

¿Cuántos agentes hay en tu tenant?

Inventario y gobierno de agentes en Microsoft 365

Alejandro Araujo · Azure AI Architect · Microsoft Certified Trainer

ARROW TD SYNNEX V-Valley CMConsulting

PATROCINADORES

Gracias a nuestros patrocinadores

Gracias a quienes hacen posible que esto sea gratis y en abierto.





Sobre mí

Alejandro Araujo

- Arquitecto de IA en Azure y Microsoft Certified Trainer
- 11 años en Microsoft como Senior Cloud Solution Architect y Senior Customer Success Account Manager
- Miembro del AI CERTs Advisory Board
- Gobernanza de IA: EU AI Act, GDPR y nFADP suiza

Redes sociales:

LinkedIn: www.linkedin.com/in/a2araujo

araujoinnovations.ch

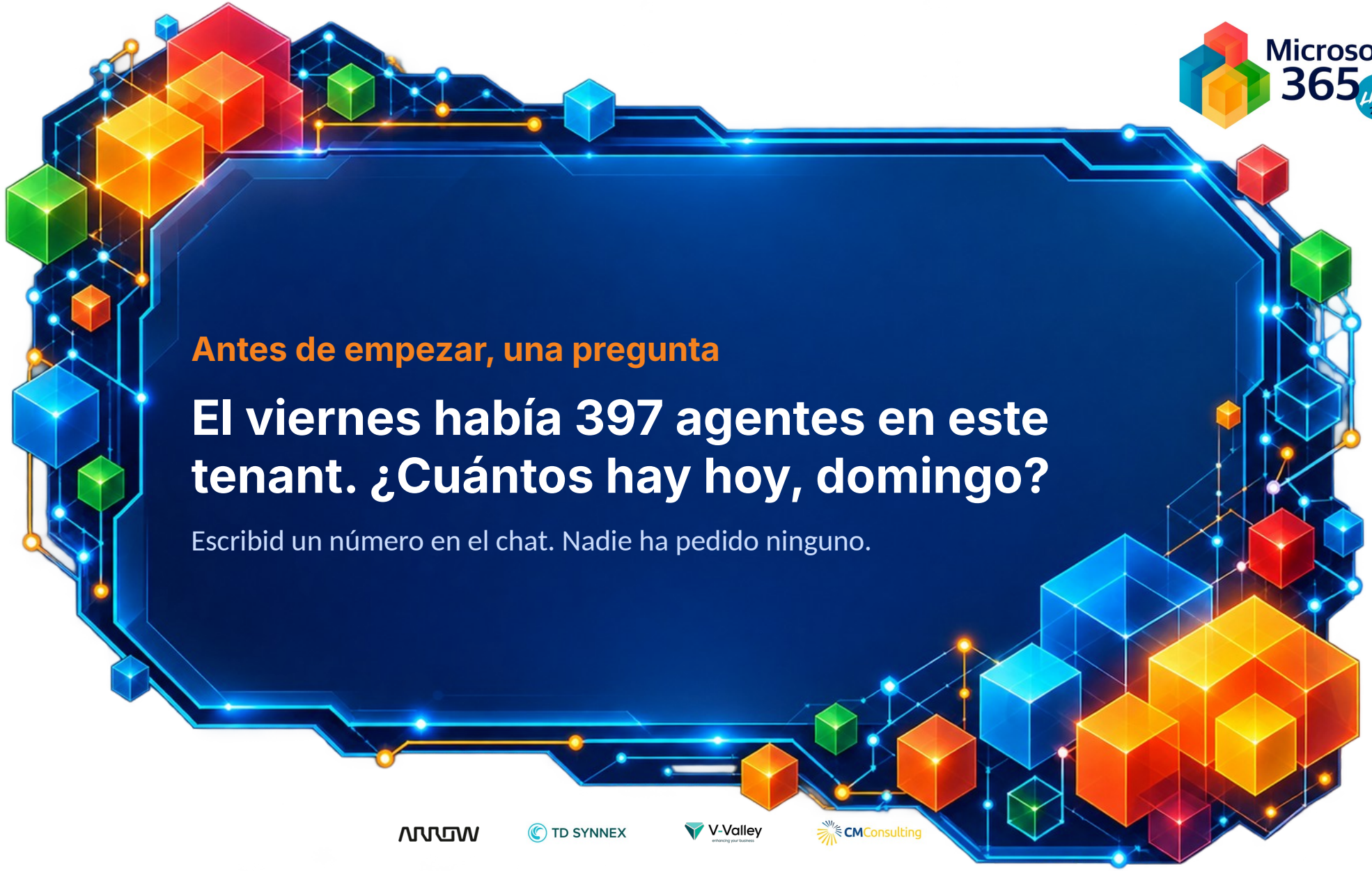
#GuardrailsFirst

#EternallyCurious

Microsoft 365 Live 4 al 8 de Noviembre del 2026

#M365live

100% Online y gratis



Microsoft 365 LIVE 2026

ARROW TD SYNNEX V-Valley CMConsulting

Microsoft 365 Live 4 al 8 de Noviembre del 2026

#M365live

100% Online y gratis

La respuesta

403

seis agentes nuevos en dos días; cuatro llegaron solos

Llegan solos: del marketplace, de Microsoft y de cualquier usuario con licencia. El inventario cambia cada día.



ARROW TD SYNNEX V-Valley CMConsulting

Microsoft 365 LIVE 2026

El auditor pregunta:

¿Cuántos agentes tenéis, quién responde de cada uno y qué pueden hacer?

¿Minutos, días o semanas? Respuesta al Q&A.

ARROW TD SYNNEX V-Valley CMConsulting

Agenda de la sesión



De dónde salen tantos agentes

Cinco tipos de agente y por qué se multiplican



El registro y la identidad

Agent 365 y Entra Agent ID, sin marketing



Tres demos en vivo

