Strecht Simulados · Guia de preparação



Guia de preparação ISO 42001 Lead Auditor

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

7 capítulos por domínio	**40** questões comentadas	**70%** nota de corte
6 provas completas no curso		

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso ISO 42001 Lead Auditor: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 70%).

Mapa do exame

Cada prova do curso tem 80 questões e 180 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA	15%	18 conceitos · 14 pegadinhas
2. Domínio 2: Requisitos do sistema de gestão de IA	10%	18 conceitos · 14 pegadinhas
3. Domínio 3: Conceitos e princípios fundamentais de auditoria	20%	18 conceitos · 14 pegadinhas
4. Domínio 4: Preparação de uma auditoria ISO/IEC 42001	11,25%	18 conceitos · 12 pegadinhas
5. Domínio 5: Condução de uma auditoria ISO/IEC 42001	23,75%	18 conceitos · 14 pegadinhas
6. Domínio 6: Encerramento de uma auditoria ISO/IEC 42001	8,75%	16 conceitos · 12 pegadinhas
7. Domínio 7: Gestão de um programa de auditoria ISO/IEC 42001	11,25%	17 conceitos · 13 pegadinhas

Como ler os capítulos: os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 12 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

A Rede de Hospitais Cuidar Bem quer que médicos consigam prever como o sistema de IA vai se comportar ao receber exames com certas características. Na ISO/IEC 22989, qual propriedade permite suposições confiáveis das partes interessadas sobre a saída?

A. Explicabilidade do sistema
B. Heteronomia
C. Previsibilidade
D. Imputação

D2 · Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

A Empresa de Telecom Sinal Forte usa um modelo para transcrever chamadas de voz, um tipo de dado sequencial. Pela ISO/IEC 22989, qual tipo de rede neural é tipicamente associado a esse processamento sequencial?

A. Rede neural convolucional para imagens
B. Árvore de decisão com regras simbólicas
C. Rede neural recorrente, como a LSTM
D. Máquina de vetores de suporte linear

D3 · Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

Um palestrante diz que o assistente de redação usado pela Agência Pena de Ouro é uma inteligência artificial geral (AGI). Pelas definições da ISO/IEC 22989, por que essa classificação tende a ser incorreta para um sistema focado em gerar textos de marketing?

A. Porque todo sistema de geração de texto é classificado como sistema especialista
B. Porque a 22989 proíbe classificar sistemas comerciais como IA geral
C. Porque é IA estreita: focada em tarefas definidas
D. Porque a AGI é definida como qualquer sistema que use redes neurais profundas

D4 · Domínio 2: Requisitos do sistema de gestão de IA

A Empresa de Energia Eólica Ventania quer entender como usar o Anexo B da ISO/IEC 42001 na implementação. A equipe pergunta se precisa registrar na declaração de aplicabilidade cada orientação do Anexo B que decidir não seguir. Qual afirmação está de acordo com a explicação da PECB?

A. Substitui o Anexo A e passa a ser a lista obrigatória de controles do AIMS
B. Lista os setores proibidos de usar IA sem aprovação de um regulador
C. Traz os requisitos de auditoria que o organismo de certificação deve seguir
D. Orienta a implementação dos controles; não exige justificar seu uso na SoA

D5 · Domínio 2: Requisitos do sistema de gestão de IA

A Rede de Clínicas Bem Estar identificou 12 riscos de IA, mas a declaração de aplicabilidade só menciona controles para 7 deles, sem explicar como os outros 5 foram tratados. A gerente do AIMS diz que esses riscos são de menor impacto. O que a nota da definição de declaração de aplicabilidade indica?

A. Riscos e controles devem se refletir na declaração
B. Riscos menores ficam fora da declaração e do AIMS
C. A declaração deve listar só os controles do Anexo A
D. A declaração é opcional para empresas da área de saúde

D6 · Domínio 2: Requisitos do sistema de gestão de IA

A introdução da ISO/IEC 42001 cita exemplos de processos de gestão cruciais que devem considerar questões específicas de IA. Qual opção corresponde a esses exemplos?

A. Contabilidade, folha de pagamento, marketing digital e vendas pela internet
B. Recrutamento, avaliação de desempenho, promoções e desligamento de pessoal
C. Objetivos e política, riscos e oportunidades, confiabilidade da IA e fornecedores
D. Manutenção predial, limpeza, segurança patrimonial e transporte de funcionários

D7 · Domínio 3: Conceitos e princípios fundamentais de auditoria

Segundo a ISO 19011:2026, quais características compõem a definição de auditoria?

A. Atividade informal e voluntária da área de TI
B. Inspeção técnica do código-fonte dos modelos
C. Processo sistemático, independente e documentado
D. Avaliação feita pela própria área sobre si mesma

D8 · Domínio 3: Conceitos e princípios fundamentais de auditoria

A auditora Lúcia simpatiza muito com a equipe da Startup Ideia Verde e acredita no propósito ambiental da empresa. Durante a auditoria, encontra evidência clara de que o controle de mudanças do modelo não é aplicado. Qual postura demonstra objetividade?

A. Pedir a outro auditor que registre, para não se indispor com a equipe
B. Registrar a constatação conforme a evidência encontrada
C. Registrar como oportunidade de melhoria por causa do propósito da empresa
D. Dar um prazo informal para a empresa corrigir antes de registrar

D9 · Domínio 3: Conceitos e princípios fundamentais de auditoria

Dois organismos de certificação diferentes vão auditar juntos, na mesma visita, o AIMS da Cooperativa Leiteira Vale Verde, cada um responsável por parte da equipe, porque a cooperativa exporta e precisa de certificados reconhecidos em dois mercados. Segundo a ISO 19011:2026, como se chama esse tipo de auditoria?

A. Auditoria conjunta
B. Auditoria de segunda parte
C. Auditoria combinada
D. Auditoria interna

D10 · Domínio 4: Preparação de uma auditoria ISO/IEC 42001

O organismo designou para auditar o AIMS do Laboratório Genoma Vivo, que usa IA em laudos de diagnóstico, uma equipe com boa experiência em ISO/IEC 42001, mas sem conhecimento de processos laboratoriais e de regulação sanitária. O que o líder deve propor?

A. Reduzir o escopo da auditoria aos documentos
B. Incluir um especialista técnico na equipe
C. Pedir ao auditado que explique o setor e aceitar o relato
D. Seguir com a equipe atual e registrar a limitação no relatório

D11 · Domínio 4: Preparação de uma auditoria ISO/IEC 42001

A líder que vai auditar o AIMS da Empresa de Pagamentos Pix Fácil precisa definir como a equipe vai amostrar alterações de modelos, avaliações de risco e registros de treinamento. Há milhares de registros de cada tipo no período auditado. O que deve preparar antes da auditoria?

A. Um plano de amostragem com critérios e tamanhos
B. Uma lista de constatações pré-redigidas para agilizar o relatório
C. Um acordo para o auditado escolher a amostra
D. Um roteiro fixo que não pode ser alterado

D12 · Domínio 4: Preparação de uma auditoria ISO/IEC 42001

O organismo vai auditar a Indústria Têxtil Seda Fina. Para uma auditoria de certificação ISO/IEC 42001, qual conjunto costuma compor os critérios de auditoria?

A. A ISO/IEC 42001, a informação documentada do AIMS e requisitos legais aplicáveis
B. As preferências pessoais do líder sobre boas práticas de ciência de dados e engenharia
C. As metas de vendas da empresa para o próximo ano e o orçamento da área de TI
D. Os critérios de avaliação de desempenho dos funcionários definidos pelo RH

01

CAPÍTULO 1 · 15% DA PROVA

Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

Aqui eu preciso saber o que é a ISO/IEC 42001, para quem ela vale e onde ela se encaixa na família de normas de IA da ISO, além dos termos de IA da ISO/IEC 22989. A prova cobra muito 'qual norma faz o quê' (22989, 23053, 23894, 38507, 42005, 42006, 17021-1, 17024) e o ecossistema de certificação (ISO, organismo de certificação, organismo de acreditação). Também cai bastante a identificação de conceitos de IA a partir de um cenário curto: tipo de aprendizado, tipo de rede, propriedade de confiabilidade. Onde mais erro: confundir robustez com resiliência, verificação com validação, hiperparâmetro com parâmetro e achar que a ISO certifica empresas.

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

ISO/IEC 42001 (AIMS)

Norma de requisitos para um sistema de gestão de IA (AI management system), passível de certificação por terceira parte. Vale para qualquer organização que desenvolve, fornece ou usa produtos ou serviços com IA, inclusive órgão público e quem só usa IA de terceiros. Certifica o sistema de gestão, não cada sistema de IA.

Referência normativa única

A seção 2 da 42001 tem uma única referência normativa: ISO/IEC 22989:2022. O conteúdo citado dela passa a constituir requisito da 42001. A 27001 aparece só na bibliografia e a 19011 não é referência normativa.

Família de normas de IA

22989 = terminologia e conceitos (sem requisitos certificáveis); 23053 = framework para sistema de IA que usa aprendizado de máquina; 23894 = gestão de riscos de IA; 38507 = implicações de governança para o órgão de governança; 42005 = avaliação de impacto de sistemas de IA; 42006 = requisitos adicionais à 17021-1 para organismos que auditam e certificam AIMS; 5338 = processos do ciclo de vida de sistemas de IA; 5259-1 = fonte da definição de qualidade de dados; ISO/IEC TR 24368 = visão geral de preocupações éticas e sociais.

ISO/IEC JTC 1/SC 42

Comitê técnico que preparou a ISO/IEC 42001 (Inteligência artificial). Distratores clássicos: SC 27 (27001), ISO/TC 176 (família 9000) e ISO/CASCO (normas de avaliação da conformidade, como a 17021-1).

Por que a IA pede gestão própria

A introdução da 42001 aponta decisão automática pouco transparente, lógica aprendida a partir de dados em vez de programada e aprendizado contínuo que muda o comportamento durante o uso. Custo, burocracia ou preferência de mercado nunca são a resposta.

Abordagem baseada em risco da 42001

Serve para aplicar o nível adequado de controle a cada caso de uso, produto ou serviço de IA no escopo. Não dispensa os requisitos das seções 4 a 10 para sistemas de baixo risco nem transfere responsabilidade a fornecedores.

42001 não é passo a passo

A norma especifica requisitos e evita orientação prescritiva: a organização pode combinar frameworks, outras normas e experiência própria para gestão de riscos, ciclo de vida e qualidade de dados. Não obriga usar a 23894 como método único.

Harmonized Structure

Estrutura, textos e termos comuns às normas de sistema de gestão (antigo Anexo SL). É o que facilita integrar a 42001 com a 27001. Por ela, monitoramento, auditoria interna e análise crítica ficam sempre na seção 9 (avaliação de desempenho).

Organização e órgão de governança

Quando o escopo cobre só parte da entidade, 'organização' é a parte incluída no escopo do AIMS. Órgão de governança é quem responde pelo desempenho e pela conformidade, como um conselho; em pequenas organizações pode não estar separado da alta direção.

Ecossistema de certificação

A ISO não realiza certificação, não emite certificados e não permite seu logotipo associado à certificação. Quem certifica é o organismo de certificação (pode ser governamental ou não); o organismo de acreditação reconhece formalmente que o certificador opera conforme normas internacionais. Para checar um certificado: CertSearch ou o próprio organismo de certificação ou de acreditação.

Esquema de certificação e normas de conformidade

Esquema = sistema de avaliação da conformidade com os mesmos requisitos, regras e procedimentos. A 17021-1 rege organismos que certificam sistemas de gestão; a 17024 rege certificação de pessoas (é a base do esquema da PECB); a certificação de AIMS pela 42006 pode ser incorporada a esquema de certificação de produtos conforme a 17065.

Sistema de IA e agente de IA (22989)

Sistema de IA é um sistema projetado que gera saídas, como previsões, recomendações ou decisões, para objetivos definidos por humanos; não envolve consciência. Agente de IA percebe o ambiente, responde e age para atingir objetivos. IA estreita foca tarefas definidas; IA geral cobre ampla gama de tarefas.

Tipos de aprendizado

Aprendizado de máquina = otimizar parâmetros do modelo para refletir dados ou experiência. Supervisionado usa só dados rotulados; não supervisionado só dados sem rótulo (agrupar por semelhança); semissupervisionado mistura os dois; por reforço aprende por recompensa e penalidade interagindo com o ambiente; aprendizado contínuo é treinamento incremental durante a operação; retreinamento é treinar de novo com outros dados.

Redes neurais e outras técnicas

Neurônio combina entradas e aplica função de ativação; rede neural tem camadas de neurônios com pesos ajustáveis; aprendizado profundo (muitas camadas ocultas) é subconjunto do aprendizado de máquina; rede recorrente (LSTM) trata dados sequenciais e convolucional é típica de imagens. Sistema especialista usa regras de especialistas; algoritmo genético evolui uma população de soluções; soft computing tolera imprecisão (lógica fuzzy); computação semântica busca significado e intenção; computação cognitiva busca interação natural pessoa-máquina; mineração de dados extrai padrões.

Propriedades de confiabilidade (22989)

Robustez = manter o desempenho em quaisquer circunstâncias; resiliência = recuperar a operação rapidamente após incidente; previsibilidade = permitir suposições confiáveis sobre a saída; explicabilidade = expressar os fatores que influenciaram o resultado; controlabilidade = humano ou agente externo pode intervir; responsabilização (accountability) = responder por ações, decisões e desempenho; heteronomia = operar sob controle externo; autonomia = mudar domínio ou objetivo sem controle externo; trustworthiness = atender às expectativas das partes interessadas de forma verificável.

Termos de dados (22989)

Ground truth = valor-alvo de referência do item rotulado; hiperparâmetro é definido antes do treino e parâmetro (pesos) é aprendido no treino; dados de validação comparam modelos candidatos, dados de teste avaliam o modelo final, dados de produção são os da operação. Anotação anexa informação sem alterar o dado; aumento cria amostras sintéticas; imputação preenche ausentes; análise exploratória examina ausentes, atípicos e representatividade.

Verificação, validação, predição e ciclo de vida

Verificação confirma que atende à especificação; validação confirma que funciona para o uso pretendido, nessa ordem. Predição é a saída primária do sistema e não precisa ser sobre o futuro. Ciclo de vida vai da concepção até a aposentadoria.

Papéis da organização frente à IA

No contexto do AIMS, a organização determina seus papéis em relação aos sistemas de IA que desenvolve, fornece e usa; um banco pode ser desenvolvedor e usuário ao mesmo tempo.

Macetes para memorizar

💡 Família de normas

22989 Dicionário, 23053 Desenho com ML, 23894 Risco, 38507 Conselho, 42005 Impacto, 42006 Certificador, 42001 Requisitos do AIMS.

💡 Robustez x resiliência

Robusto aguenta o tranco; resiliente levanta depois do tombo.

💡 Verificação x validação

V de 'Vê a especificação' vem antes de V de 'Vale para o uso'.

💡 Hiperparâmetro

HIPER = antes (definido por quem projeta); parâmetro = depois (aprendido no treino).

💡 Heteronomia

Hetero = outro manda (controle externo); auto = manda em si.

💡 Quem certifica

ISO escreve, certificador certifica, acreditador avalia o certificador.

💡 Tipos de aprendizado

Só rótulo = super; sem rótulo = não super; metade-metade = semi; prêmio e castigo = reforço.

Tabela de memorização: não confunda

Quando é...	...e quando é
Robustez O sistema mantém o mesmo desempenho com chuva, pouca luz ou dado sujo (condições adversas).	**Resiliência** O sistema caiu ou teve incidente e voltou a operar normalmente em pouco tempo.
Verificação Confirmar que o modelo atende à especificação técnica (vem primeiro).	**Validação** Confirmar que funciona para o uso pretendido, com usuários reais (vem depois).
Hiperparâmetro Escolha de projeto definida antes do treinamento, que controla o aprendizado.	**Parâmetro do modelo** Variável interna, como pesos, determinada durante o treinamento.
Aumento de dados Criar amostras sintéticas a partir de dados existentes.	**Imputação** Substituir valores ausentes por estimativas.
Transparência do sistema Disponibilizar a partes interessadas informações apropriadas sobre o sistema.	**Transparência da organização** Comunicar decisões e atividades da organização de forma compreensível.
Organismo de acreditação Avalia e reconhece formalmente o certificador; não emite certificado ao cliente.	**Organismo de certificação** Audita a organização e emite o certificado ISO/IEC 42001.
ISO/IEC 42001 Requisitos do AIMS que a organização implementa e certifica.	**ISO/IEC 42006** Requisitos adicionais à 17021-1 para o organismo que audita e certifica AIMS.

