Consejo de liderazgo tecnológico con CIOs

Del soporte a la estrategia: el responsable de tecnología ante la IA, la ciberseguridad y el talento.

Propósito del documento

Este documento recoge, de forma agregada, anónima y estructurada, los principales aprendizajes del Consejo de Liderazgo Tecnológico celebrado por ADIMUR el 24 de septiembre de 2026 con CIOs, directores de innovación y responsables de sistemas de empresas de referencia de la Región de Murcia.

El objetivo es doble: generar pensamiento directivo útil, trasladable y accionable para otros responsables de tecnología y equipos de dirección —especialmente de la pyme—, y construir una visión compartida sobre qué papel debe ocupar la función tecnológica en el gobierno de la empresa murciana.

No se trata de un documento teórico, sino de una síntesis realista construida a partir de la experiencia de quienes cada día sostienen la operación, defienden la empresa frente a ciberataques y gestionan la llegada de la inteligencia artificial. El enfoque sigue los estándares habituales de ADIMUR: rigor conceptual, conexión con tendencias actuales y orientación clara a la mejora directiva.

Este Consejo forma parte de la línea de espacios de reflexión directiva por áreas funcionales clave —tras los ya celebrados de Finanzas, Ventas, Recursos Humanos y CEOs—, con la ambición de convertir la experiencia agregada en criterios de dirección aplicables a la empresa murciana.

METODOLOGÍA

- Consejo profesional con responsables de tecnología de empresas de sectores muy diversos: agua y medio ambiente, construcción naval y defensa, servicios públicos, alimentación, química, educación y bienes de consumo.

- Sesión de debate abierto moderado de dos horas, en formato de comida de trabajo, estructurada en cinco ejes: el CIO en el comité de dirección, la incorporación de la IA, la ciberseguridad, los proyectos que aportan valor y los retos de futuro.

- Moderación a cargo de Juan Navas Pallarés, presidente de ADIMUR, con la participación de Reyes Samper, directora de ADIMUR.

- Grabación y transcripción de la sesión, tratadas de forma estrictamente confidencial y utilizadas exclusivamente para la elaboración de este documento agregado y anónimo.

- Revisión del borrador por los participantes, cuyas aportaciones posteriores se han integrado en el texto.

- Contraste con datos de referencia: KPMG Global Tech Report 2026 (edición España), Gartner CIO Agenda 2026, INCIBE Balance de Ciberseguridad 2025, Guía Salarial TIC 2026 de Adecco, INE, CaixaBank Research, PwC Digital Trust Insights 2026, Allianz, ESET e Hiscox.

DE APAGAR FUEGOS A APORTAR VALOR

Conclusiones del Consejo de Liderazgo Tecnológico de ADIMUR sobre el responsable de tecnología ante la inteligencia artificial, la ciberseguridad y la escasez de talento.

Los responsables de tecnología reunidos por ADIMUR coinciden en un diagnóstico: la tecnología ya no es un departamento de soporte, sino parte de la cadena de valor de la empresa. Cualquier inversión —una máquina, un contrato, una licitación— tiene hoy un componente tecnológico que, si no se considera desde el principio, encarece, retrasa o compromete el resultado.



Y, sin embargo, a la pregunta de quién se sienta en el comité de dirección, se levantaron pocas manos. La paradoja es conocida: el negocio reconoce que la información es una de sus prioridades, pero el responsable de tecnología sigue llegando tarde a las decisiones, a menudo cuando el sistema ya se ha comprado y solo queda «ponerlo en marcha». El reto que el Consejo se marca es doble: ganarse ese sitio hablando el lenguaje del negocio, y liberar tiempo del mantenimiento diario para dedicarlo a lo que de verdad aporta valor.

“Lo primero que tenemos que hacer es valorarnos nosotros mismos.”

Cinco ideas fuerza

1. El responsable de tecnología debe estar en el órgano de decisión: es quien tiene la visión transversal de todos los procesos de la empresa y quien puede anticipar el impacto de cada decisión. Para ganarse ese sitio, debe pasar de reactivo a proactivo y de técnico a traductor del negocio.

2. Las inversiones tecnológicas ya no se justifican con productividad, sino con euros y con riesgo: lo que se ahorra, lo que se deja de contratar, lo que se gana en licitaciones y lo que se arriesga si no se hace.

3. La inteligencia artificial generativa ha puesto un «mago» en manos de cada empleado. Sin gobierno del dato, política de uso, formación y herramientas corporativas, se multiplican la informática en la sombra y las fugas de información. La IA sin control es, además, un riesgo de ciberseguridad.

