU., existen diferentes formas para proteger una marca:

•***Common Law Rights:*** tutelan la marca únicamente en la zona geográfica en la que se haya utilizado comercialmente.

•***Protección estatal:*** se produce con el registro de la marca en los sistemas estatales. En este caso, la marca sólo estará protegida dentro de ese estado. Para ampliar la protección, deberá registrarse en los sistemas de otros estados o en el sistema federal.

•***Protección federal:*** protege la marca en todo el territorio de los EE.UU. y, una vez registrada la misma, permite utilizar el símbolo ®.

•***Protección internacional:*** a través del protocolo de Madrid.

El presente artículo tiene por objeto la protección de la marca a nivel federal.

Características de la marca

En los Estados Unidos, se entiende por marca comercial una palabra, una frase, un logotipo, un diseño o una combinación de estos elementos, que puede ser en blanco y negro o en color.

La marca comercial ha de estar asociada a los productos y/o servicios ofrecidos por el titular, utilizando como referencia las clasificaciones de bienes y servicios establecidas por la United States Patent and Trademark Office (USPTO), que es la oficina de patentes y marcas responsable de los registros.

A modo de ejemplo, si se desea registrar una marca comercial de un producto como el jamón, la clase aplicable sería la 029, mientras que para los servicios de restauración, lo sería la clase 043. Nada impide solicitar el registro de una misma marca para varias clases de productos y servicios, incluso si son totalmente diferentes.

CONTINÚA EN PRÓXIMA PÁGINA

Ahora bien, no todas las marcas son registrables. En primer lugar, la marca no puede ser similar a otra marca ya registrada con la misma categoría de productos y/o servicios, ya que podría crear un riesgo de confusión en el consumidor. Por este motivo, antes de proceder a la solicitud de registro e incurrir en un gasto de tiempo y dinero, es aconsejable realizar una búsqueda exhaustiva de marcas similares ya registradas en el sistema USPTO o ya utilizadas en el comercio estadounidense.

El diseño de una marca tampoco puede contener banderas nacionales ni describir el producto y/o servicio asociado (por ejemplo, "bronceador" para protector solar), ni tampoco ser genérico (por ejemplo, "gafas" para anteojos).

La fecha de presentación de la solicitud confiere generalmente "prioridad" a la marca. Una vez registrada, la marca es válido durante un periodo de 10 años, prorrogable por periodos de 10 años, siempre que la marca se siga utilizando para a los productos y/o servicios asociados. De hecho, durante el 5to y 6to año de cada periodo, es necesario presentar una declaración de uso de la marca.

Presentación de la solicitud

La solicitud de registro se presentará en virtud de una **"filing basis"** o, dicho de otro modo, con arreglo a una base o motivo de presentación:

1.Use in commerce basis (Trademark Act Section 1(a)), cuando el solicitante ya ha utilizado la marca en el comercio estadounidense para los productos y/o servicios indicados en la solicitud

2.Intent to Use basis (Trademark Act Section 1(b)), cuando el solicitante todavía no ha comenzado a utilizar la marca en el comercio en el momento de la solicitud, pero tiene la intención de buena fe de utilizarla en un futuro próximo. Como se ha mencionado anteriormente, la marca sólo será registrada cuando se acredite que ha sido utilizada en el comercio estadounidense para los productos y/o servicios asociados;

3.Foreign Application basis (Trademark Act Section 44(d)), cuando el solicitante ha presentado, en los seis meses anteriores, una solicitud de registro en un sistema extranjero para la misma marca y para los mismos productos y/o servicios asociados. En este caso, la "fecha de prioridad" de la solicitud presentada ante la USPTO coincidirá con la fecha de presentación de la solicitud en el sistema extranjero;

4.Foreign Registration basis (Trademark Act Section 44(e)), cuando el solicitante haya logrado registrar la misma marca en el país de origen, para los mismos productos y/o servicios asociados,.

El artículo 66(b) de la Trademark Act prevé una "filing basis" adicional, que permite extender la protección de una marca internacional en los Estados Unidos, cuando se haya registrado en un Estado miembro del protocolo de Madrid. Para ello, es necesario dirigirse a la Oficina Internacional de la Organización Mundial de la Propiedad Intelectual (OMPI).

El proceso de registro puede durar entre 6 y 15 meses, dependiendo de la "filing basis" elegida y de si se solicitan pruebas o informaciones adicionales. Si el registro se completa con éxito, se expide un certificado de registro y la marca podrá incluir el símbolo ®.

