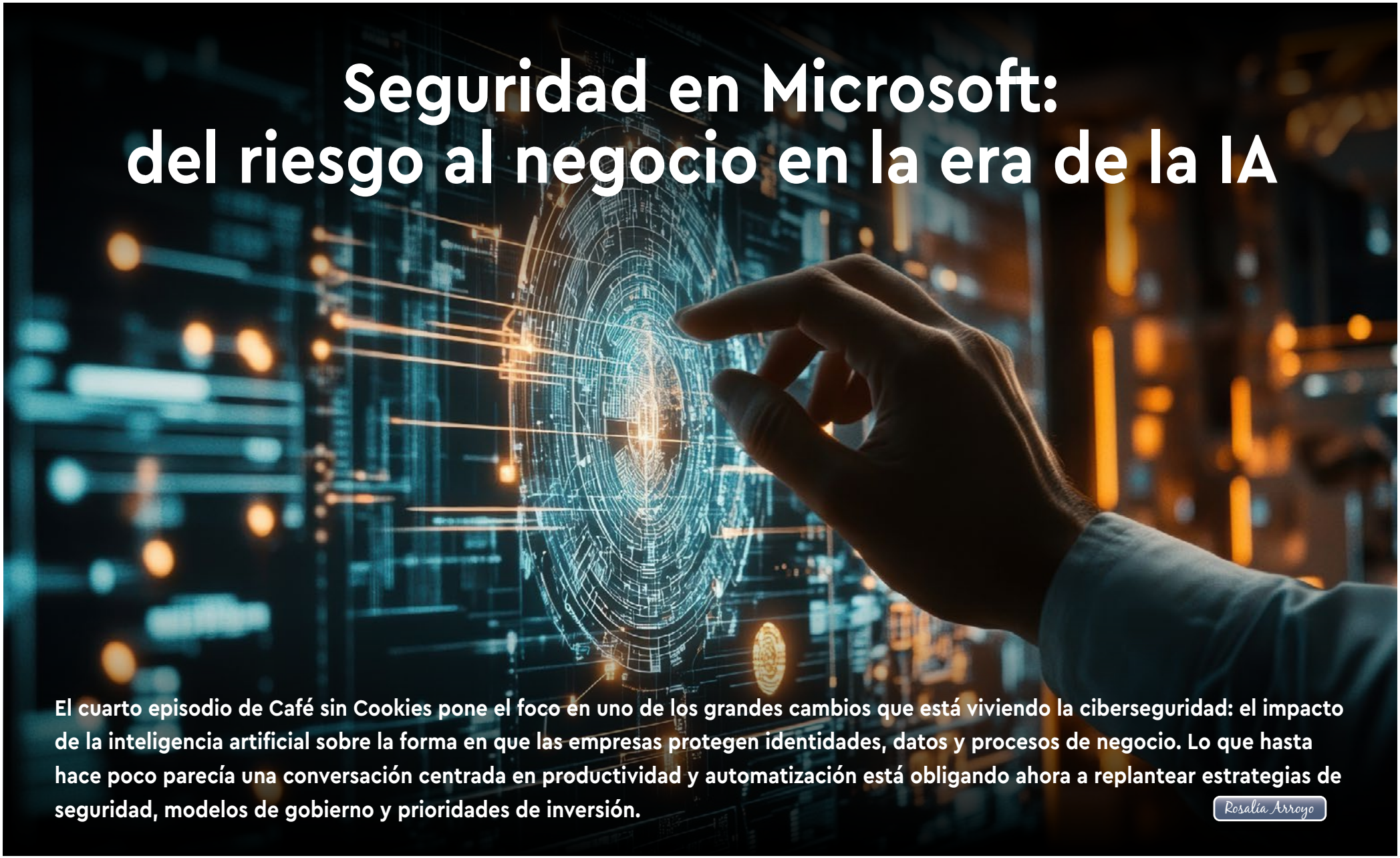
Seguridad en Microsoft: del riesgo al negocio en la era de la IA



