Regulación, IA y talento tensionan el modelo de ciberseguridad

Más de 210 profesionales, un 30 % más que el año pasado, acudieron a la quinta edición del Cybersecurity Summit que V-Valley celebró en La Granja (Segovia) que, además, como novedad, contó con un *streaming*, al que se conectaron 400 personas, que pudieron seguir el debate de manera remota. 22 fueron los fabricantes que arroparon al mayorista en esta cita cibersegura: A10 Networks, Acronis, Arexdata, Armis, Backbox, Check Point Software, Cloudflare, Elastic, Entrust, Forescout, Hornetsecurity, Iberlayer, Ironchip, Kaspersky, Netwitness, Opentext, Qualys, Sectigo, Sonicwall, Trellix, Veeam y WatchGuard. También estuvieron representadas Innoveyxa, la nueva división de servicios del Grupo Esprinet; y Esprifinance.

Rosalía Arroyo

El evento contó con un debate, en el que participaron diferentes expertos, y también con los tradicionales "*one to one*" que reúnen a los fabricantes con los profesionales de los *partners*, para permitir la detección de algunas oportunidades de negocio y que los clientes conozcan nuevas tecnologías.

El área de ciberseguridad en V-Valley ya cuenta con ocho años de recorrido y un equipo conformado por 80 personas. "Nos hemos hecho con un hueco destacado en el mercado", valoró Alberto López, *country manager* del área de ciberseguridad en el mayorista, que recordó la confianza que le concedió el Grupo Esprinet para dar forma a una división que mantiene un negocio creciente desde hace años. "El rol del mayorista, que tenemos muy claro, es que sea una pieza para que la cadena funcione. Tenemos que ser un facilitador del negocio". Con una cartera de fabricantes que ya supera los 40 nombres, López recordó que cada fabricante necesita algo diferente. "Somos una extensión suya".

Tras la compra de Lidera Networks, la trayectoria del mayorista se ha fortalecido. "El área de la ciberseguridad es más grande que nunca". López aseguró que son el único mayorista que opera en todos los mercados: pymes, *commercial*, *enterprise* y los servicios gestionados (MSP y MSSP). "Contamos con una cobertura completa, con una aproximación diferente en cada uno de los mercados".

Fortaleza del grupo

El Grupo Esprinet ejerce su liderazgo tecnológico en el sur de Europa (Italia, España y Portugal) y el norte de África. "Nuestras ventajas son la especialización y el conocimiento del mercado", señaló David Gasca, director de marketing y operaciones del área de ciberseguridad, que recordó la reciente inauguración de Innovexya, una división de

> "La ciberdelincuencia ha evolucionado hacia estructuras organizadas, globales y con un claro enfoque económico, lo que complica cada vez más su identificación y persecución"
>
> **(Víctor Sánchez. Policía Nacional)**

servicios profesionales que funciona de manera trasversal en Italia, España y Portugal. Incluye soluciones digitales, *retail*, *cloud* y software, ciberseguridad, servicios técnicos, logística y transporte.

López destacó la capacidad financiera del grupo. "Muchos proyectos, sin una cobertura financiera, no hubieran podido salir adelante", destacó. "A pesar de que nuestro tamaño es menor que el de algunos grupos internacionales, somos muy flexibles".

La fortaleza de la ciberseguridad

La ciberseguridad vive un momento de aceleración que está desbordando muchos de los modelos tradicionales. Más ataques, más automatización, más inteligencia artificial... pero también los mismos errores de base que siguen abriendo la puerta a los incidentes. Esa fue una de las ideas que anidó en el debate, conducido por el periodista José Yélamo, en el que analizó cómo está cambiando el escenario y qué implica realmente para las organizaciones.

