DEBATES ciberseguridad TIC

Más plataforma. Más IA. ¿Quién controla qué?

NTT DATA

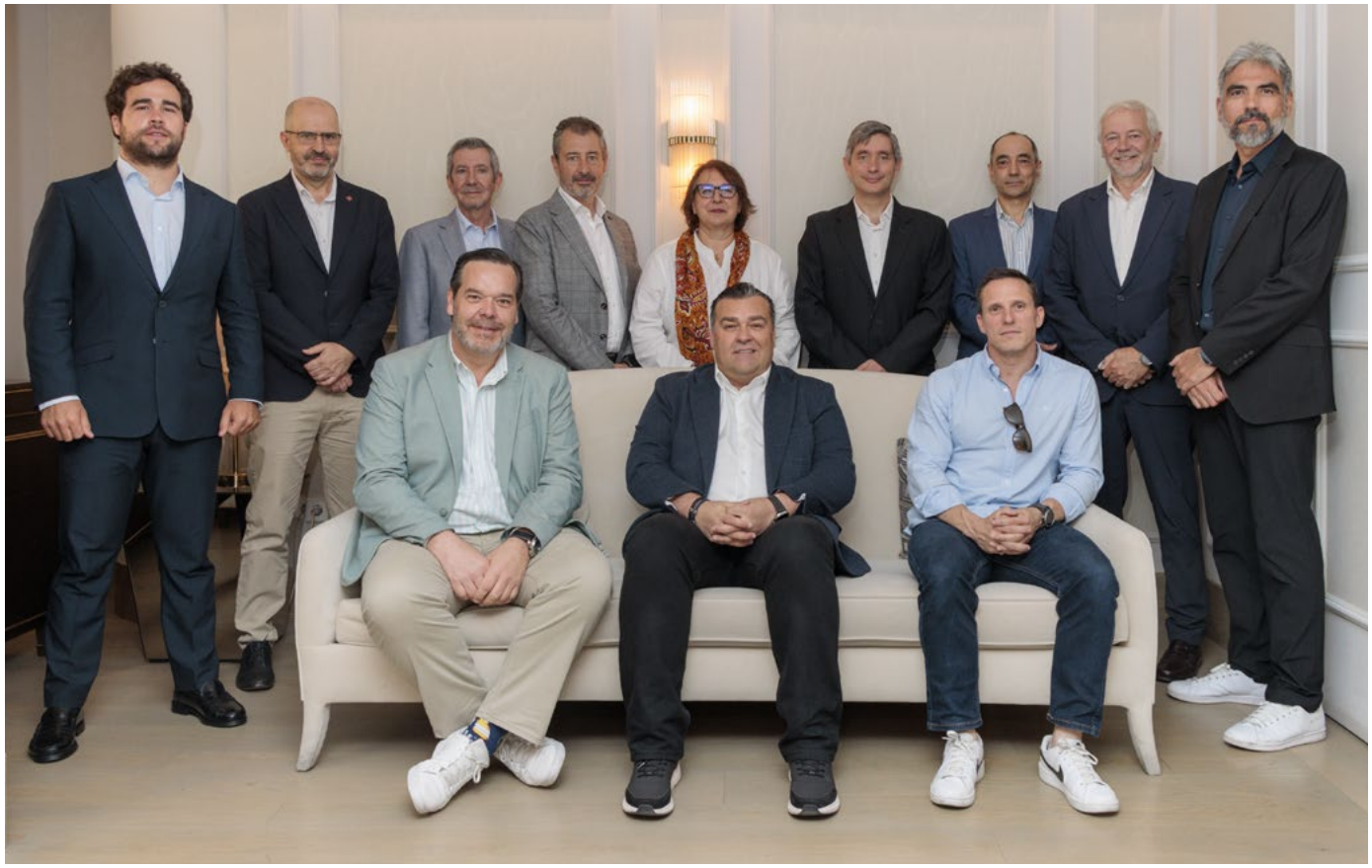
paloalto NETWORKS

IR A PÁGINA SIGUIENTE

Más plataforma. Más IA. ¿Quién controla qué?

La inteligencia artificial se ha convertido en un elemento estructural dentro de las estrategias de ciberseguridad. Se busca avanzar hacia modelos cada vez más integrados, donde se consoliden herramientas y se automaticen operaciones en torno a plataformas capaces de correlacionar contexto, identidades, datos y respuesta en tiempo real. Sobre el papel, el objetivo parece claro: reducir complejidad, ganar velocidad y operar de forma más eficiente.

Rosalía Arroyo



Sin embargo, la realidad que viven muchas compañías es bastante más compleja. El reto ya no consiste únicamente en incorporar más automatización, sino en entender hasta qué punto las organizaciones mantienen realmente el control sobre sistemas cada vez más distribuidos y autónomos.

Sobre estas cuestiones giró el almuerzo-debate “Más plataforma. Más IA. ¿Quién controla qué?”, organizado por Ciberseguridad TIC con el patrocinio de NTT DATA y Palo Alto Networks. Durante el encuentro, responsables de ciberseguridad, tecnología y operaciones de distintos sectores analizaron cómo están afrontando la evolución hacia modelos de seguridad más

integrados, qué riesgos empiezan a emerger alrededor de la IA y qué papel jugarán la automatización, la identidad y las plataformas en los próximos años.

Más plataforma, más IA... y más complejidad

La primera gran reflexión de la mesa giró alrededor de una idea compartida por buena parte de los participantes: la IA está aportando enormes capacidades de automatización y eficiencia, pero también está introduciendo nuevas capas de complejidad y dificultades de gobierno para las organizaciones.