Números que caem

Item	Valor
Peso do domínio na prova PECB	**15% (12 de 80 questões)**
Anexo A da ISO/IEC 42001 (segundo a PECB)	**38 controles e 10 objetivos de controle**
Referência normativa da 42001	**ISO/IEC 22989:2022**
Edição vigente da ISO/IEC 42001	**ISO/IEC 42001:2023, edição 1, publicada em 18/12/2023**
ISO/IEC 42006 (certificadores de AIMS)	**Publicada em 07/07/2025**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que a 27001 é referência normativa e que seus controles viram obrigatórios no AIMS.
Como não cair: A única referência normativa é a ISO/IEC 22989:2022; a 27001 está só na bibliografia.

⚠ **Alerta de prova:** Dizer que a empresa foi 'certificada pela ISO' ou que o logotipo da ISO valida o certificado.
Como não cair: A ISO não certifica, não emite certificado e não permite seu logotipo associado a certificação; quem certifica é o organismo de certificação.

⚠ **Alerta de prova:** Concluir que quem só usa IA de fornecedor, ou é órgão público, fica fora da 42001.
Como não cair: A norma vale para qualquer organização que desenvolve, fornece ou usa IA; desenvolver modelo próprio não é condição.

⚠ **Alerta de prova:** Exigir que o fornecedor de IA tenha certificação 42001 antes de a usuária se certificar.
Como não cair: Cada organização certifica o próprio AIMS; a certificação do fornecedor não é pré-requisito.

⚠ **Alerta de prova:** Usar a 22989 para certificar o AIMS por ser 'a norma principal de IA'.
Como não cair: A 22989 só define termos e conceitos; requisitos certificáveis estão na 42001.

⚠ **Alerta de prova:** Marcar 'resiliência' quando o sistema mantém o desempenho em condições adversas.
Como não cair: Manter desempenho = robustez; recuperar após incidente = resiliência.

⚠ **Alerta de prova:** Trocar a ordem: validação e depois verificação.
Como não cair: Primeiro verifica a especificação, depois valida o uso pretendido.

⚠ **Alerta de prova:** Chamar de parâmetro a escolha de projeto feita antes do treino.
Como não cair: Definido antes do treino = hiperparâmetro; aprendido no treino = parâmetro.

⚠ **Alerta de prova:** Confundir controlabilidade com transparência ou explicabilidade.
Como não cair: Controlabilidade é poder intervir (por exemplo, interromper uma ação); explicar fatores é explicabilidade; informar sobre o sistema é transparência.

⚠ **Alerta de prova:** Achar que AGI se define por usar redes neurais profundas.
Como não cair: AGI se define pela amplitude de tarefas, não pela técnica; gerador de texto de marketing é IA estreita.

⚠ **Alerta de prova:** Achar que predição só vale para valores futuros.
Como não cair: Na 22989, predição é a saída primária do sistema, inclusive sobre dados históricos.

⚠ **Alerta de prova:** Dizer que a abordagem baseada em risco dispensa as seções 4 a 10 para IA de baixo risco.
Como não cair: Ela só ajusta o nível de controle por caso de uso; os requisitos do sistema de gestão continuam aplicáveis.

⚠ **Alerta de prova:** Achar que órgão público deve usar a 38507 no lugar da 42001.
Como não cair: A 38507 orienta o órgão de governança sobre o uso de IA; não substitui o AIMS.

⚠ **Alerta de prova:** Achar que a PECB certifica o AIMS de empresas.
Como não cair: A PECB certifica pessoas, conforme a ISO/IEC 17024; AIMS é certificado por organismos sob 17021-1 e 42006.

Como cai na prova

📝 **Como cai:** Cenário curto descreve o que um sistema faz e pergunta 'pela ISO/IEC 22989, como se chama'.
Como resolver: Isole o verbo-chave (manter, recuperar, intervir, explicar, prever) e associe à definição exata; descarte as alternativas que descrevem outro termo da mesma família.

📝 **Como cai:** Empresa quer orientação sobre um tema e pergunta 'qual norma é a mais indicada'.
Como resolver: Identifique o público e o tema (termos, risco, impacto, governança, certificador) e escolha a norma da família correspondente; lembre que 17021-1 e 19011 são de auditoria e certificação, não de IA.

📝 **Como cai:** Diretor quer anunciar 'certificado pela ISO' ou validar certificado pelo logotipo.
Como resolver: Responda que a ISO não certifica nem autoriza seu logotipo; verificação é pela CertSearch ou pelo organismo.

📝 **Como cai:** Organização que só usa IA de terceiros, ou é pública, pergunta se pode se certificar.
Como resolver: Sim: a 42001 vale para quem desenvolve, fornece ou usa IA; descarte condições inventadas (desenvolver modelo, fornecedor certificado).

📝 **Como cai:** Pergunta sobre a natureza da 42001 ou o que a introdução diz.
Como resolver: Norma de requisitos do sistema de gestão, certificável, não prescritiva, com abordagem baseada em risco para dosar controles.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
termos e conceitos de IA, terminologia	**ISO/IEC 22989**
framework de sistema de IA que usa aprendizado de máquina	**ISO/IEC 23053**
orientação para gerir riscos de IA e integrá-los à organização	**ISO/IEC 23894**
conselho, o que supervisionar ao autorizar o uso de IA	**ISO/IEC 38507 (governança)**
quando avaliar impacto, escopo, responsabilidades e registro da avaliação	**ISO/IEC 42005**
requisitos para organismos que certificam AIMS	**ISO/IEC 42006 + ISO/IEC 17021-1**
desinformação, grupos vulneráveis, preocupações éticas e sociais	**ISO/IEC TR 24368**
recompensa e penalidade ao interagir com o ambiente	**Aprendizado por reforço**
poucos casos rotulados e grande volume sem rótulo	**Semissupervisionado**
voz, texto, sequência temporal	**Rede neural recorrente (LSTM)**
regras fornecidas por especialistas humanos	**Sistema especialista (IA simbólica)**
lógica fuzzy, dados imprecisos, incerteza	**Soft computing**
notas sistematicamente menores para um grupo com o mesmo perfil	**Viés (bias)**
integrar com a 27001 que a empresa já tem	**Harmonized Structure (estrutura, textos e termos comuns)**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- A ISO não certifica ninguém e não autoriza seu logotipo em certificados.
- A 42001 vale para quem desenvolve, fornece ou usa IA, mesmo só de terceiros.
- Única referência normativa: ISO/IEC 22989:2022.
- Robustez mantém desempenho; resiliência recupera após incidente.

Essenciais para a prova (checklist)

- ☐ Sei dizer o tema de cada norma: 22989, 23053, 23894, 38507, 42005, 42006, 5338, 17021-1, 17024.
- ☐ Sei que a 42001 foi preparada pelo ISO/IEC JTC 1/SC 42.

- ☐ Sei explicar o papel da ISO, do organismo de certificação e do organismo de acreditação.
- ☐ Sei distinguir aprendizado supervisionado, não supervisionado, semissupervisionado, por reforço e contínuo.
- ☐ Sei distinguir robustez, resiliência, previsibilidade, explicabilidade, controlabilidade e transparência.
- ☐ Sei diferenciar hiperparâmetro de parâmetro e dados de validação, teste e produção.
- ☐ Sei por que a introdução da 42001 diz que a IA pede gestão específica.
- ☐ Sei que a Harmonized Structure facilita integrar a 42001 com a 27001.

Questões de revisão do capítulo

R1.1 · Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

A Transportadora Rota Ótima usa um método que cria uma população de rotas candidatas, combina e altera as melhores ao longo de gerações e seleciona as mais eficientes. O método não usa redes neurais nem dados rotulados. Pela ISO/IEC 22989, como se chama essa técnica?

A. Sistema especialista
B. Algoritmo genético
C. Análise de sentimento
D. Rede neural recorrente

R1.2 · Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

Qual norma da família de IA da ISO estabelece um framework para descrever um sistema de IA genérico que usa aprendizado de máquina?

A. ISO/IEC 42006:2025
B. ISO/IEC 23053
C. ISO/IEC 42005:2025
D. ISO/IEC 17021-1:2015

R1.3 · Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

A equipe da Empresa de Diagnóstico Laboratorial Exato confirmou que o modelo atende à especificação técnica e, depois, que ele funciona para o uso pretendido com pacientes reais. Pela ISO/IEC 22989, como se chamam essas duas confirmações?

A. Calibração e, depois, imputação
B. Validação e, depois, verificação
C. Anotação e, depois, retreinamento
D. Verificação e, depois, validação

R1.4 · Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

Segundo a ISO/IEC 22989, qual característica diferencia a IA simbólica da IA subsimbólica?

A. A simbólica usa regras explícitas; a subsimbólica usa representação implícita dos dados
B. A simbólica dispensa dados de treinamento; a subsimbólica dispensa modelos
C. A simbólica opera de forma autônoma; a subsimbólica opera sob controle externo
D. A simbólica usa redes neurais profundas; a subsimbólica usa árvores de decisão

Respostas comentadas

R1.1. B) Algoritmo genético

Por quê: A 22989 trata algoritmos genéticos entre os conceitos de IA, ao lado de soft computing, computação cognitiva e semântica.

✗ A) Incorreta. Sistema especialista usa conhecimento de especialistas.
✗ C) Incorreta. Análise de sentimento classifica opiniões.
✗ D) Incorreta. Rede recorrente processa dados sequenciais.

> **Dica de prova:** População de soluções que evolui = algoritmo genético.

R1.2. B) ISO/IEC 23053

Por quê: A família de IA inclui 22989 (termos), 23053 (framework de ML), 23894 (risco), 38507 (governança), 42001 (sistema de gestão), 42005 (avaliação de impacto) e 42006 (organismos de certificação).

✗ A) Incorreta. A 42006 traz requisitos adicionais para organismos que certificam AIMS.
✗ C) Incorreta. A 42005 orienta a avaliação de impacto de sistemas de IA.
✗ D) Incorreta. A 17021-1 traz requisitos para organismos que auditam e certificam sistemas de gestão.

> **Dica de prova:** Framework de sistema de IA com ML = 23053.

R1.3. D) Verificação e, depois, validação

Por quê: A nota da definição de verificação na 22989 diz que ela só dá garantia de que o produto atende à sua especificação.

✗ A) Incorreta. Calibração e imputação não são esses conceitos.
✗ B) Incorreta. A ordem dos conceitos está trocada.
✗ C) Incorreta. Anotação e retreinamento são atividades de dados e modelo, não confirmações.

> **Dica de prova:** Verificação = especificação; validação = uso pretendido.

R1.4. A) A simbólica usa regras explícitas; a subsimbólica usa representação implícita dos dados

Por quê: Pela 22989, a IA simbólica produz saídas declarativas a partir de regras explícitas; a subsimbólica se baseia em abordagens estatísticas e produz saídas com determinada probabilidade de erro.

✗ B) Incorreta. Ambas usam modelos; a diferença está em como a informação é representada.

✗ C) Incorreta. Autonomia e heteronomia descrevem o grau de controle externo, não o tipo de representação.

✗ D) Incorreta. Redes neurais são exemplo típico de abordagem subsimbólica (conexionista), não simbólica.

Dica de prova: Simbólica = regras explícitas; subsimbólica = representação implícita e estatística.

02

CAPÍTULO 2 · 10% DA PROVA

Domínio 2: Requisitos do sistema de gestão de IA

Aqui eu preciso localizar cada falha descrita num cenário na seção certa da 42001 (4.1 a 10.2) e saber o que a declaração de aplicabilidade e os Anexos A a D fazem. A prova quase nunca pede o texto da norma: pede 'qual requisito está em foco' ou 'o que falta' num caso concreto. Também caem as definições da seção 3 (risco, controle, eficácia, desempenho, informação documentada, qualidade de dados, alta direção). Onde mais erro: confundir 8.2 (avaliação de riscos) com 8.3 (tratamento) e 8.4 (impacto), e achar que os controles do Anexo A são todos obrigatórios.

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Estrutura da 42001

Seções 1 a 10 na Harmonized Structure (requisitos nas 4 a 10) e Anexos A a D. A ordem dos requisitos não indica importância nem sequência de implementação; os itens das listas são numerados apenas para referência.

4.1 Contexto

Determinar questões externas e internas relevantes e o papel da organização em relação aos sistemas de IA. Nova lei ou regulação não refletida no contexto aponta para 4.1, junto com 4.2.

4.2 Partes interessadas

Determinar as partes interessadas relevantes, seus requisitos e quais deles serão tratados pelo AIMS. Exigência contratual de cliente (por exemplo, explicação das recomendações) ignorada é falha aqui.

4.3 Escopo e 4.4 AIMS

O escopo define limites e aplicabilidade, pode cobrir parte da organização e deve estar disponível como informação documentada; excluir sistema relevante sem justificativa é problema. A 4.4 exige estabelecer, implementar, manter e melhorar o AIMS com seus processos e interações.

5.1 Liderança e 5.2 Política de IA

A alta direção deve integrar os requisitos do AIMS aos processos de negócio e prover recursos. A política deve dar estrutura para definir objetivos de IA e conter compromissos com requisitos aplicáveis e melhoria contínua; deve estar disponível como informação documentada, ser comunicada e estar disponível às partes interessadas quando apropriado.

5.3 Papéis, responsabilidades e autoridades

Quando ninguém sabe quem pode aprovar a colocação de um modelo em produção, a lacuna é 5.3, não comunicação (7.4) nem monitoramento (9.1).

6.1 Riscos e oportunidades e declaração de aplicabilidade

Planejar ações para riscos e oportunidades e avaliar sua eficácia. A declaração de aplicabilidade (statement of applicability) contém os controles necessários e a justificativa de inclusão ou exclusão; todo risco identificado e seu controle devem se refletir nela.

6.2 Objetivos de IA e 6.3 Mudanças

Objetivos coerentes com a política de IA, mensuráveis quando praticável, monitorados e comunicados, com plano de ação, responsável e prazo. Mudanças no AIMS (novo departamento, troca de responsáveis ou do processo de risco) devem ser feitas de forma planejada, considerando propósito e consequências.

7.1 a 7.4 Apoio

7.1 recursos determinados e providos; 7.2 competência: agir para adquiri-la e avaliar a eficácia das ações; 7.3 conscientização: conhecer a política, a contribuição e as consequências de não seguir; 7.4 comunicação: o que, quando, com quem e como comunicar.

7.5 Informação documentada

Pode estar em qualquer formato e meio e abrange o sistema, documentos e registros. Exige identificação, aprovação, controle de versão e impedir uso de versões obsoletas: várias versões circulando por e-mail é 7.5.

8.1 Controle operacional

Controlar os processos operacionais, inclusive os providos externamente (rotulagem ou retreinamento terceirizados). Terceirizar não transfere a responsabilidade nem exige que o fornecedor seja certificado.

8.2, 8.3 e 8.4 Riscos e impacto

8.2 avaliação de riscos de IA a intervalos planejados ou em mudanças significativas; 8.3 tratamento de riscos, incluindo verificar se as ações reduziram o risco e analisar riscos novos; 8.4 avaliação de impacto do sistema de IA, feita antes da operação e revista após mudança grande.

Avaliação de impacto do sistema de IA

Processo formal e documentado que identifica, avalia e trata impactos em indivíduos, grupos de indivíduos e sociedades. Não é teste de precisão, retorno financeiro nem auditoria do certificador.

9.1, 9.2 e 9.3 Avaliação de desempenho

9.1 definir o que medir, métodos e quando e por quem os resultados serão analisados e avaliados; 9.2 auditoria interna com programa, frequência, métodos e auditores objetivos; 9.3 análise crítica pela direção com as entradas exigidas e saídas com decisões sobre melhoria e mudanças.

10.1 e 10.2 Melhoria

10.1 melhorar continuamente a adequação, a suficiência e a eficácia do AIMS. 10.2 reagir à NC (corrigir), avaliar ação para eliminar a causa, verificar se há casos semelhantes e analisar a eficácia da ação corretiva.

Anexos A, B, C e D

Anexo A: objetivos de controle e controles de referência (segundo a PECB, 38 controles e 10 objetivos), usados conforme os riscos, com exclusões justificadas e possibilidade de controles próprios. Anexo B: orientação de implementação, sem exigir justificativa na SoA. Anexo C: objetivos organizacionais e fontes de risco. Anexo D: uso do AIMS em setores e integração com normas setoriais.

Temas de controle do Anexo A

Organização interna (inclui processo para relatar preocupações sobre a IA), recursos, avaliação de impacto, ciclo de vida (objetivos de desenvolvimento responsável, design, testes, validação, implantação e mudanças), dados (aquisição, qualidade, proveniência, preparação), informação para partes interessadas (inclui comunicar incidentes), uso responsável (uso pretendido, limites, evitar dependência excessiva) e relações com terceiros e clientes (alocação de responsabilidades).