Conviene tener presente que el registro de una marca, ya sea en EE.UU. o en cualquier otro país, proporciona protección jurídica frente a quienes utilizan la marca sin autorización o intentan registrar una marca similar para productos y/o servicios parecidos. El registro de la marca también aumenta el valor de la empresa de cara a los consumidores, inversores o potenciales compradores. Por estas razones, se aconseja planificar con antelación la entrada en el mercado estadounidense y contar con el apoyo de profesionales cualificados en el momento de elegir la marca que se va a utilizar.

JESÚS P. LÓPEZ PELÁZ

Jesús Lopez Pelaz es director del Bufete Abogado Amigo y jurista apasionado de la tecnología, es profesor de Legaltech en la Universidad CEU Cardenal Herrera y cuenta con una larga experiencia en el desarrollo de proyectos de transformación tecnológica de la abogacía, y además de todo eso, un gran amigo y colaborador incondicional de Tecnología y Sentido Común.

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

LIVE STREAMING

Curso de
Doble Certificación

Gestión Ágil de Proyectos

OpenPM² (Ágil) + KANBAN

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (Ágil) Executive
- Certificación KANBAN Leader
- Módulo 6 MasterPPM®

MPPM®

eGob®

Del 21 al 29 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

Renato Aquilino

Yo, cuando sea mayor, quiero ser DPD (y II)

El Esquema de Certificación AEPD-DPD contiene planteamientos cuestionables para la finalidad pretendida.

FORTALEZAS Y DEBILIDADES DEL ESQUEMA AEPD-DPD

El Esquema de Certificación de DPD (el esquema, en adelante) de la Agencia Española de Protección de Datos (AEPD) tiene una finalidad muy loable pero también excesivamente ambiciosa en función de sus planteamientos y los escenarios reales de trabajo que se encontrarán las personas certificadas.

La certificación de personas que promueve el esquema es correcta siempre y cuando el ámbito de aplicación del objeto de la certificación sea abarcable por un individuo, pero no es válida cuando la competencia que evalúa es inabarcable por una persona, resultando en certificados "teóricos" que no permiten una praxis adecuada al no profundizar en los temas, muy especialmente cuando se mezclan en la misma certificación conocimientos jurídicos y técnicos.

¿Sería lógico certificar un médico como oftalmólogo-cardiólogo requiriendo que sea experto en ambas disciplinas y que, adicionalmente, sea capaz de ejercer en ambas cuando acabe el examen? Inabordable. Pues parece que este criterio no se aplica en el esquema dado que mezcla el universo jurídico con el técnico, teniendo ambos un alcance inmenso claramente candidato a una especialización diferenciada que permita abordar los escenarios reales con unos conocimientos profundos y aplicables en la práctica.

No existe la figura "DPD junior". Las expectativas de las entidades que nombran o contratan un DPD certificado son muy altas y suelen rechazar cualquier intento de contratación de soporte externo, con su coste asociado, bajo el argumento "eres un DPD certificado por la AEPD y eso implica que sabes todo lo que tienes que saber", máxime cuando la propia AEPD afirma:

> "Este Esquema es un sistema de certificación que permite certificar que los DPD reúnen la cualificación profesional y los conocimientos requeridos para ejercer la profesión"

CONTINÚA EN PRÓXIMA PÁGINA

Este planteamiento y el uso del verbo "certificar" no ha tenido en cuenta la realidad y el volumen de trabajo que debe desarrollar el rol DPD.

ESPECIALIZACIONES NECESARIAS

El rol DPD en un organismo de la Administración Pública (AAPP) desarrolla su trabajo en un escenario legal diferente al de una entidad privada, cuestión que también debería ser objeto de especialización para evitar situaciones como las que encontramos habitualmente sobre todo en la AAPP, donde su DPD certificado, sobre todo si es externo, puede desconocer la legislación específica sobre procedimientos administrativos, gestión tributaria, urbanismo, Servicios Sociales, Policía Local, violencia de género, menores, etc, de un catálogo de tratamientos entre los que se encuentran algunos clasificables como de máxima sensibilidad.

Capítulo aparte merecen los conocimientos técnicos. Dentro del examen de certificación supone 30 preguntas de las 150 totales, un 20% del total, estando su contenido especificado en el denominado "dominio 3". Entre ellas:

……3.3. La gestión de la seguridad de los tratamientos. 3.3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI). 3.3.2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación. 3.3.3. Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación del Desastres…..