4. En ciberseguridad, el factor humano sigue siendo el eslabón más débil, los entornos industriales (OT) son el gran punto ciego y la regulación (ENS, NIS2) ha llevado por fin la responsabilidad al consejo de administración.

5. El talento tecnológico compite hoy con el mundo entero gracias al teletrabajo: retener es más difícil que atraer, y la cantera propia y el talento local son la estrategia más sólida.

El CIO en el comité de dirección: del soporte a la estrategia

Históricamente, el área de tecnología ha dependido del director financiero, que la ha mirado sobre todo como un coste. Los asistentes reconocieron que esa herencia pesa todavía: en algunos casos existe un comité de IT, pero se limita a ejecutar decisiones tomadas en otro órgano, sin discutir la estrategia. Otros, en cambio, se sienten plenamente representados porque participan en los proyectos de todas las áreas, y en el caso de las organizaciones en las que el responsable de tecnología sí forma parte del órgano de gobierno, la conclusión fue unánime: facilita muchísimo la aprobación de inversiones y la alineación entre negocio y tecnología.



Se identificaron tres argumentos que cualquier responsable de tecnología puede trasladar a su CEO para reclamar su sitio en el comité:

1. **Interno: la visión transversal.** Tecnología es el único departamento que conoce todos los procesos de la empresa —finanzas, operaciones, logística, comercial, producción— y cómo se conectan entre sí. Cada área ve su parcela; el CIO ve el conjunto y puede anticipar los problemas antes de que aparezcan.

2. **Externo: la competitividad.** En sectores como el público, sin certificaciones como el Esquema Nacional de Seguridad en categoría alta, ni siquiera es posible presentarse a un concurso. Anticiparse a la siguiente norma —por ejemplo, la ISO/IEC 42001 de gestión de la IA— es una ventaja competitiva directa.

3. **Inversor: toda inversión es ya tecnológica.** Hoy no se compra una máquina que no tenga que conectarse con el MES, el ERP o los sistemas de datos. Si tecnología no participa desde el principio, el proyecto llega tarde, más caro o incompatible.

El debate fue también autocrítico. El responsable de tecnología tiende a convertirse en «el que pone pegas» porque conoce todas las implicaciones, y conviene dosificar la información y hablar en el idioma del comité. Cuando la dirección comenta que «la competencia ya lo hace todo con IA», la respuesta eficaz no es desmentirlo, sino convertir esa inquietud en una propuesta: un plan estratégico de inversión. Varias empresas han optado por figuras de enlace —«business partners» de tecnología— presentes en los comités de cada área, que actúan como puente y traductores entre negocio y sistemas.

¿Es más fácil justificar hoy una inversión tecnológica?

Los asistentes coincidieron en que la conversación ha cambiado. Ya no basta con hablar de productividad: ahorrar tres horas diarias a un empleado no es retorno si esas horas no se traducen en resultado. La dirección pide euros —lo que se ahorra, la contratación que se evita, los concursos que se ganan—, y la vía más eficaz para defender proyectos es el riesgo: qué ocurre, jurídica o operativamente, si no se hace. Se reconoció también una dificultad real: tecnología solo puede medir una parte del retorno, porque el resto depende de que las áreas de negocio cuantifiquen el beneficio que obtienen.

Las competencias del responsable de tecnología excelente

- **Habilidad comercial interna:** saber «vender» los proyectos dentro de la empresa y relacionarse con todas las áreas.
- **Empatía:** ponerse en el lugar del usuario y de cada departamento, en una función que gestiona a diario la frustración de quien no puede trabajar.
- **Conocimiento de los procesos de negocio y visión estratégica:** no hace falta ser experto del sector, pero sí entender cómo funciona la empresa para poder hablar en el comité de lo que preocupa al comité.
- **Gestión del riesgo:** saber qué riesgos asumir y cuáles no, y usarlo como argumento para justificar inversiones.
- **Capacidad de autoaprendizaje y adaptación:** en grupos diversificados, el responsable de tecnología pasa de un sector a otro en semanas y debe aprender rápido.

Dato Gartner CIO Agenda 2026

- Solo el 33% de los responsables de tecnología persigue de forma consistente resultados financieros derivados de la tecnología, pero quienes lo hacen tienen un 25% más de probabilidades de superar a sus pares.

“Tenemos que ser proactivos, no reactivos: cuando somos reactivos es porque ya nos han dicho «esto lo hemos comprado, ponedlo en marcha».”



