

## VI Congreso ISACA Iberoamérica

*Del 26 al 28 de mayo de 2026. Formato virtual*

### **IA Y RIESGOS DIGITALES**

Gobernar lo inesperado, proteger lo esencial.



*De la seguridad de la información a la seguridad de la inteligencia artificial. ¿Cómo prepararse?*

*Ing. Eva Hlušková, PhD., auditor de ciberseguridad, lead auditor ISO/IEC 27001, ISO/IEC 20000-1, ISO 22301, ISO 9001, miembro del consejo de ISACA Eslovaquia, CEO IQ ideas, s.r.o.*

## ¿Quién soy yo?

- ✓ **Auditor de los sistemas de gestión: 20 años**
- ✓ **Experiencia como copropietario de un organismo de certificación: 6 años**
- ✓ **Consultor de sistemas de gestión: más que 10 años**
- ✓ **Auditor de ciberseguridad (NIS, NIS2): 5 años**
- ✓ **más que 400 AD como LA ISMS (SGSI)**
- ✓ **aprox. 350 AD como LA de otros sistemas (BCMS, QMS, SMS):**
- ✓ **10 años de experiencia como DPO - responsable del (GDPR) RGPD**
- ✓ **Experto técnico de SNAS, Servicio Nacional de Acreditación de Eslovaquia en el ámbito de la seguridad de la información**



## **Introducción**

*Esta presentación está dirigida a todos los auditores, consultores y propietarios de empresas que ven la necesidad de gestionar los procesos de IA en relación con la gestión de la seguridad de la información.*

*Tras escuchar esta presentación, tendrá:*

- 1. una visión general de cómo incorporar la gobernanza de la IA en la seguridad de la información y cómo prepararse para la certificación en gobernanza de la IA*
- 2. descripción general de cómo realizar auditorías de seguridad de la información en relación con el uso y desarrollo de la IA*



# Audit y certificación de seguridad de la información, ciberseguridad y protección de la privacidad

## Empresa A

- La empresa utiliza agentes de IA para optimizar el trabajo, generar informes y estadísticas de gestión, y administrar la documentación interna y la base de conocimientos interna, buscando información disponible públicamente
- **posibles partes de audit centradas en la IA:** evaluación de los riesgos de seguridad de la información, *seguridad de la información en relación con los proveedores*, gestión de incidentes, continuidad del negocio, *instalación del SW*, inteligencia de amenaza (gestión de vulnerabilidades técnicas), gestión de activos, de identidad, de acceso, privacidad, derechos de propiedad intelectual



## Empresa B

- La empresa desarrolla y proporciona empleados de IA para que automatizan la atención al cliente, las ventas y las operaciones empresariales a través de IA de voz, chat e interfaces humanas digitales
- **posibles partes de audit centradas en la IA:** evaluación de los riesgos de seguridad de la información, inteligencia de amenaza (gestión de vulnerabilidades técnicas), gestión de activos, de identidad, de acceso, privacidad, derechos de propiedad intelectual, *seguridad en el ciclo de vida del desarrollo*, gestión de incidentes, continuidad del negocio



# Razones para integrar la seguridad de la información, la ciberseguridad y la gestión de la IA

sistemas de IA generan nuevos riesgos que ISO 27001 no cubre suficientemente

- bias / discriminación,
- prompt injection,
- riesgos de third-party AI,
- fuga del modelo,
- alucinaciones,
- toxic outputs, ...

preparación para el EU AI Act y futuras regulaciones

- EU AI Act,
- GDPR aplicado a IA,
- regulaciones sectoriales de IA,
- requisitos de clientes,
- requisitos de auditorías de sistemas IA

AI lifecycle governance

- Infraestructura segura,
- Gobernanza modelo,
- AI monitoring,
- Supervisión humana

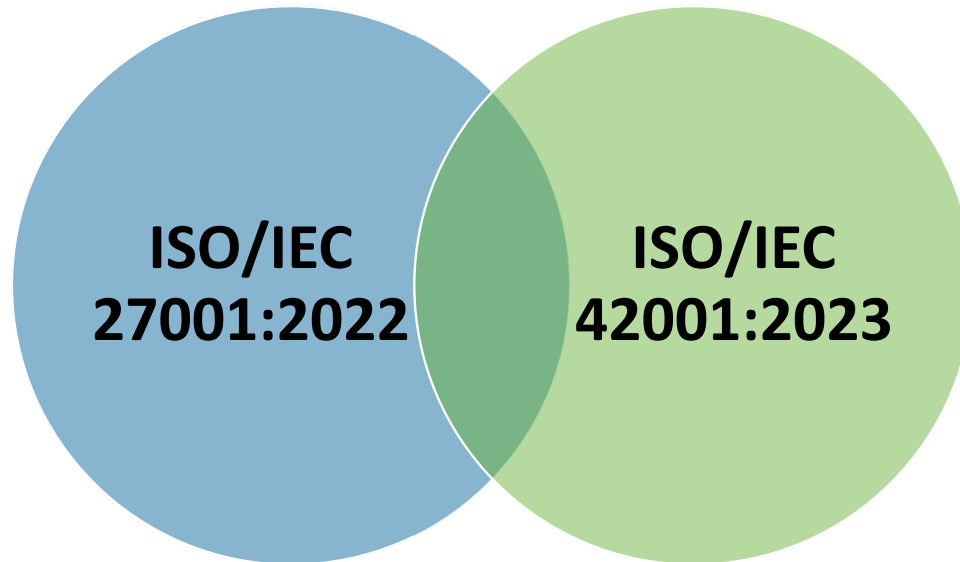
resultado de la combinación

- control de la IA de manera segura y ética,
- preparación para regulaciones IA,
- reducción de los riesgos IA,
- aumentar la confianza de clientes

## Comparación de los principales aspectos

Aspecto	ISO/IEC 27001:2022 (SGSI)	ISO/IEC 42001:2023 (SGIA)	Diferencia clave
<b>Propósito</b>	Proteger la confidencialidad, integridad y disponibilidad de la información (CIA)	Desarrollo y uso responsable de sistemas de IA	27001 – se centra en la información 42001 – en la gestión de la IA
<b>Anexo A</b>	Normativo – 93 controles	Normativo – 48 controles	Diferente naturaleza y uso
<b>Estructura principal</b>	4 dominios de control – A.5, A.6, A.7, A.8	10 áreas de control de IA – A.1-A.10	Diferente organización y enfoque
<b>Enfoque principal</b>	Seguridad de la información	Gobernanza de IA, riesgos, ciclo de vida, competencias	Diferente alcance
<b>Aplicación</b>	Se pueden tener exclusiones	Se pueden tener exclusiones	Diferente „Declaración de aplicabilidad“
<b>Certificación</b>	Certificable	<b>Certificable (ISO/IEC 42006:2025)</b>	Ambas normas son certificables
<b>Aplicación en la organización</b>	SGSI – protección de la información	SGIA – gestión responsable de sistemas de IA	Se complementan (las dos normas pueden ser integradas)
<b>Relación entre normas</b>	Puede ser base para al SGIA	Puede utilizar controles de ISO/IEC 27001:2022 (también se puede integrar con ISO 9001:2015, ISO/IEC 27701:2025 - sistema de gestión de información de privacidad)	Relación sinérgica

# Relación entre las normas



- ✓ Protección de la información
- ✓ Controles de seguridad
- ✓ Gestión de riesgos
- ✓ Controles físicos, personales y tecnológicos
- ✓ Enfoque de seguridad

- ✓ Gobernanza de IA
- ✓ Gestión de riesgos y ética de IA
- ✓ Ciclo de vida de IA
- ✓ Competencias y cultura de IA
- ✓ Mejora de sistemas de IA



# Pasos para integrar la gestión de IA a la seguridad de la información



# Integración de ISO/IEC 42001 e ISO/IEC 27001: pasos para implementación – como empezar



**Compromiso de la Alta Dirección:** la implementación de la norma ISO/IEC 42001 como complemento de la ISO/IEC 27001 debe ser una decisión de la dirección de la empresa



**Definir el alcance de la implementación de la norma ISO/IEC 42001**



**Realizar un análisis de brechas (GAP) entre los requisitos de implementación de la seguridad de la información y los requisitos de la norma ISO/IEC 42001 (capítulos 4-10, Anexo A)**



**Definir las excepciones del Anexo A para la IA (proporcionar justificaciones documentadas para excluir cualquier objetivo de control en general o para sistemas de IA específicos)**




**Considerar los requisitos legislativos para la implementación (Reglamento de IA, Reglamento general de protección de datos - GDPR, Ley de Derechos de Autor, ...)**

# Compromiso de la Alta Dirección



# Definir el alcance

## ISO/IEC 42001 – Ámbito (Scope)



Este documento ayuda a la organización a **desarrollar**, **proporcionar** o **usar** sistemas de IA de manera **responsable** para alcanzar sus **objetivos** y cumplir **requisitos, obligaciones** con las **partes interesadas** y sus expectativas.