Registro, identidad y ciclo de vida



Clasificar y gobernar

Riesgo por agente, 90 días y el lunes





Microsoft 365 Live 4 al 8 de Noviembre del 2026

#M365live

100% Online y gratis

¿Por qué ahora?

Tres cambios que convierten el inventario en un problema

Cualquiera crea agentes

Agent Builder está en el chat de Copilot. Un usuario con licencia monta uno en cinco minutos y lo comparte con un enlace.

Los agentes actúan

Ya no solo responden: leen correo, crean tickets, mueven datos. Un agente con permisos es una identidad más.

Los terceros llegan solos

El marketplace publica agentes a diario. Canva, Jira, HubSpot o Harvey aparecen en el registro sin que nadie los pida.

Cinco tipos de agente en un tenant

Cuatro aparecen en el registro. El quinto, no.

Copilot Studio: agentes gestionados, con entorno, publicación y aprobación.

Agent Builder: agentes declarativos que crea cualquier usuario desde el chat de Copilot.

Foundry: agentes de desarrollo propio con modelos y herramientas.

Terceros: del marketplace o de plataformas conectadas.

El quinto:

apps con permisos de Graph y herramientas SaaS de IA que nadie registró.

Los cuatro que se ven en el registro

1 Copilot Studio

2 Agent Builder

3 Foundry

4 Terceros

Agent 365: el plano de control

Un registro, una identidad por agente y observabilidad

Registro: todos los agentes del tenant, vengan de donde vengan.

Entra Agent ID: cada agente con identidad propia, sponsor y permisos revisables.

Plataformas conectadas: Bedrock, Vertex, Agentforce, ServiceNow, Databricks, Snowflake.

Control de acceso, bloqueo y solicitudes de publicación en el mismo sitio.

