

# Purview y la nueva batalla por el dato: cómo la IA está obligando a replantear la gobernanza de la información

En esta nueva entrega de *Café sin Cookies*, el espacio promovido desde el entorno de Ingram Micro y Microsoft para analizar la evolución de la ciberseguridad y los nuevos entornos de trabajo, la conversación se centra en uno de los grandes desafíos que ha traído la inteligencia artificial a las empresas: el control y la protección de la información. En el debate participan Manuel Muñoz Moreno, EMEA Microsoft security vendor manager en Ingram Micro; Raúl García-Romeral, vendor manager Microsoft en Ingram Micro España; y David Hurtado, responsable de innovación en Microsoft.

Rosalía Arroyo

La conversación gira alrededor de cómo la IA está obligando a replantear la forma en la que las organizaciones gestionan, comparten y securizan sus datos. De hecho, ante la pregunta de Raúl García-Romeral sobre qué preocupa hoy más a las empresas —“¿la fuga, el caos o las penalizaciones legales?”—, David Hurtado reconocía que el gran problema actual es una mezcla entre sobrecompartición y cumplimiento regulatorio. “Ahora tú le haces una pregunta a la IA y la IA encuentra la información fácilmente y la expone”, advertía, al explicar cómo herramientas como Copilot han hecho visible un problema que durante años permanecía oculto dentro de las compañías. Tras dedicar episodios anteriores a la evolución de la seguridad y al papel de Defender en el puesto de trabajo, este nuevo encuentro pone el foco en Microsoft Purview y en la necesidad de entender la gobernanza del dato no como un proyecto aislado de IT, sino como una responsabilidad transversal que afecta a toda la organización.

## VER VÍDEO



**Manuel Muñoz Moreno**, EMEA Microsoft security vendor manager en **Ingram Micro**;  
**David Hurtado**, responsable de innovación en **Microsoft** y  
**Raúl García-Romeral Moreno**, vendor manager Microsoft en **Ingram Micro España**

### La IA acelera un problema que ya existía

Raúl García-Romeral abre buena parte de la conversación intentando aterrizar conceptos complejos a ejemplos cotidianos. Lo hace recordando cómo durante años apenas existía conciencia sobre el recorrido de la información dentro de las empresas. “¿Dónde va el dato?” era una pregunta

prácticamente inexistente en una época en la que copiar archivos o compartir información formaba parte de la rutina diaria sin demasiados controles.

Ahora, según explica David Hurtado, la situación es radicalmente distinta. La llegada de la IA generativa ha multiplicado la capacidad para localizar, correlacionar y exponer infor-

mación sensible dentro de una organización. Lo que antes requería conocer exactamente dónde estaba un documento o acceder manualmente a determinadas carpetas, hoy puede resolverse mediante una simple consulta en lenguaje natural.

En ese contexto, Raúl García-Romeral resumía Purview como una especie de "tutor legal de la inteligencia artificial", una capa de control que permite decidir qué información puede consumir la IA y bajo qué condiciones. Hurtado coincide con esa idea e insiste en que "la gobernanza del dato es cosa de todo el mundo", recordando que cualquier empleado con acceso a herramientas de IA puede llegar a información crítica si no existen controles adecuados.

## De la ciberseguridad clásica al cumplimiento regulatorio

Uno de los temas que aparece repetidamente durante el episodio es cómo la protección del dato ha dejado de ser una conversación exclu-

“Cuando despliegas IA a escala, el proyecto de gobernanza del dato deja de ser opcional”

David Hurtado, responsable de innovación, Microsoft

sivamente técnica. Manuel Muñoz explica que, durante años, la ciberseguridad se justificaba principalmente desde la amenaza externa: protegerse frente al ataque, evitar malware o blindar infraestructuras. Pero la situación actual añade una presión distinta: la regulatoria. Las empresas no sólo necesitan proteger la información; también deben demostrar que lo están haciendo correctamente. Normativas, auditorías y exigencias de compliance están empujando a muchas organizaciones a acelerar proyectos relacionados con gobierno del dato y clasificación de información. Aun así, Manuel Muñoz Moreno reconoce que el mercado todavía muestra diferencias importantes de madurez. Mientras conceptos

como protección del endpoint o seguridad del correo forman ya parte del lenguaje habitual de cualquier empresa, la protección del dato sigue percibiéndose en muchos casos como un proyecto asociado a la adopción de IA o al cumplimiento normativo. "Purview es ese producto que muchas compañías descubren que necesitan cuando empiezan a desplegar inteligencia artificial", resume durante la conversación.

Raúl García-Romeral introduce aquí otra reflexión interesante: la evolución de la IA está cambiando incluso la manera en la que se producen los ataques. Ya no se trata de amenazas masivas y genéricas, sino de ataques capaces de analizar comportamiento, rutinas

“Purview es ese producto que muchas empresas descubren que necesitan cuando empiezan a desplegar IA”

Manuel Muñoz Moreno, EMEA Microsoft Security vendor manager en Ingram Micro

y contexto para encontrar el punto más vulnerable dentro de una organización.