A lo largo de la jornada se dibujó un mapa

> "El problema del talento no es solo de escasez, sino de enfoque: es necesario abrir el perfil y trabajar la retención"
>
> **(Eduvigis Ortiz. Women4Cyber Spain)**

> "En entornos industriales, la prioridad no es la confidencialidad del dato, sino garantizar la continuidad de la operación"
>
> **(Alejandro Villar. TRC)**

bastante completo del momento actual: desde la profesionalización del cibercrimen y la velocidad a la que evolucionan los ataques, hasta el impacto de la inteligencia artificial como nueva superficie de riesgo, pasando por la presión regulatoria, la seguridad en entornos industriales o la creciente dificultad para gestionar el talento. Todo ello con un hilo común: la complejidad no deja de crecer, pero la capacidad de respuesta de muchas organizaciones sigue anclada en modelos que ya no encajan.

> "La ciberseguridad debe entenderse como un problema de riesgo corporativo, no solo tecnológico"
>
> **(Ramsés Gallego. DXC Technology)**

Más velocidad, más actores... y los mismos fallos de siempre

La apertura del debate, centrada en el estado de las ciberamenazas, partió de una visión especialmente aterrizada. Víctor Sánchez, inspector jefe de la Policía Nacional y coordinador de C1b3rwall, explicó que la ciberdelincuencia ha evolucionado hacia estructuras organizadas, distribuidas y con un claro enfoque económico. "Han encontrado un nicho de negocio muy interesante", señaló, subrayando que la deslocalización y el uso de nuevas tecnologías dificultan cada vez más la identificación de los atacantes.

Ese crecimiento no implica necesariamente mayor sofisticación en todos los niveles. De hecho, una de las ideas más repetidas durante la sesión fue que el problema sigue estando en lo básico. Sergio Martínez, *senior country manager* para Italia e Iberia en SonicWall, lo resumió de forma directa: los errores siguen siendo los mismos y la mayoría de los ataques continúan empezando por el robo de identidad, mientras muchas intrusiones tardan meses en detectarse.

Fernando Martínez, *head of key account manager* Iberia en Hornetsecurity, reforzó esa idea poniendo el foco en el correo electrónico, donde el volumen de *malware* sigue creciendo, un 130 %, y donde el acceso a la persona continúa siendo el punto de entrada más eficaz. La inteligencia artificial, en este

contexto, no sustituye estos vectores, pero sí los amplifica, facilitando ataques más creíbles y accesibles.

Precisamente sobre ese impacto, Eusebio Nieva, director técnico de Check Point Software en Iberia, introdujo un matiz relevante: la barrera de entrada para los atacantes se está reduciendo gracias a la inteligencia artificial. "Es posible que esa profesionalización se invierta", advirtió, al permitir que perfiles menos especializados puedan lanzar ataques con herramientas cada vez más accesibles.

> "El *prompt injection* es una evolución de la ingeniería social que aprovecha sistemas no deterministas y amplía la superficie de ataque"
>
> **(Martín Vigo. Triskel Security)**

> "El reto no es solo tecnológico: muchas organizaciones carecen de estrategia y de capacidad real para operar la seguridad"
>
> **(Noé Villar. DQS)**

"Todo se acelera, pero no a la misma velocidad", decía David Baldomero, *team lead for Spain and Nordics* en Trellix, alertando de un desfase creciente entre la evolución del ataque y la capacidad de defensa. Una idea que Vicente Gozalbo, *enterprise sales account manager* Iberia de Netwitness, llevó más lejos al hablar de dinámicas cercanas al "*zero-day* en horas", lo que obliga a reforzar la visibilidad y la capacidad de reacción en tiempo real.

En ese escenario, el papel del canal se refuerza, pero también se complica. Miguel Carrero, vicepresidente mundial del ecosistema de *partners* y cuentas estratégicas en WatchGuard, defendió su papel como elemento de proximidad, especialmente para un tejido empresarial donde la pyme no puede asumir el nivel de especialización necesario.

