

## 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 semanas a horas: La IA, nueva aliada en la gestión de riesgos***

*José Rafael Cuevas Marchán*

# La IA no debe impresionar en una demo; debe resistir todo el proceso de gestión.

## GOBERNANZA Y GESTIÓN DE RIESGOS

### MAPA DE PROCESOS



### PRUEBAS DE CONTROLES



CONTROLES DISEÑADOS	152
CONTROLES EVALUADOS	146
EFECTIVIDAD PROMEDIO	96%



### EVIDENCIA Y SOPORTES

TIPO DE EVIDENCIA	FIAS
Políticas / Procedimientos	128
Registros de Ejecución	342
Reportes / Dashboard	267
Aprobación / Revisión	190
Otro	54



### TRAZABILIDAD Y AUDITORÍA

EVENTOS REGISTRADOS	1,842
HALLAZGOS ABIERTOS	23
ACCIONES CORRECTIVAS	87
% CIERRE ACC. VENDIDAS	76%
TIEMPO PROM. CIERRE	18 días



### MATRIZ DE RIESGOS

	Bajo	Medio	Alto	Muy Alto
Alto	2	5	8	3
Medio	1	3	6	2
Bajo	0	1	2	1

### RIESGOS CLAVE

R-01	Interrupción Operativa	Alto
R-02	Ciberseguridad	Alto
R-03	Incumplimiento Regulatorio	Medio
R-04	Terceros Críticos	Medio
R-05	Calidad de Datos	Bajo

[Ver todos los riesgos](#)

INTEGRACIÓN DE DATOS

CONTROLES AUTOMATIZADOS

MONITOREO CONTINUO

REPORTES EJECUTIVOS



# No todo se trata de **prompts**





**El riesgo no espera  
a que terminemos de  
llenar la matriz.**

ID Riesgo	Descripción del Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Estado	Responsable	Fecha Revisión
R-001	Pérdida de información crítica	Alta	Alto	Crítico	Abierto	TI	15/05/2024
R-002	Acceso no-autorizado a sistemas	Media	Alto	Alto	Abierto	Seguridad	15/05/2024
R-003	Falla en respaldos de información	Media	Medio	Medio	En progreso	TI	15/05/2024
R-004	Errores en captura de datos	Alta	Medio	Alto	Abierto	Operaciones	15/05/2024
R-005	Incumplimiento normativo	Baja	Alto	Medio	En progreso	Legal	15/05/2024
R-006	Indisponibilidad de sistemas	Media	Alto	Alto	Abierto	TI	15/05/2024
R-007	Fuga de información confidencial	Baja	Alto	Medio	Abierto	Seguridad	15/05/2024
R-008	Dependencia de terceros críticos	Media	Medio	Medio	En progreso	Compras	15/05/2024

