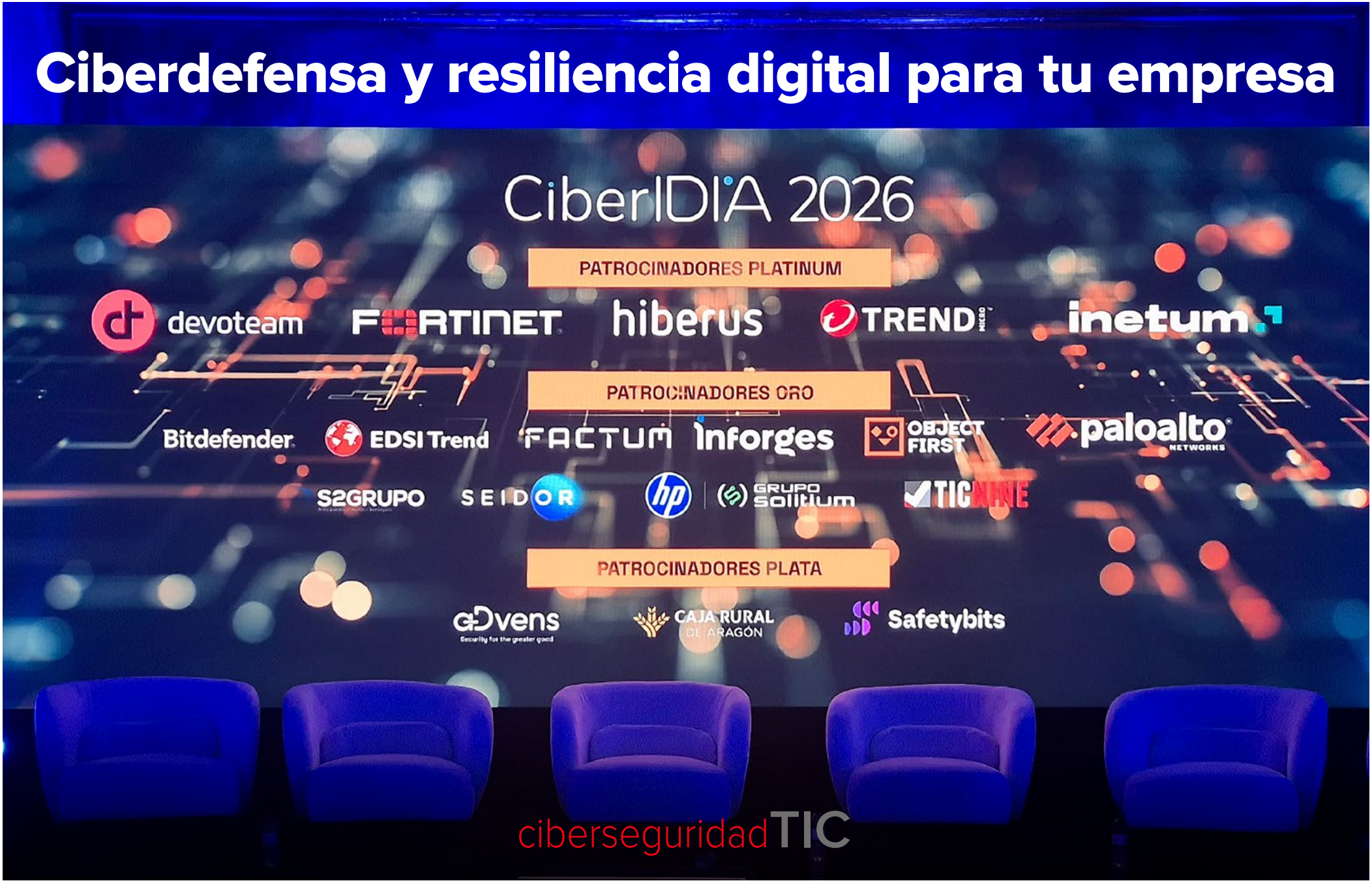
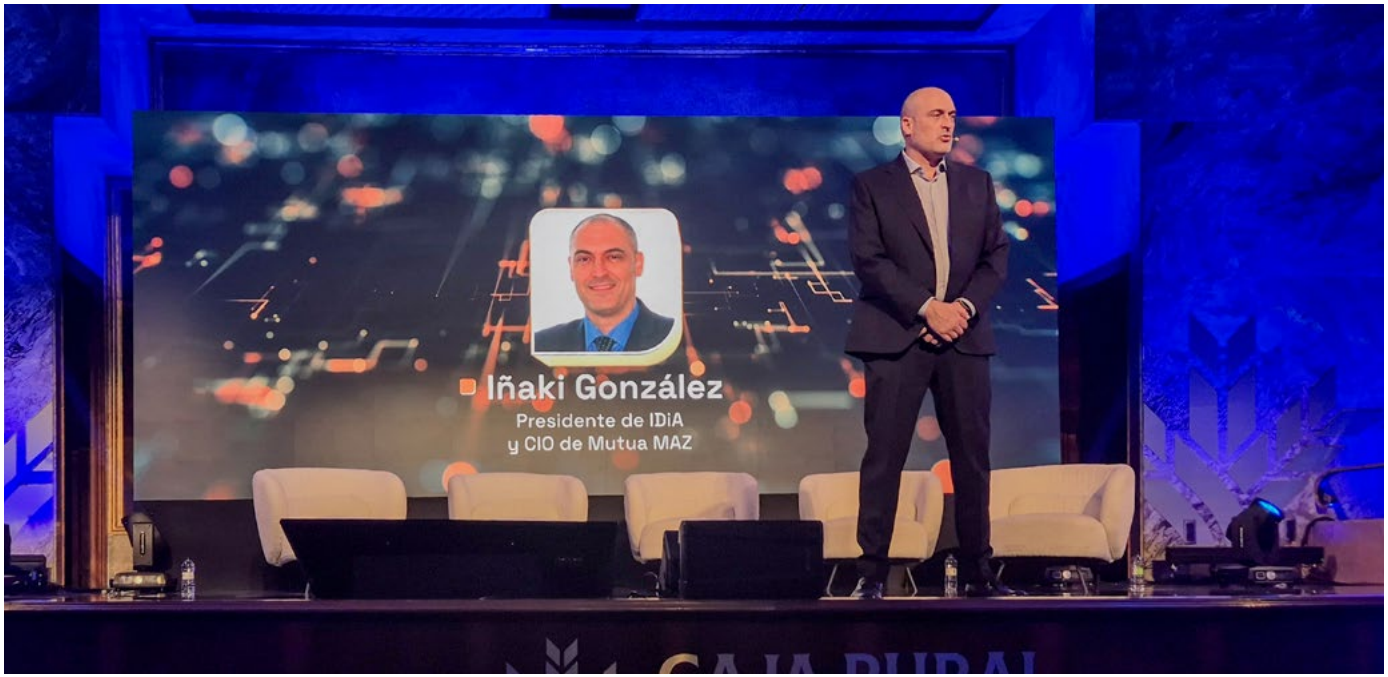
# Ciberdefensa y resiliencia digital para tu empresa



# Ciberdefensa y resiliencia digital para tu empresa

**La ciberseguridad dejó hace tiempo de ser una cuestión puramente técnica para convertirse en un reto de gestión, de negocio y de responsabilidad compartida. Esa fue la idea que articuló toda la jornada CiberIDiA 2026, organizada por el clúster IDiA en Zaragoza con el apoyo de los patrocinadores Platinum Devoteam, Fortinet, hiberus, Inetum y Trend Micro. El encuentro reunió a responsables de tecnología, ciberseguridad y dirección con un objetivo claro: hablar de ciberdefensa desde la realidad de las empresas, sin discursos teóricos ni mensajes prefabricados.**

