“No solo hay que serlo, sino parecerlo”

Guía de auditoría y evaluación de controles

Para auditores internos y externos de normas de gestión, con o sin anexos técnicos



Sobre el autor

Luciano Moreira

Auditor líder

- ISO 27001 · ISO 27017 · ISO 27018
- ISO 22301 · ISO 9001 · ISO 20000
- ISO 54001 · ISO 27701 · ISO 42001
- CSA STAR · TISAX

Auditor

- IATF 16949 · ISO 37001 · ISO 37301
- GDPR · LGPD
- STAR Audit – EuroCloud
- SOC 2



/lucianomoreiradacruz/ @Luciano_m_cruz

Sobre el autor

Martin Ambort

Auditor líder

- ISO 27001 · ISO 27701 · ISO 42001
- ISO 22301 · ISO 9001 · ISO 20000
- TISAX

Auditor

- IATF 16949 · ISO 37001 · ISO 37301
- GDPR · LGPD
- SOC 2



/martin-ambort-08a7a8b3/ @mambort2014

Sobre el autor

Christian Ibiri

Auditor líder

- ISO 27001 · ISO 27701 · ISO 42001
- ISO 22301 · ISO 9001

Auditor

- GDPR · LGPD
- SOC 2

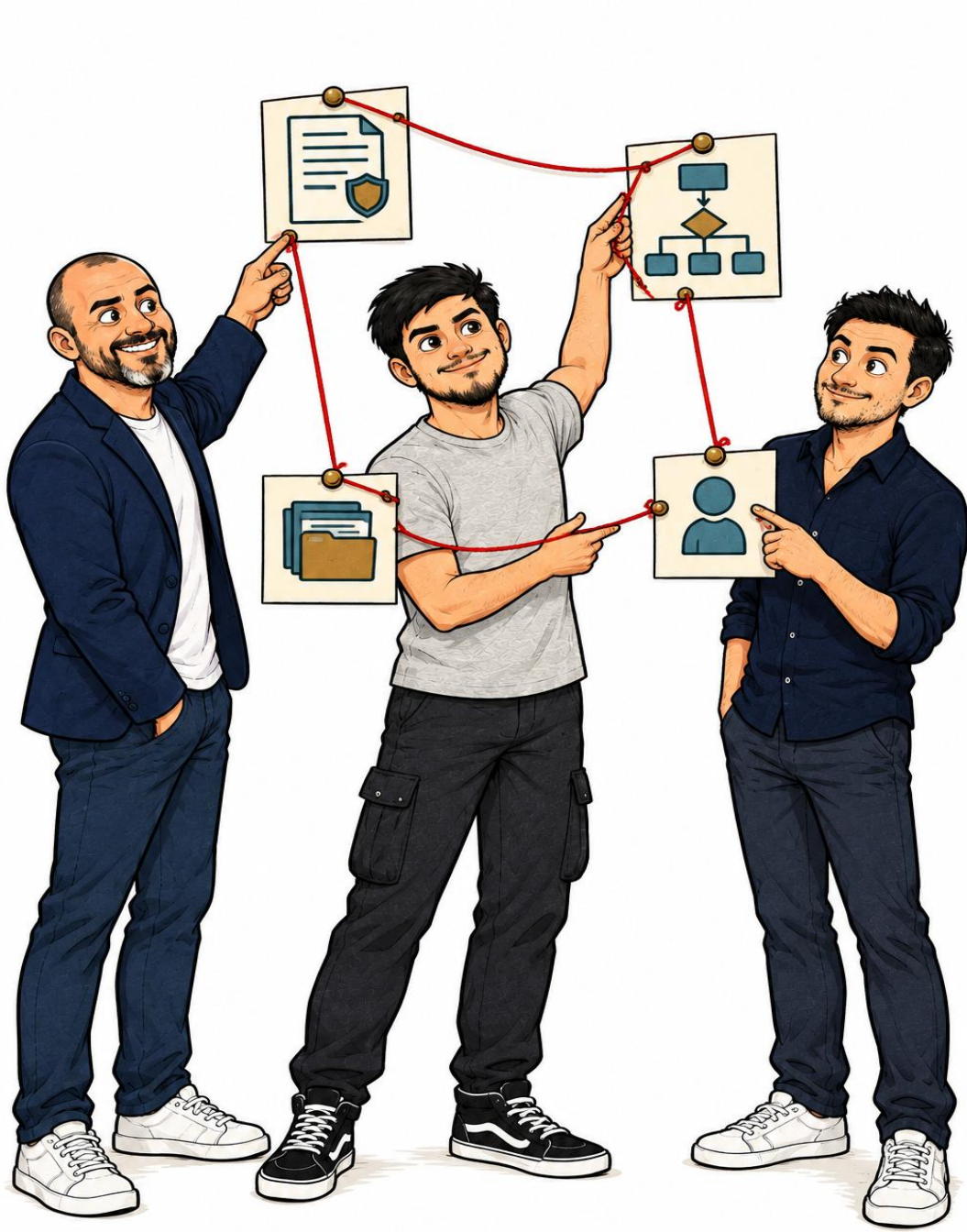


/christian-ibiri /

@Christianibiri

“No solo hay parecerlo que serlo, sino”

Un control no basta con estar escrito: tiene que operar. Y un control que opera tiene que poder demostrarse con evidencia. La tarea del auditor es unir ambas caras.



Agenda

Parte I · Cualquier sistema de gestión

1. Introducción: la maratón ISO
2. Sistemas de gestión y estructura armonizada
3. ISO 31000 y el riesgo
4. Controles, riesgo y medición
5. El auditor y los errores típicos
6. Principios y dos perspectivas
7. Planificación
8. Métodos, pruebas y muestreo
9. Mente que cuestiona y sesgos
10. El arte de hacer preguntas
11. Técnicas de interrogatorio
12. Evidencias, hallazgos e informe
13. ISO 9001, 22301 y 20000-1
14. Rutas PHVA comunes

Parte II · Anexos técnicos

15. Normas con anexos técnicos
16. ISO/IEC 27001, 27701 y 42001
17. Familias de apoyo y nube (27017, 27018)
18. Evaluación de controles (TS 27008)
19. Rutas PHVA técnicas
20. Conclusiones

Parte I · Auditar cualquier sistema de gestión

Calidad, ambiente, seguridad y salud, continuidad, servicios, antisoborno… el método es el mismo



01

Introducción: la maratón ISO

Por qué profundizar más allá del curso de Auditor Interno o Líder



Maratón ISO: ¿cuál será el próximo estándar a alcanzar?

¿A veces no sienten que estamos en una carrera tratando de alcanzar la nueva palabra del momento? Antes fue la nube, después la privacidad, ahora la inteligencia artificial. ¿La próxima? Ya habrá un curso para eso.

Spoiler: muchas de las prácticas "innovadoras" son las mismas que un buen auditor ya usa: entender el contexto, evaluar riesgos, verificar que los controles funcionen y pedir evidencia. Cambia el envoltorio, no el contenido.

ISO/IEC 42001 o la nueva ISO/IEC 27701:2025 cambian el objeto auditado, pero no el método. Y no, no hace falta un curso de Auditor Líder por cada norma… aunque el mercado opine distinto.



La idea central

No hace falta correr detrás de cada norma nueva. Hace falta dominar un método que funcione para todas. Y leer la norma antes de auditarla: detalle no menor.

Debate

¿Todos son auditores lideres o internos, verdad?

¿Recuerdan la pregunta más técnica, o asociada a un control del Anexo, de su examen de Auditor Líder?

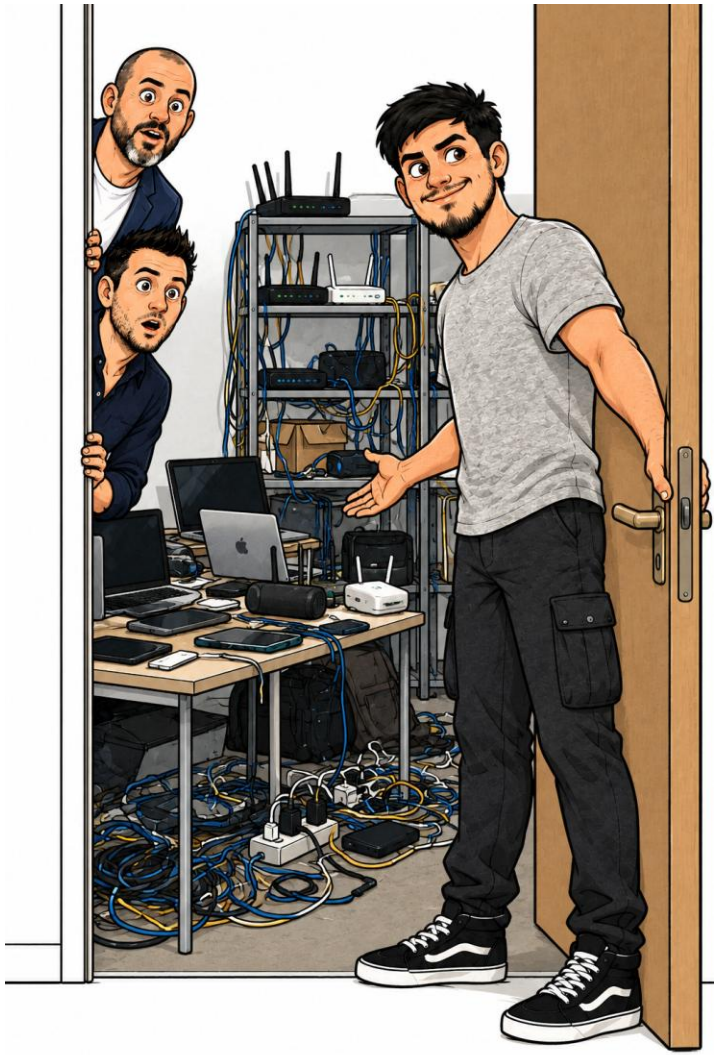


Lo que el curso de Auditor Líder no enseña

Seguro que no. Y no es falta de memoria: los cursos de Auditor Líder buscan formar auditores sobre la base de ISO 19011 e ISO/IEC 17021-1, con una pizca de la norma en cuestión.

Se supone que el participante ya conoce la norma —y la disciplina— antes de empezar el curso. En la práctica, muchos auditores salen sabiendo conducir una reunión de apertura, pero no cómo comprobar si una regla de firewall, una evaluación de impacto de IA o un control de privacidad cumplen su objetivo.

Esa brecha es aún mayor en las normas con anexos técnicos, donde cada control exige conocimiento específico.



"No solo hay que serlo, sino parecerlo"

Tener el certificado de Auditor Líder no basta: hay que demostrar competencia en cada auditoría.

¿El curso de Auditor Líder no sirve?

¿Cómo que no sirve? ¿Qué hago ahora con la capacitación carísima que pagué? ¿Puede que tenga razón o no?

1

Enojo

"¿Cómo que no sirve lo que estudié?"

2

Desesperación

"¿Qué hago con la capacitación que pagué?"

3

Aceptación

El curso es el punto de partida, no la meta

4

Transformación

Profundizar en la norma, la disciplina y la evaluación de controles



Para recordar: la mejor idea es profundizar un poco más en el tema. Spoiler: el certificado no audita solo.

02

Sistemas de gestión y estructura armonizada

La base común de todas las normas certificables



Qué es un sistema de gestión

Un enfoque sistemático para establecer, implantar, operar, supervisar, revisar, mantener y mejorar una disciplina en la organización, con el fin de alcanzar los objetivos de negocio.

1 Es sistemático

No son prácticas sueltas, sino un ciclo con responsables, objetivos, medición y mejora.

2 Está basado en riesgos

Los controles se eligen porque tratan riesgos u oportunidades identificados, no porque figuren en una lista o en un anexo.

3 Sirve al negocio

Protege activos y resultados: información financiera, propiedad intelectual, datos de empleados y clientes, información confiada por terceros, sistemas de IA confiables.

La estructura armonizada: cláusulas 4 a 10 comunes a todas las normas

Cláusula	Tema	Pregunta del auditor
4	Contexto de la organización	¿Entendió sus cuestiones internas y externas, partes interesadas y alcance?
5	Liderazgo	¿La dirección demuestra compromiso, aprobó la política y asignó roles?
6	Planificación	¿Evaluó y trató riesgos? ¿Seleccionó controles? ¿Hay objetivos medibles y cambios planificados?
7	Apoyo	¿Hay recursos, competencia, toma de conciencia, comunicación e información documentada?
8	Operación	¿Se ejecuta lo planificado, incluido el tratamiento de riesgos y los procesos externos?
9	Evaluación del desempeño	¿Se mide, se audita internamente y la dirección revisa?
10	Mejora	¿Se tratan las no conformidades y se mejora de forma continua?



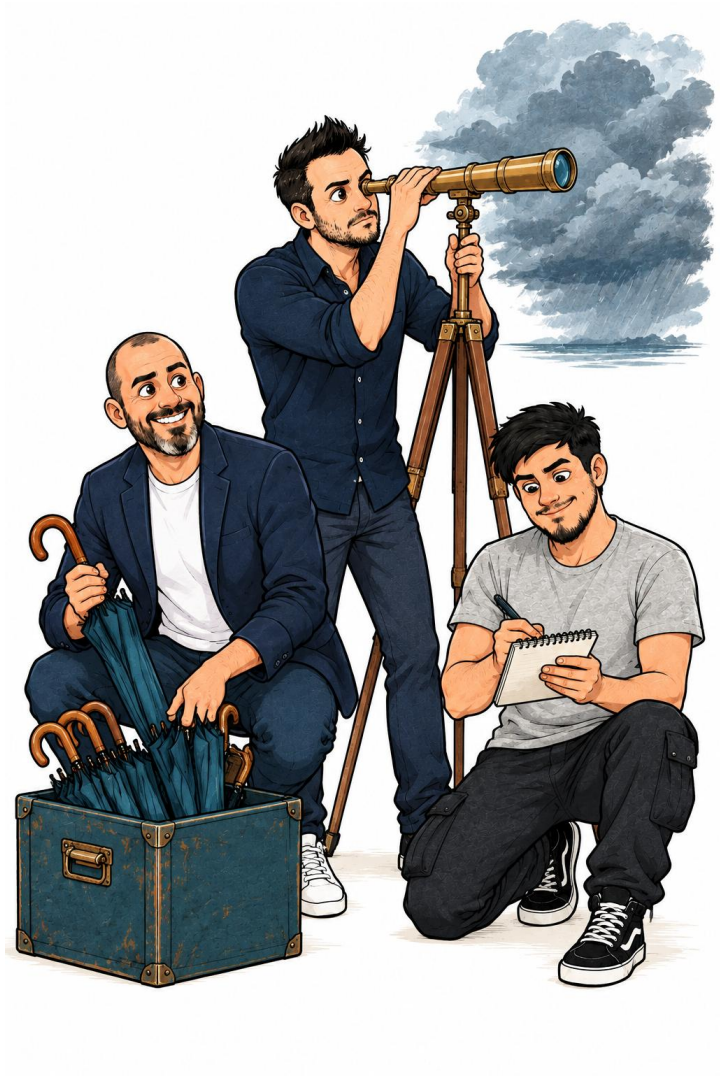
Para recordar: no se excluye ningún requisito de las cláusulas 4 a 10. Tampoco el 9.3, aunque la dirección esté “muy ocupada”.

¿El clima en el sistema de gestión? Sí, en serio

En febrero de 2024, ISO y el IAF publicaron un comunicado conjunto: las normas de sistemas de gestión incorporan una enmienda sobre acción climática. En seguridad de la información llegó como ISO/IEC 27001:2022/Amd 1:2024.

La enmienda agrega al 4.1 que la organización debe determinar si el cambio climático es una cuestión pertinente, y al 4.2 una nota: las partes interesadas pueden tener requisitos relacionados con el clima.

Para el auditor no significa pedir la huella de carbono del firewall. Significa verificar que el tema se analizó y se decidió con fundamento: un centro de datos en zona inundable sí tiene algo que decir.



Qué pedir como evidencia

El análisis de contexto actualizado, la decisión tomada (pertinente o no) y, si es pertinente, su reflejo en riesgos, objetivos o continuidad.

Cada norma = base común + capa disciplinar

Norma	Disciplina	Dónde se concentra la capa disciplinar
ISO 9001	Calidad	Requisitos del cliente, diseño, producción, liberación, salidas no conformes
ISO 14001	Ambiente	Aspectos ambientales, obligaciones de cumplimiento, emergencias
ISO 45001	Seguridad y salud	Peligros, jerarquía de controles, participación de trabajadores
ISO 22301	Continuidad	Análisis de impacto, estrategias, planes, ejercicios
ISO 37001	Antisoborno	Diligencia debida, controles financieros, regalos, denuncias
ISO 37301	Cumplimiento	Obligaciones de cumplimiento, cultura, investigaciones
ISO 50001	Energía	Revisión energética, línea de base, indicadores energéticos
ISO 22000	Inocuidad	Prerrequisitos, análisis de peligros, plan de control



No todas las normas cumplen la misma función

Tipo de norma	Verbo típico	Ejemplos	Uso en auditoría
Requisitos (certificables)	“debe”	ISO 9001, ISO/IEC 27001, 27701, 42001	Criterio de auditoría; base de no conformidades
Códigos de práctica y guías	“debería”, “puede”	ISO/IEC 27002, 27003, 27005, 27017, 27018	Interpretar y esperar buenas prácticas; nunca base única de una no conformidad
Sectoriales	“debe” o “debería”	ISO/IEC 27011, 27019, IATF 16949	Criterio adicional si el cliente o el esquema lo exige
Evaluación de la conformidad	“debe”	ISO/IEC 17021-1, 27006-1, 27706, 42006	Marco del auditor de certificación
Auditoría y evaluación	“debería”	ISO 19011, ISO/IEC 27007, TS 27008	Método del auditor



Para recordar: si la guía dice “debería” y la organización cumple el requisito por otro camino, no hay incumplimiento.

Una ruta de aprendizaje por niveles

1 Principiante

Estructura armonizada, la norma de su disciplina, ISO 19011 y vocabulario básico.

2 Avanzado

Guías de aplicación, ISO 31000, requisitos legales del sector, auditoría de sistemas integrados.

3 Experto

Evaluación de controles, muestreo, medición del desempeño, gobernanza y técnicas especializadas.



Para recordar: auditar el sistema pregunta “¿está bien gobernado?”; evaluar los controles pregunta “¿funcionan?”.

03

ISO 31000: la base del pensamiento basado en riesgo

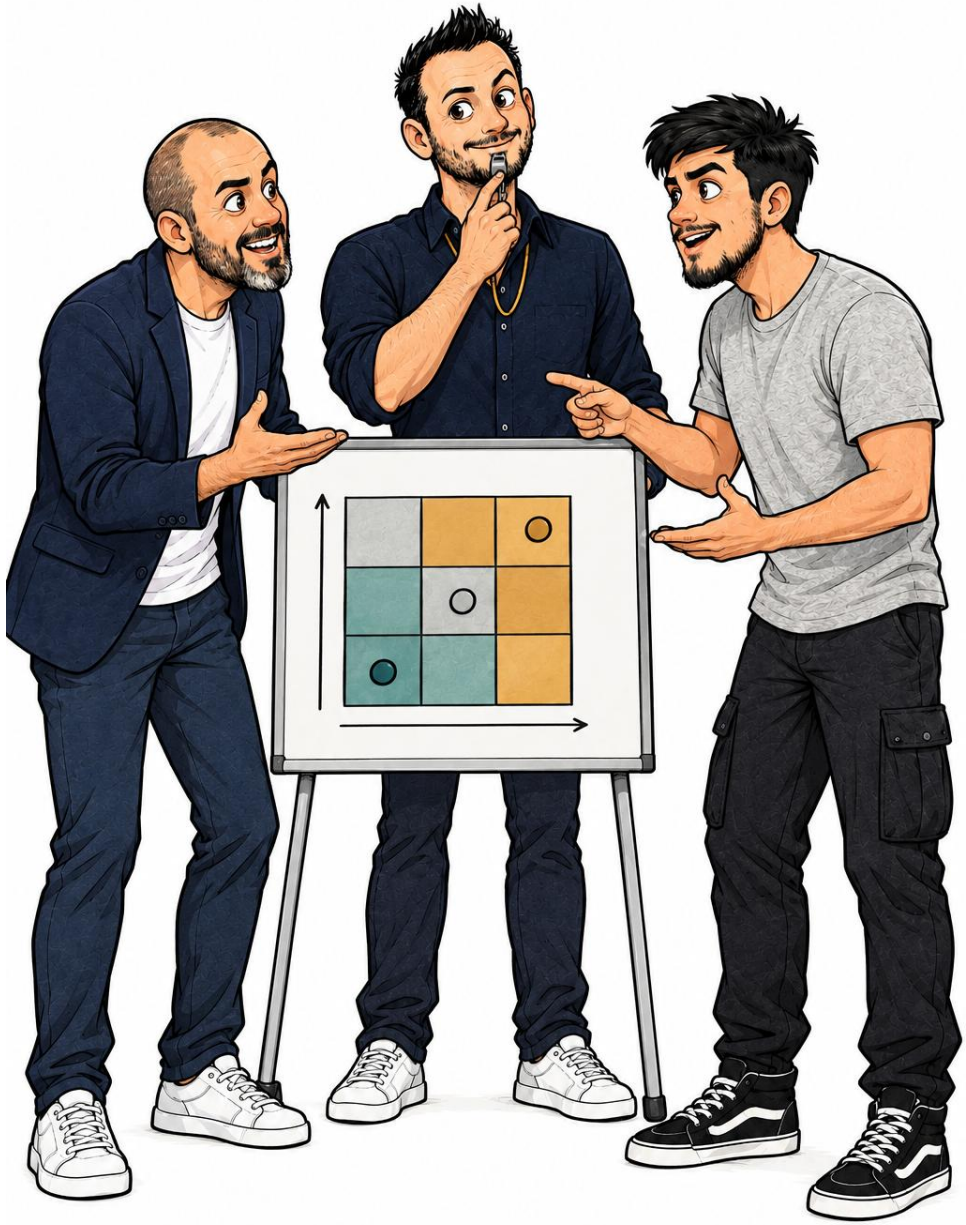
Antes de auditar riesgos, conviene saber qué es uno



Debate

¿Qué es un riesgo?

Pista: no es “lo que puede salir mal”. Tampoco es la matriz de colores que se actualiza una vez al año, justo antes de la auditoría.



Riesgo: efecto de la incertidumbre sobre los objetivos

ISO 31000 define el riesgo como el efecto de la incertidumbre sobre los objetivos. El efecto puede ser positivo, negativo o ambos: de ahí que las normas hablen de riesgos y oportunidades.

Consecuencia práctica número uno: sin objetivos claros no hay riesgo que evaluar. Si la organización no sabe qué quiere lograr, su matriz de riesgos es una lista de miedos ordenada por colores.

Consecuencia número dos: el riesgo no es la amenaza ni la vulnerabilidad. Es lo que le pasa al objetivo si la incertidumbre se materializa.



Para el auditor

Pregunte primero por los objetivos y después por los riesgos. Si los riesgos no se pueden conectar con ningún objetivo, ya tiene una conversación interesante.

Los ocho principios de la gestión del riesgo

1 Integrada

Parte de todas las actividades, no un anexo del sistema.

2 Estructurada y exhaustiva

Enfoque sistemático para resultados coherentes y comparables.

3 Adaptada

Proporcional al contexto y a los objetivos de la organización.

4 Inclusiva

Con participación oportuna de las partes interesadas.

5 Dinámica

Anticipa, detecta y responde a los cambios.

6 Mejor información disponible

Datos históricos y actuales, con sus limitaciones.

7 Factores humanos y culturales

El comportamiento y la cultura influyen en todo.

8 Mejora continua

Se mejora con el aprendizaje y la experiencia.

Para recordar: “integrada” significa que el riesgo aparece en las decisiones del negocio, no solo en la carpeta del auditor.

El marco: liderazgo, integración y el ciclo de mejora

1	2	3	4	5	6
Liderazgo y compromiso	**Integración**	**Diseño**	**Implementación**	**Valoración**	**Mejora**
La dirección asegura que el riesgo se gestione e integre (5.2)	En la estructura, la gobernanza y los procesos (5.3)	Contexto, compromiso, roles, recursos y comunicación (5.4)	Plan, plazos, recursos y decisiones (5.5)	¿El marco funciona? Medirlo contra su propósito (5.6)	Adaptar y mejorar el marco de forma continua (5.7)



Para recordar: un proceso de riesgos sin marco es como un procedimiento sin dueño: existe, pero nadie lo usa para decidir.

El proceso de gestión del riesgo (cláusula 6)

Etapa	Qué se hace	Qué evidencia pedir
6.2 Comunicación y consulta	Involucrar a las partes interesadas en todo el proceso	Participantes reales, no solo el responsable del sistema
6.3 Alcance, contexto y criterios	Definir alcance, contexto y criterios de riesgo	Criterios de probabilidad, consecuencia y aceptación aprobados
6.4 Evaluación del riesgo	Identificar, analizar y valorar	Riesgos específicos, análisis coherente con los criterios
6.5 Tratamiento del riesgo	Seleccionar opciones e implementar planes	Planes con responsables, plazos y riesgo residual aceptado
6.6 Seguimiento y revisión	Asegurar y mejorar la calidad del proceso	Revisiones periódicas y ante cambios
6.7 Registro e informe	Documentar y comunicar resultados	Información para decidir, no solo para archivar

Cómo usa cada norma el pensamiento basado en riesgo

Norma	Cómo aparece el riesgo	Matiz para el auditor
ISO 9001	Pensamiento basado en riesgos en todo el sistema (6.1)	No exige un método formal ni documentarlo de una forma particular
ISO/IEC 27001	Evaluación y tratamiento con criterios definidos (6.1.2, 6.1.3)	Resultados comparables y repetibles; dueños del riesgo
ISO 22301	Evaluación de riesgos de interrupción (8.2.3)	La propia norma remite a ISO 31000 para el proceso
ISO/IEC 27701	Evaluación y tratamiento de riesgos de privacidad	Incluye el riesgo para los titulares, no solo para la empresa
ISO/IEC 42001	Riesgos de IA y evaluación de impacto (6.1.2 a 6.1.4)	Se apoya en ISO/IEC 23894 para riesgos de IA
ISO/IEC 20000-1	Riesgos para el sistema y los servicios (6.1)	Riesgos para clientes, servicios y cumplimiento de acuerdos



Para recordar: mismo concepto, distinta profundidad: no le pida a una pyme con ISO 9001 la matriz de un banco con ISO/IEC 27001.

