

REVISTA Tecnología & Sentido Común



#60

FEBRERO
2026

Ramiro Cid

NUESTRO INVITADO
A #TYSO

24

El Gobernauta

JAVIER PERIS

08

Futuro y Seguridad

MANUEL SERRAT

12

Tecnoregulación en Prospectiva

NACHO ALAMILLO

16

Es tendencia

MARLON MOLINA

32

Ojo al dato

RICARD MARTÍNEZ
MARTÍNEZ

36

Radio Security

ALEX ALIAGA

48

La nueva Administración

VÍCTOR ALMONACID

44

El lado oscuro

DOMINGO GAITERO

20

Ai Ai Ai

MARCOS NAVARRO

40

Mentes Divergentes

MARTA MARTÍN

52



9 772951 818003

60

REVISTA **Tecnología & Sentido Común**



EQUIPO TYSC

Javier Peris - El Gubernauta
Manuel Serrat - Futuro y Seguridad
Nacho Alamillo - Tecnoregulación en Prospectiva
Domingo Gaitero - El Lado Oscuro
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Marcos Navarro - Ai Ai Ai
Víctor Almonacid - La Nueva Administración
Alex Aliaga - Radio Security
Marta Martín - Mentas Divergentes

PUBLICIDAD Y CONTRATACIÓN

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

GABINETE JURÍDICO

Jesús López Peláz

ATENCIÓN AL LECTOR

soluciones@businessandcompany.com

EDITA

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



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

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

ISSN 2951-8180

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



Curso de Certificación en: **Gobierno Corporativo**

ISO 37000 Corporate Governance Leader

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 37000
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

#60

FEBRERO 2026



índice

DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



Ramiro Cid



La geopolítica es tendencia



La IA no es una opción, es un imperativo



Equilibrio digital y TDAH

Copyright

02

Índice de Contenidos

04

Este mes te recomiendo leer...

por JAVIER PERIS

07

ITIL 5 & SMBok: Juntos pero no revueltos

EL GOBERNAUTA
JAVIER PERIS

08

Aplicaciones móviles: cuando la falta de seguridad pone en riesgo nuestros datos (I)

FUTURO Y SEGURIDAD
MANUEL SERRAT OLMOS

12

Un nuevo impulso a la normalización de los contratos electrónicos

TECNOREGULACIÓN
EN PROSPECTIVA
NACHO ALAMILLO

16

Subidas a destrucción, digo a producción

EL LADO OSCURO
DOMINGO GAITERO

20

Ramiro Cid

NUESTRO
INVITADO A TYSC

24

La geopolítica es tendencia

ES TENDENCIA
MARLON MOLINA

32

Soy persona delegada de protección de datos: NO ES MI FUNCIÓN...

OJO AL DATO
RICARD MARTÍNEZ
MARTÍNEZ

36

La IA no es una opción, es un imperativo

Ai Ai Ai
MARCOS NAVARRO

40

Cómo introducir IA en los ayuntamientos sin crear un agujero legal

LA NUEVA ADMINISTRACIÓN
VÍCTOR ALMONACID

44

El nuevo campo de batalla no se ve, se transmite

RADIO SECURITY
ALEX ALIAGA

48

Equilibrio digital y TDAH

MENTES DIVERGENTES
MARTA MARTÍN

52

La normalización, clave para generar confianza y competitividad en el análisis del Informe del Banco Mundial

NORMALIZACIÓN

56

#60 - FEBRERO 2026

Índice

#TYSC

Premios recibidos



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



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

itSMF
ESPAÑA

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



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

a pep | Asociación Profesional Española de Privacidad

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



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

 COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática



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

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

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

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

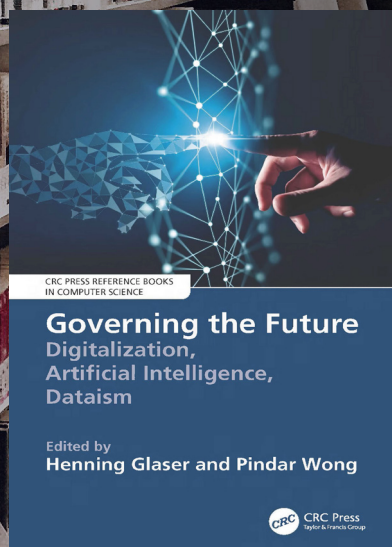
eset

Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA



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

AVIS@
ASOCIACIÓN VALENCIANA DE INFORMÁTICA SANITARIA



Governing the Future

Digitalization,
Artificial Intelligence, Dataism

Henning Glaser & Pindar Wong

Este mes, os invito a sumergiros en “Governing the Future”, una obra coordinada por Henning Glaser y Pindar Wong que aborda y disecciona de forma magistral la “*Technetronic Revolution*” o revolución “*tecnotrónica*” como la denominan los autores. En este libro, se analiza cómo la digitalización, la inteligencia artificial y el “*dataísmo*” están reconfigurando nuestra realidad.

Su gran acierto es el enfoque interdisciplinar, que une derecho, sociología y filosofía para debatir la gobernanza en un mundo donde el poder es ya eminentemente computacional. Este libro destaca por su análisis del «capitalismo de vigilancia» y la urgencia de marcos éticos que protejan la dignidad humana frente al imperio absoluto de los datos.

Una de las aportaciones fundamentales y que a mí me ha resultado especialmente valiosa es su propuesta de una educación renovada para navegar este mundo de cambios, recordándonos que el futuro no debe quedar al azar de los algoritmos. Los autores consiguen que entendamos que gobernar el futuro es, ante todo, una urgencia humana y política. Es una lectura imprescindible para quienes buscamos aplicar el sentido común a una tormenta tecnológica que, sin una brújula ética, amenaza con desbordarnos. En definitiva un libro fundamental para todos los Gobernautas.

ITIL 5 & SMBoK: Juntos pero no revueltos

El 29 de enero de 2026 quedará marcado en el calendario de la gestión de servicios como un día importante. Tras años de especulaciones, PeopleCert ha lanzado oficialmente ITIL 5, una versión que nace con la ambición de gobernar la era de la Inteligencia Artificial Generativa y las operaciones autónomas. Sin embargo, en los despachos de los Directores de Servicio más experimentados, otro acrónimo suena con igual o mayor fuerza: el **SMBoK® (Service Management Body of Knowledge)** del Service Management Institute (SMI).

¿Estamos ante una guerra de estándares? ¿Debe el profesional elegir un bando? La respuesta, cargada de ese "Sentido Común", es un rotundo no. ITIL 5 y el SMBoK no son competidores en un ring, sino los dos hemisferios de un mismo cerebro

organizacional. En este artículo, desgranamos por qué su coexistencia es la clave del éxito en el complejo ecosistema digital de 2026.

Si ITIL 4 (lanzado allá por 2019) fue el puente hacia la agilidad y el flujo de valor, ITIL 5 es el motor a reacción que permite navegar en la atmósfera de la Inteligencia Artificial. La nueva versión no reniega del Sistema de Valor del Servicio (SVS), pero reconoce que el componente humano en la ejecución de procesos ya no es el cuello de botella: es el supervisor de un sistema autónomo.

ITIL 5 introduce conceptos revolucionarios como los **"Managed AI Services"** y la **"Entrega Autónoma"**. Ya no hablamos solo de cómo gestionar un incidente, sino de cómo entrenar a un modelo de lenguaje para que resuelva el 90% de



los incidentes de forma predictiva antes de que el usuario note el impacto. El enfoque se desplaza de la gestión de activos hacia la **Gobernanza de Datos Proactiva**. En ITIL 5, el dato no es un recurso, es el combustible que mantiene viva la capacidad de servicio.

Sin embargo, ITIL sigue siendo, en esencia, un marco de trabajo de propiedad privada. Su objetivo es la eficiencia operativa y la certificación de capacidades. Es excelente para decirnos cómo configurar una organización para que sea rápida, pero a veces deja un vacío cuando nos preguntamos: *¿Qué significa ser un profesional de la gestión de servicios más allá de la herramienta?*

Aquí es donde entra el **SMBok® del Service Management Institute**. Mientras ITIL 5 evoluciona con la tecnología, el SMBok se mantiene firme como el pilar de la profesión. Si ITIL es el manual del coche de carreras (especialmente de los motores de IA actuales), el SMBok es el tratado de ingeniería y ética que define qué es un piloto profesional.

El SMBok no nació para ser un "framework" más. Es un Cuerpo de Conocimiento. Su enfoque es agnóstico y universal. No le importa si utilizas ITIL, COBIT, VeriSM o Lean; lo que le importa es que el **Director de Servicios** (una figura que el SMBok eleva a nivel directivo) domine las competencias necesarias para gobernar cualquier servicio, ya sea en el sector salud, la banca o la educación más allá por supuesto de tecnologías de la información pero con el aporte que pueden y deben dar las tecnologías de la información.

El gran valor diferencial del SMBok reside en su base empírica. Mientras que ITIL nos presenta escenarios ideales de flujo de valor, el SMBok nos entrega la realidad

cruda: sus **132 Fichas de Mejores Prácticas y sus 197 Casos de Éxito y Fracaso**. En Dirección de Servicios, saber por qué falló un proyecto de Inteligencia Artificial en una multinacional es mucho más valioso que leer la definición teórica de una práctica de gestión de cambios.

Para comprender por qué estos dos gigantes están "juntos pero no revueltos", es imperativo desgranar sus naturalezas desde una perspectiva narrativa. Mientras que ITIL 5 se manifiesta como una evolución tecnológica y táctica, el SMBok se erige como un estándar de autoridad profesional. Esta distinción comienza en su misma génesis: ITIL es un marco de trabajo de propiedad privada, gestionado por PeopleCert con una clara orientación hacia la eficiencia operativa y la acreditación masiva. Por el contrario, el SMBok es un cuerpo de conocimiento abierto, nacido del seno del Service Management Institute como una asociación sin ánimo de lucro con más de 20 años de historia y experiencia, cuyo fin no es vender un método, sino estandarizar la madurez de una profesión que, hasta ahora, carecía de un lenguaje directivo universal.

Si analizamos sus pilares estructurales, la divergencia se hace aún más evidente. ITIL 5 articula su propuesta a través de su ya conocido Sistema de Valor del Servicio, pero lo vitamina con un enfoque donde la Inteligencia Artificial no es un añadido, sino el núcleo de sus nuevas prácticas. Aquí, el objetivo es el "flujo": que el valor viaje desde la



**CONTINÚA EN
PRÓXIMA PÁGINA**



demanda hasta el consumo con la mínima fricción humana posible. El SMBoK, en cambio, organiza su sabiduría en cinco grandes capítulos y treinta y ocho áreas temáticas que no se limitan al "paso a paso" técnico, sino que exploran la dirección estratégica. Mientras ITIL nos habla de la capacidad de la organización para entregar un servicio, el SMBoK nos habla de la capacidad del individuo, el Director de Servicios, para liderar esa entrega.

El tratamiento de la Inteligencia Artificial en este 2026 es, quizás, el punto donde la convivencia se vuelve más interesante. Para ITIL 5, la Inteligencia Artificial es el motor de la "Entrega Autónoma"; es una cuestión de algoritmos, entrenamiento de modelos y gobernanza de datos para la auto reparación de sistemas. Para el SMBoK, la Inteligencia Artificial es una herramienta poderosa pero supeditada a la ética y al juicio directivo. El SMBoK no se detiene en cómo configurar un bot de soporte, sino en cómo ese bot afecta el compromiso del cliente y qué responsabilidades legales y morales asume el directivo sobre las decisiones de una máquina.

Incluso en su aproximación al riesgo y al aprendizaje, ambos modelos ofrecen perspectivas complementarias. ITIL 5 es predictivo y se apoya en el aprendizaje automático para mitigar fallos antes de que ocurran. El SMBoK, con un enfoque mucho más empírico y humano, se nutre de la experiencia acumulada: sus casi doscientos casos de éxito y fracaso documentados ofrecen una sabiduría que ninguna red neuronal puede replicar todavía. Es la diferencia entre tener un GPS de última generación (ITIL 5) y contar con la bitácora de un capitán que ha naufragado y sobrevivido para contarla (SMBoK).