Simplemente con esta enumeración de contenidos ya queda claro que una persona que provenga del ámbito jurídico, perfil claramente mayoritario entre las personas que se presentan al examen, no puede abordar este caudal de conocimientos de forma efectiva y, con ello, observamos que el nivel de las preguntas del examen relacionadas con este dominio permite aprobar el examen, pero quedan a mucha distancia del nivel de conocimiento requerido para el perfil técnico del rol DPD.

En la práctica, encontramos DPDs provenientes del ámbito jurídico que no pueden entender un escenario técnico sobre el que deben asesorar y supervisar, ni siquiera con el soporte del área de IT, dado que no disponen de una base adecuada que, en el estado de la técnica y su constante evolución, les permita aportar criterio y supervisión en este contexto.

LA EXPERIENCIA NO ES UN GRADO, ES UNA NECESIDAD

El esquema de la AEPD permite presentarse al examen a personas sin experiencia alguna en materia de protección de datos personales, tras la realización de un curso homologado de un mínimo de 180 horas y, si aprueban el examen, se les concede la misma certificación que una persona con experiencia en los escenarios reales sobre la materia. En mi opinión, **este planteamiento supone un grave error que devalúa la propia certificación y su valor en el mercad**o, dado que, para estas actividades de asesoramiento y supervisión, es improbable que una persona sin experiencia previa real pueda aportar valor en los niveles que una entidad contratante de un "DPD certificado por la AEPD" espera.

PROPUESTAS PARA LA CERTIFICACIÓN DPD

Mis propuestas para un esquema de certificación DPD que considero acordes con la realidad, volumen y complejidad de los tratamientos de datos personales actuales y las proyecciones futuras consisten, a grandes rasgos, en:

Especializaciones por perfil.

1.Certificación DPD jurídica especializada. Incluye terminología y conceptos técnicos básicos, con el fin de contextualizar "lo técnico".

2.Certificación DPD técnica especializada, con una claro enfoque en la aplicación de normas y estándares en materia de seguridad de la información. Incluye contenido básico sobre conceptos y normativa legal en materia de protección de datos personales para su contextualización.

Especializaciones sectoriales tras la especialización por perfil.

1.Administración Pública.
2.Sanidad.
3.Empresa.

Requerimiento de experiencia.

ineludible, a menos que se plantee una certificación "DPD Candidate" para el curso de 180 horas y la aprobación del examen.

CONCLUSIÓN

Es fundamental considerar el rol DPD como un "equipo DPD" donde personas con perfil jurídico y técnico trabajan integradas para ejercer con propiedad las actividades que el RGPD y la LOPDGDD asignan a este rol, **suprimiendo la percepción del DPD unipersonal por inviable.**

FIN DE TEMPORADA

Con esta edición de TySC finaliza la temporada. Espero que las temáticas tratadas hayan sido de vuestro interés.

RENATO AQUILINO

Licenciado en Informática por la Universitat Politécnica de Catalunya. E.U. en Protección de Datos y Privacidad por la Facultad de Derecho de la Universidad de Murcia. CISA, CISM, CGEIT, COBIT 5 Implemen- ter, Lead Auditor ISO 27001-TC y Auditor del Esquema Nacional de Seguridad. Carrera profesional desarro- llada en Ingeniería de sistemas, DBA y, principalmente, consultoría y auditoría sobre marcos y normas asociadas a la seguridad de la información, tanto en sector público como privado. Colaborador de ISACA HQ desde 2004, autor de numerosas publicaciones, cursos y ponencias sobre estas materias, miembro del COIICV, ISACA, itSMF España, APEP e ISMS Forum.

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

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

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Porfolios

OpenPM² (PfM) + ISO 21504

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PfM) Executive
- Certificación ISO 21504 Leader
- Módulo t MasterPPM®

MPPM®

eGob®

Del 21 al 29 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

Alex Aliaga

La nueva amenaza en el cielo: “ataques con drones que pueden sembrar el caos”

INTRODUCCIÓN

El auge de los drones de consumo ha transformado fundamentalmente la aviación, introduciendo nuevos desafíos de seguridad y protección frente a estos pequeños dispositivos. Ante esta realidad, las Autoridades de Aviación Civil de todo el mundo han impulsado la adopción de protocolos y reglas de Identificación Remota **(RemoteID)** para drones de consumo. Estos reglamentos exigen que los drones transmitan periódicamente su información, permitiendo a entidades de terceros, como las FFCCSE, identificar y localizar drones y sus operadores.