Para Juan Manuel Matalobos, head of human risk de BBVA, la IA generativa introduce "un paradigma totalmente distinto", con nuevos activos, riesgos y formas de exposición que aumentan la complejidad operativa. Además, diferenciaba claramente entre la IA predictiva tradicional, más limitada a perfiles especializados, y la IA generativa actual, mucho más extendida entre usuarios de todo tipo. Aunque reconocía que la consolidación tecnológica y la nube sí ayudan a centralizar y simplificar parte

> "La cuestión ya no es solo incorporar IA, sino cómo mantener el control sobre sistemas cada vez más autónomos"
>
> **Juan Manuel Matalobos,** head of human risk, **BBVA**

de la operación, insistía en que la incorporación de IA obliga a proteger muchos más elementos y escenarios.

La percepción de Marcos Aguado, responsable de comunicaciones y seguridad de la información de EAG / Empresarios Agrupados, iba en una línea muy similar. "Esto va a traer complicaciones serias, y solo acaba de empezar", advertía, mostrando dudas sobre la capacidad actual de las plataformas para resolver esa complejidad creciente.

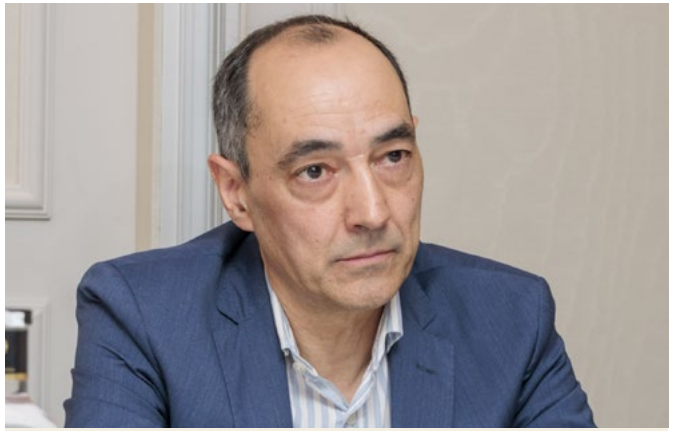
Desde una perspectiva más ligada al impacto operativo, Vicente Camus, cybersecurity manager de Globalvia, señalaba que la IA sí está ayudando al negocio a ganar eficiencia y reducir costes, lo que explica la rapidez con la que muchas áreas están impulsando su adopción. Sin embargo, esa productividad para el usuario termina trasladando más complejidad a áreas como seguridad, IT o protección de datos, especialmente cuando entran en juego datos sensibles o entornos críticos. "Desde la perspectiva de seguridad, la adopción de la IA incrementa significativamente la complejidad de gobierno de esta", resumía.

Otro de los temas que apareció rápidamente en la conversación fue la pérdida de control sobre procesos que muchas veces terminan funcionando como una "caja negra", una preocupación especialmente presente en la intervención de José Macarro, director la SGAE (Sociedad

General de Autores y Editores). A su juicio, la IA sí está simplificando determinadas tareas y procesos de negocio, pero esa eficiencia se consigue "a costa de una mayor complejidad tecnológica", desplazando capacidades hacia plataformas externas donde resulta difícil entender qué ocurre realmente con los datos y los procesos intermedios.

También surgió durante el debate otro problema creciente: la enorme velocidad a la que evoluciona la IA. David Escudero-Mancebo, director del Centro de IA de la Universidad de Valladolid, advertía de que las reglas y medidas de control que hoy parecen válidas pueden quedar rápidamente desactualizadas, mientras que la facilidad de uso de estas herramientas está provocando que muchos usuarios las adopten sin ser plenamente conscientes de los riesgos asociados al tratamiento y movimiento de los datos.

En esa misma línea incidía Cecilio Vázquez, director de tecnologías de la información y comunicaciones de Loterías y Apuestas del Estado, al referirse a la sensación de pérdida de control derivada de la democratización de la IA. Aunque reconocía las mejoras en productividad y



"El gran problema llegará cuando los usuarios empiecen a delegar accesos, decisiones y credenciales en agentes autónomos"

Marcos Aguado,
responsable de comunicaciones y seguridad de la información de, **EAG / Empresarios Agrupados**

automatización que ya están aportando estas tecnologías, alertaba de la dificultad creciente para mantener visibilidad real sobre dónde están los riesgos y cómo se mueve la información dentro de modelos y herramientas cada vez más distribuidos. "Se democratiza, pero pierdes el control", resumía.

Frente a visiones más centradas en la pérdida de control, Carlos Mourelo, director corporativo IT de Grupo CEF-UDIMA, defendió una aproximación más pragmática y recordó que el impacto de la IA depende en gran medida del caso de uso y del modelo de implantación elegido. Explicó que determinadas organizaciones están empezando a apostar por modelos locales para mantener el control sobre información especialmente sensible o estratégica. Aunque reconocía que esto implica más coste y complejidad tecnológica, también permite mantener el conocimiento crítico "dentro de casa" y reducir la exposición de determinados datos corporativos.

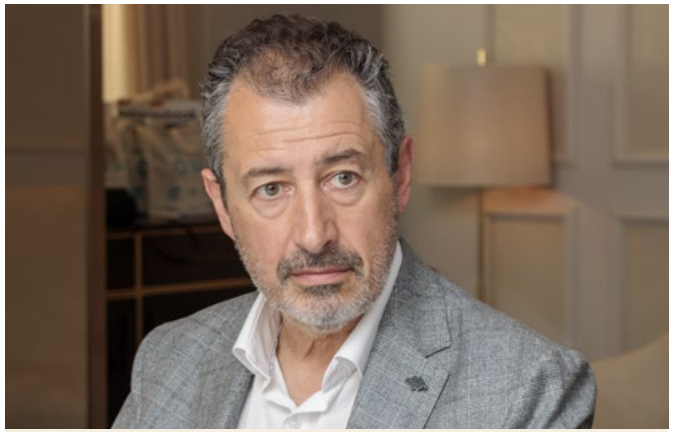
Desde la visión de los patrocinadores, Jonathan Soler, director de Cybersecurity Solutions de NTT DATA, defendía que la complejidad no desaparece, sino que se desplaza hacia otros ámbitos, especialmente hacia la transformación operativa y de gobierno. En su opinión, el mercado está avanzando hacia modelos con menos proveedores y plataformas más integradas, aunque advertía de que el verdadero reto no está única-

mente en adoptar tecnología, sino en transformar procesos, modelos operativos y estructuras de gobierno para poder obtener realmente el valor prometido por la plataforma y la IA.