En última instancia, la distinción más crítica reside en el enfoque del rol. ITIL 5 busca certificar que una persona "sabe ITIL", mientras que el SMBoK busca validar que una persona "es un Director de Servicios". El primero garantiza la competencia técnica en un marco específico; el segundo garantiza la autoridad profesional de manera agnóstica, permitiendo que un líder gestione con éxito tanto una infraestructura de nube cuántica como un servicio de atención hospitalaria, utilizando para ello las herramientas que mejor le convengan, sea ITIL 5 u otra cualquiera.

Esta es quizás la distinción más profunda. ITIL 5 se enfoca en la **Organización**. Busca que la entidad sea capaz de entregar valor. El SMBoK se enfoca en el **Individuo**. Define las cuatro interfaces críticas que un Director de Servicios debe gestionar:

1. **Hacia arriba (Gobierno):** Cómo hablar el lenguaje de la junta directiva.
2. **Hacia los lados (Horizontal):** Cómo interactuar con otras áreas de negocio.
3. **Hacia abajo (Gestión):** Cómo liderar equipos técnicos.
4. **Hacia afuera (Habilitación):** Cómo asegurar que la operación sea excelente.

Imaginemos una organización que decide implementar ITIL 5 para modernizar su Service Desk mediante agentes autónomos. Sin el SMBoK, esta organización corre el riesgo de tener una tecnología punta pero una carencia total de liderazgo profesional. Puede que los procesos fluyan, pero ¿quién asegura que la ética de esos datos sea la correcta? ¿Quién gestiona el compromiso de los empleados que se sienten desplazados por la IA?

El **sentido común** nos dice que:

• **ITIL 5 aporta la agilidad técnica:** Nos da las recetas para que los

microservicios, la IA y las prácticas de gestión operen en armonía.

• **El SMBoK aporta la madurez estratégica:** Nos da el marco ético y profesional para que esa agilidad no se convierta en caos.

Un profesional certificado como *ITIL 5 Master* tiene un conocimiento técnico envidiable. Un profesional certificado como *Service Management Professional (SMP®)* por el SMI tiene una autoridad profesional reconocida. El que posee ambas, es el líder que las empresas están buscando desesperadamente en este 2026.

A menudo se critica a ITIL por ser "demasiado limpio". El SMBoK, en cambio, se ensucia las manos. Sus 38 Áreas Temáticas profundizan en aspectos que ITIL apenas roza:

• **La Gestión del Compromiso:** No solo con los clientes, sino con todos los stakeholders en un nivel humano.

• **La Excelencia en el Servicio:** Basada en estándares como la ISO 23592, que el SMBoK integra de forma natural.

• **El aprendizaje del error:** Los casos de fracaso documentados en el SMBoK son una cura de humildad y una fuente de ahorro de costes incalculable para cualquier empresa.

Por otro lado, ITIL 5 ha dado un salto gigante en la **Gobernanza de Datos**. En un mundo donde la IA se alimenta de información, ITIL 5 explica cómo asegurar que esa alimentación sea continua y de calidad. El SMBoK toma ese dato y explica cómo el Director de Servicios debe usarlo para influir en la estrategia de la compañía. Es una cadena de valor perfecta.

La publicación de ITIL 5 hoy no invalida el SMBoK; lo hace más necesario. En un entorno de alta volatilidad tecnológica, los marcos de trabajo cambian cada pocos años (v3 en 2007/2011, v4 en 2019, v5 en 2026). Sin embargo, los principios de la Dirección de Servicios que promulga el SMI son atemporales.

El mensaje debe ser claro: **No confunda el mapa con el territorio.**

• **El mapa es ITIL 5:** te indica las rutas más rápidas, los nuevos caminos de la IA y cómo evitar los atascos operativos.

• **El territorio es la Gestión de Servicios profesional que describe el SMBoK:** el terreno real donde se juega la reputación de la empresa, la ética de los negocios y el desarrollo de las personas.

Estamos en un momento apasionante. ITIL 5 nos ofrece los juguetes más avanzados que jamás hayamos tenido: IA generativa integrada, operaciones que se autorreparan y flujos de valor casi instantáneos. Pero como bien sabemos en esta revista, la tecnología sin sentido común es solo ruido caro.

El SMBoK es el sentido común codificado. Es la voz que nos recuerda que, detrás de cada algoritmo de IA en ITIL 5, hay un servicio que debe satisfacer a una persona y un Director de Servicio que debe rendir cuentas por ello.

En 2026, la excelencia no se encuentra en elegir entre ITIL 5 o SMBoK. La excelencia reside en entender que son **juntos pero no revueltos**: ITIL en la caja de herramientas, y el SMBoK en la mente del directivo. Solo así conseguiremos que la tecnología, por muy avanzada que sea, siga estando al servicio de lo humano.



JAVIER PERIS

Javier Peris es Socio Director y CKO (Chief Knowledge Officer) de Business Technology & Best Practices (Business&Co.®) especializado en Gestión del Portfolio, Programas y Proyectos, Centros de Excelencia así como Marcos de Gobierno y Gestión de Tecnologías de la Información con más de 20 años de experiencia tanto en empresas como en Organismos Oficiales y Administración Pública. Es Profesor de IE Business School e IE Executive Education y dispone de las Acreditaciones Internacionales CGEIT®, CRISC®, COBIT5® Certified Assessor, ITIL® Expert & Trainer, PRINCE2® MSP® MoP® MoV® MoR® P30® Practitioner & Trainer, Sourcing Governance®, VeriSM™ SIAM™, OKR, Lean, Kanban, Design Thinking, Scrum & AgileSHIFT® Accredited Trainer ejerce como Business Coach, Business Angel e Interim Manager.

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

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gobierno del
Tiempo y
Gestión de la
Productividad**

**Time Slot
Governance
Yellow Belt**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el TSG4® Yellow Book
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

Aplicaciones móviles: cuando la falta de seguridad pone en riesgo nuestros datos (I)

En esta segunda parte de nuestro artículo sobre las apps móviles y su seguridad, entraremos en mayor detalle en cómo se producen esas inseguridades, y las cuestiones a las que debemos prestar atención durante la selección, instalación o uso de las mismas.

SEGUNDA PARTE: Cómo y por qué las apps inseguras exponen datos personales

Después de entender el contexto general, como hicimos en el artículo del mes pasado de Tecnología y Sentido Común, es importante profundizar en los mecanismos que hacen que una app pueda convertirse en una amenaza para nuestra privacidad o seguridad. Ojo, que no estamos hablando de aplicaciones directamente maliciosas, sino de aplicaciones legítimas cuyo funcionamiento interno puede dar lugar a desagradables sorpresas. Aunque el funcionamiento interno de las aplicaciones puede parecer complejo, los riesgos pueden explicarse de forma sencilla y accesible.

En muchas aplicaciones, el primer punto crítico aparece al instalarla: la solicitud de permisos. Por ejemplo: ¿Por qué una app para editar fotos necesita leer nuestros contactos? ¿Por qué un juego de rompecabezas pide acceso a la ubicación en tiempo real? ¿Por qué una app de linterna solicita permiso para grabar audio?

Aunque pueda parecer absurdo, estas prácticas son habituales, y muchas personas ni siquiera verifican lo que la app les está exigiendo. Algunos permisos se utilizan para mejorar la publicidad dirigida; otros, para vender datos agregados a terceros; y otros, simplemente, son restos de un diseño deficiente en el que nadie revisó qué era realmente necesario.



CONTINÚA EN
PRÓXIMA PÁGINA



Cuando un usuario otorga permisos excesivos, la aplicación puede:

- identificar localizaciones precisas a lo largo del día,
- analizar rutinas y desplazamientos,
- acceder a imágenes privadas,
- leer contactos o información de otros servicios,
- o activar sensores como el micrófono o la cámara.

Esto no significa que todas las apps realicen espionaje activo, pero **sí que tienen la capacidad técnica de hacerlo** si el desarrollador, un atacante o un error lo permite.

Otro de los focos de riesgo se encuentra en el almacenamiento. Una app puede recopilar datos legítimos, pero almacenarlos en carpetas mal protegidas. En otros casos, las contraseñas se guardan como texto plano o los tokens de autenticación se escriben en un archivo accesible a otras aplicaciones. Para un atacante con acceso físico o remoto, esto supone una puerta abierta a esas aplicaciones mal configuradas o desarrolladas. Además, muchas aplicaciones dejan archivos temporales sin cifrar, como fotos procesadas, documentos descargados, registros de actividad, o copias de seguridad incompletas. Y la "basura digital", de la misma forma que en su día lo era la basura física, puede convertirse en un auténtico tesoro para quien busque información confidencial.

Nuestro tercer foco de riesgo lo encontramos en las comunicaciones. Cuando abrimos una app de mensajería, de un banco o de un servicio de compras, asumimos que la información viaja cifrada, pero no siempre es así. Algunas aplicaciones usan versiones antiguas de protocolos seguros, envían datos sensibles sin un algoritmo de cifrado adecuado, o combinan elementos cifrados con elementos no protegidos.

El resultado es que si nos conectamos a una red WiFi pública, cualquier persona con herramientas básicas podría interceptar información potencialmente sensible, como nombres, emails o incluso contraseñas, si estamos usando esas aplicaciones que no cifran completamente sus comunicaciones.

La cuarta pata de la inseguridad de las aplicaciones móviles está en la Nube. Muchas apps almacenan datos en servidores externos del fabricante de las mismas. Si esos servidores están mal configurados, tienen vulnerabilidades en su software, o son accesibles sin autenticación adecuada, la información puede quedar expuesta. No se necesita un "gran hackeo"; basta con un enlace mal protegido o una base de datos sin contraseña y la información estará en manos de quien no debe.

En 2021 los investigadores de Check Point Research revelaron que más de 100 millones de usuarios de Android habían visto expuestos sus datos por culpa de malas configuraciones en servicios en la nube usados por sus apps. Concretamente, en 23 aplicaciones analizadas, algunas con millones de descargas,



se detectaron bases de datos públicas, sin los controles de autenticación adecuados.

Esto permitió que cualquiera, conociendo la URL correcta, accediera a información personal sensible: correos electrónicos, contraseñas, geolocalizaciones, identificadores de dispositivos, chats privados, e incluso detalles de pagos. Entre las apps afectadas había desde herramientas de diseño de logos, o apps de contabilidad, hasta apps de transporte o entretenimiento. Este escándalo demostró que el uso de la nube, y en particular de servicios populares como bases de datos en tiempo real o almacenamiento en nube, no garantiza por sí solo la seguridad: la configuración correcta y consciente es fundamental.

Finalmente, una app puede ser segura, pero si usa herramientas de terceros que no lo son, podemos sufrir impactos inesperados. Es lo que se suele denominar **cadena de suministro**. Servicios de publicidad, librerías de análisis, módulos de ubicación, motores de reconocimiento, o SDKs incluidos por comodidad, pueden recopilar información adicional sin que el desarrollador principal sea plenamente consciente. Y si son trojanizados por ciberdelincuentes, el éxito en su afán de robo de información está garantizado. Debido a las cadenas de dependencias que puede contener una sola app, los datos del usuario pasan por múltiples manos sin control directo, y la complejidad del ecosistema hace difícil saber quién tiene acceso a qué.

El artículo del próximo mes, que da fin a esta serie, se centrará en explicar cómo podemos tratar de protegernos de esta problemática, y cómo incorporar a nuestra cultura de la protección digital el uso de apps móviles.



MANUEL SERRAT OLMOS

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

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

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

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gestión
del Dato**

UNE 0078

**Data
Management
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en la Norma: UNE 0078
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

Un nuevo impulso a la normalización de los contratos electrónicos

El Comité Europeo de Normalización dispone del CEN/TC447, presidido por BSI y dedicado a la producción de estándares horizontales para la provisión de servicios, y que tiene a UNE CTN9/SC1 como espejo nacional, bajo secretaría de mi querido Service Management Institute.