Auditar el proceso de riesgos sin morir en la matriz

Preguntas que funcionan

- ¿Qué entradas usaron: contexto, partes interesadas, procesos, incidentes?
- ¿Quién participó, además del responsable del sistema?
- ¿Los criterios de aceptación los aprobó alguien con autoridad?
- Muéstreme un riesgo alto: ¿qué control lo trata y cómo saben que funciona?
- ¿Qué cambió en la matriz desde la última auditoría? ¿Por qué?

Señales de alerta

- Riesgos genéricos (“incumplimiento de requisitos”, “fallas en el proceso”)
- Todos los riesgos residuales en “bajo”: la organización perfecta
- La matriz no cambió en tres años, aunque cambió todo lo demás
- Riesgos sin dueño o con dueño “el área”
- Incidentes reales que no figuraban como riesgo

Para recordar: si el incidente del año no estaba en la matriz, la matriz no era de riesgos: era decorativa.

04

Controles, riesgo y medición

Una medida que modifica el riesgo… y que puede fallar



Control: medida que mantiene y/o modifica el riesgo

1

Nota 1

Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo.

2

Nota 2

Es posible que los controles no siempre ejerzan el efecto modificador previsto o asumido. Por eso existe la evaluación de controles.

1

¿Qué riesgo modifica?

Si nadie responde, el control puede sobrar.

2

¿Está implementado como se diseñó?

Eficacia de diseño e implementación.

3

¿Produce el efecto de forma sostenida?

Eficacia operativa en el período.

Del riesgo al control: la cadena que el auditor sigue

1	2	3	4	5	6
Contexto	**Riesgos**	**Acciones**	**Controles**	**Medición**	**Mejora**
Cláusula 4: qué importa y a quién	6.1: qué puede salir mal o bien	6.1: qué se decidió hacer	8: cómo se hace cada día	9.1: cómo se sabe si funciona	10: qué se corrige



Para recordar: riesgo alto sin control es exposición; control sin riesgo es burocracia; control sin seguimiento es suposición.

Tres tipos de control según cuándo actúan

1 Preventivo

Actúa antes del evento y busca evitarlo.

Capacitación, aprobación previa, mantenimiento preventivo, diligencia debida.

2 Detectivo

Actúa cuando ocurre o poco después; identifica y alerta.

Inspección, monitoreo, conciliación, auditoría, alarmas.

3 Correctivo

Actúa después; mitiga el daño y permite recuperarse.

Plan de emergencia, retiro de producto, plan de continuidad.

Para recordar: si todos los controles de un riesgo crítico son preventivos, nadie se enterará cuando la prevención falle.

La naturaleza del control cambia cómo se evalúa

Naturaleza	Característica	Implicancia para la evaluación
Manual	Depende de una persona cada vez	Propenso a errores y olvidos; requiere una muestra mayor
Automatizado	Lo ejecuta un sistema o dispositivo	Se comporta igual cada vez; basta probarlo una vez y verificar que no cambió
Semiautomatizado	Un sistema genera un reporte y una persona actúa	Evaluar ambas partes: fiabilidad del reporte y acción humana

Atributos útiles para describir cualquier control: riesgo u objetivo · tipo · naturaleza · frecuencia · responsable · evidencia · criterio

Diseño, implementación y eficacia operativa

Dimensión	Pregunta	Ejemplo de falla
Diseño	Si se ejecuta como está definido, ¿trata el riesgo?	La inspección de recepción verifica cantidad pero no especificación
Implementación	¿Está puesto en marcha como se definió?	El procedimiento existe pero el formulario no está en planta
Eficacia operativa	¿Se ejecutó siempre y bien durante el período?	En 4 de 20 recepciones no hay registro de inspección



Para recordar: falla de diseño → rediseñar; falla de operación → asegurar la ejecución.

Medir para saber si el control funciona

"Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre."

Tipo de indicador	Qué mide	Ejemplos
De resultado	Lo que ya ocurrió	Reclamos, accidentes, incidentes ambientales, multas
De proceso	Cómo funciona el proceso	Entregas a tiempo, rendimiento, consumo por unidad
De control	Si los controles se ejecutan	% inspecciones hechas, proveedores evaluados, acciones en plazo
De cultura	Comportamientos y actitudes	Casi accidentes reportados, denuncias, encuestas



Para recordar: un indicador que nadie analiza para decidir es decorativo: se mide pero no se gestiona.

En la práctica

Medir un control de concienciación es medir comportamientos, no asistencia a la capacitación.

El simulacro de phishing que todos aprobaron… porque nadie abrió el correo.



05

El auditor y los errores típicos

Conocer las trampas es la mejor forma de evitarlas



Tres tipos de auditor, un mismo método

Aspecto	Interno (1.ª parte)	Segunda parte	Certificación (3.ª parte)
Trabaja para	La dirección	Un cliente que evalúa a su proveedor	El organismo, frente al mercado
Mandato	Cláusula 9.2	Contrato con el proveedor	ISO/IEC 17021-1 y el esquema
Profundidad	Alta, durante todo el año	Acotada por el contrato	Acotada por los días-auditor
Riesgo principal	Falta de independencia	Alcance limitado	Superficialidad
¿Recomienda?	Sí, dentro de su rol	Según el acuerdo	No debe dar consultoría

Independencia: nadie audita su propio trabajo. Alertas: diseñó el control, depende del auditado, metas atadas al resultado, años sin rotación.

Error 1. Falta de conocimiento de la norma

En la mayoría de los casos, es posible que los auditados e incluso los propios auditores no tengan una idea clara de qué es la norma. Es una receta para el desastre: provoca que las auditorías fallen.

Los auditores que desconocen la norma tienden a seguir sus propias prácticas en lugar de las cláusulas de la norma. Como resultado, sus auditorías no logran los objetivos de la norma.

En algunas ocasiones, algunos auditores solo leen la norma para formular sus preguntas, dando una mala percepción a los auditados.



Cómo evitarlo

Estudiar la norma, su anexo y su guía (ISO/IEC 27002 o el Anexo B) antes de cada auditoría, y preparar preguntas propias en el lenguaje del auditado.

Error 2. Auditores no calificados

— Generalista

Amplio pero poco profundo; no evalúa controles técnicos.

I Experto en una cosa

Profundo en lo suyo; ignora la gestión.

T Especialidad + amplitud

Perfil mínimo para evaluar controles.

Π Dos especialidades

Fuerte en dos habilidades, por ejemplo seguridad y privacidad.

M Muchas especialidades

Conocimiento profundo en muchas; ideal para sistemas integrados.

E Las cuatro E

Experiencia, expertise, exploración y ejecución.

Para recordar: la evaluación de controles requiere análisis objetivo y conocimiento especializado de cada control.

Error 3. Imponen sus opiniones sin hechos

¿Por qué es esto malo? La norma tiene reglas claras sobre cómo implementar sus requisitos. Aunque hay margen para interpretar qué curso de acción es mejor, cualquier decisión debe estar respaldada por un requisito.

Desafortunadamente, algunos auditores tienen ideas preconcebidas sobre las mejores estrategias y recomiendan ciertas prácticas independientemente de la situación de la organización.

Un cliente solo debe seguir un consejo si el auditor puede explicar cómo ayuda a cumplir un requisito específico.



Cómo evitarlo

Hallazgo = requisito + evidencia. Distinguir no conformidad (incumple) de oportunidad de mejora (podría hacerse mejor).

Error 4. Creen en el papeleo e ignoran los hechos

¿Por qué es esto malo? Cualquier organización puede crear políticas que demuestren su compromiso con la norma, pero eso no significa que el personal realmente siga esas instrucciones.

Un mal auditor podría quedar satisfecho con la documentación y un vistazo superficial a su implementación. Debe ser más riguroso.

Los auditores no deberían conformarse con lo que la organización quiere que vean: deberían profundizar para comprobar si las reglas se siguen de manera consistente.



En normas con anexo

Una SoA con todos los controles “implementados” no prueba nada. Para cada control evaluado, pida al menos una evidencia de operación.

La política está en el papel; el control, en el escritorio. Mire el escritorio.

En la práctica

La política dice contraseñas de doce caracteres. El monitor dice otra cosa.

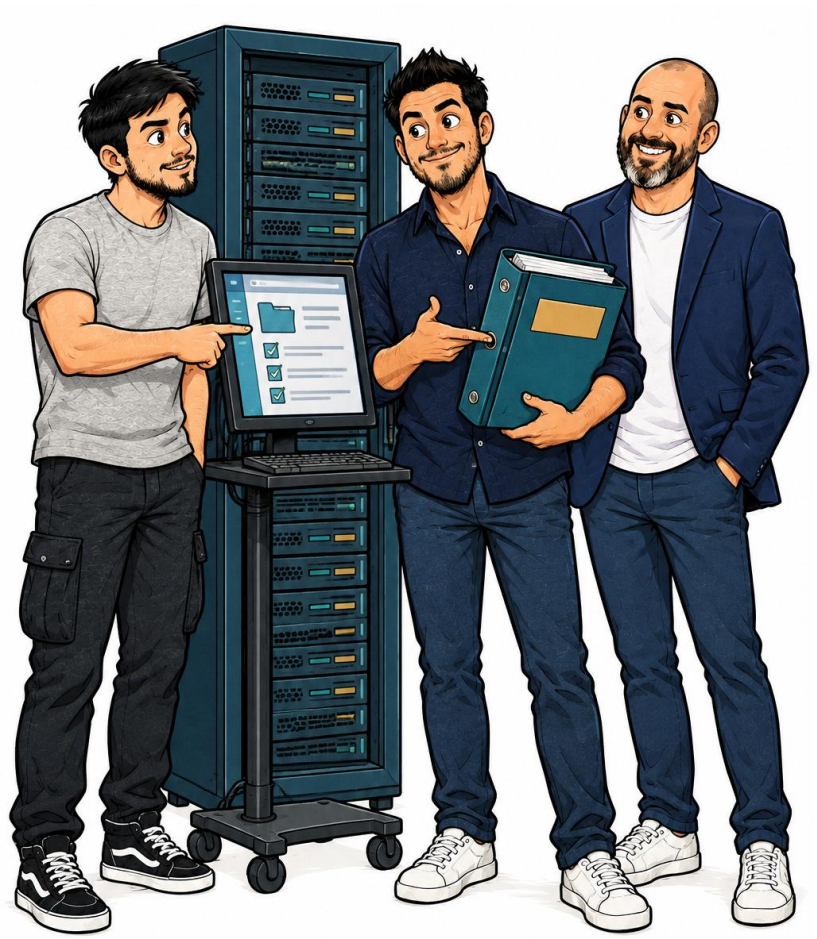


Error 5. Énfasis en controles técnicos y no en la gestión

Un SGSI define y gestiona controles para proteger la confidencialidad, integridad y disponibilidad de los activos de información. Estos activos no se limitan a TI: incluyen capital, infraestructura y personas.

Lamentablemente, muchos auditores limitan el alcance a los controles técnicos. Es curioso, porque la norma no es técnica (en serio, no es técnica). El resultado es ignorar los controles de gestión y el panorama general del sistema.

Lo mismo ocurre en IA: auditar solo el modelo y olvidar la política, los roles, la evaluación de impacto y la relación con terceros.



El dato

45 de los 93 controles del Anexo A de ISO/IEC 27001 son organizacionales o de personas. En ISO/IEC 42001, las áreas de políticas, organización, impacto y terceros pesan tanto como las técnicas.

Error 6. Se sienten obligados a encontrar errores

¿Por qué es esto malo? A veces los auditores intentan demostrar su autoridad señalando incumplimientos lo antes posible. No es necesariamente malo, pero sí lo es exagerar la magnitud de una deficiencia para demostrar un punto.

Un buen auditor no debería tardar mucho en encontrar fallas genuinas: incluso la organización mejor preparada tiene margen de mejora.

Si no lo tiene en cuenta al comienzo, terminará con una lista injustamente larga de fallas o con una interpretación inconsistente de los requisitos.



Cómo evitarlo

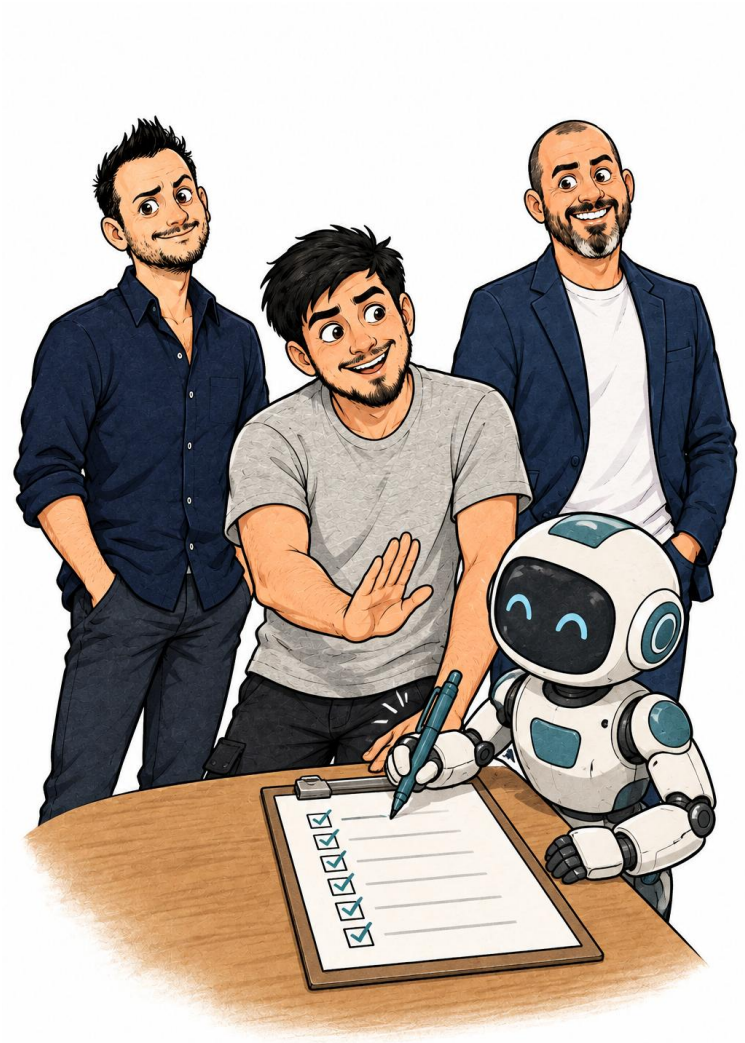
Definir los criterios de clasificación antes de auditar y revisar la consistencia de los hallazgos al cierre.

Error 7. La trampa de la lista de verificación

¿Por qué es esto malo? Las listas de verificación son una excelente manera de evaluar rápido si se cumple un conjunto de requisitos, pero lo que ofrecen en comodidad lo pierden en análisis.

La organización puede ver que se cumplió un requisito y asumir “misión cumplida”. Sin embargo, todavía puede haber margen para mejorar, e incluso puede que algunas actividades no sean necesarias.

Un buen auditor usa la lista como resumen, con una evaluación detallada en el informe, o un sistema no binario. Y ojo con la checklist “heredada”: TS 27008 advierte que usar listas genéricas escritas por otros, salvo para ahorrar tiempo, anula casi todos sus beneficios.



Riesgo especial con anexos

Convertir el Anexo A en una lista de 93 (o 38, o 78) casilleros es la forma más rápida de hacer una auditoría inútil.

Error 8. Informan hallazgos pero no proporcionan pruebas

¿Por qué es esto malo? Los auditores siempre deben aportar pruebas al señalar incumplimientos. No es necesario que sea evidencia física: el relato de un testigo puede bastar.

La cuestión es que el auditor necesita algo concreto que señalar, en lugar de citar una violación vaga o un “sentimiento” general de incumplimiento. Esto ayuda a la organización a comprender exactamente cuál es la falla y qué debe hacer.

No asuma: se espera escepticismo profesional y una mente inquisitiva, pero ser prejuicioso y asumir que todo está mal no ayuda a desempeñar bien el rol.



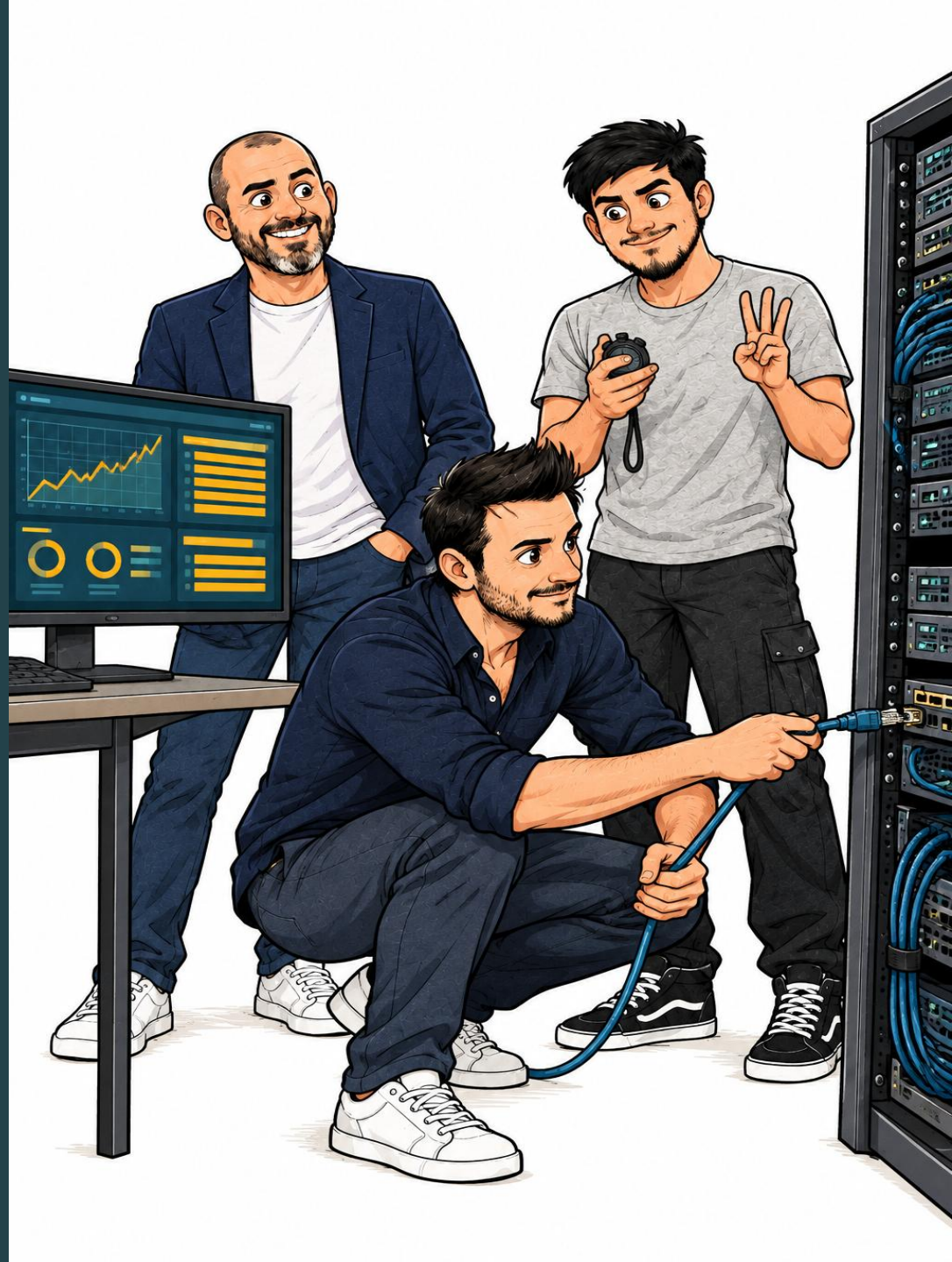
Cómo evitarlo

Redactar cada hallazgo con criterio, condición, causa y efecto, y verificar que la evidencia esté en los papeles de trabajo.

06

Principios de auditoría y dos perspectivas

Auditar el sistema y evaluar los controles



Los siete principios de auditoría de ISO 19011

1 Integridad

Honestidad, diligencia, imparcialidad.

2 Presentación imparcial

Informar con veracidad y exactitud.

3 Debido cuidado profesional

Juicio acorde a la importancia de la tarea.

4 Confidencialidad

Proteger la información obtenida.

5 Independencia

Base de la objetividad de las conclusiones.

6 Basado en la evidencia

Conclusiones verificables y reproducibles.

7 Basado en riesgos

Concentrar el esfuerzo en lo que más importa.

★ Para la evaluación de controles

Los dos últimos pesan más: dónde mirar y qué concluir.

Dos perspectivas que se complementan

Aspecto	Auditar el sistema	Evaluar los controles
Pregunta central	¿Está bien gobernado y se mejora?	¿Las medidas concretas funcionan?
Objeto	Cláusulas 4 a 7, 9 y 10	Cláusula 8 y requisitos de la disciplina
Evidencia típica	Políticas, riesgos, actas, indicadores	Registros, observación, mediciones, pruebas, muestras
Riesgo si se omite	Controles sin dirección ni mejora	Un sistema prolijo en papel que no protege nada
Ejemplo	¿La revisión por la dirección analizó a los proveedores?	¿Las 25 compras de la muestra fueron a proveedores aprobados?



Para recordar: una falla de control no detectada suele dar dos hallazgos: el control y el seguimiento que no la vio.

07

Planificación de la auditoría

Planificar es decidir dónde no mirar



Tres formas de organizar el trabajo

1 Por riesgo

Prioriza según los riesgos percibidos. Conviene con tiempo limitado y un análisis de riesgos maduro.

2 Por proceso

Sigue un proceso de punta a punta. Ideal para sistemas integrados: un recorrido por compras evalúa calidad, ambiente, seguridad y antisoborno a la vez.

3 Por cláusula

Cubre todo en orden. Conviene en la primera auditoría o en un programa de tres años.

Para recordar: los enfoques se combinan: cobertura secuencial en el ciclo, prioridad por riesgo cada año.

Objetivo, alcance, criterios y período

1 Objetivo

¿Para qué se audita?

Determinar si los controles sobre proveedores críticos operan con eficacia.

2 Alcance

¿Qué se audita y qué no?

Planta principal y depósito central; excluye oficinas comerciales.

3 Criterios

¿Contra qué se compara?

Cláusula 8.4, procedimiento de compras v4, contrato del cliente, ley aplicable.

4 Período

¿Qué período cubre la evidencia?

Enero a septiembre del año en curso.

Para recordar: los criterios incluyen lo que la propia organización se comprometió a cumplir.

Priorizar por riesgo y asignar profundidad

Factor	Pregunta	Peso
Riesgo que trata	¿Trata un riesgo alto o crítico?	Alto
Historial	¿Hubo hallazgos, quejas o incidentes?	Alto
Requisito legal	¿Su falla implica incumplimiento legal?	Alto
Cambios	¿Cambió el control o su entorno?	Medio
Complejidad	¿Depende de varias áreas o proveedores?	Medio
Naturaleza	¿Es manual o automatizado?	Medio

1 **Profunda**

Examen, prueba y muestra amplia

2 **Estándar**

Examen y prueba con muestra reducida

3 **Básica**

Entrevista y examen documental

Reglas antes de una prueba que puede afectar la operación

Activar una alarma, simular una emergencia, detener un equipo o tomar una muestra de producto exige un acuerdo previo por escrito.

1. Autorización formal del responsable del proceso o activo
2. Alcance exacto: lugares, equipos, sistemas y horarios
3. Pruebas permitidas y prohibidas
4. Medidas de seguridad para personas y ambiente
5. Contactos de escalamiento si algo falla
6. Tratamiento de los datos o muestras obtenidos
7. Quién ejecuta y quién supervisa



Para recordar: el auditor externo suele observar la prueba o revisar sus resultados, no ejecutarla.

08

Métodos, pruebas y muestreo

Preguntar, examinar, probar y muestrear



Cuatro métodos, cada uno demuestra algo distinto

Método	Qué es	Qué demuestra	Limitación
Análisis de procesos	Entender el proceso con entrevistas y recorridos	Cómo debería funcionar	Depende de lo que cuentan
Examen	Inspeccionar documentos, registros, instalaciones, actividades	Que está diseñado e implementado	Muestra un estado, no el tiempo
Prueba	Hacer actuar el control y comparar resultados	Que opera con eficacia	Exige competencia y autorización
Muestreo	Revisar una parte para concluir sobre el todo	Que opera de forma consistente	Riesgo de muestreo



Para recordar: preguntar cuenta, examinar muestra, probar demuestra, muestrear demuestra que funciona siempre.

En la práctica

Recorrer el lugar de trabajo aporta evidencia que ninguna entrevista ofrece.

La observación no figura en el plan de auditoría. El escritorio, en cambio, está ahí.



Modalidades de auditoría según ISO 19011

	Con interacción humana	Sin interacción humana
En el sitio	Entrevistas, listas de verificación con el auditado, revisión de documentos con el auditado, muestreo	Revisión de documentos, observación del trabajo, visitas al sitio, muestreo de productos
A distancia	Entrevistas por medios interactivos, revisión de documentos con el auditado a distancia	Revisión de documentos y registros, observación remota cuando sea viable, análisis de datos

ISO 19011, Anexo A: lo que casi nadie lee (y debería)

Apartado	Tema
A.1	Aplicación de métodos de auditoría
A.2	Enfoque a procesos
A.3	Juicio profesional
A.4	Resultados de desempeño
A.5	Verificación de la información
A.6	Muestreo
A.7	Cumplimiento dentro del sistema
A.8	Contexto
A.9	Liderazgo y compromiso

Apartado	Tema
A.10	Riesgos y oportunidades
A.11	Ciclo de vida
A.12	Cadena de suministro
A.13	Documentos de trabajo
A.14	Fuentes de información
A.15	Visita a las instalaciones
A.16	Actividades y lugares virtuales
A.17	Entrevistas
A.18	Hallazgos de auditoría

Para recordar: el anexo más útil de la norma de auditoría es, curiosamente, el que menos se cita en los cursos.