Por su parte, David García Cano, sales manager major accounts de Palo Alto Networks, apostó por una visión menos alarmista sobre la expansión de la IA y comparó el momento actual con otras grandes revoluciones tecnológicas. A su juicio, el objetivo no debe ser limitar la adopción de estas herramientas, sino incorporarlas de forma segura desde el principio, reforzando especialmente el control sobre identidades, agentes autónomos y modelos de IA.

¿Estamos preparados para dejar actuar a la IA?

La conversación evolucionó después hacia uno de los debates que más interés generó entre los asistentes: hasta qué punto las organizaciones terminarán delegando en la IA capacidades reales de detección y respuesta autónoma frente a amenazas. La mayoría coincidía en que, más que una posibilidad futura, se trata ya de un escenario prácticamente inevitable.



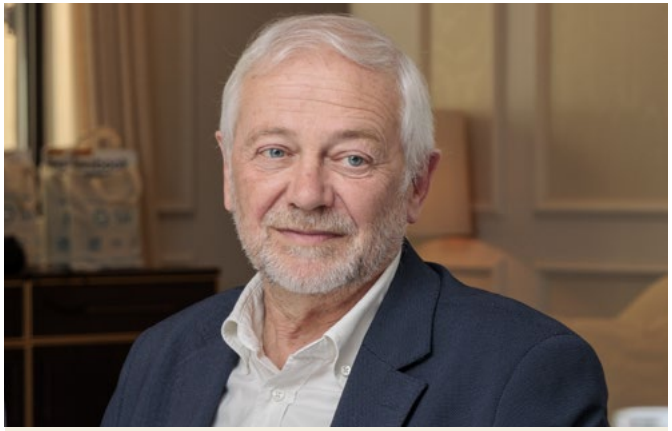
> "Muchas veces el problema no es lo que entra o lo que sale, sino no saber realmente qué ocurre en medio de todo el proceso"

José Macarro,
director de la **SGAE** (Sociedad General de Autores y Editores)

La velocidad de los ataques está empezando a dejar sin margen de reacción a los equipos humanos, advertía David Escudero-Mancebo. "No te va a quedar más remedio que delegar en sistemas inteligentes que velen por tu protección", afirmaba, aunque admitía que muchas organizaciones todavía mantienen modelos muy manuales y artesanales en determinadas áreas de seguridad.

En opinión de José Macarro, la IA ya está tomando decisiones en ámbitos como priorización, correlación o scoring de riesgos, aunque todavía exista supervisión humana detrás de muchos procesos. Aun así, consideraba que el volumen y la velocidad de las amenazas acabarán obligando a automatizar mucho más. Eso sí, insistía en que para dar ese "salto de fe" será imprescindible reforzar capacidades de trazabilidad, auditoría y explicabilidad. "¿Qué pasa en el medio?", volvía a preguntarse al hablar de sistemas que funcionan como una "caja negra".

La sensación de inevitabilidad también apareció en las intervenciones de Cecilio Vázquez y Carlos Mourelo. Ambos coincidían en que la IA terminará asumiendo tareas críticas de protección y respuesta porque la capacidad humana ya no será suficiente para gestionar el volumen de amenazas y la rapidez de los ataques. "No hay nada que tenga que ocurrir para que esto sea



"La IA obliga a replantear por completo cómo operamos la seguridad y cómo construimos las plataformas"

Marc Sarrias,
country manager, **Palo Alto Networks**

inminente", apuntaba Cecilio Vázquez, mientras Carlos Mourelo reconocía que, aunque la IA todavía esté en una fase relativamente temprana, el crecimiento es tan rápido que el escenario de operaciones autónomas parece ya cuestión de pocos años.

La cuestión ya no es si vamos a automatizar la seguridad, sino cómo mantener el control cuando las decisiones empiezan a tomarse cada vez más rápido y con menos intervención humana

Ese camino hacia operaciones autónomas ya se está produciendo en áreas como redes e infraestructuras, donde muchos procesos de Nivel 1 se encuentran completamente automatizados, explicaba Guillermo Martínez, director of digital architecture de NTT DATA. En su opinión, el paso natural es incorporar IA sobre esos entornos hiperautomatizados y trasladar progresivamente esa lógica también al ámbito de la ciberseguridad. "El camino ya está empezado", resumía.

Otra idea relevante la introdujo Juan Manuel Matalobos al recordar que determinados modelos de IA llevan años funcionando de manera efectiva en sectores como la banca, especialmente en ámbitos como detección de fraude o análisis de operaciones en tiempo real. A su juicio, el problema no es tanto la utilización de IA, sino cómo mantener el control sobre sistemas cada vez más potentes y autónomos. En ese contexto defendía un modelo de "human in the loop" diferente al tradicional, donde las personas dejan de supervisar alertas individuales para centrarse en vigilar el comportamiento y las anomalías de la propia IA.

