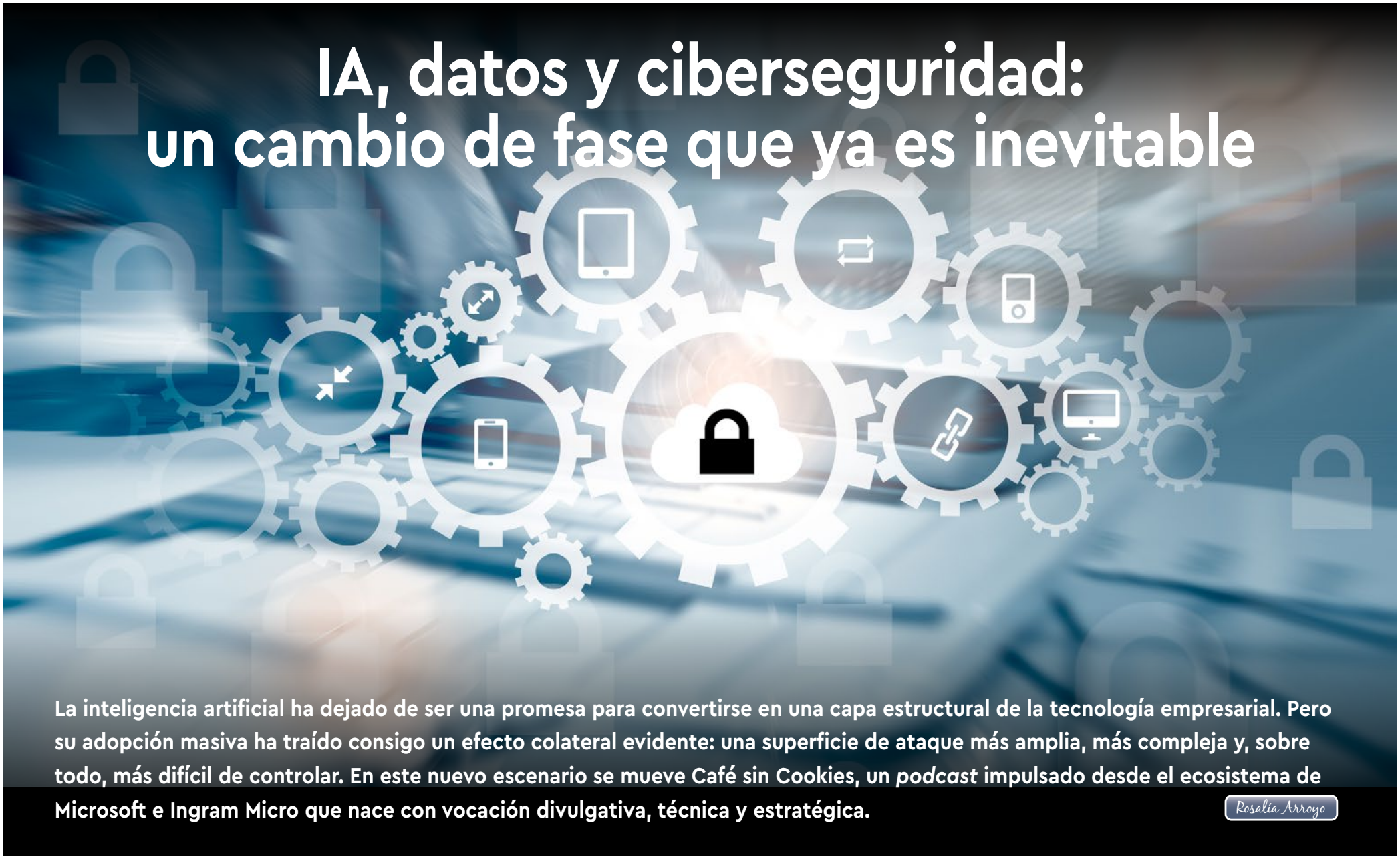
IA, datos y ciberseguridad: un cambio de fase que ya es inevitable



La inteligencia artificial ha dejado de ser una promesa para convertirse en una capa estructural de la tecnología empresarial. Pero su adopción masiva ha traído consigo un efecto colateral evidente: una superficie de ataque más amplia, más compleja y, sobre todo, más difícil de controlar. En este nuevo escenario se mueve Café sin Cookies, un *podcast* impulsado desde el ecosistema de Microsoft e Ingram Micro que nace con vocación divulgativa, técnica y estratégica.

Rosalía Arroyo

En este primer episodio participan Cristina Cañas Ávalos, responsable de PSS Seguridad en Microsoft; Manuel Muñoz Moreno, EMEA Microsoft *Security Vendor Manager* en Ingram Micro; y Raúl García-Romeral, *Vendor Manager* Microsoft en Ingram Micro España. El objetivo: analizar cómo están evolucionando la ciberseguridad, el papel de la inteligencia artificial y el valor de soluciones como Microsoft Defender y Microsoft Purview para *partners* y clientes finales.