En la misma línea, Óscar Suela, *country manager* de Iberia y UK & Ireland en Kaspersky, insistía en que el canal debe traducir la tecnología en soluciones reales para el cliente.

Desde el propio lado del *partner*, Noé Villar, CTO & CISO en DQS Consulting, apuntó

> "La resiliencia gana peso frente a la prevención como elemento clave en la estrategia de seguridad"
>
> **(Pedro Canela. V-Valley, en representación de A10)**

> "El crecimiento exponencial del dato impulsado por la IA obliga a reforzar su protección y control"
>
> **(Daniel James Kinlock. Acronis)**

que muchas organizaciones ya tienen herramientas, pero no una estrategia clara para utilizarlas. El problema no es solo tecnológico, sino de diseño y operación. Por su parte Pedro Marco, fundador y CEO de Iberlayer, añadió una variable incómoda: el cliente sigue decidiendo muchas veces por precio, tensionando el modelo y alejando la seguridad de un enfoque realmente eficaz.

Ese cambio de escala obliga también a replantear la forma de defenderse. Juan Molina, *partner solutions engineer* Iberia en Cloudflare, recordaba que ya no estamos ante un problema local, sino global: un ataque que se produce en cualquier parte del mundo puede replicarse en cuestión de minutos. Durante años, explicó, las organizaciones han construido barreras para bloquear amenazas, pero el atacante siempre encuentra nuevas formas de superarlas.

La conclusión del bloque fue clara: el entorno es más complejo, más rápido y más accesible para el atacante, pero el punto débil sigue estando en lo mismo de siempre.

IA ofensiva: nuevas puertas de entrada en un modelo que sigue sin ser determinista

El segundo bloque trasladó el foco a la inteligencia artificial como herramienta ofensiva, pero también como nuevo vector de riesgo dentro de las propias organizaciones.

Martín Vigo, *hacker, red teamer* e investigador en seguridad ofensiva y fundador de Triskel Security, aportó una visión especialmente práctica. A su juicio, el problema no es solo lo que hace la IA, sino dónde la esta-

> "Las organizaciones acumulan datos sin control, lo que aumenta su exposición y dificulta su protección"
>
> **(Alberto Tejero. Arexdata)**

mos integrando. La proliferación de asistentes, *chatbots* y sistemas conectados a datos corporativos está ampliando la superficie de ataque, muchas veces sin control claro.

El *prompt injection* se posiciona aquí como uno de los vectores más relevantes. Vigo lo describió como una evolución de la ingeniería social: no se trata de explotar una vulnerabilidad técnica, sino de engañar a un sistema para que haga algo que no debería. También rebajó el impacto de los discursos más alarmistas. La atención sobre nuevas herramientas no debería ocultar que los ataques más efectivos siguen siendo los tradicionales. La ingeniería social continúa siendo la vía más eficaz de entrada, muy por encima de los ataques más avanzados.

El debate avanzó hacia un cambio de paradigma más profundo. Eusebio Nieva explicó que la IA introduce un modelo distinto al de la seguridad tradicional: ya no se trata solo de controlar accesos, sino de gestionar sistemas que pueden ser engañados para revelar información.

Desde OpenText, Jacinto Grijalba, *cyber sales leader* en Iberia, diferenció entre vulnerabilidad e inseguridad, señalando que muchos de estos problemas no se deben a fallos técnicos clásicos, sino a cómo se diseñan los sistemas. Daniel James Kinlock, *enterprise sales manager* en Acronis, puso el foco en el crecimiento del dato y la necesidad de protegerlo, mientras que Juan Molina insistió en la importancia de una visión global y en controlar tanto el tráfico de entrada como el de salida.