Las regulaciones de RID surgieron en respuesta a las características peculiares de los drones: su pequeño tamaño, baja detectabilidad por radar, ruido casi imperceptible a distancias largas, capacidad de vuelo a altitudes extremadamente bajas y maniobrabilidad que les permite volar bajo árboles y entre edificios. Estos atributos dificultan el seguimiento fiable de drones mediante tecnologías de monitorización del espacio aéreo existentes, como los sistemas de radar y visión. Los estándares de RID buscan aumentar la seguridad para los operadores de drones y las operaciones en el espacio aéreo, minimizando riesgos en zonas críticas como aeropuertos y bases militares.

EL PROTOCOLO OPEN DRONE ID (ODID)

El protocolo **Open Drone ID** (ODID) es una solución de código abierto diseñada para cumplir con las especificaciones de RID en diversas regiones del mundo. Este protocolo define métodos de comunicación y formatos de mensajes que permiten a los drones transmitir información esencial a estaciones receptoras en tierra. La estructura del mensaje ODID incluye datos como la ubicación del dron, la altitud, la velocidad y la identificación del operador.

El ODID utiliza tecnologías, como **Wi-Fi y Bluetooth**, para transmitir datos de identificación y telemetría. La principal ventaja de este enfoque es que no requiere una conexión a internet o infraestructura en la nube para funcionar, haciendo que los datos estén disponibles para cualquier receptor cercano.

VULNERABILIDADES EN LOS PROTOCOLOS

A pesar de los beneficios de los protocolos RID (RemoteID), la implementación actual de estos sistemas presenta serias vulnerabilidades de seguridad. La falta de cifrado, autenticación y verificaciones de integridad en los datos implica que la información transmitida no puede ser considerada confiable.

Por ejemplo, un atacante podría recrear el impacto de drones en zonas de exclusión de vuelo, sin necesidad de un dron real, simplemente inyectando datos RID falsos en un canal inalámbrico. **Este tipo de ataque podría provocar interrupciones significativas en infraestructuras críticas**, como aeropuertos, con consecuencias económicas y de seguridad graves.

El protocolo Drone ID, desarrollado por DJI, presenta vulnerabilidades críticas que comprometen la integridad y seguridad del sistema de Identificación Remota (RID). En primer lugar, la transmisión de datos carece de cifrado, lo que permite que los datos puedan ser interceptados fácilmente por actores malintencionados. Esta deficiencia en la protección de la información significa que los datos transmitidos desde el dron a las estaciones receptoras pueden ser capturados y manipulados sin ninguna dificultad.

Además, el protocolo Drone ID no implementa mecanismos de autenticación ni verificaciones de integridad para los datos transmitidos. Esta falta de medidas de seguridad permite que un atacante inyecte datos falsos en los canales de comunicación. Como resultado, es posible simular la presencia de drones en ubicaciones específicas sin necesidad de utilizar un dron físico. Esta capacidad de inyectar datos falsos es particularmente preocupante en contextos donde la precisión y autenticidad de la información de vuelo son cruciales para la seguridad, como en aeropuertos y zonas de exclusión aérea.

CONTINÚA EN PRÓXIMA PÁGINA

Por último, la tecnología de radiofrecuencia propietaria de DJI, conocida como OcuSync, también adolece de la ausencia de mecanismos robustos para asegurar la confidencialidad de los datos.
Esta debilidad facilita la realización de ataques de replay, en los cuales los datos de telemetría previamente capturados son retransmitidos para crear trayectorias de vuelo falsas. Esta vulnerabilidad permite que las estaciones receptoras en tierra, como el dispositivo Aeroscope de DJI (usado por FFCCSE para la identificación y control de drones maliciosos), sean incapaces de diferenciar entre datos legítimos y falsificados. En consecuencia, la eficacia del sistema RID se ve comprometida, poniendo en riesgo la seguridad del espacio aéreo y la integridad de las operaciones que dependen de información precisa y confiable.

ESCENARIOS DE ATAQUE

El análisis de las vulnerabilidades de los protocolos, han permitido identificar diversos escenarios de ataque que explotan las debilidades intrínsecas en estos sistemas de Identificación Remota (RID). Cada uno de estos escenarios demuestra cómo un atacante puede manipular la información telemétrica y comprometer la seguridad del espacio aéreo.