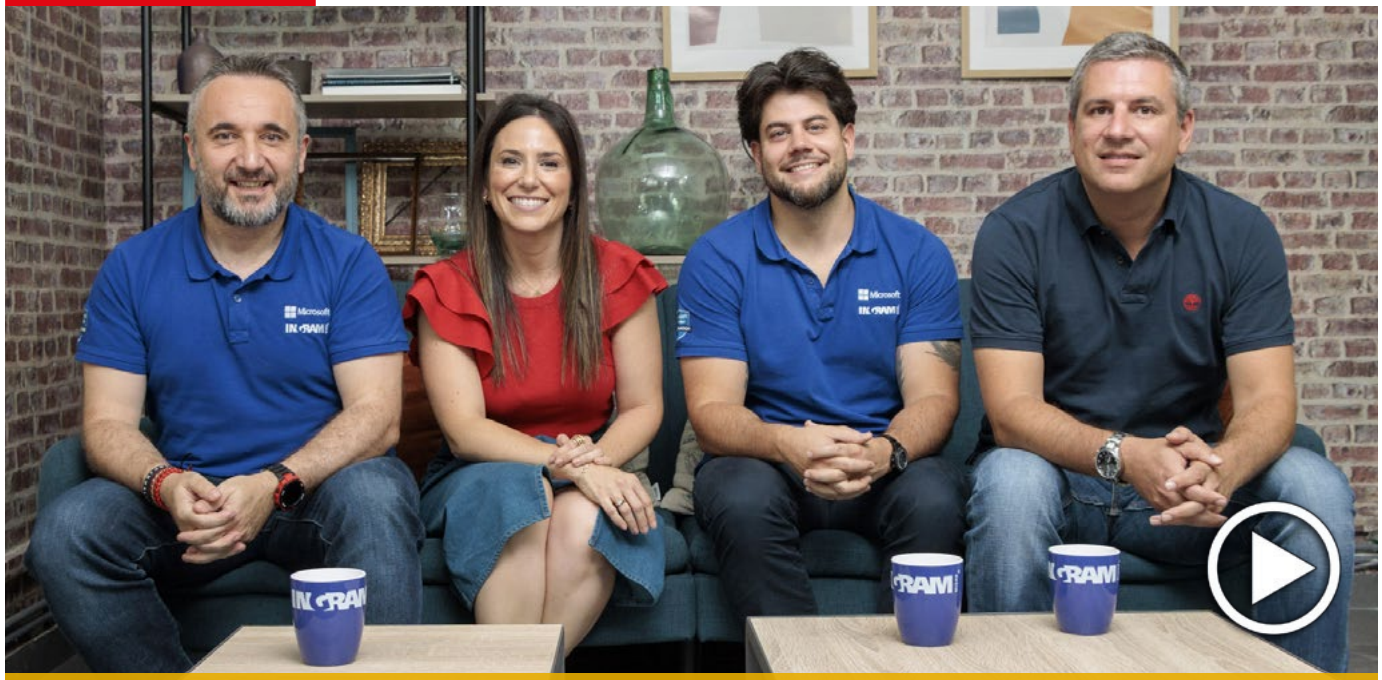
El cuarto episodio de Café sin Cookies pone el foco en uno de los grandes cambios que está viviendo la ciberseguridad: el impacto de la inteligencia artificial sobre la forma en que las empresas protegen identidades, datos y procesos de negocio. Lo que hasta hace poco parecía una conversación centrada en productividad y automatización está obligando ahora a replantear estrategias de seguridad, modelos de gobierno y prioridades de inversión.

Rosalía Arroyo

Para analizar esta evolución participan Alberto Silva, Cybersecurity Sales Director para Western Europe, France and Benelux de Microsoft; Cristina Cañas, Senior Partner Solution Sales de Seguridad en Microsoft; Manuel Muñoz Moreno, EMEA Microsoft Security Vendor Manager en Ingram Micro; y Raúl García-Romeral Moreno, Vendor Manager Microsoft en Ingram Micro España. A lo largo de la conversación comparten su visión sobre la evolución de las amenazas, el papel creciente de la identidad y los datos, la llegada de los agentes de IA y las oportunidades que se abren para el canal en este nuevo escenario.