Lo que enseña el registro

Total, sin dueño y en riesgo

Plataforma y tipo de publicador

Canal: Copilot, Teams, web

Usuarios activos y sesiones

Con quién está compartido

Último uso y última actualización

Etiquetas propias

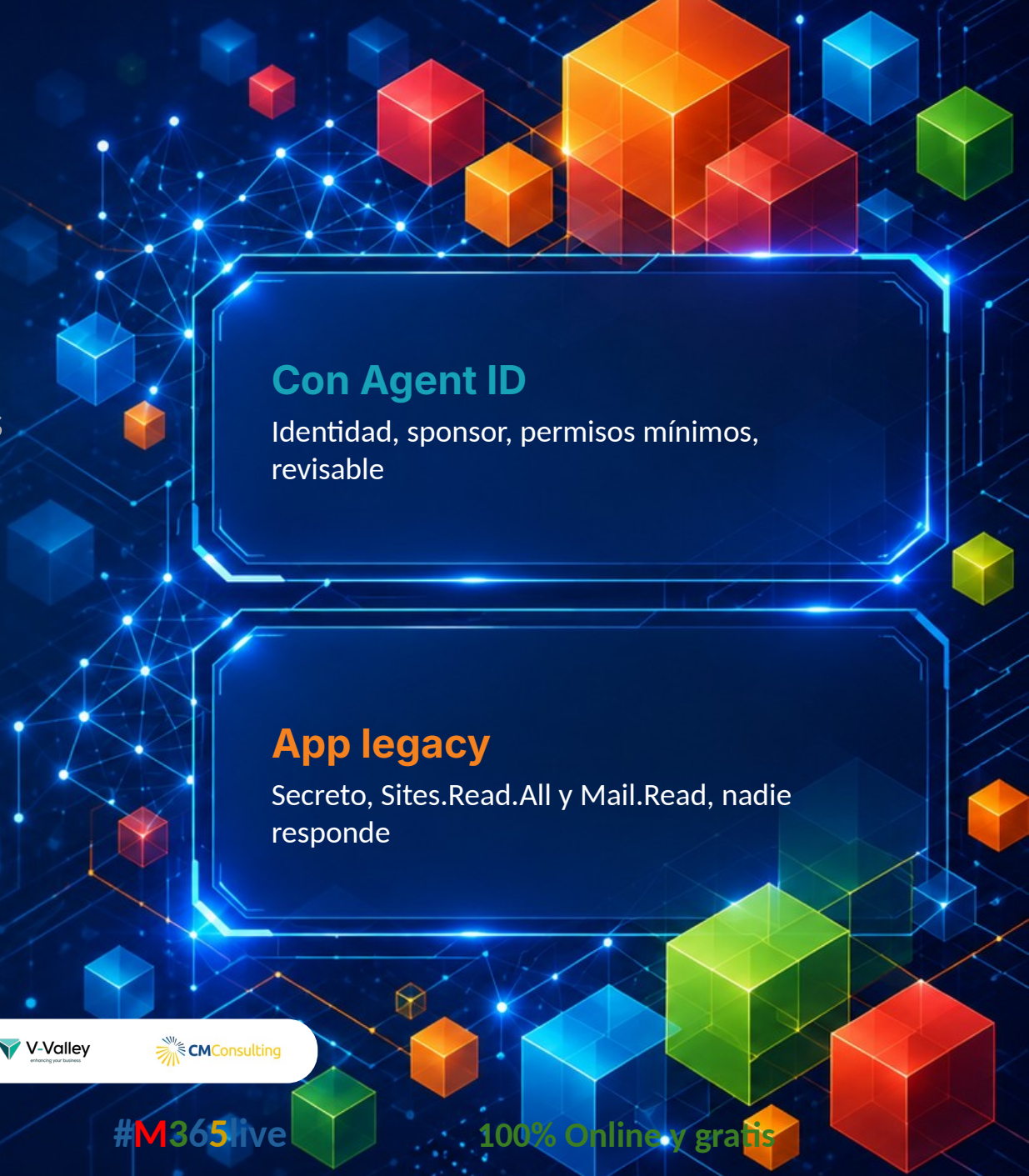
Export a CSV

Cada agente necesita una identidad

Un agente que actúa es una identidad más en Entra, igual que un usuario o un servicio.

Entra Agent ID le da identidad propia, sponsor, permisos acotados y revisión de acceso.

La alternativa de siempre: una app registration con un secreto y permisos de aplicación amplios. Sin dueño y sin caducidad.



¿Verdadero o falso?

Microsoft 365 LIVE 2026

1

Solo los agentes de Copilot Studio aparecen en el registro

2

Un agente que nadie usa no supone riesgo

3

Bloquear un agente lo elimina del tenant

Votad en el chat: Poned 1V o 1F (2V o 2F) así para cada una. Las respuestas salen en las demos.