# El humano decide

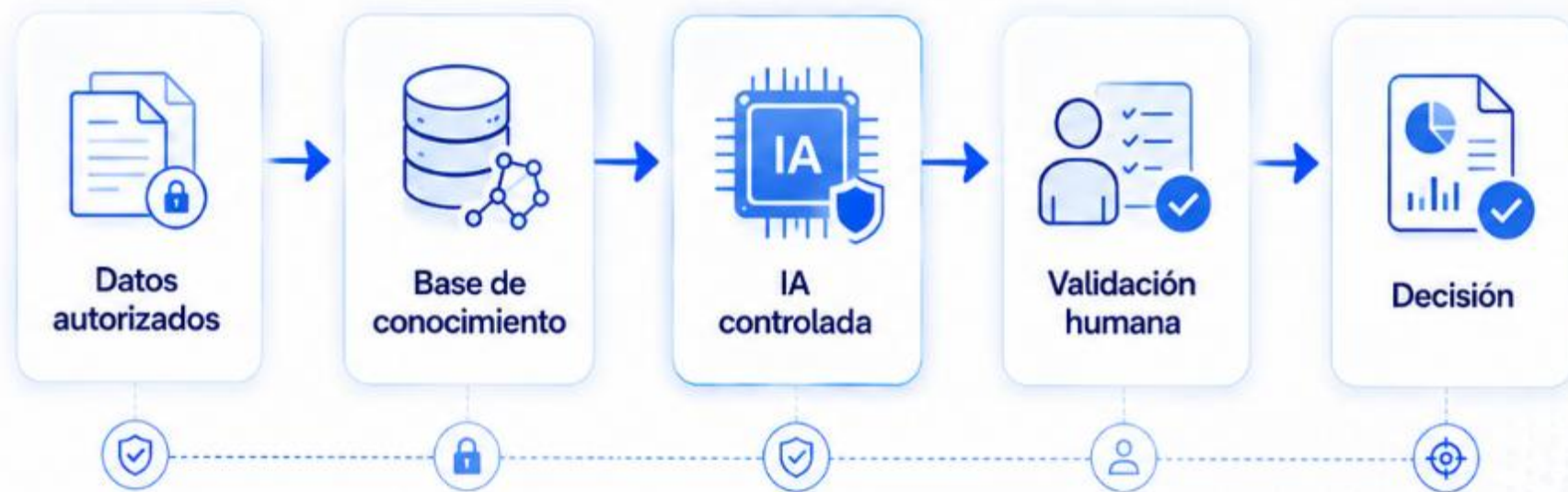


La IA no reemplaza el criterio; **lo potencia** con mejor información, mayor velocidad y más consistencia.

# No es solo prompting: es **diseño de solución**

No es solo prompting  
Es **diseño de solución**:

- ✓ Datos correctos.
- ✓ Límites claros.
- ✓ Dominio definido.
- ✓ Trazabilidad.
- ✓ Supervisión humana.



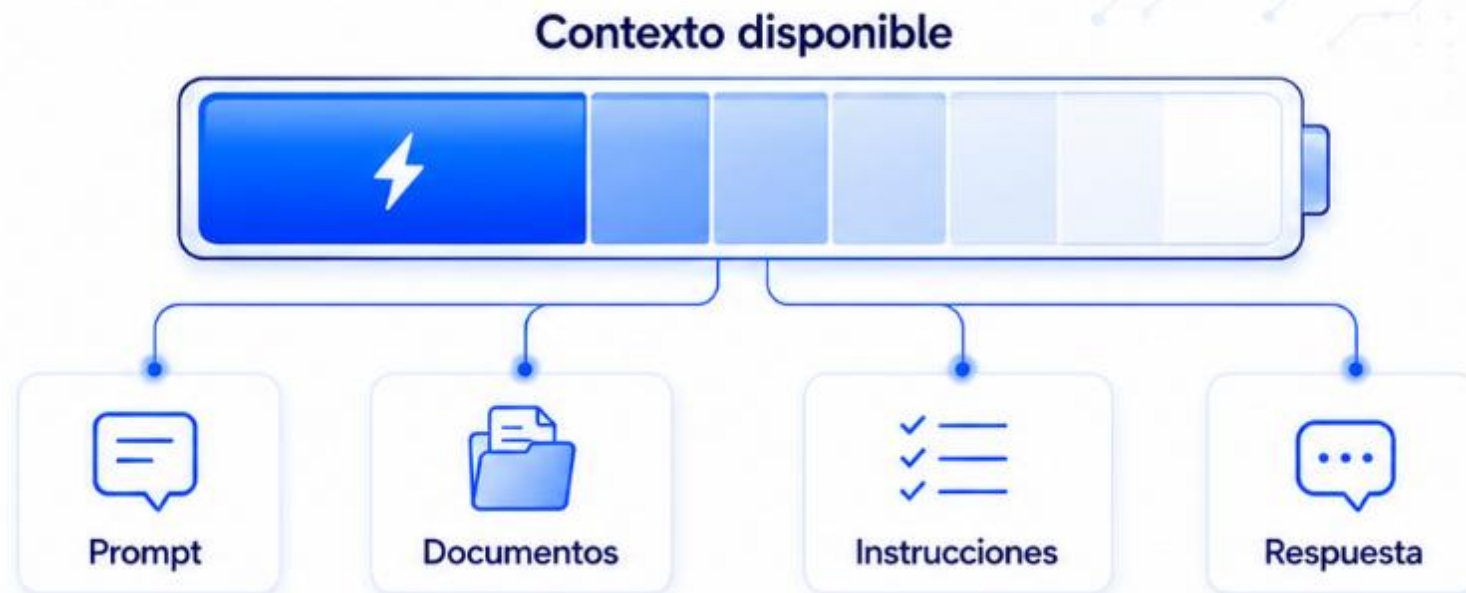
Un buen prompt ayuda a responder;  
un buen **diseño** ayuda a **gestionar**.