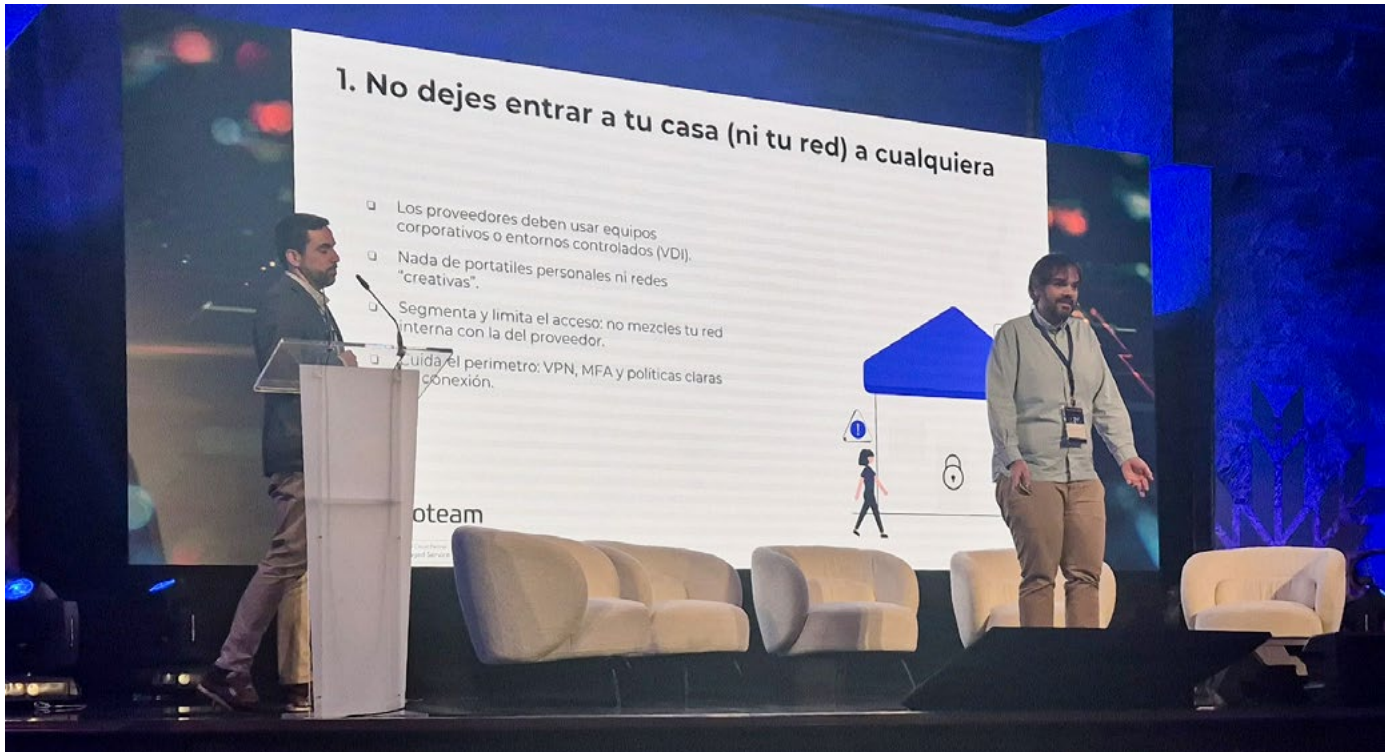



A lo largo de la jornada, celebrada el pasado 26 de enero, el encuentro propuso un recorrido desde los fundamentos técnicos —identidad, riesgo, visibilidad, detección y respuesta— hasta los retos organizativos y ejecutivos que surgen cuando un incidente deja de ser una hipótesis y pasa a afectar a la operativa, a las personas y a la toma de decisiones. Un enfoque coherente con la filosofía que IDiA defiende desde su creación: compartir experiencias reales, contrastar decisiones y aprender de lo que ya les ha ocurrido a otros.

Como defendía su presidente, Iñaki González Rico, en una entrevista concedida a Ciberseguridad TIC días antes de la celebración del evento, la ciberseguridad no puede abordarse desde compartimentos estancos ni delegarse únicamente en el área de IT. Requiere planificación, gobernanza y una implicación real de la dirección, especialmente en un contexto marcado por la profesionalización del cibercrimen, la presión regulatoria y la adopción acelerada de tecnologías como la inteligencia artificial.

Con esta premisa, CiberIDiA 2026 se estructuró en dos grandes bloques. La sesión de la mañana se centró en los pilares técnicos de la ciberdefensa en profundidad, mientras que la tarde trasladó el foco al ámbito ejecutivo, abordando la gestión de crisis y la toma de decisiones cuando un incidente deja de ser un escenario teórico.

El mensaje transversal que dejó la jornada fue claro: no existe una ciberseguridad perfecta, pero sí organizaciones mejor preparadas que otras.




## La identidad se consolida como el nuevo perímetro en entornos cloud y distribuidos

**Ponencia**

**Protección: identidad en el punto de mira**

En un entorno marcado por el trabajo remoto y la adopción acelerada del cloud, Álvaro Moreno, Cybersecurity Sales Director, y Daniel López, Google Cloud Security Strategy Lead, ambos de Devoteam, situaron la identidad como el nuevo perímetro de la ciberseguridad.

Independientemente de la ubicación del usuario o del recurso, “ya no se puede asumir confianza

por defecto; cada acceso debe verificarse", señalaron ambos, indicando que el enfoque Zero Trust se consolida como referencia. Garantizar en la nube el mismo nivel de protección que en entornos on-premise pasa, explicaron, por contar con visibilidad y contexto, apoyándose en marcos como CNAPP para analizar comportamientos y aplicar controles coherentes en infraestructuras IaaS.

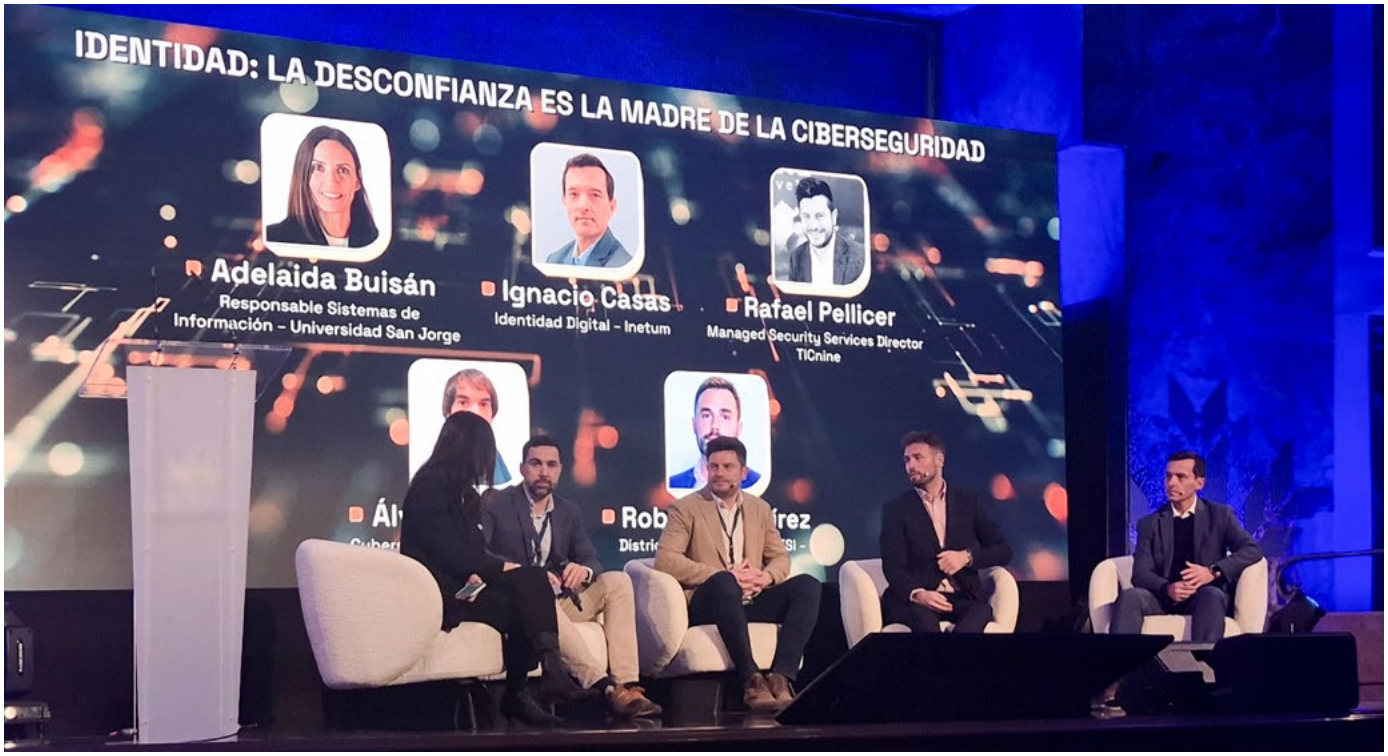
La ponencia puso especial énfasis en la necesidad de unificar la gestión de la identidad en entornos cada vez más heterogéneos. Tecnologías como IAM, PAM, ZTNA, CASB o Active Directory deben integrarse bajo una visión común que permita visualizar accesos, detectar anomalías y priorizar riesgos. En este punto, subrayaron el papel del SOC como elemento integrador, apoyado en metodologías estándar y marcos como MITRE. "En la práctica, entre el 70 % y el 80 % de los problemas de seguridad están directamente relacionados con la identidad", apuntaron.

Desde una perspectiva práctica, insistieron en el control de accesos de terceros, la segmentación de redes, el uso de entornos corporativos, la autenticación multifactor y políticas claras de conexión. Como principales barreras, señalaron la falta de liderazgo interno, visibilidad y capacidades técnicas, recomendando avanzar por fases y con objetivos realistas. Como mirada al futuro, apuntaron a la seguridad en el navegador como una de las líneas clave en el control de identidad.

**Mesa redonda**

## Identidad: la desconfianza es la madre de la ciberseguridad

La mesa dedicada a la identidad partió de una premisa compartida: el perímetro tradicional ha dejado de existir y la identidad se ha convertido en el principal punto de control —y de ataque— en los entornos digitales actuales. Moderado por Adelaida Buisán, responsable de Sistemas



El riesgo digital se ha convertido en un factor estratégico para la toma de decisiones


de Información de la Universidad San Jorge, el debate abordó la evolución tecnológica y los retos organizativos y regulatorios asociados a la gestión de identidades.