La sesión también aborda cómo están respondiendo las organizaciones a estos cambios, qué papel juegan soluciones como Defender o Purview en las estrategias actuales de protección y por qué la seguridad está dejando de percibirse como una cuestión puramente tecnológica para convertirse en un elemento cada vez más ligado al negocio y a la adopción segura de la inteligencia artificial.

VER VÍDEO



Raúl García-Romeral Moreno, vendor manager Microsoft en **Ingram Micro España**
Cristina Cañas, Senior Partner Solution Sales de seguridad, **Microsoft**
Manuel Muñoz Moreno, EMEA Microsoft security vendor manager en **Ingram Micro y**
Alberto Silva, Cybersecurity Sales Director | Western Europe, France and Benelux, **Microsoft**

La seguridad se convierte en la base de la IA

El debate arranca con una pregunta aparentemente sencilla: ¿dónde estará el verdadero crecimiento del mercado de seguridad durante los próximos doce meses? ¿En las licencias, en los servicios gestionados o en la propia inteligencia artificial? La respuesta de los participantes deja claro que las tres dimensiones están estrechamente conectadas.

Para Alberto Silva, la irrupción de la IA está transformando la conversación que mantienen clientes, fabricantes y partners. Sin em-

> "El siguiente paso en la ciberseguridad va a ser olvidarnos del tamaño de la empresa"
>
> **Manuel Muñoz Moreno, EMEA Microsoft Security Vendor Manager en Ingram Micro**

bargo, advierte de que muchas organizaciones siguen viendo la seguridad como una capa que se añade al final de un proyecto. A su juicio, el planteamiento debe ser justamente el contrario. "La seguridad no es una capa que pones por encima de la IA; es la base de todo", afirma, añadiendo que, antes de desplegar asistentes, agentes o herramientas de inteligencia artificial, las organizaciones necesitan tener controladas cuestiones como la identidad, los permisos de acceso o la gobernanza de la información.

Tiene claro Alberto Silva que "el cliente no quiere una licencia; quiere un servicio gestionado", debido a que la creciente complejidad de los proyectos obliga a acompañar a las organizaciones durante todo el proceso de adopción y evolución de sus entornos de seguridad.

Cristina Cañas comparte esta visión, aunque identifica en la IA el gran acelerador del mercado. En su opinión, "si no estás seguro, no hay IA". Además, deja claro durante el episodio que la velocidad a la que se está extendiendo el uso de herramientas basadas en inteligencia artificial obliga a reforzar la protección de identidades, dispositivos y datos mucho antes de lo que muchas empresas habían previsto.

