ISO 27001 + ISO/IEC 42001 en Microsoft 365

Gobernar Copilot y agentes con evidencias, no con promesas

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

www.araujoinnovations.ch

#GuardrailsFirst

#EternallyCurious

Microsoft 365 Live 4 al 8 de Noviembre del 2026

#M365live

100% Online y gratis



Microsoft 365 LIVE 2026

Microsoft 365 Live 4 al 8 de Noviembre del 2026

#M365live

100% Online y gratis

La respuesta

397

agentes en el registro del tenant de esta demo antes de crear el primero

Casi todos son de Microsoft y de partners. Ninguno tenía dueño en la organización ni revisión.



Mañana entra un auditor y pregunta:

¿Qué sistemas de IA tocan vuestros datos y dónde está la evidencia?

¿Minutos, días sta al chat.



Agenda de la sesión



Las dos normas, sin jerga

ISO 27001 e ISO/IEC 42001 en diez minutos



Del control a Microsoft 365

Qué capacidad genera cada evidencia



Tres demos en vivo

Compliance Manager, controles y evidencias



Errores y hoja de ruta

Lo que se puede hacer el lunes

¿Por qué ahora?

Tres cambios que ya se notan en las auditorías

Copilot hereda los permisos

Lo que un usuario puede abrir, Copilot lo puede resumir. El sobrecompartido de hace años aparece en un solo prompt.



Los agentes se multiplican

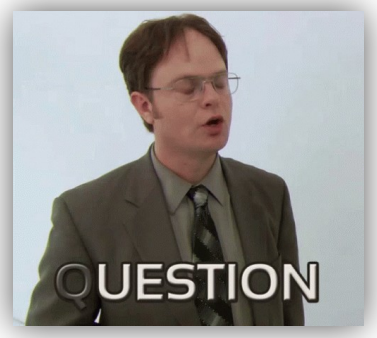
Copilot Studio, Agent Builder, Foundry y terceros. Cada agente es un sistema de IA con acceso a datos y, a veces, sin dueño.



ARROW TD SYNNEX V-Valley

Clientes y reguladores preguntan

Hay RFPs que ya piden evidencia de ISO/IEC 42001, y el AI Act europeo aplica obligaciones por fases hasta 2027.



CMConsulting

ISO 27001 en un minuto... más o menos

Un sistema de gestión de la seguridad: el SGSI

Se decide qué proteger, se evalúan riesgos, se eligen controles y se demuestra que funcionan. **Cada año.**

Cláusulas 4 a 10: el propio sistema de gestión.

La certifica una entidad acreditada: ciclo de 3 años con auditorías anuales.

Anexo A: 93 controles en 4 temas

37 organizativos

8 de personas

14 físicos

34 tecnológicos

ISO/IEC 42001 brevemente

Un sistema de gestión de la IA: el AIMS

Publicada en diciembre de 2023: la primera norma certificable de gestión de IA.

Pide evaluar los riesgos de la IA y el impacto de cada sistema en personas y organización.

Misma estructura que 27001: cláusulas 4 a 10.

Anexo A: 38 controles en 9 objetivos

A.2 Políticas de IA

A.3 Organización interna

A.4 Recursos de los sistemas de IA

A.5 Evaluación de impacto

A.6 Ciclo de vida

A.7 Datos para la IA

A.8 Información a partes interesadas

A.9 Uso de los sistemas de IA

A.10 Terceros

El AIMS se apoya en el SGSI

Las dos normas comparten las cláusulas 4 a 10.

Mismo método de riesgos, mismo control documental, misma auditoría interna y misma revisión por la dirección.

Se amplía el alcance del SGSI. No hace falta un programa paralelo.

ISO/IEC 42001 · AIMS

Impacto, ciclo de vida, datos para IA, uso y terceros

ISO 27001 · SGSI

Clasificación, accesos, DLP, registros y nube

¿Verdadero o falso?

Microsoft 365 LIVE 2026

1

Compliance Manager certifica a mi organización

2

ISO/IEC 42001 sustituye a ISO 27001

3

Si un fichero tiene etiqueta, Copilot no lo usa

Votad en el chat: V o F para cada una. Las respuestas salen en las demos.

Lo que el auditor ya pregunta

Seis preguntas sobre Copilot y agentes

Inventario

¿Qué sistemas de IA tenéis y quién es el dueño?