> "La actitud y la capacidad de colaborar son tan importantes como el conocimiento técnico en el desarrollo del talento"
>
> **(Rocío Vaquero. Armis)**

> "La inteligencia artificial reduce la barrera de entrada para los atacantes y cambia el modelo de seguridad hacia sistemas que pueden ser engañados"
>
> **(Eusebio Nieva. Check Point Software)**

> "La defensa debe ir más allá del perímetro, incorporando también el control del tráfico de salida para mejorar la detección"
>
> **(Juan Molina. Cloudflare)**

También surgió el debate sobre hasta qué punto es posible frenar estos riesgos. Vicente Gozalvo insistió en la necesidad de visibilidad total, mientras que Noé Villar volvió a poner el acento en la realidad de la empresa media, que no siempre puede asumir estos modelos.

Desde Kaspersky, Óscar Suela planteó directamente la necesidad de un cambio cultural: la seguridad ya no puede abordarse solo con herramientas, sino que exige replantear los modelos de confianza y avanzar hacia una visión de ciberresiliencia.

El cierre lo puso José Fernando Gómez, fundador y CISO en Ironchip, con tres ideas claras: evitar el uso indiscriminado de la IA, controlar el destino de los datos y reforzar la identidad como elemento clave. Además, advirtió de que no solo los nuevos modelos presentan riesgos, sino también sistemas más tradicionales como la biometría.

El factor humano

Tras dos bloques centrados en amenazas y tecnología, el encuentro giró hacia un elemento que, en realidad, había estado presente en toda la conversación: las personas. Eduvigis Ortiz, presidenta de Women4Cyber Spain, situó el debate en una doble realidad. Por un lado, el sector sigue creciendo y generando oportunidades; por otro, el déficit de talento es real. La industria necesita miles de profesionales, pero muchas organizaciones siguen buscando perfiles muy concretos, lo que limita el acceso a ese talento. En su

opinión, es necesario abrir el foco y entender que la ciberseguridad no es solo técnica: hay espacio para perfiles muy diversos, desde ingenieros hasta periodistas, criminólogos o psicólogos.

También puso el acento en la diversidad, todavía limitada, y en la necesidad de seguir visibilizando el sector y sacarlo del nicho técnico. Pero más allá de atraer talento, el problema está en retenerlo. La fatiga y el desgaste empiezan a ser habituales en los equipos. Ortiz lo vinculó con una cuestión estructural: las organizaciones siguen priorizando la tecnología frente a la gestión del cambio. "Es más fácil comprar una herramienta que trabajar con las personas", advirtió.

> "La exigencia del sector, especialmente en entornos globales, obliga a reforzar liderazgo y trabajo en equipo"
>
> **(María Campos. Elastic)**

> "La gestión del talento depende cada vez más de la cultura de empresa y de la capacidad de cuidar a los equipos en un entorno exigente"
>
> **(Rocío Martínez. Entrust)**

Desde Entrust, Rocío Martínez, *sales manager digital security*, señaló que la salud mental empieza a ser una prioridad en las empresas, impulsada en parte por la escasez de perfiles. María Campos, *regional VP sales* en Elastic, añadió otro matiz: la exigencia del sector. En entornos globales, con compañías muy competitivas y ritmos intensos, la presión es constante. Esto obliga a reforzar el liderazgo, el trabajo en equipo y la empatía para evitar que los profesionales se quemen.

Rocío Vaquero, *partner business manager* en Armis, puso el foco en la actitud y en la importancia de detectar talento más allá del perfil técnico. La ciberseguridad, insistió, es también una cuestión de equipo, colaboración y energía. El éxito, recordó, no es individual, sino colectivo.

Desde el lado del canal, Noé Villar defendió modelos de crecimiento interno basados en perfiles júnior que evolucionan dentro de la organización, frente a la práctica habitual de

> "La visibilidad total de los activos es imprescindible para poder gestionar la seguridad en entornos complejos"
>
> **(Miguel Ángel Rodríguez. Forescout)**

> "El correo electrónico sigue siendo la principal puerta de entrada, con un volumen creciente de amenazas que la IA está ayudando a sofisticar"
>
> **(Fernando Martínez. Hornetsecurity)**

rotación constante entre empresas. En un mercado claramente tensionado por la oferta y la demanda, construir talento propio se convierte en una estrategia más sostenible.

