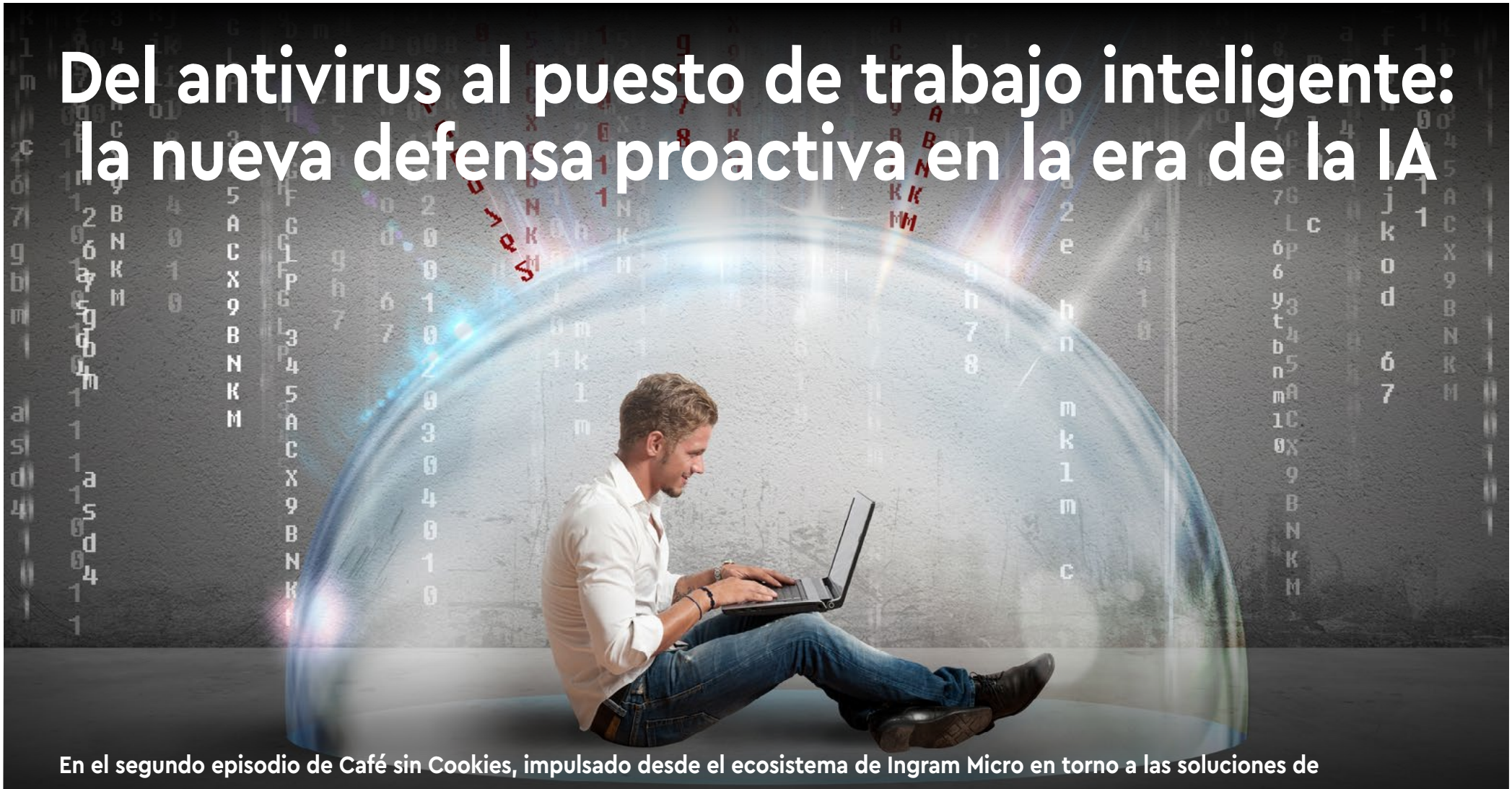
Del antivirus al puesto de trabajo inteligente: la nueva defensa proactiva en la era de la IA