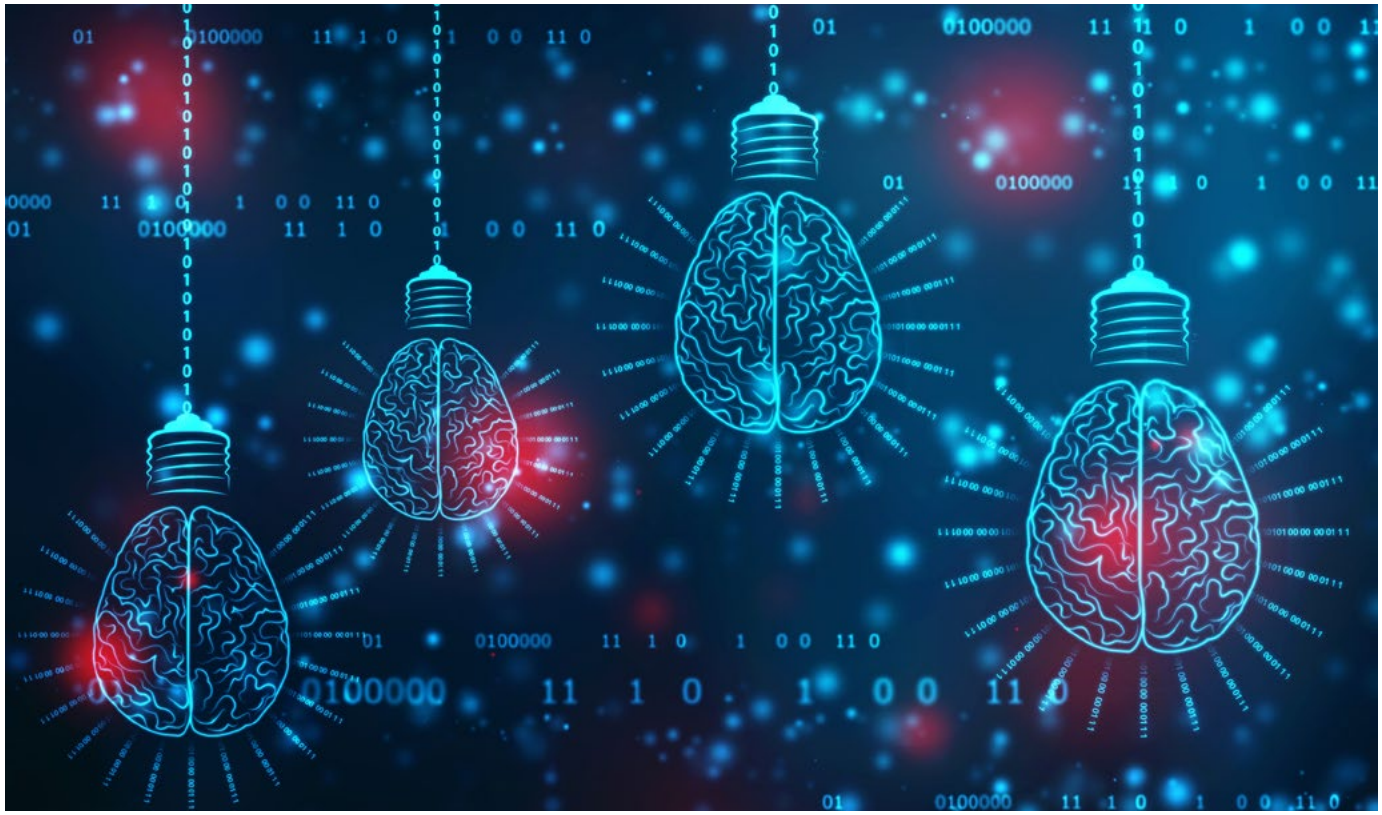
Desde la perspectiva del canal, Manuel Muñoz Moreno pone el acento en los servicios como la gran oportunidad inmediata. Aunque reconoce que la IA y Copilot arrastrarán también la venta transaccional y el licenciamiento, defiende que "la ciberseguridad pura sólo va a tener futuro si entiende el valor añadido de los servicios". Y matiza que no se refiere únicamente al acompañamiento previo a la venta, sino especialmente al servicio posterior, a la capacidad de operar, gestionar y evolucionar la seguridad del cliente en el tiempo.

La conversación deriva entonces hacia la evolución de las amenazas. Tras bromear con la posibilidad de que "un día me llame directamente el virus por teléfono", Raúl García-Romeral Moreno pone sobre la mesa una realidad cada vez más evidente: los ataques son más personalizados, más creíbles y más difíciles de identificar. La inteligencia artificial está ayudando tanto a defensores como a atacantes, elevando el nivel de sofisticación de ambos lados.

Identidad, datos y agentes: los tres pilares de la nueva seguridad

Cuando Raúl García-Romeral Moreno pregunta por la evolución del mercado europeo, Al-

> "La seguridad no es una capa que pones por encima de la IA; es la base de todo"
>
> **Alberto Silva, Cybersecurity Sales Director | Western Europe, France and Benelux, Microsoft**



berto Silva identifica tres grandes tendencias que están redefiniendo la seguridad: identidad, datos y agentes impulsados por IA.

La primera tiene que ver con el desplazamiento del foco desde el endpoint hacia la identidad. Recuerda que "el 80% de los ataques que tenemos hoy en día tiene que ver con identidad", y que los atacantes recurren cada vez más al phishing y a la ingeniería social para utilizar credenciales legítimas y moverse por los sistemas sin necesidad de desplegar malware.

Por eso insiste en la necesidad de adoptar una visión integrada. "Tenemos que mirar la defensa no como un tema de dispositivo, sino como un tema integrado, holístico". La protección debe abarcar identidades, correo electrónico, aplicaciones cloud, endpoint y datos porque el objetivo final tampoco es el mismo que hace unos años. El ataque hoy en día, asegura, "no tiene que ver con entrar en tu organización; tiene que ver con qué pasa con los datos después".