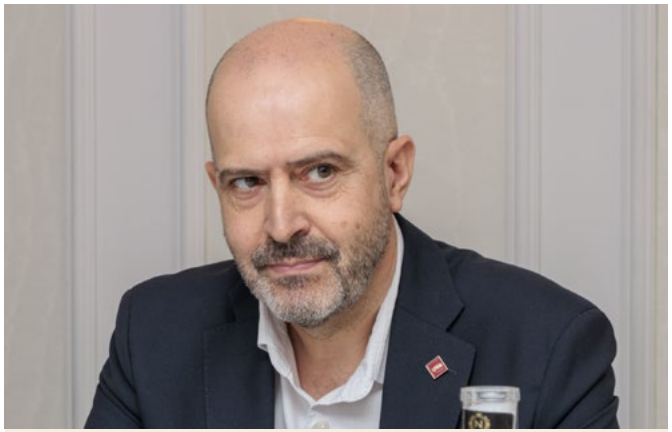
Especialmente contundente se mostró Marc Sarrias, country manager de Palo Alto Networks, al defender que el modelo tradicional de operación de ciberseguridad "ya es insostenible". En su opinión, la velocidad, complejidad y volumen de amenazas hacen imposible seguir operando con múltiples tecnologías aisladas y procesos excesivamente manuales. El directivo defendió así la necesidad de evolucionar hacia modelos mucho más integrados y basados en plataforma, capaces de trabajar sobre un contexto unificado donde la IA pueda operar de forma eficiente. "No puedes tener 200 tecnologías y

estar cosiendo tecnologías como se ha venido haciendo", advertía.

Durante su intervención también alertó sobre el impacto que tendrán nuevas capacidades ofensivas basadas en IA, especialmente en torno a modelos como Mythos, capaces de identificar vulnerabilidades y construir ataques sofisticados en tiempos extremadamente reducidos.

David García Cano reforzó esa visión recordando cómo el tiempo de reacción frente a incidentes se está reduciendo de forma drástica. Citó incluso casos donde la exfiltración de información puede producirse en apenas segundos, haciendo inviable cualquier capacidad de respuesta exclusivamente humana. Para el directivo, las organizaciones deberán asumir progresivamente ese "salto de fe" hacia la automatización y la IA, del mismo modo que otros sectores ya confiaron hace años en sistemas automáticos para procesos críticos como pagos o detección de fraude.

El contrapunto lo introdujo Jonathan Soler al insistir en que la confianza en modelos autónomos solo será posible si las organizaciones mantienen capacidad de auditoría, reversibilidad y con-



"No nos va a quedar más remedio que apoyarnos en sistemas inteligentes porque la velocidad de los ataques ya supera la capacidad humana"

David Escudero-Mancebo,
director centro IA, **Universidad de Valladolid**

texto sobre las decisiones que tome la IA. A su juicio, la explicabilidad seguirá siendo esencial, especialmente cuando determinadas acciones automáticas puedan tener impacto directo sobre operaciones críticas o continuidad de negocio.

La nueva velocidad del ataque

La irrupción de herramientas como Mythos llevó el debate hacia otra cuestión especialmente sensible para los responsables de seguridad: si las organizaciones tienen realmente visibilidad sobre su superficie de exposición y capacidad para reaccionar a ataques cada vez más automatizados y rápidos.

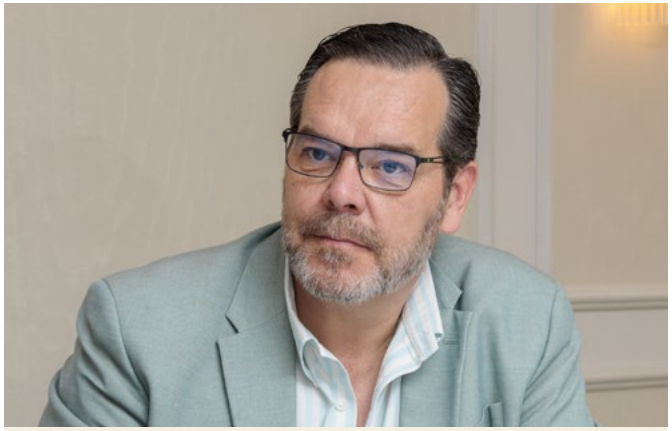
Las compañías atraviesan un momento de enorme transformación y, aunque probablemente todas desearían disponer de más tiempo para prepararse, la realidad obliga a acelerar, reconocía Juan Manuel Matalobos. "Los malos no van a esperar", resumía al explicar que el margen de reacción se está reduciendo drásticamente.

Incluso organizaciones con un conocimiento muy profundo de sus entornos siguen descubriendo exposición y vulnerabilidades inesperadas cuando utilizan este tipo de capacidades avanzadas de análisis, señalaba José Macarro. A su juicio, eso evidencia la enorme dificultad que tienen muchas empresas para conocer realmente su perímetro y superficie de ataque.

Desde una visión más ligada a operación y con-

tinuidad de negocio, Vicente Camus recordaba que los ataques más dañinos suelen apoyarse en movimientos silenciosos y persistentes dentro de las infraestructuras durante largos periodos de tiempo. Por eso defendía que, además de acelerar la respuesta, las organizaciones deben reforzar medidas de contención, segmentación y control para limitar el impacto cuando una amenaza consigue entrar. El directivo planteó además una cuestión que aparecería varias veces durante el debate: quién asume realmente la responsabilidad cuando una IA toma una decisión crítica que afecta directamente a la operación o al negocio.

Precisamente Jonathan Soler retomó esa preocupación al preguntarse quién será responsable de las decisiones tomadas por sistemas autónomos de seguridad. En respuesta, Marc Sarrias defendió que el modelo no pasa por eliminar completamente el control humano, sino por definir cuidadosamente qué decisiones pueden automatizarse y cuáles seguirán requiriendo supervisión directa. Según explicaba, el "human in the loop" ya está evolucionando hacia modelos donde la intervención humana queda reservada únicamente para los escenarios más críticos.