Escenario 1: Falsificación de un solo Dron

En este escenario, un atacante utiliza la inyección de datos falsos para simular la presencia de un único dron en una ubicación específica. El atacante puede transmitir mensajes que contienen coordenadas GPS, altitud y otros datos telemétricos falsificados, creando la ilusión de que un dron está operando en un área restringida. Esta falsificación puede desencadenar una respuesta de seguridad innecesaria, como el cierre temporal de un aeropuerto o la movilización de fuerzas del orden, causando interrupciones significativas en la operación normal de la infraestructura crítica.

Escenario 2: Falsificación de múltiples Drones

Este escenario amplía el ataque anterior al simular la presencia de múltiples drones en una zona restringida. El atacante puede inyectar varios conjuntos de datos falsos, cada uno representando un dron diferente. Esta técnica de saturación puede sobrecargar los sistemas de monitorización y complicar la respuesta de las fuerzas del orden, ya que tendrán que diferenciar entre múltiples amenazas potenciales. Además, la presencia simulada de varios drones puede desviar recursos críticos y crear un estado de caos y confusión en el área afectada.

Escenario 3: Nube de Drones

Un atacante puede crear una "nube de drones" mediante la inyección continua de datos RID falsos desde múltiples ubicaciones. Utilizando radios definidas por software (SDR) como el HackRF, el atacante puede transmitir datos telemétricos falsificados que simulan una gran cantidad de drones operando simultáneamente en una amplia zona geográfica. Este ataque puede engañar a los sistemas para que perciban una actividad de dron mucho mayor de la que realmente existe, desbordando los recursos de respuesta y afectando gravemente la seguridad del espacio aéreo. Este tipo de ataque es especialmente peligroso en eventos públicos grandes o cerca de infraestructuras críticas, donde una respuesta rápida y coordinada es esencial.

Escenario 4: Timer de DroneScout (CVE-2023-29156)

Este escenario explota una vulnerabilidad específica en el temporizador del DroneScout. El atacante puede manipular el temporizador del dispositivo mediante técnicas de "**spoofing**" o **modificación de firmware**. Al alterar la secuencia de recepción de datos, el atacante puede causar que los datos válidos sean ignorados o malinterpretados por el sistema. Esta vulnerabilidad puede ser utilizada para crear lagunas en la monitorización, permitiendo que drones no autorizados operen sin ser detectados durante periodos críticos.

Escenario 5: Canales Adyacentes del DroneScout (CVE-2023-31191)

En este escenario, el atacante explota la vulnerabilidad de los canales adyacentes del DroneScout. Al manipular las frecuencias de transmisión, el atacante puede interferir con la recepción de datos válidos, perturbando el funcionamiento normal del sistema RID (RemoteID).
Esto se logra mediante la transmisión de señales de alta potencia en frecuencias cercanas a las utilizadas por el DroneScout, causando que el receptor no pueda recibir correctamente la señal. Este ataque puede ser particularmente efectivo en áreas con alta densidad de drones, donde la interferencia en un solo canal puede afectar a múltiples dispositivos simultáneamente.

CONCLUSIÓN
El despliegue global de los protocolos de Identificación Remota (RID) de drones, como el ODID y el DroneID de DJI, son fundamentales para la seguridad y la gestión del espacio aéreo. Sin embargo, las vulnerabilidades actuales en estos sistemas presentan riesgos significativos que deben ser abordados. La falta de mecanismos robustos de seguridad, como el cifrado y la autenticación, deja a los sistemas RID abiertos a un amplio espectro de ataques, que pueden simular la presencia de drones y causar interrupciones en infraestructuras críticas con consecuencias desastrosas.

Una vez más, la seguridad de las comunicaciones radio debe ponerse en valor, ya que como venimos explicando en esta sección, deben formar parte de nuestra estrategia de seguridad.

ALEX ALIAGA

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

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno del Cambio

P3MGO + ISO 21505

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación P3MGO Executive
- Certificación ISO 21505 Leader
- Módulo 8: MasterPPM®

MPPM®

eGob®

Del 20 al 28 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Marta Martín

Doblemente excepcional

La doble excepcionalidad es una lucha de fuerzas dispares y antagónicas. Por un lado, la oportunidad de una inteligencia excepcional y por otro, las habilidades de un cerebro revolucionado y centrado en miles de estímulos a la vez.