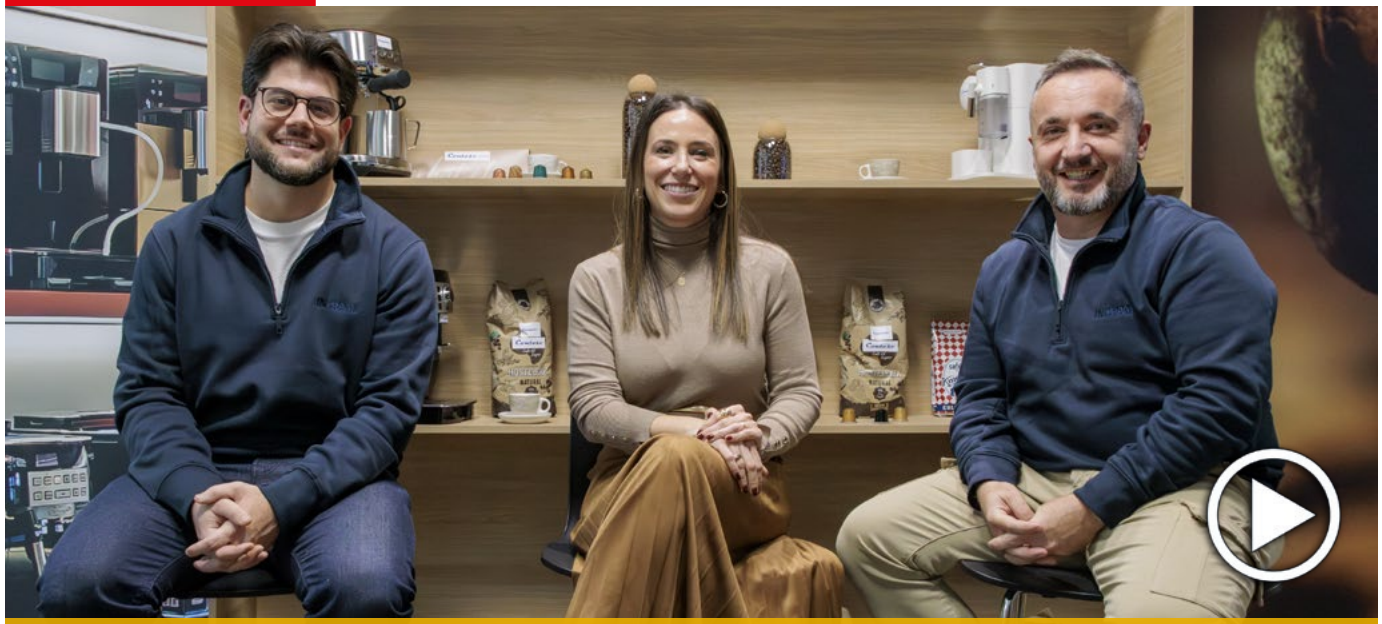
Lejos de una conversación centrada únicamente en producto, el diálogo se mueve entre contexto, experiencia práctica y lectura de mercado, con una idea transversal: ya no basta con reaccionar ante los incidentes; la seguridad debe ser predictiva, integrada y accesible para cualquier organización, independientemente de su tamaño.

IA: del arma del atacante al motor de la defensa

La conversación arranca con una constatación compartida: la inteligencia artificial "ha venido para quedarse" y lo hace acompañada de una avalancha de datos difícil de gobernar sin las herramientas adecuadas. Cristina Cañas subraya que el verdadero reto no es solo dónde residen esos datos, sino si están protegidos y bajo qué modelo de control. En ese contexto, la IA se convierte en un riesgo si no se integra desde el diseño en una estrategia de ciberseguridad sólida.

Raúl García-Romeral introduce una mirada histórica para poner en perspectiva el momento actual. Si hace 25 años ataques masivos como el virus ILOVEYOU golpeaban de forma indiscriminada, hoy la amenaza es radicalmente distinta: más selectiva, más con-

VER VÍDEO



Manuel Muñoz Moreno, EMEA Microsoft Security Vendor Manager en **Ingram Micro;**
Cristina Cañas Ávalos, responsable de PSS Seguridad en **Microsoft y**
Raúl García-Romeral, Vendor Manager Microsoft en **Ingram Micro España**

textual y mucho más orientada a explotar el comportamiento del usuario. El objetivo ya no es "atacar a todos", sino encontrar el eslabón más débil dentro de cada organización.

Frente a este escenario, la propuesta de Microsoft se apoya en un uso intensivo de la IA defensiva. Cristina Cañas recuerda que la compañía procesa decenas de billones de señales diarias para anticipar comportamientos maliciosos y ofrecer respuestas más rápidas y predictivas. La idea es clara: si los atacantes usan IA, la defensa no puede quedarse atrás.