El campo de aplicación incluye la normalización de los aspectos horizontales propios del conjunto de los sectores prestadores de servicios o de un grupo de ellos. Se consideran aspectos horizontales las etapas que habitualmente recorre un servicio (diseño, comercialización y difusión, provisión, facturación, revisión o terminación del servicio) así como los aspectos para su gestión, procedimientos y excelencia, entre otros; y de la actividad propia de sectores prestadores de servicios específicos, en todos los aspectos que sirvan para definirlos y distinguirlos (organización interna, requisitos de calidad, niveles de prestación u otros), en tanto no dispongan de un comité propio, quedando excluidos del campo de actividad los sectores de servicios competencia de otros CTN.

Algunas de las normas producidas por el CEN/TC447 abordan cuestiones contractuales; en concreto, en el pasado se han publicado las normas UNE-EN 17371-1:2021. Prestación de servicios. Parte 1: Compra de servicios. Guía para la evaluación de la capacidad de los proveedores de servicios y evaluación de las propuestas de servicios; UNE-EN 17371-2:2022. Prestación de servicios. Parte 2: Contratos de servicios. Guía para el diseño, el contenido y la estructura de los contratos; y UNE-EN 17371-3:2021. Prestación de servicios. Parte 3: Gestión de la medición del desempeño. Guía sobre el mecanismo para medir el desempeño como parte de los contratos de servicios.

El pasado mes de enero he tenido el honor de ser nombrado coordinador del CEN/TC447/WG1, a propuesta de UNE y tras el correspondiente voto, por un periodo de seis años. Este grupo de trabajo precisamente se encuentra dedicado a los contratos y acuerdos de servicio, y como primera acción del nuevo programa de trabajo, se ha iniciado la votación de un nuevo proyecto de norma, dedicada a los Contratos electrónicos – directrices sobre accesibilidad, presentación y formalización. Como se explica en la propuesta de trabajo sometida a votación, cada vez son más las empresas que anuncian, contratan y prestan servicios y suministran productos, ya sea parcial o totalmente, a través de un medio digital. Dada esta tendencia creciente y la naturaleza del medio digital, existe tanto una oportunidad como una importancia cada vez mayor para garantizar la claridad y la certeza en torno a la contratación electrónica para ambas partes contratantes.

En un mundo analógico, una copia impresa de un contrato se enviaría generalmente de una parte a otra para su revisión, negociación y, finalmente, formalización. En el mundo digital, donde el contrato se ha digitalizado, puede haber numerosas formas de acceder, presentar y formalizar dichos contratos. Esta propuesta pretende establecer las mejores prácticas para acceder, presentar y ejecutar contratos electrónicos, especialmente los términos y condiciones no negociados.



CONTINÚA EN
PRÓXIMA PÁGINA



Photographer's Signature



En efecto, la contratación electrónica a través de Internet, y no sólo en el ámbito de las relaciones con los consumidores, se instrumenta como contratos con cláusulas predispuestas, generalmente publicadas en la página web del proveedor, frecuentemente en forma de avisos legales, términos y condiciones, o centros de cumplimiento, lo que dificulta la aplicación de las técnicas tradicionales de formalización contractual. A veces es francamente difícil conocer qué versión de los términos y condicionales se ha aceptado, o qué versión actual resulta aplicable.

El contenido propuesto inicialmente para la futura norma sería la disponibilidad y ubicación en línea de un contrato electrónico; la gestión de los cambios en un contrato electrónico; la presentación del contrato electrónico para su revisión por parte de los clientes; la navegación por el contrato electrónico y la ubicación de su información clave; y la formalización de un contrato electrónico.

Por ello, es especialmente pertinente establecer directrices técnicas para facilitar la accesibilidad y la presentación de los contratos electrónicos, pero también para su formalización, siempre asumiendo que nos referimos a trabajo de tipo técnico y no jurídico. Y es que los organismos de normalización no deben, ni pueden, producir normas que desplacen la aplicación del Derecho, en especial de las normas de la contratación civil, mercantil o administrativa. Sí, pueden, sin embargo, aportar directrices y otras pautas en orden a facilitar el cumplimiento

de la normativa aplicable a cada caso, desde esta perspectiva técnica, con un especial foco puesto en favorecer los servicios excelentes.

De otra parte, y como también se indica en la propuesta, resulta especialmente pertinente que la misma no pretenda sustituir otros trabajos de normalización, especialmente los relacionados con las firmas electrónicas u otros servicios de confianza, que tienen su propio marco de desarrollo, particularmente en el Instituto Europeo de Normas de Telecomunicación. Dichas normas se citarían adecuadamente, para evitar cualquier posible solapamiento o contradicción. Del mismo modo se debería realizar con las normas de accesibilidad por personas con diversidad funcional, que se encuentran ampliamente desarrolladas.

Sirva esta breve publicación, finalmente, para hacer un llamamiento a expertos a contribuir a este revitalizado proyecto, de modo que se convierta en una palanca adicional para la prestación de servicios digitales.



NACHO ALAMILLO

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

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

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

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

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gestión de la
Inteligencia
Artificial**

**ISO 42001
AI Management
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

Domingo Gaitero

Subidas a destrucción, digo a producción

Lunes, 09:00 de la mañana, en cualquier oficina de Madrid (pero podía ser de España sinceramente).

Mónica, la responsable de calidad llega apresuradamente a la oficina porque ha sido avisada de que ha ocurrido un problema grave en un cliente importante al que parece ser se le ha emitido 8 facturas de un servicio que no había pedido, y lo peor de todo es que se le ha cobrado. Se ha convocado al comité de crisis y el tema no pinta bien.

Al llegar a la reunión ve a todo el mundo muy nerviosos y chillando, al verla a ella todos se callan se sienta y Don Francisco pide que comience la reunión. Mónica se fija que ni Alfonso, el de seguridad, ni Enrique el de legal están presentes, al preguntar por ellos se entera, atónita, que ambos han comunicado que no consideran necesario asistir ya que ha sido claramente un problema de desarrollo.

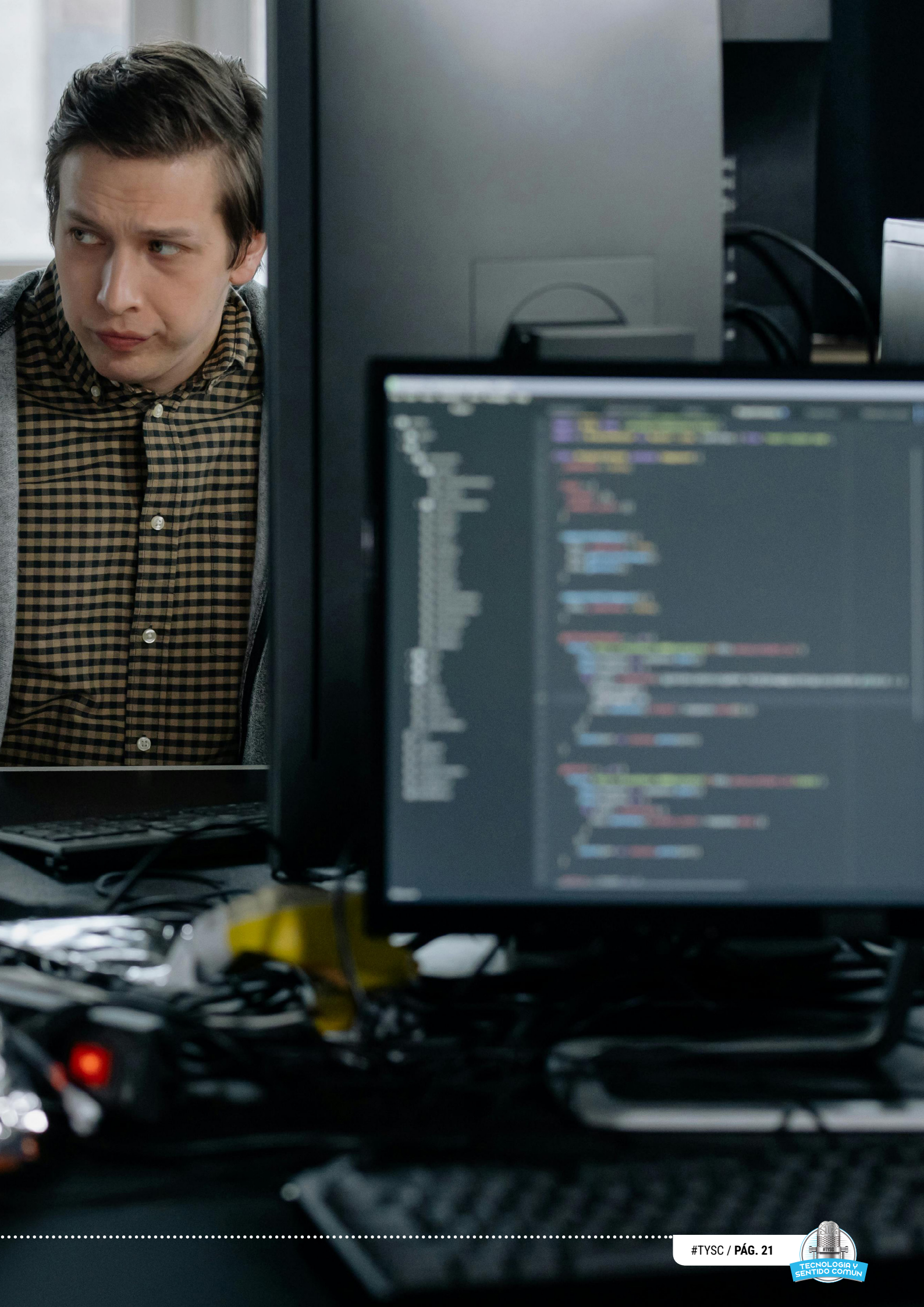
Don Francisco no le da importancia y quiere saber como solucionarlo, Mónica levanta la mano y propone enterarse antes de lo que ha pasado y como ha pasado. Allí recibe el primer bofetón donde la dicen que ya hará el informe más tarde y que ahora lo importante es solucionar el tema.

Lo que resulta de entender es porque están discutiendo Javier y Rodrigo que son del mismo equipo, al parecer Javier alega que "sólo era un cambio pequeño", mientras que Rodrigo dice que cuando el estaba trabajando "nadie más estaba tocando la aplicación". Mónica preguntó que quien era el responsable de subir a producción la versión final y ahí Antonio el jefe de desarrollo, indicó que ellos son un equipo altamente capacitado y que cualquier podía subir cosas a producción, ya que "todos somos responsables".

Sergio, el quality software, añadió que en este caso concreto se lavaba las manos ya que esas subidas no habían pasado por testing, debido a que corría prisa hacer esa subida de versión, que por cierto había dudas de si era la 24 o la 25 porque el responsable de la herramienta de configuración estaba de vacaciones.



CONTINÚA EN
PRÓXIMA PÁGINA



En aquel momento, Raquel, la directora de legal, mujer de armas tomar, comunicó que el cliente había aceptado las disculpas y que no iba a poner ninguna denuncia, a cambio había bajado dos ofertas presupuestadas y además les tenía que dar entradas para ir a ver al Madrid, eso no les preocupó mucho porque el siguiente partido era de copa frente al Albacete así que accedieron y todo se solucionó así. En ese momento Don Francisco miró a Mónica y la dijo, "ahora si puedes hacer el informe", tema solucionado.

No lo sabían, pero estaban atrapados por EL LADO OSCURO.

Esa guerra no declarada oficialmente que se vive en las empresas en la frontera que está entre la entrega final del software y su puesta en marcha en el cliente, conocido como "subida a Producción", es uno de los puntos más críticos que viven la mayoría de las empresa a pesar de haber creado un nemotécnico llamado "Devops".

Desde los tiempos de la Ingeniera de software de Roger Pressmann, existe un proceso TI denominado Gestión de la configuración que une un triangulo mágico que se establece entre otros tres procesos "core": requisitos, desarrollo y pruebas.

Desde mi punto de vista el enfoque para solucionar esa guerra está equivocado, porque hay mucha tecnología (SCM, Dockers, Github...) y hay procesos, lo que no existe es una "gestión de Egos", y os aseguro que entre desarrollo y producción los egos superan al mismísimo vestuario de cualquier equipo de élite.

Y aquí es donde no vemos que el uso de un producto software será ejecutado como un servicio, y que la forma de crear un producto y hacerlo con calidad para que funciones, no tiene que ver con las habilidades y el conocimiento necesario para saber gestionar un servicio y atender a un cliente en base a su "día a día".