Tipos de prueba

Tipo	En qué consiste	Ejemplo
Reejecución	El auditor repite el control	Recalcular un indicador; repetir una medición con un patrón
Recorrido	Seguir un caso real por todos sus controles	Un reclamo desde su ingreso hasta su cierre
Inspección física	Verificar el estado real de un elemento	Extintor cargado y vigente; producto identificado
Confirmación externa	Evidencia de un tercero independiente	Laboratorio que emitió el certificado; operador de residuos
Condición contraria	Intentar lo que el control debe impedir	Ingresar a un área restringida sin credencial
Simulacro	Activar un plan en condiciones controladas	Evacuación, continuidad, retiro de producto
Análisis de datos	Revisar toda la población	Cruzar todas las compras con proveedores aprobados

¿Es correcto hacer pruebas durante la auditoría?

Nivel	Quién ejecuta	Ejemplo	Fuerza
1. Revisión de resultados	La organización o un tercero	Informe del último simulacro	Media
2. Ejecución observada	El auditado, ante el auditor	Verificación de arranque de una máquina	Alta
3. Ejecución sin intervenir	El auditor	Recalcular un indicador con datos fuente	Alta
4. Prueba activa	Auditor o especialista autorizado	Simulacro no anunciado	Muy alta



Para recordar: sí, si están autorizadas, son proporcionales al riesgo y las ejecuta alguien competente.

Pruebas no anunciadas: las que mejor evalúan controles que dependen de conductas; exigen más autorización y cuidado.

Muestreo en ocho pasos

1 Objetivo

¿Todas las compras fueron a proveedores aprobados?

2 Población

Todas las órdenes del período

3 Completitud

Obtenida del sistema y conciliada

4 Desviación

Definir qué cuenta como falla

5 Tamaño

Según frecuencia y riesgo

6 Selección

Aleatoria o sistemática, documentada

7 Evaluación

Registrar cada elemento

8 Conclusión

¿Aislada o sistémica? ¿Ampliar?

Por juicio: rápido y dirigido, sin extrapolación estadística · Estadístico: confianza conocida, exige más tiempo

Tamaños de muestra orientativos (riesgo moderado)

Frecuencia del control	Ocurrencias al año	Muestra mínima
Anual	1	1
Trimestral	4	2
Mensual	12	2 a 5
Semanal	52	5 a 15
Diaria	250 a 365	20 a 40
Varias veces al día	Más de 365	25 a 60
Automatizado	—	1 prueba + verificar que no cambió

Práctica habitual

No es un requisito normativo: ajústela en la metodología de la organización.

Análisis de datos

Cruzar toda la población suele ser más rápido y concluyente que una muestra de 25.

09

Mente que cuestiona vs. hacer la pregunta correcta

Dos habilidades distintas que los sesgos atacan



Mente que cuestiona vs. hacer la pregunta correcta

Como auditor, usted necesita tener una mente inquisitiva y la habilidad de hacer la pregunta correcta. Sin embargo, estos dos conceptos no son lo mismo.

Una persona puede tener una mente inquisitiva pero no saber cómo hacer la pregunta correcta, y viceversa.

Un auditor puede dudar de la exactitud de un registro, pero si no sabe qué preguntar para obtener evidencia relevante, no podrá verificar ni refutar su sospecha. Otro puede saber qué preguntar, pero si acepta la información sin más análisis, pasará por alto señales de alerta o riesgos.



Ejemplo

"Revisamos los accesos privilegiados cada trimestre."

El auditor eficaz pide la revisión del último trimestre, quién la hizo, cuántas cuentas revisó, cuáles se dieron de baja, y compara con las cuentas que existen hoy en el sistema.

Cuestionar y saber preguntar no son lo mismo

	Sabe preguntar	No sabe preguntar
Cuestiona	**Auditor eficaz** Duda y obtiene evidencia para resolver la duda	**Auditor frustrado** Sospecha pero no logra demostrar
No cuestiona	**Auditor ingenuo** Obtiene respuestas y las acepta	**Auditor de lista** Tilda casilleros

Escepticismo profesional: no aceptar sin evidencia, sin presuponer el resultado.

¿Cuáles son algunos sesgos comunes que afectan a ambos?

1 Confirmación

Percibir de forma selectiva información que confirma nuestras creencias. Por ejemplo, por la presión de los plazos o por aceptar evidencia sin cuestionarla.

2 Anclaje

Confiar demasiado en la primera información recibida, como un informe de pruebas “limpio” cuyo alcance nadie verificó.

3 Exceso de confianza

Confianza excesiva en los propios juicios, como cuando se confía en un responsable que fue colega y se omite el examen de la evidencia.

4 Pensamiento grupal

Priorizar la armonía del grupo sobre el análisis crítico. Un auditor junior no denuncia un problema si el líder no está de acuerdo.

5 Disponibilidad

Considerar más probable la información que se recuerda fácil, como la de las noticias, sin considerar otros factores.

✓ Cómo superarlos

Conocer los propios sesgos y evitar las trampas que impiden usar bien la mente interrogativa.

Cómo contrarrestar cada sesgo

Sesgo	Contramedida práctica
Confirmación	Formular la hipótesis contraria: “¿qué tendría que ver para concluir que este control no funciona?”
Anclaje	Obtener evidencia de al menos dos fuentes independientes antes de concluir
Exceso de confianza	Documentar como si otro auditor fuera a revisar el papel de trabajo sin conocer al auditado
Pensamiento grupal	Pedir primero la opinión de los menos experimentados; asignar el rol de abogado del diablo
Disponibilidad	Partir del análisis de riesgos y de la SoA de la organización, no de las noticias
Halo y autoridad	Evaluar cada control por separado, con su propia evidencia
Statu quo	Revisar los cambios desde la última auditoría antes de reutilizar el plan

10

El arte de hacer las preguntas correctas

Quién, qué, dónde, cuándo, por qué y cómo



Debate

¿Para ustedes qué es el arte de hacer las preguntas correctas en auditoría?

¿Tu nombre es…?



El arte de hacer la pregunta correcta

Como auditor, usted necesita saber cómo hacer las preguntas correctas para reunir evidencia relevante y confiable para sus procedimientos de auditoría.

Sin embargo, hacer las preguntas correctas no es una tarea sencilla. Requiere una consideración cuidadosa del contexto, el propósito de la investigación y la información necesaria para tomar decisiones informadas.

El éxito de una auditoría depende en gran medida de una comunicación eficaz entre los auditores y sus auditados. La piedra angular de esta comunicación es hacer las preguntas correctas.



¿Por qué es importante hacer la pregunta correcta?

1 Comprender

La naturaleza de un proceso o transacción y sus implicancias.

2 Evaluar riesgos

De error material, falla del control o fraude.

3 Diseñar

Procedimientos para obtener evidencia suficiente.

4 Evaluar evidencia

Su suficiencia y fiabilidad.

5 Concluir

Con conclusiones y recomendaciones razonables.

6 Evaluar controles

La eficacia de los controles internos.

7 Fortalecer la relación

La confianza fomenta información más precisa.

8 Pensar críticamente

Estimular el razonamiento del auditado.

El marco de las cinco W y una H

Para vincular la mente interrogativa con las habilidades de indagación:

W · Who · ¿Quién?

Personas, aprobadores, partes relacionadas

W · What · ¿Qué?

Proceso, documentos, controles

W · Where · ¿Dónde?

Ubicación, evidencia, jurisdicción

W · When · ¿Cuándo?

Ocurrencia, registro, revisión, cierre

W · Why · ¿Por qué?

Razón de ser y del tratamiento

H · How · ¿Cómo?

Proceso, autorización, verificación

Quién

La pregunta

- Ayuda a identificar quién participa en una transacción, quién debe aprobarla, quién sabe más sobre ella y quiénes pueden ser partes relacionadas
- Al preguntar “¿con quién estás hablando?”, considere lo que esa persona puede saber: un gerente de ventas sabe más de los riesgos de ventas que contabilidad
- ¿Quién debe aprobar? Un préstamo, alguien con autoridad; una orden de compra, alguien que verificó cantidad y calidad
- Terceros independientes pueden confirmar: la autoridad fiscal, el proveedor del servicio

En un sistema de gestión

- ¿Quién es el responsable del proceso y quién lo ejecuta en realidad?
- ¿Quién aprobó esta excepción? ¿Tenía autoridad para hacerlo?
- ¿Quién verifica que el control se hizo y es independiente de quien lo ejecuta?
- ¿Quién reemplaza al responsable cuando está de vacaciones?

Para recordar: “lo aprueba el área” no es un quién. Un quién tiene nombre, cargo y firma.

Qué

La pregunta

- Ayuda a comprender qué tipo de transacción es, qué documentos están disponibles o faltan, qué controles existen y qué afirmaciones son relevantes
- Afecta cómo se captura la población: si la factura es el documento fuente, deben incluirse todas en la selección
- Para comprender los controles, hay que saber qué documento inicia la transacción en el sistema
- Si falta una orden de compra, hay que verificar si los bienes se recibieron y pagaron

En un sistema de gestión

- ¿Qué dispara el proceso: un pedido, un cambio, un evento?
- ¿Qué registro queda cuando se ejecuta el control?
- ¿Qué criterio se usa para decidir si el resultado es aceptable?
- Si falta el registro de inspección de un lote, ¿cómo se liberó?

Para recordar: si la población la armó a mano el auditado, lo que se audita es su prolijidad, no el control.

Dónde

La pregunta

- Ayuda a determinar dónde ocurre la transacción, dónde están sus elementos clave, dónde buscar evidencia y qué leyes locales aplican
- Ejemplo financiero: dónde se almacena el inventario y si hay mercadería en tránsito
- Los términos FOB y CIF indican dónde se transfiere la responsabilidad entre vendedor y comprador
- Distintos países pueden tener distintas leyes que afectan cómo se registra una transacción

En un sistema de gestión

- ¿En qué sitios se realiza el proceso? ¿Los controles son iguales en todos?
- ¿Dónde se guardan los productos químicos, los residuos o los registros?
- ¿En qué país operan los proveedores críticos?
- ¿Qué legislación local aplica en cada sitio?

Para recordar: “en el depósito” no es una ubicación: es una forma elegante de no saber dónde está.

Cuándo

La pregunta

- Ayuda a identificar cuándo ocurre una transacción, cuándo se registra, liquida, revisa o concilia, y cuándo se aplican los cortes
- Ejemplo: si se otorgó un préstamo a un director, ¿cuándo se pagó?
- El momento puede revelar fraudes, como el kiting de cheques para ocultar faltantes de efectivo
- Un acuerdo firmado después del cierre puede cambiar el período en que se reconoce un resultado

En un sistema de gestión

- ¿La aprobación es anterior o posterior a la ejecución?
- ¿Cuándo venció la calibración y cuándo se usó el instrumento por última vez?
- ¿Cuánto tardó en investigarse el accidente o el reclamo?
- ¿Cuándo se cerró la acción correctiva y cuándo se verificó su eficacia?

Para recordar: comparar fechas es una de las pruebas más potentes y simples.

Por qué

La pregunta

- Ayuda a comprender por qué se inicia una transacción, por qué se registra así, por qué es inusual o significativa y si los juicios de la dirección son razonables
- Si se vende un activo con acuerdo de recompra vigente, la operación puede ser un préstamo
- Importa entender por qué una transacción se canaliza a través de distintas entidades

En un sistema de gestión

- ¿Por qué este requisito se declaró no aplicable?
- ¿Por qué este riesgo se aceptó en lugar de tratarse?
- ¿Por qué se aprobó este proveedor con puntaje bajo?
- ¿Por qué la revisión es anual y no trimestral?

Para recordar: “siempre se hizo así” es una respuesta muy honesta… y un excelente punto de partida para un hallazgo.

Cómo

La pregunta

- Ayuda a comprender cómo se procesa una transacción, cómo se autoriza, cómo se verifica, cómo se valora y cómo se divulga
- Ejemplo: emitir acciones, bonos o pagar en efectivo cambia los gastos por intereses u otras pérdidas
- Al entender estos factores, el auditor asegura que se consideró toda la información relevante

En un sistema de gestión

- ¿Cómo saben que el producto cumple antes de liberarlo?
- ¿Cómo se asegura que un contratista conoce los riesgos del sitio?
- ¿Cómo se mide la eficacia de la formación?
- ¿Cómo se detectaría un pago indebido?

Para recordar: “confiamos en el equipo” describe un clima laboral, no un control.

Dominar el arte de hacer preguntas

1 Escucha activa

Atención a respuestas y lenguaje corporal.

2 Esté preparado

Investigue operaciones, industria y procesos.

3 Plan de preguntas

Estructurado, pero flexible según las respuestas.

4 Diálogo abierto

Que el auditado se sienta cómodo para compartir.

5 Adapte su estilo

Al estilo de comunicación del auditado.

6 Lenguaje claro

Preguntas sencillas, sin jerga innecesaria.

7 Técnica del embudo

De lo amplio y abierto a lo específico.

8 Paciencia

Dé tiempo; no interrumpa ni apure.

Para recordar: neutralidad activa, validación de lo entendido y reflexión después de cada auditoría completan el arte.

11

Técnicas de interrogatorio del auditor

Empiece abierto, termine cerrado



Técnicas de interrogatorio del auditor ISO

Todos podemos hacer preguntas sencillas, pero el truco consiste en formularlas de manera que el auditado se sienta cómodo y sienta que puede responder abiertamente, sin críticas.

Los auditores no están ahí para juzgar a las personas, sino para buscar el cumplimiento de un conjunto de requisitos basados en el sistema de gestión de la organización.

Siempre conviene comenzar con una breve introducción sobre lo que se va a hacer, preguntar si el auditado ya pasó por esto antes y explicar lo que viene, con la idea de “romper muros”. Pedirle que hable de su proceso lo tranquiliza.



Elegir la técnica

Depende de la situación y de cómo responde el auditado: ¿es parco y da poca información, o abierto y comunicativo, describiendo bien las actividades?

Técnicas de interrogatorio (1)

Técnica	Ejemplo	Beneficios
Abierta: ¿Cómo…? ¿Por qué…? ¿Dónde…? ¿Qué…?	¿Cómo se reciben y procesan los pedidos de los clientes?	Relaja al auditado, fomenta el debate abierto y lo anima a describir las actividades en detalle
Cerrada: ¿Hace…? ¿Puede…? ¿Siempre…?	¿Siempre envían una copia del pliego de condiciones con el pedido? ¿Qué día se comprueban las alarmas?	Obtiene respuestas definitivas y aclara ambigüedades; a veces basta una respuesta breve
Reflexiva: Ha dicho que…	Ha dicho que los clientes no siempre dan todos los detalles. ¿Qué problemas puede causar?	Amplía información previa, explora “qué pasaría si” y muestra que el auditor escucha

Técnicas de interrogatorio (2)

Técnica	Ejemplo	Beneficios
Comparativa	¿En qué se diferencian los pedidos por teléfono de los pedidos por escrito?	Se centra en cuestiones específicas, abre la discusión y permite comparar
Hipotética: Imagine…	¿Qué pasaría si el pedido llegara sin las instrucciones completas?	Permite preguntar sobre situaciones que quizás no ocurrieron
Inductiva (liderazgo)	Cuando recibe el pedido lo revisa, lo firma y lo pasa a producción, ¿no?	Confirma la comprensión y resume; no debe ser fuente principal de evidencia



Para recordar: las preguntas capciosas sugieren una respuesta: evítelas salvo para confirmar comprensión o probar consistencia.

Tipos de preguntas en auditoría

Para obtener información

- Abiertas: alientan a dar detalle. “¿Cuál es el proceso para aprobar nuevos proveedores?”
- Cerradas: confirman hechos. “¿Todas las facturas fueron aprobadas por personal autorizado?”
- De sondeo: profundizan o aclaran. “¿Puede explicar el motivo de esta excepción a la política?”

Para evaluar comprensión

- Hipotéticas: evalúan cómo se manejaría un escenario. “¿Cómo manejaría un error importante en un informe?”
- Capciosas: sugieren una respuesta. “¿No estaría de acuerdo en que el proceso actual es ineficiente?” Evitarlas en la mayoría de los casos

Para recordar: la pregunta capciosa obtiene la respuesta que el auditor quería, no la que muestra la evidencia.

La técnica del embudo

1	2	3	4	5	6
Abierta	**Sondeo**	**Comparativa**	**Hipotética**	**Reflexiva**	**Cerrada**
¿Cómo gestionan los cambios?	¿Y si el cambio es urgente?	¿Igual para materia prima que para equipos?	Si mañana falta un insumo, ¿quién decide?	Entonces, los urgentes se aprueban por teléfono…	¿Me muestra los cambios del trimestre?



Para recordar: toda entrevista bien hecha termina con una solicitud de evidencia.

Consejos de interrogatorio

La secuencia

- Una buena auditoría de un proceso siempre comienza con una pregunta abierta y termina con una cerrada
- Una combinación de técnicas da una comprensión más profunda del proceso y la actividad
- Toda entrevista bien hecha termina con una solicitud de evidencia: “¿me lo muestra?”

La actitud

- No tenga miedo de decir “no entiendo” y pedir más información
- El silencio puede animar al auditado a dar más información
- Esté atento y concéntrese, sin tomar muchas notas: la interacción es vital
- Compare las respuestas con las de otro auditado a la misma pregunta
- Sepa qué requieren los procedimientos o normas para reconocer una respuesta y una evidencia aceptables

Para recordar: en controles técnicos, cada respuesta debe poder contrastarse con el sistema; si no, es solo una afirmación.

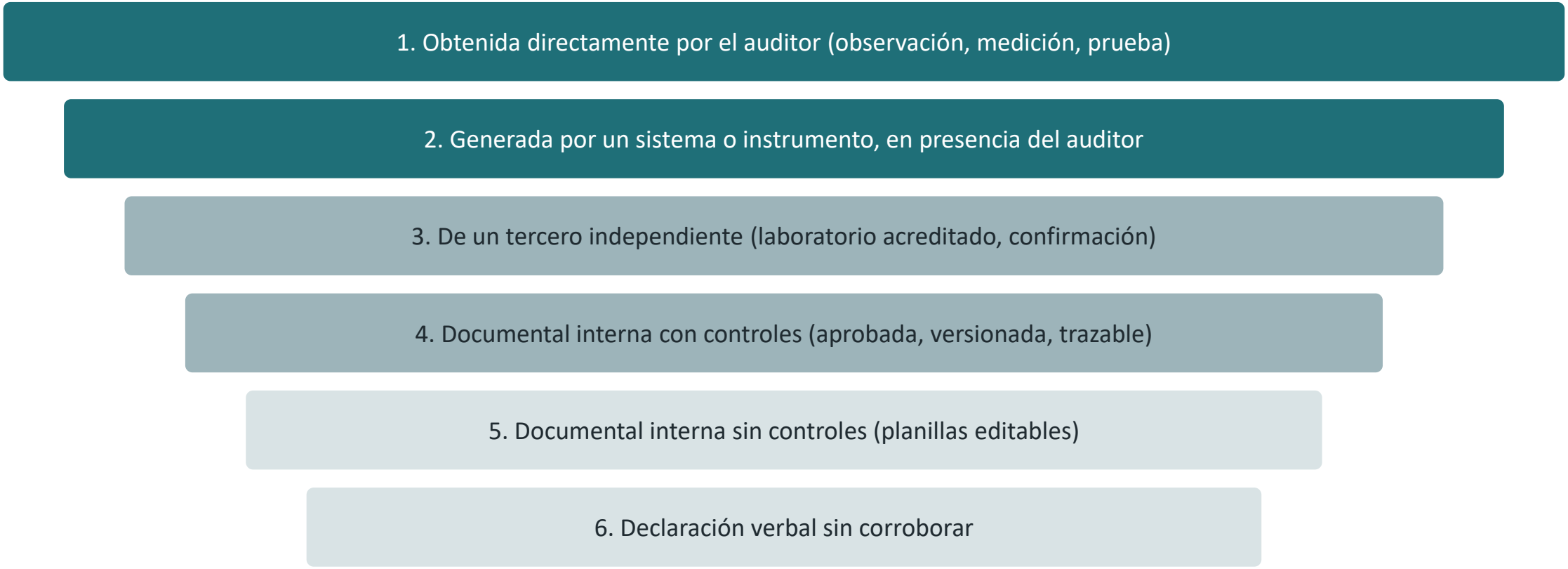
12

Evidencias, hallazgos e informe

Sin evidencia no hay hallazgo; sin seguimiento, vuelve



Jerarquía de fiabilidad de la evidencia



Para recordar: una evidencia débil gana fuerza cuando se corrobora con otra independiente.

Qué debe tener un papel de trabajo

Campo	Contenido
Identificación	Código, auditoría, control evaluado, auditor, fecha
Criterio	Requisito de la norma, procedimiento, ley o contrato
Objetivo	Qué se busca demostrar
Población y muestra	Fuente, tamaño, método de selección, elementos
Procedimiento	Pasos, métodos, personas entrevistadas
Resultados	Lo encontrado en cada elemento, con desviaciones
Conclusión	Eficaz, con observaciones o no eficaz; referencia al hallazgo
Revisión	Revisor y fecha

La prueba del papel

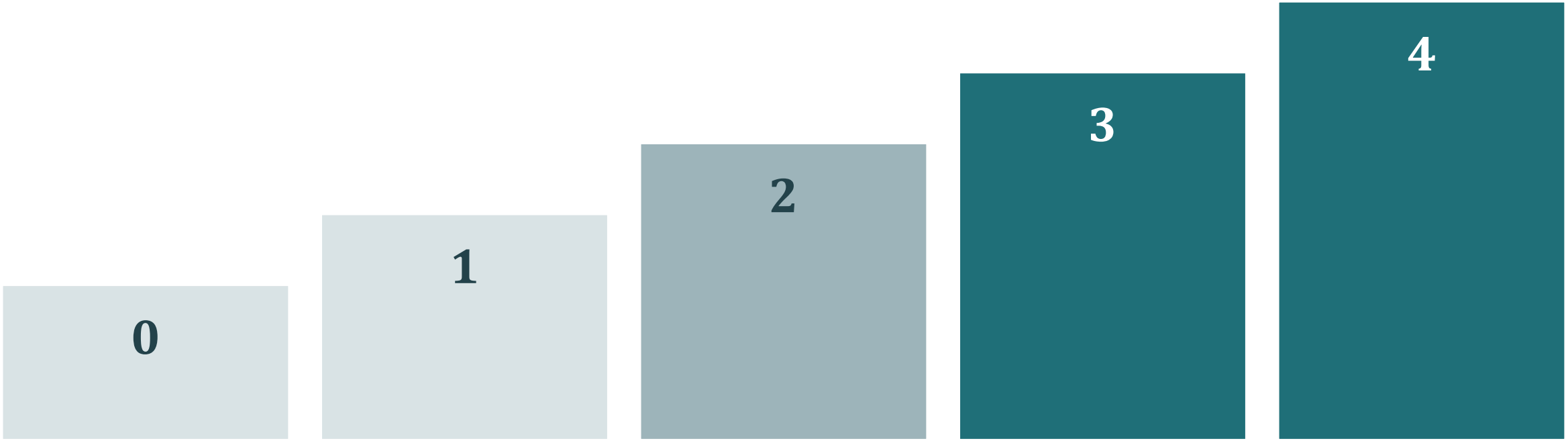
Otro auditor competente, sin haber estado, debe entender el trabajo y llegar a la misma conclusión.

Confidencialidad

Solo lo necesario, repositorio protegido, eliminación segura al vencer el plazo.

Una escala no binaria para cada control

Antes de concluir: ¿es realmente una desviación? ¿aislada o sistémica? ¿causa? ¿impacto? ¿controles compensatorios?



0 — No implementado
No existe o no se aplica

1 — Parcial
En parte del alcance o solo en papel

2 — Implementado
Sin evidencia de operación sostenida

3 — Eficaz
Opera de forma consistente, con evidencia

4 — Eficaz y en mejora
Además, se mide y se mejora

En la práctica

Una escala no binaria obliga a justificar cada color con evidencia, no con optimismo.

Verde, amarillo, rojo… y un auditor que pregunta por qué está en verde.



Clasificación de los hallazgos

Categoría	Definición	Ejemplo
No conformidad mayor	Afecta la capacidad del sistema de lograr sus resultados	No se realizó ninguna auditoría interna en el ciclo
No conformidad menor	Incumplimiento puntual que no afecta esa capacidad	2 de 25 órdenes sin aprobación
Observación	Puede derivar en incumplimiento	El control depende de una sola persona sin suplente
Oportunidad de mejora	Hacerlo mejor, sin incumplimiento	Bloquear en el sistema a proveedores vencidos



Para recordar: defina la clasificación antes de auditar y revise la consistencia al cierre.

En la práctica

Una no conformidad vale por su evidencia y su efecto, no por el tamaño de la pila de papeles.

Encontrar un hallazgo no es una competencia de alpinismo.



Criterio, condición, causa y efecto

1 Criterio

El procedimiento exige evaluar y aprobar a todo proveedor crítico antes de comprarle, y reevaluarlo cada año.

2 Condición

14 de 312 órdenes se emitieron a dos proveedores con la reevaluación vencida desde marzo.

3 Causa

El vencimiento se controla en una planilla aparte; el sistema no bloquea a los vencidos.

4 Efecto

Riesgo de recibir insumos de proveedores no verificados.

Mal redactado: “La gestión de proveedores es deficiente y no cumple la norma.”

Hechos y no opiniones · el sistema y no las personas · requisito exacto · evidencia referenciada

La reunión de cierre

1	2	3	4	5	6
Agradecer	**Limitaciones**	**Fortalezas**	**Hallazgos**	**Dudas**	**Próximos pasos**
Recordar objetivo, alcance y criterios	Muestras y tiempo disponible	Con ejemplos concretos	Por importancia, con evidencia	Se corrigen hechos, no se negocia la clasificación	Informe, plan de acción, seguimiento



Para recordar: el resumen ejecutivo responde en lenguaje de negocio: ¿hay confianza?, ¿qué riesgos?, ¿qué decisiones?

En la práctica

Si la dirección se sorprende en el cierre, la comunicación durante la auditoría falló.

La reunión de cierre: el momento en que nadie debería sorprenderse.



Del plan de acción a la eficacia comprobada

1 Implementación

La acción se hizo: procedimiento actualizado, sistema configurado, formación dada.

2 Eficacia

La acción eliminó la causa: nueva prueba con una muestra posterior.

3 Sostenibilidad

El control sigue funcionando: indicadores en los períodos siguientes.

- Distinguir corrección (arreglar el caso) de acción correctiva (eliminar la causa)
- La causa no puede ser solo “error humano”
- Cada acción necesita un criterio de eficacia medible

En la práctica

Cerrar un hallazgo es verificar la eficacia de la acción, no la fecha prometida en el plan.