1

### Organización que DESARROLLA IA



#### Ejemplos de IA que pueden usar:

- ✓ Crear modelos propios de IA (p. ej., predicción de demanda, detección de fraude).
- ✓ Entrenar modelos con datos de la organización.
- ✓ Integrar modelos de IA en sus productos o servicios.

2

### Organización que PROPORCIONA IA (a otros)



#### Ejemplos de IA que pueden usar:

- ✓ Ofrecer plataformas de IA como servicio (SaaS).
- ✓ Proporcionar APIs o modelos de IA a clientes.
- ✓ Operar asistentes virtuales, chatbots o motores de recomendación para terceros.

3

### Organización que USA IA (de terceros)



#### Ejemplos de IA que pueden usar:

- ✓ Usar herramientas de IA comerciales (p. ej., Copilot, ChatGPT, Gemini, asistentes de código).
- ✓ Análisis de documentos con IA (OCR, clasificación automática).
- ✓ Automatización de procesos (RPA + IA) con soluciones de terceros.



*Decida qué sistemas, productos y departamentos de IA están dentro del alcance.*

# Realizar un análisis de brechas (GAP)

## Comparación ISO/IEC 27001:2022 vs. ISO/IEC 42001:2023

### Capítulos 4 – 10 (Requisitos del sistema de gestión)

Capítulo	ISO/IEC 27001:2022	ISO/IEC 42001:2023	Diferencia principal
4 Contexto de la organización	Definición del contexto del SGSI, partes interesadas y alcance de la seguridad de la información	Definición del contexto del SGIA, partes interesadas de IA, riesgos e impactos de IA	42001 - considerar <b>el propósito previsto de los sistemas de IA</b> que son desarrollados, proporcionados o utilizados por la organización (roles relacionados con el sistema de IA)
5 Liderazgo	Liderazgo para el SGSI, política de seguridad, roles y responsabilidades	Liderazgo para SGIA, política de IA, gobernanza de IA y uso responsable	42001 - áreas de funciones y <b>responsabilidades</b> : evaluaciones de impacto de sistemas de IA, seguridad, privacidad, desarrollo, supervisión humana, relaciones con proveedores, requisitos legales
6 Planificación	Riesgos y oportunidades de seguridad de la información	Riesgos de IA, impactos de IA, objetivos de IA confiable	42001 - análisis de riesgos de IA, impactos de IA (evaluar las posibles <b>consecuencias para los individuos o grupos de individuos, o ambos, y las sociedades</b> que pueden resultar del sistema de IA a lo largo de su ciclo de vida), declaración de aplicabilidad
7 Soporte	Competencias, awareness, comunicación y documentación	Competencias en IA, awareness de IA y documentación del ciclo de vida de IA	42001 - exige <b>competencias específicas en IA</b> y transparencia
8 Operación	Operación del SGSI, tratamiento de riesgos y gestión de cambios	Riesgos de IA, evaluación del impacto de los sistemas de IA	42001 - <b>plan de tratamiento de riesgos de IA</b> , documento con los resultados de todas las <b>evaluaciones de impacto de los sistemas de IA</b>
9 Evaluación del desempeño	Monitoreo, auditorías internas y revisión por la dirección	Monitoreo, auditorías internas y revisión por la dirección de IA	42001 - establecer <b>auditorías internas</b> de acuerdo con SGIA
10 Mejora	No conformidades y mejora continua	No conformidades y mejora continua	42001 - incluye mejora adaptativa y madurez de gobernanza de IA



# ISO/IEC 27001:2022 vs. ISO/IEC 42001

## ISO/IEC 27001:2022

### Sistemas de gestión de la seguridad de la información

1	Objeto y campo de aplicación
2	Normas para consulta
3	Términos y definiciones
4	Contexto de la organización
5	Liderazgo
6	Planificación
7	Soporte
8	Operación
9	Evaluación del desempeño
10	Mejora

#### Anexo A (Normativo)

Controles de la seguridad de la información de referencia

## ISO/IEC 42001:2023

### Sistemas de gestión de IA

1	Objeto y campo de aplicación
2	Normas para consulta
3	Términos y definiciones
4	Contexto de la organización
5	Liderazgo
6	Planificación
7	Soporte
8	Operación
9	Evaluación del desempeño
10	Mejora

#### Anexo A (Normativo)

#### Anexo B (Normativo)

#### Anexo C (Informativo)

#### Anexo D (Informativo)

## ISO/IEC 27001:2022 – Anexo A (controles)



### A.5 Controles organizacionales

(37 controles)



### A.6 Controles de personas

(8 controles)



### A.7 Controles físicos

(14 controles)



### A.8 Controles tecnológicos

(34 controles)

**Declaración de aplicabilidad**

**definir las excepciones del Anexo A**

## ISO/IEC 42001:2023 – Anexo A (áreas de controles)



A.1 General (aplicabilidad)



A.2 Políticas relacionadas con la IA



A.3 Organización interna



A.4 Recursos para sistemas de IA



A.5 Evaluación de los impactos de los sistemas de IA



A.6 Ciclo de vida del sistema de IA (el desarrollo de sistemas de IA, ciclo de vida del sistema de IA)



A.7 Datos para sistemas de IA



A.8 Información para las partes interesadas de los sistemas IA



A.9 Uso de sistemas de IA



A.10 Relaciones con terceros y clientes

## Anexo B (guía de implementación para controles de IA)



Ejemplo de la „Empresa A“



## Empresa „A“ - según ISO/IEC 42001 solo “usa IA”



### Utiliza:

OpenAI ChatGPT,  
Microsoft Copilot,  
herramientas gráficas con IA,  
IA para traducciones,  
IA para análisis de campañas

no desarrolla modelos propios de IA,  
no proporciona IA a terceros,  
no es propietaria del modelo,  
no entrena modelos,  
no hospeda servicios de IA,  
únicamente usa IA en su trabajo diario

**Aunque la organización solo use IA, la norma sigue siendo aplicable.**

## Empresa „A“ - según ISO/IEC 42001 solo “usa IA”

Capítulo	Aplicación	¿Por qué?
<b>4 Contexto</b>	SÍ	La organización utiliza IA → existen riesgos relacionados con IA
<b>5 Liderazgo</b>	SÍ	Deben existir políticas y governance de IA
<b>6 Planificación</b>	SÍ	Se requiere evaluación de riesgos de IA y evaluación del impacto
<b>7 Soporte</b>	SÍ	Formación, awareness y competencias
<b>8 Operación</b>	SÍ	Procesos relacionados con el uso de IA
<b>9 Evaluación del desempeño</b>	SÍ	Monitoreo del uso de IA
<b>10 Mejora</b>	SÍ	Gestión de incidentes y mejora continua

### Documentos:

- Política de IA,
- Matriz de responsabilidades,
- Nombramiento de un gerente responsable del mantenimiento del sistema,
- **Análisis de riesgos de IA,**
- **Análisis de impacto de IA,**
- se puede crear un Manual del SGIA que describa estos capítulos del estándar 4-10 (integrado con seguridad de información)
- se puede usar SW para implementación

## Empresa „A“ - según ISO/IEC 42001 solo “usa IA”

Anexo	Aplicabilidad	¿Por qué?
A.2 Políticas relacionadas con la IA	SÍ	Se necesitan reglas para el uso de IA
A.3 Organización interna	SÍ	Roles y responsabilidades
A.4 Recursos	SÍ	Herramientas de IA y competencias
A.5 Evaluación de impactos	SÍ	Riesgos de IA sobre personas y negocio
A.6 Ciclo de vida del sistema de IA	PARCIALMENTE	Solo las partes relevantes para el “uso”
A.7 Datos	PARCIALMENTE	Datos introducidos en la IA
A.8 Partes interesadas	SÍ	Transparencia hacia clientes
A.9 Uso de sistemas IA	SÍ	Es el capítulo principal
A.10 Terceros y clientes	SÍ	Proveedores de IA (OpenAI, Microsoft...)