"Homogeneización y estandarización son las que realmente permiten automatizar y ganar eficiencia"

Guillermo Martínez,
director of digital architecture, **NTT Data**

Sarrias insistió además en que el modelo tradicional basado en múltiples tecnologías aisladas ya no es capaz de responder a la velocidad actual de los ataques y volvió a defender la necesidad de construir plataformas mucho más integradas y apoyadas sobre contexto unificado. A su juicio, solo así será posible mantener tiempos de respuesta compatibles con amenazas que ya empiezan a desarrollarse y desplegarse en cuestión de minutos.

La conversación derivó finalmente hacia el papel que deben jugar fabricantes e integradores en este nuevo escenario. Vicente Camus reclamaba más acompañamiento práctico y casos de uso concretos que permitan a las organizaciones entender hasta dónde automatizar y dónde mantener controles humanos. Tanto Marc Sarrias como Guillermo Martínez defendieron entonces la importancia de combinar tecnología, experiencia operativa y conocimiento de negocio para adaptar estos nuevos modelos de automatización al contexto específico de cada organización.

Identidades, agentes y el nuevo perímetro invisible

El debate avanzó después hacia otro de los grandes focos de preocupación que está empezando a emerger alrededor de la IA: el papel de

La IA está ayudando a simplificar procesos y ganar eficiencia, pero también está obligando a replantear gobierno, identidad, operación y capacidad real de supervisión

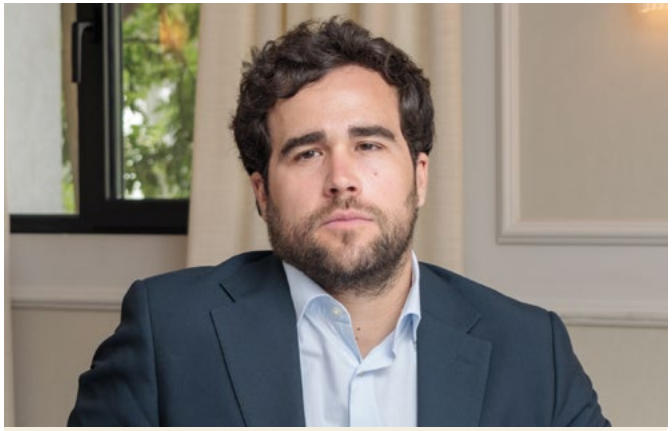
las identidades de máquina, los agentes autónomos y los nuevos riesgos asociados a entornos cada vez más automatizados e interconectados.

Marcos Aguado advertía sobre la complejidad creciente derivada de la combinación entre usuarios, identidades y agentes de IA. A su juicio, el problema se agravará cuando los usuarios empiecen a delegar capacidades y credenciales en agentes capaces de operar de forma autónoma. “Va a ser muy difícil”, reconocía, insistiendo además en que las técnicas de robo y suplantación de identidad son cada vez más sofisticadas y creíbles.

También Carlos Mourelo consideraba que los mayores riesgos terminarán llegando probablemente desde los propios modelos inteligentes y sistemas agénticos, precisamente por la velocidad con la que se están extendiendo y por la capacidad de integración y automatización que ofrecen. En su opinión, la evolución tecnológica va claramente más rápido que la capacidad real de control de las organizaciones.

Otro elemento poco habitual en este tipo de conversaciones lo introdujo David Escudero-Mancebo al poner el foco en el coste económico de la IA. Según explicaba, la enorme capacidad computacional que requieren algunos modelos avanzados podría convertirse también en un elemento indirecto de control y gobernanza dentro de las organizaciones porque hay aplicaciones como la generación de código que multiplican el consumo de tokens. Además, el directivo alertó sobre otro problema creciente: la utilización masiva de código generado por IA dentro de los entornos de desarrollo complica las tareas de mantenimiento del mismo.

Marc Sarrias profundizó especialmente en los riesgos asociados a los entornos agénticos y



“Automatizar está bien, pero tiene que haber controles adicionales porque antes o después algo va a fallar”

Vicente Camus,
cybersecurity manager, **Globalvia**

al uso creciente de asistentes integrados en navegadores, plataformas de desarrollo o herramientas corporativas. Según explicaba, muchos de estos sistemas operan ya dentro de contextos aparentemente legítimos, utilizando identidades válidas y comportamientos que

las herramientas tradicionales de seguridad no siempre son capaces de detectar como anómalos. A su juicio, esto obliga a desplazar la seguridad hacia nuevas capas de contexto, identidad y comportamiento.

Aunque reconocía que todavía resulta difícil anticipar con claridad todos los riesgos que traerán los agentes autónomos, Cecilio Vázquez se mostraba convencido de que introducirán nuevos escenarios de exposición que las organizaciones tendrán que aprender a gestionar. Aun así, insistía en que el usuario seguirá siendo durante mucho tiempo uno de los puntos más débiles dentro de la cadena de seguridad.

La conversación derivó después hacia la dificultad de controlar agentes capaces de actuar de manera autónoma sobre sistemas corporativos utilizando privilegios legítimos. David García Cano explicaba que el verdadero problema aparece cuando un agente recibe permisos válidos para resolver una tarea y empieza a generar planes alternativos de actuación hasta conseguir completarla. “El agente, su cometido, es resolver un problema”, resumía, advirtiendo de que muchos de esos comportamientos pueden parecer

> “Hay ataques donde la exfiltración ocurre en segundos y ningún equipo humano tiene capacidad de reacción a esa velocidad”

David García Cano,
sales manager major accounts, **Palo Alto Networks**

completamente legítimos desde el punto de vista de las herramientas tradicionales de seguridad.

Otro de los grandes debates actuales alrededor de la IA generativa apareció de la mano de David Escudero-Mancebo, que recordó las dificultades para predecir completamente el comportamiento de modelos basados en LLMs. El directivo señalaba que estos sistemas continúan cometiendo errores difíciles de explicar y defendía que la industria todavía está aprendiendo cómo introducir redundancia, validación y mecanismos de supervisión más robustos para reducir esos riesgos.