Ignacio Casas, responsable de Identidad Digital en Inetum, abrió la conversación con una reflexión sobre la identidad digital como elemento de confianza social, apoyándose en la evolución del DNI electrónico hacia el entorno móvil. Este avance permite trasladar al mundo digital "el mismo nivel de confianza que históricamente se ha depositado en la identidad física", aunque requiere una adopción progresiva y una adecuada protección del usuario.

Desde una perspectiva centrada en la amenaza, Rafael Pellicer, Managed Security Services Director en TICnine, fue contundente al afirmar que la identidad se ha convertido en el vector de ataque dominante. Explicando que "cuando un atacante obtiene una identidad válida, deja de comportarse como un elemento sospechoso", recordó que más del 80 % de los ataques actuales se basan en abuso de credenciales e ingeniería social.

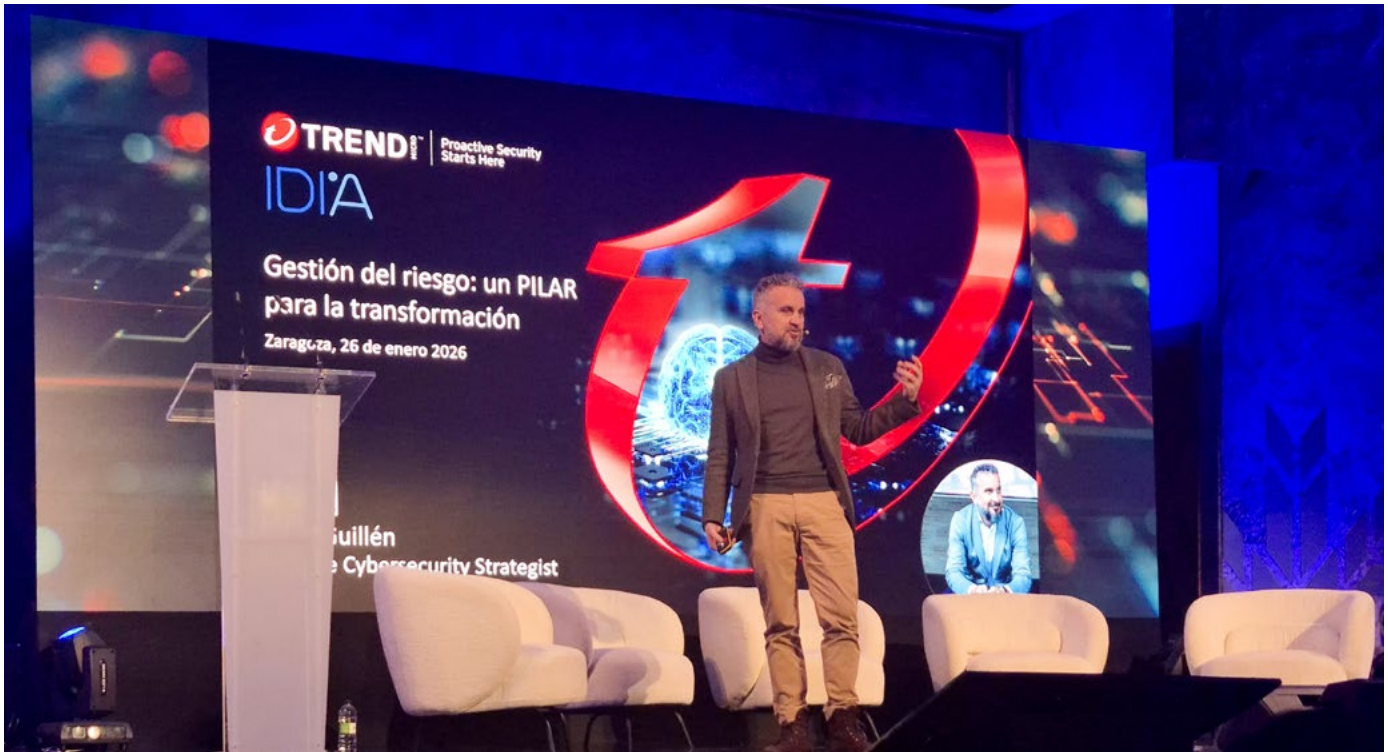
Daniel López, Google Cloud Security Strategy Lead de Devoteam volvió a incidir en la necesidad de identificar primero los activos críticos del negocio antes de desplegar tecnología. "La seguridad son salvaguardas sobre los activos reales de nuestros clientes", apuntó, defendiendo el papel del integrador como socio estratégico.

Por su parte, Roberto Ramírez, District Sales Manager – FSI de Palo Alto, amplió el foco al papel de las identidades no humanas y al navegador como nueva capa de control. "Hoy gran parte de la identidad, las credenciales y la ingeniería social pasan por el navegador", señaló.

El consenso fue claro: gestionar la identidad no es sólo un reto tecnológico, sino un equilibrio constante entre seguridad y productividad.

**Ponencia**

## Gestión del riesgo: un pilar para la transformación




Para Raúl Guillén, responsable de Cybersecurity Strategies en Trend Micro, la gestión del riesgo se ha convertido en el verdadero eje de la ciberseguridad y en un factor determinante para la transformación de las organizaciones, en un contexto marcado por la inestabilidad geopolítica, la presión regulatoria y la adopción masiva de la inteligencia artificial.

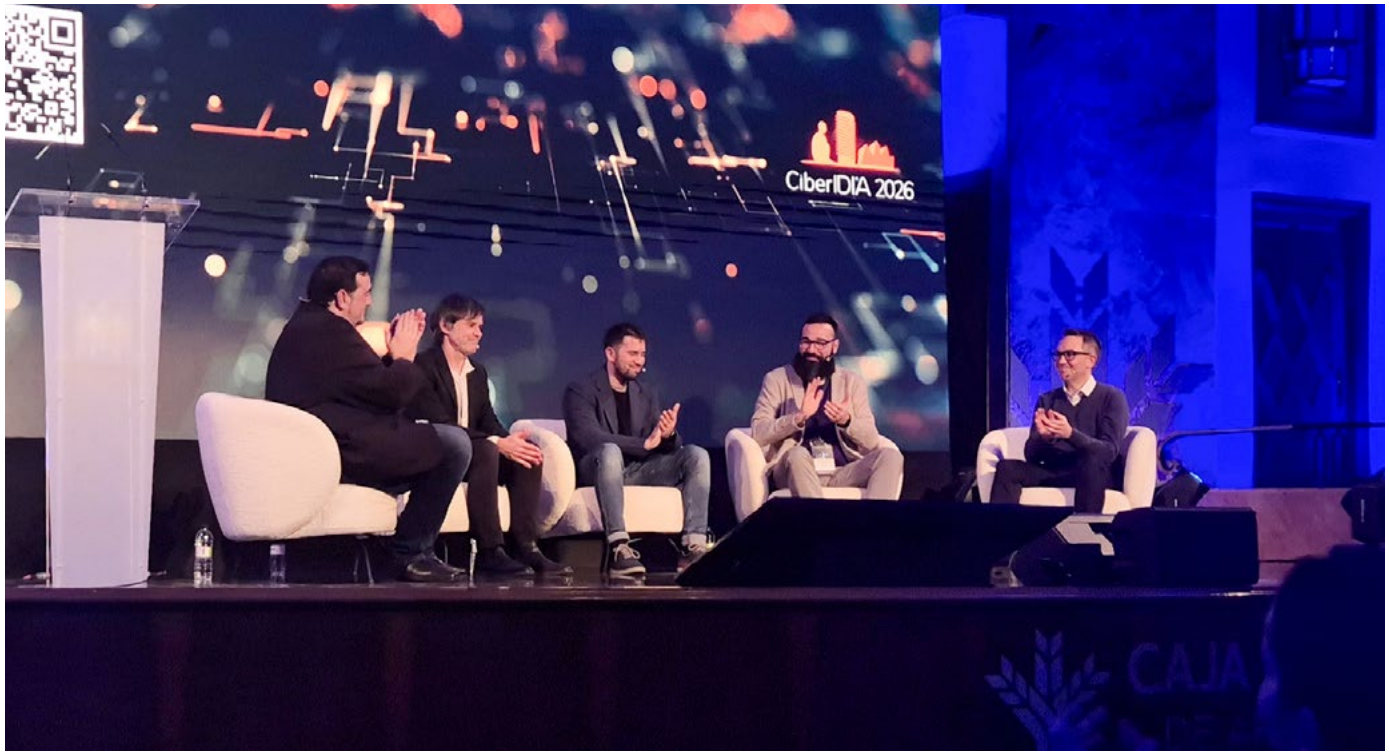
Los ciberataques, explicó, ya no persiguen únicamente objetivos económicos. “Cada vez vemos más ataques que no sólo buscan dinero, sino desestabilizar, hacer daño o responder a posicionamientos ideológicos o geopolíticos”. Este cambio, unido a la profesionalización del cibercrimen, ha dado lugar a grupos organizados “como auténticas multinacionales”, con un uso intensivo de la IA para ganar eficiencia y escala.