Inteligencia artificial: gobernar antes que desplegar

Los asistentes pidieron separar dos realidades. La IA analítica y predictiva —basada en datos y modelos matemáticos— lleva años en las empresas y no genera grandes problemas. La IA generativa, en cambio, ha puesto en manos de cualquier usuario una herramienta que «parece magia», y ese es precisamente el problema: los proveedores comerciales alimentan esa expectativa y el responsable de tecnología queda en la incómoda posición de rebajarla.

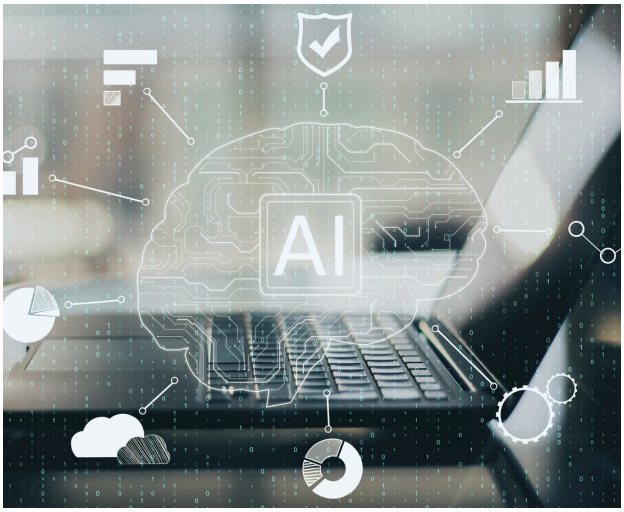
El resultado es un fenómeno que preocupa a todos: la aparición de «magos internos». Se citaron casos de áreas que contratan soluciones de IA por su cuenta, de máquinas que envían datos a proveedores externos sin conocimiento de sistemas, de un empleado que subió años de documentación de I+D a una herramienta pública para preparar una presentación, y de usuarios que, con herramientas de programación asistida, desarrollan aplicaciones propias al margen de sistemas. La disyuntiva es clara: si tecnología no las acompaña, se convierten en informática en la sombra que antes o después habrá que auditar y mantene

“No le podemos poner puertas al campo: o se ofrecen herramientas corporativas seguras, o cada uno hará lo que le dé la gana.”

¿Quién decide y cómo se gobierna?

En la mayoría de las empresas presentes la decisión sobre los casos de uso recae todavía en tecnología. Las organizaciones más avanzadas destinan una parte muy relevante de su esfuerzo —en un caso, la mayor parte del presupuesto horario del área de IA— a los «guardarraíles»: entornos controlados, reglas de paso a producción y supervisión. Las prácticas compartidas fueron:

- **Política de uso de IA** que explique a los empleados qué pueden hacer, cómo y con qué consecuencias en caso de fuga de información.
- **Licencias corporativas** de los grandes modelos en entornos cerrados, y en algunos casos infraestructura propia, para evitar el uso descontrolado de versiones gratuitas.
- **Formación por niveles con certificación interna,** al estilo de los niveles de idiomas: superar un nivel avanzado exige presentar un caso de uso real, y a cambio se da acceso a herramientas más potentes.
- **Comités de ética** donde el uso de la IA tiene implicaciones sobre personas o datos sensibles.



¿Quién decide y cómo se gobierna?

El caso más claro surgió en la contratación pública: una IA que cruza la solvencia y clasificación de la empresa con las licitaciones publicadas, preselecciona las convenientes, analiza qué competidores se presentan y qué bajas suelen ofertar, y reutiliza décadas de memorias técnicas. El resultado: más concursos presentados, mejor selección y menos horas de técnicos perdidas en ofertas inviables, aunque una parte sustancial del trabajo sigue requiriendo supervisión humana. Se señaló también el reverso: al bajar el coste de presentarse, concursos que antes atraían a cinco empresas reciben ahora treinta.

Otros casos citados fueron la gestión de correo en posventa —decenas de buzones e incidencias sin trazabilidad, ordenadas en media hora— y, por encima de todos, el desarrollo de software, señalado como el caso de uso con retorno económico más evidente. Se recordó además un dato del libro blanco de buenas prácticas para la adopción de la IA en la pyme: solo un 13% de las pymes españolas estaría obteniendo valor real de la IA.