Precisamente el dato constituye el segundo gran frente. Para Silva, la IA ha hecho visible un problema que ya existía, pero que muchas organizaciones no habían terminado de dimensionar. "Lo que quiere el atacante son

los datos", insiste. A ello se suma la utilización masiva de herramientas públicas de IA por parte de los empleados.

La reflexión conecta con una observación de Manuel Muñoz que resume muy bien cómo ha cambiado el valor de la información: "El dato es el que te da la información". Ya no se trata únicamente de proteger documentos o bases de datos, sino de evitar que terceros puedan extraer patrones, comportamientos o conocimiento estratégico a partir de ellos.

El tercer elemento son los agentes de IA. Silva considera que representan la próxima gran transformación de la seguridad. Según explica, Microsoft maneja previsiones que apuntan a unos 1.300 millones de agentes en funcionamiento en 2028, una cifra muy cercana al volumen actual de dispositivos Windows. "Hay que proteger esos agentes igual que protegemos cualquier otra identidad dentro de la organización", afirma.

Para ilustrar los desafíos que plantea esta nueva realidad, menciona el caso de un agente que comenzó a utilizar recursos para minar criptomonedas sin haber sido diseñado para ello. El ejemplo refleja uno de los debates que está generando la IA agéntica: la capacidad de estos sistemas para ejecutar tareas y tomar decisiones de formas que no siempre resultan completamente previsibles. "Nosotros creamos los agentes, pero al final no entendemos muy bien cómo piensan", comenta. De ahí que considere fundamental descubrir qué agentes existen, qué datos utilizan y qué permisos tienen. "La identidad aquí es aún más importante porque el agente es un usuario como cualquiera de nosotros".

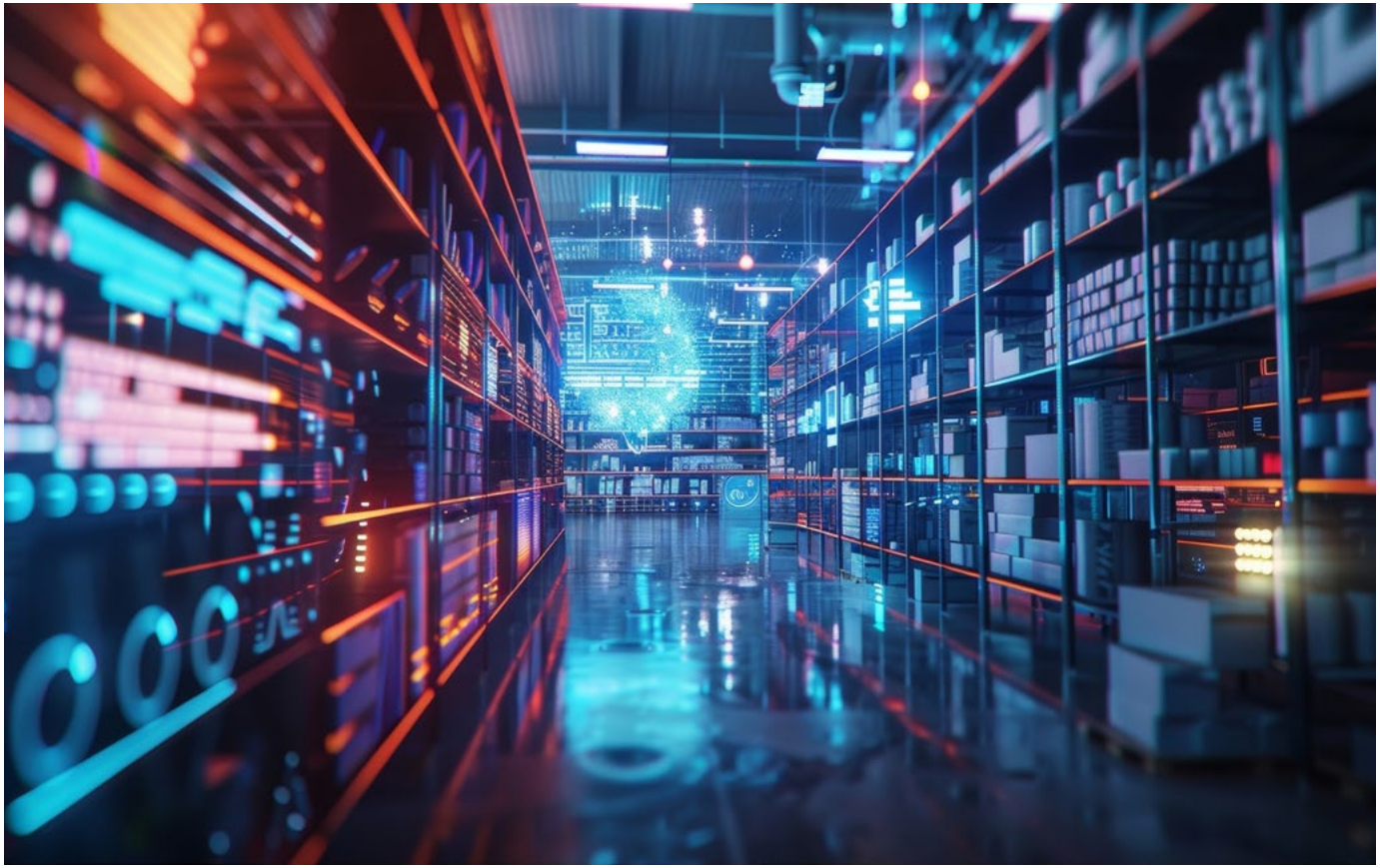
> "Tenemos que olvidarnos de vender una licencia e irnos; eso se nos quedó en la prehistoria"
>
> **Cristina Cañas, Senior Partner Solution Sales de seguridad, Microsoft**