Este escenario amplía de forma notable la superficie de riesgo, especialmente en sectores como la sanidad o los entornos OT, y pone el foco en la cadena de suministro. “El eslabón más fácil de atacar sigue siendo la cadena de suministro que, al mismo tiempo, es uno de los más difíciles de gestionar”, afirmó, en línea con normativas como DORA o NIS2.

Más allá de la tecnología, Guillén defendió un cambio de enfoque al asegurar que tenemos que ser capaces de medir el impacto de la tecnología en el negocio, “y eso se hace con KPIs e indicadores de negocio”, recalcó, apostando por un rol más estratégico de la función de seguridad. Como cierre, lanzó un mensaje claro: “Las compañías que gestionen mejor el riesgo digital competirán mejor que sus competidores”.

**Mesa redonda**

## Si no lo veo, no lo protejo... y si lo veo, ¿qué hago?




La visibilidad del riesgo fue el eje de una mesa que giró en torno a un dilema cada vez más común en las organizaciones: no basta con saber qué activos existen, sino que es imprescindible entender qué hacer con esa información y cómo convertirla en decisiones útiles para el negocio. Moderada por Francisco Javier Fabra Caro, vicerrector de Estrategia Digital e IA de la Universidad de Zaragoza, la conversación puso el foco en la distancia que aún existe entre dato, análisis y acción.

Julián Sánchez, Cybersecurity Specialist en EDSI, abrió el debate con una advertencia directa: muchas organizaciones viven atrapadas entre la falta de visibilidad real y el exceso de información. “O estás sufriendo ya una brecha o la vas a sufrir”, afirmó, subrayando la necesidad de identificar de forma continua activos, riesgos y prioridades, y de asumir la ciberseguridad como un proceso permanente.

Desde una óptica más tecnológica, Daniel Justicia, Sales Engineer en Trend Micro, defendió la evolución hacia modelos de gestión de la exposición. La clave, explicó, no está únicamente en detectar amenazas, sino en contextualizarlas. Señaló que la defensa tiene que ser proactiva y destacó el papel de la automatización y la inteligencia artificial para priorizar riesgos en función de su impacto real.

Pablo Ballarín, fundador de Balusian, trasladó el debate al terreno del negocio, recordando que la visibilidad aporta valor cuando se traduce en las preguntas adecuadas. “No se trata sólo de detectar un problema, sino de entender qué ocurre cuando algo no funciona como debería”, afirmó, insistiendo en la conexión entre riesgo técnico e impacto económico.

Por su parte, Néstor Salceda, CEO de Safetybits,

puso el foco en la continuidad del negocio. “Tenemos que ser capaces de ver cómo un problema técnico acaba impactando en la operación”, explicó, reclamando modelos que prioricen procesos críticos y no únicamente activos individuales.

La mesa concluyó con un mensaje compartido: ver no es suficiente. La ciberseguridad madura empieza cuando la visibilidad se convierte en criterio para decidir y actuar con rapidez.

## Ponencia

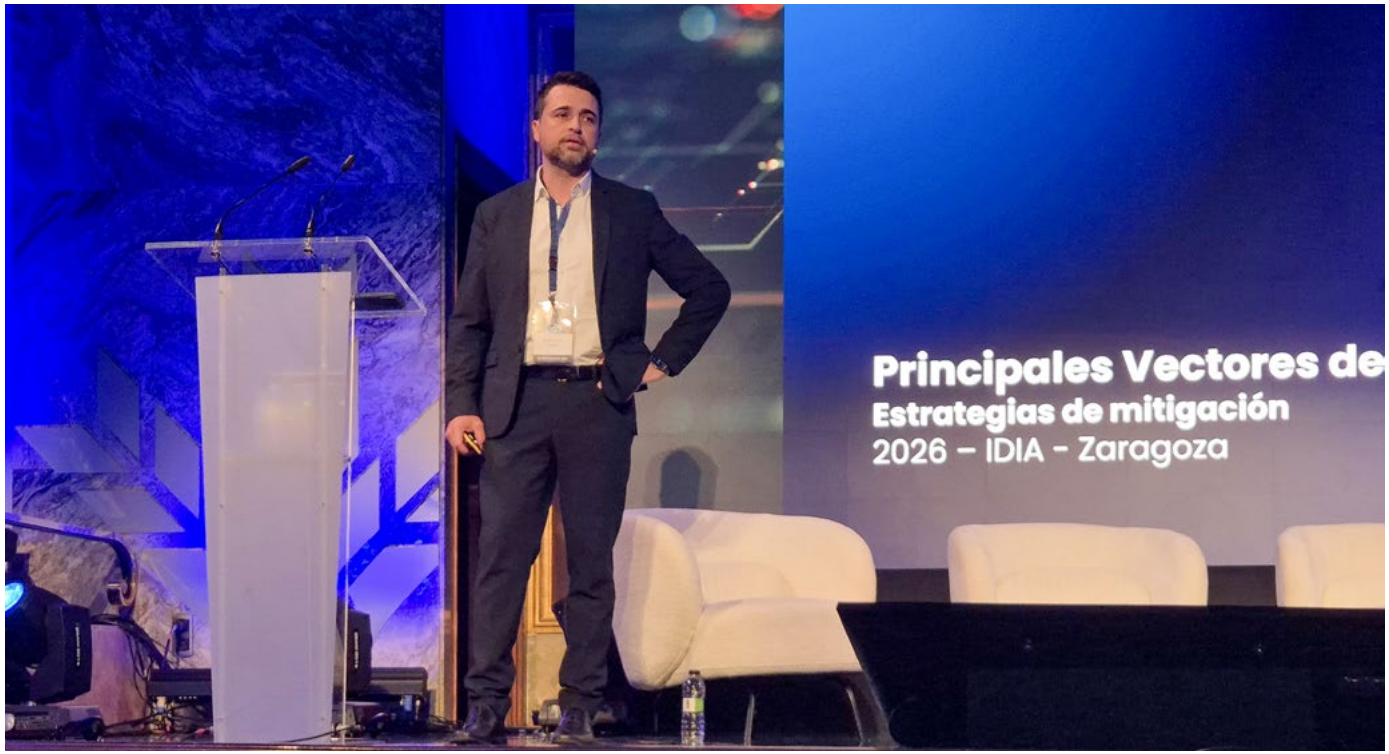
### Vectores principales de ataque

Cuando una organización presta servicios e infraestructuras críticas en más de 45 países, los vectores de ataque dejan de ser teóricos. Desde esa experiencia habló Rubén Mora, CISO global de SEIDOR, quien abordó los principales riesgos desde una perspectiva eminentemente práctica. “Somos ese backoffice que no se ve, pero que está en la trinchera”, explicó al inicio.

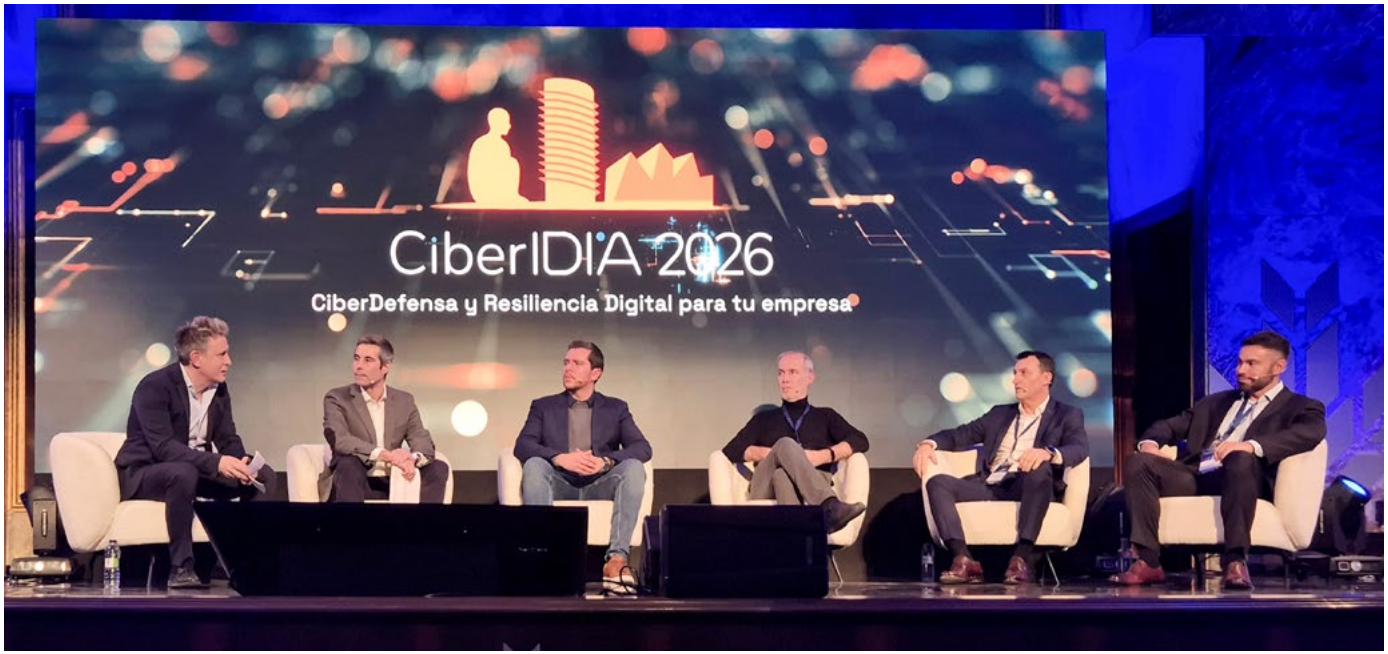
El contexto actual, recordó, es especialmente exigente: crecimiento constante de los intentos de explotación, millones de credenciales robadas y un tiempo medio de apenas 5,4 días entre la publicación de una vulnerabilidad y su explotación. En este escenario, los atacantes priorizan rapidez e impacto, lo que obliga a revisar de forma continua las prioridades defensivas.