La recomendación: primero el dato

La conclusión fue unánime: sin gobierno y calidad del dato no hay IA fiable. Cuando los datos están mal estructurados, cada consulta exige explicaciones interminables a la herramienta; cuando están bien gobernados, basta una frase. Una de las empresas ha incorporado incluso un responsable de datos (CDO) a raíz de este aprendizaje. Se advirtió además de dos riesgos: el coste actual de muchas herramientas está fuertemente subvencionado y el precio real llegará, y el uso intensivo puede erosionar la capacidad de análisis crítico de los equipos. Por último, se insistió en que automatizar no es lo mismo que reinventar: aplicar IA a un mal proceso solo produce un mal proceso más rápido.

IA y ciberseguridad, dos caras del mismo riesgo. En la revisión del documento se quiso subrayar que los dos grandes ejes de este Consejo van entrelazados. Una IA descontrolada, es decir, sin gobernanza del dato, puede convertirse en una de las mayores vulnerabilidades de la empresa, tanto por la pérdida de confidencialidad de la información como desde el punto de vista de la ciberseguridad. No es una preocupación teórica: en Japón, grandes multinacionales conocidas por todos están parando proyectos de IA por temor a perder el control del dato.

Lo que confirman los datos (KPMG Global Tech Report 2026, España)

- El 65% de los responsables tecnológicos españoles percibe ya valor empresarial en sus iniciativas de IA, aunque solo el 23% ha logrado un retorno repetible en múltiples casos de uso. El 85% espera que la IA se convierta en generadora de retorno antes de que termine el año.
- El 81% de las empresas españolas ya incorpora agentes de IA en sus sistemas, y el 90% espera que «gestionar agentes de IA» sea una habilidad crítica dentro de cinco años.
- Las prioridades de gobernanza del dato en España para 2026 son, por este orden: seguridad, accesibilidad, análisis y cultura del dato.

Murcia, frente a España: la adopción de la IA en la empresa

- **INE, Encuesta TIC en empresas (2025):** el 21,1% de las empresas españolas de 10 o más empleados utiliza IA, 8,7 puntos más que un año antes. En la Región de Murcia la cifra es del 15,3%, casi seis puntos por debajo, y también va por detrás en servicios en la nube (37,0% frente a 44,3%) y en análisis de datos (37,0% frente a 41,4%).
- **CaixaBank Research (2026):** casi tres de cada cinco grandes empresas usan IA, frente al 31% de las medianas, el 18% de las pequeñas y el 13% de las microempresas. La principal barrera es la falta de capacidades, seguida de los datos y la gobernanza.
- **ESET, SMB Cyber Readiness Index 2026:** el 87% de las pymes españolas ya usa aplicaciones de IA, la cifra más alta de los trece países analizados, pero el 38% no tiene políticas que limiten su uso fuera de los procesos aprobados por la dirección.

Ciberseguridad: el eslabón humano y el punto ciego industrial

La exposición varía mucho según el sector, pero entre los presentes había organizaciones especialmente sensibles: defensa, servicios de emergencias, gestión del ciclo del agua y datos de investigación. Algunas reciben ataques constantes —incluidos actores de otros países— cada vez que su nombre aparece en una noticia. La respuesta pasa por ecosistemas completos: centros de operaciones de seguridad (SOC), agentes que detectan comportamientos anómalos, gestión continua de vulnerabilidades, pruebas de intrusión externas e internas al menos una vez al año y desarrollo seguro de software, con control estricto de las librerías de terceros.

El gran punto ciego: la tecnología de operación (OT)

El riesgo que más preocupó a los perfiles industriales fueron los entornos de planta: autómatas (PLC) con código antiguo que no se pueden actualizar en cinco minutos y procesos físicos —reactores, redes de agua— cuyo fallo tiene consecuencias reales. Ahí, la única defensa viable hoy es la monitorización de comportamientos anómalos. Hubo también escepticismo ante la convergencia entre IT y OT que promueve el mercado: conectar ambos mundos multiplica la superficie de ataque.

Un foco crítico es el **acceso de proveedores externos** a la planta: el técnico que viene a actualizar una máquina y conecta su portátil o su móvil sin control. Las soluciones compartidas incluyen herramientas de acceso privilegiado específicas para entornos OT, plataformas de acceso único que habilitan cada conexión por tiempo limitado y la graban, y el control de los dispositivos móviles dentro de la planta mediante redes 5G privadas.