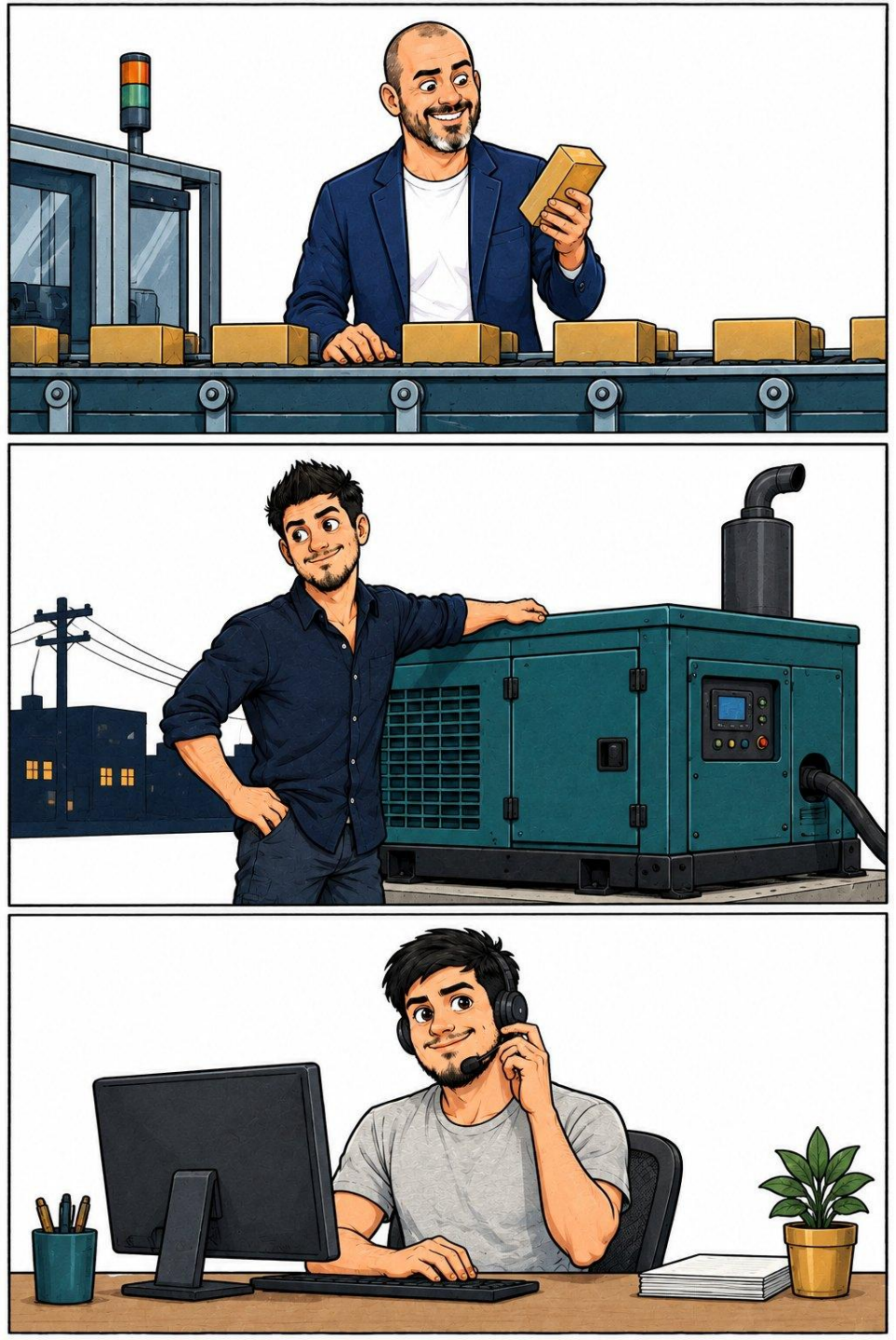
Las acciones correctivas también hay que regarlas.



13

ISO 9001, ISO 22301 e ISO/IEC 20000-1

Normas sin catálogo de controles… pero llenas de controles



Directrices y controles: parecidos, pero no iguales

Guía de controles

- Explica un control a la vez: propósito, implementación esperada, otra información
- Acompaña a un catálogo normativo: Anexo A de ISO/IEC 27001, 27701 o 42001
- Ejemplos: ISO/IEC 27002 para 27001; el Anexo B de 27701 y de 42001
- Su contenido se refleja en la Declaración de Aplicabilidad: control por control
- El auditor la usa para evaluar si un control seleccionado es eficaz

Guía de uso (directrices)

- Explica una cláusula a la vez, con la misma numeración que la norma de requisitos
- No agrega controles ni requisitos: dice qué se espera razonablemente de cada uno
- Ejemplos: ISO 22313 para 22301, ISO/TS 9002 para 9001, ISO/IEC 20000-2 para 20000-1, ISO/IEC 27003 para 27001
- No es certificable ni se declara: nadie firma una “Declaración de Aplicabilidad de la 22313”
- El auditor la usa para calibrar su criterio antes de auditar un requisito

Para recordar: “debe” es requisito, “debería” es recomendación. Un hallazgo contra una directriz es una opinión con formato de no conformidad.

Las guías de uso de cada norma (y sus parientes)

Norma de requisitos	Guía de uso (directrices)	Guías complementarias útiles para el auditor
ISO 9001:2015	ISO/TS 9002:2016	ISO 9004 (éxito sostenido); APG de ISO 9001 (Auditing Practices Group)
ISO 22301:2019	ISO 22313:2020	ISO/TS 22317 (BIA), ISO/TS 22318 (cadena de suministro), ISO/TS 22331 (estrategias), ISO/TS 22332 (planes y procedimientos)
ISO/IEC 20000-1:2018	ISO/IEC 20000-2:2019	ISO/IEC 20000-3 (definición del alcance y aplicabilidad)
ISO/IEC 27001:2022	ISO/IEC 27003:2017	ISO/IEC 27002 (guía de controles), ISO/IEC 27005 (riesgos)
ISO 31000 e ISO 19011	Ya son directrices	IEC 31010 (técnicas de evaluación de riesgos). Ninguna de las dos se certifica



Para recordar: la guía de uso no amplía la norma. Si la organización cumple el requisito por otro camino, el camino es válido.

ISO 9001: la norma que todos creen conocer

Es la norma de sistemas de gestión más difundida del mundo, y quizás por eso la más subestimada. Se apoya en siete principios: enfoque al cliente, liderazgo, compromiso de las personas, enfoque a procesos, mejora, toma de decisiones basada en evidencia y gestión de las relaciones.

Combina el enfoque a procesos, el ciclo PHVA y el pensamiento basado en riesgos. Y no, no exige un método formal de gestión de riesgos: exige pensar. Algo bastante más difícil de evidenciar con una plantilla.

Solo admite declarar no aplicables requisitos que no afecten la capacidad de dar productos y servicios conformes (4.3). “No diseñamos nada” suele durar hasta que alguien pregunta quién cambió el producto el mes pasado.



Para el auditor

La 9001 no tiene anexo de controles, pero su cláusula 8 está llena de ellos: requisitos del cliente, diseño, proveedores externos, producción, liberación y salidas no conformes.

ISO 9001: los controles escondidos en la cláusula 8

Cláusula	Control	Prueba sugerida
7.1.5	Recursos de seguimiento y medición	Instrumentos en uso: calibración vigente y trazable; qué se hizo con lo medido con un equipo fuera de tolerancia
7.1.6	Conocimientos de la organización	¿Qué pasa cuando se jubila el que “sabe cómo se hace”?
8.2	Requisitos de productos y servicios	Muestra de pedidos: revisión antes de aceptar; cambios comunicados
8.3	Diseño y desarrollo	Un desarrollo reciente: revisión, verificación, validación y control de cambios
8.4	Control de procesos externos	Compras a proveedores evaluados; seguimiento del desempeño
8.5	Producción y provisión del servicio	Recorrido de una orden: condiciones controladas, identificación y trazabilidad
8.6	Liberación	¿Quién liberó el lote y con qué evidencia?
8.7	Salidas no conformes	Producto no conforme: identificado, segregado y decidido por alguien con autoridad

Auditar el pensamiento basado en riesgos (APG de ISO 9001)

Lo que recomienda el APG

- No se audita aislado: debe estar implícito en toda la auditoría, incluida la entrevista con la alta dirección
- Entradas a verificar: cuestiones internas y externas, dirección estratégica, partes interesadas, alcance y procesos
- No hay requisito específico sobre cómo documentar los riesgos y oportunidades
- La evidencia puede ser variada: actas, planes, análisis, decisiones

Traducción práctica

- No pida “la matriz de riesgos” como si fuera obligatoria
- Pregunte cómo decidieron qué controlar y con qué intensidad
- Busque el riesgo en las decisiones: compras, diseño, cambios, capacidad
- Una organización chica puede pensar en riesgos sin escribir 40 páginas sobre eso

Para recordar: si el auditor exige un documento que la norma no exige, el hallazgo es del auditor.

ISO 22301: continuidad del negocio

Especifica los requisitos de un sistema de gestión de la continuidad del negocio: prepararse para las interrupciones, responder y recuperarse. Su corazón está en la cláusula 8: análisis de impacto, evaluación de riesgos, estrategias, planes, ejercicios y evaluación.

El análisis de impacto en el negocio (8.2.2) define tipos y criterios de impacto, identifica actividades, evalúa los impactos en el tiempo y fija el plazo en que no reanudar se vuelve inaceptable: el período máximo tolerable de interrupción (MTPD). Dentro de ese plazo se fijan los objetivos de tiempo de recuperación (RTO).

Y la evaluación de riesgos (8.2.3) remite a ISO 31000. Sí, todo vuelve a la 31000. Para interpretar cada requisito existe ISO 22313:2020, que da directrices, no controles: ayuda a entender qué se espera, pero no agrega nada que auditar.



La frase que conviene recordar

Un plan de continuidad que nunca se ejercitó no es un plan: es literatura. Bien escrita, a veces.

ISO 22301: la cláusula 8 como mapa de auditoría

Cláusula	Tema	Qué evidencia pedir
8.2.2	Análisis de impacto en el negocio (BIA)	Criterios de impacto, actividades priorizadas, MTPD, RTO, recursos y dependencias (incluidos proveedores)
8.2.3	Evaluación de riesgos	Riesgos de interrupción de actividades priorizadas y sus recursos
8.3	Estrategias y soluciones	Opciones evaluadas, seleccionadas y con recursos asignados
8.4	Planes y procedimientos	Estructura de respuesta, alerta y comunicación, planes y recuperación
8.5	Programa de ejercicios	Ejercicios con objetivos, escenarios realistas, informes y mejoras
8.6	Evaluación de la documentación y capacidades	Revisión tras ejercicios, incidentes y cambios



Para recordar: compare el RTO del BIA con el tiempo real del último ejercicio. Si nunca lo midieron, ya sabe dónde mirar.

Auditar continuidad sin creer en el plan

Preguntas incómodas

- ¿Quién definió el MTPD y con qué criterio? ¿El dueño del negocio o el área de sistemas?
- ¿Los RTO del BIA coinciden con lo que contrataron a los proveedores?
- ¿El último ejercicio tuvo un escenario realista o el de siempre?
- ¿Qué falló en el último ejercicio? (“Nada” no es una respuesta creíble)
- ¿Se puede activar el plan si el responsable está de vacaciones?

Pruebas sugeridas

- Seguir una actividad priorizada desde el BIA hasta su estrategia, su plan y su último ejercicio
- Verificar los contactos del árbol de llamadas: llamar a uno
- Comparar dependencias del BIA con contratos y acuerdos de nivel de servicio
- Revisar que las mejoras de ejercicios anteriores se implementaron

Para recordar: un ejercicio en el que todo salió perfecto suele indicar que el escenario fue perfecto, no la organización.

En la práctica

Un plan se prueba en el escenario en que se va a usar, no en la sala de reuniones.

El plan de continuidad funciona perfecto. Mientras haya luz para leerlo.



ISO/IEC 20000-1: el sistema de gestión de servicios

Especifica los requisitos para un sistema de gestión de servicios (SGS): planificar, diseñar, entregar y mejorar servicios que cumplan los requisitos acordados. Sigue la estructura armonizada, y su cláusula 8 concentra los procesos de servicio.

Para quien viene de ITIL, la sorpresa es que la norma no pide “implementar ITIL”: pide procesos con resultados demostrables. Para quien viene de ISO/IEC 27001, la sorpresa es que la seguridad de la información aparece como un proceso más del servicio (8.7.3).

Y si la organización terceriza parte de los servicios, debe seguir controlándola (8.2.3). Tercerizar el proceso no terceriza la responsabilidad. Nunca. En ninguna norma.



El dato

La cláusula 8 de ISO/IEC 20000-1 tiene siete bloques: porfolio de servicios, relación y acuerdo, oferta y demanda, diseño y transición, resolución y ejecución, y aseguramiento del servicio.

ISO/IEC 20000-1: la cláusula 8 en una tabla

Bloque	Procesos	Prueba sugerida
8.2 Porfolio de servicios	Planificación, catálogo, activos, configuración, partes involucradas	Comparar el catálogo publicado con lo que realmente se presta
8.3 Relación y acuerdo	Relación con el negocio, niveles de servicio, proveedores	Niveles de servicio acordados frente a los medidos
8.4 Oferta y demanda	Presupuesto y contabilidad, demanda, capacidad	Planes de capacidad frente a incidentes por saturación
8.5 Diseño, construcción y transición	Cambios, diseño y transición, entregas y despliegues	Muestra de cambios: evaluación, aprobación, prueba y vuelta atrás
8.6 Resolución y ejecución	Incidencias, peticiones, problemas	Incidentes recurrentes: ¿se abrió un problema y se encontró la causa?
8.7 Aseguramiento de servicios	Disponibilidad, continuidad, seguridad de la información	Disponibilidad medida y prueba de continuidad del servicio

Para recordar: un incidente que se repite diez veces y nunca generó un problema no es mala suerte: es un proceso que no funciona.

En la práctica

La gestión de cambios se evalúa por la vuelta atrás que funcionó, no por la firma de aprobación.

El cambio estaba aprobado. El efecto dominó, no tanto.



14

Rutas de auditoría comunes a cualquier norma

Catorce áreas Planificar–Hacer–Verificar–Actuar



Catorce áreas comunes y sus cláusulas

N.º	Área	Cláusula
1	Contexto y partes interesadas	4
2	Liderazgo, política y roles	5
3	Riesgos y oportunidades	6.1
4	Objetivos y cambios	6.2, 6.3
5	Recursos, competencia, comunicación	7.1 a 7.4
6	Información documentada	7.5
7	Control operacional	8.1

N.º	Área	Cláusula
8	Procesos y proveedores externos	8
9	Requisitos legales	4.2, 6.1, 9.1
10	Emergencias e interrupciones	8
11	Seguimiento e indicadores	9.1
12	Auditoría interna	9.2
13	Revisión por la dirección	9.3
14	No conformidades y mejora	10

Área 8. Control de proveedores y procesos externos

Aplica a: ISO 9001 (8.4), ISO/IEC 20000-1 (8.2.3, 8.3.4), ISO/IEC 27001 (A.5.19 a A.5.22) · **Justificación:** cada vez más procesos críticos los hacen terceros; tercerizar el proceso no terceriza la responsabilidad.

Planificar

- ¿Hay criterios de evaluación, selección y reevaluación?
- ¿Se gradúan por criticidad o riesgo del proveedor?
- ¿Se definieron los requisitos que se trasladan al proveedor?
- ¿Se identificaron los procesos tercerizados que afectan al sistema?

Hacer

- ¿Los proveedores críticos se evaluaron antes de contratarlos?
- ¿Los contratos incluyen requisitos y derecho a verificar?
- ¿Se verifica lo recibido antes de usarlo?
- ¿Se comunican los cambios de requisitos?

Área 8. Control de proveedores y procesos externos (cont.)

Verificar

- ¿Hay indicadores de desempeño de proveedores?
- ¿Se reevalúan en plazo?
- ¿Se analizan sus no conformidades?

Actuar

- ¿Qué se hace con los de bajo desempeño?
- ¿Se comparten lecciones aprendidas?
- ¿Se ajustan criterios ante nuevos riesgos?

Para recordar: prueba sugerida: cruzar todas las compras del período con la lista de proveedores aprobados y vigentes.

Área 10. Análisis de impacto y ejercicios de continuidad

Aplica a: ISO 22301 (8.2, 8.5), ISO/IEC 27001 (A.5.30), ISO/IEC 20000-1 (8.7.2) · **Justificación:** el BIA define qué recuperar primero y en cuánto tiempo; los ejercicios demuestran si es posible.

Planificar

- ¿Están definidos los tipos y criterios de impacto?
- ¿Se identificaron las actividades que soportan productos y servicios?
- ¿Se definió el MTPD y el RTO de cada actividad priorizada?
- ¿Se identificaron recursos y dependencias, incluidos proveedores?
- ¿Hay un programa de ejercicios con objetivos y escenarios?
- ¿Quién aprobó los resultados del BIA?

Hacer

- ¿El BIA se actualizó tras cambios del negocio?
- ¿Las estrategias cubren las actividades priorizadas dentro del RTO?
- ¿Los contratos con proveedores críticos son coherentes con los RTO?
- ¿Se realizaron los ejercicios planificados?
- ¿Participaron las personas que actuarían en una crisis real?
- ¿Se documentaron los resultados?

Área 10. Análisis de impacto y ejercicios de continuidad (cont.)

Verificar

- ¿Se compararon los tiempos reales con los RTO?
- ¿Se evaluaron los planes tras ejercicios e incidentes?
- ¿Se verificaron los contactos y recursos alternativos?
- ¿La dirección conoce los resultados?

Actuar

- ¿Se implementaron las mejoras de ejercicios anteriores?
- ¿Se ajustaron estrategias que no cumplieron el RTO?
- ¿Se repitieron los ejercicios fallidos?
- ¿Se actualizaron BIA y riesgos con lo aprendido?

Para recordar: prueba sugerida: seguir una actividad priorizada desde el BIA hasta su último ejercicio y comparar RTO con tiempo real.

Adaptar el método a cada norma

Norma	Cómo identifica lo que puede salir mal	Prueba sugerida
ISO 9001	Riesgos sobre la conformidad y la satisfacción del cliente	Recorrido de un pedido; reejecución de una inspección
ISO 14001	Aspectos ambientales y obligaciones de cumplimiento	Seguir un residuo hasta su disposición final
ISO 45001	Peligros y evaluación de riesgos con participación	Observación no anunciada de tareas críticas
ISO 22301	Análisis de impacto y riesgos de interrupción	Comparar tiempos de un ejercicio con objetivos
ISO 37001	Riesgo de soborno por actividad, país y socio	Análisis de pagos a terceros de alto riesgo
ISO 50001	Revisión energética y usos significativos	Recalcular un indicador energético
ISO 22000	Análisis de peligros para la inocuidad	Prueba de trazabilidad hacia atrás y adelante

Síntesis: la eficacia del sistema a través de sus controles

P Planificar

¿Los controles que fallan tratan riesgos identificados como altos?

H Hacer

¿Las fallas se deben a recursos, competencia o procedimientos?

V Verificar

¿La organización las había detectado con sus indicadores y auditorías?

A Actuar

¿Las acciones anteriores fueron eficaces? ¿La dirección decidió?



Para recordar: aquí se encuentran las dos perspectivas: el control que falla y el sistema que no lo vio.

En la práctica

El ciclo PHVA no termina; un sistema que dejó de mejorar ya empezó a degradarse.

La mejora continua: empujar cuesta arriba, siempre.



Parte II · Normas con anexos técnicos

ISO/IEC 27001, 27701, 42001, 27017, 27018: riesgo, anexo, Declaración de Aplicabilidad y evaluación de controles



15

Normas de gestión con anexos técnicos

Requisitos de gestión + catálogo de controles

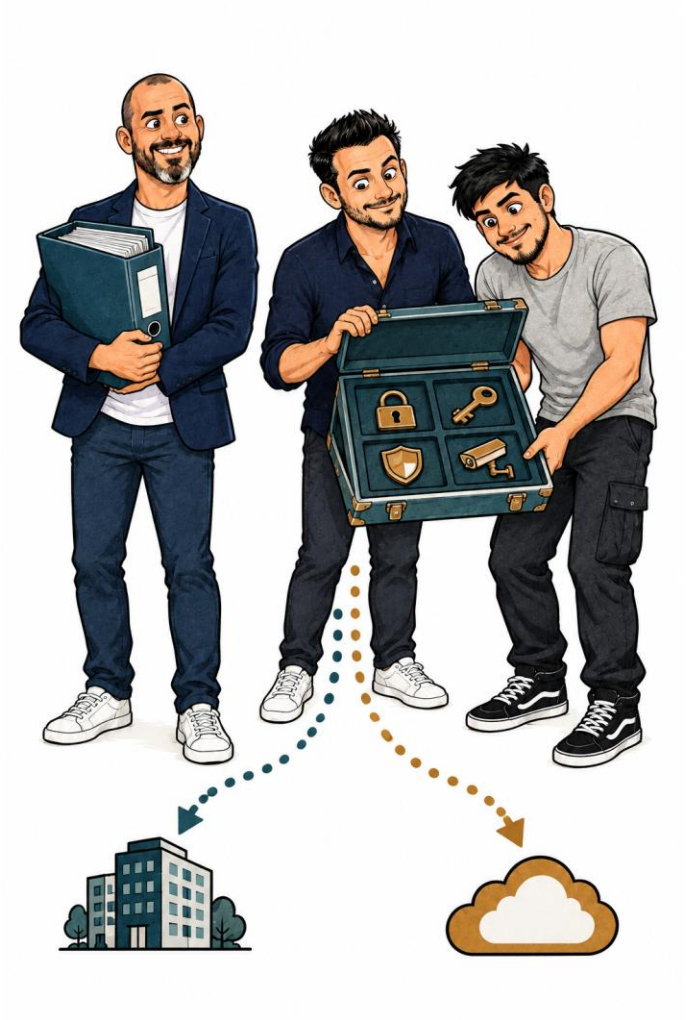


Qué es una norma con anexo técnico

Algunas normas de gestión agregan a las cláusulas 4 a 10 un anexo con un catálogo de controles de referencia. Es el caso de ISO/IEC 27001 (seguridad de la información), ISO/IEC 27701 (privacidad) e ISO/IEC 42001 (inteligencia artificial).

El anexo es normativo, pero no obliga a implementar todos sus controles: la organización elige los necesarios a partir de su tratamiento de riesgos, compara su selección con el anexo para no omitir nada y documenta la decisión en una Declaración de Aplicabilidad.

Otras normas, como ISO 14001, ISO 45001 o ISO 37001, tienen anexos informativos de orientación: ayudan a interpretar, pero no son un catálogo de controles a declarar.



Para el auditor

Con un anexo técnico, la auditoría tiene dos objetos: el sistema de gestión (4 a 10) y los controles seleccionados. Por eso se necesitan dos métodos: auditar el sistema y evaluar los controles.

Normas con y sin catálogo de controles

Norma	Disciplina	Anexo	Contenido del anexo
ISO/IEC 27001:2022	Seguridad de la información	Anexo A normativo	93 controles en 4 temas; guía en ISO/IEC 27002:2022
ISO/IEC 27701:2025	Privacidad (PIMS)	Anexo A normativo + Anexo B guía	78 controles en 3 tablas: responsables, encargados y seguridad compartida
ISO/IEC 42001:2023	Inteligencia artificial	Anexo A normativo + Anexo B guía	38 controles en 9 áreas (A.2 a A.10); Anexos C y D informativos
ISO/IEC 27017 y 27018	Nube y datos personales en nube	Controles extendidos	Amplían ISO/IEC 27002 para proveedores y clientes de nube
ISO 14001, 45001, 37001	Ambiente, SST, antisoborno	Anexo A informativo	Orientación para interpretar requisitos; no es un catálogo a declarar
ISO 9001, 22301, 37301	Calidad, continuidad, cumplimiento	Sin catálogo de controles	Los controles surgen del riesgo y de la cláusula 8; tienen guías de uso con directrices (ISO/TS 9002, ISO 22313)

Anatomía de una norma con anexo técnico

1 Requisitos de gestión

Cláusulas 4 a 10: contexto, liderazgo, riesgos, apoyo, operación, evaluación y mejora. No admiten exclusiones.

2 Anexo de controles

Catálogo normativo de referencia (“debe”). Se usa para seleccionar controles y verificar que no se omitió ninguno necesario.

3 Guía de implementación

ISO/IEC 27002 o el Anexo B de 27701 y 42001 (“debería”). Dice qué esperar de cada control.

4 Declaración de Aplicabilidad

Une todo: controles necesarios, justificación de inclusión y exclusión, y estado de implementación.

Para recordar: la Declaración de Aplicabilidad es el mapa del auditor: de ahí salen los controles a evaluar.

Del riesgo al control en una norma con anexo

1 — Evaluar riesgos

Identificar, analizar y valorar con criterios definidos

2 — Elegir opciones

Tratar, evitar, transferir o aceptar

3 — Determinar controles

Los necesarios, de cualquier fuente

4 — Comparar con el anexo

Verificar que no se omitió ninguno necesario

5 — Declaración de Aplicabilidad

Incluidos, excluidos, justificación, estado

6 — Plan de tratamiento

Aprobado por los dueños del riesgo



Para recordar: el anexo no es el punto de partida: es el control de calidad de la selección hecha por riesgo.

Qué auditar en la Declaración de Aplicabilidad

Preguntas clave

- ¿Incluye todos los controles necesarios, del anexo y adicionales?
- ¿Justifica la inclusión de cada control con el riesgo que trata?
- ¿Justifica cada exclusión con argumentos verificables?
- ¿Indica si cada control está implementado o no?
- ¿Coincide con el plan de tratamiento y con la realidad?
- ¿Está aprobada, versionada y vigente?

Señales de alerta

- Todos los controles “aplica” sin vínculo con riesgos
- Exclusiones como “no aplica a nuestro negocio” sin más
- Controles “implementados” que nadie puede mostrar
- Una SoA copiada de una plantilla o de otra empresa
- Controles adicionales necesarios que no figuran
- Fecha de la SoA anterior a cambios relevantes

Para recordar: pruebe la SoA en ambos sentidos. Si todos los controles dicen “aplica”, felicitaciones: encontraron una plantilla.