## Declaración de aplicabilidad – excepciones de ISO/IEC 42001

Artículo	Aplicabilidad	Motivo
<b>A.6.1 Desarrollo responsable de IA</b> 6.1.2 Objetivos para el desarrollo responsable del sistema de IA 6.1.3 Procesos para el diseño y desarrollo responsable de sistemas de IA	N/A o parcial	La empresa no desarrolla IA (aunque una organización no esté desarrollando un sistema de IA, puede tener requisitos definidos: objetivos y un proceso de desarrollo de IA, definiendo los requisitos para el proveedor)
<b>A.6.2 Lifecycle de desarrollo IA</b> <ul style="list-style-type: none"> <li>• Requisitos y especificaciones del sistema de IA</li> <li>• Documentación del diseño del sistema de IA</li> <li>• Verificación y validación del sistema de IA</li> <li>• Implementación del sistema de IA</li> <li>• Operación y monitoreo del sistema de IA</li> <li>• Documentación técnica del sistema de IA</li> <li>• Registro de eventos del sistema de IA</li> </ul>	N/A	No existe desarrollo de modelos, lo realiza el proveedor
<b>A.7.2 Datos para el desarrollo y la mejora de los sistemas de IA</b>	N/A	No existe desarrollo de modelos



# Empresa „A“ - según ISO/IEC 42001 solo “usa IA”

Hay que gestionar -  
por ejemplo al usar  
ChatGPT

¿los empleados pueden introducir  
datos personales?

¿pueden introducir código fuente?

¿quién aprueba las herramientas  
de IA?

¿qué prompts están prohibidos?

¿cómo se verifican los outputs  
generados por IA?

¿se requiere revisión humana?

# Empresa „A“ - según ISO/IEC 42001 solo “usa IA” - integración con la norma ISO/IEC 27001 (Anexo A – qué controles deben volver a analizarse)

ISO 27001 Anexo A	Qué debe añadirse para IA	Nuevos documentos/procesos
A.5.1 Políticas	Política IA	Responsible AI Policy
A.5.2 Funciones y responsabilidades	AI responsabilidades	Matriz RACI IA
<b>A.5.7 Inteligencia sobre amenazas</b>	Amenazas IA	AI threat landscape
A.5.8 Gestión de proyectos	AI governance en proyectos	AI project checklist
A.5.19 Seguridad del proveedor	Evaluación de proveedores IA	AI vendor due diligence
A.5.23 Servicios en la nube	Gobernanza IA SaaS	Reglas de uso cloud IA
A.5.24 Gestión de incidentes	Incidentes IA	AI plan de respuesta ante incidentes
<b>A.5.31 Requisitos legales</b>	AI Act, copyright, ethics	AI registro de cumplimiento
A.5.32 Propiedad intelectual	Contenido generado por IA	Reglas de propiedad
<b>A.5.34 Protección de la privacidad</b>	Datos personales en prompts	Prompt normas de privacidad
A.5.36 Conformidad	Auditorías AI gobernancia	Evaluación de cumplimiento de la IA

## A.5.7 Nuevo alcance del threat intelligence

Amenazas clásicas de SGSI	Amenazas específicas de IA	Shadow AI	Data Leakage
<p>Malware Phishing Ransomware Cloud compromise Insider threats Zero-day vulnerabilities Credential theft</p>	<p>Prompt injection <b>Data leakage</b> mediante prompts <b>Shadow AI</b> Alucinaciones AI misuse por empleados Unsafe AI outputs Adversarial prompts</p>	<p><b>Riesgo - los empleados utilizan:</b> ChatGPT no aprobado, plugins IA, extensiones IA del navegador, apps móviles IA,</p> <p><b>Qué debe añadirse:</b> registro de herramientas IA aprobadas, monitoring del tráfico IA, política de uso aceptable de la IA, detección de servicios IA no autorizados</p>	<p><b>Riesgo - datos sensibles se filtran mediante prompts IA</b> <b>Datos típicos:</b> datos personales, source code, contratos, datos HR, información financiera</p> <p><b>Qué debe añadirse</b> DLP para IA, clasificación de prompts, bloqueo de sensitive keywords, directrices de privacidad de la IA.</p>

## A.5.31 Legal , estatutario , reglamentario y requisitos contractuales

Área	Qué cubre ya ISO 27001	Qué debe añadirse para ISO 42001 / AI User	Documentos / evidencias
Requisitos legales	Registro de leyes, regulaciones y obligaciones contractuales	Añadir AI Act, GDPR en contexto IA, copyright, derecho del consumidor y requisitos sectoriales IA	AI Compliance Register
EU AI Act	Generalmente aún no cubierto en el SGSI	Determinar si la empresa es solo user/deployer IA, qué herramientas IA utiliza y si alguna entra en categoría high-risk	AI Act Applicability Assessment
Requisitos contractuales	Contratos con proveedores y clientes	Verificar si los contratos permiten uso de IA para tratamiento de datos de clientes o generación de outputs	Lista de verificación para la revisión de contratos de IA
Obligaciones regulatorias	Regulaciones de seguridad y privacy	Añadir obligaciones hacia reguladores, clientes y personas afectadas cuando se usa IA	Registro de obligaciones legales y reglamentarias
Requisitos éticos	Generalmente no tratados en detalle	Añadir principios de transparencia, fairness, no discriminación y human oversight	Política de IA responsable



## 5.34 Protección de la privacidad la información personal ( PII )

Área	Qué cubre ya ISO 27001	Qué debe añadirse para ISO 42001 / AI User	Documentos / evidencias
Protección de datos personales	GDPR, PII register, DPA y privacy controls	Reglas para datos personales en prompts y outputs IA	Normas de privacidad de la IA
Prompts	Normalmente no tratados como canal de datos independiente	Determinar si el prompt puede contener nombres, emails, historial cliente o datos HR	Prompt Privacy Standard
Proveedores IA	Supplier security y DPA	Verificar si el proveedor IA usa datos para entrenamiento, dónde procesa datos y cómo los almacena	Evaluación de la privacidad de los proveedores de IA
DPIA	DPIA para privacy risks	DPIA/AIIA para AI use cases con datos personales	AI DPIA / Impact Assessment
Retención de datos	Reglas de retención	Retención de prompts, logs, outputs y conversaciones	Política de retención de datos de IA

Declaración de aplicabilidad

## Empresa „A“ - según ISO/IEC 42001 solo “usa IA” - integración con la norma ISO/IEC 27001 (Anexo A – qué controles deben volver a analizarse)

ISO 27001 Anexo A	Qué debe añadirse	Ejemplo práctico
A.6.3 Conocimiento	Formación AI awareness	Riesgos de hallucinations
A.6.4 Proceso disciplinario	Misuse of AI	Introducción de datos sensibles en ChatGPT
A.6.7 Trabajo remoto	Uso IA desde casa	Uso de IA fuera del entorno corporativo

ISO 27001 Anexo A	Relevancia IA
Controles físicas - mayoritariamente mínima	Relevante solo si la infraestructura IA es on-prem

ISO 27001 Anexo A	Qué debe añadirse para IA	Ejemplo práctico
A.8.2 Acceso privilegiado	Accesos administradores IA	Gestión de tenants IA
A.8.7 Protección contra malware	Seguridad de plugins IA	Plugins IA no autorizados
A.8.9 Gestión de la configuración	Configuraciones IA	Ajustes de herramientas IA
<b>A.8.12 Prevención de fugas de datos</b>	Prompt leakage	Bloqueo de prompts sensibles
A.8.15 Logging	Logging IA	Logs de prompts
A.8.16 Monitoring	Monitoring misuse IA	Detección de Shadow AI
A.8.23 Web filtering	Governance de sitios IA	Plataformas IA autorizadas
A.8.31 Segregación	Entornos IA	Separación de sandbox IA

## A.8.12 Medidas para prevenir la fuga de datos (DLP)

DLP clásico – cubre ISO 27001	Riesgos	AI DLP	AI DLP riesgos
Protegemos emails	Email exfiltration	Protegemos prompts/bloqueo de sensitive prompts	Prompt leakage
Protegemos archivos	USB copy	Protegemos conversations	Prompt prohibido
Monitorizamos uploads	Cloud upload	Monitorizamos AI interactions (Detección PII)	Keyword detection
Cloud governance	File transfer	AI governance	AI plugin upload
Data exfiltration	SaaS leakage	User warnings	Real-time alerts



### ¿Qué cambia con la IA?

El prompt se convierte en un nuevo canal de datos (datos personales, source code, datos financieros, credentials, datos médicos).