Proveedores críticos y fugas internas

Evaluar a los proveedores críticos sigue siendo difícil: los cuestionarios de seguridad no permiten verificar lo que se declara. Una de las empresas ha optado por una decisión estratégica costosa pero eficaz: proveer al colaborador externo de todo el ecosistema —equipo, licencias y programas— bajo su control. Otra relató cómo una memoria técnica fue filtrada a un competidor desde una de sus oficinas, después de que tecnología hubiera advertido del riesgo sin conseguir el presupuesto para evitarlo. Y otra recordó que fue un ataque de ransomware lo que desbloqueó, en su día, la inversión que no se había logrado antes.

“Si has hecho algo y pasa, es un accidente; si no has hecho nada, es una responsabilidad.”

La regulación —Esquema Nacional de Seguridad y NIS2— fue valorada como un avance decisivo, porque deja claro que **los consejos de administración son responsables.** El reverso es que en muchas pymes la ciberseguridad se aborda por miedo a la sanción, no por convicción.

Recomendaciones para un directivo no técnico

La primera recomendación fue unánime: concienciación de las personas. Una empresa que realiza simulacros de phishing trimestrales con grupos de 1.500 usuarios constata que en torno al 15% sigue cayendo, pese a la formación. Sobre esa base, el Consejo propuso un decálogo mínimo para cualquier empresa:

1. Concienciación y formación continua de todos los usuarios, con simulacros periódicos.
2. Doble factor de autenticación en todos los accesos.
3. Protección avanzada de equipos (EDR) y, si es posible, servicio gestionado de detección y respuesta.
4. Gestión de identidades: saber quién accede, a qué y cuándo.
5. Gestión de vulnerabilidades y auditorías periódicas.
6. Segmentación de redes, especialmente entre oficina y planta.
7. Copias de seguridad inmutables y probadas.
8. Control de los accesos de proveedores externos.
9. Seguro de ciberriesgo, revisando bien las coberturas: además de indemnizar, aporta equipos especializados para reducir el tiempo de parada.
10. Responsabilidad explícita del comité de dirección sobre el riesgo ciber.

El contexto en España

- **INCIBE, Balance de Ciberseguridad 2025:** 122.223 incidentes gestionados en España (+26% interanual). El malware lideró las categorías con 55.411 casos, incluidos 392 ataques de ransomware, y el 60% de los incidentes afectó a pymes.
- **NIS2:** la Ley de Coordinación y Gobernanza de la Ciberseguridad que transpone la directiva quedará aplicable a entidades de 50 o más empleados o 10 M€ de facturación en sectores esenciales (energía, transporte, banca, salud, infraestructura digital) e importantes (industria, alimentación, servicios digitales), con notificación de incidentes en 24 horas y sanciones de hasta 10 M€ o el 2% de la facturación global para entidades esenciales.

Lo que confirman PwC, Allianz, ESET e Hiscox

- **PwC, Global Digital Trust Insights 2026:** el 60% de las empresas aumenta su inversión en ciberseguridad, pero solo el 6% se siente «muy capaz» frente a todas las vulnerabilidades evaluadas y el 27% ha sufrido incidentes con pérdidas superiores al millón de dólares. Solo el 24% invierte significativamente más en medidas proactivas que reactivas.
- **Allianz, Barómetro de Riesgos 2026:** el ciberriesgo es la principal preocupación para el 48% de las empresas españolas, en primer lugar; la inteligencia artificial aparece ya en quinto puesto (22%).
- **ESET, SMB Cyber Readiness Index 2026:** el 45% de las pymes españolas sufrió al menos un incidente de ciberseguridad en el último año; España es el tercer país con más pymes afectadas.
- **Hiscox, Informe de Ciberpreparación 2025:** seis de cada diez pymes han sufrido ataques en el último año, y más de la mitad de las empresas cree haber sufrido ciberataques relacionados con la IA.

Proyectos que aportan valor: liberar tiempo para transformar

El debate puso nombre a una realidad compartida: el trabajo del área de tecnología se reparte entre mantener (run), crecer (grow) y transformar (transform), y el mantenimiento —equipos, impresoras, incidencias, actualizaciones— consume en torno al 80% del tiempo. Mientras el responsable de tecnología esté apagando fuegos, la dirección no le verá aportar valor. De ahí una recomendación muy práctica: automatizar y «abaratar» al máximo el soporte, y dedicar el tiempo liberado a proyectos con visibilidad para el negocio.

“Si estoy apagando fuegos, no me ven. Tengo que liberar tiempo para aportar algo que la dirección pueda ver.”