Trampas propias de las normas con anexos

Del lado de la organización

- Implementar el anexo como checklist, sin análisis de riesgos
- Copiar la redacción del anexo en las políticas
- Declarar exclusiones para reducir el esfuerzo
- Confundir “documentado” con “implementado”
- Olvidar los controles complementarios de proveedores de nube o de IA

Del lado del auditor

- Auditar solo el anexo y olvidar las cláusulas 4 a 10
- Auditar solo las cláusulas y no bajar a los controles
- Evaluar los 93 (o 38, o 78) controles de forma superficial
- No tener competencia técnica para el control evaluado
- Aceptar capturas o documentos como prueba de operación

Para recordar: auditar 93 controles en dos días se puede; que alguno quede evaluado de verdad, es otra historia.

16

ISO/IEC 27001, 27701 y 42001 en detalle

Tres normas, un mismo patrón de anexo



ISO/IEC 27001: requisitos del SGSI

Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) dentro del contexto de la organización.

Incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos son genéricos y aplicables a cualquier organización, independientemente de su tipo, tamaño o naturaleza.

La exclusión de cualquiera de los requisitos de las cláusulas 4 a 10 no es aceptable cuando una organización declara conformidad. Unas 19 páginas de requisitos más el Anexo A.



El Anexo A

93 controles de referencia (edición 2022), agrupados en 4 temas. La guía de cada control está en ISO/IEC 27002:2022, de unas 152 páginas.

Anexo A de ISO/IEC 27001:2022: de 114 a 93 controles

Aspecto	Edición 2013	Edición 2022
Número de controles	114	93
Agrupación	14 dominios	4 temas
Controles nuevos	—	11
Descripción	Objetivo, control y guía	Atributos, control, propósito y guía

Tema	Controles
5. Organizacionales	37
6. De personas	8
7. Físicos	14
8. Tecnológicos	34

La reducción no eliminó exigencias: la mayoría de los controles se agruparon, unos pocos se eliminaron por redundantes y se agregaron 11 nuevos.



Para recordar: 45 de los 93 controles son organizacionales o de personas: la norma “en serio no es técnica”.

Los 11 controles nuevos de ISO/IEC 27002:2022

Control	Nombre	Qué debe buscar el auditor
5.7	Inteligencia de amenazas	Fuentes, análisis y uso en decisiones de seguridad
5.23	Seguridad en el uso de servicios en la nube	Procesos para adquirir, usar, gestionar y abandonar servicios
5.30	Preparación de las TIC para la continuidad	Requisitos derivados del análisis de impacto, y pruebas
7.4	Monitoreo de la seguridad física	Vigilancia para detectar accesos no autorizados
8.9	Gestión de la configuración	Configuraciones de referencia documentadas, aplicadas y revisadas
8.10	Eliminación de información	Borrado cuando ya no se necesita, con evidencia
8.11	Enmascaramiento de datos	Datos personales o sensibles enmascarados según política
8.12	Prevención de fuga de datos	Detección y prevención en sistemas, redes y dispositivos
8.16	Actividades de monitoreo	Detección de comportamiento anómalo
8.23	Filtrado web	Gestión del acceso a sitios externos
8.28	Codificación segura	Principios de codificación segura en el desarrollo

La nueva descripción de los controles: atributos

Atributo	Valores	Pregunta que responde
Tipo de control	Preventivo, Detectivo, Correctivo	¿Cuándo actúa respecto del incidente?
Propiedades de seguridad	Confidencialidad, Integridad, Disponibilidad	¿Qué propiedad protege?
Conceptos de ciberseguridad	Identificar, Proteger, Detectar, Responder, Recuperar	¿En qué función del ciclo encaja?
Capacidades operativas	Gobernanza, gestión de activos, identidades y accesos, amenazas y vulnerabilidades, continuidad…	¿Qué área operativa lo gestiona?
Dominios de seguridad	Gobernanza y ecosistema, Protección, Defensa, Resiliencia	¿En qué gran dominio se ubica?

Ejemplo, control 5.1 Políticas de seguridad de la información: #Preventivo · #Confidencialidad #Integridad #Disponibilidad · #Identificar · #Gobernanza · #Gobernanza_y_Ecosistema #Resiliencia

Para recordar: para el auditor, el “propósito” de cada control vale más que su letra.

Debate

¿Por qué es importante plantear los controles por atributos y qué relación tiene con el pensamiento basado en riesgo?

Pista: ¿qué pasa si todos los controles que tratan un riesgo crítico son preventivos?



ISO/IEC 27701: de extensión a sistema de gestión propio

La primera edición (2019) definía el sistema de gestión de la información de privacidad (PIMS) como una extensión de ISO/IEC 27001 e ISO/IEC 27002: no podía certificarse sin un SGSI.

La segunda edición (2025) eliminó esa dependencia: el PIMS puede implementarse de forma independiente, con sus propias cláusulas 4 a 10, o integrarse con un SGSI. La certificación se rige por ISO/IEC 27706.

Anexo A (normativo): controles. Anexo B (normativo): guía de implementación con la misma numeración. Anexos C a F (informativos): correspondencias con ISO/IEC 29100, el RGPD, ISO/IEC 27018 y 29151, y con la edición 2019. Traducción: ya no hay excusa para no saber qué control responde a qué artículo.



Anexo A de 27701:2025

78 controles en 3 tablas:

- A.1: 31 para responsables del tratamiento
- A.2: 18 para encargados del tratamiento
- A.3: 29 de seguridad compartidos por ambos roles

Cómo auditar un sistema de privacidad (ISO/IEC 27701)

Antes de evaluar controles

- ¿La organización determinó si actúa como responsable, encargado o ambos, por cada tratamiento?
- ¿Identificó la legislación aplicable: RGPD, LGPD, leyes locales?
- ¿Hay un inventario de tratamientos con finalidad y base legal?
- ¿La SoA distingue los controles de responsable y de encargado?
- ¿El análisis de riesgos considera el riesgo para las personas, no solo para la organización?

Controles con mayor valor de prueba

- Evaluaciones de impacto en la privacidad: muestra y calidad
- Derechos de los titulares: muestra de solicitudes y plazos
- Consentimiento: registro, vigencia y retiro
- Transferencias internacionales y subencargados
- Minimización, retención y eliminación de datos personales
- Notificación de violaciones de datos en plazo

Para recordar: si el auditado no sabe si es responsable o encargado, no hace falta abrir el Anexo A: ya tiene el primer hallazgo.

En la práctica

Preguntar a dónde van los datos es más útil que preguntar si existe una política de privacidad.

Los datos personales no se fugan: salen volando, de a uno.

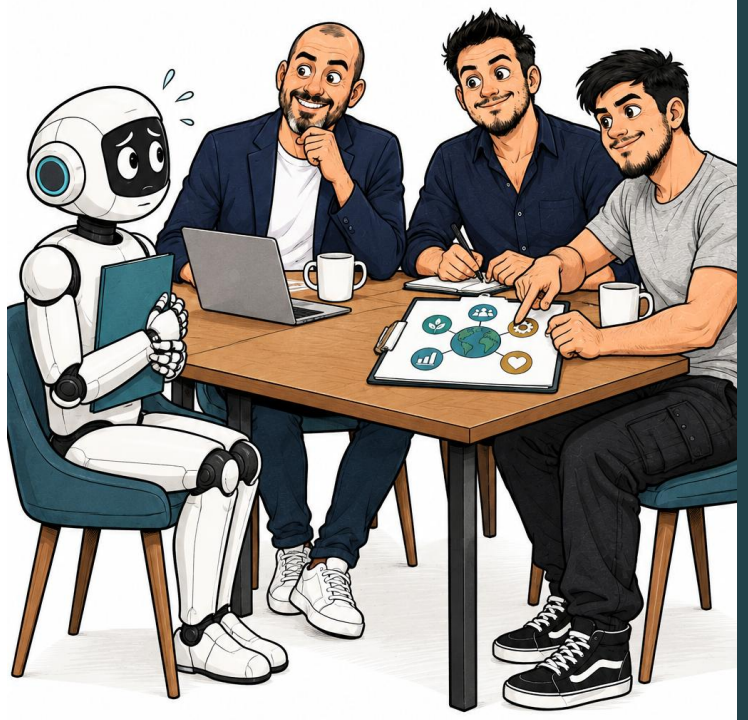


ISO/IEC 42001:2023: sistema de gestión de inteligencia artificial

Especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de IA (AIMS) en organizaciones que desarrollan, proveen o usan sistemas de inteligencia artificial.

Sigue la estructura armonizada e incorpora requisitos propios, como la evaluación de impacto de los sistemas de IA sobre las personas, grupos y la sociedad.

La evaluación de impacto (6.1.4) determina las consecuencias potenciales para personas, grupos y sociedades, y puede integrarse en la evaluación de riesgos; la cláusula 8.4 exige llevarla a la práctica. Como en ISO/IEC 27001, hay que seleccionar controles por riesgo, compararlos con el Anexo A y documentar una Declaración de Aplicabilidad.



Sus anexos

A (normativo): 38 controles en 9 áreas.
B (normativo): guía de implementación.
C (informativo): objetivos y fuentes de riesgo de IA.
D (informativo): uso por sectores e integración con otras normas.

Anexo A de ISO/IEC 42001: 38 controles en 9 áreas

Área	Nombre	Controles	Qué buscar como auditor
A.2	Políticas relacionadas con la IA	3	Política de IA alineada con otras políticas y revisada
A.3	Organización interna	2	Roles, responsabilidades y reporte de inquietudes
A.4	Recursos para los sistemas de IA	5	Inventario de datos, herramientas, cómputo y personas
A.5	Evaluación de impactos de los sistemas de IA	4	Proceso, documentación y alcance de las evaluaciones
A.6	Ciclo de vida de los sistemas de IA	9	Requisitos, diseño, verificación, despliegue, monitoreo, registros
A.7	Datos para los sistemas de IA	5	Origen, calidad, procedencia y preparación de datos
A.8	Información para las partes interesadas	4	Documentación para usuarios, comunicación de incidentes
A.9	Uso de los sistemas de IA	3	Uso responsable y dentro del propósito previsto
A.10	Relaciones con terceros y clientes	3	Responsabilidades con proveedores y clientes

Cómo auditar un sistema de gestión de IA (ISO/IEC 42001)

Antes de evaluar controles

- ¿Hay un inventario de sistemas de IA dentro del alcance, con su rol (desarrollador, proveedor, usuario)?
- ¿Los objetivos de IA consideran equidad, transparencia, seguridad, privacidad y rendición de cuentas?
- ¿La evaluación de riesgos incluye fuentes propias de la IA (datos, aprendizaje automático, opacidad)?
- ¿Se evalúa el impacto sobre personas y sociedad, además del riesgo para la organización?

Pruebas sugeridas

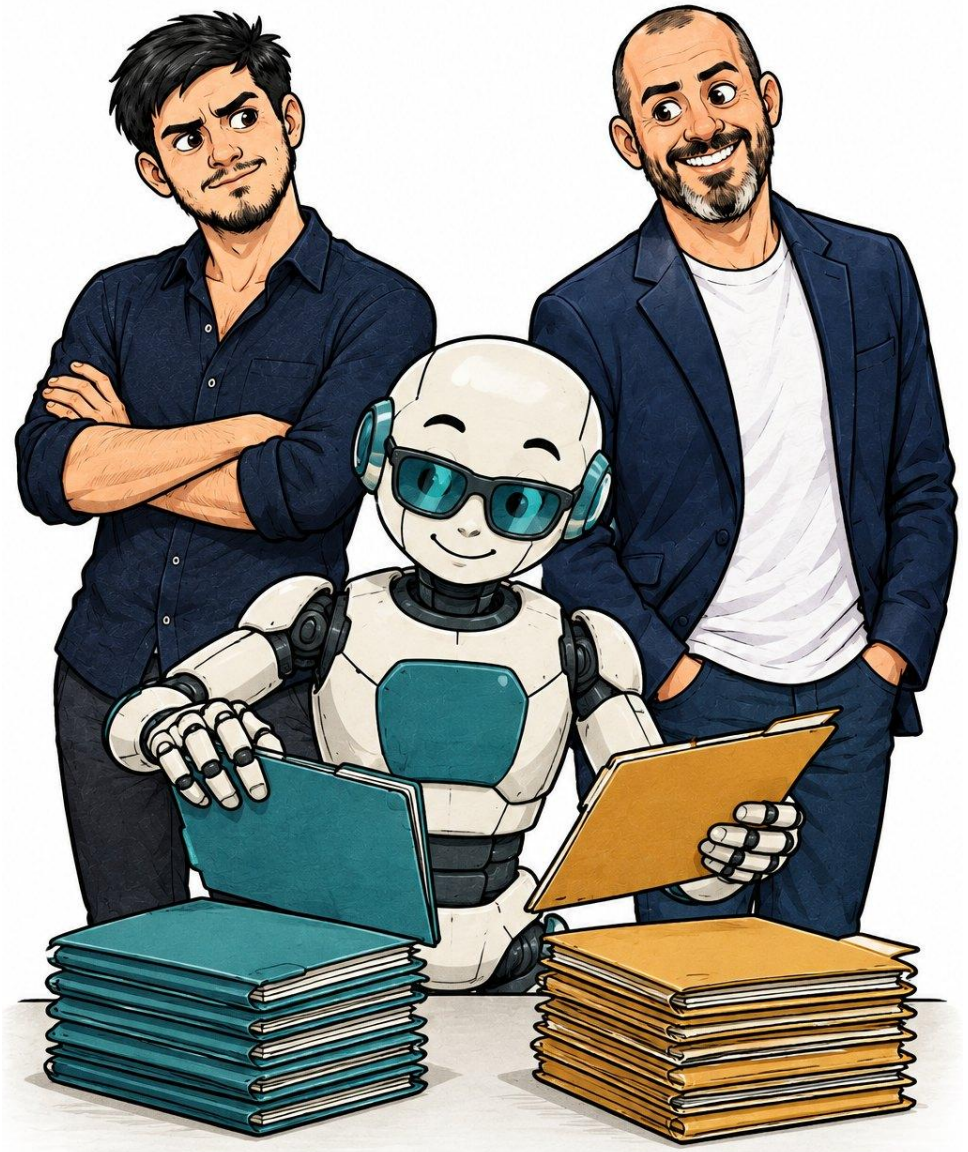
- Tomar un sistema de IA y recorrer su ciclo de vida: requisitos, datos, pruebas, aprobación, despliegue y monitoreo
- Revisar una evaluación de impacto y verificar que sus conclusiones se reflejan en controles
- Verificar la procedencia y calidad de un conjunto de datos de entrenamiento
- Revisar cómo se informa a los usuarios que interactúan con IA

Para recordar: “usamos IA, pero no tenemos sistemas de IA” es la nueva versión de “acá no manejamos información sensible”.

En la práctica

El modelo no discrimina. Solo aprendió muy bien de los datos.

Auditar IA es auditar también los datos con los que aprendió, no solo el modelo.



ISO/IEC 27090: las amenazas que no aparecen en la política de IA

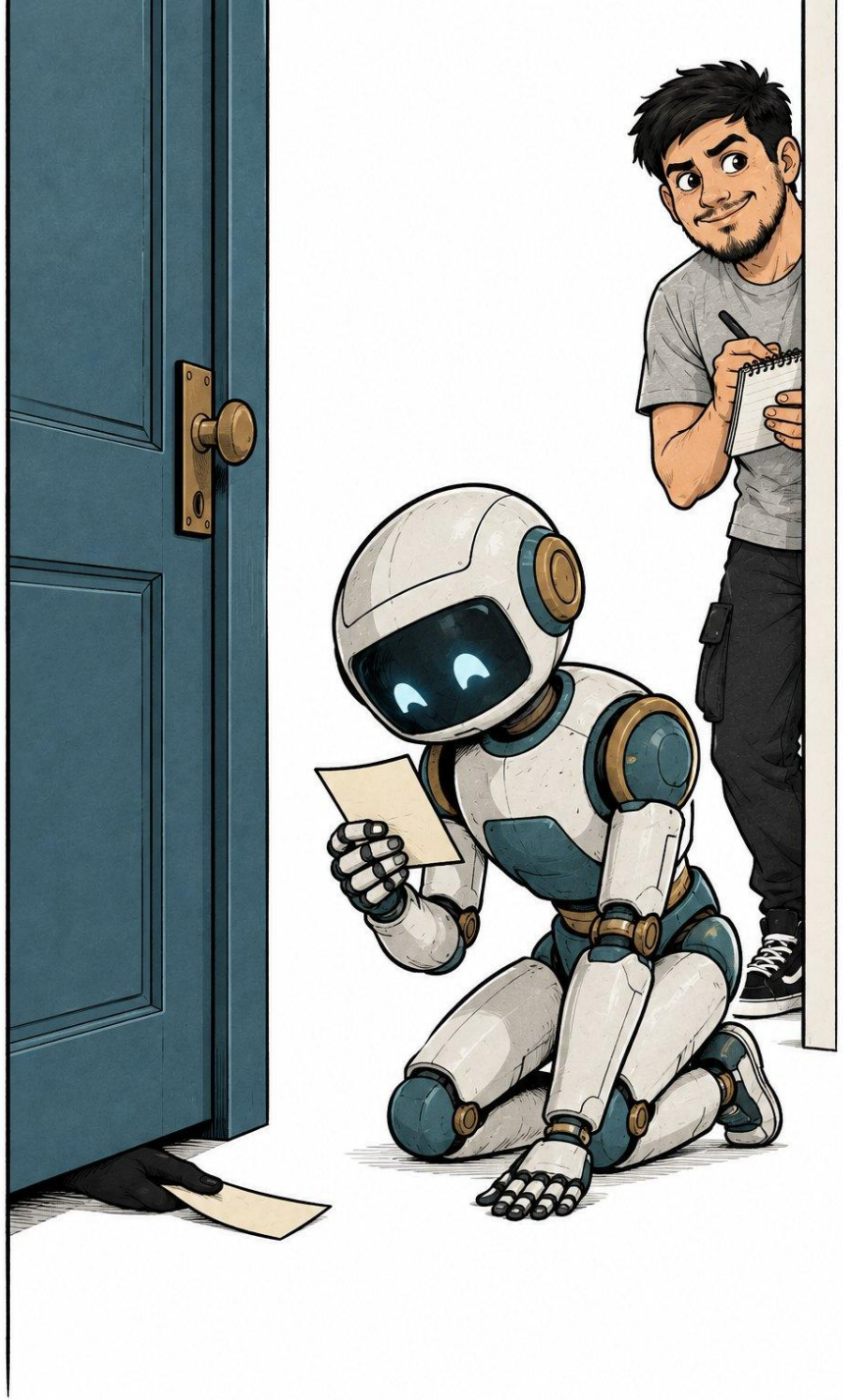
La nueva ISO/IEC 27090 describe amenazas propias de los sistemas de IA, cómo detectarlas y cómo mitigarlas. Spoiler: ninguna se resuelve con un PDF firmado.

Amenaza	Qué es, en criollo	Pregunta incómoda para el auditado
Envenenamiento de datos	Alterar los datos de entrenamiento para torcer el modelo	¿Cómo saben que nadie manipuló el conjunto de entrenamiento?
Evasión	Entradas diseñadas para engañar al modelo en producción	¿Probaron el modelo con entradas adversarias?
Inferencia de pertenencia	Deducir si un dato estuvo en el entrenamiento	¿El modelo se entrenó con datos personales? ¿Quién lo evaluó?
Exfiltración e inversión del modelo	Robar el modelo o reconstruir datos a partir de él	¿Quién puede consultar el modelo y cuántas veces?
Envenenamiento directo del modelo	Modificar el modelo o sus pesos	¿El modelo desplegado es el que se aprobó? ¿Cómo lo verifican?
Inyección de prompts	Instrucciones maliciosas que el modelo obedece	¿Qué pasa si un usuario le pide al asistente que ignore sus reglas?
Salidas sensibles o con inyección	El modelo revela datos o devuelve código malicioso	¿Se filtran las salidas antes de usarlas en otros sistemas?

En la práctica

La inyección de instrucciones explota la confianza del sistema en sus entradas; el control está en lo que se deja entrar.

Nadie le dijo al modelo que no leyera las notas que pasan por debajo de la puerta.



Tres normas, un mismo patrón

Aspecto	ISO/IEC 27001:2022	ISO/IEC 27701:2025	ISO/IEC 42001:2023
Objeto	Seguridad de la información	Privacidad de datos personales	Inteligencia artificial
Anexo A	93 controles, 4 temas	78 controles, 3 tablas	38 controles, 9 áreas
Guía de controles	ISO/IEC 27002	Anexo B	Anexo B
Declaración de Aplicabilidad	Sí	Sí	Sí
Evaluación propia	Riesgos de seguridad	Riesgos para los titulares; EIPD	Riesgos de IA; evaluación de impacto
Certificación	ISO/IEC 27006-1	ISO/IEC 27706	ISO/IEC 42006

Para recordar: domine el patrón —riesgo, anexo, SoA, evaluación de controles— y podrá auditar cualquier norma con anexo.

Auditar sistemas integrados con anexos

Oportunidades

- Una sola evaluación de riesgos con criterios comunes
- Una SoA integrada que indique a qué norma responde cada control
- Controles compartidos: acceso, registros, proveedores, incidentes
- Una auditoría interna y una revisión por la dirección únicas

Riesgos para el auditor

- Perder de vista requisitos propios de cada norma
- Equipos sin competencia en las tres disciplinas
- Hallazgos que no indican qué norma afectan
- Controles de privacidad o de IA tratados como simples controles de seguridad

Para recordar: un control de acceso puede servir a 27001, 27701 y 42001, pero su criterio de eficacia puede ser distinto en cada una.

17

Familias de apoyo y normas de nube

ISO27k, IA, ISO/IEC 27017 y 27018

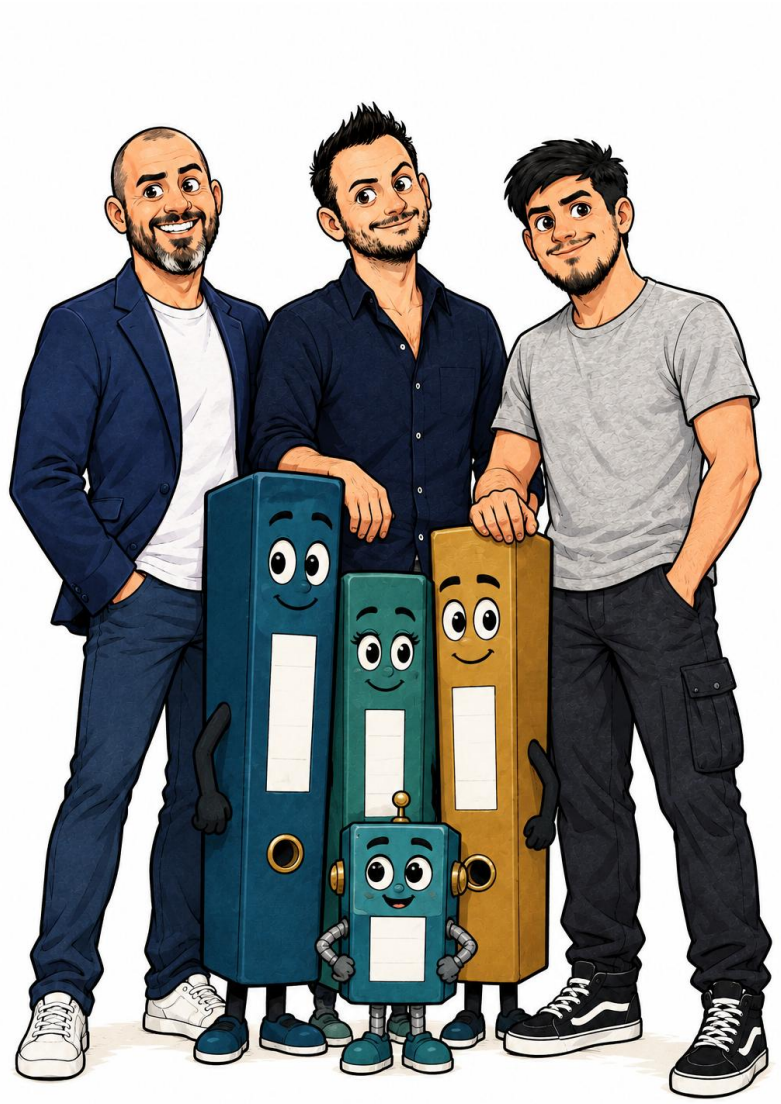


La familia de normas del SGSI (ISO27k)

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un enfoque sistemático para establecer, implantar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información de una organización con el fin de alcanzar los objetivos empresariales.

La familia incluye normas que: definen requisitos para un SGSI y para quienes los certifican; dan apoyo, orientación detallada o interpretación; abordan directrices sectoriales; y abordan la evaluación de la conformidad.

Son más de 70 normas. No hay una lista única: cambia continuamente. El auditor debe verificar qué edición está vigente antes de cada auditoría.



Lo mismo vale para la IA

ISO/IEC 42001 se apoya en otras normas: ISO/IEC 22989 (conceptos), 23894 (gestión de riesgos de IA), 42005 (evaluación de impacto) y 42006 (organismos de certificación).

Las normas más importantes de la familia ISO27k

Norma	Título	Aporte al auditor	Págs.
27000	Visión general y vocabulario	Definiciones comunes: control, riesgo, eficacia	27
27001	Requisitos del SGSI	Requisitos auditables y Anexo A	19
27002	Controles de seguridad	Guía de implementación de cada control	152
27003	Orientación del SGSI	Interpretar requisitos (“debería”, “puede”)	45
27004	Seguimiento y medición	Evaluar indicadores (cláusula 9.1)	58
27005	Gestión de riesgos	Método de identificación y tratamiento	—
27007	Auditoría del SGSI	Programa de auditoría y competencia, junto con ISO 19011	39
TS 27008	Evaluación de controles	Revisar implementación y operación de controles	91
27701	Privacidad (PIMS)	Sistema de privacidad con anexo propio	—

Qué dice cada norma (1)

ISO/IEC 27000: visión general y vocabulario

- Proporciona la visión general de los SGSI y los términos y definiciones de uso común en la familia
- Aplica a todo tipo y tamaño de organización: empresas, organismos públicos, entidades sin fines de lucro
- No cubre todos los términos de la familia ni impide que otras normas definan términos nuevos

ISO/IEC 27002: controles de seguridad

- Conjunto de referencia de controles genéricos, con guía de implementación
- Para usar en el contexto de un SGSI basado en ISO/IEC 27001
- Para implementar controles basados en buenas prácticas reconocidas internacionalmente
- Para desarrollar directrices propias de la organización

Para recordar: ISO/IEC 27000 resuelve casi todas las discusiones sobre qué significa “control”. Las demás se resuelven leyéndola.