En el segundo episodio de Café sin Cookies, impulsado desde el ecosistema de Ingram Micro en torno a las soluciones de ciberseguridad de Microsoft, el foco se desplaza desde la visión estratégica general hacia el núcleo operativo: el puesto de trabajo. Participan Manuel Muñoz Moreno, EMEA Microsoft Security Vendor Manager en Ingram Micro; Raúl García-Romeral Moreno, Vendor Manager Microsoft en Ingram Micro España; y Daniel Benítez Serrano, consultor especialista IT certificado en Microsoft 365. Rosalía Arroyo

La conversación arranca con una mirada retrospectiva que no es anecdótica. Recordar los tiempos del antivirus por firmas, los gusanos que reiniciaban equipos con sólo conectarse a Internet o los primeros intentos de protección integrada sirve para entender cuánto ha cambiado el escenario. Hoy el usuario ya no trabaja desde un único ordenador de sobremesa dentro de una red cerrada. Trabaja desde múltiples dispositivos, desde cualquier lugar y con una dependencia absoluta de la nube. Y eso ha transformado por completo la seguridad.

El mensaje de fondo no es alarmista, sino práctico: el modelo de defensa tradicional ya no es suficiente. La seguridad debe ser proactiva, integrada y adaptada a un entorno donde la inteligencia artificial juega en ambos bandos.

De los gusanos al ataque automatizado: cómo ha cambiado la amenaza

El recorrido histórico que plantea Raúl García-Romeral Moreno no es nostalgia tecnológica. Es una forma de evidenciar la transición desde ataques masivos y relativamente simples a amenazas mucho más sofisticadas y automatizadas. Si antes el foco estaba en el "virus" o el "troyano", hoy el problema es distinto: la automatización del ataque mediante IA permite dirigirse tanto a grandes corporaciones como a pymes con la misma facilidad.

VER VÍDEO

Raúl García-Romeral Moreno, Vendor Manager Microsoft en **Ingram Micro España;**
Daniel Benítez Serrano, consultor especialista IT certificado en **Microsoft 365 y**
Manuel Muñoz Moreno, EMEA Microsoft Security Vendor Manager en **Ingram Micro**

Daniel Benítez subraya que hemos pasado de protegernos de personas a protegernos de sistemas inteligentes capaces de generar campañas masivas, personalizadas y creíbles. La consecuencia es clara: ya no se trata de si una empresa es lo suficientemente grande como para ser objetivo, sino de si está preparada para cuando le toque.

Manuel Muñoz aporta una visión de mercado asegurando que el segmento SMB, especialmente relevante en España, ha entendido que la ciberseguridad no es un lujo ni un complemento, sino un requisito básico para poder adoptar nuevas tecnologías, incluida la inteligencia artificial. Sin una base sólida de seguridad, cualquier avance digital deja un hueco abierto.

> "La ciberseguridad de hace diez años no tiene nada que ver con la actual; hoy todo tiene que funcionar como una plataforma"
>
> **Manuel Muñoz Moreno, EMEA Microsoft Security Vendor Manager en Ingram Micro**

Defender Suite: proteger el dispositivo y el acceso a la nube

Cuando la conversación aterriza en Defender Suite, el enfoque cambia: ya no se habla de un antivirus tradicional, sino de una arquitectura pensada para un entorno híbrido. Daniel Benítez insiste en que limitar la seguridad al equipo del usuario es quedarse a medias. El puesto de trabajo actual combina endpoint, correo, colaboración y acceso a la nube, y todos esos vectores deben estar coordinados.

El día a día de cualquier profesional lo demuestra. La bandeja de entrada se llena de mensajes urgentes, archivos adjuntos y enlaces que exigen decisiones rápidas. En ese contexto, el phishing ya no es solo un correo mal escrito, sino campañas cada vez más creíbles, generadas incluso con inteligencia artificial, que explotan la prisa y la confianza del usuario.

Defender aborda ese escenario desde una doble capa: protege lo que ocurre en el dispositivo —descargas, conexiones, ejecución de archivos— y al mismo tiempo vigila el entorno de Microsoft 365, filtrando amenazas antes de que lleguen a convertirse en un problema real. La idea es reducir la exposición sin añadir fricción innecesaria al trabajo cotidiano.