ARROW TD SYNNEX V-Valley CMConsulting

Lo que el auditor ya pregunta

Seis preguntas sobre los agentes

Inventario

¿Cuántos agentes tenéis y en qué plataformas?

¿Cuáles son de terceros?

Identidad

¿Quién responde de cada uno?

¿Con qué permisos actúa cada agente?

Ciclo de vida

¿Quién aprueba que un agente llegue a toda la organización?

¿Cómo se retira uno?

Qué revela el registro y qué hacer

Señal	Dónde se ve	Qué hacer
Agentes sin dueño	Tile Agents without owners	Asignar dueño o bloquear
Agentes de terceros	Filtro Publisher type	Registro de proveedores y DPA
Compartido con toda la organización	Columna Shared with	Revisar alcance y aprobación
Sin uso en 90 días	Columnas Last used y Active users	Retirar
Solicitudes pendientes	Pestaña Requests	Aprobar con criterio o rechazar
Plataformas externas	Manage connected platforms	Conectar y ver sus agentes

Clasificar el riesgo de cada agente

Criterio	Riesgo bajo	Riesgo alto
Datos que alcanza	Un site público o general	Datos confidenciales o personales
Acciones	Solo responde	Ejecuta acciones: correo, tickets, pagos
Audiencia	Su creador o un equipo	Toda la organización o clientes
Decisiones sobre personas	Ninguna	Selección, evaluación, acceso a servicios
Proveedor	Microsoft o desarrollo propio	Tercero sin contrato de IA
Identidad	Agent ID con sponsor	App con secreto y permisos amplios

Contoso, dos días después

Microsoft, marketplace y los míos: HR Policy Assistant, Sales RFP Assistant y Finance FAQ

Copilot Studio, Agent Builder, terceros y una app registration legacy

El agente de RR. HH. espera aprobación para publicarse a toda la organización

El mismo tenant Microsoft 365 E7 del viernes. Empresa ficticia y datos de prueba, en inglés.

Demo 1

El registro: ¿cuántos y de quién?

- Total, sin dueño y en riesgo
- Filtrar por plataforma y tipo de publicador
- Un agente de terceros por dentro
- Export: el inventario en un CSV

Microsoft 365 admin center › Agents › Registry

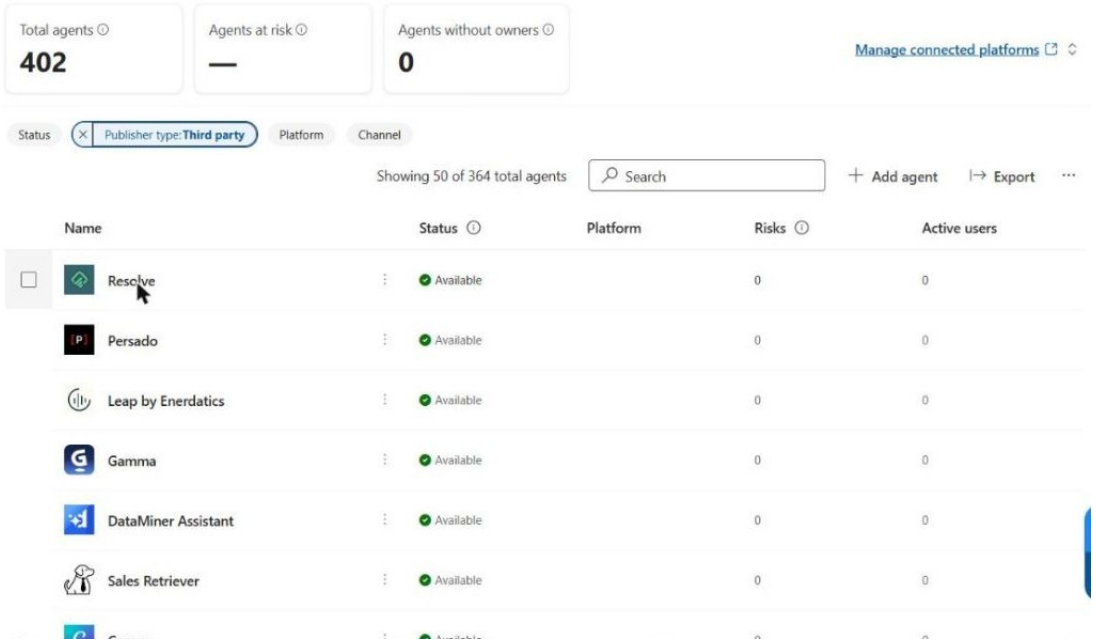
Demo 2

Identidad y permisos

- Entra Agent ID: identidades de agente y sponsor
- LegacyBot-Pilot: una app con secreto y permisos amplios
- La diferencia que verá un auditor

Entra admin center › Agent ID · App registrations

¿Qué falta aquí?