Entre los vectores más relevantes situó la ingeniería social, claramente reforzada por el uso de inteligencia artificial. “Hoy es trivial suplantar una voz o una identidad”, alertó, recordando la facilidad para replicar la imagen o la voz de un directivo a partir de contenido público. Este tipo de ataques exige nuevos protocolos, verificación multicanal y formación continua.

El compromiso de identidades apareció como otro foco crítico. Robo de credenciales, fatiga del MFA o abuso de privilegios siguen siendo habituales, reforzando principios como el mínimo privilegio y la verificación continua.



También destacó la explotación de vulnerabilidades, especialmente en sistemas expuestos a Internet. “No es razonable parchear una vulnerabilidad crítica más allá de 72 horas si sabemos que ya está siendo explotada”, afirmó. Como cierre, recordó que muchas amenazas son evitables: “Una buena higiene, segmentación y control de identidades puede reducir hasta un 60 % de los ataques”.




### Mesa redonda

## Vigilar, detectar y responder: el corazón de la ciberseguridad

La mesa dedicada a vigilancia, detección y respuesta dejó una idea clara: la ciberseguridad ya no se decide en la prevención, sino en la capacidad real de reaccionar cuando algo ocurre. El debate, moderado por Enrique Martínez, CISO de SAICA, y José Ángel Montolio, Director IT Infraestructuras y Operaciones en SESE, reunió a fabricantes, proveedores de servicios gestionados y expertos en respuesta a incidentes, poniendo el foco en la profesionalización del adversario y en la necesidad de alinear tecnología, procesos y personas.

Acacio Martín, vicepresidente de Fortinet Iberia, abrió la conversación señalando que la complejidad actual obliga a replantear los modelos clásicos de defensa. “Cuando ocurre un ataque, la pregunta no debe centrarse únicamente en qué ha pasado, sino qué estaba ocurriendo meses antes”, apuntó, insistiendo en la importancia de contar con planes de respuesta y simulación bien definidos.

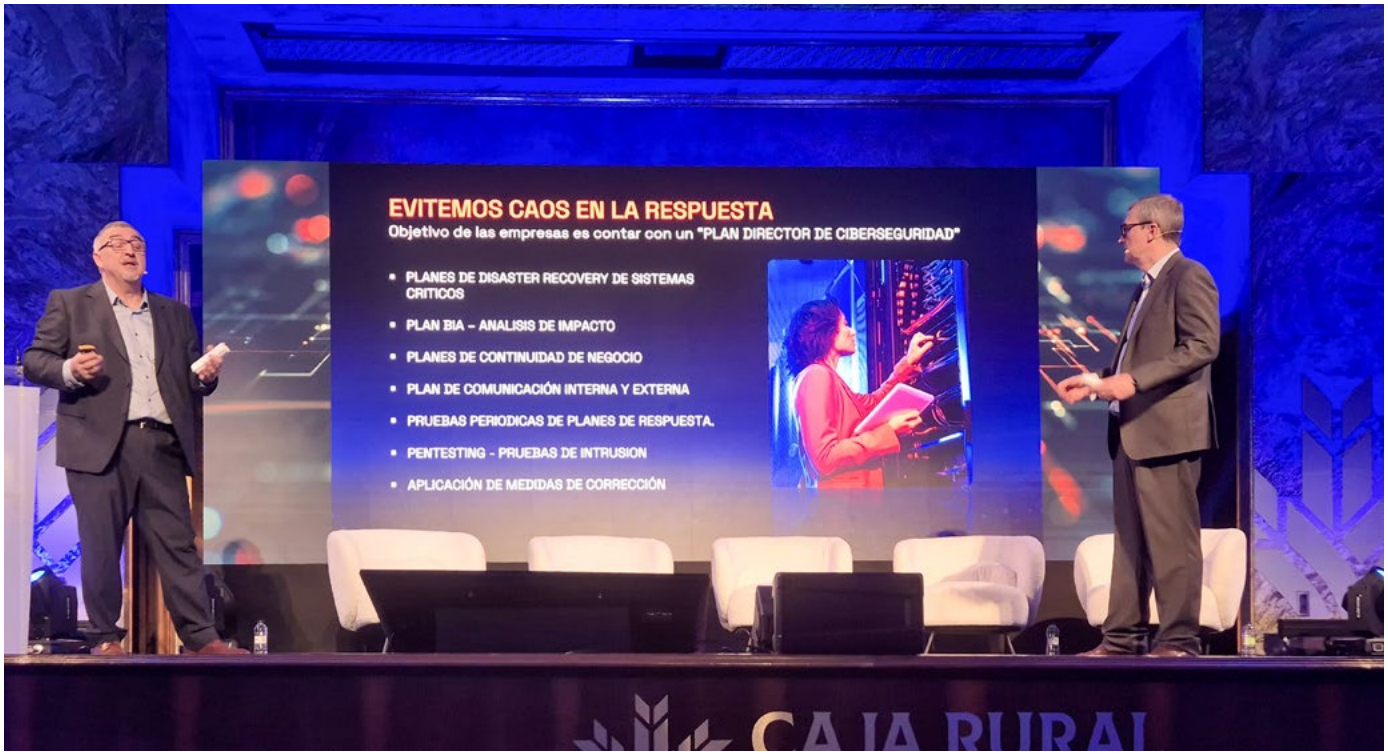
Desde la perspectiva ofensiva, Julián Delgado, Head of Offensive Security & MDR en Factum, fue contundente: “Si el cibercrimen fuera un país, sería la tercera potencia mundial”. En este contexto, advirtió de que los modelos basados únicamente en alertas ya no funcionan frente a campañas estructuradas que suelen arrancar con credenciales comprometidas.

Antonio Sanz, Head of DFIR en S2 Grupo, puso el acento en el tiempo de reacción. “Hemos pasado de semanas a horas; en algunos casos, a

tres horas", explicó, alertando de que muchas organizaciones no saben cómo reaccionar cuando sufren un incidente.

Por su parte, Joseph Michell, Managing Director Cyber Security and Network en SEIDOR, insistió en que la diferencia no la marcan las herramientas. "Puedes tener un SOC con la mejor tecnología, pero si no sabes quién decide a las tres de la mañana qué hacer, no sirve de nada", señaló.

El debate dejó claro que vigilar, detectar y responder es un ejercicio continuo de preparación, donde la rapidez y la claridad en la toma de decisiones marcan la diferencia.




**Ponencia**

## Pilares fundamentales de la ciberseguridad para cualquier empresa

Aterrizar la ciberseguridad en lo esencial fue el objetivo de la ponencia conjunta de Javier Ramos, CISO de Grupo Pikolín, y Rafael Fueris, CISO de Mutua MAZ. Ambos coincidieron en que la protección digital no puede entenderse como un problema exclusivo del área de IT, sino como una cuestión transversal que afecta a toda la organización.

"El ciberataque no sólo impacta en sistemas; afecta a procesos financieros, operaciones y reputación", subrayó Rafael Fueris, insistiendo en la necesidad de implicar a todas las áreas. En la misma línea, Javier Ramos advirtió de un error recurrente: "Pensar que esto sólo le pasa a las grandes compañías es un error", recordando que muchos ataques son oportunistas y afectan especialmente a organizaciones con menor preparación.

La gestión del riesgo fue uno de los pilares centrales de la intervención, entendida como una herramienta práctica para tomar decisiones. "El riesgo cero no existe y acercarse a él es carísimo; lo importante es saber qué tenemos y qué estamos dispuestos a aceptar", explicó Fueris. El factor humano ocupó otro lugar

> El riesgo digital se ha convertido en un factor estratégico para la toma de decisiones

clave. Para Ramos, la concienciación no puede ser puntual: “La mejor defensa frente a muchos ataques es que la gente sepa qué tiene que mirar y cuándo avisar”.

La identidad y la protección del dato completaron los mensajes esenciales. Ambos coincidieron en que credenciales débiles siguen estando detrás de muchos incidentes y que medidas básicas marcan una diferencia real. Ramos fue especialmente claro al hablar de copias de seguridad: “No tienes copias hasta que las pruebas y sabes que puedes restaurar”.