Aunque la mayoría de los desarrolladores lo nieguen, su trabajo se realiza muy lejos del cliente, de ahí la importancia de incorporar metodologías ágiles que involucren al cliente en el desarrollo.

Otro gran fallo es el desprecio por las pruebas. Hay tiempo para todo, hasta para documentar, sin embargo probar no encuentra su tiempo.

Y llegados a este punto volvemos a hablar sobre la falta de responsabilidad, porque desarrollar sin validar con el cliente es irresponsable, subir a producción una aplicación si probar es una irresponsabilidad, subir a producción si una gestión de la configuración es irresponsable, como lo es pensar que un error de este tipo no es un error de seguridad, o que el departamento legal no se sienta afectado por un problema ocasionado en esta parta del ciclo de vida.



Y desde mi punto de vista la subida a producción no se rompe por falta de talento la mayoría de las veces, sino que se rompe por ausencia de proceso técnicos o por falta de automatización, o mucho más grave, por falta de respeto al entorno.

Permitir en una organización que cualquiera pueda subir a producción no empodera al equipo sino que lo expone y si realmente la estrategia de tu empresa es "esperemos que no pase nada", tu no tienes una cultura de calidad, tienes Fe, y la fe no escala.

La próxima vez que hagas una subida a producción en tu empresa procura que el proceso "lo dispare" la aprobación de pruebas, obliga a que la subida la haga un responsable de este proceso, íntimamente ligado al de gestión de la configuración, y que el equipo de deploy tenga todo lo necesario para actuar en el cliente.

Trabajar en equipo da muchas más ventajas que no hacerlo, y no solo en este proceso, sino en todos, nuestra informática debe ser de producción no de destrucción.

Todo lo escrito aquí es imaginado, cualquier parecido con la realidad de los hechos o nombres es pura coincidencia.



DOMINGO GAITERO

Domingo Gaitero es un consultor y emprendedor que, pese a haber sufrido varias adversidades desde su temprana juventud, ha logrado construir una carrera distinguida en el sector de las Tecnologías de la Información.

Domingo se caracteriza por ser un ponente excepcional dotado de un enorme sentido del humor, así como por ser un maestro de la resiliencia. Con su amplio bagaje de conocimientos y experiencia, su pasión es ayudar a todo aquel que quiera mejorar o cambiar su forma de vida.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



Curso de Certificación en: Excelencia en el Servicio Público

ISO 11637 Public Service Excellence Leader

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 11637
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001: 2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**



Ramiro Cid

Introducción

Hola Ramiro, es un verdadero placer tenerte aquí para esta entrevista. Tu trayectoria en ciberseguridad tiene una combinación poco usual de experiencia en entornos IT y OT (industrial) sumada recientemente a una visión estratégica de la Inteligencia Artificial.

Hablando antes de la entrevista me comentaste que intentas situarte en la vanguardia de un cambio de paradigma que pasa por el uso de la IA no solo como una herramienta de cyber-defensa, sino como el eje central de la gobernanza corporativa moderna. Ramiro, estoy seguro de que tienes mucho que compartir con nosotros hoy.

¿Quién es Ramiro Cid?

Si tuviera que realizar una definición de mi mismo, diría que soy intelectualmente curioso muy persistente y sociable. Viví 27 años en Buenos Aires y el resto de mi vida en Barcelona (con un breve paso por Andorra).

Quienes me conocen bien suelen describirme como una persona abierta a escuchar y muy entusiasta. Son cualidades que van conmigo en mi vida profesional y personal.

En lo que respecta a liderar personas o proyectos, intento siempre acompañar, aconsejar y hasta donde es posible, inspirar y motivar a las personas de mi entorno.

Me gusta pensar antes de tomar decisiones y ser reflexivo en mi manera de comunicar y explicar el "por qué" hacemos las cosas y "qué valor" se consigue con lo que hacemos, son cuestiones que agregan sentido a nuestro trabajo y ayudan a conseguir generar el valor que buscamos dar a nuestras empresas.

¿Como fueron tus comienzos en el mundo de la tecnología?

Comencé a trabajar en ciberseguridad en una época que no existía esa palabra (o nadie la conocía), se hablaba de "seguridad informática" o "seguridad de la información". Comencé en 2005 a trabajar en Andorra en proyectos de ciberseguridad estando en Accenture para bancos clientes. La experiencia fue altamente gratificante.

Retomé la ciberseguridad en 2007, ya en forma definitiva y hasta el día de hoy.

En esa ocasión en una consultora especializada únicamente en ciberseguridad (cosa que no era habitual). En esa empresa aprendí a trabajar en ámbitos de privacidad: adecuación y auditoría a la LOPD (no existía aún el RGPD) y en ámbitos de gestión con la ISO/IEC 27001. Durante esa etapa aprendí el estándar en profundidad y trabajé en varios proyectos de adecuación a ese estándar, experiencia que me sirvió mucho en mi siguiente empresa.



CONTINÚA EN
PRÓXIMA PÁGINA



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



Ramiro, cuentas con más de 25 años en el sector tecnológico ¿cuál consideras que ha sido el cambio más profundo en la gestión de la ciberseguridad desde tus inicios hasta hoy?

El cambio más radical ha sido sin duda la transición de la "seguridad por aislamiento", hacia una hiperconectividad absoluta. Cuando comencé a trabajar en ciberseguridad, el paradigma pasaba por la gestión de riesgos (con el foco en la parte técnica) y el control del perimetral siendo básicamente estática. Desde hace unos años y mucho más con la entrada de la IA, los procesos de negocio de las empresas pasan por la hiperconectividad, los datos están en múltiples sitios complejizando la gestión eficiente y segura de los sistemas de información y del dato.

Actualmente el riesgo es mucho mayor, complejo y cambiante debido a la aparición (cada vez más rápida) de nuevas tecnologías disruptivas que agregan potencialidad a las organizaciones al mismo tiempo que agregan nuevas amenazas y vectores de ataque.

Hemos pasado de proteger equipos individuales a proteger los datos sea donde sea que se encuentren y los procesos de negocio globales donde la caída de un sistema crítico puede parar la producción ocasionado impacto en todo tipo de ámbitos (financiero, operativo, reputacional, legal, seguridad de las personas, etc.), todo eso en un mundo cada vez más inseguro donde nuevas amenazas aparecen como la explotación de nuevas tecnologías por parte de los ciberdelincuentes.

La tecnología ha democratizado la defensa, pero también ha facilitado la vida a los delincuentes otorgándoles un ROI aún mayor (si cabe) a sus actos delictivos. Lo que antes era una preocupación técnica del CISO o del director de sistemas, hoy es una prioridad de la junta directiva.

¿Cuál es tu rol y responsabilidad actual? ¿Cuáles han sido los hitos más importantes de tu trayectoria profesional en tu empresa actual?

Soy Product Security Leader en GE Vernova para la unidad de negocio de Wind que engloba el negocio de las granjas eólicas de onshore (en tierra) y offshore (en mar).

Comencé a trabajar en GE Vernova en junio de 2020, en medio de la pandemia de COVID, cuando estábamos todos encerrados en nuestras casas, fue un momento difícil porque la curva de aprendizaje se alargó al no tener un ámbito de encuentro físico con los nuevos compañeros.

Como hitos importantes mencionaré dos: Primero, el haber conseguido la certificación en la IEC 62443-4-1 (Requisitos del ciclo de vida de desarrollo de productos seguros) y la segunda el haber conseguido implantar la metodología de gestión de riesgos de la IEC 62443 (parte 3-2) primero para un cliente y luego internamente juntamente con los requerimientos de sistemas (parte 3-3) y los requerimientos de componentes (parte 4-2).



CONTINÚA EN
PRÓXIMA PÁGINA

Nuestro invitado a #TYSO

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Nuestro invitado a #TYSC



Háblanos de tus éxitos o logros profesionales

Adicionalmente a los que comentaba antes, recuerdo gratamente algunos en otras empresas como fueron el haber obtenido la certificación ISO/IEC 27001 para una consultora especializada en ciberseguridad en la que trabajé hace unos años, tuve la suerte de poder comenzar a trabajar en el desarrollo del SGSI (Sistema de gestión de la seguridad de la información) desde un inicio conjuntamente con otra persona crear toda la estructura del sistema (políticas, procedimientos y documentos operativos más la implementación de los controles técnicos con la ayuda del responsable de IT) con ello adecuarnos al estándar y lograr luego la certificación.

Otro gran éxito fue el poder haber migrado el data center de Linde, una empresa en la que trabajé por más de 10 años. Fue un caso extremo porque tuve que coordinar a 7 empresas proveedoras con un total de 22 personas, las cuales trabajaron intensamente para lograr mudar el data center de una planta a otra del edificio un viernes al mediodía acabando de madrugada al día siguiente. El éxito en esa ocasión se debió al esfuerzo realizado durante la etapa de preparación y coordinación previa, la cual fue compleja ya que había que hacer una mudanza tipo "big bang". El director general adjunto me elogió (le costó creer al lunes siguiente que todo funcionaba correctamente).

A nivel profesional me he ido reinventado, comenzando primero en áreas de soporte, pasando luego a infraestructura y comunicaciones para acabar luego en ciberseguridad, primero en ámbitos IT para luego en el mundo OT.

En los 2 últimos años estoy potenciando mi conocimiento y experiencia en mi ámbito con el uso de la IA, tengo un interés especial en aprender todo lo que esté relacionado y que pueda aportar valor para mejorar la efectividad en mi trabajo.

Tu perfil destaca un enfoque muy fuerte en la gobernanza (GRC). ¿Por qué crees que, en el contexto actual de la IA, la gobernanza es más crítica que la implementación técnica de ésta?

La técnica sin gobierno es un riesgo inaceptable. En los últimos años, con la explosión de la IA generativa y los modelos predictivos, muchas organizaciones han corrido a implementar soluciones sin entender quién es responsable del dato ni centrándose en garantizar la ética del algoritmo o el cumplimiento de marcos como la ISO 38507 (Implicaciones de gobernanza del uso de la IA por parte de las organizaciones).

Mi enfoque siempre ha sido el de alinear la gobernanza de la ciberseguridad con los objetivos de negocio. Si la IA va a optimizar procesos, debe hacerlo bajo un marco de control que garantice la seguridad, la transparencia, los aspectos legales y éticos. Todos estos aspectos no se pueden dejar al azar con la IA generativa.

Como comentas, la IA ha irrumpido de forma disruptiva. ¿Cómo ha transformado esta tecnología tu día a día en la gestión de ciberseguridad?

Si tuviera que poner un título a esta charla, sería algo como "Gobernanza de la IA: El nuevo imperativo de la Ciberseguridad".

La IA ha sido un catalizador de la eficiencia, está permitiendo por ejemplo automatizar la toma de decisiones en tareas de cumplimiento, sobre todo a través del mapeo con los requerimientos de múltiples marcos y análisis de riesgos que antes requerían semanas de trabajo manual.

Para citar algunos ejemplos, la evaluación de proveedores o en la interpretación de normativas complejas como NIS2 o la CRA (Cyber Resilience Act) se puede hacer uso de la IA ya que proporciona la capacidad de procesar volúmenes ingentes de datos para detectar anomalías en tiempo real que el ojo humano simplemente ignoraría. Por otro lado, también ha democratizado



**CONTINÚA EN
PRÓXIMA PÁGINA**

el ataque (los delincuentes también usan la IA para conseguir sus objetivos), obligándonos a elevar nuestras defensas al mismo nivel de sofisticación.

Nuevas amenazas aparecieron con la IA como prompt injection o ataques adversarios (por citar sólo algunos), los cuales requieren nuevos controles cyber, los controles tradicionales como Firewalls, IPS, DLP, SIEM, SOC, etc. no son efectivos.

Existen nuevos usos de la IA que permiten potenciar los controles existentes, en ese sentido ejemplos como "Agentic AI Security" (Agentes IA desarrollados para la gestión activa de la ciberseguridad), se presenta como un nuevo paradigma que complementa servicios tan consolidados como son el SOC.

Actualmente estás terminado un Máster en IA e Innovación y recientemente finalizaste un Máster Ejecutivo en IA. ¿Qué te impulsa a seguir en la "primera línea" de formación académica?