Ejemplo de la „Empresa B“



# Empresa „B“ - según ISO/IEC 42001 “Desarrollador de IA”



Capítulo	Aplicación	Qué debe añadirse para ISO 42001 (AI Developer)	Nuevos documentos / procesos	Ejemplo práctico
4 Contexto	Sí	Contexto IA, AI lifecycle, AI impacts, stakeholders IA, scope AIMS incluyendo modelos, datasets y APIs	Análisis de contexto de IA Registro de partes interesadas en IA Inventario de sistemas de IA	El chatbot IA impacta clientes, Candidatos afectados por IA de contratación, Plataforma LLM
5 Liderazgo	Sí	Responsible AI leadership, roles de responsabilidad de la IA	Política de IA Matriz RACI de IA	AI Ethics Committee, Fairness y transparency rules
6 Planificación	Sí	Se requiere evaluación de riesgos de IA y evaluación del impacto, objetivos	<b>Análisis de riesgos de IA</b>	Hallucinations en IA generativa
7 Soporte	Sí	Formación, awareness y competencias (Skills ML, AI ethics, explainability)	Matriz de competencias de IA Programa de Sensibilización sobre IA	Formación ML engineer AI disclosures a usuarios
8 Operación	Sí	Procesos relacionados con AI ciclo de vida de las operaciones, riesgos y impacto	<b>AIIA - Análisis de impactos de IA</b> Registro de medidas de seguridad de la IA	Evaluación de bias Prompt filtering
9 Evaluación del desempeño	Sí	Monitoreo del uso de IA	Programa de auditoría de IA	Auditoría del modelo
10 Mejora	Sí	Gestión de incidentes y mejora continua	Gestión de incidentes de IA	Mitigación de bias



*“Debemos gestionar el comportamiento, impactos, seguridad, transparencia y lifecycle de la propia IA.”*



## Empresa „B“ - según ISO/IEC 42001 “Desarrollador de IA”

Anexo	Relevancia	¿Por qué?
A.2 Políticas relacionadas con la IA	SÍ	Se necesitan reglas para el desarrollo de IA
A.3 Organización interna	SÍ	Roles y responsabilidades
<b>A.4 Recursos</b>	SÍ	Herramientas de IA y competencias
<b>A.5 Evaluación de impactos</b>	SÍ	Evaluación del impacto del sistema de IA en individuos o grupos de individuos Evaluación de los impactos sociales de los sistemas de IA
<b>A.6 Ciclo de vida del sistema de IA</b>	SÍ	Es el capítulo principal
A.7 Datos	SÍ	Datos desarrollados y introducidos en la IA
A.8 Partes interesadas	SÍ	Transparencia hacia clientes
A.9 Uso de sistemas IA	SÍ	Proceso, objetivo y uso previsto de IA
<b>A.10 Terceros y clientes</b>	SÍ	Proveedores de IA (OpenAI, Microsoft...) y clientes – responsabilidades de desarrollo y uso de IA

# ISO/IEC 42001 – ANEXO A.4

## Recursos para sistemas de IA (Resources for AI systems)



El Anexo A.4 especifica los tipos de recursos que una organización necesita gestionar para poder desarrollar, operar, mantener y mejorar de forma continua los sistemas de IA de manera responsable.

Incluye: documentación de recursos, datos, herramientas (tooling), recursos del sistema y de cómputo, y recursos humanos.

### A.4 RECURSOS PARA SISTEMAS DE IA

#### A.4.1 GENERALIDADES



##### QUÉ SIGNIFICA

La organización debe identificar y gestionar todos los recursos necesarios para el ciclo de vida completo del sistema de IA.

- cubre todas las categorías de recursos
- garantiza su disponibilidad, idoneidad, seguridad y calidad
- permite la planificación, asignación, monitoreo y mejora de los recursos

##### EJEMPLO EN LA PRÁCTICA



Un banco identifica que para su modelo de IA de evaluación de crédito necesita datos, modelos, infraestructura tecnológica, herramientas de desarrollo y un equipo competente. Define, documenta y monitorea la disponibilidad de estos recursos durante todo el ciclo de vida del modelo.

#### A.4.2 DOCUMENTACIÓN DE RECURSOS (RESOURCE DOCUMENTATION)



##### QUÉ SIGNIFICA

La organización debe mantener información documentada de todos los recursos de IA.

- qué es el recurso y para qué se usa
- quién es el propietario / responsable
- versión, origen, dependencias
- ubicación, acceso y requisitos de seguridad
- cambios e historial

##### EJEMPLO EN LA PRÁCTICA



El área de TI mantiene un inventario de recursos de IA donde registra todos los modelos, conjuntos de datos, bases vectoriales, herramientas y servicios en la nube utilizados, incluyendo responsables, licencias, configuraciones y fecha de la última actualización.

#### A.4.3 RECURSOS DE DATOS (DATA RESOURCES)



##### QUÉ SIGNIFICA

Los datos utilizados por los sistemas de IA deben ser apropiados, representativos, seguros y gestionados durante todo el ciclo de vida.

- origen y calidad de los datos
- procesamiento, limpieza y etiquetado
- almacenamiento, acceso y protección
- retención y eliminación de datos
- datos para entrenamiento, validación, pruebas y operación

##### EJEMPLO EN LA PRÁCTICA



Una empresa de e-commerce utiliza datos históricos de compras del CRM, de la web y del call center para entrenar su modelo de recomendación. Los datos se anonimizaron, se limpiaron, se validaron y se almacenan en una plataforma de datos segura y controlada.

#### A.4.4 RECURSOS DE HERRAMIENTAS (TOOLING RESOURCES)



##### QUÉ SIGNIFICA

Incluye las herramientas de software y hardware, plataformas y aplicaciones necesarias para el desarrollo, operación y monitoreo del sistema de IA.

- herramientas de desarrollo (IDE, librerías, frameworks)
- plataformas de IA/ML y modelos preentrenados
- herramientas para gestión de datos y modelos
- herramientas MLOps (CI/CD, monitoreo)
- herramientas de seguridad
- licencias y versiones de herramientas

##### EJEMPLO EN LA PRÁCTICA



Un equipo de IA utiliza Python, PyTorch, MLflow para el seguimiento de experimentos, Docker para contenerización y Prometheus para monitoreo de modelos en producción. Todas las herramientas están documentadas con sus versiones y licencias.

#### A.4.5 RECURSOS DEL SISTEMA Y DE CÓMPUTO (SYSTEM AND COMPUTING RESOURCES)



##### QUÉ SIGNIFICA

Incluye la infraestructura de TI y los servicios necesarios para operar los sistemas de IA.

- capacidad de cómputo (CPU, GPU, TPU)
- almacenamiento (datos, copias de seguridad)
- redes y conectividad
- entornos cloud/on-premise
- sistemas operativos, bases de datos, middleware
- escalabilidad, alta disponibilidad y recuperación ante desastres
- monitoreo de infraestructura

##### EJEMPLO EN LA PRÁCTICA



Una startup despliega su asistente de IA en la nube (AWS). Usa instancias GPU para inferencia de modelos, S3 para almacenamiento de datos, RDS PostgreSQL para base de datos y CloudWatch para monitoreo y alertas.

#### A.4.6 RECURSOS HUMANOS (HUMAN RESOURCES)



##### QUÉ SIGNIFICA

La organización debe asegurarse de que las personas que realizan actividades relacionadas con sistemas de IA sean competentes y estén capacitadas para todas las funciones relevantes.

- roles y responsabilidades (p. ej., científico de datos, ingeniero de ML, propietario de IA, administrador de datos, especialista en seguridad)
- competencia y formación
- disponibilidad y asignación de capacidad
- apoyo al uso ético de la IA
- involucramiento de expertos en riesgos, legales, protección de datos y dominio del negocio

##### EJEMPLO EN LA PRÁCTICA



Una aseguradora cuenta con un equipo multifuncional: científico de datos que crea el modelo, ingeniero de ML que lo implementa, especialista de datos que garantiza la calidad de los datos, gestor de riesgos que evalúa los riesgos y experto legal que verifica el cumplimiento (GDPR, Ley de IA). Todos reciben formación continua sobre IA y ética.



#### RESUMEN

A.4 garantiza que los sistemas de IA se construyan y operen sobre recursos adecuados y gestionados correctamente – documentación adecuada, datos de calidad, herramientas apropiadas, infraestructura segura y personas competentes.