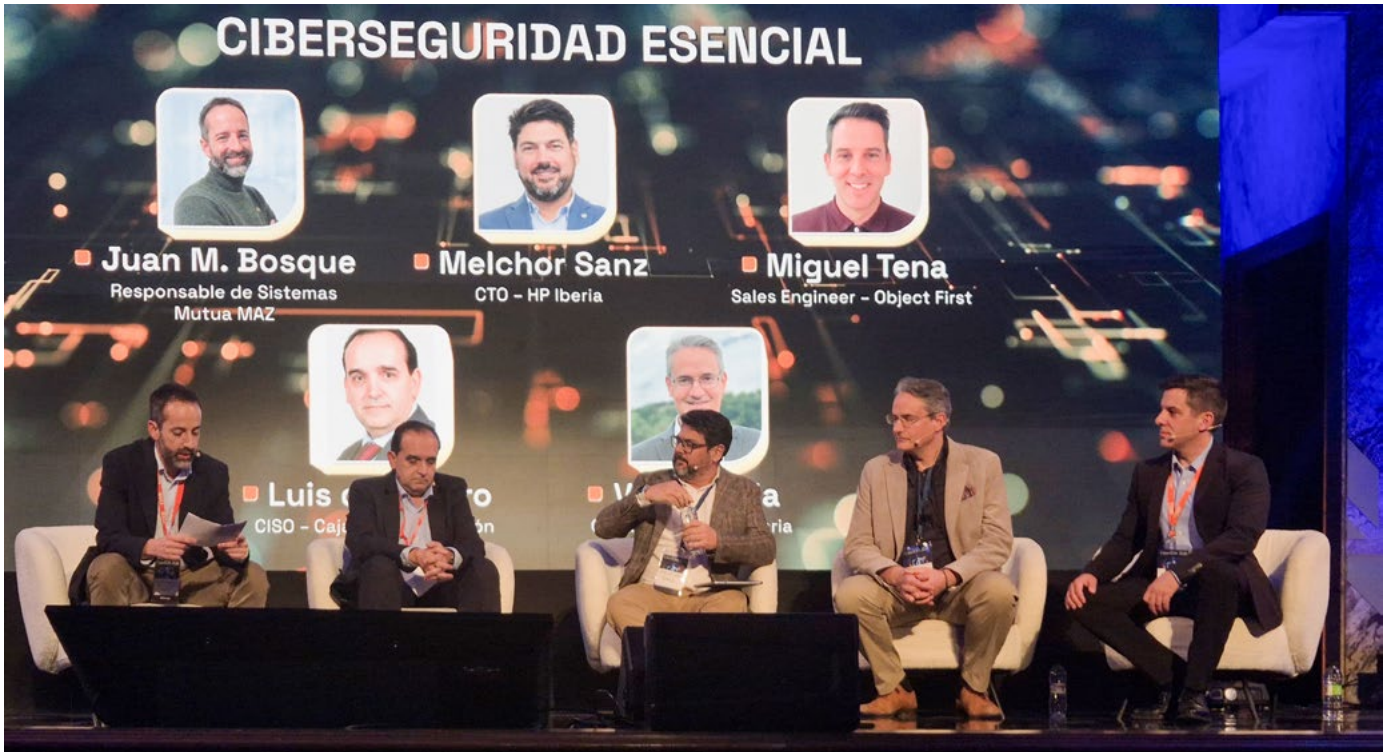
El cierre fue compartido: la ciberseguridad es un camino progresivo. “Se trata de empezar, tener un plan e ir avanzando paso a paso”, concluyó Ramos.

**Mesa redonda**

## Ciberseguridad esencial: lo imprescindible para proteger el negocio

La mesa dedicada a la ciberseguridad esencial abordó una pregunta directa: qué es realmente imprescindible para proteger y recuperar el negocio ante un incidente, especialmente en un contexto de recursos limitados y creciente presión regulatoria. Moderada por Juan M. Bosque, responsable de Sistemas de Mutua MAZ, la conversación combinó visiones tecnológicas y de negocio.

Miguel Tena, Sales Engineer en Object First, defendió las copias de seguridad como última línea de defensa frente al ransomware. La inmutabilidad, explicó, debe ser un requisito básico, no opcional, al garantizar que las copias “no puedan ser modificadas, cifradas ni borradas”,



incluso si el entorno principal se ve comprometido. Eso sí, recordó que únicamente aportan valor si se prueban y validan de forma periódica.

Desde la perspectiva del endpoint, Vicenç Vila, Channel Manager Iberia de Bitdefender, alertó contra la falsa sensación de seguridad. Muchas organizaciones siguen pensando que “no les va a pasar”, cuando los ataques actuales son generalistas y oportunistas. En este contexto, defendió combinar prevención, detección y respuesta, apoyándose en inteligencia artificial y en servicios gestionados.

Melchor Sanz, CTO de HP Iberia, introdujo la seguridad del dispositivo y la cadena de suministro como un elemento a menudo infravalorado. El endpoint, recordó, actúa como puerta de entrada al resto de la infraestructura, por lo que asegurar el hardware desde su fabricación resulta crítico.

La visión del cliente llegó de la mano de Luis de Castro, CISO de Caja Rural de Aragón, quien subrayó la importancia de la gobernanza, la gestión del riesgo y la implicación de la dirección en marcos como DORA o NIS2.

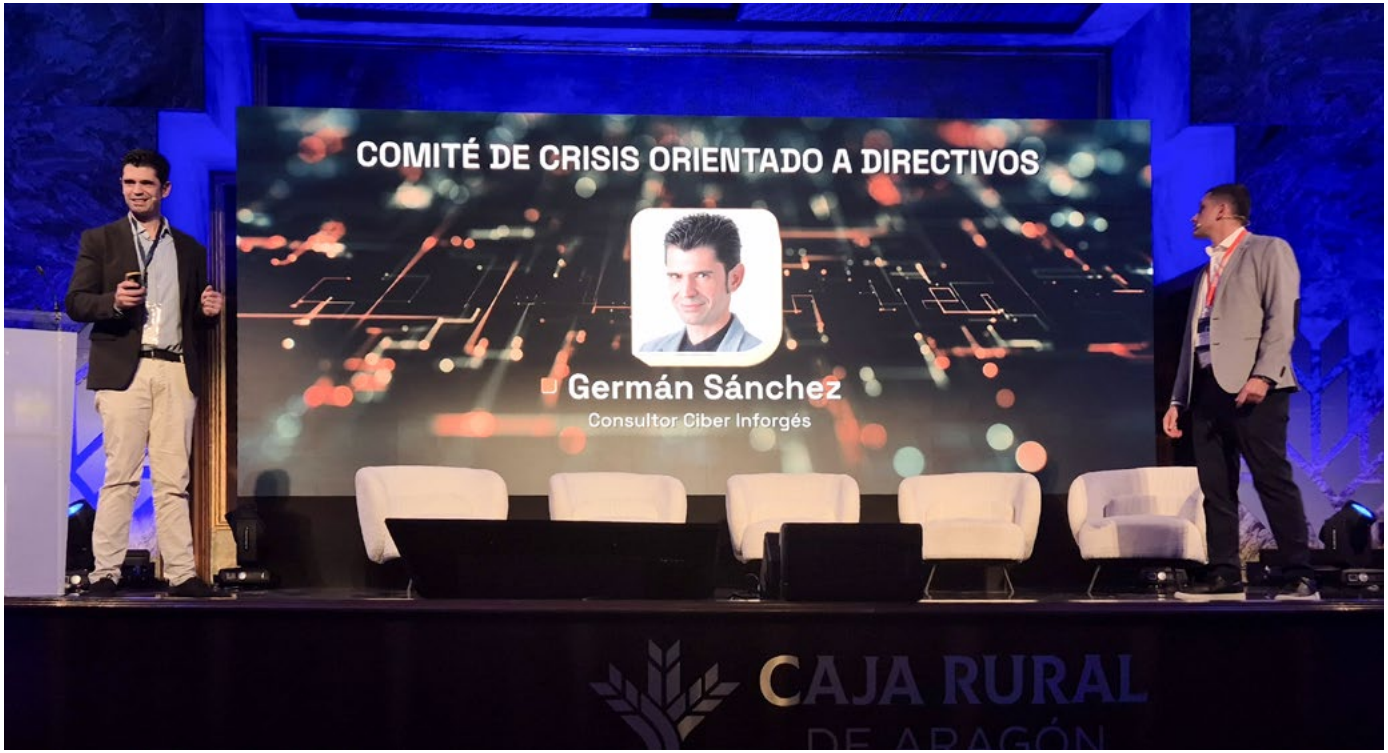
**Ponencia**

## Comité de crisis orientado a directivos

Prepararse para el peor escenario fue el eje de la intervención de Germán Sánchez, consultor de ciberseguridad en Inforges, quien defendió que el ciberataque ya no es una hipótesis, sino un escenario operativo con el que las organizaciones deben convivir.

“Hoy no hablamos de si nos van a atacar o no; hablamos de cuándo”, afirmó, recordando que los intentos de acceso y explotación son constantes. A esta realidad se suma la profesionalización del cibercrimen y el impacto de la inteligencia artificial. “La IA ha hecho que todo vaya mucho más rápido, tanto del lado del atacante como del defensor”, explicó.