Qué dice cada norma (2)

ISO/IEC 27003: orientación del SGSI

- Orienta sobre los requisitos de ISO/IEC 27001
- Da recomendaciones (“debería”), posibilidades (“puede”) y permisos (“puede”)
- No pretende ser una guía general de todos los aspectos de la seguridad

ISO/IEC 27007: auditoría del SGSI

- Orienta sobre la gestión del programa de auditoría, la realización de auditorías y la competencia de los auditores
- Complementa ISO 19011
- Aplica a auditorías internas y externas de un SGSI

Para recordar: ISO/IEC 27003 explica la 27001 mejor que muchos consultores… y cobra una sola vez.

ISO/IEC 27004: seguimiento y medición

“Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre.” — atribuida a Lord Kelvin

Qué establece

- El seguimiento y la medición del desempeño de la seguridad
- El seguimiento y la medición de la eficacia del SGSI, incluidos sus procesos y controles
- El análisis y la evaluación de los resultados
- Ayuda a cumplir la cláusula 9.1 de ISO/IEC 27001

35 ejemplos de indicadores (selección)

- Compromiso de la dirección; asignación de recursos; revisión de políticas
- Exposición al riesgo; programa de auditoría; acciones correctivas
- Formación y concienciación; preparación ante ingeniería social
- Calidad de contraseñas; revisión de derechos de acceso
- Reglas de firewall; revisión de registros; configuración de dispositivos
- Pruebas de penetración; cobertura de vulnerabilidades; tendencia de incidentes

Ruta de aprendizaje en la familia ISO27k e IA

1 Principiantes

ISO/IEC 27000, 27001, 27002, 27003, 27005 e ISO 19011.

En otras disciplinas: la norma de requisitos, su guía y la norma de riesgos.

2 Avanzado

ISO/IEC 27701, 27035 (incidentes), 27036 (proveedores), 27100 (ciberseguridad).

En IA: ISO/IEC 22989 y 23894.

3 Expertos

ISO/IEC 27004, 27007, TS 27008, 27014 (gobernanza), 27022 (procesos) y normas sectoriales.

En IA: ISO/IEC 42005 y 42006.

Para recordar: la evaluación de controles es de nivel experto: presupone dominar la disciplina y la lógica de riesgo.

ISO/IEC 27017: seguridad en la nube, de los dos lados

Da orientación de controles de seguridad para servicios en la nube, distinguiendo qué le toca al cliente del servicio y qué al proveedor. Esa distinción es la que más se olvida en las auditorías.

La edición 2015 agregaba guía cloud a 37 controles de ISO/IEC 27002:2013 y sumaba 7 controles propios (los “CLD”). La nueva edición de 2026 adopta la estructura de 27002:2022 y agrega 4 controles específicos de nube: roles y responsabilidades (5.38 y 5.39), segregación en entornos virtuales (8.35) y detección y prevención del uso no autorizado de la nube (8.36).

Antes de auditar, confirme qué edición declara la organización: el certificado puede no estar al día con la norma… o viceversa.



La responsabilidad compartida

“Eso lo hace el proveedor” es la frase más repetida en auditorías de nube. A veces es cierta. Siempre hay que preguntar dónde está la evidencia.

ISO/IEC 27017:2015: los siete controles CLD

Control	Nombre	Qué verificar
CLD.6.3.1	Roles y responsabilidades compartidos en la nube	Matriz de responsabilidades cliente–proveedor documentada y acordada
CLD.8.1.5	Remoción de activos del cliente	Qué pasa con los datos al terminar el contrato y cómo se evidencia
CLD.9.5.1	Segregación en entornos virtuales	Aislamiento entre clientes (inquilinos) y entre entornos
CLD.9.5.2	Endurecimiento de máquinas virtuales	Configuraciones de referencia aplicadas a las imágenes
CLD.12.1.5	Seguridad operativa del administrador	Procedimientos para operaciones administrativas críticas
CLD.12.4.5	Monitoreo de los servicios en la nube	Capacidad del cliente de monitorear su parte del servicio
CLD.13.1.4	Alineación de redes virtuales y físicas	Coherencia de la política de seguridad entre ambas capas



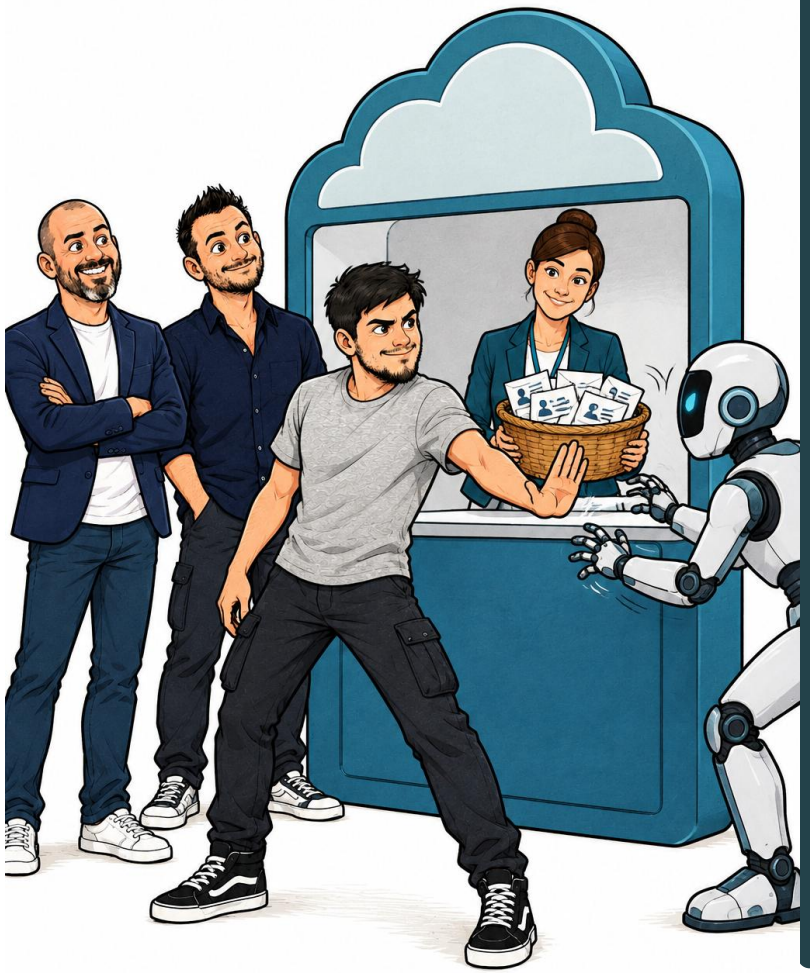
Para recordar: en la edición 2026, estos temas se reorganizan en la estructura de 27002:2022: use la tabla de correspondencia de su Anexo A.

ISO/IEC 27018: datos personales en la nube pública

Es un código de práctica para proveedores de nube pública que actúan como encargados del tratamiento de datos personales. Agrega guía específica a controles de ISO/IEC 27002 y un conjunto extendido de controles en su Anexo A, basado en los principios de privacidad de ISO/IEC 29100.

La segunda edición (2019) fue una revisión menor de la de 2014. Su lógica es simple: el cliente sigue siendo el responsable del tratamiento, y el proveedor debe poder demostrar que trata los datos solo según sus instrucciones.

ISO/IEC 27701:2025 incluye un mapeo con ISO/IEC 27018 en su Anexo E, así que no hace falta auditarlas como si fueran dos universos paralelos.



La pregunta clave

¿El proveedor usa los datos personales de sus clientes para algo más? Por ejemplo, ¿para entrenar un modelo de IA? Ahí 27018, 27701 y 42001 se encuentran en la misma mesa.

ISO/IEC 27018: los principios del Anexo A

Apartado	Principio	Qué verificar en el proveedor de nube
A.2	Consentimiento y elección	Ayuda al cliente a cumplir con los derechos de los titulares
A.3	Legitimidad y especificación del propósito	Trata los datos solo según instrucciones del cliente; no los usa para publicidad sin consentimiento
A.5 y A.6	Minimización; limitación de uso, retención y divulgación	Borrado de archivos temporales; divulgaciones a autoridades registradas y notificadas
A.8	Apertura, transparencia y notificación	Informa a los clientes sobre subencargados y su ubicación
A.10	Rendición de cuentas	Notifica violaciones de datos; conserva y devuelve o destruye datos según política
A.11	Seguridad de la información	Acuerdos de confidencialidad, restricción de copias, control de soportes y cifrado
A.12	Cumplimiento de la privacidad	Ubicación geográfica de los datos y transferencias previstas

Cómo se conectan estas normas entre sí

Si audita…	Mire también…	Por qué
ISO/IEC 20000-1, 8.7.2 (continuidad)	ISO 22301	Mismo BIA, mismos RTO; o al menos coherentes
ISO/IEC 20000-1, 8.7.3 (seguridad)	ISO/IEC 27001	Controles de seguridad del servicio y del SGSI
ISO/IEC 27001 en un proveedor de nube	ISO/IEC 27017 y 27018	Responsabilidades compartidas y datos personales de clientes
ISO/IEC 27701	ISO/IEC 27018 (Anexo E de 27701)	Controles de encargado en nube pública
ISO/IEC 42001	ISO/IEC 27001, 27701 y 27090	Seguridad, privacidad y amenazas propias de la IA
Cualquiera de ellas	ISO 31000	El mismo lenguaje de riesgo para todas



Para recordar: auditar normas por separado en una organización integrada es como revisar las ruedas de un auto sin mirar si está andando.

18

Evaluación de controles: ISO/IEC TS 27008

Keep calm and assess controls



ISO/IEC TS 27008: guía para evaluar controles

Proporciona orientación sobre la revisión y evaluación de la implementación y operación de los controles de seguridad de la información, incluida la evaluación técnica de los controles de los sistemas de información.

La evaluación se hace frente a los requisitos de seguridad establecidos por la organización, incluido el cumplimiento técnico respecto de criterios de evaluación basados en esos requisitos.

También orienta sobre cómo revisar y evaluar los controles gestionados a través de un SGSI conforme a ISO/IEC 27001. Unas 91 páginas.



Estado de la norma

Edición vigente: ISO/IEC TS 27008:2019, alineada con 27001/27002:2013. Revisión en curso para alinearla con 27002:2022 (borrador de comité a fines de 2025).

Generalidades: el auditor debe estar bien preparado

Para las evaluaciones, los auditores asignados deben estar bien preparados, tanto en el lado del control como en el lado de las pruebas: el funcionamiento de las herramientas aplicables y el objetivo técnico de cada prueba.

Los elementos del trabajo pueden priorizarse según los riesgos percibidos, planificarse para seguir un proceso o sistema de negocio particular, o diseñarse para cubrir todas las áreas del alcance en secuencia.

El mundo está en constante cambio, al igual que los riesgos para la reputación y los resultados de la empresa. Las organizaciones deben ser proactivas y construir una defensa sólida en torno a la auditoría de los controles. Para esto se diseñó la norma.



Tres formas de organizar

Por riesgo · por proceso o sistema · secuencial por áreas.

Se pueden combinar a lo largo del programa de auditoría.

Antes del trabajo de campo (6.1.2 y 6.1.3)

Información preliminar

- Manuales, normas técnicas, políticas propias e investigación sobre riesgos y controles del área
- Resultados de evaluaciones, pruebas y auditorías previas, aunque las haya hecho otro
- Incidentes, casi incidentes, problemas de soporte y cambios recientes
- Revisar el alcance si el plan se armó hace meses: el mundo siguió girando

Hablar con la gente (sí, antes)

- Contactar a responsables y contactos del área desde el inicio
- Al final, ellos tienen que entender y aceptar los hallazgos
- Empatía, respeto mutuo y explicar el proceso mejoran mucho la calidad y el impacto del resultado
- La checklist propia prepara al auditor; la heredada solo lo hace sentir preparado

Para recordar: llegar al campo sin haber leído nada no es “mente abierta”: es improvisación con credencial.

No es exclusiva de ISO/IEC 27001

Aunque está pensada para usarse con ISO/IEC 27001 y 27002, no es exclusiva de esas normas: se aplica a cualquier escenario que requiera evaluar controles.

Es esencial para organizaciones de todas las formas y tamaños, incluidas empresas públicas y privadas, organismos de gobierno y organizaciones sin fines de lucro que realizan revisiones de gestión y pruebas de cumplimiento operativo.

Propone un marco integral de evaluación para dar confianza en que los controles se implementaron y administran correctamente y en que la seguridad es “adecuada para el propósito”.



Aplicarla a otros anexos

Su método —analizar, examinar, probar y muestrear— sirve igual para los 78 controles de ISO/IEC 27701 o los 38 de ISO/IEC 42001.

¿Cuál es el propósito de ISO/IEC TS 27008?

Propósitos

1. Ayudar en la preparación e implementación de auditorías del sistema y del método de gestión de riesgos
2. Dar directrices para auditar los controles de acuerdo con la guía de ISO/IEC 27002
3. Mejorar las auditorías optimizando la relación entre los procesos del sistema y los controles necesarios

- Garantizar que los recursos de auditoría se usen de forma eficaz y eficiente
- Agregar valor salvando la diferencia entre revisar el sistema “en principio” y verificar con pruebas los controles aplicados: operaciones de negocio, estructuras de TI y entornos operativos

Para recordar: el centro es cerrar la distancia entre el papel y la operación real.

Alcance y funcionamiento

¿Cuál es su alcance?

- Orienta a los auditores sobre los controles del sistema de gestión
- Guía evaluaciones internas, externas y de terceros, mostrando la relación entre el sistema y sus controles
- Indica cómo probar en qué medida se aplican los controles necesarios
- Ayuda a cumplir los criterios de conformidad y sirve como plataforma técnica para la gobernanza de TI

¿Cómo funciona?

- Define procedimientos generales, no técnicas para un control en particular
- Define revisiones sistemáticas
- Describe los enfoques y formas de revisión aplicables a los controles
- Analiza las prácticas necesarias para un proceso de revisión exitoso

Para recordar: TS 27008 no trae la receta de cada control: trae el método. La receta sigue siendo responsabilidad del cocinero.

Relación con otras normas y destinatarios

Relación con ISO/IEC 27001, 27002 y 27007

- Es muy similar a ISO/IEC 27007, pero 27007 revisa el sistema de gestión (cláusulas 4 a 10)
- TS 27008 se centra en auditar controles específicos, como los de ISO/IEC 27002 y el Anexo A
- Evalúa controles, incluido el cumplimiento, frente al estándar de implementación de la organización
- No da pautas detalladas sobre medición (27004), riesgos (27005) ni auditoría del SGSI (27007)

¿Quién debería usarla?

- Auditores internos y externos que revisan los controles de un sistema de gestión
- Cualquiera que analice o evalúe controles, dentro o fuera de una auditoría estructurada
- Principalmente auditores que verifican que los controles cumplen técnicamente con ISO/IEC 27002 y con los demás requisitos de control de la organización

Para recordar: 27007 pregunta si el sistema funciona; TS 27008, si los controles funcionan. Hacer solo una es auditar a medias.

ISO/IEC TS 27008 les ayudará de las siguientes maneras

1 Reconocer problemas

Comprender el alcance de posibles problemas y debilidades en los controles.

2 Comprender consecuencias

Identificar las consecuencias para la empresa de riesgos mal mitigados.

3 Priorizar

Priorizar las prácticas de control según la gestión de riesgos.

4 Verificar cierres

Asegurar que vulnerabilidades o defectos encontrados antes se resolvieron.

5 Aplicar en cualquier organización

Empresas públicas y privadas, organismos de gobierno y entidades sin fines de lucro.

Para recordar: TS 27008 no dice qué controles tener; dice cómo comprobar que los elegidos funcionan.

Análisis de procesos (7.2) y examen (7.3)

El proceso dice si el control…

1. está diseñado para producir el efecto deseado, en teoría
2. está correctamente implementado
3. opera según lo diseñado
4. se administra, monitorea y gestiona correctamente
5. produce realmente el efecto previsto, en la práctica

Examinar es…

- Observar copias de seguridad y resultados de ejercicios de contingencia
- Observar la respuesta a incidentes en vivo, si la hay
- Revisar la configuración de un sistema, directamente o con un operador calificado
- Observar el transporte y destrucción de papeles confidenciales
- Que una alerta exista indica que el control funciona; no que sea fiable ni eficaz

Para recordar: un log lleno de alertas prueba que el control habla; falta saber si alguien lo escucha.

Anexo A: recopilación inicial de información (distinta de TI)

Recursos humanos y políticas

- ¿El personal se siente responsable de sus acciones?
- ¿Hay conocimiento de seguridad disponible para responder preguntas y motivar?
- ¿Las políticas son claras y SMART (específicas, medibles, alcanzables, realistas, con plazo)?
- ¿Las políticas derivan de los objetivos y la estrategia del negocio?
- ¿Son un “copiar y pegar” de la norma o están adaptadas?

¿Cada acción define quién, cuándo, por qué, qué, dónde y cómo?

- Sin quién: nadie será responsable
- Sin cuándo: la acción nunca se terminará
- Sin por qué: nadie entenderá su importancia
- Sin qué ni dónde: no se sabrá sobre qué actuar
- Sin cómo: no se ejecutará correctamente
- Sin indicadores: no se sabrá si se logró el objetivo

Anexos B y C: evaluación técnica y nube

Anexo B: guía práctica de evaluación técnica

- Recorre los controles de ISO/IEC 27002 uno por uno
- Para cada uno indica qué revisar y qué pruebas técnicas aplicar
- Ejemplos: políticas (5.1), organización interna, dispositivos móviles y teletrabajo, verificación de antecedentes
- La versión vigente usa la numeración de 2013: use la tabla de correspondencia con 2022

Anexo C: servicios en la nube (IaaS)

- Relaciona cada control con cuatro capas: virtualización de servidores, de red, de almacenamiento y gestión del servicio
- Indica si la evaluación técnica aplica, y si del lado del proveedor o del cliente
- Lección: en la nube no todos los controles se prueban en el mismo lugar
- Algunos solo se verifican con informes del proveedor (27001, 27017, 27018, CSA STAR, SOC 2)

Para recordar: en la nube, “eso lo hace el proveedor” es una respuesta; “y acá está la evidencia” es otra muy distinta.

Debate

¿Para ustedes es correcto realizar pruebas técnicas durante la auditoría?

¿Quién ejecuta la prueba? ¿Con qué autorización? ¿Qué demuestra?



¿Prueba de técnicas de validación? Según el conocimiento de las partes

Tipo	El evaluador conoce el objetivo	El objetivo conoce la prueba	Qué mide
Ciega (blind)	No	Sí	La habilidad del evaluador ante un objetivo preparado
Doble ciego	No	No	La preparación real del objetivo
Caja gris	Parcialmente	Sí	La seguridad con conocimiento limitado
Doble caja gris	Parcialmente	Parcialmente	La respuesta con información limitada
Tándem	Sí	Sí	Los controles en profundidad (caja blanca)
Invertida (reversal)	Sí	No	La capacidad de detección y respuesta



Para recordar: según TS 27008, la ciega y la de caja gris son de uso limitado y deberían evitarse: miden más al auditor que al objeto.

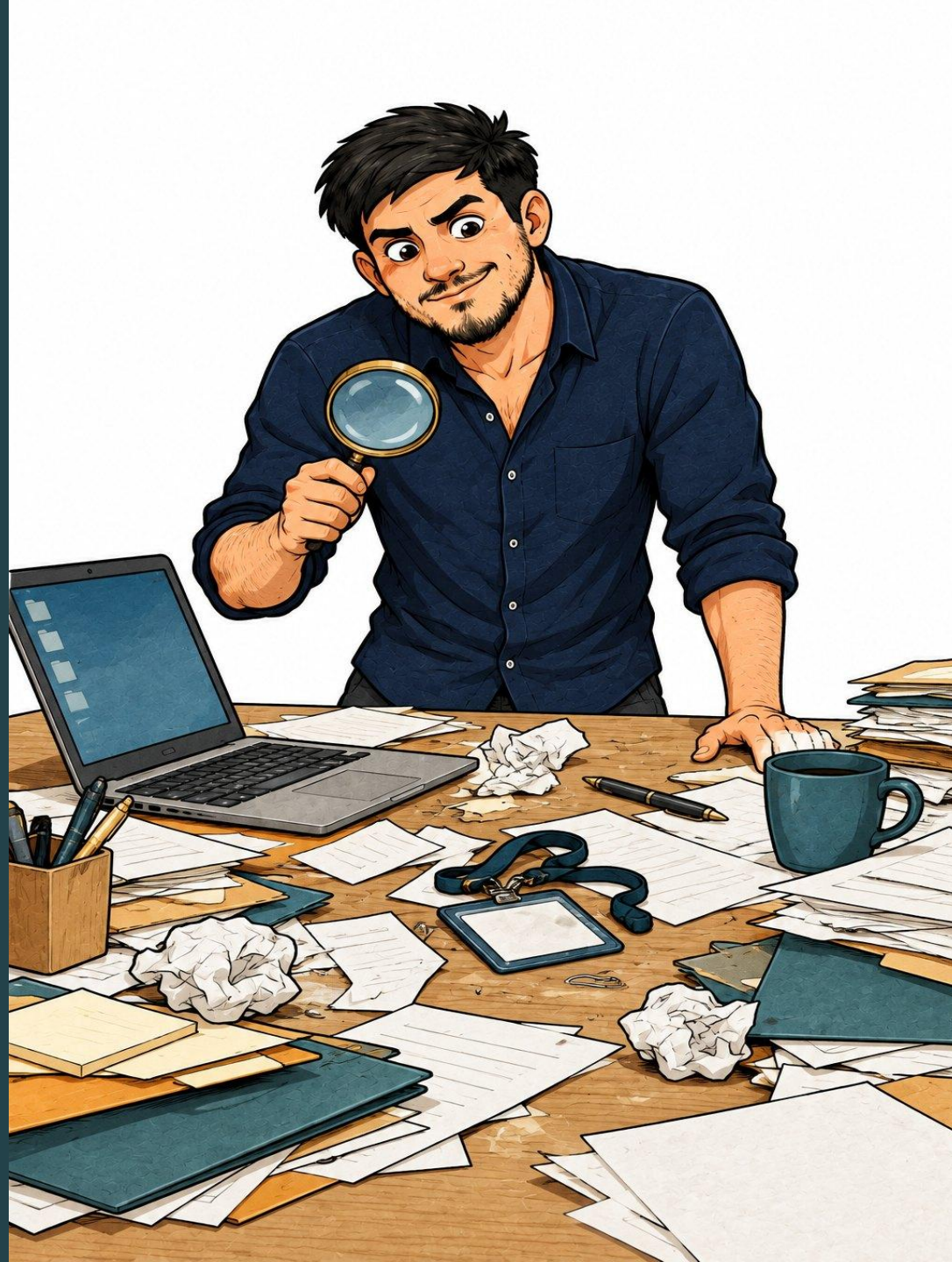
Área de muestreo según ISO/IEC TS 27008

Área (27001:2022)	Población	Atributo a verificar
Altas y bajas (5.16, 5.18, 6.5)	Cuentas creadas y desvinculaciones	Aprobación previa; baja en plazo
Revisión de accesos (5.18, 8.2)	Sistemas críticos y cuentas privilegiadas	Revisión realizada y acciones ejecutadas
Cambios (8.32)	Cambios a producción	Aprobación, prueba y vuelta atrás
Vulnerabilidades (8.8)	Servidores y estaciones	Parches críticos en plazo
Copias (8.13)	Trabajos de copia	Ejecución y prueba de restauración
Incidentes (5.24 a 5.27)	Incidentes registrados	Respuesta, causa raíz, lecciones
Privacidad (27701)	Solicitudes de titulares	Respuesta en plazo legal
IA (42001 A.5, A.6)	Sistemas de IA desplegados	Evaluación de impacto y aprobación previas

Debate

¿Cuál es la mejor técnica si pensamos en controles técnicos según ISO/IEC TS 27008?

Abiertas con demostración · hipotéticas para controles detectivos · comparativas entre entornos · cerradas con dato verificable



Las 5W y 1H aplicadas a normas con anexo

? ¿Quién?

¿Quién es el propietario del activo, del tratamiento de datos o del sistema de IA? ¿Quién aprobó este acceso privilegiado? ¿Es distinto de quien lo usa?

? ¿Qué?

¿Qué evento dispara el alta de un usuario o el despliegue de un modelo? ¿Qué registro deja el control cuando actúa?

? ¿Dónde?

¿En qué país y región de nube se almacenan los datos personales? ¿Dónde se guardan las copias fuera del sitio y los registros?

? ¿Cuándo?

¿La cuenta se deshabilitó antes o después del egreso? ¿Cuándo se detectó el incidente y cuándo se notificó a la autoridad?

? ¿Por qué?

¿Por qué este control del Anexo A se declaró no aplicable? ¿Por qué este riesgo se aceptó en lugar de tratarse? ¿Quién lo aprobó?

? ¿Cómo?

¿Cómo saben que la copia se puede restaurar? ¿Cómo se detectaría un acceso no autorizado?

19

El libro gordo de… áreas de enfoque técnicas

Quince rutas para normas con anexos técnicos



Cómo usar las rutas de auditoría

Cada área de enfoque indica a qué norma y sector aplica, por qué merece atención y una ruta de preguntas organizada en Planificar, Hacer, Verificar y Actuar.

Las preguntas no son una lista para leer al auditado: son la base para preparar la entrevista, decidir qué examinar y qué probar, y no olvidar ninguna fase del ciclo.

En cada diapositiva se muestran las preguntas principales. La ruta completa de cada área está en las notas del orador.



Áreas técnicas

T1 Codificación segura · T2 Inteligencia de amenazas · T3 Proveedor de nube · T4 Registros · T5 Seguridad en continuidad · T6 RGPD · T7 Controles de TI · T8 Seguridad en la nube · T9 Clasificación · T10 Ágil · T11 SDLC · T12 Normas de codificación · T13 Impacto de IA · T14 Derechos de titulares · T15 Nube compartida

Área T1. Directrices de codificación segura

Aplica a: ISO/IEC 27001 (A.8.25, A.8.28), cualquier sector · **Justificación:** un SDLC seguro es la piedra angular de una aplicación robusta y protege confidencialidad, integridad y disponibilidad.