# Entendiendo los tokens

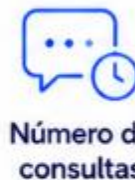
## Tokens: el combustible del contexto

Cada consulta consume capacidad.

- Entrada.
- Documentos.
- Instrucciones.
- Respuesta.
- Todo consume tokens.



Los límites varían según plan, modelo o configuración



Si no entiendes los tokens, no estás diseñando una solución: solo estás gastando contexto.



# Base de conocimiento: de documentos pesados a información útil

## Base de conocimiento

De documentos extensos a conocimiento consultable.

- ✓ Menos ruido.
- ✓ Más precisión.
- ✓ Mejor contexto.
- ✓ Mejor análisis.



✓ Menos ruido. Más precisión. Mejor contexto. Mejor análisis. ✓



La calidad de la respuesta depende de la **calidad del conocimiento** que la sostiene.



# Caso práctico: Diseño de Controles

## Caso 1: diseño de controles

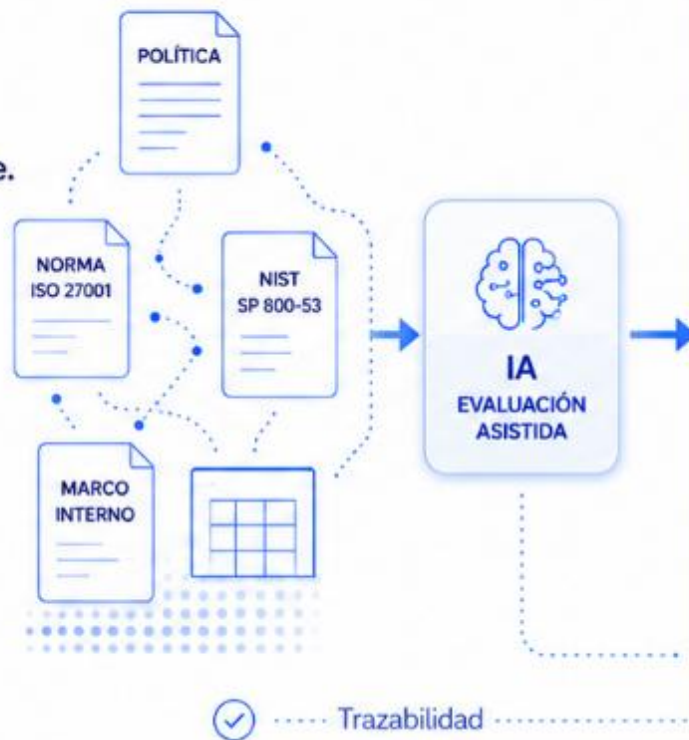
De criterios dispersos a evaluación asistida, consistente y trazable.



La IA estructura.



El experto decide.



## Evaluación de diseño de control



Atributo	Resultado	Trazabilidad
Objetivo	Cumple	<input checked="" type="checkbox"/> Fuente
Responsable	Parcial	<input checked="" type="checkbox"/> Criterio
Frecuencia	Cumple	<input checked="" type="checkbox"/> Evaluación IA
Evidencia	Brecha	<input checked="" type="checkbox"/> Revisión experto
Alineación normativa	Requiere validación	<input checked="" type="checkbox"/> Decisión



Un control no está bien diseñado porque suena bien; está bien diseñado porque puede operar, evidenciarse y defenderse.



# Caso 2: evaluación de pruebas de control

## Caso 2: evaluación de pruebas

¿La prueba realmente prueba el control?

- Alcance.
- Criterio.
- Evidencia.
- Conclusión.
- Trazabilidad.



Evaluación de la revisión		
	Alineación con el control	OK
	Criterios claros	PARCIAL
	Evidencia suficiente	NO
	Conclusión sustentada	PARCIAL
	Estado general:	ATENCIÓN



Una prueba no vale por estar documentada; vale por demostrar lo que afirma.