Definições da seção 3

Risco = efeito da incerteza, positivo ou negativo. Controle = medida que mantém ou modifica risco e pode não ter o efeito pretendido. Eficácia = atingir o planejado; desempenho = resultado mensurável. Qualidade de dados (fonte 5259-1) = dados atendem aos requisitos da organização para um contexto. Alta direção, com escopo parcial, é quem dirige aquela parte. Auditoria interna pode ser feita por externo em nome da organização.

Macetes para memorizar

Cláusulas 4 a 10

C-L-P-A-O-A-M: Contexto, Liderança, Planejamento, Apoio, Operação, Avaliação, Melhoria.

Riscos na seção 8

8.2 Avalia, 8.3 Trata, 8.4 Impacta (pessoas e sociedade).

Comunicação 7.4

4 perguntas: O quê? Quando? Com quem? Como?

Anexos

A = Arsenal de controles; B = Bula de implementação; C = Causas (fontes de risco) e objetivos; D = Domínios setoriais.

10.2

CCSE: Corrige, Causa, Semelhantes, Eficácia.

Objetivo de IA

Mede, Dono, Prazo, Plano e combina com a política.

Tabela de memorização: não confunda

Quando é...	...e quando é
Correção Arrumar o caso: refazer a avaliação de impacto que faltava, desligar o sistema como contenção.	**Ação corretiva** Mudar a causa: alterar o processo para exigir avaliação de impacto antes de todo novo sistema.
8.2 Avaliação de riscos de IA A avaliação foi feita uma vez e nunca repetida após retreino ou mudança significativa.	**8.3 Tratamento de riscos de IA** As ações foram implantadas, mas ninguém verificou se reduziram o risco nem analisou riscos novos.
Eficácia Grau em que o planejado foi alcançado.	**Desempenho** Resultado mensurável.
Anexo A Lista de objetivos de controle e controles de referência para selecionar e justificar na SoA.	**Anexo B** Orientação de como implementar os controles; não exige justificar seu uso na SoA.
Anexo C Exemplos de objetivos organizacionais e fontes de risco de IA para alimentar a avaliação de riscos.	**Anexo D** Aplicação do AIMS em setores (saúde, finanças, transporte) e integração com normas setoriais.
7.3 Conscientização Pessoas não sabem que a política existe, como contribuem nem as consequências de não seguir.	**7.2 Competência** Pessoas não têm a formação ou experiência necessária para a tarefa (por exemplo, avaliar viés).
5.3 Papéis e autoridades Não se sabe quem pode decidir ou aprovar.	**7.4 Comunicação** Não se definiu o que, quando, com quem e como comunicar.

Números que caem

Item	Valor
Peso do domínio na prova PECB	**10% (8 de 80 questões)**
Controles do Anexo A (segundo a PECB)	**38 controles e 10 objetivos de controle**
Seções com requisitos	**4 a 10**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que os 38 controles do Anexo A são obrigatórios para a certificação.
Como não cair: Usam-se os necessários conforme os riscos, com exclusões justificadas, e podem existir controles próprios.

⚠ **Alerta de prova:** Achar que o Anexo A é informativo e pode ser ignorado.
Como não cair: Ele é a referência para a seleção de controles e não pode ser desconsiderado; exclusões precisam de justificativa na SoA.

⚠ **Alerta de prova:** Deixar riscos 'de menor impacto' fora da declaração de aplicabilidade.
Como não cair: Todos os riscos identificados e seus controles devem se refletir na SoA.

⚠ **Alerta de prova:** Achar que corrigir o caso pendente encerra a não conformidade.
Como não cair: A 10.2 exige ainda avaliar a causa, buscar casos semelhantes e analisar a eficácia.

⚠ **Alerta de prova:** Considerar 'refazer a avaliação que faltava' como ação corretiva.
Como não cair: Isso é correção; ação corretiva muda o processo que deixou a falha acontecer.

⚠ **Alerta de prova:** Achar que risco é sempre negativo ou sinônimo de não conformidade.
Como não cair: Risco é efeito da incerteza, positivo ou negativo; NC é não atendimento de requisito.

⚠ **Alerta de prova:** Acreditar que um controle implementado elimina o risco.
Como não cair: A nota da definição diz que controles podem não ter o efeito pretendido.

⚠ **Alerta de prova:** Achar que terceirizar rotulagem ou retreino tira o processo do AIMS ou exige fornecedor certificado.
Como não cair: Pela 8.1 o processo externo continua sob controle da organização; a norma não exige certificação do fornecedor.

⚠ **Alerta de prova:** Avaliar riscos só no lançamento ou só na recertificação.
Como não cair: A 8.2 pede intervalos planejados e reavaliação em mudanças significativas.

⚠ **Alerta de prova:** Achar que a alta direção é sempre o conselho da holding.
Como não cair: Com escopo parcial, alta direção é quem dirige e controla aquela parte no mais alto nível.

⚠ **Alerta de prova:** Exigir que o escopo do AIMS cubra a organização inteira.
Como não cair: O escopo pode ser parcial, desde que defina limites e aplicabilidade e esteja documentado.

⚠ **Alerta de prova:** Pensar que mudanças no AIMS dependem de autorização prévia do organismo de certificação.
Como não cair: A 6.3 pede mudança planejada; o organismo deve ser informado de mudanças significativas, mas não autoriza antes.

⚠ **Alerta de prova:** Achar que informação documentada é só procedimento escrito ou precisa estar em papel assinado.
Como não cair: Qualquer formato e meio, incluindo registros (evidência de resultados).

⚠ **Alerta de prova:** Colocar objetivos de IA dentro da declaração de aplicabilidade.
Como não cair: A SoA trata de controles; objetivos estão na 6.2, com medida, responsável, prazo e plano.

Como cai na prova

📝 **Como cai:** Cenário descreve uma falha e pergunta 'qual requisito está em foco'.
Como resolver: Pergunte qual é o centro da falha (quem decide, o que mede, que versão, que impacto) e vá à cláusula; descarte cláusulas apenas tangenciais, como liderança em falha operacional.

📝 **Como cai:** Organização fez parte do requisito e pergunta 'o que ainda falta'.
Como resolver: Lembre a lista completa do requisito (10.2: causa, semelhantes, eficácia; 9.1: quem e quando analisa; 7.2: avaliar eficácia da ação de competência) e escolha o pedaço ausente.

📝 **Como cai:** Pergunta se todos os controles do Anexo A ou do Anexo B devem constar ou ser justificados.
Como resolver: Anexo A: selecionar conforme risco e justificar inclusão e exclusão na SoA; Anexo B: só orienta implementação.

📝 **Como cai:** Definição da seção 3 com alternativas parecidas (risco, controle, eficácia, informação documentada).
Como resolver: Procure a palavra das notas: incerteza positiva ou negativa, pode não ter o efeito pretendido, qualquer formato e meio, planejado alcançado.

📝 **Como cai:** Cenário com tema do Anexo A (dados, terceiros, uso responsável, incidentes).
Como resolver: Ligue o problema ao tema de controle que o resolve diretamente e descarte temas laterais como recursos computacionais.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
questões internas e externas, papel frente aos sistemas de IA	**4.1 Contexto**
limites vagos do AIMS, documento não disponível	**4.3 Escopo**
política aprovada, mas as áreas usam IA sem passar pelo AIMS	**5.1 Integração dos requisitos aos processos de negócio**
ninguém sabe quem aprova a colocação em produção	**5.3 Papéis, responsabilidades e autoridades**
objetivo 'melhorar a IA', sem medida, dono nem prazo	**6.2 Objetivos de IA**
várias versões por e-mail, sem saber qual é a vigente	**7.5 Informação documentada**
ninguém conhece a política nem as consequências de não seguir	**7.3 Conscientização**
sistema entrou em operação sem avaliação de impactos em pessoas e sociedade	**8.4 Avaliação de impacto do sistema de IA**
mede a métrica, mas ninguém analisa nem decide o que fazer	**9.1 Monitoramento, medição, análise e avaliação**
gerente do AIMS audita processos que ele mesmo coordena	**9.2 Auditoria interna (objetividade)**
ata da análise crítica sem nenhuma decisão	**9.3 Saídas: decisões sobre melhoria e mudanças**
origem, licença, transformações e qualidade dos dados sem registro	**Controles de dados do Anexo A**
score usado em decisão automática além do previsto	**Uso responsável: uso pretendido e limites (Anexo A)**
funcionária percebeu problema na IA e não tinha onde relatar	**Organização interna: processo para relatar preocupações (Anexo A)**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- A SoA lista os controles necessários com justificativa de inclusão e exclusão; nem todo controle do Anexo A é obrigatório.
- 8.2 avalia, 8.3 trata e checa eficácia, 8.4 avalia impacto em pessoas, grupos e sociedade.
- Correção arruma o caso; ação corretiva elimina a causa.
- Processo terceirizado continua sob controle da organização (8.1).

Essenciais para a prova (checklist)

- ☐ Sei associar cada cenário típico às cláusulas 4.1 a 10.2.
- ☐ Sei o que a declaração de aplicabilidade deve conter.
- ☐ Sei a função de cada Anexo (A, B, C e D).
- ☐ Sei diferenciar correção de ação corretiva e o que a 10.2 exige.
- ☐ Sei quando a avaliação de riscos de IA deve ser repetida.
- ☐ Sei definir avaliação de impacto do sistema de IA.
- ☐ Sei as definições de risco, controle, eficácia, desempenho e informação documentada.
- ☐ Sei listar os temas de controle do Anexo A (dados, uso responsável, terceiros, informação a partes interessadas, organização interna, ciclo de vida).

Questões de revisão do capítulo

R2.1 · Domínio 2: Requisitos do sistema de gestão de IA

O programa de auditoria interna do AIMS da Agência de Crédito Popular prevê auditorias, mas não define frequência, métodos, responsáveis nem como os resultados chegam à direção; as duas auditorias feitas foram conduzidas pelo próprio gerente do AIMS sobre processos que ele coordena. Que requisito está em foco?

A. Seção 6.3, planejamento de mudanças
B. Seção 9.2, auditoria interna
C. Seção 7.4, comunicação
D. Seção 4.2, partes interessadas

R2.2 · Domínio 2: Requisitos do sistema de gestão de IA

Uma rede hospitalar já certificada em um sistema de gestão setorial quer saber onde a ISO/IEC 42001 trata da aplicação do AIMS em setores como saúde, finanças e transporte e da integração com normas setoriais. Qual parte da norma trata disso?

A. Seção 3
B. Anexo D
C. Seção 10
D. Anexo A

R2.3 · Domínio 2: Requisitos do sistema de gestão de IA

A Construtora Base Sólida definiu que fará avaliação de impacto dos sistemas de IA. No estágio 2, o auditor nota que o novo sistema que prioriza obras em áreas de risco entrou em operação sem avaliação e que a avaliação do sistema antigo não foi revista após uma mudança grande no modelo. Qual requisito operacional está em foco?

A. Seção 5.1, liderança e comprometimento da alta direção
B. Seção 8.4, avaliação de impacto do sistema de IA
C. Seção 4.4, sistema de gestão de IA
D. Seção 7.3, conscientização das pessoas

R2.4 · Domínio 2: Requisitos do sistema de gestão de IA

Segundo a ISO/IEC 42001, qual é a diferença entre eficácia (effectiveness) e desempenho (performance)?

A. Eficácia é a opinião da direção; desempenho é a opinião dos clientes
B. Eficácia é o custo do AIMS; desempenho é o número de modelos de IA
C. Eficácia é atingir o planejado; desempenho é resultado mensurável
D. Eficácia é um termo financeiro; desempenho é um termo técnico de TI

Respostas comentadas

R2.1. B) Seção 9.2, auditoria interna

Por quê: A auditoria interna (primeira parte) verifica se o AIMS atende aos requisitos da organização e da norma e se está implementado e mantido de forma eficaz.

✗ A) Incorreta. Planejamento de mudanças não trata do programa de auditoria.
✗ C) Incorreta. Comunicação não é o foco das falhas descritas.
✗ D) Incorreta. Partes interessadas não são o foco.

> **Dica de prova:** Programa interno sem frequência, métodos e objetividade = 9.2.

R2.2. B) Anexo D

Por quê: Segundo a PECB, o Anexo D destaca a aplicabilidade do AIMS em setores como saúde, finanças e transporte e defende a integração com normas genéricas ou setoriais.

✗ A) Incorreta. A seção 3 traz definições.
✗ C) Incorreta. A seção 10 trata de melhoria e não conformidade.
✗ D) Incorreta. O Anexo A traz objetivos de controle e controles.

> **Dica de prova:** Uso por setor e integração com normas setoriais = Anexo D.

R2.3. B) Seção 8.4, avaliação de impacto do sistema de IA

Por quê: O artigo da PECB sobre a 42001 descreve a seção 8 como planejamento e controle operacional, incluindo avaliações de impacto de sistemas de IA e gestão de mudanças.

✗ A) Incorreta. Liderança é relevante, mas a falha descrita é operacional.
✗ C) Incorreta. A 4.4 é o requisito geral de estabelecer e manter o AIMS.
✗ D) Incorreta. Conscientização trata do conhecimento das pessoas sobre política e responsabilidades.

> **Dica de prova:** Avaliação de impacto não feita ou não revista na operação = 8.4.

R2.4. C) Eficácia é atingir o planejado; desempenho é resultado mensurável

Por quê: A nota 3 da definição de desempenho na 42001 diz que o termo abrange resultados obtidos com sistemas de IA e resultados do sistema de gestão de IA.

✗ A) Incorreta. As definições não se baseiam em opiniões.
✗ B) Incorreta. Nenhum dos termos é definido por custo ou quantidade de modelos.
✗ D) Incorreta. As definições não são financeiras nem restritas a TI.

> **Dica de prova:** Eficácia = planejado alcançado; desempenho = resultado mensurável.

03

CAPÍTULO 3 · 20% DA PROVA

Domínio 3: Conceitos e princípios fundamentais de auditoria

Este é um dos domínios mais pesados e mistura definições da ISO 19011 (auditoria, evidência, critérios, constatação, conclusão), os sete princípios de auditoria, os tipos de auditoria e a lógica de imparcialidade da ISO/IEC 17021-1. Na prova, vem quase sempre como dilema de conduta: pressão do cliente, presente, parente, ex-funcionária, auditor que redige procedimento, dados pessoais. Também caem o modelo de risco de auditoria (inerente, controle, detecção), materialidade e garantia razoável. Onde mais erro: confundir auditoria combinada, conjunta e integrada e escolher a resposta 'diplomática' que suaviza a constatação.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Auditoria

Processo sistemático, independente e documentado para obter evidência objetiva e avaliá-la objetivamente frente aos critérios. Autoavaliação da própria área não é auditoria.

Critérios, evidência, constatação e conclusão

Critérios são a régua (norma, política, procedimento, requisito legal). Evidência são registros, declarações de fatos ou outras informações relevantes para os critérios e verificáveis. Constatação é o resultado de avaliar a evidência frente aos critérios e pode indicar conformidade, NC ou boa prática. Conclusão é o resultado após considerar os objetivos e todas as constatações.

Evidência objetiva e requisito

Evidência objetiva são dados que sustentam a existência ou veracidade de algo, obtidos por observação, medição, ensaio ou outros meios. Requisito é necessidade ou expectativa declarada, geralmente implícita ou obrigatória. Conformidade é atender requisito; não conformidade é não atender; com critério legal, usa-se compliance e non-compliance.

Sete princípios de auditoria

Integridade, apresentação justa, devido cuidado profissional, confidencialidade, independência, abordagem baseada em evidência e abordagem baseada em risco. Lucratividade do cliente ou rapidez nunca são princípio.

Apresentação justa

Relatar com veracidade e exatidão, incluindo falhas, obstáculos significativos (acesso negado) e opiniões divergentes não resolvidas. Vale também para auditoria interna: suavizar para agradar o diretor fere o princípio.

Devido cuidado profissional e julgamento

Diligência proporcional à importância da tarefa e à confiança do cliente: processo crítico (crédito, triagem clínica, bolsas de sangue) pede mais tempo e amostra maior. Quando faltar conhecimento técnico, pede-se especialista técnico, mas o julgamento continua do auditor.

Independência, imparcialidade e conflito de interesse

Independência é a base da imparcialidade e da objetividade das conclusões. Ações do auditado, parentesco, presente de valor, ter implantado o processo ou ter prestado consultoria recente (dois anos) são ameaças. Conflito deve ser declarado antes de aceitar a designação ou, se descoberto depois, informado ao líder.

Consultoria (17021-1)

Redigir o procedimento do auditado, propor solução específica ou indicar consultoria é consultoria e compromete a imparcialidade, mesmo de graça. Explicar requisitos de forma genérica e dar treinamento aberto sem soluções específicas não é consultoria.