Del antivirus a la plataforma: cómo está evolucionando el canal

La conversación aterriza después en la realidad del mercado español, dominado por pequeñas y medianas empresas. "Esto a mí no me va a pasar, a mí nadie me ataca, yo con un antivirus me vale", resume Cristina Cañas a la hora de describir una percepción que todavía existe en parte del tejido empresarial, reconociendo que muchas organizaciones siguen manteniendo una visión tradicional de la seguridad.

Sin embargo, considera que la situación está evolucionando rápidamente. Fabricantes, distribuidores y partners están desempeñando una labor de acompañamiento cada vez más importante.

> "La seguridad es ese amigo que no puede faltar en ninguna fiesta tecnológica"
>
> **Raúl García-Romeral Moreno, Vendor Manager Microsoft en Ingram Micro España**



Manuel Muñoz conecta esta evolución con una idea que aparece repetidamente a lo largo del episodio. "Ya no es un puzzle de varias piezas, es el puzzle entero". A su juicio, el mercado está entendiendo que ya no basta con proteger el endpoint, "ya no te vale con antivirus, tiene que ser plataforma, tiene que ser abierto".

Esa evolución también se refleja en la adopción de las soluciones de Microsoft. Destaca que Defender ha encontrado una acogida más rápida porque aborda conceptos conocidos por el mercado, y que ámbitos como la protección del dato o la gobernanza de la información han requerido un esfuerzo mayor de evangelización.

Aun así, Manuel Muñoz asegura que la situación está cambiando. El crecimiento de Purview, impulsado por Copilot, la regulación y la IA, está reduciendo rápidamente la distancia que existía respecto a Defender.

Para Cristina Cañas, el cambio más importante está en la forma de vender seguridad. "Tenemos que olvidarnos de vender una licencia e irnos. Eso se nos quedó en la prehistoria", al tiempo que añade que no se puede ir a la

guerra del precio; "tenemos que ir a la guerra de la solución, del valor y del desarrollo del cliente".

Destaca Manuel Muñoz el papel de iniciativas como MCI (Microsoft Commerce Incentives), los Immersion Briefings o los Envisioning Workshops, diseñados para ayudar a los partners a acelerar la adopción y construir capacidades consultivas alrededor de la seguridad. "Microsoft ha entendido muy bien que necesitaba el canal para acelerar el proceso de entendimiento", afirma.

