Checklist de evidencias para Copilot y agentes

ISO/IEC 27001:2022 e ISO/IEC 42001:2023 · Microsoft 365 Live 2026 · Alejandro Araujo

Use esta lista para preparar la carpeta de evidencias que pedirá el auditor. Marque cada punto cuando la evidencia esté reunida, fechada y guardada en una ubicación controlada.

1. Inventario y responsables

Hecho	Evidencia	Referencia
	Registro de sistemas de IA: cada agente y servicio de IA con dueño, sponsor, finalidad, fuentes de datos, nivel de riesgo y estado	27001 A.5.9 · 42001 A.4
	Export del registro de Agent 365 (Microsoft 365 admin center > Agents > All agents > Export)	27001 A.5.9
	Lista de agentes sin dueño y la acción tomada con cada uno	42001 A.3
	Plataformas de terceros conectadas y sus agentes	42001 A.10

2. Políticas e impacto

Hecho	Evidencia	Referencia
	Política de IA responsable aprobada y vinculada a la política de seguridad de la información	42001 A.2
	Método de evaluación de riesgos de IA (reutilizando el método del SGSI, documentado)	42001 cláusula 6.1
	Evaluación de impacto firmada para cada agente en producción	42001 A.5
	Declaración de aplicabilidad que cubra los dos Anexos A	27001 6.1.3 · 42001 6.1.3

3. Controles de protección de datos

Hecho	Evidencia	Referencia
	Política de etiquetas de sensibilidad e informe de uso de etiquetas	27001 A.5.12
	Política DLP para la ubicación Microsoft 365 Copilot, en modo On, con condición por etiqueta	27001 A.8.12 · 42001 A.7
	Política DLP para información sensible en los prompts de Copilot, en modo On	27001 A.8.11
	Resultados de la evaluación de sobrecompartido y riesgo de datos, con su corrección	27001 A.5.15 · 42001 A.7

4. Registro y monitorización

Hecho	Evidencia	Referencia
	Purview Audit activado y export de los registros CopilotInteraction del periodo auditado	27001 A.8.15
	Informes de DSPM para IA: interacciones, interacciones sensibles y uso de riesgo	27001 A.8.16
	Políticas de Insider Risk y Communication Compliance para IA, con registros de revisión	42001 A.9

5. Ciclo de vida y cambios

Hecho	Evidencia	Referencia

	Registros de aprobación para publicar agentes en la organización	42001 A.6
	Estrategia de entornos (desarrollo, pruebas, producción) para agentes	42001 A.6
	Registros de retirada de agentes eliminados o bloqueados	42001 A.6

6. Aseguramiento

Hecho	Evidencia	Referencia
	Export de Compliance Manager de las evaluaciones ISO/IEC 27001 e ISO/IEC 42001	27001 A.5.23
	Informe de auditoría interna que cubra los sistemas de IA	27001 · 42001 cláusula 9.2
	Actas de la revisión por la dirección que traten riesgos y objetivos de IA	27001 · 42001 cláusula 9.3

Microsoft 365 genera la evidencia técnica. Las políticas, las evaluaciones de impacto, la auditoría interna y la revisión por la dirección siguen siendo responsabilidad de la organización. La puntuación de Compliance Manager mide progreso; no es una certificación.