> "Tenemos que pasar de una actitud reactiva a una totalmente predictiva, y eso sólo es posible entendiendo bien dónde están los datos y cómo se usan"
>
> **Cristina Cañas Ávalos, responsable de PSS Seguridad en Microsoft**

Microsoft Defender: de soluciones aisladas a una defensa unificada

Al entrar en el terreno de Microsoft Defender, el foco se desplaza hacia la necesidad de simplificar un ecosistema de seguridad tradicionalmente fragmentado. Cristina Cañas explica cómo Defender ha evolucionado hacia una *suite* unificada que integra capacidades que antes se contrataban de forma independiente: protección del *endpoint*, del correo, del entorno *cloud* o de las identidades.

Esta unificación no sólo reduce complejidad técnica, sino también barreras económicas. En la conversación se insiste en que la percepción histórica de Microsoft como una opción "cara" en seguridad ha cambiado de forma significativa, hasta situarse —según se comenta— con ahorros relevantes frente a otras alternativas del mercado cuando se analizan capacidades equivalentes.

Raúl García-Romeral aporta además una visión operativa: el valor de Defender está en que las herramientas "se hablan entre sí". Frente a modelos SIEM tradicionales, pensados para grandes organizaciones con *SOCs* dedicados, la seguridad integrada de Microsoft permite correlacionar señales de forma automática, anticiparse al incidente y reducir la dependencia del análisis puramente humano.

Del *endpoint* al multidispositivo: la seguridad ya no es estática

Otro de los ejes del debate es el cambio radical en la forma de trabajar. Hoy nadie opera desde un único dispositivo ni desde una única ubicación. La seguridad, por tanto, ya no puede limitarse al perímetro ni al correo electrónico. Microsoft Defender se concibe como un "guardián silencioso" que acompaña al usuario allí donde esté, desde cualquier dispositivo y red.

Manuel Muñoz insiste en que esta democratización de la seguridad es clave: ya no hay excusas para que las pymes queden fuera de modelos avanzados de protección. El ciberataque no entiende de tamaño y las necesidades básicas de defensa son las mismas para una empresa pequeña que para una gran corporación, aunque cambie la escala de la superficie de ataque.

Purview: proteger, gobernar y dar valor al dato

Si Microsoft Defender aborda el "cómo" se produce el ataque, Microsoft Purview se centra en el "qué" se protege: el dato. Cristina Cañas subraya que la gobernanza de la información se ha vuelto crítica, impulsada tanto por la adopción de la IA como por un entorno regulatorio cada vez más exigente.

Microsoftr Purview permite clasificar datos, aplicar políticas de cumplimiento y prevenir la pérdida de información de forma integrada. Pero, más allá de la protección, abre una oportunidad clara para el canal: los *partners* pueden construir servicios de valor añadido —auditorías, *assessments*, planes de madurez— que les permitan diferenciarse y acompañar estratégicamente a sus clientes.

> "La clave está en simplificar la complejidad y hacer accesible la seguridad avanzada a cualquier tipo de empresa"
>
> **Manuel Muñoz Moreno, EMEA Microsoft *Security Vendor Manager* en Ingram Micro**

Raúl García-Romeral lo resume con una idea sencilla: sin una correcta regularización del dato, cualquiera puede acceder a información crítica. Y en un mundo donde Copilot, Defender y Purview convergen, la seguridad y la privacidad dejan de ser capas separadas para convertirse en un todo coherente.

> "Si los atacantes usan inteligencia artificial, la única respuesta lógica es defenderse también con inteligencia artificial"
>
> **Raúl García-Romeral, *Vendor Manager* Microsoft en Ingram Micro España**

El papel del *partner*: evangelizar, acompañar y traducir

La parte final del *podcast* pone el foco en el ecosistema de *partners*. Todos coinciden en que el mayor reto no es tecnológico, sino de adopción. Los programas de incentivos, *workshops*, laboratorios prácticos y evaluaciones de seguridad se presentan como herramientas claves para ayudar al canal a entender, explicar y desplegar estas soluciones.

Cristina Cañas destaca la importancia de partir de lo que el cliente ya tiene y optimizarlo, mientras que Raúl García-Romeral insiste en la necesidad de hablar dos lenguajes: el del negocio y el técnico. Solo así se puede trasladar el valor real de la seguridad, no como un coste, sino como un habilitador del crecimiento.

Conclusión: seguridad integrada para un mundo impulsado por IA

El primer episodio de Café sin Cookies deja una conclusión clara: la ciberseguridad ha entrado en una nueva fase. La inteligencia artificial ha elevado tanto el nivel de la amenaza como el de la defensa, y solo los enfoques integrados, predictivos y accesibles permitirán a las organizaciones avanzar con confianza.

Microsoft Defender y Microsoft Purview no se presentan aquí como productos aislados, sino como piezas de una plataforma que busca simplificar la complejidad, proteger el dato y ofrecer valor real a clientes y *partners*.

En un entorno donde el ataque ya no es una posibilidad, sino una certeza, la pregunta no es si invertir en seguridad, sino cómo hacerlo de forma inteligente.