El ejemplo más ilustrativo fue el de una empresa que, tras un cambio de propiedad y de CEO, revisó su plan estratégico a cinco años: de las 32 iniciativas surgidas en todos los departamentos, el 80% implicaba digitalización. La lección es doble. Por un lado, diseñar un plan estratégico sin tecnología en la mesa es diseñarlo a ciegas. Por otro, la mejor manera de defender el presupuesto tecnológico es derivar el plan de sistemas directamente del plan estratégico de la compañía y mostrar, iniciativa a iniciativa, cómo contribuye a cada objetivo de negocio.



Se apuntó, además, un cambio en cómo la dirección pide los números: ya no un presupuesto cerrado, sino **escenarios,** del peor al mejor, ante subidas de costes de componentes, tensiones en la cadena de suministro o crisis geopolíticas. Esa misma incertidumbre se traslada a los contratos tecnológicos y logísticos, cada vez más abiertos y difíciles de cerrar a precio fijo.

La tecnología como generadora de nuevos negocios. El valor de la función tecnológica no se agota en mejorar la productividad y reducir costes. El conocimiento acumulado durante años en las empresas, combinado con la IA y otras tecnologías, puede convertirse en la base de nuevos productos, servicios y oportunidades de negocio. Es el paso de una tecnología que optimiza lo que ya existe a una tecnología que abre mercados nuevos, y el terreno donde el tiempo liberado del mantenimiento puede tener más impacto en la cuenta de resultados.

Lo que confirman los datos

- **Gartner CIO Agenda 2026:** solo el 48% de las iniciativas digitales cumple o supera sus objetivos. El 94% de los responsables de tecnología espera cambios significativos en sus planes en los próximos 24 meses. La IA aplicada a eficiencia puede generar ahorros de entre el 5% y el 30% según el caso de uso.
- **KPMG Global Tech Report 2026:** el 66% de las empresas españolas reconoce que sus procesos heredados generan inversiones con escaso retorno. Las empresas de mejor desempeño invierten más en crecimiento precisamente porque arrastran menos deuda tecnológica.

Talento y retos de futuro: el próximo paso del CIO

Retener es más difícil que atraer

El teletrabajo ha cambiado las reglas: un profesional tecnológico en Murcia compite hoy con empleadores de todo el mundo, y algunas empresas han perdido perfiles fichados por compañías extranjeras que pagan varias veces más sin necesidad de mudanza. A ello se suman fenómenos como el abandono de procesos de selección sin aviso o la baja disposición a asumir trabajos exigentes. La captación puede resolverse con una buena oferta, pero «la píldora dorada dura seis meses»: lo difícil es generar sentimiento de pertenencia.

Las estrategias compartidas fueron tres: **formar la cantera propia** con alumnos en prácticas que se incorporan al terminar; **priorizar el talento local** —de Murcia o Cartagena— frente al de Madrid, por su mayor arraigo; y poner en valor lo que la empresa ofrece además del salario: estabilidad, flexibilidad, buen liderazgo y calidad de vida. Murcia es un lugar muy atractivo para vivir, pero su conectividad e infraestructuras de transporte siguen siendo una barrera para atraer perfiles sénior de fuera. Algunos asistentes anticiparon además que el mercado tecnológico, hoy muy tensionado, puede ajustarse a la baja a medida que la IA asuma parte del trabajo.

El siguiente gran salto

La respuesta mayoritaria fue **gobernar equipos híbridos de personas, máquinas y agentes de IA:** lo difícil no es gobernar la tecnología, sino gobernarla con personas. Algunas empresas trabajan ya en IAs que gobiernan a otras IAs, y una de ellas prueba robots humanoides en su cadena de producción. Este salto cambia la naturaleza del puesto. En los próximos cinco años, el responsable de tecnología pasará de gestionar sistemas a gestionar organizaciones en las que convivirán personas, agentes de IA y máquinas autónomas. Ello abre retos nuevos de supervisión (quién controla lo que hace cada agente y con qué criterios), de seguridad (cada agente y cada máquina conectada es un nuevo punto de exposición) y de responsabilidad (quién responde de una decisión tomada, total o parcialmente, por un sistema autónomo).



La convergencia de tecnologías

La IA no llegará sola. Su combinación con sensores, satélites, sistemas de información geográfica (GIS), robótica y gemelos digitales va a transformar en los próximos años sectores clave para la Región de Murcia, como la agricultura, el agua, la industria o el medio ambiente: desde el riego y la gestión de cultivos basados en datos hasta redes de agua o plantas industriales replicadas y simuladas en entornos virtuales antes de intervenir en ellas. Para el responsable de tecnología, el reto será integrar estas piezas en una arquitectura coherente y segura, y no como proyectos aislados.