La identidad volvió entonces al centro de la conversación. En opinión de José Macarro, en un entorno completamente interconectado y basado en APIs, agentes y automatismos, la capacidad de controlar privilegios y limitar el alcance de las identidades agénticas será crítica para evitar que los riesgos “se vayan de las manos”.

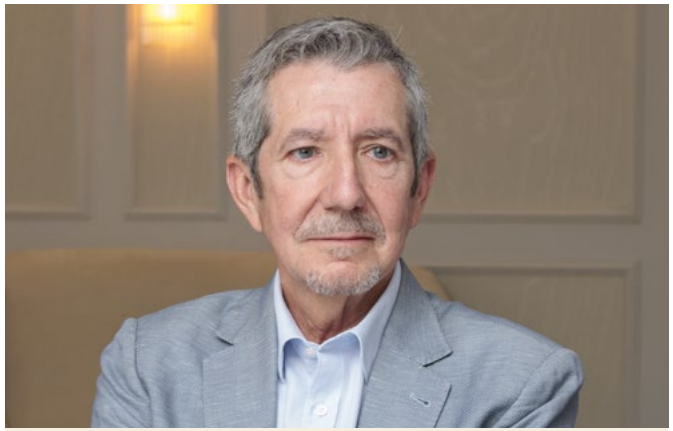
Marc Sarrias vinculó precisamente esa evolución con la creciente importancia estratégica de la identidad dentro de la industria de ciberseguridad y explicó que conceptos como Zero Trust o Zero Standing Privileges buscan limitar privilegios permanentes y conceder acceso únicamente durante el tiempo estrictamente necesario para realizar una tarea concreta. Según defendía, este tipo de modelos solo pueden gestionarse apoyándose en plataformas tecno-

lógicas capaces de automatizar y gobernar ese ciclo completo de identidades y privilegios.

Del entusiasmo por la IA a la realidad de la gobernanza

La conversación abordó también una cuestión especialmente compleja para muchas organizaciones: cómo aterrizar realmente una estrategia de IA y plataforma dentro de entornos donde conviven presión de negocio, limitaciones operativas y necesidades de control cada vez mayores.

Las iniciativas de IA no nacen desde ciberseguridad, sino desde las propias áreas de negocio, que buscan automatizar procesos y ganar eficiencia, aseguraba Vicente Camus durante una de sus intervenciones. En ese contexto, reconocía que uno de los principales retos está siendo contener el "hype" alrededor de la inteligencia artificial y evitar que cualquier necesidad termine convirtiéndose automáticamente en un proyecto basado en IA o agentes autónomos. A su juicio, la principal dificultad sigue estando en la gobernanza y en gestionar la fricción entre la velocidad que reclama el negocio y los controles que seguridad necesita implantar antes de avanzar.



"Todavía no somos capaces de visualizar todos los riesgos que pueden introducir los agentes autónomos"

Cecilio Vázquez, director de tecnologías información y comunicaciones, **Loterías y Apuestas del Estado**

Juan Manuel Matalobos ampliaba esa reflexión señalando que muchas organizaciones están acelerando su apuesta por la IA "a costa del control". El directivo describía además cómo los equipos de ciberseguridad se encuentran atrapados entre tres frentes simultáneos: ataques cada vez más sofisticados impulsados por IA, presión interna para adoptar nuevas capacidades tecnológicas y necesidad de garantizar que todo ese proceso se realice manteniendo supervisión y capacidad de gobierno.

En plena fase de decisión sobre hasta dónde automatizar y cómo integrar la IA dentro de los procesos de seguridad existentes situaba Marcos Aguado a su organización. En su caso, explicaba, la principal preocupación está hoy en la integración y en definir hasta qué punto determinadas capacidades pueden delegarse realmente en modelos automatizados.

Gobernanza y talento volvieron a aparecer poco después en la intervención de Carlos Mourelo. Según explicaba, muchas organizaciones todavía están en fases muy iniciales de adopción y carecen tanto de estructuras maduras de control como de perfiles especializados capaces de mantener y supervisar estos nuevos entornos de IA.

Más allá de la tecnología, Cecilio Vázquez admitía incluso que muchas compañías todavía no

pueden hablar realmente de una estrategia definida alrededor de IA y plataforma. Aunque reconocía que existen necesidades, proyectos e interés creciente, insistía en que barreras como el talento, la operación o directamente el presupuesto siguen condicionando enormemente la velocidad de adopción. “No todo es estrategia y planificación”, apuntaba al recordar el peso que siguen teniendo las inversiones dentro de este tipo de decisiones.

Una de las visiones más completas sobre cómo ordenar este escenario la aportó José Macarro. Explicó que, tras una primera explosión de interés interno por la IA, optaron por frenar el despliegue masivo y construir primero un modelo formal de gobernanza alineado con la regulación europea. Según detallaba, ese modelo permite evaluar qué iniciativas son realmente IA, qué nivel de riesgo presentan y cómo deben gestionarse antes de llegar a producción. En paralelo, la organización ya trabaja con pilotos internos y arquitecturas específicas para incorporar estas capacidades sin comprometer el control sobre datos y procesos críticos.