En definitiva, no se trata únicamente de atraer más profesionales, sino de entender cómo integrarlos, desarrollarlos y mantenerlos en un entorno cada vez más exigente.

Regulación, dato y cadena de suministro

El peso de la regulación en ciberseguridad ya no es una previsión, es una realidad que está redefiniendo cómo las empresas entienden el riesgo. No solo por el volumen de normativas —NIS2, DORA, RGPD o el futuro AI Act—, sino por lo que implican: la seguridad deja de ser un asunto del área técnica para convertirse en una cuestión de negocio.

"De lo que hablamos es de riesgo corporativo", aseguraba Ramsés Gallego, *Chief Technologist Cybersecurity* en DXC Technology y presidente del capítulo de Barcelona para Isaca. Más que amenazas o herramientas, lo relevante es cuánto riesgo puede asumir una organización y cómo lo gestiona. Un cambio de enfoque que obliga a conectar la ciberseguridad con conceptos como el valor en riesgo, la continuidad de negocio o la propia estrategia empresarial.

Ese marco regulatorio, lejos de ser homogéneo, se presenta como una suma de exigencias que llegan al mismo tiempo. Lo describía Gallego como un "tsunami" y defendía una idea sencilla: más allá de la normativa,

> "La presión regulatoria está descendiendo hacia la cadena de suministro, afectando también a las pymes"
>
> **(Dámaso Ramos. Innovexya)**

hay principios que no cambian. Proteger, detectar y responder siguen siendo la base.

La regulación, en cualquier caso, está teniendo un efecto claro: obliga a ordenar. Santiago Pérez, *channel director* en Veeam Software, lo interpretaba como una oportunidad para estructurar entornos que, en muchos casos, han crecido sin una lógica clara. Especialmente cuando el dato se ha convertido en el activo central y, a la vez, en uno de los más descontrolados.

Ese impacto no se queda en las grandes organizaciones. Dámaso Ramos, responsable de servicios de ciberseguridad en Innovexya, ponía el foco en la cadena de suministro. La exigencia regulatoria está descendiendo hacia proveedores que, aunque no estén obligados directamente, tendrán que cumplir si quieren seguir operando. Esto cambia el escenario para muchas pymes que pasan a formar parte del problema —y de la solución— sin haberlo previsto.

En ese punto, el canal aparece como pieza clave para acompañar ese proceso. Pero no todos ven el impacto de la normativa de la misma forma. Desde una perspectiva más práctica, Martín Vigo cuestionaba hasta qué punto el cumplimiento se traduce en seguridad real. En su experiencia, no es raro encontrar organizaciones donde se prioriza el cumplimiento formal frente a la corrección de vulnerabilidades, lo que deja una brecha evidente entre norma y práctica.

> "El precio sigue condicionando muchas decisiones, alejando la ciberseguridad de un enfoque realmente eficaz"
>
> **(Pedro Marco. Iberlayer)**

> "La identidad y el control del dato son claves en un entorno donde la IA facilita nuevos vectores de ataque"
>
> **(José Fernando Gómez. Ironchip)**

La discusión sobre el papel de la regulación continuó desde distintos ángulos. Javier Fernández, *enterprise regional sales manager* en Sectigo, recordaba que las normativas establecen un marco, pero no sustituyen la toma de decisiones. Cada organización tiene su propio nivel de riesgo asumible y eso condiciona tanto la inversión como la forma de aplicar la seguridad.