Confidencialidade

Examinar dados pessoais no ambiente do auditado, no mínimo necessário; não copiar para equipamento pessoal, não enviar por e-mail sem proteção, não colar documento em chatbot público, não comentar em evento. Exigência legal válida pode obrigar a divulgar, informando o cliente quando permitido.

Abordagem baseada em evidência e em risco

Conclusão só com evidência verificável; declaração do auditado é pista a corroborar. Abordagem baseada em risco prioriza o que tem mais impacto nos objetivos (sistemas clínicos com incidente antes do chatbot) e vale também na gestão do programa.

Tipos de auditoria

Primeira parte = interna, mesmo feita por terceiro em nome da organização. Segunda parte = parte interessada, como cliente auditando fornecedor. Terceira parte = certificação e auditorias estatutárias e regulatórias. Combinada = dois ou mais sistemas no mesmo auditado; conjunta = duas ou mais organizações auditoras; integrada = sistema único que atende várias normas.

Cliente da auditoria x auditado

Cliente da auditoria é quem solicita (a rede que contrata a auditoria do fornecedor); auditado é quem é examinado. O organismo contratado conduz e não é nenhum dos dois.

ISO 19011 x ISO/IEC 17021-1

A 19011 dá diretrizes com foco em auditorias de primeira e segunda parte; a 17021-1 rege a certificação e usa a 19011 como apoio. A 19011:2026 (4ª edição) ampliou métodos remotos e o Anexo A, com locais virtuais. Os princípios da 17021-1 (imparcialidade, competência, responsabilidade, abertura, confidencialidade, resposta a reclamações e risco) fundamentam os requisitos, mas não são auditáveis por si.

Modelo de risco de auditoria

Risco inerente = suscetibilidade da área a falhas relevantes antes dos controles; risco de controle = controles do auditado não evitam nem detectam; risco de detecção = procedimentos do auditor não detectam. O auditor só atua no risco de detecção, ampliando amostra e usando testes mais fortes quando inerente e controle são altos.

Materialidade, garantia razoável e risco de amostragem

Materialidade pondera a importância do desvio: falha pontual (registro de treinamento incompleto) pesa menos que falha sistêmica (nenhum modelo validado). A auditoria dá garantia razoável, não absoluta, porque usa amostras com tempo e recursos limitados; toda amostra tem risco de não refletir a população.

Tecnologia e IA na auditoria

Software de auditoria permite seleção objetiva e reprodutível e exame da população inteira, mas exige validar a integridade dos dados e o funcionamento da ferramenta. Alerta de ferramenta é pista, não NC; resumo gerado por IA precisa ser conferido com as anotações.

Anexo A da ISO 19011 (temas de auditoria)

Orienta auditar liderança (decisões, recursos, política, objetivos, análise crítica), contexto (questões e partes interessadas atualizadas), riscos e oportunidades (como a organização determina e trata), cadeia de suprimentos, ciclo de vida, conformidade legal (como a organização identifica e avalia requisitos legais) e desempenho (resultados, não só documentos).

Equipe e conduta pessoal

A equipe pode ter auditores em treinamento e tem um líder designado, responsável final pela condução e pelas conclusões. Diante de auditado hostil: diplomacia e firmeza. A conformidade com a norma é responsabilidade do cliente, não do organismo nem do auditor.

Macetes para memorizar

💡 Sete princípios

I-A-D-C-I-E-R: Integridade, Apresentação justa, Devido cuidado, Confidencialidade, Independência, Evidência, Risco.

💡 Combinada x conjunta x integrada

Combinada = combo de normas; conjunta = junta de auditores; integrada = sistema já integrado.

💡 Risco de auditoria

Inerente é da natureza, controle é do auditado, detecção é do auditor.

💡 Cliente x auditado

Quem solicita a auditoria é o cliente; quem é examinado é o auditado (na auditoria interna, podem coincidir).

💡 Garantia razoável

Amostra + tempo limitado = razoável, nunca absoluta.

💡 Conduta sob pressão

Evidência manda: não sobe, não desce, não some.

💡 Princípios da 17021-1

I-C-R-A-C-R-R: Imparcialidade, Competência, Responsabilidade, Abertura, Confidencialidade, Reclamações, Risco.

Tabela de memorização: não confunda

Quando é...	...e quando é
Auditoria combinada O mesmo organismo audita 42001 e 27001 juntas no mesmo auditado.	**Auditoria conjunta** Duas organizações auditoras auditam juntas o mesmo auditado.
Auditoria integrada O auditado tem um sistema único (política, procedimentos e auditoria interna integrados) que atende várias normas.	**Auditoria combinada** Sistemas de gestão distintos auditados juntos.

Segunda parte Cliente audita fornecedor com base em contrato.	**Terceira parte** Certificação por organismo independente ou auditoria de regulador.
Risco de controle Os controles do auditado (revisões por amostra pequena e sem critério) não pegam a falha.	**Risco de detecção** Os testes do auditor não pegam a falha; é o único que o auditor controla.
Critérios de auditoria Procedimento interno e requisitos da 42001 (a régua).	**Evidência de auditoria** Relatórios de validação dos últimos meses (o que é comparado).
Consultoria Redigir o procedimento, indicar solução específica ou consultoria.	**Informação genérica** Explicar o requisito e práticas comuns de mercado sem documento nem solução para aquele cliente.

Números que caem

Item	Valor
Peso do domínio na prova PECB	**20% (16 de 80 questões)**
Princípios de auditoria cobrados (ISO 19011)	**7**
Consultoria prestada ao cliente que impede designar o auditor	**Nos últimos dois anos**
Edição vigente da ISO 19011	**ISO 19011:2026, 4ª edição, publicada em 27/05/2026 (substitui a 2018)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Rebaixar a NC maior para menor ou para oportunidade de melhoria porque o cliente ameaçou trocar de certificador.
Como não cair: A classificação segue a evidência; pressão comercial se registra e se informa ao organismo.

⚠ **Alerta de prova:** Atender ao pedido de trocar 'não conformidade' por 'ponto de atenção' porque o relatório vai para investidores.
Como não cair: Mantenha o texto fiel à evidência e explique os processos de contestação.

⚠ **Alerta de prova:** Aceitar a declaração do gerente responsável como suficiente.
Como não cair: Testemunho é evidência fraca sozinho: corrobore com registros ou observação.

⚠ **Alerta de prova:** Registrar NC porque declarações verbais 'não têm valor'.
Como não cair: Declaração tem valor como pista; o erro é concluir sem corroborar, em qualquer direção.

⚠ **Alerta de prova:** Manter a auditora que implantou o processo porque ela conhece a empresa.
Como não cair: Auditar o que ajudou a implantar é autoavaliação: substitua.

⚠ **Alerta de prova:** Auditar o processo do parente 'com mais rigor para compensar'.
Como não cair: Rigor extra também é viés; informe o líder para tratar o conflito.

⚠ **Alerta de prova:** Aceitar parte do presente para não ofender o anfitrião.
Como não cair: Recuse ofertas que influenciem ou pareçam influenciar o julgamento.

⚠ **Alerta de prova:** Redigir o procedimento do auditado 'como cortesia' e achar que só seria problema se cobrasse.
Como não cair: É consultoria com ou sem cobrança e compromete a imparcialidade.

⚠ **Alerta de prova:** Achar que qualquer explicação sobre requisitos ou curso sobre a norma é consultoria.
Como não cair: Informação e treinamento genéricos, sem solução específica, não são consultoria.

⚠ **Alerta de prova:** Concluir que o processo é eficaz em toda a empresa com base em um único registro.
Como não cair: Um caso não sustenta conclusão sobre a população; o problema é suficiência da amostra.

⚠ **Alerta de prova:** Achar que o auditor pode reduzir o risco inerente ou o risco de controle.
Como não cair: Ele só atua no risco de detecção (natureza e extensão dos testes).

⚠ **Alerta de prova:** Classificar tudo como NC maior 'por cautela' ou tudo como menor 'para não pesar'.
Como não cair: Materialidade: grade cada constatação pela importância para os resultados.

⚠ **Alerta de prova:** Achar que a certificação garante que o sistema de IA nunca terá incidentes.
Como não cair: Ela dá garantia razoável sobre o sistema de gestão, não ausência de falhas.

⚠ **Alerta de prova:** Ignorar irregularidade fora do escopo ou denunciá-la nas redes sociais.
Como não cair: Integridade: informe o líder e siga os procedimentos do organismo, sem expor nem aconselhar.

Como cai na prova

📝 **Como cai:** Dilema ético: cliente, diretor ou colega pede para omitir, suavizar ou reclassificar uma constatação.
Como resolver: Elimine toda alternativa que muda a constatação sem nova evidência; escolha a que mantém o registro fiel e usa o canal formal (líder, organismo, contestação).

📝 **Como cai:** Pergunta 'qual princípio foi violado' com várias opções plausíveis.
Como resolver: Ache o núcleo do erro: conflito de interesse = independência; vazamento = confidencialidade; concluir sem prova = evidência; relatar torto = apresentação justa; foco errado = risco; falta de diligência = devido cuidado.

📝 **Como cai:** Cenário de designação com relação prévia (parente, ex-funcionária, consultoria, ações).
Como resolver: Qualquer relação que ameace imparcialidade: declarar antes e não designar ou substituir; medidas paliativas (evitar entrevistar o parente, só não auditar a parte afetada) não resolvem.

📝 **Como cai:** Classificar o tipo de auditoria pelo enunciado.
Como resolver: Pergunte quem audita quem (1ª, 2ª ou 3ª parte) e quantos sistemas ou quantas organizações auditoras (combinada, conjunta, integrada).

📝 **Como cai:** Escolher a evidência mais confiável entre quatro fontes.
Como resolver: Prefira evidência direta, obtida pelo auditor e corroborada (extração na presença do auditor) a declarações, slides e afirmações verbais.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
auditor tem ações do fornecedor auditado	**Independência comprometida**
comentou detalhes do cliente em evento ou colou documento em chatbot público	**Confidencialidade**
concluiu 'adequado' só com o relato do gerente	**Abordagem baseada em evidência**
pouco tempo e vários sistemas para escolher	**Abordagem baseada em risco: maior impacto primeiro**
mesmo tempo para sistema crítico e chatbot de perguntas frequentes	**Devido cuidado profissional: redistribuir tempo**
auditor sem conhecimento do setor ou da técnica	**Especialista técnico, julgamento com o auditor**

divergência com o auditado sem acordo	**Apresentação justa: registrar opiniões divergentes**
requisito atendido sem procedimento escrito obrigatório	**Julgamento profissional**
milhões em operações, mudanças frequentes, decisão automática	**Risco inerente alto: testes mais profundos**
regulador audita a concessionária	**Terceira parte (Tabela 1 da 19011)**
cliente audita fornecedor por cláusulas contratuais	**Segunda parte**
dado de critério legal como a LGPD	**Compliance ou non-compliance**
desenvolvimento e operação totalmente on-line, equipes remotas	**Local virtual auditável por métodos remotos**
funcionário desabafa fora da entrevista	**Pista a verificar, não constatação**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Pressão comercial nunca muda a constatação: vale a evidência.
- Combinada = várias normas; conjunta = várias organizações auditoras; integrada = sistema único.
- O auditor só atua no risco de detecção.
- Conflito de interesse se declara antes de aceitar; consultor do cliente nos últimos dois anos não audita esse cliente.

Essenciais para a prova (checklist)

- ☐ Sei listar os sete princípios de auditoria e reconhecer a violação de cada um.
- ☐ Sei definir auditoria, critérios, evidência, evidência objetiva, constatação e conclusão.
- ☐ Sei classificar auditorias de primeira, segunda e terceira parte.
- ☐ Sei diferenciar auditoria combinada, conjunta e integrada.
- ☐ Sei explicar risco inerente, de controle e de detecção.
- ☐ Sei aplicar materialidade e garantia razoável na conclusão.
- ☐ Sei separar consultoria de informação genérica pela 17021-1.
- ☐ Sei os princípios da 17021-1 e que eles não são auditáveis por si.
- ☐ Sei como tratar dados pessoais e ferramentas de IA respeitando a confidencialidade.

Questões de revisão do capítulo

R3.1 · Domínio 3: Conceitos e princípios fundamentais de auditoria

Na Padaria Industrial Trigo de Ouro, com 40 funcionários, a responsável pelo AIMS também cuida da preparação de dados para o modelo de previsão de vendas e foi escalada para auditar esse processo na auditoria interna. Qual é o problema e uma alternativa razoável?

A. Ela deve auditar, mas sem registrar nenhuma constatação sobre o próprio processo
B. Nenhum problema, pois em empresas pequenas o princípio de independência não se aplica à auditoria interna
C. Ela auditaria o próprio trabalho; outra pessoa capacitada ou auditor externo pode auditar
D. O processo de preparação de dados deve sair do programa de auditoria interna

R3.2 · Domínio 3: Conceitos e princípios fundamentais de auditoria

Ao auditar a Hidrelétrica Rio Claro, a auditora compara o procedimento de validação de modelos do auditado e os requisitos da ISO/IEC 42001 com os relatórios de validação dos últimos seis meses. Nessa comparação, o que são os critérios e o que é a evidência?

A. Critérios: o plano de auditoria; evidência: a lista de verificação
B. Critérios: o procedimento e a norma; evidência: os relatórios de validação
C. Critérios: os relatórios de validação; evidência: o procedimento e a norma
D. Critérios e evidência: a opinião do gerente de dados

R3.3 · Domínio 3: Conceitos e princípios fundamentais de auditoria

Para verificar se a Indústria Química Solvex controla o acesso aos dados de treinamento, o auditor tem quatro fontes. Em geral, qual delas oferece a evidência mais confiável?

A. A declaração por escrito do gerente de TI garantindo que o acesso é restrito
B. A lista de permissões extraída do repositório na presença do auditor e conferida
C. A afirmação verbal do analista de dados sobre quem tem acesso aos dados
D. O slide da apresentação de integração que descreve a política de acesso

R3.4 · Domínio 3: Conceitos e princípios fundamentais de auditoria

Segundo a ISO 19011:2026, como se define competência, conceito usado tanto para auditores quanto para o pessoal do AIMS?

A. Certificado emitido por organismo acreditado após prova presencial
B. Número de horas de treinamento concluídas pela pessoa nos últimos três anos de trabalho
C. Capacidade de aplicar conhecimento e habilidades para atingir resultados pretendidos
D. Cargo ocupado na organização e tempo de experiência na mesma função

Respostas comentadas

R3.1. C) Ela auditaria o próprio trabalho; outra pessoa capacitada ou auditor externo pode auditar

Por quê: A 42001 permite que a auditoria interna seja feita por terceiro em nome da organização; a 9.2 exige objetividade e imparcialidade do processo de auditoria.

✗ A) Incorreta. Auditar sem registrar constatações não é auditoria e fere a apresentação justa.

✗ B) Incorreta. Em empresas pequenas a independência total pode ser difícil, mas deve-se evitar auditar o próprio trabalho.

✗ D) Incorreta. Retirar o processo do programa compromete a cobertura da 9.2.

> **Dica de prova:** Pequena empresa: evitar auditar o próprio trabalho (pode usar externo).

R3.2. B) Critérios: o procedimento e a norma; evidência: os relatórios de validação

Por quê: Critérios de auditoria podem incluir requisitos da norma, políticas, procedimentos e requisitos legais; constatações resultam da comparação da evidência com esses critérios.

✗ A) Incorreta. Plano e lista de verificação são ferramentas da auditoria, não critérios nem evidências do auditado.

✗ C) Incorreta. A descrição inverte os conceitos: os relatórios são registros (evidência) e a norma e o procedimento são a referência.

✗ D) Incorreta. Opinião não é critério nem evidência verificável por si só.

> **Dica de prova:** Critério = régua (norma, procedimento); evidência = o que é comparado (registros).

R3.3. B) A lista de permissões extraída do repositório na presença do auditor e conferida

Por quê: Na avaliação de evidências, observação direta, verificação técnica e registros de sistemas, corroborados por outras fontes, costumam ser mais confiáveis que declarações do auditado.

✗ A) Incorreta. Uma declaração escrita do próprio auditado continua sendo testemunho, não verificação.

✗ C) Incorreta. A afirmação verbal é evidência testemunhal e precisa de corroboração.

✗ D) Incorreta. O slide descreve a política, mas não demonstra o controle em operação.

> **Dica de prova:** Evidência direta e corroborada vale mais que declaração do auditado.

R3.4. C) Capacidade de aplicar conhecimento e habilidades para atingir resultados pretendidos

Por quê: A seção 7 da ISO 19011:2026 trata de determinar, avaliar e manter a competência dos auditores; a 7.2 da 42001 trata da competência das pessoas no AIMS.