La ampliación de la superficie de ataque y la dependencia de terceros ocuparon un lugar cen-



tral. “Muchas veces no entran directamente a la empresa objetivo, sino a través de un proveedor con una postura de seguridad más débil”, advirtió, subrayando el papel crítico de la cadena de suministro.

Sánchez describió el ransomware como un proceso prolongado. “El cifrado es solo la parte final; cuando llega, el atacante lleva tiempo dentro”, alertó. Las consecuencias, añadió, trascienden lo técnico y pueden afectar gravemente a la viabilidad del negocio.

Asegurando que la improvisación no es una opción, recordó que el día del incidente “no es el momento de decidir quién hace qué”, por lo que dejó claro que debe apostarse por comités de crisis entrenados y simulacros periódicos. “Todo se puede entrenar”, concluyó.

> La visibilidad sólo aporta valor cuando se traduce en decisiones accionables

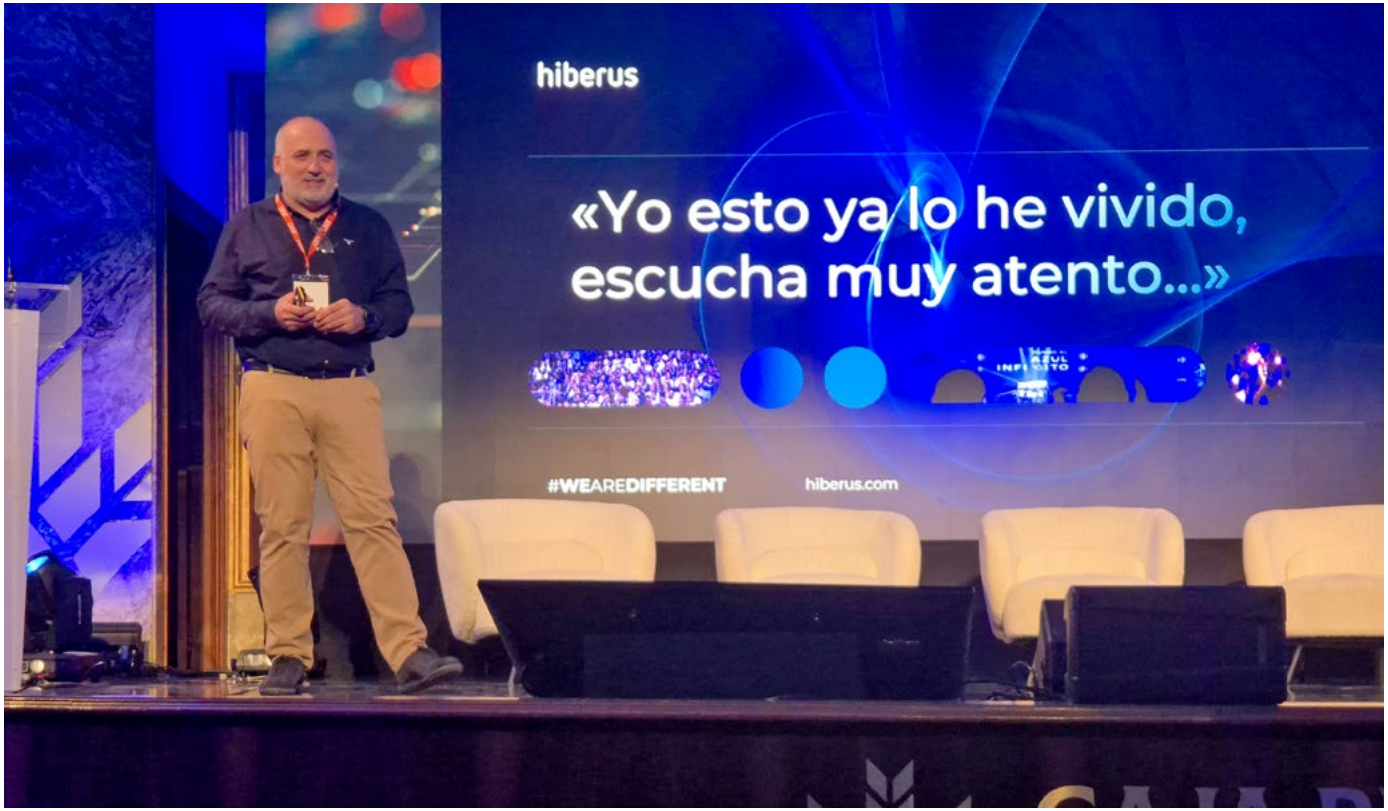
**Ponencia**

## Yo esto ya lo he vivido, escucha muy atento...

Desde la experiencia directa en la gestión de incidentes graves, Eduardo Gistau, Global Head of Cybersecurity en hiberus, quiso explicar qué ocurre cuando una empresa se detiene de verdad y cómo se toman decisiones bajo presión.

“Quiero contar esto para humanos, para que se entienda qué se siente cuando alguien entra en tu casa y te para la actividad”, afirmó al inicio. Los incidentes, explicó, nunca llegan en un momento cómodo y suelen producirse con recursos mínimos. “Te encuentras una empresa vacía, parada, con tres o cuatro personas de IT que lo están pasando realmente mal”.

En las primeras horas, cuando no hay visibilidad



> La seguridad que no se mantiene en el tiempo acaba fallando

ni sistemas operativos, lo prioritario no es la tecnología, sino el orden. “Lo primero que pedimos es una sala y una pizarra”, relató, para construir un inventario básico y responder a la pregunta clave: “¿Tienes con qué sobrevivir?”.

Uno de los mensajes más relevantes fue la necesidad de traducir el incidente a impacto de negocio. “Hay que preguntar cuánto dinero se deja de facturar cada día”, afirmó, porque poner cifras sobre la mesa ayuda a tomar decisiones realistas.

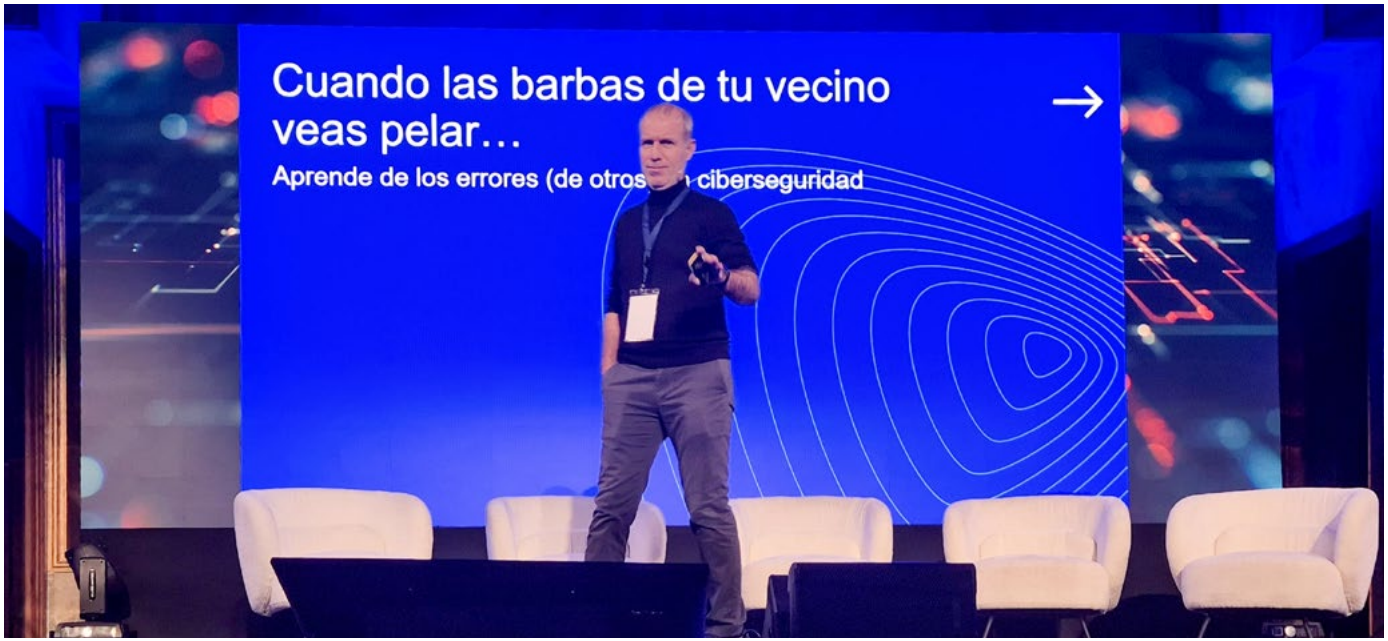
Eduardo Gistau también puso el foco en la gestión del relato. “La sociedad no te juzga por tener un incidente, te juzga por mentir o por no saber gestionarlo”, advirtió. Como cierre, recordó que un incidente marca un antes y un después: “Esto hay que recordarlo, porque la memoria es corta”.