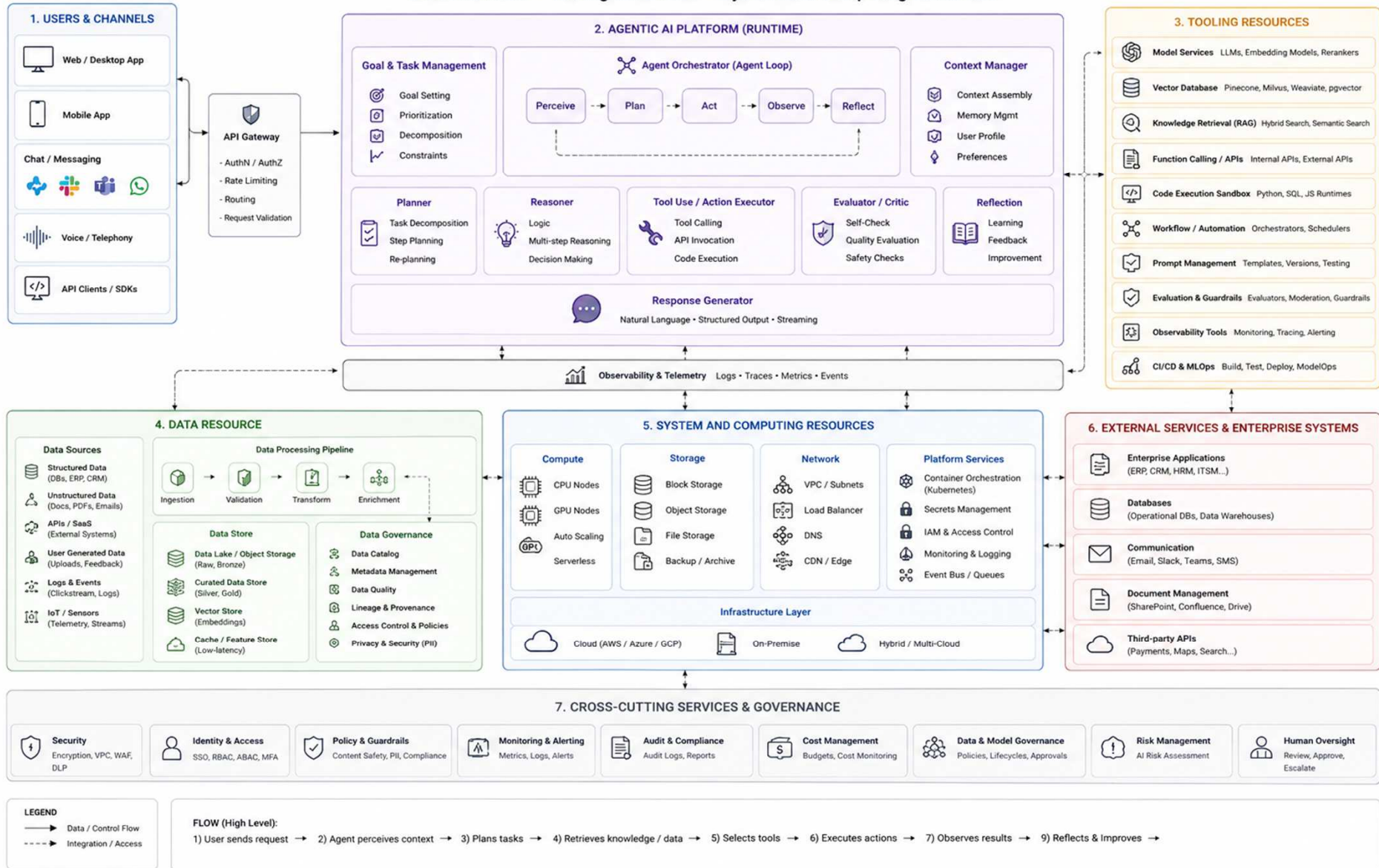


#### BENEFICIOS PARA LA ORGANIZACIÓN

Mejor control sobre el sistema de IA, menor riesgo, mayor calidad de las salidas, transparencia y cumplimiento de los requisitos de ISO/IEC 42001.

# AGENTIC AI ARCHITECTURE

Data Resource • Tooling Resources • System and Computing Resources






# ISO/IEC 42001 vs. ISO/IEC 27001 (integración)






## A.4 Recursos

ISO/IEC 42001	4.2 Documentación de recursos	4. 3 Recursos de datos	4.4 Recursos de herramientas / 4.5 Sistema y recursos informáticos	4.6 Recursos humanos
<b>ISO/IEC 27001</b>	<p>Información documentada</p> <p>Inventario de información y otros activos asociados</p> <p>Clasificación de la información</p> <p>Control de acceso</p> <p>Autenticación</p> <p>Derechos de propiedad intelectual (DPI)</p> <p>Privacidad y protección de datos de carácter personal (DCP)</p> <p>Documentación de procedimientos operacionales</p> <p>Acuerdos de confidencialidad o no divulgación</p> <p>Notificación de los eventos de seguridad de la información</p> <p>Acceso al código fuente</p> <p>Eliminación de la información</p> <p>Enmascaramiento de datos</p>	<p>Inventario de información y otros activos asociados</p> <p>Uso aceptable de la información y activos asociados</p> <p>Clasificación de la información</p> <p>Transferencia de la Información</p> <p>Control de acceso</p> <p>Seguridad de la información para el uso de servicios en la Nube</p> <p>Derechos de propiedad intelectual (DPI)</p> <p>Privacidad y protección de datos de carácter personal (DCP)</p> <p>Eliminación de la información</p> <p>Enmascaramiento de datos</p> <p>Uso de la criptografía</p> <p>Desarrollo seguro</p>	<p>Inventario de información y otros activos asociados</p> <p>Control de acceso</p> <p>Autenticación</p> <p>Seguridad de la información en las relaciones con los proveedores</p> <p>Seguridad de la información para el uso de servicios en la nube</p> <p>Gestión de incidentes</p> <p>Seguridad de la información durante la interrupción</p> <p>Derechos de propiedad intelectual (DPI)</p> <p>Gestión de privilegios de acceso</p> <p>Acceso al código fuente</p> <p>Gestión de vulnerabilidades</p> <p>Técnicas</p> <p>Registros de eventos</p> <p>Monitoringo</p> <p>Desarrollo seguro</p> <p>Gestión de cambios</p>	<p>Roles, responsabilidades y autoridades</p> <p>Competencia</p> <p>Concienciación (awareness)</p> <p>Controles de personas</p>
<b>posible conexión de artículos</b>	7.5, A.5.9, A.5.12, A.5.13, A.5.15, A.5.18, A.5.32, A.5.34, A.5.36, A.5.37, A.6.6, A.6.8, A.8.2, A.8.3, A.8.4, A.8.10, A.8.11, A.8.12, A.8.15, A.8.16, A.8.33	A.5.9, A.5.10, A.5.12, A.5.13, A.5.14, A.5.15, A.5.18, A.5.23, A.5.32, A.5.34, A.8.2, A.8.3, A.8.10, A.8.11, A.8.24, A.8.25-8.31	A.5.9, A.5.15, A.5.16, A.5.17, A.5.19, A.5.23, A.5.24-5.28, A.5.29, A.5.32, A.8.2, A.8.3, A.8.4, A.8.5, A.8.8, A.8.15, A.8.16, A.8.25-8.31, A.8.32	5.3, 7.2, 7.3, A.6