✗ A) Incorreta. Certificado pode ser evidência, não a definição.

✗ B) Incorreta. Horas de treinamento podem ser evidência, mas não definem competência.

✗ D) Incorreta. Cargo e tempo de casa não garantem competência.

> **Dica de prova:** Competência = aplicar conhecimento e habilidades para atingir resultados.

04

CAPÍTULO 4 · 11,25% DA PROVA

Domínio 4: Preparação de uma auditoria ISO/IEC 42001

Aqui eu preciso dominar o que acontece antes de pisar no auditado: análise do pedido, viabilidade, objetivos, escopo e critérios, termos do trabalho, contato inicial, seleção da equipe e plano de auditoria. A prova cobra muito os papéis (líder, membro, auditor em treinamento, especialista técnico, guia, observador) e o que fazer quando o cliente tenta mexer no escopo, na data ou na equipe. Onde mais erro: confundir escopo com critério e achar que lista de verificação ou plano engessam a auditoria.

Neste capítulo

18 tópicos-chave · 12 pegadinhas · 6 macetes · 12 gatilhos · 4 questões comentadas

Tópicos-chave

Análise do pedido

Antes de definir equipe e plano, o organismo analisa o pedido: escopo, locais, competência necessária e tempo de auditoria. Não existe certificado provisório nem pular o estágio 1.

Objetivos, escopo e critérios

Objetivo é o que a auditoria pretende alcançar (na certificação: determinar a conformidade do AIMS e sua capacidade de atingir resultados). Escopo é extensão e limites: locais físicos e virtuais, funções, unidades, atividades, processos e período. Critérios são a régua: ISO/IEC 42001, informação documentada do AIMS (política de IA, procedimentos) e requisitos legais aplicáveis.

Escopo da auditoria x escopo do AIMS

A auditoria (por exemplo, uma supervisão concentrada numa fábrica) pode cobrir parte do escopo do AIMS, mas nunca ultrapassar o escopo certificado. O auditor não altera o escopo do cliente; inconsistências entre escopo declarado e atividades reais são esclarecidas com cliente e organismo.

Viabilidade

Avaliar se há informação suficiente, cooperação do auditado e tempo e recursos adequados. Sem acesso a pessoas e registros, a auditoria é inviável e se propõe alternativa ao cliente; AIMS sem auditoria interna nem análise crítica indica prontidão em dúvida, a informar ao cliente.

Termos do trabalho e contato inicial

Antes da auditoria ficam acordados objetivos, escopo, critérios, datas e duração, equipe e regras de confidencialidade. No contato inicial confirmam-se canais de comunicação e autoridade, pede-se informação documentada e combina-se a logística; escopo não se negocia informalmente.

Plano de auditoria

Contém objetivos, escopo, critérios, locais, datas, duração, métodos e papéis da equipe. É comunicado ao auditado com objeções resolvidas antes de começar, não é publicado nem aprovado pelo acreditador, e deve ser flexível: imprevistos ajustam o plano mantendo os objetivos, com acordo do auditado.

Líder da equipe

Planeja a auditoria, designa tarefas, conduz, conclui e relata. Não implementa correções, não atua como guia e não decide a certificação (decisão do organismo, por quem não auditou).

Membro da equipe e auditor em treinamento

O membro coleta e avalia evidências nas áreas designadas e registra constatações. O auditor em treinamento faz atividades de auditoria sob supervisão e orientação de um auditor qualificado, nunca sem supervisão.

Especialista técnico

Fornece conhecimento específico (setor, aprendizado de máquina, regulação sanitária, idioma) à equipe, sob orientação de um auditor, sem atuar como auditor nem decidir constatações. É a resposta quando a equipe não tem conhecimento do setor.

Guia e observador

Guia é indicado pelo auditado para apoiar a equipe (marcar entrevistas, dar acesso, esclarecer). Observador (por exemplo, banco financiador) é acordado antes com cliente e organismo não audita, não conduz entrevistas e não interfere.

Seleção da equipe

Considerar competência em IA e no setor, idioma e cultura, independência e tamanho da equipe; distribuir tarefas por competência e independência. O auditado pode apresentar objeção justificada a um auditor; se procedente, trata-se com o organismo e substitui-se.

Tempo de auditoria x duração

Tempo de auditoria inclui planejar e relatar; duração vai da reunião de abertura à de encerramento. Mais locais, mais sistemas de IA, mais complexidade e mais riscos aumentam o tempo; pedido do cliente para terminar cedo não reduz.

Informação documentada para o estágio 1

O mais útil a pedir é escopo do AIMS, política de IA, declaração de aplicabilidade e avaliações de risco e de impacto. A análise prévia serve de mira para o trabalho de campo (por exemplo, exclusão de controles de dados incoerente com a política), não para registrar NC antecipada.

Documentos de trabalho e amostragem

Plano de amostragem com critérios e tamanhos e plano de teste com requisito, método, itens selecionados e registro esperado. Lista de verificação apoia, mas não limita: risco relevante dentro do escopo é investigado. A amostra é escolhida pela equipe, por risco, impacto, mudanças e histórico.

Insumos do planejamento

Reclamações de partes interessadas, novas exigências de reguladores e resultados de auditorias anteriores (incluindo verificar a eficácia das ações sobre NC passadas) orientam o foco. Riscos da própria auditoria (pouco tempo, auditor novo, acesso restrito) entram no plano.

Auditoria remota, acesso e segurança

Avaliar viabilidade técnica, segurança e confidencialidade dos meios remotos e o acesso à evidência; combinar métodos conforme riscos, objetivos e viabilidade. Com dados sensíveis, acordar confidencialidade e regras de acesso e verificar no ambiente do auditado. Visitas a áreas de risco exigem regras de segurança e equipamentos de proteção para os auditores.

Mudanças antes da auditoria

Pedido de adiamento é avaliado com o organismo respeitando a supervisão anual; inclusão de novos objetivos exige reavaliar viabilidade, recursos e plano e acordar com cliente e auditado; pedido para deixar área crítica fora sem mudar o escopo solicitado é levado ao organismo.

Auditoria combinada na preparação

Garantir competência e tempo para cada norma, aproveitando a estrutura comum; não há redução automática do tempo à metade nem auditar só os requisitos comuns.

Macetes para memorizar

Objetivo, escopo, critério

Por quê? Onde? Contra o quê?

Viabilidade

ICT: Informação, Cooperação, Tempo e recursos.

Plano de auditoria

OECLDDMP: Objetivos, Escopo, Critérios, Locais, Datas, Duração, Métodos, Papéis.

Papéis

Guia é da casa; especialista é da equipe; observador só olha; treinando só com tutor.

Documentos de trabalho

Lista de verificação é bússola, não cerca.

Escopo parcial

Auditoria pode ser fatia do AIMS, nunca maior que o bolo certificado.

Tabela de memorização: não confunda

Quando é...	...e quando é
Escopo da auditoria Onde, o quê e quando: locais, unidades, processos e período.	**Critérios da auditoria** Contra o quê se compara: 42001, política de IA, procedimentos, requisitos legais.
Guia Pessoa do auditado que acompanha, marca entrevistas e dá acesso.	**Especialista técnico** Integra a equipe auditora e traz conhecimento técnico, sem atuar como auditor.
Observador Acompanha sem auditar, com presença acordada antes e sem interferir.	**Auditor em treinamento** Integra a equipe e audita sob supervisão de auditor qualificado.
Tempo de auditoria Todo o esforço, inclusive planejamento e relatório.	**Duração da auditoria** Da reunião de abertura à de encerramento.
Objetivo da auditoria O que se pretende alcançar, como determinar a conformidade do AIMS.	**Escopo da auditoria** Extensão e limites em que isso será verificado.

Números que caem

Item	Valor
Peso do domínio na prova PECB	**11,25% (9 de 80 questões)**
Consultoria ao cliente que impede designar o auditor	**Nos últimos dois anos**
Frequência mínima da supervisão a respeitar ao remarcar	**Ao menos uma vez por ano civil**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Aceitar que o cliente deixe o centro de pesquisa com os modelos críticos fora da auditoria sem mudar o escopo solicitado.
Como não cair: A auditoria precisa cobrir o escopo pedido; leve a questão ao organismo.

⚠ **Alerta de prova:** Recusar a objeção do auditado porque 'o cliente não opina sobre a equipe'.
Como não cair: Objeção justificada é avaliada e, se procedente, o auditor é substituído.

⚠ **Alerta de prova:** Manter o auditor que fez consultoria para o cliente porque ela terminou há meses ou porque ele não auditará a política.
Como não cair: Consultoria recente (dois anos) impede a designação para aquele cliente.

⚠ **Alerta de prova:** Deixar o auditado escolher a amostra, os sistemas ou as lojas mais preparadas.
Como não cair: A seleção é da equipe, justificada por risco, impacto e regras do esquema.

⚠ **Alerta de prova:** Tratar a lista de verificação como limite do trabalho de campo.
Como não cair: Documentos de trabalho não restringem a auditoria; risco relevante no escopo é investigado com o líder.

⚠ **Alerta de prova:** Manter o plano em segredo para o auditado 'não se preparar'.
Como não cair: O plano é comunicado ao auditado e as objeções são resolvidas antes.

⚠ **Alerta de prova:** Seguir com a equipe sem conhecimento do setor e registrar a limitação no relatório.
Como não cair: A competência é assegurada na formação da equipe: inclua especialista técnico.

⚠ **Alerta de prova:** Cancelar a supervisão deste ano e somar ao próximo ano civil.
Como não cair: A supervisão anual deve ocorrer no ano civil; avalie data viável com o organismo.

⚠ **Alerta de prova:** Reduzir o tempo à metade numa auditoria combinada.
Como não cair: Reduções devem ser justificadas; garanta competência e tempo para cada norma.

⚠ **Alerta de prova:** Registrar NC maior já na análise documental prévia.
Como não cair: A análise prévia orienta o foco; a constatação depende da verificação em campo.

⚠ **Alerta de prova:** Achar que o objetivo de auditoria não pode mudar depois de definido, ou que pode mudar sem ajustar o plano.
Como não cair: Pode mudar, desde que se reavalie viabilidade, recursos e plano e se acorde com as partes.

⚠ **Alerta de prova:** Pedir ao auditado que traduza registros no dia ou excluir áreas por idioma.
Como não cair: Confirme o idioma na preparação e prepare intérprete ou especialista.

Como cai na prova

📝 **Como cai:** Cliente pede algo na preparação (adiar, tirar área, trocar auditor, incluir objetivo).
Como resolver: Nem aceite cegamente nem recuse de cara: avalie impacto em viabilidade, regras do esquema e plano e trate com o organismo e o auditado.

📝 **Como cai:** Pergunta qual papel tem uma pessoa descrita.
Como resolver: Veja de onde ela vem (auditado ou equipe) e o que faz (apoio logístico, conhecimento, só acompanhar, auditar sob supervisão).

📝 **Como cai:** Quatro definições parecidas de objetivo, escopo, critério e plano.
Como resolver: Critério é referência de comparação; escopo é limite; objetivo é propósito; atividades e datas são plano.

📝 **Como cai:** Lacuna de competência, idioma ou acesso a dados na preparação.
Como resolver: Resolva na formação da equipe e nos acordos prévios (especialista, intérprete, confidencialidade, verificação no ambiente do auditado), nunca reduzindo o escopo.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
equipe experiente em 42001, mas sem conhecimento do setor	**Incluir especialista técnico**
pessoa do auditado marca entrevistas e dá acesso às áreas	**Guia**
representante do banco quer acompanhar	**Observador acordado antes, sem interferir**
milhares de registros de cada tipo no período	**Plano de amostragem com critérios e tamanhos**
25 sistemas e três dias de supervisão	**Priorizar por risco, impacto, mudanças e histórico**
tempo cobrado maior que os dias no local	**Tempo de auditoria inclui planejar e relatar**
recusa de acesso a pessoas e registros	**Auditoria inviável: propor alternativa**
AIMS implantado há dois meses sem auditoria interna nem análise crítica	**Prontidão em dúvida: avaliar e informar o cliente**

reclamações e nova exigência regulatória antes da auditoria	**Usar para orientar o foco**
NC maior fechada na auditoria anterior	**Verificar a eficácia das ações no novo plano**
dados de pacientes que não podem sair da empresa	**Acordar meios de verificar no ambiente do auditado**
área com risco de explosão	**Regras de segurança, acesso e EPI para os auditores**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Critério é a régua; escopo é o limite; objetivo é o propósito.
- Especialista técnico não audita; guia é do auditado; observador não interfere.
- Plano é comunicado ao auditado e é flexível, mantendo os objetivos.
- A amostra é escolhida pela equipe, por risco, nunca pelo auditado.

Essenciais para a prova (checklist)

- ☐ Sei o que se analisa no pedido de certificação antes de planejar.
- ☐ Sei os três fatores de viabilidade e o que fazer quando a auditoria é inviável.
- ☐ Sei distinguir objetivo, escopo e critérios e o que compõe os critérios de uma certificação 42001.
- ☐ Sei o conteúdo do plano de auditoria e que ele é comunicado ao auditado.
- ☐ Sei os papéis de líder, membro, auditor em treinamento, especialista técnico, guia e observador.
- ☐ Sei a diferença entre tempo de auditoria e duração.
- ☐ Sei que documentos pedir antes do estágio 1.
- ☐ Sei como tratar objeção à equipe, conflito por consultoria e mudança de objetivos.

Questões de revisão do capítulo

R4.1 · Domínio 4: Preparação de uma auditoria ISO/IEC 42001

Antes de planejar a auditoria, o organismo recebe o pedido de certificação da Indústria de Tecidos Algodoeira Real. Qual atividade deve ocorrer antes de definir a equipe e o plano?

A. Agendar o estágio 2 diretamente, dispensando o estágio 1 por economia
B. Emitir um certificado provisório enquanto a auditoria não acontece
C. Enviar ao cliente modelos de documentos para que ele os adapte ao AIMS
D. Analisar o pedido, com escopo, locais, competência e tempo de auditoria

R4.2 · Domínio 4: Preparação de uma auditoria ISO/IEC 42001

A auditoria da Startup Visão Médica exigirá acesso a imagens de pacientes e ao código de modelos proprietários. A equipe terá um especialista técnico externo em visão computacional. O que deve ser providenciado antes de qualquer acesso?

A. Publicação dos modelos no site do organismo de certificação
B. Autorização verbal do estagiário que acompanha a equipe
C. Compromissos de confidencialidade e regras de acesso acordados
D. Cópias dos dados enviadas ao e-mail pessoal dos auditores da equipe

R4.3 · Domínio 4: Preparação de uma auditoria ISO/IEC 42001

O líder da equipe que vai auditar a Vidraçaria Cristal está montando o plano de auditoria. Qual conjunto de informações o plano deve conter?

A. Objetivos, escopo, critérios, locais, datas, duração, métodos e papéis da equipe
B. Nome de consultorias recomendadas e modelos de documentos a serem copiados pelo auditado
C. Lista de não conformidades esperadas e as soluções para corrigi-las
D. Valores do contrato, forma de pagamento e multas por atraso do cliente

R4.4 · Domínio 4: Preparação de uma auditoria ISO/IEC 42001

Na preparação da supervisão da Plataforma de Empregos Vaga Certa, o organismo recebeu duas reclamações de candidatos sobre decisões do sistema de triagem e soube de nova exigência de um regulador sobre transparência em processos seletivos automatizados. Como essas informações devem ser usadas?

A. Enviadas ao auditado para que ele escolha se serão auditadas
B. Desconsideradas, pois só documentos do auditado são insumo
C. Usadas para orientar o foco da auditoria nesses temas
D. Publicadas no site do organismo antes da auditoria

Respostas comentadas

R4.1. D) Analisar o pedido, com escopo, locais, competência e tempo de auditoria

Por quê: O handbook cobra planejar e gerenciar o processo de certificação com eficiência; a análise do pedido é a primeira etapa das atividades de pré-certificação.

✗ A) Incorreta. A auditoria inicial tem dois estágios.
✗ B) Incorreta. Não se emite certificado sem auditoria e decisão.
✗ C) Incorreta. Fornecer modelos de documentos específicos seria consultoria.

> **Dica de prova:** Antes de planejar: análise do pedido.

R4.2. C) Compromissos de confidencialidade e regras de acesso acordados

Por quê: Confidencialidade é princípio da auditoria (ISO 19011) e da certificação (ISO/IEC 17021-1); acordos formais protegem o auditado e o organismo.

✗ A) Incorreta. Publicar modelos viola a confidencialidade.
✗ B) Incorreta. Autorização deve vir de quem tem autoridade e de forma acordada.
✗ D) Incorreta. E-mail pessoal expõe dados sensíveis.