> "La ciberseguridad exige un cambio cultural y avanzar hacia modelos de ciberresiliencia más allá de la simple adopción de herramientas"
>
> **(Óscar Suela. Kaspersky)**

El dato volvió a aparecer como uno de los puntos más sensibles. "Tenemos diógenes de datos en las compañías", señalaba Alberto Tejero, CEO de Arexdata, para describir una realidad bastante extendida: información acumulada sin control, sin clasificación y sin una visión clara de su ciclo de vida. La regulación, en este caso, actúa como catalizador para abordar un problema que ya existía.

En paralelo, la identidad se consolida como uno de los ejes más críticos. Rocío Martínez explicaba que el crecimiento de usuarios, dispositivos y sistemas automatizados está complicando su gestión. Ya no se trata solo de autenticar, sino de gobernar quién accede a qué y en qué condiciones.

Sin visibilidad, todo lo anterior pierde sentido. Miguel Ángel Rodríguez, *regional sales account manager* en Forescout, insistía, recordando que, en entornos cada vez más distribuidos, identificar activos y entender su comportamiento es el primer paso para cualquier estrategia.

La normativa también introduce efectos positivos, aunque no siempre se perciban así. José Fernando Gómez recordaba que en ámbitos como la biometría esa normativa ha servido para poner límites claros. Aun así, advertía de que la velocidad a la que evolucionan algunos vectores, especialmente en identidad, supera la capacidad de adaptación de la regulación.

El bloque fue incorporando otra idea que gana peso en el mercado. Pedro Canela,

enterprise security technical presales de V-Valley y en representación de A10 Networks, introdujo el concepto de resiliencia como complemento necesario a la prevención, mientras que María Campos añadió que esto obliga a romper silos y a trabajar de forma coordinada entre áreas.

Ciberdefensa industrial: cuando la prioridad es que todo siga funcionando

Si el bloque anterior ampliaba el foco hacia el negocio, el siguiente lo llevó a un terreno aún más sensible: el industrial. Aquí, la ciberseguridad no se mide solo en datos comprometidos, sino en impacto físico, continuidad operativa e incluso seguridad de las personas.

"No podemos hablar de *malware* o vulnerabilidades en una planta igual que en IT". Alejandro Villar, *strategic advisor en industrial cybersecurity* en TRC y ex Global CISO de Repsol, introdujo así un cambio de perspectiva necesario. En estos entornos, explicó, la prioridad no es proteger información, sino garantizar que los sistemas sigan funcionando sin poner en riesgo la operación.

> "La velocidad de la amenaza obliga a reforzar la visibilidad y la auditoría continua para poder entender qué ha ocurrido y reaccionar a tiempo"
>
> **(Vicente Gozalbo. Netwitness)**

> "Muchos riesgos no responden a vulnerabilidades técnicas, sino a sistemas que pueden ser engañados por diseño"
>
> **(Jacinto Grijalba. OpenText)**

Esa diferencia condiciona todas las decisiones. Detener un sistema puede ser, en determinados casos, más crítico que mantenerlo operativo bajo riesgo. Por eso, la ciberseguridad en OT exige soluciones adaptadas y un equilibrio constante entre protección y continuidad.

El legado tecnológico complica aún más el escenario. Muchas infraestructuras críticas siguen funcionando con sistemas que no pueden sustituirse fácilmente, lo que obliga a buscar fórmulas intermedias para reducir el riesgo sin intervenir directamente en la operación.

> "La regulación fija el marco, pero son las organizaciones las que deben decidir cómo gestionar su exposición al riesgo en función de su realidad"
>
> **(Javier Fernandez. Sectigo)**

> "Los ataques siguen aprovechando los mismos errores de siempre, especialmente en identidad, mientras muchas organizaciones tardan meses en detectar intrusiones"
>
> **(Sergio Martínez. SonicWall)**

La falta de visibilidad vuelve a ser un punto crítico. Miguel Ángel Rodríguez insistía en que en muchas organizaciones ni siquiera se tiene un inventario completo de los activos. En un entorno donde conviven IT, OT e IoT, esa falta de control multiplica la exposición.