Planificar

- ¿Hay una política de codificación segura para el desarrollo?
- ¿Existe un proceso documentado y se comunica al equipo?
- ¿Se adoptaron referencias como OWASP, PA-DSS o IEC 62443?
- ¿Se definieron objetivos de las directrices?
- ¿Algún cliente especificó directrices en su contrato?
- ¿Cuál es la política sobre componentes de código abierto?

Hacer

- ¿Las directrices están disponibles para los desarrolladores?
- ¿Se exige formación en codificación segura?
- ¿Se validan los parámetros de entrada en cliente y servidor?
- ¿Los componentes de terceros vienen de fuentes de confianza o se evaluó su riesgo?
- ¿Se implementaron bien contraseñas, expiración de sesión e inicio administrativo?
- ¿Está controlado el acceso al repositorio y hay registros de auditoría?

Área T1. Directrices de codificación segura (cont.)

Verificar

- Comprobar la concienciación del equipo en los principios
- ¿Se aplican las directrices acordadas con el cliente?
- ¿Se revisa el código entre pares?
- ¿Hay información crítica (contraseñas, usuarios administradores) incrustada en el código?
- ¿Se gestionan bien errores como desbordamientos de búfer?
- ¿Qué pruebas (incluidas VA/PT) cubren las directrices?

Actuar

- ¿Se registran los problemas de la revisión de código?
- ¿Se hace análisis causal y se da retroalimentación a los desarrolladores?
- ¿Se corrigen y vuelven a probar los casos fallidos antes de producción?
- ¿Se dan sesiones de formación cuando el análisis revela brechas?
- ¿Qué se hace con los resultados de VA/PT?
- ¿Se actualizan políticas y directrices con lo aprendido?

Para recordar: prueba sugerida: buscar secretos en el repositorio y muestrear pull requests fusionados para verificar la revisión por pares.

Área T2. Proceso de inteligencia de amenazas

Aplica a: ISO/IEC 27001 (A.5.7), cualquier sector · **Justificación:** información para comprender las amenazas que atacaron, atacarán o están atacando a la organización, y prepararse, prevenir e identificarlas.

Planificar

- ¿Hay un proceso para identificar lo valioso o “tentador” (datos de empleados, de clientes, propiedad intelectual)?
- ¿Cuáles son los objetivos de la inteligencia de amenazas? ¿Reflejan C, I y D?
- ¿Hay un proceso para identificar amenazas internas y externas?
- ¿Por qué canales se accede a los datos críticos?
- ¿Se evaluaron vulnerabilidades como baja seguridad de red o Wi-Fi?
- ¿Hay impactos legales o contractuales por pérdida de datos?

Hacer

- ¿Se identificaron y clasificaron los activos valiosos?
- ¿Los objetivos son claros y verificables?
- ¿Existe una estructura de respuesta a eventos?
- ¿La inteligencia está organizada en niveles estratégico, táctico y operativo?
- ¿Se forma periódicamente al personal y se evalúa después?
- ¿Se aplican parches y controles de red?

Área T2. Proceso de inteligencia de amenazas (cont.)

Verificar

- ¿Se hacen evaluaciones periódicas de amenazas? ¿Con qué frecuencia?
- ¿Se cumplen los objetivos de supervisión?
- ¿Se cerraron los problemas de VA/PT o se evaluaron sus riesgos?
- ¿Se revisan los registros de acceso a sistemas críticos por alguien que no otorga accesos?
- ¿Se notifican y cierran los incidentes a tiempo?
- ¿La comunicación a clientes y autoridades fue oportuna?

Actuar

- ¿Qué acciones correctivas evitan que los incidentes se repitan?
- ¿Se hizo análisis causal de los incidentes?
- ¿Hay plan de acción si no se alcanzaron los objetivos?
- ¿Se repite la formación que no fue eficaz?
- ¿Hay plan si los parches no se aplicaron por motivos de negocio?
- ¿Se guardan de forma segura las pruebas de incidentes?

Para recordar: prueba sugerida: seguir una alerta de inteligencia hasta una decisión concreta (un bloqueo, un parche priorizado).

Área T3. Monitoreo de la seguridad del proveedor de nube

Aplica a: ISO/IEC 27001 (A.5.19 a A.5.23), 27017, 27018 · **Justificación:** el monitoreo verifica que los controles funcionen; eventos prohibidos por la política en el flujo de seguridad indican que la política no se aplica.

Planificar

- ¿Hay criterios de seguridad para seleccionar al CSP?
- ¿Se evaluó su tamaño y reputación?
- ¿El contrato prevé compartir los protocolos de seguridad?
- ¿Hay requisitos legales sobre país o plazo de almacenamiento?
- ¿Cuál es la política del CSP sobre privacidad y datos?
- ¿Qué seguridad física aplica? ¿Se puede visitar?

Hacer

- ¿Se compararon CSP y el elegido cumplió los criterios?
- ¿El acuerdo es claro sobre responsabilidades de cada parte?
- ¿Se comprobaron controles del CSP como accesos y copias?
- ¿Se registran los incidentes y cómo se resuelven?
- ¿Se conservan los registros de acceso el tiempo acordado?
- ¿La infraestructura crítica se parchea a tiempo?

Área T3. Monitoreo de la seguridad del proveedor de nube (cont.)

Verificar

- ¿La política del CSP está alineada con la propia? ¿Hay acuerdo firmado?
- ¿Se dispone de registros de acceso según el acuerdo?
- ¿Se clasifican los incidentes y se documenta el análisis causal?
- ¿Hay copias en ubicaciones alternativas, con control de acceso y destrucción?
- ¿Se cierran los resultados de VA/PT en plazo?
- ¿El CSP subcontrata? ¿Audita a sus subcontratistas?

Actuar

- ¿Qué acciones se tomaron ante incidentes? ¿Son eficaces?
- ¿Cómo se hace el seguimiento con el CSP?
- ¿Cómo respondió el CSP a medidas de reguladores?
- ¿Se repiten los mismos resultados en la siguiente VA/PT?
- ¿Se confirman los cambios en el entorno del CSP?
- ¿Se atienden los cambios de capacidad solicitados?

Para recordar: prueba sugerida: leer el informe del CSP y verificar alcance, vigencia y controles complementarios del cliente.

Área T4. Gestión y análisis de registros

Aplica a: ISO/IEC 27001 (A.8.15 a A.8.17), cualquier sector · **Justificación:** el análisis de registros es lo más difícil de su gestión, pero también lo más importante; una infraestructura robusta produce resultados valiosos.

Planificar

- ¿Cuál es la política de registros?
- ¿Qué objetivos se buscan con la información de registros?
- ¿Se identificaron los activos de los que deben recogerse?
- ¿Cuál es el tamaño y el período de conservación?
- ¿Hay requisitos contractuales, legales o regulatorios?
- ¿Quién accede, quién genera, quién revisa y con qué frecuencia?

Hacer

- ¿Se generan según la política?
- ¿Dónde se guardan?
- ¿Quién está autorizado y qué controles de acceso hay?
- ¿Los revisa el responsable? ¿Qué análisis hace y qué medidas toma?
- ¿Otra persona verifica la revisión?
- ¿Se destruyen de forma segura y queda registro?

Área T4. Gestión y análisis de registros (cont.)

Verificar

- ¿Se revisan con la frecuencia definida?
- ¿Hay lista de personas con acceso?
- ¿Se pueden modificar o borrar los registros?
- ¿Las herramientas son eficaces y se usan bien?
- ¿Cuánto tiempo pasa entre generación y análisis?
- ¿Se conservan según requisitos legales?

Actuar

- ¿Se prioriza la gestión de registros en la organización?
- ¿Se formó al personal responsable?
- ¿Qué cambios se hacen en generación, recopilación y revisión?
- ¿Se resuelven problemas de espacio y tamaño?
- ¿Hay medidas disciplinarias ante pérdida o alteración?
- ¿Se auditan las herramientas de análisis?

Para recordar: prueba sugerida: generar un evento conocido y verificar que aparece en el registro central con la hora correcta.

Área T5. Seguridad durante la continuidad del negocio

Aplica a: ISO/IEC 27001 (A.5.29, A.5.30), ISO 22301 · **Justificación:** la pandemia llevó a un trabajo remoto masivo con más amenazas; la seguridad debe mantenerse durante cualquier crisis.

Planificar

- ¿Hay un enfoque integrado de riesgos para seguridad y continuidad?
- ¿El análisis de impacto considera aspectos de seguridad?
- ¿Los planes definen expectativas de seguridad?
- ¿Incluyen controles para trabajo remoto ampliado?
- ¿Incluyen oficinas cerradas o parcialmente cerradas?
- ¿Qué proveedores se movilizarán para seguridad física, de comunicaciones y de equipos?

Hacer

- ¿La respuesta de continuidad incluye procedimientos de seguridad?
- ¿Se comunica a los trabajadores remotos la necesidad de más concienciación?
- ¿Cómo se asegura el suministro de portátiles, VPN o autenticación multifactor en una crisis?
- ¿Hay medidas proactivas para el equipamiento de contingencia?
- ¿Hay registros de la participación de seguridad en el comité de crisis?
- ¿Participó seguridad en la vuelta a la normalidad?

Área T5. Seguridad durante la continuidad del negocio (cont.)

Verificar

- ¿Hay evidencia de supervisión de la seguridad durante el incidente?
- ¿Se informó periódicamente a la alta dirección?
- ¿Las violaciones se gestionaron según el proceso de incidentes?
- ¿Qué análisis se hizo de la pérdida de datos?
- ¿Se comunicó a las partes interesadas?

Actuar

- ¿Hubo revisiones posteriores con lecciones aprendidas?
- ¿Se comunicaron las mejoras al personal?
- ¿Hay disposición clara de los incidentes ocurridos?
- ¿Se actualizaron las evaluaciones de riesgo e impacto?

Para recordar: prueba sugerida: verificar que las cuentas y excepciones temporales de la contingencia se dieron de baja.

En la práctica

Un respaldo sin prueba de restauración es una expectativa, no un control.

El respaldo existe. La restauración la vamos a probar algún día.



Área T6. Protección de datos personales (RGPD)

Aplica a: ISO/IEC 27001 (A.5.34; antes A.18.1.4), ISO/IEC 27701 · **Justificación:** el RGPD rige desde el 25 de mayo de 2018 y alcanza a empresas de la UE y de fuera que tratan datos de personas en la UE.

Planificar

- ¿Se determinó la aplicabilidad del RGPD y sus aspectos críticos?
- ¿Figura entre los requisitos legales aplicables?
- ¿Se evaluaron los riesgos del RGPD y sus controles operativos?
- ¿Están definidas las responsabilidades del delegado de protección de datos?
- ¿Hay metodología de evaluación de impacto en la privacidad?
- ¿Hay procedimientos de identificación, clasificación y tratamiento de IIP?

Hacer

- ¿Se nombró delegado de protección de datos (cuando procede)?
- ¿Las rutinas del sistema están alineadas con el RGPD?
- ¿Se realizaron evaluaciones de impacto?
- ¿La IIP está registrada y contemplada en los procedimientos?
- ¿El personal recibió formación sobre RGPD y tratamiento de IIP?

Área T6. Protección de datos personales (RGPD) (cont.)

Verificar

- ¿Hay revisiones periódicas y auditorías internas de cumplimiento?
- ¿Los procedimientos cumplen su finalidad?
- ¿La revisión usa un método estructurado de riesgos?
- ¿Considera requisitos del cliente, legales y de otras partes?

Actuar

- ¿Hay un proceso para mejorar la eficacia del cumplimiento?
- ¿Se busca un enfoque equilibrado entre partes interesadas?
- ¿Se inician proyectos de mejora a partir de datos?
- ¿Se pueden demostrar los esfuerzos de mejora y sus resultados?

Para recordar: en ISO/IEC 27701:2025, contraste esta ruta con las tablas A.1 (responsables) y A.2 (encargados).

En la práctica

Un consentimiento válido es informado; si hace falta una lupa, no lo es.

El consentimiento existe.
Encontrarlo requiere lupa.



Área T7. Eficacia de los controles de TI

Aplica a: ISO/IEC 27001 (A.6.7, A.7.10, A.8.1, A.8.5, A.8.20, A.8.24), cualquier sector · **Justificación:** las TI son la columna vertebral de la información; medir su eficacia ayuda a decidir inversiones en tecnología.

Planificar

- ¿Hay política de dispositivos móviles y teletrabajo?
- ¿Y de manipulación, eliminación y transferencia de soportes?
- ¿Cuál es la política de control de acceso?
- ¿Se planificó el acceso a redes y servicios de red?
- ¿Se aplican controles criptográficos?
- ¿Hay procedimientos operativos y objetivos de seguridad de las operaciones?

Hacer

- ¿Se aplican los procedimientos de móviles y teletrabajo?
- ¿Se gestionan los soportes según la política?
- ¿Se controla el acceso a redes? ¿Hay segregación VLAN?
- ¿Se controla estrictamente el acceso administrativo?
- ¿Cómo se aplica el cifrado y se gestionan las claves? ¿Tecnológicamente o por proceso?
- ¿Se actualiza el antimalware y se revisan los registros?

Área T7. Eficacia de los controles de TI (cont.)

Verificar

- ¿Se analizan los incidentes de móviles y se supervisa el teletrabajo?
- ¿Se revisan los registros de soportes y de acceso?
- ¿Qué herramientas verifican el acceso a la red?
- ¿Se revisan las actividades administrativas?
- ¿Existe el principio “hacedor–verificador”?
- ¿Se rastrean los dispositivos sin parches?

Actuar

- ¿Hay medidas de concienciación o disciplinarias por incidentes?
- ¿Se calibran las herramientas de supervisión de red?
- ¿Se cambian regularmente las contraseñas administrativas?
- ¿Los administradores reciben formación suficiente?
- ¿Qué se hace si el cifrado no es adecuado?
- ¿Se parchean y escanean de inmediato los dispositivos detectados?

Para recordar: prueba sugerida: porcentaje de equipos con cifrado de disco y reglas de firewall “cualquiera a cualquiera”.

En la práctica

Revisar accesos es comparar quién tiene permisos con quién los necesita, no contar llaves.

Todos tienen una llave. Nadie sabe cuál abre qué.



Área T8. Seguridad de la computación en la nube

Aplica a: ISO/IEC 27001 (A.5.23), 27017, 27018 · **Justificación:** la seguridad en la nube abarca lo físico y lo lógico en los modelos de software, plataforma e infraestructura como servicio.

Planificar

- ¿Hay diligencia debida para evaluar proveedores de nube?
- ¿Hay planes contra violaciones y pérdida de datos?
- ¿Qué precauciones hay contra compromiso de credenciales, secuestro de cuentas y ataques internos?
- ¿Hay medidas contra ataques DoS y DDoS?
- ¿Se planificaron los requisitos de almacenamiento por región?
- ¿Hay seguridad prevista para interfaces y datos de dispositivos IoT?

Hacer

- ¿La diligencia verificó controles y nivel de servicio?
- ¿Hay cifrado y autenticación multifactor?
- ¿Hay distribución multizona y copias externas?
- ¿Existe una cultura de credenciales seguras?
- ¿Hay CDN o WAF contra DDoS?
- ¿Se controlan enumeración de cuentas, credenciales por defecto, XSS e inyección SQL?

Área T8. Seguridad de la computación en la nube (cont.)

Verificar

- ¿Se verifica la eficacia de la diligencia debida?
- ¿Cómo se revisan las violaciones de datos?
- ¿Hay un proceso para asegurar que todas se informen?
- ¿Qué análisis se hace de la pérdida de datos?
- ¿Se verifica que funcionan las precauciones sobre credenciales?
- ¿Con qué frecuencia se revisan las medidas de IoT?

Actuar

- ¿Qué se hace si el proveedor no cumple el nivel de servicio?
- ¿Se revisa la distribución multizona ante nuevos riesgos?
- ¿Se actualizan las credenciales?
- ¿Qué medidas surgen de las auditorías de recursos compartidos?
- ¿Qué se hace ante riesgos de ataques internos?
- ¿Se corrigen los controles de IoT no eficaces?

Para recordar: prueba sugerida: buscar almacenamiento con acceso público y administradores globales sin autenticación multifactor.

Área T9. Clasificación y tratamiento de la información

Aplica a: ISO/IEC 27001 (A.5.12 a A.5.14), ISO/IEC 27701 · **Justificación:** la información existe en papel, electrónica, software, servicios, personas y forma física; todos tienen contacto con ella.

Planificar

- ¿Están definidas las directrices de clasificación y tratamiento?
- ¿Cubren todas las formas de información?
- ¿Consideran la información de clientes?
- ¿Hay requisitos legales o regulatorios?
- ¿Forman parte de la formación?
- ¿Cómo se comprueba su cumplimiento?

Hacer

- ¿Cómo se aplican y se hacen cumplir?
- ¿Cómo se comunican a todo el personal?
- ¿Cómo se maneja la información de clientes?
- ¿Se cumplen los requisitos legales de tratamiento?
- ¿Se abordan todos los riesgos relacionados?

Área T9. Clasificación y tratamiento de la información (cont.)

Verificar

- ¿Cómo se controla la eficacia del tratamiento?
- ¿Se analizan los incidentes relacionados?
- ¿Qué mecanismos detectan infracciones?
- ¿Se revisan las directrices periódicamente?

Actuar

- ¿Qué medidas se adoptan ante infracciones?
- ¿Cómo se tratan los incidentes?
- ¿Se actualizan las políticas para que sigan siendo adecuadas?

Para recordar: prueba sugerida: muestrear documentos de un repositorio compartido y comparar etiqueta con contenido.

Área T10. Eficacia de la agilidad en el desarrollo

Aplica a: ISO/IEC 27001 (A.5.8, A.8.25), cualquier sector

Justificación: Ágil llegó para quedarse: mejora plazos, reduce costos y produce software de mayor calidad. La dirección necesita información cuantitativa, no anécdotas, para decidir.

Ruta de auditoría

- Verificar la estrategia y el plan de implementación ágil
- Entrevistar al scrum master, al equipo, al product owner y a otras partes
- Participar en las reuniones diarias para ver la metodología en acción
- Observar el uso saludable de los gráficos burn-down
- Comparar requisitos con entregables (artefactos)
- Revisar las lecciones aprendidas
- Verificar requisitos de seguridad en las historias de usuario y en la definición de “terminado”

Para recordar: la seguridad debe estar en cada iteración, no al final del proyecto.

Área T11. Eficacia y adecuación del SDLC

Aplica a: ISO/IEC 27001 (A.8.25 a A.8.33), cualquier sector

Justificación: Donde el software es clave para el negocio, un SDLC adecuado evita costos por fallas, asegura el cumplimiento legal, evita reacciones adversas del cliente y facilita el mantenimiento.

Ruta de auditoría

- Evaluar que cada fase tenga objetivos, entregables, tareas y objetivos de control
- Verificar normas metodológicas para calidad y mantenimiento
- Evaluar políticas, procedimientos y medidas
- Evaluar la capacidad de mantenerse al día con la normativa
- ¿Hay objetivos de gestión del SDLC y medidas para reducir errores?
- ¿Qué indicadores usan y cómo se presentan?
- Evaluar la comunicación externa, si existe

Área T12. Normas de codificación para calidad y seguridad

Aplica a: ISO/IEC 27001 (A.8.28), cualquier sector

Justificación: La mayoría de las normas de seguridad y calidad promueven una norma de codificación; algunas exigen reglas específicas. El objetivo es aumentar la fiabilidad con prácticas inteligentes.

Ruta de auditoría

- Evaluar objetivos, resultados clave, tareas y objetivos de control
- Verificar normas de codificación para calidad y mantenimiento; el código heredado puede “cumplir” y ser un espagueti difícil de mantener
- Evaluar políticas, procedimientos y medidas de reducción
- Evaluar prácticas de codificación en una muestra real
- ¿Hay objetivos y medidas de reducción de costo y tiempo?
- ¿Qué indicadores usan y cómo se presentan?

Área T13. Evaluación de impacto de los sistemas de IA

Aplica a: ISO/IEC 42001 (6.1.4, A.5, A.6), ISO/IEC 42005 · **Justificación:** los sistemas de IA pueden afectar a personas, grupos y a la sociedad; la organización debe evaluar esas consecuencias además de su propio riesgo.

Planificar

- ¿Hay un proceso definido para evaluar el impacto de los sistemas de IA?
- ¿Está definido cuándo se evalúa: diseño, cambios relevantes, antes del despliegue?
- ¿Hay inventario de sistemas de IA con su rol y propósito?
- ¿Los criterios consideran equidad, transparencia, seguridad y privacidad?
- ¿Se consideraron las fuentes de riesgo del Anexo C?
- ¿Quién aprueba las evaluaciones?

Hacer

- ¿Se evaluó el impacto de cada sistema de IA del alcance?
- ¿Participaron partes afectadas o sus representantes?
- ¿Se documentaron resultados y medidas de mitigación?
- ¿Los datos de entrenamiento tienen procedencia y calidad verificadas?
- ¿Se informa a los usuarios cuando interactúan con IA?
- ¿Los proveedores de IA cumplen las responsabilidades acordadas?

Área T13. Evaluación de impacto de los sistemas de IA (cont.)

Verificar

- ¿Se monitorea el desempeño y la deriva del modelo en producción?
- ¿Se reevalúa el impacto ante cambios o incidentes?
- ¿Se registran y analizan las quejas de usuarios afectados?
- ¿Las conclusiones de la evaluación se reflejan en controles de la SoA?

Actuar

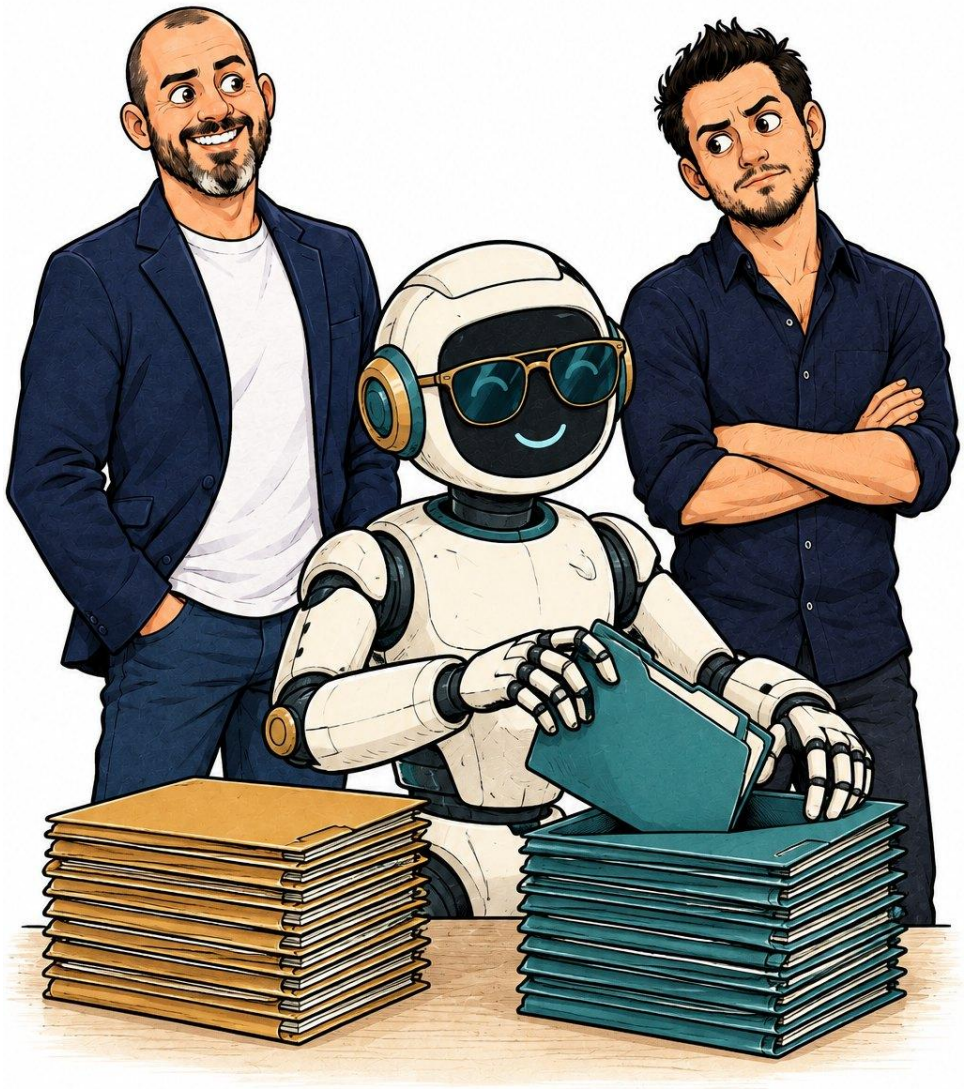
- ¿Qué se hace cuando un sistema produce resultados no previstos?
- ¿Se retiran o ajustan sistemas con impacto inaceptable?
- ¿Se actualizan los criterios con lo aprendido?
- ¿La revisión por la dirección considera los impactos de la IA?

Para recordar: prueba sugerida: tomar un sistema de IA desplegado y verificar que su evaluación de impacto fue previa y está vigente.

En la práctica

La evaluación de impacto se hace antes de desplegar, no después del titular del diario.

Evaluación de impacto: lo que el sistema hace cuando nadie lo está mirando.



Área T14. Derechos de los titulares de datos

Aplica a: ISO/IEC 27701:2025 (Anexo A, tabla A.1), RGPD, LGPD y leyes locales · **Justificación:** el ejercicio de derechos es donde el titular ve si el sistema de privacidad funciona; los plazos legales lo hacen fácil de probar.

Planificar

- ¿Están identificados los derechos aplicables según cada ley?
- ¿Hay procedimiento con plazos, roles y canales?
- ¿Está definido cómo verificar la identidad del solicitante?
- ¿Se previó la colaboración con encargados del tratamiento?

Hacer

- ¿Los canales están disponibles y son fáciles de usar?
- ¿Se registran todas las solicitudes?
- ¿Se responde en el plazo legal?
- ¿Se aplican las respuestas en todos los sistemas, incluidos los de terceros?

Área T14. Derechos de los titulares de datos (cont.)

Verificar

- ¿Se mide el cumplimiento de plazos?
- ¿Se analizan reclamos ante la autoridad de control?
- ¿Se audita una muestra de respuestas?