Imaginemos una persona con TDAH, el trastorno neurobiológico más común, caracterizado por la presencia de síntomas de inatención, impulsividad e hiperactividad que se pueden traducir en inquietud, nerviosismo, dificultad para esperar o para inhibir estímulos irrelevantes o conductas irreflexivas, entre otras manifestaciones. Un trastorno difícil de diagnosticar en adultos, con relativamente pocos años de estudio a sus espaldas, y que siempre viaja rodeado de una polémica alimentada por falsos mitos, negacionismo y estigmas de toda clase.

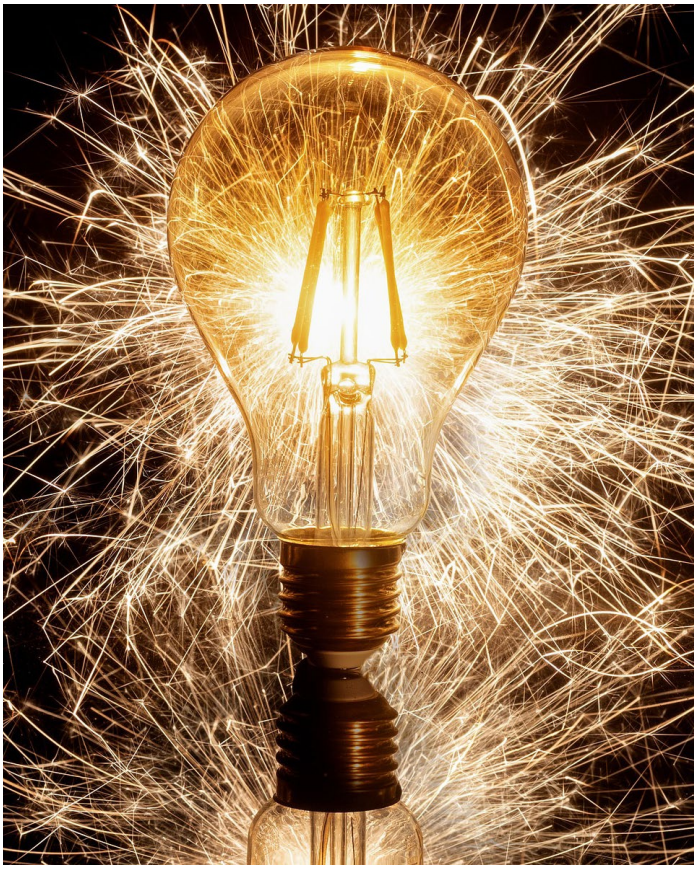
Imaginemos ahora una persona con altas capacidades (AACC) es decir, una persona con una inteligencia muy superior a la media, con un gran potencial, con una forma de aprender y de sentir diferente y con un desarrollo asincrónico.

No hay duda de que ambas son dos condiciones complejas por separado. Ahora imaginemos que confluyen en la misma persona, es decir, alguien que presenta TDAH y además altas capacidades. El resultado es la doble excepcionalidad. Por lo tanto, podemos decir que las personas doblemente excepcionales son aquellas que presentan altas capacidades intelectuales y creativas de forma simultánea con uno o varios trastornos limitantes, como por ejemplo el trastorno por déficit de atención e hiperactividad (TDAH), el trastorno del espectro del autismo (TEA) o dificultades de aprendizaje (dislexia, disgrafía, discalculia, etc.).

Si ya resulta difícil el diagnóstico por separado de cada una de estas condiciones, la detección de la doble excepcionalidad lo es aún más. Y esto es así por la escasez de información que existe al respecto, por su especial sintomatología, porque existen pocos profesionales capaces de identificarla, lo que nos da un error de diagnóstico o la falta del mismo, o porque una excepcionalidad solapa a la otra por lo que, en el mejor de los casos, una persona solo es diagnosticada o bien de su dotación intelectual, o bien de su dificultad de aprendizaje, con lo que no es tratado debidamente.

Lo más curioso es que la doble excepcionalidad no es la suma de dos condiciones complejas y paradójicas, sino que la suma de ambas es algo completamente distinto. Sin duda, la mejor forma de explicarlo es con la “metáfora del verde”, un concepto creado por Susan Baum, que relaciona la doble excepcionalidad con dos colores.

CONTINÚA EN PRÓXIMA PÁGINA



El amarillo representa la fortaleza de las AACC y el azul, el desafío del TDAH. Cuando se juntan, el resultado no es un trozo azul y otro amarillo, sino una gama infinita de verdes, con tantas combinaciones como personas doblemente excepcionales existen. E incluso, este verde no permanece inalterable ya que una misma persona, según el contexto puede un día aparecer más verde, otro más amarillo y otro más azul.