## COMPARACIÓN: ISO/IEC 27001 BIA vs. ISO/IEC 42001 AI IMPACT ASSESSMENT (ANEXO A.5)

PUNTO	ISO/IEC 27001 – BUSINESS IMPACT ANALYSIS (BIA)	ISO/IEC 42001 – IMPACT ASSESSMENT DE LOS SISTEMAS DE IA (A.5)
<p><b>1</b> OBJETIVO PRINCIPAL</p> 	<p>Identificar el impacto de interrupciones o fallos en la disponibilidad o seguridad de los procesos e información.</p> <ul style="list-style-type: none"> <li>• Enfoque en continuidad del negocio</li> <li>• Prioridades de recuperación</li> <li>• Resiliencia operacional</li> </ul>	<p>Identificar el impacto que puede tener el comportamiento de un sistema de IA en las personas, la organización, la sociedad y las regulaciones.</p> <ul style="list-style-type: none"> <li>• Enfoque en IA responsable</li> <li>• Gobernanza de riesgos de IA</li> <li>• Confianza y ética en la IA</li> </ul>
<p><b>2</b> ¿EN QUÉ SE ENFOCA?</p> 	<p>Se enfoca en procesos, servicios IT, aplicaciones, datos y su disponibilidad.</p> <ul style="list-style-type: none"> <li>• Procesos y servicios críticos</li> <li>• Disponibilidad, interrupciones y recuperación</li> <li>• Impacto financiero y operativo</li> </ul>	<p>Se enfoca en sistemas de IA, casos de uso, comportamiento de modelos y sus salidas.</p> <ul style="list-style-type: none"> <li>• Sesgos, equidad, ética y transparencia</li> <li>• Impacto en las personas y en la sociedad</li> <li>• Explicabilidad, supervisión humana y privacidad</li> </ul>
<p><b>3</b> PREGUNTAS TÍPICAS</p> 	<p>Responde preguntas como:</p> <ul style="list-style-type: none"> <li>• ¿Qué sucede si el sistema falla?</li> <li>• ¿Cuál es el impacto financiero?</li> <li>• ¿Cuánto tiempo puede estar indisponible?</li> <li>• ¿Cuál es el RTO/RPO?</li> <li>• ¿Qué procesos son críticos?</li> </ul>	<p>Responde preguntas como:</p> <ul style="list-style-type: none"> <li>• ¿Puede la IA discriminar?</li> <li>• ¿Puede la IA perjudicar al usuario?</li> <li>• ¿Es la IA explicable y transparente?</li> <li>• ¿Cuál es el impacto en la privacidad y en la sociedad?</li> <li>• ¿Puede la IA generar salidas inseguras o incorrectas?</li> </ul>

# COMPARACIÓN: ISO/IEC 27001 BIA vs. ISO/IEC 42001 AI IMPACT ASSESSMENT (ANEXO A.5)

PUNTO	ISO/IEC 27001 – BUSINESS IMPACT ANALYSIS (BIA)	ISO/IEC 42001 – IMPACT ASSESSMENT DE LOS SISTEMAS DE IA (A.5)
<p><b>4</b> ÁREAS DE EVALUACIÓN</p> 	 <p>Disponibilidad   Confidencialidad   Integridad   Impacto financiero   Continuidad del negocio   Reputación</p>	 <p>Sesgos y equidad   Explicabilidad y transparencia   Supervisión humana   Privacidad y datos   Impacto en las personas   Impacto social y ético</p>
<p><b>5</b> RESULTADOS DEL ANÁLISIS</p> 	<p><b>Resultados típicos:</b></p> <ul style="list-style-type: none"> <li>• Lista de procesos críticos</li> <li>• RTO / RPO y tolerancia a la interrupción</li> <li>• Mapa de dependencias</li> <li>• Estrategia de recuperación y prioridades</li> <li>• Planes de continuidad y recuperación</li> </ul>	<p><b>Resultados típicos:</b></p> <ul style="list-style-type: none"> <li>• Evaluación de impacto de IA</li> <li>• Registro de riesgos de IA y clasificación</li> <li>• Evaluación de sesgos y equidad</li> <li>• Evaluación de privacidad (DPIA de IA)</li> <li>• Plan de mitigación y controles de IA</li> <li>• Requisitos de supervisión humana y transparencia</li> </ul> 









# ISO/IEC 42001 – ANEXO A.6.1

## Ciclo de vida de los sistemas de IA – Guía de gestión para el desarrollo de sistemas de IA



### OBJETIVO:

Garantizar que la organización identifica y documenta los objetivos e implementa procesos para el diseño y desarrollo responsables de sistemas de IA.

CL.	TEMA	EXPLICACIÓN (QUÉ SIGNIFICA)	EJEMPLO PRÁCTICO
A.6.1.2	 <p><b>Objetivos para el desarrollo responsable de sistemas de IA</b></p>	<p>La organización debe identificar y documentar los objetivos que guían el desarrollo responsable de sistemas de IA, y considerar e integrar estos objetivos y medidas para alcanzarlos en el ciclo de vida del desarrollo.</p> <p><b>¿QUÉ SIGNIFICA?</b></p> <ul style="list-style-type: none"> <li>Los objetivos definen qué quiere lograr la organización con la IA (p. ej., seguridad, equidad, transparencia, protección de datos, fiabilidad, inclusividad).</li> <li>Los objetivos deben documentarse, comunicarse al equipo y considerarse en cada etapa del ciclo de vida.</li> <li>Deben apoyarse en principios concretos (p. ej., principios éticos, listas de verificación, pruebas, evaluación de impactos).</li> </ul>	 <p><b>EJEMPLO PRÁCTICO</b></p> <ul style="list-style-type: none"> <li>Una empresa desarrolla un sistema de IA para la evaluación automática de solicitudes de crédito.</li> <li>Define objetivos: toma de decisiones justa y no discriminatoria, protección de datos personales, explicabilidad de las decisiones, seguridad y fiabilidad.</li> <li>Documenta estos objetivos en su “Política de IA Responsable” y los comparte con el equipo de desarrollo.</li> <li>Integra medidas: utiliza pruebas de sesgo en los datos, mecanismos de explicabilidad, documentación de decisiones y un plan de monitoreo continuo.</li> </ul>
A.6.1.3	 <p><b>Procesos para el diseño y desarrollo responsable de sistemas de IA</b></p>	<p>La organización debe definir y documentar los procesos específicos para el diseño y desarrollo responsable de sistemas de IA.</p> <p><b>¿QUÉ SIGNIFICA?</b></p> <ul style="list-style-type: none"> <li>Deben establecerse pasos y actividades necesarios para un diseño y desarrollo responsable de sistemas de IA.</li> <li>Los procesos deben documentarse, ser comprensibles y utilizables por los equipos.</li> <li>Los procesos deben cubrir, por ejemplo: gestión de requisitos, gestión de datos, diseño del modelo, pruebas, evaluación de riesgos, validación, documentación, verificación y monitoreo.</li> </ul>	 <p><b>EJEMPLO PRÁCTICO</b></p> <p>La organización documenta su proceso de desarrollo de sistemas de IA para detección de fraudes en transacciones en línea.</p> <ul style="list-style-type: none"> <li>El proceso comienza con la recopilación y evaluación de datos (calidad, legalidad, sesgos).</li> <li>Luego sigue el diseño del modelo con enfoque en minimizar errores y sesgos.</li> <li>El modelo se prueba (rendimiento, robustez, seguridad) y se evalúa su impacto en los usuarios.</li> <li>Antes del despliegue, se realiza una evaluación de riesgos y validación.</li> <li>Después del despliegue, el sistema se monitorea regularmente y se actualiza según el proceso establecido.</li> </ul>
<p><b>¿POR QUÉ ES IMPORTANTE?</b></p> <div style="display: flex; justify-content: space-between;"> <div style="width: 25%;">  <p><b>Responsabilidad y confianza</b> Objetivos y procesos claros aumentan la confianza de los usuarios, clientes y reguladores en los sistemas de IA.</p> </div> <div style="width: 25%;">  <p><b>Reducción de riesgos</b> Ayuda a anticipar riesgos como discriminación, decisiones injustas, errores del modelo o violaciones de la privacidad.</p> </div> <div style="width: 25%;">  <p><b>Cumplimiento normativo</b> Facilita el cumplimiento de los requisitos de ISO/IEC 42001 y otras normas legales (p. ej., AI Act, GDPR, leyes de protección de datos).</p> </div> <div style="width: 25%;">  <p><b>Mejores decisiones y calidad</b> Procesos de calidad conducen a sistemas de IA más fiables, seguros, efectivos y preparados para un uso a largo plazo.</p> </div> </div>			
<p><b>EN RESUMEN</b></p> <p>A.6.1.2 requiere definir objetivos para el desarrollo responsable de sistemas de IA e integrarlos en todo el ciclo de vida. A.6.1.3 requiere definir y documentar procesos que garanticen un diseño y desarrollo responsables de sistemas de IA.</p>			