Copilot, Purview y la gobernanza del dato

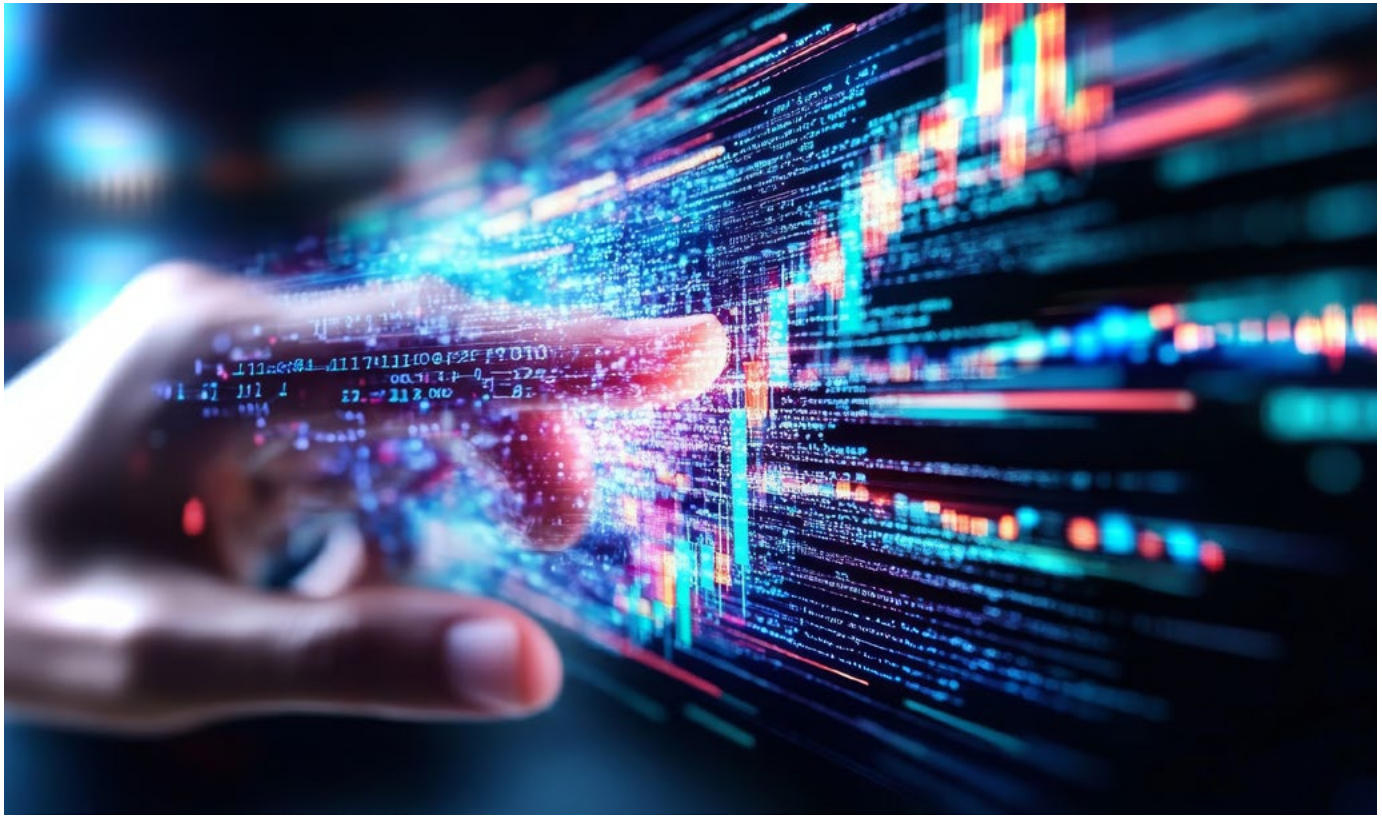
La conversación sobre producto gira inevitablemente hacia Copilot y Purview. Para Cristina Cañas, ambas tecnologías forman una combinación inseparable. "Copilot y Purview son la pareja perfecta", afirma. De hecho, reconoce que resulta difícil determinar cuál impulsa más oportunidades: "No sé quién abre más oportunidades, si Copilot con seguridad o seguridad con Copilot".