Ahora bien, automatizar no significa desentenderse. Los participantes subrayan que la tecnología puede detectar y bloquear, pero necesita reglas claras, revisión constante y la intervención del equipo de IT para ajustar políticas y prioridades. La seguridad proactiva es una ayuda decisiva, pero sigue requiriendo dirección humana para ser verdaderamente eficaz.

Teletrabajo, dispositivos personales y el reto del control: el papel de Intune

El siguiente gran bloque de la conversación gira en torno a un cambio estructural: la normalización del teletrabajo. Desde la pandemia, el perímetro se diluyó. El puesto de trabajo ya

> "Cada perfil de usuario tiene un riesgo distinto; la clave es evaluar y entender dónde está tu punto débil"
>
> **Raúl García-Romeral Moreno, Vendor Manager Microsoft en Ingram Micro España**

no está en la oficina, y el empleado utiliza múltiples dispositivos, incluidos personales.

Aquí entra en juego Intune como herramienta de gestión de dispositivos (MDM). Recuerda Daniel Benítez que ya no hablamos sólo de proteger el ordenador corporativo, sino de gestionar qué ocurre cuando la información de la empresa convive en un teléfono personal junto a aplicaciones bancarias o fotos familiares. La capacidad de aplicar políticas, restringir aplicaciones, ofrecer soporte remoto o eliminar únicamente la información corporativa en caso de incidente se convierte en un elemento clave.

Raúl García-Romeral Moreno insiste en que cada perfil de usuario tiene un nivel de exposición diferente. Recursos Humanos, marketing o finanzas no enfrentan exactamente los mismos riesgos. Por eso la evaluación previa y el análisis de madurez son esenciales antes de decidir qué capas de protección implementar.

Seguridad como plataforma: el fin de las piezas aisladas

Manuel Muñoz introduce una idea central: la ciberseguridad ya no puede abordarse como un conjunto de piezas independientes. Endpoint, correo, identidad y gestión de dispositivos forman parte de un mismo ecosistema. Un correo protegido no sirve de mucho si el endpoint no lo está, y viceversa.

> "Security Copilot no sustituye al equipo técnico, pero es esa ayuda extra que acelera la respuesta cuando el tiempo es crítico"
>
> **Daniel Benítez Serrano, Consultor Especialista IT certificado en Microsoft 365**

Para el segmento SMB, esto tiene implicaciones directas. La eficiencia económica es importante, pero también lo es entender que ciertas capacidades ya no son opcionales. No se trata de elegir un módulo suelto, sino de adoptar una base mínima que permita sentirse razonablemente protegido y crecer desde ahí.

Daniel Benítez añade un elemento práctico: la complejidad del licenciamiento. Elegir correctamente el mix de licencias y soluciones requiere asesoramiento especializado. El valor del partner y del mayorista no está solo en vender tecnología, sino en ayudar a configurarla y dimensionarla correctamente.

Security Copilot: asistencia inteligente, no sustitución

La inteligencia artificial vuelve al centro del debate con Security Copilot. Daniel Benítez lo define como una capa intermedia que ayuda a correlacionar eventos, proponer acciones y acelerar la respuesta ante incidentes. No sustituye a un SIEM ni al equipo de IT, pero facilita la toma de decisiones cuando el tiempo es crítico.

Manuel Muñoz refuerza esta idea: en un entorno donde los incidentes pueden producirse a cualquier hora y desde cualquier ubicación, contar con una herramienta que ayude a interpretar rápidamente lo que está ocurriendo marca la diferencia. La intervención humana sigue siendo necesaria, pero ahora cuenta con apoyo inteligente.

El siguiente paso: el dato y la gobernanza

El episodio se cierra anticipando el siguiente gran bloque temático: la protección y gobernanza del dato con Purview. Manuel Muñoz apunta que, en un entorno donde la IA consume y correlaciona grandes volúmenes de información, el control sobre quién accede a qué y por qué se vuelve crítico.

No basta con proteger el acceso; hay que entender el flujo de datos, especialmente en entornos cloud. La seguridad del puesto de trabajo, la identidad y el dato forman parte de una arquitectura que debe funcionar de manera holística.

Lejos de un discurso alarmista, el mensaje final es claro: no se trata de generar miedo, sino de estar preparados. El puesto de trabajo ha evolucionado, el modelo de amenaza también y las herramientas disponibles lo han hecho en paralelo.