364 de los 403 agentes son de terceros: el marketplace publica a diario. El registro enseña lo que está publicado en el tenant.

No enseña lo que la gente usa en el navegador: ChatGPT, Manus, Gemini o cualquier SaaS con IA.

Eso se descubre con Defender for Cloud Apps y DSPM para IA, y se registra a mano en el inventario.

EN EL REGISTRO

FUERA DEL REGISTRO

Microsoft 365 LIVE 2026

La regla

Un agente sin dueño es un riesgo sin responsable

Si nadie responde de un agente, nadie lo revisa, nadie lo retira y nadie contesta al auditor.

Demo 3

Ciclo de vida: aprobar, bloquear, retirar

- Requests: aprobar el agente de RR. HH. para toda la organización
- Bloquear un agente desde el registro
- Políticas de datos en Power Platform
- DSPM para IA: qué hace cada agente

Admin center › Requests · PPAC · Purview › DSPM



El inventario mínimo de un agente

- ✓ Nombre, plataforma y publicador
- ✓ Dueño y sponsor con nombre y apellidos
- ✓ Propósito y audiencia
- ✓ Datos y fuentes de conocimiento que alcanza
- ✓ Acciones y permisos con los que actúa
- ✓ Identidad: Agent ID o app registration
- ✓ Nivel de riesgo y fecha de la evaluación
- ✓ Estado: piloto, producción, bloqueado, retirado



Seis errores frecuentes

Error	Mejor así
Contar solo los agentes de Copilot Studio	Registro completo: las cuatro plataformas y terceros
Inventario en un Excel que nadie actualiza	El registro como fuente y el Excel para lo que no se ve
Agentes sin dueño con nombre	Dueño y sponsor antes de publicar
Apps con secretos eternos para automatizar	Entra Agent ID y permisos mínimos
Aprobar solicitudes sin criterio	Nivel de riesgo y evaluación antes de aprobar
Bloquear y olvidar	Retirar, documentar y revisar cada trimestre

Hoja de ruta de 90 días

Descubrir, clasificar y gobernar

Días 1 a 30 · Descubrir

- Export del registro
- Apps con permisos de Graph
- Shadow AI con Defender for Cloud Apps
- Un dueño por agente

Días 31 a 60 · Clasificar

- Nivel de riesgo por agente
- Evaluación de impacto para los altos
- Retirar los que nadie usa
- Agent ID para los que actúan

Días 61 a 90 · Gobernar

- Aprobación con criterio
- Políticas de datos en Power Platform
- Revisión mensual del registro
- Carpeta de evidencias

El lunes por la mañana

Tres pasos para empezar:

1. Exportar el registro de agentes y contar.
2. Poner nombre y apellidos al dueño de los diez agentes con más uso.
3. Revisar las app registrations con permisos de aplicación y sin dueño.

Ante un auditor

Enseñar el registro, no el Excel

«Cada agente tiene dueño, identidad, nivel de riesgo y una fecha de revisión.»

Para llevar

Microsoft 365 LIVE 2026

Plantilla de inventario

Los campos mínimos por agente, lista para rellenar

Guía de clasificación

Seis criterios y tres niveles de riesgo

Contacto

LinkedIn: Alejandro Araujo · araujoinnovations.ch

Los descargables, en mi post de LinkedIn tras la sesión.

ARROW TD SYNNEX V-Valley CMConsulting

Gracias

Nos vemos en la comunidad.
Comparte la sesión y sigue la conversación con #M365Live

Alejandro Araujo

Preguntas al chat

#GuardrailsFirst
#EternallyCurious