Desgraciadamente, toda esta gama de colores tan vistosos se traduce en problemas reales. Lo más normal es que un adulto con doble excepcionalidad no llegue a ser consciente de su condición si no ha sido diagnosticado en la infancia o en la adolescencia. Con mucha probabilidad, será un adulto que sabe que es muy inteligente pero que no se explica el porqué de tantos despistes, de tantos errores, de la dificultad para organizarse, para planificar su trabajo, para conseguir sus objetivos. Lo que le ocurre es que el potencial de las AACC tira hacia arriba, pero los síntomas del TDAH tiran hacia abajo.

Las personas con TDAH corrigen mejor las limitaciones de su sintomatología gracias a las AACC, buscan estrategias para compensar sus déficits. Sus altas capacidades intelectuales les proporcionan la motivación intrínseca que necesitan para cumplir objetivos, la perseverancia cuando algo es de su interés, los trucos para tener menos olvidos, para solucionar problemas…Es decir, tienen dos formas de afrontar esta complejidad, ponerse en modo AACC en lugar de en modo TDAH. Dicho así, parece sencillo, incluso ventajoso, pero no podemos perder de vista que en este caso también hay una doble ración de hipersensibilidad, de hiperactividad mental, de tendencia a frustrarse con facilidad, de animadversión hacia las críticas, etc.

Y es más, la persona con doble excepcionalidad siente por partida doble que no encaja. Los adultos con TDAH se pasan la vida intentando encontrar su sitio en una sociedad diseñada para los neurotípicos. Lo mismo les ocurre a las personas con altas capacidades, que no dudan en sacrificar su inteligencia y su potencial con tal de sentir la pertenencia al grupo. Pero cuando una persona es doblemente excepcional, no es ni TDAH ni AACC en sentido estricto. No pertenece a ningún sitio.

La doble excepcional sigue siendo el gran desconocido. A pesar de que el interés en el asunto ha ido en aumento con el consiguiente incremento de la investigación en este terreno, lo cierto es que la complejidad del diagnóstico diferencial hace que no siempre haya un consenso sobre la doble excepcionalidad, incluso que haya quienes dentro de la comunidad científica sigan insistiendo en que la doble excepcionalidad no existe.

El objetivo final no puede ser otro que poder diagnosticar porque sin un diagnóstico se corre el peligro de ser etiquetado como un vago, un irresponsable, un asocial, cuando en realidad no estamos frente a un problema de conducta, sino frente a una realidad neurobiológica. El diagnóstico es la explicación de lo que nos ocurre, de porqué somos como somos, cuáles son nuestras debilidades y cuáles las fortalezas que debemos trabajar.

MARTA MARTÍN

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

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

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

LIVE STREAMING

Curso de
Doble Certificación

Gobierno de la Externalización

SGF +
ISO 37500

Director Académico:
Javier Peris

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

MPPM®

eGob®

Del 18 al 26 de octubre

+ 34 96 109 44 44
campus@escueladegobierno.es

UNE y CEOE presentan el primer estándar global de igualdad de género

La Asociación Española de Normalización, UNE, y la Comisión de Igualdad y Diversidad de CEOE han presentado la Norma UNE-ISO 53800 Directrices para la promoción e implementación de la igualdad de género y el empoderamiento de las mujeres.

La Norma UNE-ISO 53800 propone un modelo para trabajar la igualdad entre mujeres y hombres en cualquier organización y con vocación de mejora continua, que incluye directrices, herramientas, buenas prácticas y otros recursos.

España ha participado activamente en su desarrollo a través del Comité UNE de Igualdad de género, presidido por Val Díez, presidenta de la Comisión de Igualdad y Diversidad de CEOE y directora general de STANPA.

En la imagen, de izda. a dcha.: Elena Ordozgoiti, UNE; Isabel Alonso, EJE&CON; Javier García, UNE e ISO; Val Díez, STANPA y CEOE; Julián Vicente Bravo, SIEMENS; María Muñoz, Ministerio de Industria y Turismo; y María Jesús Aguado, Ministerio de Igualdad.

La Asociación Española de Normalización, UNE, y la Comisión de Igualdad y Diversidad de CEOE han presentado hoy, en la sede de CEOE en Madrid, la Norma UNE-ISO 53800 Directrices para la promoción e implementación de la igualdad de género y el empoderamiento de las mujeres.