Soy un ferviente creyente e impulsor del aprendizaje continuo, además de esos dos másteres he realizado recientemente otros cursos y he conseguido nuevas certificaciones, en pocos días comenzaré un curso de IA aplicada a ciberseguridad. Me gusta tanto recibir como dar formación en los ámbitos de ciberseguridad e IA.

La obsolescencia en nuestro campo no se mide en años, ¡sino en meses! Mi interés por la formación continua nace de una convicción: no puedes gobernar lo que no comprendes profundamente.

Para liderar la digitalización segura de una organización, debo entender cómo funcionan los modelos de lenguaje (LLM), las redes neuronales, etc. y cómo los controles de ciberseguridad deben adaptarse a éstos. Debo confesar que es un tema que me apasiona personalmente, aplicar la IA en mi día a día tanto a nivel profesional como personal es un proceso que no tiene fin y es por definición cambiante y evolutivo a velocidades que no estábamos acostumbrados hasta hace unos años.

Ramiro, ¿qué controles técnicos en ciberseguridad crees que las empresas están olvidando hoy?

Estamos muy enfocados en el cumplimiento normativo teniendo múltiples frameworks en ciberseguridad impuestos (desde el Compliance como son leyes y requerimientos en los contratos con los clientes) y autoimpuestos (estándares en los que estamos adecuados o certificados), pero olvidamos que la IA introduce vectores de ataque inéditos.

Amenazas provenientes del uso de la IA como son Data Poisoning (envenenamiento de datos) o la Inyección de Prompts (por mencionar sólo dos) requieren una atención especial y los controles cyber tradicionales no pueden mitigarlos.

En mi enfoque de gobernanza bajo la ISO 38507, no veo estos controles como opciones, sino como requisitos previos. No puedes decir que tu organización es segura si no tienes visibilidad sobre cómo se entrenan tus modelos o si no has implementado capas de explicabilidad (XAI) que permitan a un auditor entender la toma de decisiones algorítmica.

En el ámbito de la ciberseguridad industrial (OT), donde la seguridad física y lógica se dan la mano, ¿qué papel juega la IA en la protección de infraestructuras críticas?

Es fundamental. En sectores como el de las energías renovables donde me encuentro, los activos están distribuidos y son críticos. Es esencial que nuestra gobernanza de la ciberseguridad OT cuente con un marco de ciberseguridad reconocido internacionalmente como es la IEC 62443 o la NIST CSF junto con NIST SP 800-82.

La IA nos permite implementar modelos de "mantenimiento predictivo de seguridad". Podemos anticipar vulnerabilidades antes de que sean explotadas analizando patrones de tráfico en redes industriales para buscar potenciales fallos e intentar anticiparse incluso aplicando agentes para mitigar vulnerabilidades. Es esencial mantener los datos en forma íntegra, confidencial y segura por diseño durante todas las fases, desde el diseño de un sistema hasta su desmantelamiento.

Para los jóvenes profesionales que están comenzado a trabajar en ciberseguridad, ¿qué habilidades crees que serán imprescindibles en el próximo lustro?



Más allá de la capacidad técnica, destacaría la curiosidad intelectual y el pensamiento crítico. La técnica se puede aprender en un manual o preguntar a la IA, pero la capacidad de entender el impacto ético de una decisión tecnológica o de comunicar un riesgo complejo a la alta dirección es lo que marca la diferencia.

Otro punto a destacar es la capacidad de mejorar la cyber-resiliencia como elemento que facilita ese objetivo, el fallo es una posibilidad constante; lo importante es cómo se diseña el sistema para recuperarse, el paradigma ha cambiado desde hace unos años pasando de centrarse sólo en la prevención (reduciendo la probabilidad de ocurrencia de amenazas) a complementarse con la reducción del impacto (se asume que todos seremos impactados por amenazas ocasionando contingencias graves a nuestros procesos de negocio en algún momento).

Lo importante es como recuperarse, tal como decía Muhammad Ali, "...No tiene nada de malo caer, lo malo es quedarse abajo".

Conclusiones

Como cierre de esta charla quisiera dejar un mensaje final, me gustaría comentar en forma breve algunos de los aspectos que considero esenciales para la vida profesional y personal:

Primero, nuestro mayor valor reside en el proceso (camino) compartido, más que en la meta alcanzada. El impacto positivo en las relaciones creadas y mantenidas en ese largo camino que transitamos posee un valor mayor incluso que nuestras metas. La huella que dejamos en cada persona con la que nos relacionamos nos define como individuo y será lo que quede de nosotros en la memoria de las personas (siendo este camino largo o corto y tanto en el ámbito profesional como personal).

Segundo, el cambio y la evolución es constante, tanto en nuestras empresas, como nosotros mismos. Desde la perspectiva profesional este cambio nos obliga a adaptarnos, a aceptar el cambio y nos vemos "obligados" a autoimponernos el realizar formación constante durante toda nuestra vida; es la manera de poder reciclarnos y seguir adelante con la adaptación constante que nos requiere el mundo actualmente.

Y tercero, no temer al fracaso, a pesar de que en nuestra cultura no se vea con buenos ojos, es una parte intrínseca del camino al éxito en todo lo que hacemos, lo importante no es conseguir el éxito en el primer intento, si no la constancia en la búsqueda de la mejora continua, procurar evolucionar (perfeccionarse) en todo lo que hacemos

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



Curso de Certificación en: Gobierno de la Inteligencia Artificial

ISO 38507 AI Governance Leader

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 15 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad



Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**



Marlon Molina

La geopolítica es tendencia

Iniciamos el año abrumados por movimientos geopolíticos que impactan más allá de sus propios territorios. Los tres grandes jugadores han movido cartas para 2026, China, Rusia, y Estados Unidos.

Cada uno de estos jugadores ha movido ficha iniciando el año. Cada uno lo ha hecho en su patio, en su frontera inmediata, aunque vistos desde fuera, parecen movimientos coordinados.

Estados Unidos es el claro líder y Donald Trump no parece esconder ni intenciones ni armas. Presenciamos un despliegue importante en la construcción de alianzas, en la influencia como mediador, y lo más importante para este espacio de opinión: en tecnología.

China, el segundo jugador está apostando por la autosuficiencia, lo que también incluye la tecnológica. China sabe que no puede ser la fábrica eternamente, que no puede seguir construyendo lo que los demás diseñan si quiere ser considerado un jugador serio y no la sombra de Estados Unidos.

La apuesta de **Rusia** pasa principalmente (y casi únicamente) por la energía, la fuerza del Kremlin está en su posición estratégica para vender energía a Europa y China, y con un poco de suerte a algún país africano. La tecnología conocida es principalmente la relacionada con la carrera armamentística.

India está muy por detrás de los tres primeros, pero se ha ganado su cuarto lugar con crecimiento de la población, y constituyéndose en la fábrica tecnológica y posiblemente quien absorba los desarrollos tecnológicos de Europa principalmente aprovechando los bandazos de Brasil.



CONTINÚA EN
PRÓXIMA PÁGINA

En un ranking **Europa** sería la quinta potencia en bloque, pero no en puesta en escena. La fortaleza de Europa es el conjunto, también su debilidad ya que no posee una estrategia común, no quiere ser un seguidor de Estados Unidos, pero mucho menos de los otros jugadores, y desde luego no puede liderar.

El efecto Bruselas: Europa crea, China Escala

Europa ha sido la cuna de las telecomunicaciones, de la investigación y la creación, pero no de la venta. Este es un ejemplo perfecto para escenificar lo que ocurre con la sobrerregulación que nace en Bruselas y que lamentablemente (en mi opinión) los Estados acogen con felicidad.

El conocimiento y desarrollo de las tecnologías 5G y 6G se han financiado con dinero europeo dentro de programas de desarrollo de la Unión. Las investigaciones se registran de forma abierta, posteriormente no se pueden desarrollar fácilmente debido a la regulación, conocimiento que usa China para inyectarlo en su modelo de “capitalismo de Estado”, y posteriormente vende a Europa. No es el único ejemplo, energía solar, agricultura, los vehículos eléctricos, la biotecnología, y ahora también la Inteligencia Artificial. En este último punto -la Inteligencia Artificial, India está inundando de comerciales y oficinas de venta para Europa y otras regiones, pero especialmente en el territorio europeo donde básicamente se limita el desarrollo, pero no la compra.

La tecnología de la información y la geopolítica

El principal “campo de batalla” de las principales tres potencias es en realidad las tecnologías de la información. No es que Estados Unidos lo juegue mejor, es que el tablero lo ha propuesto este país. Es como si en un duelo alguien preguntara qué armas y dónde, es así como la respuesta ha sido: las tecnologías de la información.

La soberanía digital tan cuidada por China, y tan descuidada en Europa es la pieza fundamental para la soberanía del dato, del nuevo petróleo, de la privacidad y del cuidado de la ciudadanía.

Si finalmente el estándar mundial de telecomunicaciones se basara en patentes chinas, todo el mundo deberá pagar regalías a Pekín y usar su arquitectura de red, lo que les da una ventaja competitiva y de espionaje estructural por décadas.



Las fronteras físicas se han llenado de agujeros con una geopolítica de bits. La soberanía no se ejerce sobre un territorio que se mide en kilómetros cuadrados, sino en centros de procesamiento del dato.

Como cierre, y como una nota para la reflexión, algunas grandes tecnológicas tienen una actuación como si fueran Estados, tienen presupuestos de I+D mucho mayores al PIB de un país medio, y una influencia con mucho mayor impacto. Empresas como Meta, Google, OpenAI, X, y TikTok tienen la capacidad de dictar las reglas de la plaza pública digital, estas corporaciones ejercen una autoridad paraestatal que desafía el monopolio del poder político tradicional. Comparando el valor bursátil de estas empresas juntas, solo Estados Unidos y China tendrían una economía superior, es decir, si se juntan serían la tercera potencia mundial y con más poder de influencia que los países.



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
Certificación en:**

**Gestión de
Proyectos**

**P4MGO! PjM
Project
Management**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el P4MGO! PjM BoK
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

Ricard Martínez Martínez



Soy persona delegada de protección de datos: NO ES MI FUNCIÓN...

En los últimos tiempos se ha suscitado una cierta discusión sobre cuáles sean las funciones que deben desplegar las personas delegadas de protección de datos (DPD). Existen dos grandes líneas de debate. La primera se centra en el alcance de las tareas que les corresponden. La segunda se extiende a los nuevos ámbitos que, de la mano de la innovación tecnológica o normativa, abren un conjunto de campos interrelacionados con el RGPD.

Esta discusión alcanza una intensidad significativa en el ámbito del sector público en el contexto de la rigidez que confiere a la administración el marco regulador de la función pública en las atribuciones funcionales a cada posición en las relaciones de puestos de trabajo. La definición funcional del puesto de trabajo permite dotar de seguridad jurídica y organizativa al conjunto de tareas que se despliegan. Además, contribuye a evitar abusos como encargar tareas no correspondientes con el puesto o utilizar los efectivos para funciones no previstas. Es aquí donde la frase "no es mi función" adquiere pleno significado. Existe una leyenda urbana en las universidades públicas, y en no pocas administraciones, según la cual aquellos que aprobaron su oposición realizando un examen de mecanografía se negaban a utilizar los primeros ordenadores personales al exigir la ejecución de comandos. Como se suele decir, si non è vero, è ben trovato, y ejemplifica cómo la rigidez de la estructura profesional en lo público puede conducir a una petrificación funcional poco coherente con las necesidades de flexibilidad y adaptación evolutiva que el avance tecnológico y científico acelerado imponen para el despliegue de las tareas de cualquier trabajador.

En el contexto de los DPD, la discusión se sitúa en el territorio de tareas en las que la interacción con el responsable del tratamiento es más intensa y podría comprometer el principio de independencia. Destacan, a título de ejemplo, las evaluaciones de impacto en la protección de datos (EIPD), el desarrollo de aplicaciones y la seguridad de los sistemas de información. La tesis que parece imponerse defiende escindir por completo las tareas de las DPD respecto de la acción del responsable. Así, su función se limitaría estrictamente a la orientación y la supervisión. Esta posición sería coherente con las funciones que atribuye el artículo 39 del RGPD a esta figura, en la medida en que le corresponden tareas de información y asesoramiento, supervisión, colaborar asesorando en el desarrollo de las EIPD y cooperar con la autoridad de control. Evidentemente, y desde una interpretación estricta, colaborar en el desarrollo de las EIPD implicaría la existencia de un proceso en el que la persona delegada de protección de datos no se implicaría bajo ninguna condición hasta la revisión final, salvo ser requerida expresamente para ello por el responsable del tratamiento.