> **Dica de prova:** Dados sensíveis: confidencialidade e regras de acesso antes de tudo.

R4.3. A) Objetivos, escopo, critérios, locais, datas, duração, métodos e papéis da equipe

Por quê: ISO 19011:2026: plano de auditoria é a descrição das atividades e arranjos para uma auditoria; deve ser flexível e proporcional ao escopo e à complexidade.

✗ B) Incorreta. Indicar consultorias e modelos de documentos compromete a imparcialidade.
✗ C) Incorreta. O plano não antecipa constatações nem propõe soluções.
✗ D) Incorreta. Condições comerciais pertencem ao contrato, não ao plano de auditoria.

> **Dica de prova:** Plano = objetivos, escopo, critérios, locais, datas, métodos, papéis.

R4.4. C) Usadas para orientar o foco da auditoria nesses temas

Por quê: Supervisões verificam o tratamento de reclamações e mudanças; a preparação usa essas informações para planejar.

✗ A) Incorreta. O auditado não define o que será auditado.
✗ B) Incorreta. Informações de partes interessadas e reclamações são insumos relevantes.
✗ D) Incorreta. Divulgar reclamações viola a confidencialidade.

> **Dica de prova:** Reclamações e novas exigências orientam o foco da auditoria.

05

CAPÍTULO 5 · 23,75% DA PROVA

Domínio 5: Condução de uma auditoria ISO/IEC 42001

É o domínio de maior peso e quase todo em cenário: estágio 1 x estágio 2, reunião de abertura, coleta e verificação de evidência, entrevistas, amostragem e, principalmente, classificar o que se encontrou (NC maior, NC menor, oportunidade de melhoria, boa prática ou nada). A prova adora a situação 'o procedimento existe, mas na prática...' e as desculpas do auditado: 'ninguém reclamou', 'o modelo funciona bem', 'já corrigimos', 'é do fornecedor'. Onde mais erro: aceitar declaração como evidência, chamar de NC algo sem evidência e esquecer que no estágio 1 se fala em área de preocupação.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Estágio 1

Avalia a informação documentada (política, SoA, escopo) e a prontidão para o estágio 2, verifica se auditoria interna e análise crítica foram planejadas e realizadas, obtém informações sobre escopo, processos, locais e requisitos legais e avalia condições do local. As constatações são documentadas e comunicadas por escrito ao cliente como áreas de preocupação, que podem virar NC no estágio 2.

Estágio 2 e intervalo entre estágios

Avalia a implementação e a eficácia do AIMS nos locais e processos do escopo, com base no que o estágio 1 apontou; não repete a análise documental. O intervalo considera o tempo para o cliente tratar as áreas de preocupação, sem prazo fixo de um ano nem dia seguinte por conveniência.

Reunião de abertura

Formal, com a direção do cliente e registro de presença. Confirma o plano, apresenta a equipe, confirma canais de comunicação e informa como as constatações serão classificadas e as condições de encerramento antecipado. Não se dispensa por familiaridade e não se apresentam NC nela.

Comunicação durante a auditoria

O líder informa progresso e preocupações ao auditado e ajusta o plano; reuniões diárias da equipe revisam constatações, ajustam tarefas e acompanham o progresso. Risco imediato e significativo (alerta de segurança desativado) é comunicado sem demora ao auditado e, se apropriado, ao cliente.

Métodos de coleta

Entrevista, análise de informação documentada, observação, amostragem e verificação técnica (por exemplo, reexecutar o teste de validação na frente do auditor e comparar). Com grandes populações eletrônicas, análise de dados para achar padrões e exceções e aprofundar nelas.

Entrevistas

Explicar o propósito, usar perguntas abertas e neutras (como, o que, quando), escutar ativamente e pedir um caso concreto com registro. Evitar perguntas indutoras ('não é?') ou que presumem culpa. Entrevistar quem executa a tarefa corrobora o gestor; individual reduz influência mútua, em grupo mostra a interação.

Corroboração e evidência suficiente e apropriada

Evidência boa é verificável, relevante ao critério e corroborada por fontes independentes. Quando entrevista e registro conflitam, aprofunda-se e segue-se a evidência objetiva. Relatório de ferramenta automática ou captura de tela suspeita exige avaliar confiabilidade e, se possível, verificação ao vivo.

Amostragem

Por julgamento usa a experiência do auditor; estatística usa seleção aleatória e inferência. Em populações grandes, amostra representativa e orientada a risco, rastreada até registros, escolhida pelo auditor. Amostra 100% conforme também é registrada com referência à evidência.

Benefício da dúvida

Sem evidência suficiente (relato isolado não corroborado, testes amostrados sem o problema), não se registra NC; pode-se anotar e aprofundar. Com evidência objetiva do não atendimento, o benefício da dúvida não se aplica.

NC maior, NC menor, oportunidade e boa prática

NC maior afeta a capacidade do sistema de atingir resultados ou indica falha sistêmica (processo central inexistente, como nenhuma avaliação de riscos de IA); várias NC no mesmo requisito podem configurar NC maior. NC menor é falha isolada com processo funcionando. Oportunidade de melhoria é requisito atendido com espaço para melhorar, sem prescrever solução. Boa prática exemplar é registrada com base em evidência.

Controle definido pela própria organização

Quando o AIMS define um controle (logs retidos, revisão trimestral, informar clientes, aviso de que é IA, aprovação de risco residual), ele vira critério de auditoria; não cumpri-lo é NC, não oportunidade. Procedimento aprovado não prova execução.

Redação da não conformidade

Requisito + evidência rastreável (o quê, onde, quando, quem) + declaração do não atendimento, sem generalizar, sem adjetivos e sem recomendar solução ou consultoria.

Correção durante a auditoria e causa

Se o auditado corrige na hora, registra-se a constatação e anota-se a correção. Analisar a causa e definir ações cabe à organização; o auditor avalia depois. Auditado que discorda: mostrar evidência e critério e aceitar só nova evidência verificável.

Situações de campo

Acesso negado a área do plano: registrar a recusa, avaliar o efeito nos objetivos e informar o cliente. Observador ou guia respondendo pelos entrevistados: o líder intervém. Intérprete deve ser imparcial. Entrevista remota: confirmar identidade, confidencialidade e conexão. Achado fora do escopo: comunicar ao líder, sem NC do AIMS.

Mudanças de escopo e plano em campo

Sistema relevante não previsto, processo no escopo do AIMS fora do escopo da auditoria ou atraso de agenda: o líder comunica, repriorizando pelo risco, e acorda as mudanças com cliente e auditado. Nunca declarar conforme o que não foi auditado.

Papéis de trabalho e preparação do encerramento

Papéis de trabalho registram evidências, amostras, fontes e constatações, inclusive de conformidade ('tudo ok' não serve). Antes do encerramento a equipe revisa e consolida as constatações, acorda conclusões e prepara a recomendação.

Temas de IA típicos de NC

Exclusão de controle na SoA sem justificativa; revisão humana feita em lote sem abrir os casos; uso fora do uso pretendido; dados sem proveniência ou licença verificada; fornecedor de dados ou rotulagem sem avaliação; mudança significativa sem nova avaliação de riscos; critérios de risco ausentes; avaliação de impacto sem grupos vulneráveis ou sem efeitos sociais; documentação técnica de versão antiga; dados de validação e teste não separados; retirada de modelo sem seguir o ciclo de vida.

Eficácia da ação corretiva

Procedimento atualizado e treinamento dado não demonstram eficácia; é preciso evidência de resultado após a mudança (registros de revisão posteriores, monitoramento).

Macetes para memorizar

Estágios

Estágio 1 lê e prepara (papel e prontidão); estágio 2 vê e testa (prática e eficácia).

Classificação

Sistema caiu = maior; ponto isolado = menor; dá para melhorar = OM; exemplar = boa prática.

Redação da NC

REQ + EVI + DEC: requisito, evidência rastreável, declaração do não atendimento.

Evidência rastreável

O quê, onde, quando e quem.

Desculpas do auditado

Ninguém reclamou, funciona bem, já corrigi, é do fornecedor: nenhuma apaga a NC.

Entrevista

Abre, escuta, pede caso e registro; nunca 'não é?'.

Métodos de coleta

E-D-O-A-V: Entrevista, Documentos, Observação, Amostragem, Verificação técnica.

Tabela de memorização: não confunda

Quando é...	...e quando é
Estágio 1 Documentação, prontidão, condições do local e planejamento; gera áreas de preocupação por escrito.	**Estágio 2** Implementação e eficácia em campo; gera NC classificadas.
NC maior Processo central inexistente ou falha sistêmica que afeta a capacidade de atingir resultados.	**NC menor** Falha isolada (um registro de competência faltando) com o processo funcionando.

Oportunidade de melhoria Requisito atendido, mas há como melhorar (alertas em tempo real).	**Não conformidade** Requisito ou controle definido pela organização não cumprido.
Amostragem por julgamento Seleção pela experiência do auditor, focando risco.	**Amostragem estatística** Seleção aleatória com inferência probabilística.
Entrevista individual Reduz influência mútua e opiniões dominantes.	**Entrevista em grupo** Mostra como as pessoas interagem no processo.
Benefício da dúvida Relato isolado sem corroboração: não registrar NC, anotar e aprofundar.	**Evidência objetiva** Registro mostra o não atendimento: registra-se, mesmo que 'nunca deu problema'.

Números que caem

Item	Valor
Peso do domínio na prova PECB	**23,75% (19 de 80 questões), o maior da prova**
Estágios da auditoria inicial de certificação	**2 (estágio 1 e estágio 2)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Aceitar 'ninguém relatou problema' ou 'o modelo funciona bem' como prova de conformidade.
Como não cair: Ausência de incidentes e bom desempenho não demonstram que o controle definido é executado.

⚠ **Alerta de prova:** Registrar como oportunidade de melhoria um controle que a própria organização definiu e não cumpre.
Como não cair: Controle definido no AIMS é critério; não cumprir é NC.

⚠ **Alerta de prova:** Considerar fora do escopo porque a migração, o modelo ou os dados vieram de fornecedor.
Como não cair: Processos providos externamente continuam sob controle e responsabilidade da organização.

⚠ **Alerta de prova:** Retirar a constatação porque o auditado corrigiu em uma hora.
Como não cair: Registre a constatação e anote a correção; o fato já ocorreu.

⚠ **Alerta de prova:** Registrar NC 'por precaução' com base no relato de um motorista ou vendedor.
Como não cair: Sem corroboração não há NC; aplique o benefício da dúvida e aprofunde se houver meios.

⚠ **Alerta de prova:** Registrar NC maior no estágio 1 e suspender o estágio 2.
Como não cair: No estágio 1 há áreas de preocupação, comunicadas por escrito; a classificação formal vem no estágio 2.

⚠ **Alerta de prova:** Comentar os pontos do estágio 1 só verbalmente com o gerente.
Como não cair: Constatações do estágio 1 são documentadas e comunicadas ao cliente.

⚠ **Alerta de prova:** Aceitar a exclusão de controle na SoA porque a organização é livre para excluir.
Como não cair: Pode excluir, mas com justificativa coerente com os riscos; sem justificativa é NC.

⚠ **Alerta de prova:** Achar que um registro de aprovação para cada recusa prova a revisão humana.
Como não cair: Se a observação mostra aprovação em lote sem abrir casos, a revisão não ocorre: NC.

⚠ **Alerta de prova:** Considerar 98% de aderência suficiente e ignorar as exceções.
Como não cair: Exceções sem justificativa podem revelar falha de controle: investigue antes de concluir.

⚠ **Alerta de prova:** Indicar a causa e a solução ao gerente para acelerar o fechamento.
Como não cair: Causa e ação são do auditado; o auditor avalia depois. Indicar é consultoria.

⚠ **Alerta de prova:** Descartar as falhas repetidas no mesmo requisito e registrar uma só NC menor.
Como não cair: Avalie o conjunto: várias falhas no mesmo requisito podem indicar falha sistêmica e NC maior.

⚠ **Alerta de prova:** Entrar na sala restrita com ajuda de outro funcionário ou declarar a área conforme.
Como não cair: Registre a recusa, avalie o efeito nos objetivos e informe o cliente.

⚠ **Alerta de prova:** Aceitar o gerente do auditado como intérprete por conhecer o processo.
Como não cair: Use intérprete imparcial, sem vínculo com a área auditada.

Como cai na prova

📝 **Como cai:** 'O procedimento exige X; o auditor verifica que na prática Y. Qual é a constatação?'
Como resolver: Se o controle está definido no AIMS e não ocorre, é NC; descarte 'fora do escopo', 'oportunidade' e 'conformidade' que se apoiam em desempenho, ausência de reclamações ou terceirização.

📝 **Como cai:** Classificar a gravidade da constatação.
Como resolver: Pergunte se a falha é isolada com processo funcionando (menor) ou se o processo central não existe ou falha em série (maior); sem requisito descumprido, é OM.

📝 **Como cai:** Escolher a evidência ou o método mais adequado para testar um controle.
Como resolver: Prefira amostra de registros reais rastreada até o controle, observação ou reexecução; declaração, procedimento aprovado e fluxograma provam desenho, não execução.

📝 **Como cai:** Situação delicada em campo (acesso negado, observador interferindo, risco imediato, atraso).
Como resolver: Líder comunica e ajusta com o auditado e o cliente; nunca declara conforme o que não viu, nunca age por conta própria nem intervém na operação.

📝 **Como cai:** Pergunta sobre estágio 1 (propósito, saída, o que fazer com falhas encontradas).
Como resolver: Documentos e prontidão; saída por escrito com áreas de preocupação; elas influenciam o plano e o intervalo até o estágio 2.

📝 **Como cai:** Pergunta qual cláusula usar como critério para uma falha observada em campo.
Como resolver: Mapeie o centro da falha à cláusula (5.2 política comunicada, 6.2 objetivos, 7.5 versões, 9.1 métodos de monitoramento, 9.3 entradas) e descarte as tangenciais.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
nenhum sistema teve riscos identificados e não há critérios de risco	**NC maior: falha sistêmica**
um analista recém-contratado sem evidência de competência, demais completos	**NC menor (7.2)**
requisito atendido e ideia que reduziria perdas	**Oportunidade de melhoria sem prescrever solução**
registro alterado à mão, sem identificar quem, quando e por quê	**Integridade dos registros e controle de alterações (7.5)**
versão em uso sem identificação nem aprovação	**7.5 Controle de informação documentada**

objetivo sem indicador, meta e responsável	**6.2 Objetivos de IA**
ata da análise crítica sem auditorias, desempenho, mudanças externas e reclamações	**NC com 9.3 (entradas)**
nova lei não refletida na análise de contexto	**4.1 e 4.2**
trocou a arquitetura do modelo e a avaliação de riscos é anterior	**NC: mudança significativa sem reavaliar riscos**
duas avaliações do mesmo modelo com conclusões opostas	**Falta de critérios de risco**
pergunta 'o senhor sempre confere, não é?'	**Pergunta indutora**
pede que o analista rode de novo o teste e compara com o registrado	**Verificação técnica por reexecução**
18 mil eventos de acesso e meio dia	**Análise de dados para padrões e exceções**
achado grave em processo fora do escopo	**Comunicar ao líder, sem NC do AIMS**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Controle definido pela própria organização e não executado é NC, não oportunidade.
- No estágio 1 há áreas de preocupação por escrito; NC classificada é do estágio 2.
- Sem evidência não há NC; com evidência objetiva não há benefício da dúvida.
- Correção feita durante a auditoria não apaga a constatação.
- Causa e solução são do auditado; o auditor não prescreve.

Essenciais para a prova (checklist)

☐ Sei o propósito e a saída do estágio 1 e do estágio 2.

☐ Sei o que se faz e o que se informa na reunião de abertura.

☐ Sei os métodos de coleta de evidência e quando usar cada um.

☐ Sei formular perguntas abertas e reconhecer perguntas indutoras.

☐ Sei diferenciar amostragem por julgamento e estatística.

☐ Sei classificar NC maior, NC menor, oportunidade de melhoria e boa prática.

☐ Sei redigir uma NC com requisito, evidência e declaração.

☐ Sei aplicar o benefício da dúvida só quando falta evidência.

☐ Sei agir diante de acesso negado, risco imediato, achado fora do escopo e interferência de guia ou observador.

Questões de revisão do capítulo

R5.1 · Domínio 5: Condução de uma auditoria ISO/IEC 42001

Na auditoria de estágio 2 da Fábrica Ventura, que usa um modelo de manutenção preditiva, o auditor amostrou 25 pessoas da equipe de dados. A organização definiu a competência exigida e mantém registros, mas não encontrou a evidência de competência de um analista contratado há duas semanas; os demais registros estão completos. Como essa constatação tende a ser classificada?