Qué piden a las instituciones y a ADIMUR

- **Mesura:** no trasladar a las empresas la urgencia de cada nueva tendencia. Muchas pymes murcianas están aún en la «industria 2.0» y no pueden saltar a la 5.0 por decreto.

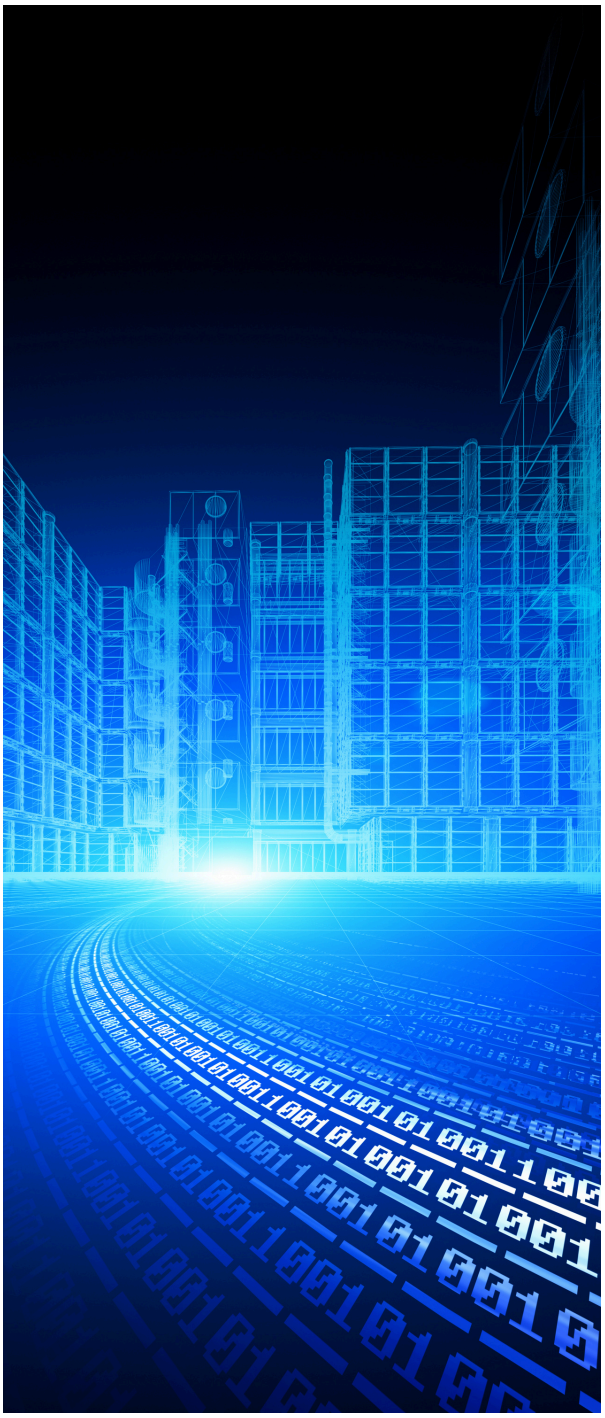
- **Infraestructuras:** conectividad, transporte y, cada vez más, capacidad energética, que será la gran limitación de la IA.

- **A ADIMUR:** trasladar estas conclusiones a empresas que avanzan a distinta velocidad —especialmente a la pyme— y defender en los comités de dirección el valor de la función tecnológica. Y mantener espacios como este Consejo, que permiten salir del día a día y compartir experiencias entre pares.

El talento, prioridad compartida

- **KPMG Global Tech Report 2026:** el 67% de los responsables tecnológicos españoles carece del talento necesario para ejecutar sus planes de transformación, frente al 53% de la media global. Es la principal limitación señalada, por delante de la inversión.

- **Guía Salarial TIC 2026 (Adecco):** el sector tecnológico español sumó 28.850 profesionales en 2025 (+4,5%), pero las ofertas de empleo solo crecieron un 1,8%: el mercado ya no busca contratar más, sino contratar mejor. Los perfiles sénior de IA, ciberseguridad, cloud y datos son los más escasos y mejor pagados.



Cierre: una reflexión autocrítica

La sesión terminó con una mirada hacia dentro. Uno de los asistentes trazó un paralelismo con la sanidad: durante décadas los hospitales los dirigían médicos, hasta que se entendió que la gestión requería perfiles con visión de conjunto. La función tecnológica vive un cambio similar: dejar de pensar solo en la tecnología y empezar a pensar en la empresa. Otro lo resumió con una imagen: pasar del estereotipo del técnico encerrado en su sala al directivo que se sienta en la mesa con el resto del comité.