CONTINÚA EN
PRÓXIMA PÁGINA



La verdad es que, sobre el papel, el dibujo parece bastante coherente, si no fuera porque, como suele decirse, el papel lo aguanta todo. En ese contexto, debemos ser honestos. La clave reside en determinar bajo qué condiciones puede desplegarse la función de asesoramiento al responsable del tratamiento, teniendo en cuenta cuál es la estructura real de la protección de datos en las administraciones públicas en este país.

En primer lugar, reto a los lectores informados a que me indiquen cuál sea el nivel de formación específica que han recibido las personas que prestan sus servicios en su respectiva administración, y hasta qué punto los técnicos de alto nivel están preparados para realizar una EIPD. La realidad que yo conozco es que las carencias formativas son significativas y, en muchos casos, alcanzan a las capacidades de las propias personas delegadas de protección de datos. Y aquí se produce una situación verdaderamente paradójica. En no pocas administraciones de este país, las DPD sí que entienden que entre su tarea de informar y asesorar se encuentra la de participar, organizar, dirigir y participar en todos y cada uno de los cursos de formación continua en protección de datos. Una tarea debidamente remunerada que genera ingresos adicionales. Y, sin embargo, se defiende la posición de separación absoluta de estas personas respecto de la EIPD, reivindicando la subcontratación de las tareas en terceros en aquellos casos en los que el responsable carece de las capacidades que, por

cierto, deberían derivar de la función de información, soporte y asesoramiento del propio DPD.

Lo mismo sucede en la seguridad y el desarrollo de aplicaciones, que plantean cuál debería ser el rol de DPD en los comités de seguridad y en la conformación de equipos de trabajo con el responsable de seguridad, con los administradores de sistemas y los desarrolladores, allí donde existan. En ambas tareas es imposible alcanzar el modelo de gestión del riesgo de los artículos 24, 32 y 35 del RGPD y la activación de las respuestas que exigen la gestión de las brechas de seguridad. Además, si el DPD carece de capacidades para aplicar ingeniería de privacidad al desarrollo de aplicaciones y desplegar la protección de datos desde el diseño y por defecto es sencillamente inviable.

El segundo ámbito de ausencia buscada resulta preocupante. Asistimos a una ampliación sistémica del código de derecho digital de la UE. A partir del Reglamento de Gobernanza de Datos, las administraciones deberían generar espacios de datos para su compartición y entender cómo integrar datos que provengan de entornos privados, ya deriven del altruismo de datos o mediante la portabilidad del Reglamento de Datos. El Espacio Europeo de Datos de Salud, a su vez incrementa el control de la historia clínica, del derecho a la portabilidad de la información sanitaria y revoluciona la reutilización de los datos electrónicos de salud. Basta con leer el artículo 4 del Reglamento de Inteligencia Artificial sobre formación, el 5 sobre usos prohibidos y, en particular el artículo 10 sobre gobernanza de datos en sistemas de alto riesgo, para entender por qué interpelan a los DPD. Todas y cada una de estas normas sitúan al RGPD como una clave de bóveda sin la cual no es posible generar y utilizar datos. Esto determina la interpretación sistemática de la nueva legislación y rige el propio desarrollo tecnológico. Las DPD, les guste o no, no pueden huir de los retos que les presenta la nueva normativa.

Deberíamos plantearnos cuál sea el origen de este tipo de actitudes en el sector público. Sin duda, la cultura de nombrar personas delegadas de protección de datos de manera discrecional y, a ser posible, a coste cero, o de subcontratar el servicio por costes sencillamente ridículos, pueda ser el origen de gran parte de este problema. La ausencia de responsabilidades económicas no ayuda demasiado y la inveterada costumbre de la Agencia Española de Protección de Datos de no indagar las responsabilidades disciplinarias favorece este ecosistema de ausencia decisonal. Por otra, como ya he señalado, el sector público favorece en más de una ocasión el atricheramiento del personal en posiciones conservadoras desde el punto de vista del despliegue de sus funciones. Los retos que plantea la Década Digital Europea y la construcción de espacios de datos sitúan a la administración en un punto nuclear para la generación de un mercado de datos que contribuya a la investigación, la innovación y la competitividad de la Unión Europea. Sería muy triste que la "ausencia" de las personas delegadas de protección de datos nos condujera al fracaso.



RICARD MARTÍNEZ

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

LinkedIn:

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

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gobierno
del Dato**

**UNE 0077
Data
Governance
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en la Norma: UNE 0077
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**



La IA no es una opción, es un imperativo

El coste de la inacción en la era en la que la inteligencia artificial se ha convertido en el sistema operativo del negocio

Durante más de una década, la inteligencia artificial ha sido tratada como una promesa de futuro, un campo experimental reservado a laboratorios, startups o departamentos de innovación. Entre 2015 y 2025, muchas organizaciones pudieron permitirse observar desde la barrera: pilotos limitados, pruebas de concepto, pequeños modelos predictivos o chatbots con impacto marginal.

Esta época ha terminado.

En 2026, la IA ya no es una tecnología emergente. Es la infraestructura cognitiva sobre la que, las empresas con visión de futuro están ejecutando sus procesos de negocio. Es el sistema operativo invisible que conecta procesos, personas, datos y decisiones en tiempo real. Y, como ocurrió con Internet, la nube o la primera revolución industrial, no adoptarla no es una postura neutral, es una decisión estratégica con consecuencias directas en el porvenir de la empresa.

El mayor riesgo hoy no es equivocarse al implementar IA, sino no implementarla.

Analicemos tres dimensiones críticas del coste de la inacción:

- 1.El fin de la ventaja competitiva tradicional basada en el tamaño, el capital o la cuota de mercado.
- 2.La brecha de eficiencia entre empresas aumentadas por IA y organizaciones rezagadas.
- 3.El riesgo del retraso en la adopción: por qué llegar tarde a la IA es más costoso que en cualquier otra revolución tecnológica anterior.

El fin de la ventaja competitiva tradicional

Durante gran parte del siglo XX y principios del XXI, las ventajas competitivas se basaban en barreras de entrada clásicas, como las economías de escala, el acceso al capital, las infraestructuras físicas, las redes de distribución y el número de personas que trabajaban en la empresa. Las grandes empresas eran grandes porque serlo importaba.

La IA ha comenzado a erosionar sistemáticamente estas barreras. Hoy, una organización de 50 personas, bien potenciada o aumentada por la inteligencia artificial, puede competir y, en algunos nichos, superar a compañías con miles de empleados. No porque sea más creativa o valiente, sino porque opera con otra lógica de productividad.

La ventaja ya no reside en cuántas personas ejecutan tareas, sino en:

- Qué tan bien se orquestan agentes de IA
- Qué tan rápido se convierten datos en decisiones
- Qué tan profundamente la IA está integrada en el flujo operativo

Hoy, una empresa pequeña puede analizar mercados globales con modelos generativos; automatizar ventas, marketing y soporte con agentes autónomos; diseñar, simular y testear productos digitalmente; optimizar precios y operaciones en tiempo real.

Todo esto era impensable sin una estructura empresarial pesada hace apenas cinco años. La ventaja competitiva ya no se calcula por el número de empleados, sino por la calidad de los modelos, datos y procesos.

Las empresas que siguen compitiendo con estructuras pensadas para el siglo XX están jugando un juego distinto... y perdiéndolo.

La brecha de eficiencia: cuando el margen se convierte en destino

Las empresas que han implementado la automatización y la IA en sus procesos operativos presentan niveles de eficiencia estructuralmente superiores.

No se trata de mejoras marginales del 3 o 5%. En muchos casos, los diferenciales operativos se sitúan en rangos del 20 al 30% en costes operativos, precisión en la toma de decisiones, y productividad por empleado (datos de estudios de McKinsey & Company y Boston Consulting Group).



CONTINÚA EN
PRÓXIMA PÁGINA



¿Por qué? Por un factor crítico: los datos y el aprendizaje acumulado.

Los sistemas de IA no mejoran solo por existir, mejoran porque observan procesos reales, aprenden de excepciones, ajustan los modelos con datos históricos e integran feedback humano

Una empresa que lleva 3–5 años operando con IA:

- Tiene conjuntos de datos propios únicos
- Ha entrenado modelos en su contexto específico
- Ha cometido errores... y aprendido de ellos

Una empresa que empieza hoy no solo empieza desde cero, empieza desde atrás.

Así, el riesgo no es solo tecnológico; es organizativo y cultural, ya que los equipos no están acostumbrados a trabajar con IA, los procesos son rígidos y difíciles de automatizar, las decisiones se toman sin apoyo algorítmico y existe una falta de gobernanza de los datos específicos de la empresa y del sector.

Esto genera lo que muchos analistas ya denominan un retraso estructural: una brecha que no se cierra con una inversión puntual, sino que exige una transformación profunda y sostenida.

La ventaja no está solo en automatizar tareas. Está en rediseñar el modelo de operativo completamente:

- Mejora de las decisiones mediante modelos predictivos avanzados; optimización dinámica de precios, inventario y recursos; reducción drástica de errores humanos recurrentes.
- Operaciones autónomas mediante procesos end-to-end sin intervención manual; uso de RPA + IA generativa para excepciones complejas y disponiendo de sistemas que se autoajustan según contexto.
- Talento *aumentado* con profesionales que trabajan con asistentes de IA, que dedican menos tiempo a tareas mecánicas y más a valor estratégico.

Aquí aparece un elemento clave: la eficiencia impulsada por la IA es acumulativa.

Una empresa que hoy es un 25% más eficiente, reinvierte antes, innova más rápido, atrae más y mejor talento, genera y se entrena con mejores datos.

Esto crea un círculo virtuoso difícil de romper desde fuera.

Mientras tanto, las empresas rezagadas no solo operan con menos margen, sino que también pierden la capacidad de financiar su propia transformación.

El riesgo del retraso en la adopción

En transformaciones tecnológicas anteriores, llegar tarde era incómodo, pero recuperable. Bastaba con comprar la tecnología adecuada, contratar expertos y ejecutar un proyecto intensivo. Con la IA, esta lógica falla. Llegar tarde en IA no es como llegar tarde a la nube

IA como sistema operativo del negocio

En 2026, las organizaciones que quieren ser líderes en sus respectivos mercados ya no “usan IA”, es la IA que da soporte a sus procesos de negocio.

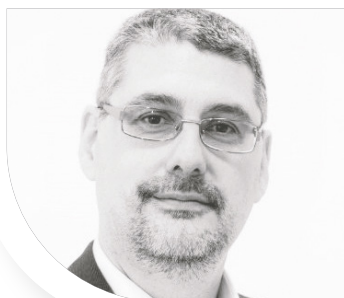
La IA, orquesta procesos, prioriza decisiones, da soporte a cada rol profesional y conecta la estrategia y la ejecución. Es el equivalente moderno del sistema operativo empresarial, del mismo modo que Windows o Linux lo fueron en la informática personal. No adoptarlo no significa quedarse quieto. Significa operar con un sistema obsoleto mientras el mercado avanza en tiempo real.

La inteligencia artificial no elimina la necesidad de liderazgo, visión o criterio humano. Al contrario: los hace más importantes. Pero cambia una premisa fundamental, ya no es posible competir de forma sostenible sin IA integrada en el núcleo del negocio.

En 2026, la pregunta no es si podemos permitirnos invertir en IA, sino si podemos permitirnos no hacerlo.

Porque en esta nueva fase, la inacción no es prudencia. Es una estrategia... y una perdedora.

La inteligencia artificial no elimina la necesidad de una visión estratégica. La amplifica. Obliga a las empresas a redefinir sus modelos de operación, a decidir qué delegar en las máquinas, qué preservar en los humanos y cómo rediseñar completamente la empresa.