A. Conformidade plena, sem registro
B. Não conformidade maior
C. Suspensão imediata do AIMS
D. Não conformidade menor

R5.2 · Domínio 5: Condução de uma auditoria ISO/IEC 42001

A Financeira Lar Seguro usa IA para definir limites de crédito. A avaliação de impacto cobre efeitos financeiros para a empresa, mas não considera clientes idosos com baixa familiaridade digital nem pessoas com renda informal, grupos para os quais as recusas cresceram. O que o auditor deve verificar?

A. Se as recusas de crédito seguem a política comercial vigente da financeira
B. Se a avaliação de impacto calcula o retorno financeiro do sistema para a empresa
C. Se o processo de avaliação de impacto considera indivíduos e grupos afetados, como os mais vulneráveis
D. Se o sistema foi desenvolvido por fornecedor certificado na ISO/IEC 27001

R5.3 · Domínio 5: Condução de uma auditoria ISO/IEC 42001

Na Indústria Química Fórmula Segura, a auditora verifica quem pode alterar os modelos em produção. Dez pessoas têm acesso de administrador, incluindo três ex-funcionários e dois estagiários, embora o procedimento limite esse acesso a dois engenheiros. Como avaliar?

A. Não conformidade: o controle de acesso definido não é aplicado na prática
B. Fora do escopo, pois controle de acesso é tema da ISO/IEC 27001
C. Conformidade, pois ninguém relatou alterações indevidas nos modelos
D. Oportunidade de melhoria, pois o número de administradores é questão de estilo

R5.4 · Domínio 5: Condução de uma auditoria ISO/IEC 42001

A Indústria de Autopeças Freio Firme apresenta ao auditor um relatório gerado automaticamente por uma ferramenta de IA que 'confirma 100% de conformidade' dos controles de dados. Não há informação sobre como a ferramenta foi configurada, quais dados usou nem quem revisou o resultado. Como o auditor deve tratar esse relatório?

A. Avaliar a confiabilidade da ferramenta e corroborar com outras evidências
B. Copiar o relatório para o relatório de auditoria como constatação final
C. Aceitar como evidência conclusiva, pois foi gerado por ferramenta automática
D. Rejeitar qualquer evidência produzida com o apoio de ferramentas de IA

Respostas comentadas

R5.1. D) Não conformidade menor

Por quê: Pela ISO/IEC 17021-1, NC maior afeta a capacidade do sistema de gestão de atingir os resultados pretendidos (ou há dúvida significativa sobre o controle eficaz do processo); NC menor não afeta essa capacidade.

✗ A) Incorreta. Houve não atendimento de requisito (reter evidência de competência), então a constatação deve ser registrada.
✗ B) Incorreta. NC maior é a que afeta a capacidade do sistema de atingir os resultados pretendidos ou indica falha sistêmica, o que a evidência não mostra.
✗ C) Incorreta. Suspensão é decisão do organismo de certificação sobre um cliente já certificado, não uma classificação de constatação.

> **Dica de prova:** Falha isolada com processo funcionando = NC menor.

R5.2. C) Se o processo de avaliação de impacto considera indivíduos e grupos afetados, como os mais vulneráveis

Por quê: A ISO/IEC 42005:2025 orienta avaliações de impacto que vão além do risco de negócio, considerando efeitos em pessoas e grupos, inclusive usos sensíveis e restritos.

✗ A) Incorreta. Seguir a política comercial não demonstra que os impactos em grupos afetados foram avaliados.
✗ B) Incorreta. Retorno financeiro é importante para o negócio, mas a avaliação de impacto foca efeitos em indivíduos, grupos e sociedade.
✗ D) Incorreta. A certificação do fornecedor em segurança da informação não responde à falta de análise de impacto em grupos.

> **Dica de prova:** Avaliação de impacto = efeitos em indivíduos, grupos e sociedade, não só no negócio.

R5.3. A) Não conformidade: o controle de acesso definido não é aplicado na prática

Por quê: A introdução da 42001 cita segurança entre as preocupações de confiabilidade de IA; controles definidos pela organização são critérios de auditoria.

✗ B) Incorreta. Proteger modelos e dados de IA é parte do AIMS, mesmo havendo sobreposição com a 27001.

✗ C) Incorreta. Ausência de incidentes não demonstra que o controle funciona.

✗ D) Incorreta. O controle foi definido pela organização e é critério de auditoria.

> **Dica de prova:** Acesso real maior que o definido = NC.

R5.4. A) Avaliar a confiabilidade da ferramenta e corroborar com outras evidências

Por quê: O Anexo A da ISO 19011:2026 trata de verificar informações e selecionar fontes; a evidência precisa ser verificável e relevante para os critérios.

✗ B) Incorreta. O auditor forma suas constatações com base em evidência verificada, não copia conclusões do auditado.

✗ C) Incorreta. Ferramenta automática não garante confiabilidade; é preciso entender origem e método.

✗ D) Incorreta. Evidências geradas com IA podem ser usadas, desde que verificáveis.

> **Dica de prova:** Relatório automático do auditado: avaliar a fonte e corroborar.

06

CAPÍTULO 6 · 8,75% DA PROVA

Domínio 6: Encerramento de uma auditoria ISO/IEC 42001

Aqui eu preciso saber o que acontece depois do trabalho de campo: consolidação, reunião de encerramento, relatório, tratamento das NC pelo cliente e decisão de certificação. A prova cobra o que a ISO/IEC 17021-1 exige na reunião de encerramento e no relatório, quem decide a certificação e a diferença de tratamento entre NC maior e NC menor. Também aparece muito o cliente pedindo para tirar a NC, editar o relatório ou receber o certificado na hora. Onde mais erro: achar que o auditor-líder concede a certificação e que NC menor dispensa resposta.

Neste capítulo
16 tópicos-chave · 12 pegadinhas · 5 macetes · 12 gatilhos · 4 questões comentadas

Tópicos-chave

Reunião pré-encerramento da equipe

Antes do encerramento a equipe analisa as constatações frente aos objetivos e critérios, completa papéis de trabalho rastreáveis e acorda conclusões e recomendação. Se dois auditores divergem, o líder decide com base na evidência e nos critérios e registra a justificativa.

Reunião de encerramento

Formal, com a direção do cliente e responsáveis pelas funções auditadas, e registro de presença; ocorre em toda auditoria, haja ou não NC. Não é substituída por mensagem e não tem a presença do acreditador.

O que se informa no encerramento

Que a evidência foi obtida por amostragem e há incerteza; o método e o prazo de relato; o tratamento das NC e suas consequências para a certificação; as atividades pós-auditoria; e a existência dos processos de reclamação e apelação. Não se garante o certificado.

Divergência no encerramento

Se o auditado discorda e não há acordo, a divergência não resolvida é registrada e encaminhada ao organismo. Não se retira a constatação nem se adia o encerramento até o cliente concordar; promessa de corrigir em uma semana não tira a NC.

Conteúdo do relatório (17021-1)

Identificação do organismo, do cliente, do tipo de auditoria, critérios, objetivos e escopo; líder e membros da equipe, datas e locais; constatações com referência à evidência e às NC; desvios do plano e suas razões; recomendação da equipe; avaliação do uso de documentos e marcas de certificação; declaração de que a auditoria se baseia em amostragem.

Declaração de amostragem

Indica que podem existir não conformidades não detectadas; não significa auditoria incompleta. Por isso não se escreve que 'todo o sistema foi verificado' e ausência de NC numa área não significa perfeição.

Redação de constatações e conclusões

Claras, objetivas e apoiadas em evidência, sem 'parece frágil', sem adjetivos fortes e sem recomendar soluções específicas nem indicar consultorias. A conclusão expressa o grau de conformidade e a capacidade de atingir os resultados pretendidos. Boas práticas e oportunidades podem constar.

Propriedade e confidencialidade do relatório

O relatório é do organismo; o cliente não edita. Terceiros (banco financiador) só recebem com consentimento do cliente.

Registros da auditoria

Retidos pelo tempo definido pelo organismo, com proteção de integridade, disponibilidade e confidencialidade e acesso controlado; não se apagam logo após o encerramento nem ficam em pasta aberta.

Resposta do cliente às NC

No prazo definido, o cliente apresenta análise de causa e descrição da correção e da ação corretiva. Plano só com correção ('ajustar manualmente os casos'), com causa 'erro humano' e 'conscientizar', ou sem prazos e responsáveis é questionado.

NC menor x NC maior na decisão

NC menor: o organismo analisa e aceita o plano do cliente (verificação da eficácia depois, normalmente na supervisão). NC maior: o organismo verifica a correção e a ação corretiva antes da decisão, por análise de documentos ou nova visita, conforme o caso.

Decisão de certificação

Tomada pelo organismo de certificação por pessoas que não realizaram a auditoria, após análise independente do relatório e da recomendação para garantir informação suficiente e imparcialidade. A equipe recomenda; não há certificado automático nem emitido pelo líder ou pelo acreditador.

Apelação

Se o cliente discorda da decisão de não conceder a certificação, usa o processo de apelação do organismo. A ISO e o organismo de acreditação não revisam a decisão.

Encerramento antecipado

Se os objetivos não podem ser atingidos (por exemplo, sistemas indisponíveis por incidente), o líder comunica as razões ao cliente e ao auditado e acorda a ação, como reprogramar ou encerrar.

Acompanhamento e eficácia

A eficácia da ação corretiva se prova com resultado medido após a mudança (monitoramento mostrando recomendações equilibradas), não com ata, contrato ou declaração. O relatório de supervisão registra o resultado da verificação de cada NC anterior.

Auditoria interna (42001)

Na auditoria interna do AIMS, os resultados são relatados à gerência pertinente, não ao organismo de certificação nem ao regulador.

Macetes para memorizar

💡 NC menor x maior

Menor: aceito o PLANO. Maior: verifico a AÇÃO.

💡 Quem decide

Quem audita recomenda; quem não auditou decide.

💡 Encerramento

A-M-T-P-R: Amostragem, Método e prazo de relato, Tratamento das NC, Pós-auditoria, Reclamações e apelações.

💡 Resposta à NC

Causa + Correção + Ação corretiva, dentro do prazo.

💡 Relatório

Relatório é do organismo: cliente lê, não edita; terceiro só com o sim do cliente.

Tabela de memorização: não confunda

Quando é...	...e quando é

NC menor Organismo analisa e aceita o plano de correção e ação corretiva antes da decisão.	**NC maior** Organismo verifica a implementação (documentos ou nova visita) antes da decisão.
Correção Ajustar os casos afetados, suspender o modelo como contenção.	**Ação corretiva** Atacar a origem: alterar o processo de validação ou de dados.
Recomendação da equipe Apresentada pelo líder no encerramento e no relatório.	**Decisão de certificação** Tomada pelo organismo, por pessoas que não auditaram.
Apelação Cliente contesta a decisão de certificação do organismo.	**Divergência registrada no encerramento** Auditado discorda de uma constatação durante a reunião de encerramento.
Reunião pré-encerramento Só a equipe, consolida constatações e acorda conclusões.	**Reunião de encerramento** Com a direção do cliente, formal, com presença registrada.

Números que caem

Item	Valor
Peso do domínio na prova PECB	**8,75% (7 de 80 questões)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que o líder pode aprovar a certificação porque conhece bem o caso, ou com a assinatura de outro auditor da equipe.
Como não cair: Quem auditou não decide; a decisão é do organismo por pessoas que não participaram.

⚠ **Alerta de prova:** Achar que NC menor não exige resposta formal.
Como não cair: O cliente apresenta plano com causa, correção e ação corretiva, que o organismo analisa e aceita.

⚠ **Alerta de prova:** Aceitar só o plano de ação para uma NC maior.
Como não cair: NC maior exige verificar correção e ação corretiva antes de decidir.

⚠ **Alerta de prova:** Exigir verificação no local das NC menores antes de qualquer decisão.
Como não cair: Isso é o tratamento de NC maior; para NC menor basta aceitar o plano.

⚠ **Alerta de prova:** Aceitar 'erro humano' como causa e 'conscientizar a equipe' como ação.
Como não cair: Erro humano costuma ser sintoma: questione por que o processo permitiu a falha.

⚠ **Alerta de prova:** Considerar adequado um plano que só ajusta os casos afetados.
Como não cair: Isso é correção; falta análise de causa e ação sobre a origem.

⚠ **Alerta de prova:** Considerar inadequado suspender o modelo como contenção.
Como não cair: Não há proibição; plano com correção imediata mais ação corretiva sobre a causa é adequado.

⚠ **Alerta de prova:** Retirar a NC porque o diretor prometeu resolver em uma semana.
Como não cair: Apresente a NC como registrada e informe o processo e o prazo de resposta.

⚠ **Alerta de prova:** Enviar o relatório ao banco financiador por interesse legítimo.
Como não cair: Só com consentimento do cliente.

⚠ **Alerta de prova:** Permitir que o cliente edite termos do relatório antes de enviar aos bancos.
Como não cair: O relatório é do organismo e não é alterado pelo cliente.

⚠ **Alerta de prova:** Omitir a mina não visitada ou declará-la conforme com base na outra.
Como não cair: Registre o desvio do plano, as razões e o efeito nas conclusões.

⚠ **Alerta de prova:** Pedir à ISO ou ao acreditador para revisar a decisão de certificação.
Como não cair: Discordância da decisão vai para a apelação no organismo de certificação.

Como cai na prova

📝 **Como cai:** Cliente pede algo no encerramento (tirar NC, certificado na hora, editar relatório, garantir aprovação).
Como resolver: Mantenha a constatação, explique o processo formal (prazo de resposta, decisão do organismo, apelação) e descarte qualquer concessão que altere o relatório.

📝 **Como cai:** O que o organismo faz com NC antes de decidir.
Como resolver: Identifique a gravidade: menor = analisar e aceitar plano; maior = verificar implementação, por documentos ou visita, antes da decisão.

📝 **Como cai:** Avaliar um plano de ação apresentado pelo cliente.
Como resolver: Cheque se há análise de causa real, correção e ação corretiva, prazos e responsáveis; o organismo pede complementos, não prescreve solução nem exige demissão.

📝 **Como cai:** O que deve constar no relatório ou na reunião segundo a 17021-1.
Como resolver: Lembre a lista: identificação, equipe, datas, locais, constatações com evidência, desvios, recomendação, uso de marcas, declaração de amostragem; descarte notas, rankings, orçamento de melhorias, nomes para punição e indicação de consultorias.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
diretor pede o certificado no mesmo dia	**Equipe recomenda; organismo decide por quem não auditou**
duas NC menores e decisão pendente	**Analisar e aceitar o plano do cliente**
NC maior e cliente diz que resolveu	**Verificar correção e ação corretiva (documentos ou visita)**
pessoa que não participou analisa relatório e recomendação	**Revisão independente para decisão imparcial**
diretor discorda da constatação e não há acordo	**Registrar a divergência e encaminhar ao organismo**
cliente discorda da decisão de não certificar	**Apelação junto ao organismo de certificação**
cliente quer texto dizendo que 'todo o sistema foi verificado'	**Declaração de amostragem: podem existir NC não detectadas**
'a gestão de dados parece frágil' no relatório	**Redação clara, objetiva e com evidência**
plano de ação sem datas e sem responsáveis	**Pedir prazos definidos e ações específicas**
sistemas indisponíveis e objetivos inatingíveis	**Comunicar razões e acordar reprogramar ou encerrar**
papéis de trabalho sem local da evidência e anotações sem data	**Completar e revisar para ficarem rastreáveis**
resultado da auditoria interna, a quem relatar	**Gerência pertinente**

🎯 Se você lembrar de só uma coisa deste capítulo...

- A decisão de certificação é do organismo, por pessoas que não auditaram.
- NC menor: aceitar o plano; NC maior: verificar a ação antes de decidir.
- O relatório é do organismo; terceiros só com consentimento do cliente.
- Sem NC não quer dizer perfeito: a auditoria é por amostragem.

Essenciais para a prova (checklist)

- ☐ Sei o que a equipe faz antes da reunião de encerramento.
- ☐ Sei quem participa e o que se informa na reunião de encerramento.
- ☐ Sei o conteúdo do relatório exigido pela 17021-1.
- ☐ Sei tratar divergência não resolvida e pedidos do cliente para alterar o relatório.
- ☐ Sei a diferença de tratamento entre NC menor e NC maior antes da decisão.
- ☐ Sei avaliar se um plano de ação tem causa, correção e ação corretiva.
- ☐ Sei quem decide a certificação e como funciona a apelação.
- ☐ Sei como guardar e proteger os registros da auditoria.