**Ponencia**

## Cuando las barbas de tu vecino veas pelar... Aprende de los errores (de otros) en ciberseguridad

Los incidentes graves rara vez responden a un único fallo, defendió Antonio Sanz, Head of DFIR en S2 Grupo, durante su ponencia. “Un incidente nunca es una cosa; es una cadena de cosas que se van acumulando”, explicó, insistiendo en la importancia de aprender de experiencias reales. “Da igual el tamaño o el sector: si tienes información, procesos o clientes, hay alguien que va a quererlo”, recordaba el directivo, quien, a lo largo de su intervención, compartió patrones recurrentes: reutilización de credenciales, ausencia de doble factor, entornos mal segmentados o proyectos de seguridad que se quedan a medias. “Muchas veces no hablamos de ataques sofisticados, sino de cosas básicas que se dejan pendientes”, aseguró.

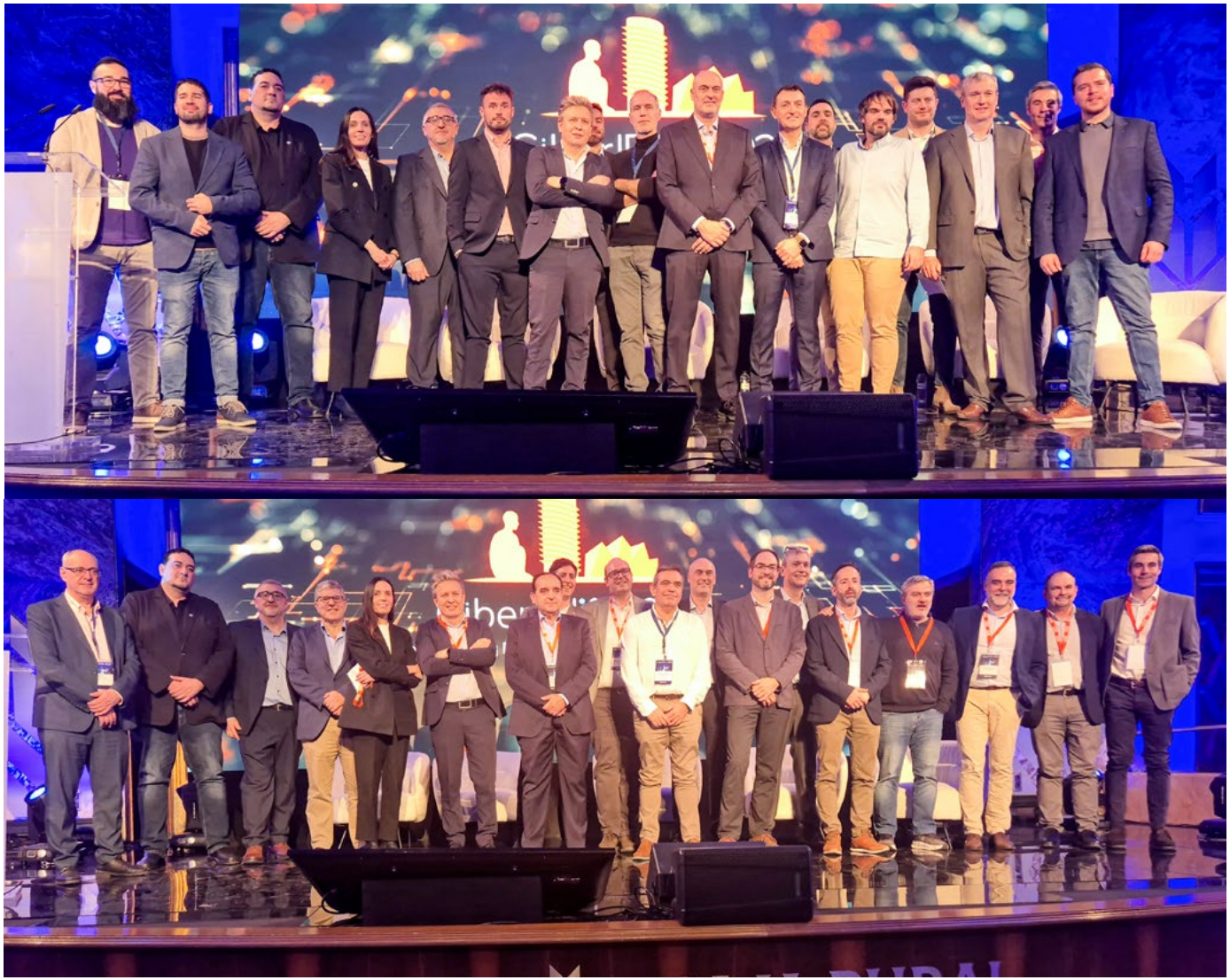
Otro de los mensajes clave fue la necesidad de sostener las medidas de seguridad en el



tiempo. “La seguridad no es algo que haces una vez y ya está; es algo que tienes que sostener”, afirmó, advirtiendo de que cuando se relajan los controles “el atacante suele volver por el mismo sitio”.

La identidad volvió a aparecer como foco crítico. “Si no gestionas bien la identidad, te van a pasar cosas”, alertó. También puso el foco en terceros y cadena de suministro: “Cuando tú tienes un problema, también lo tienen tus proveedores y tus clientes”.

En el plano tecnológico fue claro: “Tener un EDR sin que nadie mire las alertas es como no tener nada”. El cierre resumió su mensaje: no se trata de ser perfectos, sino de aprender.



## Conclusiones y cierre

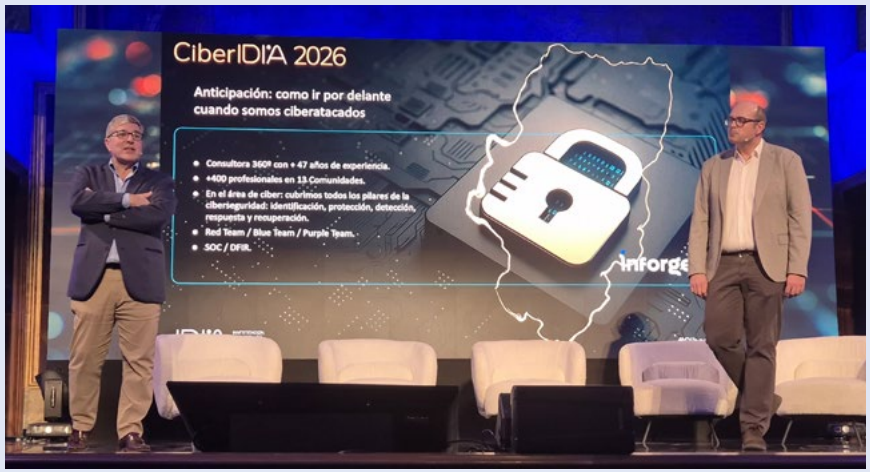
### De la tecnología a la responsabilidad compartida

En el cierre de la jornada, Iñaki González Rico, presidente de IDiA y CIO de Mutua MAZ, resumió el espíritu del encuentro con un mensaje claro: la ciberseguridad ya no puede abordarse como un asunto exclusivamente técnico, sino como una responsabilidad transversal que afecta a toda la organización.

“Hay una serie de dimensiones que hay que trabajar sí o sí, tengas muchos recursos o muy pocos”, señaló, mencionando la gestión del

## IDiA: una comunidad para avanzar juntos en ciberseguridad

**El clúster IDiA nació como un espacio de confianza entre profesionales, orientado a compartir experiencias reales y aprendizajes prácticos en torno a la tecnología y la ciberseguridad. Durante su intervención, Antón Borraz, CIO de Grupo Lobe, subrayó que el valor diferencial del clúster está en las personas: "Aquí podemos hablar con libertad de los problemas reales, aprender de lo que a otros ya les ha pasado y avanzar sin miedo a equivocarnos".**




**En la misma línea, Ignacio Brieba, CIO de Grupo Pikolín, destacó la importancia de la colaboración frente a retos cada vez más complejos. "La tecnología y la ciberseguridad ya no se pueden abordar en solitario; compartir experiencias nos permite tomar mejores decisiones y avanzar más rápido".**

**Ambos coincidieron en que este tipo de foros aceleran la madurez digital de las organizaciones, reducen la incertidumbre en la toma de decisiones y permiten construir una visión más realista de los riesgos y oportunidades. En un entorno marcado por el cambio constante, IDiA se consolida así como una red de apoyo entre iguales, basada en la transparencia y el aprendizaje continuo.**

riesgo, la organización básica de la seguridad, la protección del dato, la continuidad de negocio y un mínimo de gobernanza. No se trata, insistió, de aspirar a la perfección, sino de tener un plan y saber por dónde empezar.

González Rico puso especial énfasis en ampliar la mirada más allá del área de IT. "Cuando hay un incidente, IT no tiene la solución a todo", recordó, subrayando la necesidad de coordinar a todas las áreas implicadas y evitar respuestas improvisadas.

También quiso desmontar una idea recurrente: "No se trata de que el CISO o el CIO se coman el problema". La ciberseguridad, afirmó, solo funciona cuando cuenta con el respaldo real de la dirección y cuando toda la organización entiende su papel.

Como reflexión final, apeló a la concienciación y al aprendizaje continuo. "Esto no es una cuestión menor; estamos hablando de cosas muy serias", concluyó.