MARCOS NAVARRO ALCARAZ

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

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

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

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

Gestión de Programas P4MGO! PgM Programme Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el P4MGO! PgM BoK
- A tu ritmo con toda comodidad



Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>

**PgM Book
Programme
Management
Body of Knowledge
P4MGO!®**



21001: 2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

Víctor Almonacid

Cómo introducir IA en los ayuntamientos sin crear un agujero legal

Los municipios que implementan IA sin marcos claros se exponen a impugnaciones, sanciones por incumplimiento de derechos fundamentales y, lo peor, a tomar decisiones injustas y poco transparentes.

¿IA sí o IA no? Evidentemente, sí, pero no de cualquier manera. Los ayuntamientos se enfrentan a una encrucijada. La presión por eficiencia crece, los recursos escasean, y la tecnología promete soluciones. Pero la IA no es la panacea a todos nuestros problemas, e incluso podría traer otros nuevos; es una herramienta tremendamente útil pero con riesgos legales reales. Los municipios que implementan IA sin marcos claros de seguridad se exponen a impugnaciones, sanciones por incumplimiento de derechos fundamentales y, lo peor, a tomar decisiones injustas o discriminatorias que no van a poder o saber explicar.

Un riesgo muy real son las decisiones automatizadas sin garantías. Imaginemos un ayuntamiento que usa IA para evaluar licencias de obras. El algoritmo analiza cientos de solicitudes, identifica patrones y rechaza automáticamente aquellas que percibe como "de riesgo". ¿Cuál es el riesgo? Que el algoritmo sea opaco, que niegue trazabilidad, que perpetúe sesgos históricos en los datos de entrenamiento, y que el ciudadano nunca sepa por qué le fue denegada su licencia. Esto es ilegal bajo el Reglamento de IA de la UE (AI Act) y vulnera principios de la Ley 39/2015 (motivación, audiencia, control judicial). Pero puede suceder.

El marco jurídico obliga y protege simultáneamente. ¿Qué normas debemos cumplir a toda costa? A saber:

A nivel europeo, fundamentalmente el AI Act (Reglamento UE 1689/2024). Clasifica sistemas según riesgo. Los "sistemas de alto riesgo" en administración pública requieren auditoría, trazabilidad, supervisión humana, transparencia explicable. Los sistemas que denieguen derechos fundamentales son "de alto riesgo".

A nivel estatal:

- Ley 39/2015 (Procedimiento Administrativo Común). Exige motivación, audiencia, posibilidad de revisión. Nada de esto es compatible con una IA opaca.
- LOPDGDD. Desarrolla la normativa europea en materia de protección de datos y recoge un catálogo de derechos digitales de las personas.
- LSSI-CE (Ley 34/2002, de 11 de julio). Responsabilidad de la plataforma por contenidos generados.
- Normativa sobre seguridad y ciberseguridad, donde destacamos el ENS.
- Normativa estatal y autonómica sobre transparencia (distintas leyes).



CONTINÚA EN
PRÓXIMA PÁGINA





En base a todo lo anterior, entendemos que estas son las cinco garantías que todo ayuntamiento debe implementar:

1. Transparencia algorítmica (inteligibilidad). No podemos usar un algoritmo si no puedes explicar por qué tomó esa decisión. Esto significa:

- Documentar cómo se entrenó, con qué datos, con qué sesgos potenciales.
- Poder "abrir la caja negra" ante impugnación ciudadana.
- Usar modelos interpretables cuando sea posible; si usas "black box", exigir auditabilidad externa.
- Herramientas prácticas: Claude (con explicabilidad), Perplexity (que cita fuentes), son opciones más transparentes que ChatGPT genérico.

2. Supervisión humana obligatoria. Ninguna decisión que afecte derechos fundamentales puede ser 100% automatizada. Siempre debe existir:

- Revisión humana de decisiones de "alto riesgo" (denegación de intereses legítimos y otras peticiones, sanciones, etc.).
- Mecanismo de objeción ciudadana accesible (alegaciones, recursos).
- Establecimiento de un sistema de responsabilidad claro: ¿quién es responsable si el algoritmo yerra?
- Regla de oro: la IA puede recomendar, filtrar, alertar. Pero nunca debe decidir sola en contextos donde un humano tendría que motivar su decisión.

3. Trazabilidad de datos. La decisión automatizada debe ser auditable en todos estos sentidos:

- Qué datos se usaron (y si eran legales, recopilarlos).

• Cómo se procesaron.

• En qué momento se tomó la decisión.

• Quién supervisó.

• Sin trazabilidad, ante una reclamación no podemos defender la legalidad. La AEPD (Agencia Española de Protección de Datos) es clara: sin trazabilidad, es ilegítimo.

4. Evaluación de sesgos periódica. Los algoritmos aprenden de datos históricos. Si históricamente se han denegado más licencias en ciertos barrios, el algoritmo perpetuará esa discriminación. En consecuencia, cada 6-12 meses deberíamos:

- Auditar resultados por grupos demográficos, zonas, tipos de solicitud.
- Identificar si hay divergencias injustificadas.
- Corregir el modelo si es necesario.
- Documentarlo todo.

5. Conformidad con AI Act y RGPD. El AI Act ya es de obligatorio cumplimiento (aunque de manera escalonada en cuanto a su entrada en vigor). En base al mismo, los ayuntamientos deben:

- Clasificar sistemas según riesgo.
- Para sistemas alto riesgo: registrarse en base de datos, auditoría anual, supervisión humana.
- Respetar RGPD: consentimiento informado, derecho olvido, portabilidad.
- Publicar información sobre uso de IA en procedimientos.



VÍCTOR ALMONACID

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

LinkedIn:

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

Twitter:

<https://twitter.com/nuevadmon>

Blog:

<http://nosoloaytos.wordpress.com/>

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:
Excelencia
en el Servicio
ISO 23592
Service
Excellence
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 23592
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001: 2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**



Alex Aliaga



El nuevo campo de batalla no se ve, se transmite

Durante décadas, la radio ha sido sinónimo de fiabilidad. Invisible, silenciosa y omnipresente, ha sostenido la aviación civil, la navegación marítima, los sistemas de emergencia y buena parte de la infraestructura crítica global sin levantar sospechas.

Sin embargo, esa confianza histórica empieza a resquebrajarse. Hoy, las señales de radio ya no son únicamente un medio de comunicación: se han convertido en un vector de ataque tal y como hemos ido reflejando en esta sección a lo largo de múltiples artículos.

Como ya hemos visto en artículos anteriores, las señales de radio no solo transportan datos. En muchos sistemas modernos, forman parte indispensable de infraestructuras críticas. Determinan, entre otras muchas funciones, dónde está un avión, cuándo aterriza, qué ruta sigue un buque o cómo se sincroniza una red eléctrica.

Estos sistemas funcionan porque los receptores confían en lo que reciben. Interpretan que una señal con la frecuencia correcta, la modulación esperada y la estructura válida es legítima. Pero hoy en día, y como ya hemos visto en artículos anteriores, ya no podemos fiarnos de lo que recibimos, los ciberdelincuentes han encontrado la manera de suplantar señales reales para realizar actos ilícitos que pueden tener consecuencias desastrosas.

Lo inquietante es que esta debilidad no es teórica. En la actualidad, las señales no siempre llevan una "firma" que permita distinguir lo auténtico de lo falso. Para un receptor estándar, una señal bien construida es indistinguible de la real, aunque haya sido generada desde una habitación con un SDR conectado a un portátil.

Los SDR, un arma de doble filo

Actualmente, un SDR comercial, software libre y conocimiento técnico bastan para reproducir ataques funcionales. El SDR actúa como una navaja suiza de la radiofrecuencia. Permite generar cualquier señal, en casi cualquier banda, con control total sobre modulación, fase y potencia. En manos defensivas es una herramienta de análisis formidable. En manos maliciosas, se puede convertir en un arma que puede tener impacto en el mundo físico.

La barrera ya no es económica, sino intelectual. Y ese conocimiento está publicado, documentado y enseñado. Esto obliga a replantear el modelo de seguridad: no se puede basar en la dificultad técnica cuando la técnica se ha democratizado.

Este problema no es solo tecnológico. Es estratégico. Afecta a infraestructuras críticas, a la seguridad aérea y a la resiliencia de sistemas civiles en contextos de crisis o conflicto híbrido. Ignorarlo no lo hará desaparecer.

De la teoría a la práctica: ataques reales

Las noticias más recientes confirman que la interferencia deliberada de señales GNSS no es solo una posibilidad técnica, sino un fenómeno que está ocurriendo en el mundo real. En septiembre de 2025, el avión que transportaba a la presidenta de la Comisión Europea, **Ursula von der Leyen**, experimentó una importante pérdida de señal GPS mientras sobrevolaba Bulgaria, obligando a la aeronave a dar vueltas durante casi una hora antes de aterrizar con sistemas de navegación alternativos. Las autoridades europeas atribuyeron el incidente a interferencias de GPS que se sospecha provienen de emisiones deliberadas de radiofrecuencia, posiblemente relacionadas con actividades de guerra electrónica por parte de Rusia.



CONTINÚA EN
PRÓXIMA PÁGINA

Este episodio no fue aislado. En 2024, otro vuelo con el entonces ministro de Defensa del Reino Unido, Grant Shapps, sufrió una interferencia similar cerca de Polonia, y varias aerolíneas reportaron fallos de navegación en vuelos entre Helsinki y Tartu.

En el ámbito marítimo, organizaciones como Windward han registrado **más de 13.000 buques con interferencias GPS**, con tramas AIS que muestran posiciones imposibles o movimientos erráticos que ponen en riesgo la seguridad de la navegación. El sistema **AIS**, que transmite posiciones de barcos por radio en VHF, es conocido por ser vulnerable a inyección de paquetes falsos o transmisiones maliciosas, permitiendo que un actor externo cree tramas de posición incorrectas.

No solo la navegación satelital está en el punto de mira. Las intrusiones en señales de radiodifusión o telecomunicaciones tradicionales son un caso práctico de manipulación. El **"broadcast signal intrusion"** se ha usado en radio y TV para secuestrar transmisiones legales utilizando transmisores que superan la potencia o interceptan frecuencias, algo que demuestra que incluso servicios de difusión masiva son vulnerables a interferencias intencionadas en radio.

Un ejemplo dramático no relacionado con GNSS o navegación pero centrado en radio como medio de control es el incidente de septiembre de 2024 en Líbano y Siria, donde miles de **walkie-talkies y pagers explotaron simultáneamente**, armas diseñadas para parecer dispositivos de comunicación y que lesionaron a miles, deshabilitando canales críticos de coordinación.

Es importante entender que los sistemas afectados por interferencias o manipulación no se limitan a la aviación o la navegación marítima. El GNSS proporciona **tiempo preciso y sincronización** a redes eléctricas, sistemas de telecomunicaciones, servicios financieros (timestamps para transacciones), transporte terrestre y marítimo, logística y hasta redes de emergencias.

Esto significa que cualquier actor con acceso a equipamiento de transmisión adecuado puede, en teoría, interferir con estos sistemas, comprometiendo la disponibilidad de servicios esenciales o provocando errores operativos graves. La radio, antes vista como un recurso confiable, se ha convertido en un punto de fragilidad crítica que requiere atención urgente por parte de los responsables de seguridad nacional y los operadores de infraestructuras estratégicas.

Las comunicaciones radio ya no son seguras, debemos prepararnos para protegerlas como un activo más

El aire que nos rodea está lleno de señales cuya integridad antes se daba por sentada. Hoy esa confianza se tambalea ante



ataques reales. Las señales de radio, desde GPS hasta ADS-B, pueden ser bloqueadas, manipuladas o suplantadas por actores con habilidades técnicas crecientes y acceso a herramientas democratizadas.

Este fenómeno ya ha tenido efectos comprobados, desde interrupciones de navegación en vuelos de alto perfil hasta miles de incidentes diarios de interferencia en aviones civiles. Ignorar esta realidad no solo es imprudente, es incompatible con la seguridad de las sociedades altamente conectadas de hoy.