> “La gobernanza sigue siendo uno de los puntos más débiles en muchas organizaciones que están empezando a trabajar con IA”

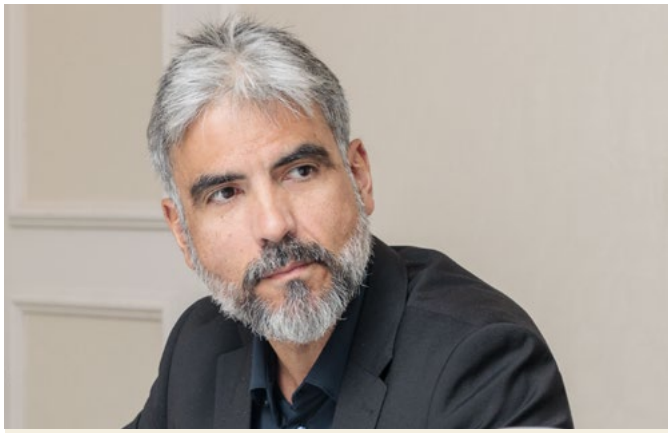
Carlos Mourelo,
director corporativo IT, **Grupo CEF-UDIMA**

El directivo introdujo además otro ángulo especialmente relevante: el impacto de la IA sobre determinados modelos de negocio. En su caso, explicaba, la organización vive simultáneamente la IA como oportunidad tecnológica y como amenaza potencial para sectores basados en propiedad intelectual y generación de contenidos.

El bloque lo cerró David Escudero-Mancebo poniendo sobre la mesa un factor del que apenas se habla en muchos debates sobre IA: el coste real de estas infraestructuras. El directivo explicaba las dificultades que muchas organizaciones públicas están encontrando para financiar capacidades de computación avanzadas o para asumir modelos de consumo cloud difíciles de predecir presupuestariamente. Aun así, reconocía que la idea de plataformas unificadas y centralizadas para gestionar datos, servicios y capacidades de IA resulta especialmente atractiva en entornos muy fragmentados y distribuidos, aunque todavía quede mucho camino por recorrer para hacer viable ese modelo a gran escala.

Qué esperar de fabricantes y partners

La última parte de la mesa se centró en una cuestión muy práctica: qué esperan realmente las organizaciones de fabricantes, integradores y partners tecnológicos en un escenario donde la complejidad, la velocidad del cambio y la presión operativa no dejan de crecer.



"El valor ya no está solo en integrar tecnología, sino en acompañar a las organizaciones en toda esa transformación"

Jonathan Soler,
director cybersecurity solutions, **NTT Data**

Las organizaciones coinciden en que el reto ya no es solo incorporar más tecnología o más plataformas, sino entender cómo operar entornos cada vez más complejos, automatizados y difíciles de controlar

Juan Manuel Matalobos resumía la situación como un contexto donde todo escala al mismo tiempo: modelos, agentes, ataques y necesidades de negocio. Por eso defendía que las organizaciones ya no pueden renunciar ni a la tecnología ni al acompañamiento especializado. "Nosotros no vamos a conocer la tecnología mejor que Palo Alto o sus partners", reconocía, insistiendo además en la importancia de contar con capacidad de ejecución para evolucionar al ritmo que exige el mercado.

La tecnología se ha convertido ya en un elemento imprescindible, coincidía Marcos Aguado, aunque ponía también mucho peso en el acompañamiento de partners y fabricantes durante fases como integración, despliegue o incluso servicios gestionados.

Vicente Camus introducía un componente mucho más ligado a la confianza. Más allá de la tecnología, aseguraba que lo verdaderamente importante es saber que, cuando aparezca un problema —"porque los va a haber"—, el partner responderá y acompañará a la organización. "Al final, dentro de la organización existe una responsabilidad clara sobre este tipo de decisiones", reconocía al explicar el nivel de responsabilidad que asumen muchos responsables de seguridad en este tipo de decisiones.

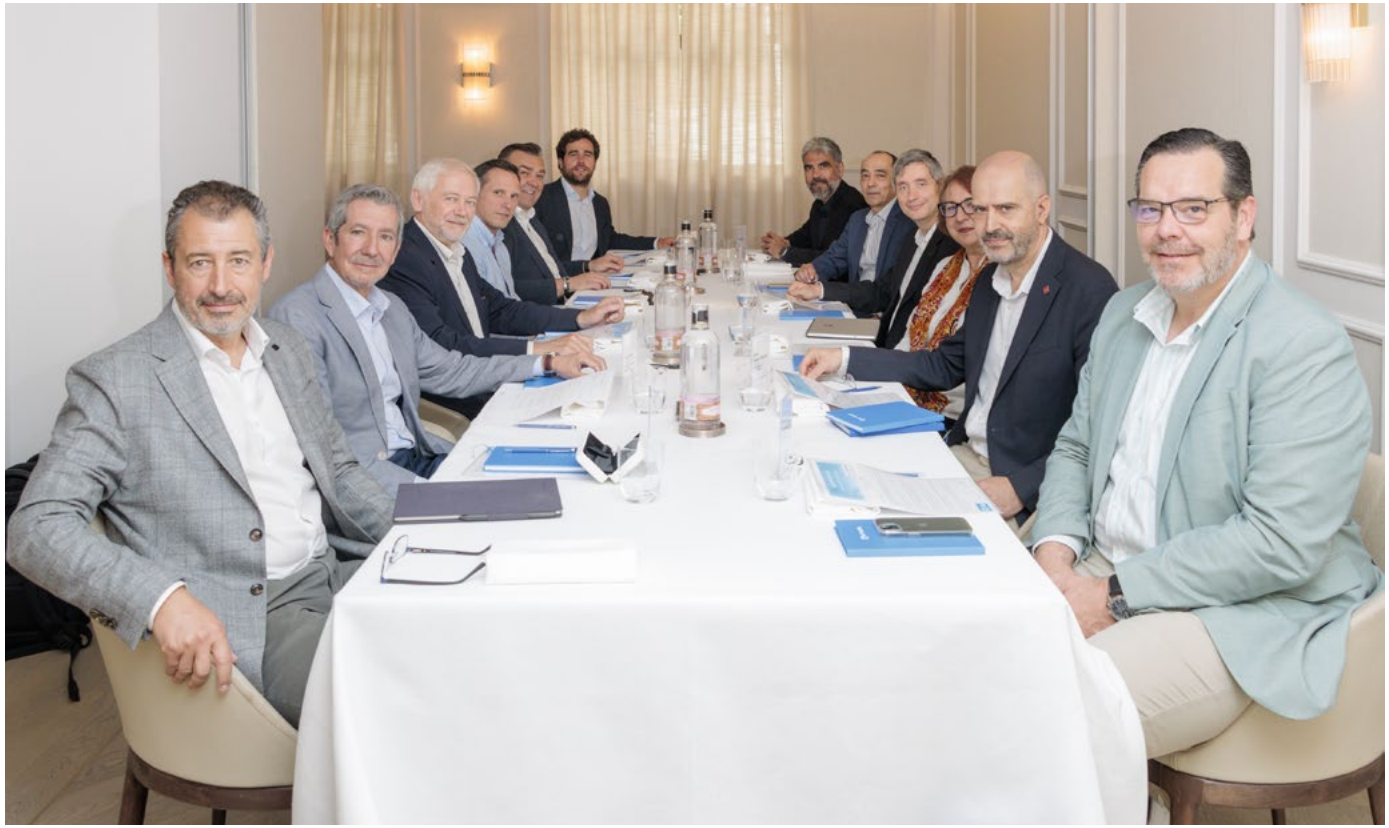
Carlos Mourelo reforzaba precisamente esa idea de acompañamiento, considerándolo incluso más importante que la propia tecnología porque, a su juicio, es lo que realmente termina condicionando la capacidad de ejecución posterior de los proyectos. Cecilio Vázquez, en cambio, admitía que en su caso ese acompañamiento ya se da prácticamente por supuesto y que el verdadero elemento diferencial sigue siendo la tecnología.