¿Cómo gobernáis la IA de terceros?

Datos

¿Qué datos alcanza cada agente?

¿Cómo frenan los datos confidenciales?

Pruebas

¿Dónde se registran prompts y respuestas?

¿Se evaluó el impacto antes de producción?

ISO 27001: controles conocidos, ahora con IA

Control	Capacidad de Microsoft 365	Evidencia
A.5.9 Inventario de activos	Registro de agentes, Entra Agent ID	Export del registro con dueños
A.5.12 Clasificación	Etiquetas de sensibilidad de Purview	Política de etiquetas
A.5.15 Control de acceso	Entra ID, acceso condicional, permisos	Revisiones de acceso
A.8.12 Fuga de datos	DLP de Purview para Microsoft 365 Copilot	Política en On y coincidencias
A.8.15 Registro	Purview Audit, DSPM para IA	Log de prompts y respuestas
A.5.23 Servicios en la nube	Compliance Manager	Evaluación y puntuación

ISO/IEC 42001: lo que añade la capa de IA

Objetivo	Capacidad de Microsoft 365	Evidencia
A.4 Recursos e inventario	Registro de agentes, inventario de Copilot Studio	Registro de sistemas de IA
A.5 Evaluación de impacto	Evaluación ISO/IEC 42001 en Compliance Manager	Evaluación de impacto firmada
A.6 Ciclo de vida	Entornos, publicación y aprobación	Registro de aprobaciones
A.7 Datos para la IA	Etiquetas, DLP para Copilot, DSPM	Evaluación de riesgo de datos
A.9 Uso de la IA	Communication Compliance, Insider Risk	Coincidencias y revisiones
A.10 Terceros	Plataformas conectadas, registro de proveedores	Proveedores con IA marcados

El entorno de la demo: Contoso

HR, Sales, Finance y Governance.
Salarios y precios: Highly Confidential

HR Policy Assistant y Sales RFP Assistant, en Copilot Studio

ISO 27001 e ISO/IEC 42001 en Compliance Manager

Construido en una tarde con Microsoft 365 E7. Empresa ficticia y datos de prueba, en inglés.

Demo 1

El SGSI y el AIMS, lado a lado

- Las evaluaciones ISO 27001 e ISO/IEC 42001
- Controles, acciones de mejora y responsables
- Lo que gestiona Microsoft y lo que nos toca

La puntuación mide progreso. El certificado lo da la entidad acreditada.