La ciberseguridad y la ciberdefensa deben extenderse más allá de los circuitos y las redes informáticas para proteger también **los canales físicos de comunicación que sustentan la operativa de nuestras infraestructuras más críticas**. La radio ya no es un sitio seguro por defecto; es un dominio que hay que defender con la misma intensidad con la que se protege cualquier red digital.



ALEX ALIAGA

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



Curso de Certificación en:

Gestión de Centros de Operaciones de Seguridad (SOC)

SOC Management Leader

Docente:
Alejandro Aliaga

- Formato: Grabado con Tutorías
- Tutorías en directo: Lunes Tardes
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Importe del Curso: 995€
- Tasas Examen: Incluidas
- En tu horario, a tu ritmo.
- Con toda comodidad
- Solicita tu admisión

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo



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



21001: 2018
EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS

Equilibrio digital y TDAH

El desafío para las personas con TDAH consiste en que la tecnología no se adueñe de nuestro tiempo ni nuestra atención, sino que se ponga al servicio de nuestros cerebros que aprenden, piensan y viven a un ritmo diferente.

Para los adultos con TDAH el uso de la tecnología representa un reto considerable. Por un lado, nos encontramos con una herramienta valiosa para la organización, el aprendizaje, la creatividad y la autonomía. Pero, por otro, si no se controla adecuadamente puede derivar en sobreestimulación, distracción y hábitos poco saludables. Problemas que **no afectan únicamente** a personas con TDAH, pero que pueden tener un impacto más profundo en nosotros. Estos son algunos de los riesgos que implican un mal uso de la tecnología.

•**Sobreestimulación y dificultad para desconectar** ya que las pantallas generan una gran cantidad de estímulos visuales y auditivos que pueden captar la atención de forma casi automática. Para quienes ya presentamos mayores dificultades en cuanto a la regulación de la atención, esta sobreestimulación puede derivar en problemas para desconectar, dormir o cambiar de actividad. No podemos obviar que muchas aplicaciones están diseñadas para prolongar el tiempo de uso mediante algoritmos que recomiendan contenido personalizado, lo que puede conducir a ciclos de uso prolongado difíciles de interrumpir.

•**Hiperfoco digital**, es decir, un estado de concentración intensa y sostenida en una actividad altamente estimulante que puede ser un problema cuando la actividad elegida es un videojuego, una red social o una serie, y que desplaza otras responsabilidades importantes.

•**Distracción constante**. Las notificaciones, las ventanas emergentes y la multitarea digital fragmentan la atención lo que reduce la productividad, aumenta la frustración y genera la sensación de no avanzar, especialmente en actividades que requieren concentración sostenida. La exposición continua a estímulos digitales breves y altamente recompensantes, como redes sociales o videojuegos competitivos, estimula el sistema de recompensa de manera similar a los refuerzos inmediatos que caracterizan los patrones de impulsividad. Esto puede conducir a una reducción en la capacidad de demora de la gratificación y a dificultades adicionales en la autorregulación emocional.



CONTINÚA EN
PRÓXIMA PÁGINA



•**Impacto emocional y social.** Para las personas con TDAH con una baja autoestima y con dificultad para la gestión del rechazo, el uso excesivo de redes sociales puede aumentar la comparación constante con los otros, la búsqueda de validación externa y la ansiedad, problemas ya de por sí comunes en los cerebros neurodivergentes.

•**Problemas de sueño,** una de las comorbilidades más frecuentes en el TDAH que se ve incrementada por una sobreexposición a las pantallas ya que presenta una relación con la alteración de los ritmos circadianos y con la activación sostenida del sistema nervioso central durante las horas de descanso.

EQUILIBRIO Y CONCIENCIA DIGITAL

A pesar de todos los riesgos que conlleva el uso inapropiado de la tecnología, la clave no está en rechazarla, sino en mantener con ella una relación saludable. Lo más inteligente es aprovecharla para comprender, potenciar y equilibrar una mente que, por su propio dinamismo, está mejor preparada que muchas otras para navegar el mundo acelerado en que vivimos.

Estas son algunas de las estrategias más eficaces para que la tecnología sea nuestra aliada.

•**Regular el tiempo** frente a las pantallas con horarios claros para revisar las redes o jugar, poner límites para los momentos de conexión y establecer pausas tecnológicas programadas. Estos horarios de uso son especialmente relevantes antes de dormir o durante el estudio. Existen múltiples funciones de bienestar digital que permiten bloquear apps, limitar tiempo de pantalla y programar pausas.

•**Minimizar las distracciones.** Se pueden usar aplicaciones que bloqueen las distracciones durante el trabajo o el estudio, como temporizadores o aplicaciones enfocadas en la productividad. También resulta muy útil silenciar las notificaciones no esenciales y usar modos de concentración.

•**Emplear la tecnología con objetivos definidos** dentro del tratamiento o del aprendizaje individualizado. Cuando se pueda, hacer un uso activo y no pasivo, es decir, crear contenido como dibujar, programar, escribir o editar videos, ya que siempre es más enriquecedor que consumirlo pasivamente.

•**Fomentar la alfabetización digital crítica** para distinguir entre herramientas funcionales y distractores según nuestros objetivos. En este sentido, es necesario priorizar las aplicaciones que aporten valor y las herramientas que



ayuden a la productividad, la organización o el aprendizaje en lugar de aplicaciones centradas en el entretenimiento.

•**Crear entornos laborales adaptativos** donde el uso tecnológico esté enfocado en la eficiencia y no en la hiperconectividad.

•**Combinar tecnología con estrategias analógicas.** A pesar de las ventajas digitales, métodos como escribir a mano, usar agendas físicas o realizar ejercicios de respiración sin dispositivos siguen siendo beneficiosos y complementarios.

•**Aplicar técnicas de mindfulness digital** orientadas a la regulación emocional frente a la hiperestimulación.

•**Mantener espacios libres de dispositivos** en momentos de descanso o convivencia familiar.

El impacto de la tecnología en nuestras vidas dependerá del modo en el que la utilicemos. Con una orientación adecuada, puede convertirse en un recurso poderoso para potenciar la atención, fomentar la autonomía y mejorar la calidad de vida de quienes tenemos esta condición neurodivergente. Para nosotros, el reto deberá centrarse en desarrollar entornos digitales diseñados específicamente para las necesidades neurocognitivas del TDAH, así como en establecer criterios éticos y clínicos para su implementación. Sin duda, esta será la mejor base sobre la que construir una relación consciente y equilibrada con el entorno digital.



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_23DRlw

Instagram:

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

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>

**Curso de
Certificación en:**

**Diseño de
Servicios
Excelentes**

**ISO 24082
Service
Excellence
Designer**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 24082
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001: 2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

La normalización, clave para generar confianza y competitividad en el análisis del Informe del Banco Mundial

La importancia de la normalización técnica ha dejado de ser una cuestión meramente operativa para transformarse en un pilar estratégico de la economía global contemporánea. En un escenario marcado por la volatilidad de los mercados y la creciente complejidad de las cadenas de suministro internacionales, la labor de instituciones como la Asociación Española de Normalización y la Organización Internacional de Normalización se vuelve fundamental. La reciente intervención de Javier García Díaz en Ginebra, en el marco de las sesiones de análisis sobre el Informe del Banco Mundial, subraya precisamente esta realidad. Como Director General de UNE y Vicepresidente de ISO, García Díaz ha puesto de manifiesto que los estándares no son solo documentos técnicos, sino verdaderas herramientas de diplomacia económica y de fomento de la competitividad. Su discurso se centró en cómo estos marcos comunes permiten a las empresas navegar en entornos regulatorios que a menudo resultan asfixiantes por su falta de cohesión.



CONTINÚA EN
PRÓXIMA PÁGINA



El contexto en el que se produce esta reflexión es particularmente relevante, ya que el Banco Mundial ha estado evolucionando sus metodologías de medición del clima de negocios, pasando de los antiguos indicadores a un modelo mucho más integral que valora la preparación de las empresas para operar de manera eficiente y transparente. En este nuevo paradigma, la normalización actúa como un lubricante que reduce las fricciones entre las distintas jurisdicciones nacionales. Cuando una organización adopta una norma internacional, está enviando una señal clara al mercado sobre su compromiso con la excelencia y la seguridad.

Esto no solo facilita el acceso a nuevos clientes en el extranjero, sino que también minimiza los riesgos legales y financieros asociados a la exportación. La previsibilidad de la que habla Javier García Díaz se traduce, en términos prácticos, en que un inversor en cualquier parte del mundo puede confiar en que una empresa que cumple con estándares ISO sigue procesos verificables y comparables a nivel global.

Además de su función como facilitadora del comercio, la normalización técnica desempeña un papel crucial en la integración de los nuevos requisitos de sostenibilidad y digitalización. Actualmente, las organizaciones se enfrentan al reto de demostrar su impacto ambiental y social de una manera que sea creíble y no se perciba como una simple operación de marketing. Aquí es donde los estándares internacionales proporcionan el rigor necesario, ofreciendo metodologías precisas para medir la huella de carbono, gestionar la economía circular o asegurar la debida diligencia en los derechos humanos dentro de las cadenas de suministro. La coherencia que aportan estas normas permite que las leyes nacionales no se conviertan en obstáculos insalvables para las pymes, ya que las normas técnicas actúan como una guía práctica para cumplir con la legalidad de forma estructurada. De este modo, la normalización contribuye directamente a un desarrollo más ordenado de los mercados, evitando la fragmentación que se produciría si cada región o sector decidiera imponer sus propios requisitos técnicos de forma aislada.

Desde una perspectiva macroeconómica, el impacto de la normalización es cuantificable y significativo. Diversos estudios realizados en países de la Unión Europea sugieren que la aplicación de normas técnicas contribuye anualmente a un incremento de entre el cero coma tres y el uno por ciento del Producto Interior Bruto. Este crecimiento no es accidental, sino que es el resultado directo de la mejora en la eficiencia de los procesos productivos y de la aceleración del ciclo de innovación. Al existir estándares previos sobre los que construir, las empresas no tienen que "reinventar la rueda" en cada

iniciativa, lo que les permite dedicar sus recursos a la creación de valor diferencial. Javier García Díaz enfatizó en Ginebra que esta capacidad de las normas para reducir la incertidumbre es lo que finalmente refuerza la confianza de los consumidores y de los socios comerciales. En un entorno donde la desinformación y la falta de transparencia pueden dañar gravemente la reputación de una marca, contar con una certificación basada en normas internacionales se convierte en un activo intangible de un valor incalculable.

Por otro lado, la normalización es también un motor de innovación responsable. A menudo se piensa erróneamente que las normas frenan la creatividad por ser demasiado rígidas, pero la realidad es la opuesta. Al definir un lenguaje común y unos requisitos de seguridad básicos, las normas crean un campo de juego seguro donde las empresas pueden experimentar con nuevas tecnologías, como la inteligencia artificial o el internet de las cosas, sabiendo que sus desarrollos serán interoperables con los de otros proveedores. La labor de ISO y UNE en la creación de estándares para la gestión ética de la inteligencia artificial es un claro ejemplo de cómo la normalización se anticipa a los problemas sociales y técnicos, aportando referencias compartidas que estabilizan el funcionamiento de los mercados tecnológicos antes de que estos se vuelvan caóticos.

Finalmente, la presencia de líderes españoles en puestos de alta responsabilidad dentro de la Organización Internacional de Normalización refuerza la posición de la industria nacional en el exterior. Que Javier García Díaz ejerza como Vicepresidente de ISO garantiza que la visión y las necesidades de las empresas españolas sean escuchadas en los foros donde se definen las reglas del juego global. La normalización, en definitiva, se consolida como un elemento de apoyo indispensable para afrontar los desafíos económicos actuales, desde la transición energética hasta la transformación digital, aportando siempre esa base de estabilidad y buenas prácticas que permite a las organizaciones crecer de manera sostenible y competitiva en un mundo cada vez más interconectado. La confianza que generan estos marcos comunes es el cimiento sobre el cual se construye la economía del futuro, una economía donde la calidad y la coherencia son las mejores defensas contra la incertidumbre.

**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.



**Normalización
Española**

**Progreso
compartido**

une.org

Deja de perder el tiempo intentando Gestionarlo
y aprende definitivamente a Gobernarlo.



Time Slot Governance TSG4 White Belt
Porque lo que no es Método es Improvisación

