Guía de clasificación de riesgo de agentes

Inventario y gobierno de agentes en Microsoft 365 · Microsoft 365 Live 2026 · Alejandro Araujo

Seis criterios, de 0 a 2 puntos cada uno. La suma da el nivel: bajo (0 a 3), medio (4 a 6) o alto (7 a 12). Los criterios están alineados con la lógica de riesgo del AI Act europeo y con los objetivos A.4, A.5 y A.10 de ISO/IEC 42001. Úsela con la plantilla de inventario: las columnas R1 a R6 calculan el nivel.

1. Los seis criterios

Criterio	0 puntos	1 punto	2 puntos
R1 Datos que alcanza	Información pública o general	Datos internos de un equipo	Datos confidenciales, personales o financieros
R2 Acciones que ejecuta	Solo responde	Crea o modifica contenido en nombre del usuario	Ejecuta acciones en sistemas: correo, tickets, pagos, cambios de datos
R3 Audiencia	Su creador	Un equipo o departamento	Toda la organización o clientes externos
R4 Decisiones sobre personas	Ninguna	Recomienda o prioriza	Decide o filtra: selección, evaluación, acceso a servicios
R5 Proveedor	Microsoft o desarrollo propio	Tercero con contrato de IA y DPA	Tercero sin contrato de IA revisado
R6 Identidad	Agent ID con sponsor y permisos mínimos	Identidad delegada del usuario	App con secreto y permisos de aplicación amplios, o sin identidad

2. Qué exige cada nivel

Nivel	Puntos	Gobierno mínimo	Evidencia para el auditor
Bajo	0 a 3	Dueño con nombre. Revisión anual. Puede seguir el flujo de aprobación estándar.	Fila en el inventario con dueño y fecha de revisión
Medio	4 a 6	Dueño y sponsor. Aprobación documentada antes de publicar a toda la organización. Revisión semestral.	Registro de aprobación (Requests), inventario y política de datos aplicable
Alto	7 a 12	Evaluación de impacto antes de producción. Identidad con Agent ID y permisos mínimos. Contrato de IA si es de tercero. Revisión trimestral.	Evaluación de impacto firmada, revisión de permisos, contrato y extracto de DSPM para IA

3. Tres ejemplos

Agente	R1	R2	R3	R4	R5	R6	Total	Nivel
Asistente de políticas de RR. HH. (Copilot Studio, toda la organización, site general)	1	0	2	0	0	0	3	Bajo
Agente de ventas con acceso a la matriz de precios confidencial	2	0	0	0	0	0	2	Bajo
App legacy con Mail.Read y Sites.Read.All, sin dueño	2	2	0	0	0	2	6	Medio
Agente de terceros que filtra candidaturas con datos personales	2	1	2	2	2	1	10	Alto

Nota: el agente de ventas sale bajo por puntos y, aun así, en la sesión del viernes recuperó la matriz de precios. La puntuación ordena el trabajo; no sustituye a probar los controles.

4. Revisión mensual del registro, en diez minutos

Señal	Dónde se ve	Qué hacer
Agentes sin dueño	Tile Agents without owners	Asignar dueño o bloquear
Agentes de terceros nuevos	Filtro Publisher type	Registro de proveedores, contrato de IA 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 y documentar
Solicitudes pendientes	Pestaña Requests	Aprobar con la tabla de riesgo o rechazar
Apps con permisos de aplicación amplios	Entra > App registrations > API permissions	Dueño, caducidad del secreto o migración a Agent ID
Herramientas SaaS de IA en el navegador	Defender for Cloud Apps, DSPM para IA	Bloquear o aprobar con política de uso; añadir al inventario

El registro de agentes es la fuente; el inventario completa lo que el registro no ve. Un agente sin dueño es un riesgo sin responsable.