Actuar

- ¿Se corrigen las causas de demoras?
- ¿Se actualizan procedimientos y formación?
- ¿Se informa a la dirección?

Para recordar: prueba sugerida: muestrear solicitudes del período y comparar fecha de ingreso, respuesta y ejecución en los sistemas.

En la práctica

Cada dato personal necesita finalidad, base legal y un lugar donde encontrarlo cuando el titular pregunte.

El dato personal se manipula con guantes. Y con registro.



Área T15. Responsabilidades compartidas en la nube

Aplica a: ISO/IEC 27017, 27018, 27001 (A.5.23), 27701 · **Justificación:** cada modelo (IaaS, PaaS, SaaS) reparte distinto las responsabilidades; lo que nadie asume, nadie lo controla.

Planificar

- ¿Hay inventario de servicios en la nube con su modelo?
- ¿Hay una matriz de responsabilidades cliente–proveedor por servicio?
- ¿Se evaluaron las certificaciones y los informes del proveedor?
- ¿Se definieron requisitos de ubicación de datos y de salida?
- ¿Se identificaron los controles complementarios que quedan del lado del cliente?

Hacer

- ¿Los controles del lado del cliente están implementados (identidades, configuración, cifrado, registros)?
- ¿El contrato refleja la matriz de responsabilidades?
- ¿Se gestionan los subencargados del proveedor?
- ¿Se controla el uso de nube no autorizada?

Área T15. Responsabilidades compartidas en la nube (cont.)

Verificar

- ¿Se revisan periódicamente los informes del proveedor y sus excepciones?
- ¿Se monitorea la configuración de los servicios del cliente?
- ¿Se verificó la segregación entre entornos?

Actuar

- ¿Qué se hace ante excepciones en los informes del proveedor?
- ¿Se actualiza la matriz ante nuevos servicios?
- ¿Se probó la salida o la portabilidad de datos?

Para recordar: prueba sugerida: tomar un control complementario del informe del proveedor y pedir su evidencia del lado del cliente.

En la práctica

Lo que el contrato y la matriz de responsabilidades no asignan, nadie lo controla.

Responsabilidad compartida: cada uno sostiene su mitad. El problema es la línea punteada.



Conclusiones

Dominar el arte de hacer las preguntas correctas en una auditoría es crucial para obtener información precisa y completa y garantizar la eficacia del proceso de auditoría.

Al comprender diferentes tipos de preguntas, utilizar la escucha activa y emplear diversas técnicas de interrogatorio, los auditores pueden fomentar la comunicación abierta, fortalecer la relación con los auditados y mejorar sus habilidades de pensamiento crítico.

En última instancia, esto contribuye a una auditoría más exhaustiva y reveladora, que ayuda a las organizaciones a identificar riesgos, mejorar los controles internos y alcanzar sus objetivos. Reflexionar y perfeccionar continuamente las propias habilidades es esencial en el siempre cambiante mundo de la auditoría.



Y en normas con anexos

Riesgo → anexo → Declaración de Aplicabilidad → evaluación de controles. El patrón se repite en ISO/IEC 27001, 27701 y 42001: domínelo una vez y úselo siempre. La próxima norma de moda va a traer el mismo patrón… con otro logo.

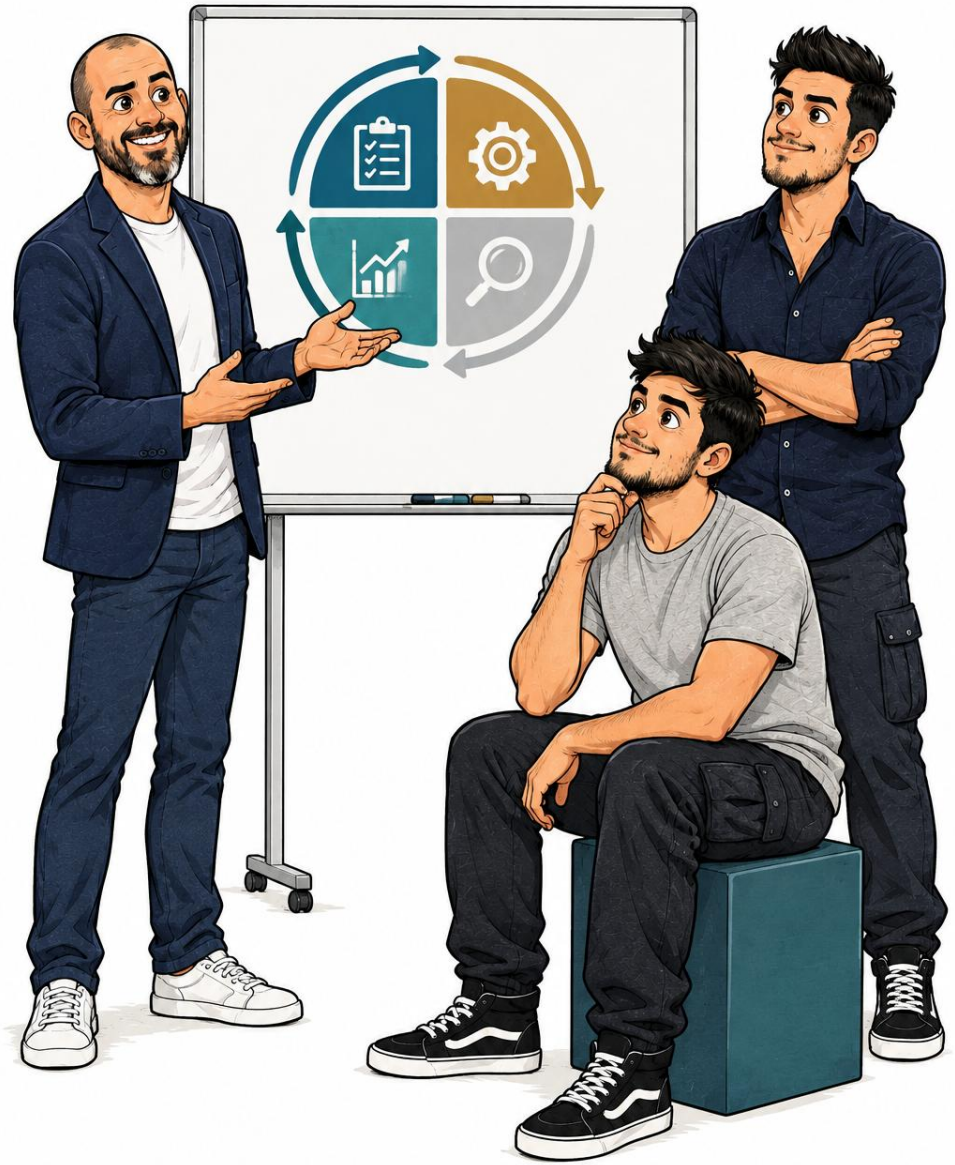
Diez ideas para llevarse

1. Un control puede no lograr el efecto previsto: por eso se evalúa
2. Auditar el sistema y evaluar los controles: se necesitan ambas
3. El anexo no es el punto de partida: lo es el riesgo
4. La SoA es el mapa del auditor; pruébela en ambos sentidos
5. 27001, 27701 y 42001 comparten el mismo patrón
6. Analizar, examinar, probar y muestrear
7. Pruebas autorizadas, proporcionales y competentes
8. Cuestionar y preguntar son habilidades distintas
9. Empiece abierto, termine cerrado, pida que le muestren
10. Sin evidencia no hay hallazgo; sin seguimiento, vuelve

En la práctica

Y recuerde: no solo hay que serlo, sino parecerlo.

Hasta la próxima auditoría.



Anexo: códigos EA de sectores de actividad

Código	Sector	Código	Sector
EA 01	Agricultura, silvicultura y pesca	**EA 11**	Combustible nuclear
EA 02	Minería y canteras	**EA 12**	Químicos
EA 03	Alimentos, bebidas y tabaco	**EA 13**	Farmacéuticos
EA 04	Textiles	**EA 14**	Caucho y plástico
EA 05	Cuero	**EA 15**	Minerales no metálicos
EA 06	Madera	**EA 16**	Hormigón, cemento, cal
EA 07	Pulpa y papel	**EA 17**	Metales básicos
EA 08	Editoriales	**EA 18**	Maquinaria y equipos
EA 09	Imprentas	**EA 19**	Equipos eléctricos y ópticos
EA 10	Coque y petróleo refinado	**EA 20**	Construcción naval

Anexo: códigos EA de sectores de actividad

Código	Sector	Código	Sector
EA 21	Aeroespacial	**EA 31a**	Logística
EA 22	Otros equipos de transporte	**EA 31b**	Correos y telecomunicaciones
EA 23	Manufactura no clasificada	**EA 32**	Intermediación financiera
EA 24	Reciclaje	**EA 33**	Tecnología de la información
EA 25	Electricidad	**EA 34**	Servicios de ingeniería
EA 26	Gas	**EA 35**	Otros servicios
EA 27	Agua	**EA 36**	Administración pública
EA 28	Construcción	**EA 37**	Educación
EA 29a	Comercio mayorista y minorista	**EA 38**	Salud y trabajo social
EA 30	Hoteles y restaurantes	**EA 39**	Otros servicios sociales



No somos solo consultores

Somos Legionarios Digitales

Somos…

“Arquitectos de la confianza digital. En Cloud Legion fusionamos la transformación digital con una gobernanza sólida para que la innovación tecnológica —desde la nube hasta la IA— sea el motor de crecimiento seguro de su organización.”

Nuestra misión

Asegurar la victoria de nuestros aliados en el campo de batalla digital. Forjamos el camino para una transformación segura, ética y ágil en un entorno global de alta presión regulatoria y cambio constante, donde la IA y la nube sean armas de crecimiento, no flancos de vulnerabilidad.

No somos solo consultores: somos legionarios digitales

Somos un cuerpo de élite multidisciplinario. En un mundo de amenazas híbridas, nuestra legión protege el activo más sagrado de las organizaciones: su integridad y su capacidad de innovar sin miedo.

Para recordar: la innovación sin gobernanza es velocidad sin frenos. Y los frenos también se auditan.

Nuestra filosofía: las cinco C

Cinco valores que guían a la Legión.

1 Compromiso

Enfoque total en las necesidades del cliente. Cada organización tiene necesidades distintas, por eso cada implementación se piensa en detalle y se enfoca en las necesidades verdaderas de cada cliente.

2 Creatividad

Soluciones simples, fáciles e intuitivas, que difícilmente requieren manuales. Ningún proyecto es una mercancía más: todo proyecto existe para resolver una necesidad del cliente de forma simple.

3 Competencia

Ser buenos no es suficiente. La transformación digital también es nuestra responsabilidad: innovamos y rompemos paradigmas como un grupo académico de investigadores en tecnología y seguridad de la información.

Nuestra filosofía: calidad, compliance y comunidad

4 Calidad / Compliance

Brindar soluciones de alta calidad para lograr la satisfacción de nuestros clientes y superar sus expectativas, bajo un sistema de gestión según los estándares ISO, orientado a la mejora continua de los procesos.







5 Comunidades

DevSecOps Latinoamérica nació en 2017 como DevSecOps Argentina, fundada por el equipo de Cloud Legion para profesionales dedicados a incorporar la seguridad en las prácticas ágiles y DevOps. Hoy, tras un camino recorrido junto a la comunidad, es DevSecOps Latinoamérica (devsecops-latam.org).





Cloud Legion en cifras

+40

personas

+500

certificaciones

+20

premios y reconocimientos

85 %

de la facturación en proyectos de nuevas tecnologías

+100

proyectos en 10 países de América y Europa

+99 %

índice de satisfacción de clientes

Premios y reconocimientos (1/2)

2024
GLOBEE AWARDS SILVER WINNER
CYBERSECURITY
Business Philanthropist of the Year (Cybersecurity)

2023 CHAMPION
CYBERSECURITY AWARENESS MONTH
2023 Nuevamente somos **"Cybersecurity Awareness Month champion"** by NCSA & CISA of the U.S. Department of Homeland Security.

2023
GLOBEE AWARDS BRONZE WINNER
CYBERSECURITY
Chief Technology Officer of the Year (Cybersecurity)

TOP CYBERSECURITY COMPANY Clutch ARGENTINA 2023
TOP CLOUD CONSULTING COMPANY Clutch BUENOS AIRES 2023

TÜVRheinland CERTIFIED
Management System
ISO 9001:2015
ISO/IEC 27001:2022
ISO/IEC 27701:2019
ISO/IEC 42001:2023
www.tuv.com
ID 9000006672
Adicional a nuestras normas ISO 27001, 27701 y 9001 en todos los procesos de la empresa. Somo la **primer empresa Argentina en certificar ISO 42001**

2022 CHAMPION
CYBERSECURITY AWARENESS MONTH
Somos **"Cybersecurity Awareness Month champion"** by NCSA & CISA of the U.S. Department of Homeland Security.

Info Security Products Guide 2020 GLOBAL EXCELLENCE BRONZE
Fuimos nombrados ganadores en la 16ta edición de los Premios a la excelencia **global** 2020 de Info Security PG´s **(Silicon Valley, USA)**

NETWORK PRODUCTS GUIDE IT World Awards 2020 BRONZE
NETWORK PRODUCTS GUIDE IT World Awards 2020 GOLD
Fuimos nombrados ganadores CTO of the Year | IT Software & Security Software en la 15th Annual IT World Awards 2020 de Network Products Guide **(Silicon Valley, USA)**

2019 to date Nuestro CDSO Chief DevSecOps strategy Officer fue reconocido como **Ambassador of DevOps Institute (Global Association)**
DEVOPS INSTITUTE Ambassador by PeopleCert

Premios y reconocimientos (2/2)

2021
GLOBEE AWARDS BRONZE WINNER
CYBER SECURITY GLOBAL EXCELLENCE AWARDS

Como respuesta a las tendencias y necesidades de la comunidad local, en 2017 fundamos la iniciativa y organización DevSecOps Argentina

DEVSECOPS Argentina by Cloud Legion

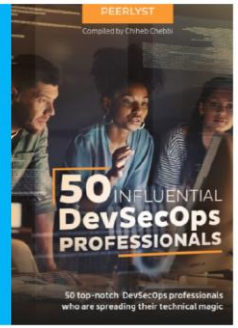
Ganamos el premio Cybersecurity Excellence Awards 2018 en la categoría Best Cybersecurity Startup

CYBER SECURITY EXCELLENCE AWARDS WINNER 2018

Ganamos el premio Cybersecurity Excellence Awards 2019 como **Best Cybersecurity Startup y Cybersecurity Team of the Year (Global Association)**

CYBER SECURITY EXCELLENCE AWARDS WINNER 2019

2019 Christian Ibiri & Luciano Moreira, fueron seleccionados por la gente de peerlyst, **"50 Influential DevSecOps Professionals" (Global Association)**



Cloud Legion es la primer consultora en Latinoamérica en lograr ser **CSA Global Consultancy de Cloud Security Alliance (American continent)**

CLOUD SECURITY ALLIANCE Trusted Cloud Consultant CSA

Microsoft MVP Most Valuable Professional

Nuestro CDSO - Chief DevSecOps strategy Officer otro año es seleccionado como **MVP en Microsoft Azure, Developer Technologies & Security AI**

Fuimos finalistas del premio Cybersecurity Excellence Awards 2017 en la categoría Best Cybersecurity Startup

CYBER SECURITY EXCELLENCE AWARDS FINALIST 2017

CYBERSECURITY Excellence Awards Cybersecurity Consultant of the Year WINNER 2016
CYBER SECURITY EXCELLENCE AWARDS WINNER 2017
CYBER SECURITY EXCELLENCE AWARDS WINNER 2018

Nuestro CDSO - Chief DevSecOps strategy Officer fue elegido Cybersecurity Consultant of the Year en los premios Cybersecurity Excellence Awards 2016, 2017 y 2018.

CLOUD LEGION

Certificaciones del equipo

Seguridad

Isc2 Cissp
Isaca Cisa
Cobit
Pci
Mcse + Security
CSA CCSK V3 Y V4
Certified Integrator In Secure Cloud Services
Cybersecurity For Industrial Control Systems
Operational Security (Opsec) For Control Systems

Nube

Mcse Private Cloud

Mcsa Office 365

Mcts Implementing Microsoft Azure Infrastructure

Mcts Administering Office 365 For Small Business

Cloudu - Rackspace

Aws Business Professional

Aws Technical Professional

Aws Security Fundamentals

Aws Solutions Architect – Associate

Aws Developer – Associate

Aws Sysops Administrator – Associate

Red Hat Delivery Specialist - Cloud Automation

Red Hat Delivery Specialist - Cloud Management

Red Hat Delivery Specialist - (Iaas)

Red Hat Delivery Specialist - (Paas) Administration

Red Hat Delivery Specialist - (Paas) Development

GRC

ISO/IEC 27001 Irca Certified Lead Auditor

ISO/IEC 27001 Lead Auditor & Implementer

ISO/IEC 27032 Lead Cybersecurity Manager

ISO 22301 Senior Lead Auditor & Implementer

ISO 31000 Lead Risk Manager

ISO/IEC 27701 Senior Lead Auditor & Auditor

ISO/IEC 20000-1:2018 Lead Auditor

ISO/IEC 27017:2015 Lead Auditor

ISO/IEC 27018:2019 Lead Auditor

ISO / TS 54001:2019 Gestion de Calidad Electoral

ISO/IEC 42001:2023 Lead Auditor & Implementer

CSA STAR Lead Auditor

TISAX Auditor

Staraudit (Ambassador)

Staraudit (Foundation)

Staraudit (Professional)

Staraudit (Internal Auditor

LGPD

Varias

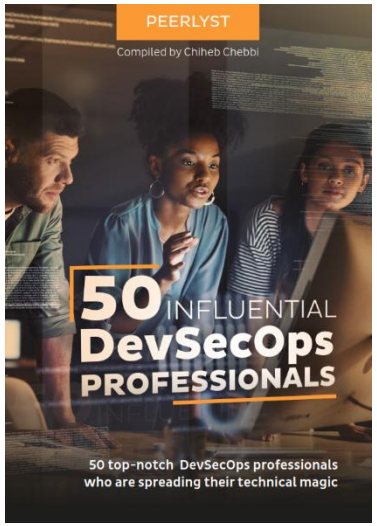
Cobit
Mcse Communication
Mcse Server Infrastructure
Mcts Server Virtualization With Windows Server
Red Hat (Rhcsa)
Lpi
Mcse Sharepoint & Productivity
Ccna
Itil
Certified Scrummaster
Atlassian Marketing Professional
Atlassian Accredited Technical Sales Professional
Atlassian Accredited Sales Professional
Atlassian Accredited Operations Professional
Devops Leader (Dol)
Devsecops Engineering (Dsoe)

Referentes en DevOps y DevSecOps

DEVSECOPS Argentina by Cloud Legion

DEVSECOPS Latinoamérica

Somos fundadores de la iniciativa y organización de la comunidad **DevSecOps Argentina y Latam**



Christian Ibiri & Luciano Moreira, fueron seleccionados por la comunidad peerlyst, **"50 Influential DevSecOps Professionals“**





Nuestro CDSO Chief DevSecOps strategy Officer fue reconocido como **Ambassador del DevOps Institute y de WAZUH**

Referentes en seguridad de la nube

Somos la primera consultora en la región en calificar como CSA Global Consultant y contar con un Certified CSA STAR Auditor

El Programa de consultoría global de CSA (CSA GCP) es un marco que permite a los clientes de la nube trabajar con una red de profesionales y organizaciones de seguridad de confianza que ofrecen servicios profesionales cualificados basados en las mejores prácticas de CSA. Estos proveedores tienen un amplio conocimiento de los retos a los que se enfrentan las organizaciones al pasar a la nube.

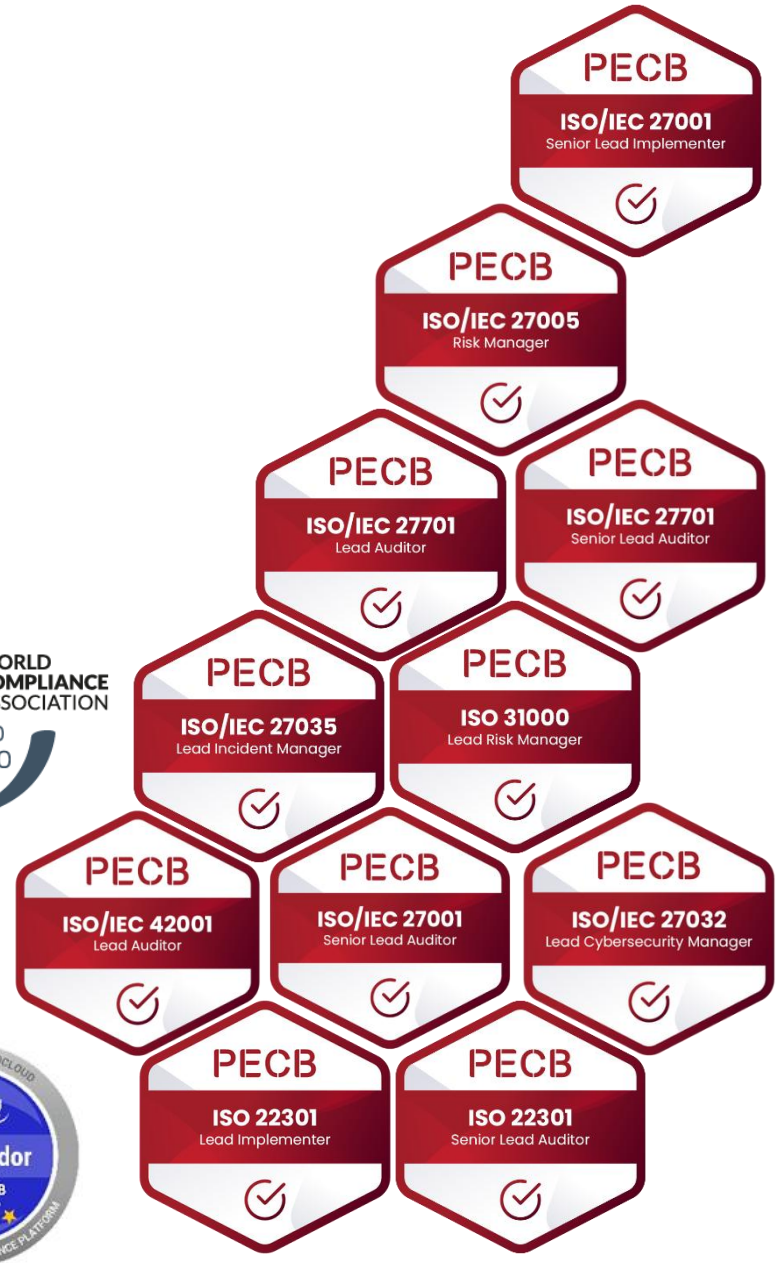
https://cloudsecurityalliance.org/global-consultancy/registry/

Nuestro CDSO - Chief DevSecOps strategy Officer es **MVP en Microsoft Azure, Developer Technologies, Cloud Security, Security AI**

Referentes en cumplimiento normativo

Contamos con profesionales, certificado y acreditados por diferentes entidades en las principales normas de la industria. Expertos en Sistemas de Gestión, Cumplimiento Normativo ISO y Cumplimiento Legal.

Nos respaldan el 100% de empresas certificadas a la primera, y un 95% clientes que repiten .



WORLD COMPLIANCE ASSOCIATION
MIEMBRO ASOCIADO

CQI | IRCA

TISAX®

bsi.

ISO 27018 CERTIFIED
Privacy Protection

ISO 27017 CERTIFIED
Cloud Security

GENERAL LAW FOUNDATION
CertiProf
Professional Knowledge
DATA PROTECTION
LGPDF™

CSA STAR
LEAD AUDITOR

onetrust
Privacy
PROFESSIONAL

TÜVRheinland
CERTIFIED

PROVIDED BY EUROCLOUD
EuroCloud
Internal Auditor
StarAudit-IA
TRUSTED DIGITAL COMPETENCE PLATFORM

PROVIDED BY EUROCLOUD
EuroCloud
Professional
StarAudit-PF
TRUSTED DIGITAL COMPETENCE PLATFORM

PROVIDED BY EUROCLOUD
EuroCloud
Foundation
StarAudit-FD
TRUSTED DIGITAL COMPETENCE PLATFORM

PROVIDED BY EUROCLOUD
EuroCloud
Ambassador
StarAudit-AB
TRUSTED DIGITAL COMPETENCE PLATFORM

CLOUD LEGION

Referentes en inteligencia artificial

Somos la primera empresa en Argentina y la primer consultora en Latam en lograr la certificación ISO 42001.

Contamos con el primer caso de éxito de adecuación y certificación ISO 42001 de la región Latam.

Somos la primer consultora de Latinoamérica en hacer parte del Compromiso de Confianza en IA de la CSA, afirmado nuestro compromiso a los principios fundamentales de seguridad, transparencia, responsabilidad ética y privacidad en los sistemas de IA.

Contamos con el equipo mas preparado de la región, con auditores/ implementadores certificados y acreditados en la ISO 42001.



Nuestro Chief Transformation & Strategy Officer otro año es seleccionado como MVP de Microsoft y paso a formar parte de la comunidad de MVP de Microsoft Security Copilot: un grupo selecto de expertos de confianza, reconocidos por su experiencia, liderazgo y pasión. Juntos, impulsamos el futuro de la inteligencia artificial aplicada a la seguridad.

Servicios

Un ecosistema de innovación basado en tecnología, conocimiento y la calidad de nuestros profesionales, para las empresas más exigentes.

Auditoría y aseguramiento

Governance & Strategic Planning

GRC Consulting & Services

ISO 27001

ISO 22301

ISO 25000

ISO 20000

ISO 31000

ISO 42001

ISO 27701

ISO 27017

ISO 27018

PCI DSS

TISAX

IA GRC

Servicios profesionales

Cloud Security

DevSecOps

Security & Compliance

DevOps

Cloud Computing

Business Transformation
Innovation & Disruption

Digital Products Development

Secure AI Lifecycle

Servicios gestionados

Security Management

Cloud Management

Cloud Cost Management

Cloud Security Management
Cloud Center of Excellence

IT Management

Applications Management

SQUAD

Velites

Hastati

Équites

Pretorian

Para recordar: contacto: info@cloudlegion.com.ar

¡Gracias!

11000010 10100001 01000111 01110010 01100001
01100011 01101001 01100001 01110011 00100001

“No solo hay que serlo, sino parecerlo” (y viceversa)