### **Purview: controlar el dato, el contexto y el acceso**

Cuando el debate aterriza en Purview, la conversación deja claro que el objetivo ya no es simplemente etiquetar documentos confidenciales. El reto es mucho más amplio: controlar el ciclo de vida de la información, saber quién accede a ella, desde dónde y con qué contexto.



David Hurtado introduce una idea especialmente relevante al explicar que la IA ha convertido cualquier documento en “dato explotable”. Antes, gran parte de la seguridad se concentraba en proteger bases de datos, aplicaciones o identidades. Ahora cualquier archivo puede ser utilizado, resumido o correlacionado automáticamente por una herramienta de IA, lo que obliga a trabajar concep-

tos como trazabilidad, permisos de extracción o “linaje de la información”, una capacidad que permite seguir el recorrido del dato y entender de dónde procede determinada información utilizada por la IA. Hurtado resume esa necesidad con una frase muy clara: “la seguridad tiene que estar en el documento”. Raúl García-Romeral complementa esa idea recordando que el usuario actual trabaja des-

de múltiples ubicaciones, dispositivos y servicios cloud. Por eso insiste en que Purview no puede entenderse como una herramienta aislada, sino como parte de un ecosistema más amplio de protección.

## El puzzle completo: identidad, dato y comportamiento

A medida que avanza el episodio, el concepto de plataforma gana protagonismo. Manuel Muñoz insiste en que la ciberseguridad ya no puede funcionar como un conjunto de piezas separadas. Defender protege dispositivos y comportamiento; Entra controla identidades; Purview gobierna la información; y las capacidades de IA ayudan a correlacionar señales y detectar anomalías.

La conversación deriva así hacia un modelo de seguridad mucho más contextual. Manuel Muñoz pone un ejemplo sencillo: un usuario puede tener permisos legítimos para acceder a un documento, pero si su comportamiento cambia, el dispositivo desde el que accede

“La gobernanza del dato no es un freno: es la base para trabajar con confianza”

Raúl García-Romeral, vendor manager Microsoft en Ingram Micro España

no es habitual o el contexto resulta anómalo, el sistema debe ser capaz de detectarlo.

Deja claro David Hurtado que la IA ha aumentado enormemente la complejidad porque conecta agentes, documentos, prompts y sistemas distintos. Y eso obliga a correlacionar toda la información de manera coordinada.

Raúl García-Romeral refuerza esa visión recordando que el usuario moderno ya no trabaja únicamente desde la oficina ni desde un único equipo. La seguridad, insiste, tiene que seguir al dato y al usuario allí donde estén.

## Del área de IT al comité de dirección

Otro de los cambios que refleja claramente el debate es el desplazamiento de estas

conversaciones desde IT hacia el negocio. En opinión de David Hurtado los proyectos relacionados con IA y gobernanza del dato ya no pueden plantearse únicamente como iniciativas tecnológicas.

De hecho, ante la pregunta de Raúl García-Romeral sobre quién debe liderar realmente este tipo de proyectos dentro de las compañías, Hurtado responde de forma directa: “el cliente interno no debe ser IT”. La razón es que el impacto afecta a *compliance*, legal, ciberseguridad y negocio al mismo tiempo. Según explica el directivo de Microsoft, muchas organizaciones empiezan implantando IA por razones de productividad o eficiencia, pero rápidamente descubren que necesitan

## La IA no creó el problema del dato, pero sí lo hizo visible

reforzar el control sobre la información para avanzar con seguridad. Y ahí es donde aparecen Purview y las políticas de gobernanza como piezas imprescindibles.

Manuel Muñoz añade además que este tipo de despliegues requieren una fase previa de análisis y *assessment* muy importante. Antes de implantar tecnología, insiste, es necesario entender cómo trabaja la empresa, dónde reside la información, qué riesgos existen y qué grado de madurez tiene la organización.

**Definitivamente, la gobernanza del dato deja de ser opcional**

El tercer episodio de Café sin Cookies deja



una idea clara: la inteligencia artificial ha acelerado un problema que llevaba años creciendo silenciosamente dentro de las empresas. La sobrecompartición de información, la falta de trazabilidad y el exceso de acceso a datos sensibles ya no son riesgos teóricos. Purview aparece aquí como una pieza clave dentro de una estrategia más amplia donde

identidad, comportamiento, dispositivos y dato deben funcionar de forma coordinada. Pero quizá la reflexión más importante del episodio sea otra: gobernar la información ya no es únicamente una cuestión de IT o compliance. En la era de la IA, se ha convertido en una responsabilidad transversal que afecta a toda la organización.