# ISO/IEC 42001 – ANEXO A.6.2

## Ciclo de vida de los sistemas de IA: criterios y requisitos por etapa

<p><b>A.6.2.2</b></p> <p><b>Requisitos y especificación del sistema de IA</b></p> 	<p><b>¿QUÉ SIGNIFICA?</b></p> <p>La organización debe definir y documentar los requisitos para nuevos sistemas de IA o mejoras a sistemas existentes.</p> <ul style="list-style-type: none"> <li>✓ Funcionales (qué hace el sistema)</li> <li>✓ No funcionales (rendimiento, seguridad, privacidad, ética)</li> <li>✓ Restricciones y límites de uso</li> </ul>	<p><b>EJEMPLO PRÁCTICO</b></p> <p>Una empresa que crea un asistente virtual define que debe responder solo con información aprobada, no almacenar datos sensibles y ser accesible 24/7. Documenta requisitos de precisión mínima (ej. 90 % de respuestas correctas) y límites de uso (no dar asesoría legal).</p> 
<p><b>A.6.2.3</b></p> <p><b>Documentación del diseño y desarrollo del sistema de IA</b></p> 	<p><b>¿QUÉ SIGNIFICA?</b></p> <p>La organización debe documentar el diseño y desarrollo según objetivos, requisitos y criterios de especificación.</p> <ul style="list-style-type: none"> <li>✓ Arquitectura del modelo y datos usados</li> <li>✓ Decisiones de diseño y justificaciones</li> <li>✓ Riesgos identificados y medidas adoptadas</li> </ul>	<p><b>EJEMPLO PRÁCTICO</b></p> <p>Una empresa documenta que su modelo de predicción de riesgo crediticio usa datos históricos, describe el algoritmo (XGBoost), variables utilizadas, criterios de selección de datos y cómo mitigó sesgos (balanceo de clases, exclusión de variables sensibles como género).</p> 
<p><b>A.6.2.4</b></p> <p><b>Verificación y validación del sistema de IA</b></p> 	<p><b>¿QUÉ SIGNIFICA?</b></p> <p>Definir y documentar medidas de verificación (cumplimiento de requisitos) y validación (adecuación al uso previsto) e indicar los criterios.</p> <ul style="list-style-type: none"> <li>✓ Pruebas técnicas (precisión, robustez, seguridad)</li> <li>✓ Validación con datos representativos</li> <li>✓ Aceptación según criterios definidos</li> </ul>	<p><b>EJEMPLO PRÁCTICO</b></p> <p>Antes de lanzar, la empresa prueba el modelo con datos de prueba, verifica sesgos por edad/género, realiza pruebas de estrés ante entradas atípicas y comprueba que cumple con la exactitud <math>\geq 90\%</math> y latencia máxima de 2 segundos.</p> 
<p><b>A.6.2.5</b></p> <p><b>Despliegue del sistema de IA</b></p> 	<p><b>¿QUÉ SIGNIFICA?</b></p> <p>Documentar un plan de despliegue y asegurar que se cumplan los requisitos antes del lanzamiento.</p> <ul style="list-style-type: none"> <li>✓ Plan de despliegue (entorno, fases, responsables)</li> <li>✓ Requisitos previos (seguridad, privacidad, aprobaciones)</li> <li>✓ Comunicación a usuarios y partes interesadas</li> </ul>	<p><b>EJEMPLO PRÁCTICO</b></p> <p>La empresa lanza el chatbot en producción primero para 10 % de usuarios (piloto), con checklist de seguridad completado, backup de datos, monitoreo habilitado y capacitación del equipo de soporte.</p> 
<p><b>A.6.2.6</b></p> <p><b>Operación y monitoreo del sistema de IA</b></p>  <p><b>¿QUÉ SIGNIFICA?</b></p> <p>Definir y documentar operaciones mínimas:</p> <ul style="list-style-type: none"> <li>✓ Monitoreo del rendimiento en uso</li> <li>✓ Reparaciones, actualizaciones y soporte</li> <li>✓ Alertas e incidentes</li> </ul> <p><b>EJEMPLO PRÁCTICO</b></p> <p>Se monitorea la precisión del modelo en producción diariamente; si baja del 90 %, se genera alerta, se revisan datos y se reentrena el modelo.</p> 	<p><b>A.6.2.7</b></p> <p><b>Documentación técnica del sistema de IA</b></p>  <p><b>¿QUÉ SIGNIFICA?</b></p> <p>Mantener documentación técnica para cada categoría de partes interesadas (usuarios, socios, supervisores, auditores, equipo de soporte) en formato apropiado.</p> <p><b>EJEMPLO PRÁCTICO</b></p> <p>Se prepara guía para usuarios (cómo usarlo), documento técnico para TI (arquitectura, APIs, configuración) y reporte para reguladores con métricas y controles.</p>	<p><b>A.6.2.8</b></p> <p><b>Conservación de registros de eventos del sistema de IA</b></p>  <p><b>¿QUÉ SIGNIFICA?</b></p> <ul style="list-style-type: none"> <li>✓ Determinar qué eventos del ciclo de vida deben registrarse y durante cuánto tiempo.</li> <li>✓ Registros mínimos cuando el sistema está en uso.</li> </ul> <p><b>EJEMPLO PRÁCTICO</b></p> <p>Se guardan logs de predicciones, decisiones, versiones del modelo, cambios de datos y acciones de administradores durante 24 meses para auditorías y trazabilidad.</p> 



**BENEFICIOS**



Transparencia y trazabilidad en todo el ciclo de vida.



Cumplimiento de requisitos legales y normativos.



Mejor gestión de riesgos y decisiones responsables.



Mayor confianza de usuarios, clientes y reguladores.



# ISO/IEC 42001 vs. ISO/IEC 27001 (integración)

## A.6 Ciclo de vida del sistema de IA

ISO/IEC 42001	6.1 Orientación de gestión para el desarrollo de sistemas de IA	6.2 Ciclo de vida del sistema de IA
<b>ISO/IEC 27001</b>	Seguridad de la información en las relaciones con los proveedores Seguridad de la información para el uso de servicios en la nube Gestión de incidentes Seguridad de la información durante la interrupción Identificación de requisitos legales, reglamentarios y Contractuales Derechos de propiedad intelectual (DPI) Privacidad y protección de datos de carácter personal (DCP) Seguridad en el ciclo de vida del desarrollo Requisitos de seguridad de las aplicaciones	Gestión de vulnerabilidades técnicas Registros de eventos Seguimiento de actividades Seguridad en el ciclo de vida del desarrollo Requisitos de seguridad de las aplicaciones Arquitectura segura de sistemas y principios de Ingeniería Codificación segura Pruebas de seguridad en desarrollo y aceptación Externalización del desarrollo Separación de los entornos de desarrollo, prueba y Producción Gestión de cambios Datos de prueba Protección de los sistemas de información durante las pruebas de auditoría
<b>posible conexión de artículos</b>	A.5.19-5.23, A.5.24-5.28, A.5.29, A.5.31-5.32, A.5.34, A.8.25-8.26	A.8.8, A.8.15, A.8.16, A.8.25-8.31, A.8.32, A.8.33, A.8.34