En la elaboración de este estándar internacional pionero han colaborado más de 100 expertos de 62 países de todo el mundo. España ha participado activamente a través del Comité UNE de Igualdad de género (CTN-UNE 194), liderado por Val Díez, presidenta de la Comisión de Igualdad y Diversidad de CEOE y directora general de STANPA. Además, UNE ha liderado el proceso de traducción al español de la Norma ISO 53800, como miembro nacional de ISO, para facilitar su comprensión y utilización a los cerca de 500 millones de hispanohablantes del mundo.

CONTINÚA EN PRÓXIMA PÁGINA

Este estándar global, pionero, propone un modelo de trabajo de la igualdad en las organizaciones, con independencia de su actividad, naturaleza o tamaño, que incluye directrices, herramientas, buenas prácticas y otros recursos que ayudarán a las organizaciones a evaluar su situación actual, identificar barreras y oportunidades, y a desarrollar acciones concretas.

El objetivo es que cada entidad se comprometa con la igualdad de género y fije sus objetivos partiendo de su situación y contexto, y que busque socios y colaboradores igualmente comprometidos creando una red de igualdad real y efectiva.

"La igualdad es determinante para la competitividad empresarial, impulsa la innovación y es un factor crucial para el avance de la sociedad. Las empresas españolas encontrarán en la Norma UNE-ISO 53800 un respaldo objetivo para afianzar su compromiso con la igualdad", ha destacado Val Díez.

Para Javier García, director general de UNE y vicepresidente de ISO, "Este estándar internacional marca el camino para alcanzar una igualdad de género efectiva y real en las organizaciones.

La Norma movilizará voluntades y provocará un efecto en cadena, de una entidad a otra, de una región del planeta a otra".

Destacados expertos en la Norma han explicado en la Jornada los fundamentos de este estándar internacional, su potencial impacto transformador y su aplicabilidad a la cultura organizacional. Así, han intervenido: Val Díez, presidenta del Comité UNE de Igualdad de género; Javier García, director general de UNE y vicepresidente de ISO; Elena Ordozgoiti, responsable del Sector Servicios de UNE; María Muñoz, vocal asesora de la Dirección General de Estrategia Industrial y de la PYME del Ministerio de Industria y Turismo; María Jesús Aguado, consejera técnica de la Subdirección para el Emprendimiento, la Igualdad en la Empresa y la Negociación Colectiva del Instituto de las Mujeres del Ministerio de Igualdad; Isabel Alonso, vocal de Buen Gobierno Corporativo de la Asociación Española de Ejecutiv@s y Consejer@s (EJE&CON); y Julián Vicente Bravo, responsable TPM, Ingeniería y Soporte Técnico Proyecto Airbus de SIEMENS.

Accede a la Norma UNE-ISO 53800 Directrices para la promoción e implementación de la igualdad de género y el empoderamiento de las mujeres.

Sobre la Asociación Española de Normalización, UNE

La Asociación Española de Normalización, UNE, es una organización global cuyo propósito es desarrollar normas técnicas o estándares que contribuyan al progreso compartido de la sociedad y a la creación de un mundo más seguro, sostenible y competitivo.
Las normas recogen el consenso del mercado sobre las mejores prácticas en aspectos clave para la competitividad de las organizaciones y para los intereses de toda la sociedad, siendo el resultado del diálogo y la colaboración conjunta de los sectores económicos y las Administraciones públicas.
Con la participación de más de 13.000 profesionales en sus mesas de trabajo, UNE es el representante español en los organismos de normalización internacionales (ISO e IEC), europeos (CEN-CENELEC y ETSI) y americanos (COPANT). Actualmente, el vicepresidente de ISO es el español Javier García, director general de UNE.

#UNEProgresoCompartido

Sobre CEOE

CEOE es la principal representante de las empresas en España ante la Administración, los organismos del Estado, las organizaciones sindicales, los partidos políticos y las instituciones internacionales. En Europa, CEOE es miembro activo de BusinessEurope, que agrupa a las asociaciones empresariales de todo el continente.
Desde su fundación en 1977, CEOE representa y defiende los intereses de los empresarios españoles. Agrupa, con carácter voluntario, a la mayoría de las empresas y empresarios individuales de cualquier tamaño o sector a través de asociaciones de base, que forman una red de más de 200 organizaciones empresariales.

Hace mucho tiempo que hablas.

¿Pero hace cuánto no dialogas?

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

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

UNE Normalización Española

Progreso compartido

une.org

NUEVOS MASTERS

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