El tipo de tecnología también cambia. David Baldomero señalaba que las soluciones tradicionales no siempre son válidas en estos entornos, donde la disponibilidad es prioritaria y cualquier intervención puede tener impacto directo en la producción.

A esa complejidad técnica se suma una realidad operativa. Rocío Vaquero recordaba que el riesgo no se limita a los sistemas industriales, sino que afecta a todo el ecosistema: dispositivos conectados, redes, usuarios... y, en última instancia, al propio negocio.

Frente a ese escenario, varias intervenciones coincidieron en recuperar principios básicos. Vicente Gozalbo apuntaba a la necesidad de inventariar, monitorizar y controlar, adaptando esos conceptos a protocolos industriales que poco tienen que ver con los entornos IT tradicionales.

El factor humano volvía a aparecer como punto débil. José Fernando Gómez recordaba que prácticas como compartir credenciales siguen siendo habituales en entornos industriales y Pablo Collantes, *country manager* de WatchGuard en Iberia, insistía en que, sin

> "El ataque evoluciona más rápido que la defensa, generando un desfase creciente que exige mayor capacidad de respuesta en tiempo real"
>
> **(David Baldomero. Trellix)**

formación y concienciación, cualquier estrategia pierde eficacia.

El canal: traducir la complejidad en algo que el cliente pueda asumir

El cierre del evento volvió a poner el foco en el canal, pero desde una perspectiva muy práctica. La complejidad tecnológica, la presión regulatoria y la evolución de las amenazas convergen en un punto: el cliente final, especialmente la pyme.

Noé Villar situó el debate en la realidad del *partner*. La mayoría opera en entornos donde los recursos son limitados y donde la ciberseguridad compite con otras prioridades. Ahí es donde aparecen las oportunidades, pero también las limitaciones. Sergio Martínez apuntaba a una carencia evidente: muchas organizaciones no cuentan con monitorización continua. Esto abre la puerta a servicios gestionados que cubran esa necesidad.

El reto para el canal no es menor. Fernando Martínez describía la situación como un entorno donde hay que construir soluciones a partir de múltiples piezas: identidad, red, correo, IoT, inteligencia artificial... Un puzzle cada vez más complejo que requiere integración y conocimiento.

> "La regulación puede ayudar a ordenar entornos complejos, especialmente en la gestión del dato"
>
> **(Santiago Pérez. Veeam Software)**

> "Sin formación, concienciación y cambio cultural, cualquier estrategia se queda a medio camino"
>
> **(Pablo Collantes. WatchGuard)**

Aun así, el contexto también permite evolucionar. David Baldomero señalaba que la creciente relevancia de la seguridad abre la puerta a modelos más orientados a valor, donde el *partner* puede ir más allá de la venta de producto.

No todo es crecimiento. Pedro Marco recordaba que la regulación, aunque necesaria, también genera incertidumbre cuando no está clara o resulta difícil de aplicar en el día a día.

En su intervención Pablo Collantes insistió

en que, por mucha tecnología que se despliegue, el eslabón más débil sigue siendo la persona. Y sin formación, concienciación y cambio cultural, cualquier estrategia se queda a medio camino.

La sensación que dejó el encuentro es que la ciberseguridad ya no puede abordarse como una suma de herramientas ni como un problema exclusivamente técnico. La velocidad del ataque, la presión regulatoria, la expansión del dato y la irrupción de la inteligencia artificial están obligando a replantear el modelo desde la base.

En ese contexto, la tecnología sigue siendo necesaria, pero no suficiente. La visibilidad, la capacidad de respuesta, la gestión del dato, la identidad o el papel del canal son piezas claves, pero todo converge en un mismo punto: la organización. Cómo se diseña, cómo se gestiona y, sobre todo, cómo integra a las personas en ese proceso. Porque, en un entorno cada vez más automatizado, el factor humano sigue siendo, al mismo tiempo, el mayor riesgo y la mejor defensa.