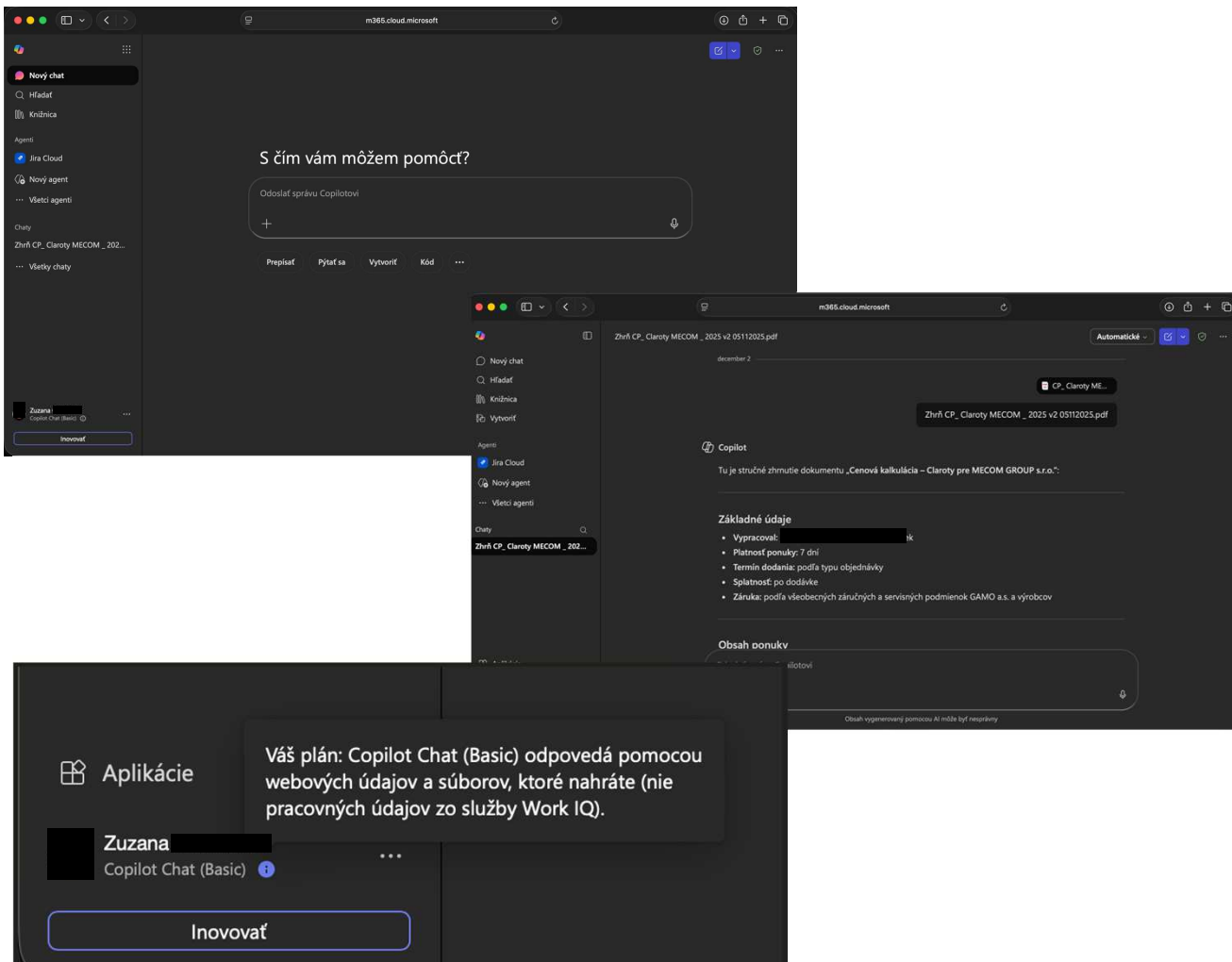


**¿Por qué es importante la gestión de la IA para cualquier empresa?**



# Incidente de IA: uso de „Copilot MS 365“

riesgo de autonomía excesiva de la IA



1. Inicializado sesión en el entorno en línea de M365 a través de la web
2. A la persona no se le asigna una licencia de copilot
3. Sin embargo, cuenta con una versión básica de Copilot que puede trabajar con información de la web y con lo que una persona sube a ella
4. El copiloto sacó agentes del propio Jira, por ejemplo
5. El copiloto de chat se puso en marcha solo
6. Escribió una pregunta y descargó un documento al que la persona no tiene acceso (documento con datos confidenciales: presupuesto para el cliente)
7. El documento no se guardó en los archivos compartidos de MS Teams ni en el OneDrive personal de la persona, ni en los correos



# Incidente de IA: uso de „Copilot MS 365“

Si Copilot (u otro asistente IA) comienza durante el chat a:

- hacer preguntas de forma autónoma,
- desarrollar la conversación,
- obtener información adicional,
- o dirigir al usuario hacia cierta dirección,

en ISO/IEC 27001:2022 esto no se asociaría a un único riesgo, sino a múltiples controles y áreas de riesgo al mismo tiempo.

## ISO 27001:

•no define explícitamente un “AI manipulation risk”, pero estos riesgos IA se relacionan con:

- information security,
- access control,
- acceptable use,
- human factor,
- data leakage,
- social engineering,
- supplier risk,
- cloud risk,
- governance risk.

## El mayor problema

ISO 27001:

originalmente no fue diseñada para **comportamiento autónomo de IA.**

Por eso:

- AI manipulation,
- behavioral influence,
- prompt harvesting,
- excessive autonomy

deben:

- interpretarse utilizando controles tradicionales de seguridad

## Por eso ISO/IEC 42001 es importante

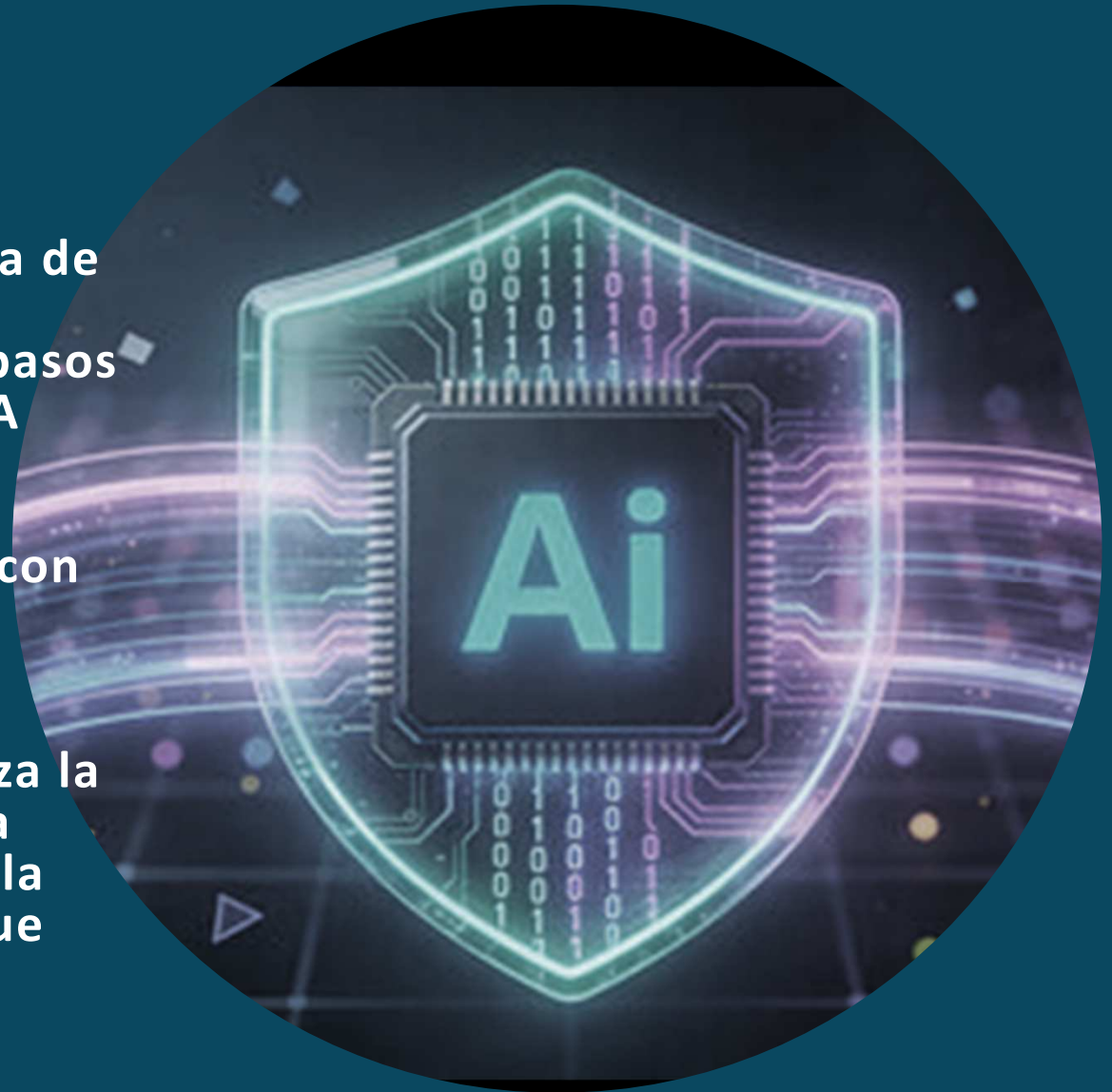
ISO 42001 aborda explícitamente:

- AI behavior,
- AI autonomy,
- human oversight,
- AI ethics,
- AI societal impact,
- AI transparency,
- responsible AI use.

Y precisamente esa es el área que ISO 27001 por sí sola **no cubre suficientemente.**

## Conclusión

1. después de implementar la norma de gestión de la seguridad de la información, se requieren algunos pasos para implementar la gestión de la IA
2. los riesgos de seguridad de la información están interconectados con los riesgos de la IA; es necesario identificarlos y mitigarlos
3. incluso si su empresa „solo“ utiliza la IA para sus procesos básicos, podría sufrir un incidente de seguridad de la información debido a su uso, hay que estar preparado



*¡Muchas gracias!*

*Eva Hlušková*  
*[eva.hluskova@isaca.sk](mailto:eva.hluskova@isaca.sk)*