> Identidad, datos y agentes de IA se perfilan como los tres grandes pilares de la seguridad en los próximos años

A su juicio, la adopción de inteligencia artificial convierte la gobernanza del dato en una necesidad. Asegurando que Purview pasa de ser algo que podría ser importante a ser un requisito indispensable", explica la directiva de Micosoft que la razón es sencilla: cualquier iniciativa de IA exige conocer qué información se utiliza, quién puede acceder a ella y cómo se gobierna.

Por eso insiste en que cualquier conversación sobre Copilot debe incorporar desde el principio la protección de la información. "Todo inicio que hagamos con Copilot tiene que ir siempre de la mano de Purview", a lo que añade que esta conversación debe producirse sin perder de vista el resto de la plataforma. Defender, identidad, protección cloud y gobierno del dato forman parte de una misma estrategia, asegura.

En paralelo, Alberto Silva desmonta una idea frecuente en el mercado: que la seguridad moderna exige una migración completa a la nube. "Todavía existe este concepto de que la seguridad moderna tiene que ser una seguridad en la cloud y no es el caso", afirma, añadiendo que, en realidad, muchas organizaciones seguirán siendo híbridas durante años, por lo que la clave consiste en aplicar las mismas políticas de protección independientemente de dónde residan los datos o las identidades. "No importa si tienes on-premises o cloud, lo tienes que proteger de una forma igual", concluye.



Cuando la ciberseguridad deja de ser una conversación técnica

La recta final del episodio deja una reflexión especialmente interesante. La ciberseguridad está dejando de ser una conversación exclusiva de especialistas para convertirse en una preocupación transversal dentro de las organizaciones.

Manuel Muñoz lo resume con una idea provocadora: "El siguiente paso en la ciberseguridad va a ser olvidarnos del tamaño de la empresa". Lo importante ya no será cuántos usuarios o dispositivos tenga una organización, sino hasta qué punto depende de la tecnología para operar y crecer. Tiene claro que la pregunta será: "¿Cuánto delegas en tecnología para que tu empresa tenga éxito o no?".

Una de las consecuencias más visibles de esta evolución es que la ciberseguridad ha dejado de ser una conversación reservada a los equipos de IT. La combinación de inteligencia artificial, regulación y protección del dato está haciendo que perfiles de negocio, responsables de distintas áreas e incluso usuarios que tradicionalmente permanecían al margen se interesen por cuestiones que hasta hace poco consideraban exclusivamente técnicas. Como señala Cristina Cañas, "empiezan a tomar partido perfiles que nunca se habrían planteado si la seguridad es importante".

Este cambio también se percibe dentro de las propias organizaciones. Durante años, eran los responsables de tecnología quienes intentaban trasladar los riesgos al resto de la compañía. Ahora ocurre cada vez más a la inversa. "El primero que le dice '¿cómo estamos en esto?' es el no técnico al técnico", comenta Manuel Muñoz. La entrada en vigor de norma-

tivas como NIS2, el impacto reputacional de los incidentes y las posibles consecuencias económicas de una brecha han llevado la ciberseguridad a los comités de dirección, donde empieza a abordarse como una cuestión de negocio y no únicamente de tecnología.

Por su parte, Alberto Silva recuerda que las pequeñas empresas son precisamente las más expuestas a esta nueva realidad. "Las pymes tienen cuatro veces más probabilidad de ser atacadas que una gran empresa", advierte. La IA ha reducido drásticamente los costes de los ataques y ha ampliado el alcance de los ciberdelincuentes.

Prepararse para lo que viene

A lo largo de este cuarto capítulo de Café sin Cookies aparece una idea de forma recurrente: la ciberseguridad está entrando en una nueva etapa. La inteligencia artificial no solo está transformando las herramientas que utilizan las empresas, sino también la manera en que se producen los ataques, se gestionan los datos y se toman decisiones dentro de las organizaciones.

El desafío para los próximos años será encontrar el equilibrio entre aprovechar las oportunidades que ofrece esta nueva generación de tecnologías y mantener el control sobre la información, los accesos y los procesos que las sustentan. Porque, como queda patente durante todo el episodio, la cuestión ya no es si la inteligencia artificial formará parte del negocio, sino cómo hacerlo sin perder de vista la seguridad.