Se reivindicó también la innovación como función: aprovechar el tiempo que libera la IA para buscar nuevos proyectos, apoyarse en los fondos europeos y, sobre todo, parar de vez en cuando para reflexionar. Algo que, como se reconoció, requiere madurez y valentía.

“Tenemos que dejar de pensar tanto en la tecnología y empezar a pensar en la empresa.”

Síntesis: seis palancas para el responsable de tecnología del futuro

A modo de cierre operativo, estas son seis líneas de acción directamente alineadas con lo debatido en el Consejo y respaldadas por la evidencia recogida en este documento:

- **Ganarse la silla en el comité de dirección:** argumentar desde la visión transversal de los procesos, la competitividad y el impacto en cada inversión, y pasar de reactivo a proactivo.
- **Hablar en euros y en riesgo, no en productividad:** traducir cada proyecto a ahorro, ingresos, contrataciones evitadas o riesgos jurídicos y operativos mitigados.
- **Gobernar la IA antes de desplegarla:** gobierno y calidad del dato, política de uso, herramientas corporativas y formación certificada; acompañar a los «magos internos» en lugar de ignorarlos.
- **Hacer de la ciberseguridad una responsabilidad del consejo:** concienciación continua, control de accesos de terceros, atención específica a los entornos industriales y un decálogo mínimo para cualquier empresa.
- **Liberar tiempo del mantenimiento para transformar:** automatizar el soporte y alinear el plan de sistemas con el plan estratégico de la compañía, iniciativa a iniciativa; y aprovechar el conocimiento acumulado de la empresa para crear nuevos productos y servicios.
- **Cuidar el talento propio:** cantera, talento local, sentimiento de pertenencia y preparación para liderar equipos híbridos de personas y agentes de IA.

El Consejo de Liderazgo Tecnológico de ADIMUR confirma que la tecnología se ha convertido en la columna vertebral de la empresa murciana, pero que su valor no depende de las herramientas, sino de la capacidad de quienes la dirigen para sentarse en la mesa, hablar el lenguaje del negocio y anticiparse. Desde ADIMUR queremos consolidar estos Consejos como espacios estables de reflexión y aprendizaje entre pares, y contribuir a que el responsable de tecnología sea reconocido como lo que ya es: un directivo clave para el futuro de la empresa.

Fuentes y participantes

Fuentes

KPMG. Global Tech Report 2026 (edición España) y Perspectivas 2026.

Gartner. CIO Agenda 2026.

INCIBE. Balance de Ciberseguridad 2025.

Adecco. Guía Salarial TIC 2026.

INE. Encuesta sobre el uso de TIC y del comercio electrónico en las empresas 2024-2025.

CaixaBank Research. La adopción de la IA en la empresa española avanza con rapidez, pero sigue siendo limitada y desigual (mayo 2026).

PwC. Global Digital Trust Insights 2026.

Allianz Commercial. Barómetro de Riesgos 2026.

ESET. SMB Cyber Readiness Index 2026.

Hiscox. Informe de Ciberpreparación 2025.

Directiva (UE) 2022/2555 (NIS2) y Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

Participantes

Nuestro más sincero agradecimiento a las personas que, de forma desinteresada, pusieron su conocimiento al servicio de los demás:

Juan Navas Pallarés, Presidente ADIMUR — Director Territorial de INFORGES-moderador
Reyes Samper, Directora ADIMUR
Fernando Alcaraz, Innovación y Tecnología, VEOLIA
Eloy Jiménez, Director de Innovación, Grupo HOZONO GLOBAL
José Miguel Sánchez, Estrategia y Transformación Digital, NAVANTIA
Miguel Ángel Guillén, Director TIC, UCAM
Juan Francisco García, Responsable de Sistemas de Información, GRUPO FUERTES
Ángel Prieto, Responsable de Informática y Comunicaciones, JAKE
Pablo Caja, Responsable de Sistemas, ZUKAN
José Martínez, CIO de GOBIK
Fernando Martínez, Dirección IT, Seguridad y Medio Ambiente, TAKASAGO
Alvaro Manteca, Responsable de Sistemas, MTHELMET

ADIMUR
ASOCIACIÓN DE DIRECTIVOS DE LA REGIÓN DE MURCIA