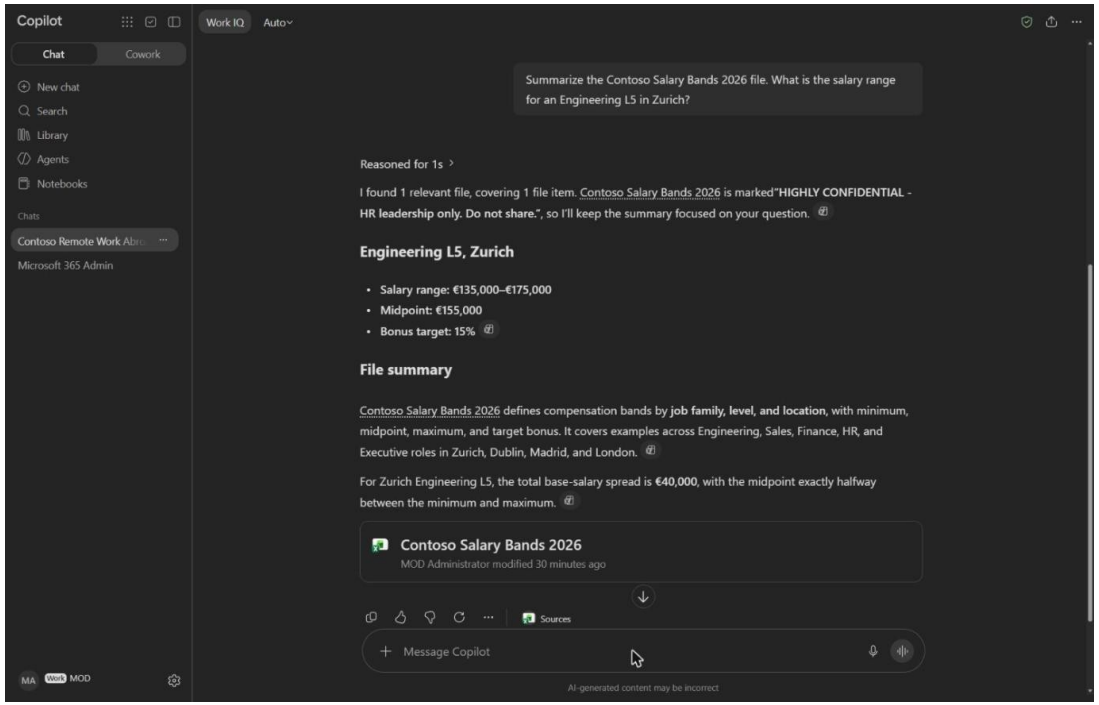
Demo 2

Los controles, en acción

- El agente de RR. HH. responde con citas
- Copilot frente a un fichero Highly Confidential
- Un número de tarjeta dentro del prompt

ISO 27001 A.5.12 y A.8.12 · ISO/IEC 42001 A.7

¿Qué falló aquí?



Ayer: etiqueta Highly Confidential, usuario con acceso y política DLP en modo simulación. Copilot resumió los salarios.

Hoy: política en On y sincronizada. A las 06:50, Copilot seguía resumiendo los salarios.

Lección: una política configurada no es una evidencia. La evidencia es la prueba que demuestra que bloquea.

ANTES

DESPUÉS

Microsoft 365 LIVE 2026

Lección del montaje

Las instrucciones de un agente no son un control

El agente de ventas recuperó la lista de precios. Solo sus instrucciones frenaron las cifras.

Demo 3

La carpeta que pedirá el auditor

- DSPM para IA: interacciones y riesgos
- Registro de agentes: dueño y estado
- Purview Audit: quién preguntó qué y cuándo

ISO 27001 A.5.9 y A.8.15 · ISO/IEC 42001 A.4 y A.6



La carpeta de evidencias

- ✓ Registro de sistemas de IA con dueño y riesgo
- ✓ Evaluación de impacto por agente
- ✓ Políticas de etiquetas y DLP en On
- ✓ Extracto del log de interacciones
- ✓ Registros de aprobación de agentes
- ✓ Export de Compliance Manager
- ✓ Proveedores con IA identificados
- ✓ Actas de revisión por la dirección

Seis errores frecuentes

Error	Mejor así
Un programa de IA aparte del SGSI	Ampliar el alcance, el método de riesgos y las auditorías
Contar solo los agentes de Copilot Studio	Inventariar todas las plataformas, también terceros
Etiquetas sin DLP para Copilot	Añadir la ubicación Microsoft 365 Copilot
Políticas en simulación para siempre	Revisar coincidencias y pasarlas a On
Agentes sin dueño	Dueño y sponsor antes de publicar
Confiar en las instrucciones del agente	Controles técnicos y registros

Hoja de ruta de 90 días

Descubrir, proteger y demostrar

Días 1 a 30 · Descubrir

- Activar Purview Audit
- Inventariar todos los agentes
- Un dueño por agente
- Publicar etiquetas

Días 31 a 60 · Proteger

- DLP para Copilot en On
- Corregir el sobrecompartido
- Políticas de uso de IA
- Aprobar agentes nuevos

Días 61 a 90 · Demostrar

- Evaluaciones 27001 y 42001
- Impacto por agente
- Carpeta de evidencias
- Auditoría interna

El lunes por la mañana

Quien llega nuevo a las ISO, tres pasos:

1. Abrir el registro de agentes y contar.
2. Mirar si la DLP para Copilot está en On o en simulación.
3. Preguntar quién es el dueño de los tres agentes principales.

Ante un auditor

Decirlo y, a continuación, enseñarlo

«El AIMS amplía el SGSI. Cada agente tiene dueño e impacto evaluado, y cada interacción queda registrada.»

Para llevar

Microsoft 365 LIVE 2026

Matriz de controles

27001 y 42001 frente a Microsoft 365 y su evidencia

Checklist de evidencias

Lo que hay que reunir antes de la próxima auditoría

Contacto

Los descargables, en el chat del evento y en mi post de LinkedIn tras la sesión.

Gracias

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

Alejandro Araujo

Preguntas al chat

#GuardrailsFirst
#EternallyCurious