Una visión más crítica sobre el papel de los partners la aportó José Macarro, que reconocía que muchas veces el problema no está en la tecno-

logía, sino en la capacidad real de integración y ejecución. Según explicaba, incluso grandes proveedores pueden terminar generando problemas si no entienden correctamente los procesos, el contexto o la cultura de la organización. “La tecnología al final acaba funcionando”, resumía, insistiendo en que el verdadero reto suele aparecer durante la implantación y adaptación al negocio.

David Escudero-Mancebo aprovechó además para poner sobre la mesa una reflexión muy ligada al sector público y a la dificultad de transformar el potencial de la IA en casos de uso concretos y medibles. A su juicio, muchas organizaciones siguen esperando propuestas más tangibles y orientadas a negocio, capaces de justificar claramente inversión, retorno y ahorro real. “Faltan pepitas”, comentaba al referirse a la necesidad de convertir todo el “polvo de oro” alrededor de la IA en productos y soluciones concretas.

Desde NTT DATA, Guillermo Martínez defendía que el reto ya no puede resolverse únicamente comprando tecnología aislada. En su opinión, la IA obliga a integrar múltiples componentes, infraestructuras y capacidades que evolucionan constantemente y que requieren una aproximación mucho más amplia y compleja. Aun así, reconocía que empiezan a aparecer modelos y soluciones que permiten avanzar hacia ese escenario.



El cierre de esta primera parte del almuerzo corrió a cargo de Marc Sarrias, country manager de Palo Alto Networks, que defendió precisamente cómo la evolución hacia modelos de plataforma obliga también a fabricantes y partners a asumir un papel mucho más cercano y continuo con los clientes. El directivo explicaba que este enfoque exige acompañar permanentemente a las organizaciones y mantener niveles muy altos de ejecución y soporte en todos los ámbitos de seguridad. “Nuestra vocación es estar muy cerca de nuestros clientes en ese acompañamiento”, resumía.

De la plataforma al SOC autónomo: la visión de Palo Alto Networks

Buena parte de las ideas defendidas por Palo Alto Networks durante el debate giraron alrededor de una tesis clara: los modelos tradicionales de operación de seguridad ya no son capaces de responder a la velocidad, complejidad y escala de las amenazas actuales. Según explicó Marc Sarrias, country manager de la compañía en España, el reto no consiste únicamente en incorporar más herramientas, sino en replantear cómo se opera la seguridad en un entorno marcado por la IA, los agentes autónomos y la creciente fragmentación tecnológica.

La respuesta de Palo Alto pasa por una estrategia de plataformización que busca consolidar capacidades de protección, detección, respuesta e identidad bajo un mismo contexto operativo. El ejemplo más visible es Cortex XSIAM, la plataforma de operaciones de seguridad impulsada por IA de la compañía, una propuesta que integra datos, analítica, automatización e inteligencia artificial para unificar detección, investigación y respuesta dentro de una única plataforma.

La compañía sostiene que este enfoque es especialmente relevante en un momento en el que los ataques se desarrollan a velocidad de máquina. De hecho, Palo Alto presenta XSIAM como la base de lo que denomina SOC autónomo, un modelo donde la IA asume buena parte de las tareas de investigación y respuesta, manteniendo supervisión humana en las acciones más sensibles.

Durante el almuerzo también adquirieron protagonismo los riesgos asociados a la IA y a los agentes autónomos. En este ámbito, Palo Alto está reforzando su apuesta por lo que denomina "Security for AI". Su plataforma Prisma AIRS está diseñada para proteger el ciclo de vida completo de aplicaciones, modelos, datos y agentes de IA, incorporando capacidades de validación, análisis, gobierno y protección en tiempo de ejecución. Entre otras funciones, permite supervisar prompts, respuestas, flujos de datos e interacciones entre aplicaciones, modelos y agentes para detectar amenazas específicas de IA en tiempo real.

La identidad aparece como otro de los pilares de esta estrategia. Tanto Marc Sarrias como David García Cano insistieron en que el crecimiento de agentes, automatismos e identidades de máquina obligará a reforzar los modelos Zero Trust y a controlar con mucho más detalle quién accede a qué recursos, durante cuánto tiempo y con qué privilegios, dejando claro que el control de identidades y privilegios será uno de los elementos clave para mantener la gobernanza y la confianza en los sistemas automatizados.