# Caso práctico 3: pruebas operativas sobre universos completos

## Caso 3: de muestras a universos



Más cobertura



Más patrones



Mejor evidencia

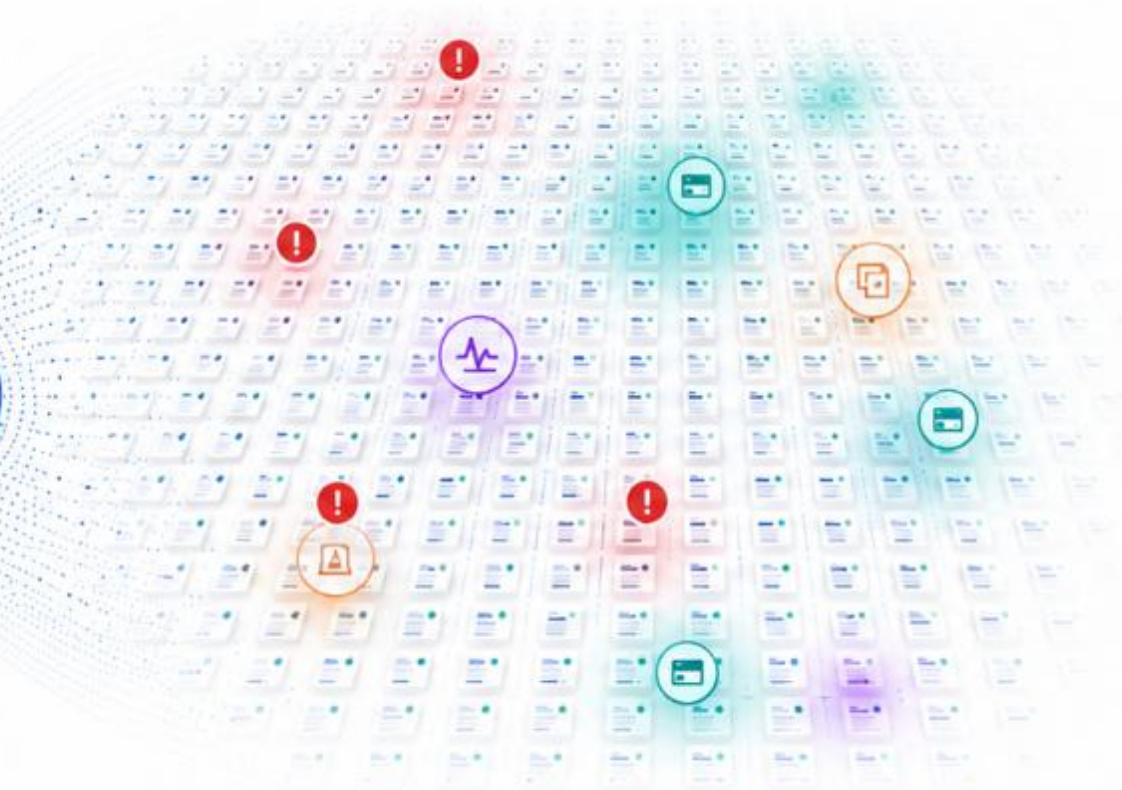


Mejores decisiones

Muestra: 30 casos



Universo: 18,000 registros



La muestra nos da una señal; el universo nos da mayor certeza.



# Caso 4: Auditoría predictiva

De hallazgos históricos a anticipación de riesgos



“ La mejor auditoría no es la que solo responde; es la que permite **anticiparse**. ”



# Qué hace diferente a una solución seria de IA

*Demo vs. solución real*



**En riesgos, una respuesta corta y honesta vale más que una respuesta elegante pero infundada.**

# La IA también necesita controles



**No hay IA para riesgos sin controles sobre la IA.**

# Modelo responsable de adopción



# Roadmap práctico de implementación



La IA no fracasa por falta de potencial; fracasa por falta de **diseño**.




# ¿Qué proceso de riesgo te está robando tiempo experto?



# Criterio humano amplificado



“ La IA amplifica capacidades; el criterio humano conserva la responsabilidad.



La **IA** no sustituye  
la gestión de riesgos;  
la hace más **ágil**,  
más **amplia** y  
más **confiable**.





# Preguntas

RISK MANAGEMENT

***¡Muchas gracias!***

*José Rafael Cuevas Marchán*