Questões de revisão do capítulo

R6.1 · Domínio 6: Encerramento de uma auditoria ISO/IEC 42001

O relatório da auditoria da Mineração Pedra Verde precisa registrar que o plano previa visitar duas minas, mas uma delas foi fechada por chuvas e não foi visitada. O cliente não aceitou remarcar a visita dentro do prazo da auditoria. Como o relatório deve tratar essa situação?

A. Cancelar todo o relatório e refazer a auditoria completa
B. Omitir o fato, pois o fechamento por chuva não é culpa do cliente
C. Registrar o desvio do plano, as razões e o efeito nas conclusões
D. Declarar a mina não visitada conforme, com base na outra mina

R6.2 · Domínio 6: Encerramento de uma auditoria ISO/IEC 42001

Antes de enviar o relatório final da auditoria da Indústria Química Vale Azul, o líder percebe que algumas constatações não têm registro de onde a evidência foi vista e que há anotações soltas sem data. O que deve ser feito antes de concluir os trabalhos?

A. Completar e revisar os documentos de trabalho para que sejam rastreáveis
B. Enviar assim mesmo, pois o relatório já resume tudo o que importa ao cliente
C. Pedir ao auditado que complete as referências que faltam
D. Apagar as anotações sem data para evitar questionamentos

R6.3 · Domínio 6: Encerramento de uma auditoria ISO/IEC 42001

A auditoria de certificação da Clínica Pulmão Livre terminou com duas não conformidades menores. O que o organismo de certificação precisa fazer em relação a elas antes de decidir pela certificação?

A. Analisar e aceitar o plano do cliente para correção e ação corretiva
B. Converter as não conformidades menores em oportunidades de melhoria
C. Verificar no local a implementação das ações antes de qualquer decisão
D. Aguardar a recertificação para tratar as não conformidades menores

R6.4 · Domínio 6: Encerramento de uma auditoria ISO/IEC 42001

O auditor-líder da equipe que auditou a Indústria de Laticínios Vale Verde quer ele mesmo aprovar a certificação, pois conhece bem o caso. Pela ISO/IEC 17021-1, isso é permitido?

A. Sim, desde que outro auditor da equipe também assine
B. Sim, pois o líder conhece o caso
C. Não; a decisão cabe ao organismo de acreditação
D. Não; a decisão é tomada por pessoas que não realizaram a auditoria

Respostas comentadas

R6.1. C) Registrar o desvio do plano, as razões e o efeito nas conclusões

Por quê: Pela ISO/IEC 17021-1, o relatório registra desvios do plano e razões e quaisquer questões significativas que impactem o programa de auditoria.

✗ A) Incorreta. O desvio é tratado no relatório e no programa; não exige refazer tudo.
✗ B) Incorreta. Omitir desvios fere a apresentação justa.
✗ D) Incorreta. Declarar conforme sem evidência fere a abordagem baseada em evidência.

> **Dica de prova:** Desvio do plano = registrar com motivo no relatório.

R6.2. A) Completar e revisar os documentos de trabalho para que sejam rastreáveis

Por quê: O handbook cobra boas práticas para completar documentos de trabalho e realizar revisões de qualidade da documentação da auditoria.

✗ B) Incorreta. Registros incompletos enfraquecem as conclusões e a revisão de qualidade.
✗ C) Incorreta. Os papéis de trabalho são da equipe auditora, não do auditado.
✗ D) Incorreta. Apagar registros compromete a integridade da evidência.

> **Dica de prova:** Antes do relatório: papéis de trabalho completos e rastreáveis.

R6.3. A) Analisar e aceitar o plano do cliente para correção e ação corretiva

Por quê: A ISO/IEC 17021-1 diferencia: NC maior exige verificação de correção e ação corretiva antes da decisão; NC menor exige análise e aceitação do plano do cliente.

✗ B) Incorreta. A classificação baseada em evidência não é alterada para facilitar a decisão.
✗ C) Incorreta. Verificar a implementação antes da decisão é exigido para não conformidades maiores.
✗ D) Incorreta. As NC menores são tratadas no ciclo, não deixadas para a recertificação.

> **Dica de prova:** NC menor = plano aceito; NC maior = ação verificada antes da decisão.

R6.4. D) Não; a decisão é tomada por pessoas que não realizaram a auditoria

Por quê: A equipe apresenta conclusões e recomendação; o organismo, por pessoas independentes da auditoria, analisa as informações e decide.

✗ A) Incorreta. A assinatura de outro membro da equipe mantém o problema: ambos auditaram.

✗ B) Incorreta. Conhecer o caso não supera a exigência de separação entre auditar e decidir.

✗ C) Incorreta. A decisão é do organismo de certificação, não do de acreditação.

Dica de prova: Quem auditou não decide a certificação.

07

CAPÍTULO 7 · 11,25% DA PROVA

Domínio 7: Gestão de um programa de auditoria ISO/IEC 42001

Aqui eu preciso dominar o ciclo de certificação (três anos, supervisões, recertificação), as medidas sobre o certificado (suspensão, retirada, redução, extensão, transferência, auditoria com pouca antecedência) e a gestão do programa de auditoria pelo PDCA. A prova também cobra uso indevido de marcas e do logotipo da ISO e as regras de certificação pessoal da PECB. Onde mais erro: confundir redução de escopo com retirada, achar que supervisão precisa ter a mesma extensão da certificação inicial e achar que supervisão perdida pode ser somada à recertificação.

Neste capítulo

17 tópicos-chave · 13 pegadinhas · 6 macetes · 13 gatilhos · 4 questões comentadas

Tópicos-chave

Processo e ciclo de certificação

Sequência: análise do pedido, programa do ciclo, estágio 1, estágio 2, decisão. O ciclo dura três anos, com auditorias de supervisão e recertificação antes do vencimento; não há ciclo de dois ou cinco anos nem prorrogação automática.

Supervisão

Ao menos uma vez por ano civil (exceto em ano de recertificação), e a primeira em no máximo 12 meses após a decisão de certificação. Não precisa ser auditoria completa; costuma verificar auditorias internas, análise crítica, ações sobre NC, reclamações, mudanças e uso de marcas, com rodízio para cobrir todo o escopo no ciclo.

Recertificação

Avalia a continuidade da conformidade e da eficácia do AIMS como um todo, considerando o desempenho no período. Mudança significativa (passou a desenvolver modelos próprios, nova equipe em outro estado) pode exigir atividade de estágio 1. Concluída antes do vencimento, a validade do novo certificado se baseia no vencimento do atual; não concluída antes do vencimento, a certificação expira.

Suspensão

Torna a certificação temporariamente inválida; cabe quando o cliente não permite a supervisão na frequência exigida ou mantém NC maior sem tratamento. Durante a suspensão o cliente não pode promover a certificação. Encerrada a suspensão após verificação, o ciclo continua com supervisões e recertificação.

Redução x retirada

Redução: parte do escopo sai do certificado (unidade encerrada, fim do uso de IA em Campinas). Retirada: o certificado inteiro cai (cancelamento voluntário total, falhas graves não resolvidas após suspensão, cliente deixou de existir).

Extensão de escopo e mudanças do cliente

Incluir um novo sistema de IA no meio do ciclo exige auditoria especial, sem esperar a recertificação nem repetir a certificação inicial. Mudança relevante (troca de controle acionário) deve ser informada ao organismo, que avalia se precisa de auditoria especial.

Auditoria com pouca antecedência

Usada para investigar reclamações graves sobre cliente certificado ou verificar ações de cliente suspenso antes da próxima supervisão. O organismo de acreditação nunca audita clientes do certificador.

Transferência entre organismos

O novo organismo analisa validade do certificado, relatórios anteriores e NC pendentes antes de aceitar a transferência.

Certificado e uso de marcas

O certificado traz organização, norma, escopo, datas de emissão e validade e organismo emissor; não traz NC nem nomes de auditores. Marcas de certificação e de acreditação seguem as regras de seus donos; selo de sistema de gestão em embalagem sugere certificação de produto e é indevido; divulgar certificação além do escopo é enganoso; 'certificado pela ISO' com logotipo da ISO é inadequado.

Gerente do programa e PDCA

O gerente do programa estabelece, implementa, monitora, analisa criticamente e melhora o programa. Não redige documentos de clientes, não escolhe constatações e não decide sozinho certificações. Problemas recorrentes (atrasos, falta de competência em IA) pedem análise crítica e melhorias, como capacitar auditores.

Objetivos e proporcionalidade do programa

Objetivo de um programa interno: verificar conformidade e eficácia do AIMS e apoiar a melhoria contínua, nunca metas de NC ou avaliação de bônus. A extensão de cada programa é proporcional a tamanho, natureza, complexidade e riscos da organização e de seus sistemas de IA, não ao preço do contrato.

Riscos e recursos do programa

Concentração de auditorias num mês, aposentadoria de auditor-chave e falta de competência em IA generativa são riscos do programa: identificar e agir (redistribuir agenda, formar auditores, usar especialistas). Não se corta tempo de auditoria nem se usa autoavaliação no lugar de supervisão.

Monitoramento do programa e dos auditores

Indicadores adequados: cumprimento do cronograma, auditorias no prazo, NC tratadas, desempenho das equipes, feedback e reclamações. A competência dos auditores se avalia por registros, feedback, entrevista, observação e exame, de forma contínua; número de NC por auditor distorce o julgamento.

Registros do programa

Planos, relatórios, NC e ações, competência e avaliação dos auditores, retidos com acesso controlado; não pertencem ao auditor, não vão para pendrive pessoal e não se guardam cópias integrais de dados pessoais. Cada auditoria alimenta o planejamento da seguinte (NC abertas, mudanças, riscos, áreas pendentes).

Programa de auditoria interna e de segunda parte

Auditores internos são escolhidos para assegurar objetividade e imparcialidade (o gestor não audita o próprio processo; o organismo de certificação não faz auditoria interna). Frequência e profundidade seguem importância, riscos e resultados anteriores, inclusive constatações externas. Auditar fornecedores por contrato é programa de segunda parte gerido pelos princípios da ISO 19011.

Organismos que certificam AIMS

Seguem a ISO/IEC 17021-1 mais os requisitos adicionais de competência e processo da ISO/IEC 42006 (2025). Para vários locais, planejam amostras de unidades ao longo do ciclo com base em risco e regras do esquema; para clientes com 27001 e 42001, podem planejar auditorias combinadas garantindo os requisitos de cada norma.

Certificação pessoal PECB

Lead Auditor exige cinco anos de experiência (dois em gestão de IA) e 300 horas de auditoria; Auditor exige dois anos (um em gestão de IA) e 200 horas; Senior Lead Auditor exige dez anos (sete em gestão de IA) e 1.000 horas. Certificações PECB valem três anos e exigem CPD e taxa anual (AMF); sem eles, suspensão de 12 meses para regularizar.

Macetes para memorizar

Ciclo

3 anos: ano 1 certifica, anos 2 e 3 supervisão, recertifica antes de vencer.

Primeira supervisão

Doze meses, nem um dia a mais.

Redução x retirada

Reduz = tira um pedaço; retira = tira tudo.

Programa

Estabelece, Implementa, Monitora, Analisa, Melhora: o PDCA do gerente.

Suspensão

Suspenso não divulga; resolvido, o ciclo segue sem reiniciar.

Credenciais PECB

Auditor 2-1-200; Lead 5-2-300; Senior 10-7-1.000 (anos, anos em IA, horas).

Tabela de memorização: não confunda

Quando é...	...e quando é
Suspensão Certificação temporariamente inválida (supervisão não permitida, NC maior sem tratamento); pode ser encerrada e o ciclo segue.	**Retirada** Certificado inteiro deixa de existir (cancelamento total, falha grave não resolvida após suspensão).
Redução de escopo Parte sai do certificado: organismo avalia o pedido e reduz.	**Extensão de escopo** Novo sistema entra no meio do ciclo: auditoria especial.
Supervisão Anual, parcial, foca temas obrigatórios e rodízio do escopo.	**Recertificação** Sistema completo e desempenho do ciclo, antes do vencimento; pode incluir estágio 1.
Auditoria com pouca antecedência Investigar reclamação grave ou verificar ações de cliente suspenso.	**Auditoria especial de extensão** Avaliar inclusão de novo escopo durante o ciclo.

Programa de primeira parte Auditorias internas da própria organização (cláusula 9.2).	**Programa de segunda parte** Organização audita seus fornecedores com base em contrato.
Expiração Recertificação não concluída antes do vencimento: certificado vence e só se restabelece conforme as regras.	**Suspensão** Certificado ainda vigente, mas temporariamente inválido por falha do cliente.

Números que caem

Item	Valor
Peso do domínio na prova PECB	**11,25% (9 de 80 questões)**
Ciclo de certificação de sistema de gestão	**3 anos**
Frequência da supervisão	**Ao menos uma vez por ano civil, exceto em ano de recertificação**
Primeira supervisão	**No máximo 12 meses após a decisão de certificação**
PECB Certified ISO/IEC 42001 Auditor	**2 anos de experiência (1 em gestão de IA) e 200 horas de auditoria**
PECB Certified ISO/IEC 42001 Lead Auditor	**5 anos de experiência (2 em gestão de IA) e 300 horas de auditoria**
PECB Certified ISO/IEC 42001 Senior Lead Auditor	**10 anos de experiência (7 em gestão de IA) e 1.000 horas de auditoria**
Validade das certificações PECB	**3 anos, com CPD e taxa anual (AMF)**
Suspensão por falta de CPD e AMF (PECB)	**12 meses para regularizar**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Manter o certificado e somar a supervisão perdida à recertificação.
Como não cair: Supervisão é ao menos anual por ano civil; cliente que não permite pode ter a certificação suspensa.

⚠ **Alerta de prova:** Programar a primeira supervisão para até 24 meses ou só no terceiro ano.
Como não cair: A primeira supervisão ocorre em no máximo 12 meses após a decisão.

⚠ **Alerta de prova:** Achar que a supervisão de dois dias é irregular por ser menor que a inicial.
Como não cair: Supervisões não precisam ser auditorias completas; o ciclo cobre o escopo.

⚠ **Alerta de prova:** Chamar de retirada o fim de uma unidade no certificado.
Como não cair: Parte do escopo saindo é redução; retirada é o certificado inteiro.

⚠ **Alerta de prova:** Esperar a recertificação para incluir novo sistema ou exigir nova certificação inicial.
Como não cair: Extensão de escopo é feita por auditoria especial durante o ciclo.

⚠ **Alerta de prova:** Manter o selo de certificação em propostas e site durante a suspensão.
Como não cair: Certificação suspensa não pode ser promovida.

⚠ **Alerta de prova:** Achar que citar número do certificado ou organismo acreditado torna adequado 'certificado pela ISO'.
Como não cair: A ISO não certifica nem autoriza seu logotipo, e a certificação é do sistema, não da IA.

⚠ **Alerta de prova:** Recertificação antecipada reduz a validade ou dá prêmio de cinco anos.
Como não cair: A validade se baseia no vencimento do certificado atual, mantendo o ciclo de três anos.

⚠ **Alerta de prova:** Pedir ao organismo de acreditação para investigar reclamação contra o cliente.
Como não cair: O certificador faz auditoria com pouca antecedência; o acreditador só avalia o certificador.

⚠ **Alerta de prova:** Usar número de NC por auditor como indicador ou meta do programa.
Como não cair: Meta de NC distorce o julgamento; use prazos, NC tratadas, feedback e reclamações.

⚠ **Alerta de prova:** Deixar o cliente escolher auditores ou processos a mostrar a cada ano.
Como não cair: Escolhas do programa são do organismo, com base em risco e regras do esquema.

⚠ **Alerta de prova:** Contratar o organismo de certificação para fazer a auditoria interna.
Como não cair: O certificador não pode fazer auditoria interna do cliente; seria ameaça à imparcialidade.

⚠ **Alerta de prova:** Achar que a certificação de auditor PECB é vitalícia ou rebaixa automaticamente para Foundation.
Como não cair: Vale três anos, exige CPD e AMF; sem eles, suspensão de 12 meses antes de outras medidas.

Como cai na prova

📝 **Como cai:** Evento no ciclo (supervisão perdida, recertificação atrasada, NC maior sem tratamento) e pergunta qual medida.
Como resolver: Supervisão não permitida ou NC maior pendente = suspensão; recertificação não concluída antes do vencimento = expiração; descarte prorrogações automáticas e transferência ao acreditador.

📝 **Como cai:** Mudança no escopo do cliente durante o ciclo.
Como resolver: Entrou algo = auditoria especial de extensão; saiu parte = redução; mudança relevante = cliente informa e o organismo avalia auditoria especial.

📝 **Como cai:** Uso de marca, selo ou logotipo pelo cliente percebido na supervisão.
Como resolver: Verifique se sugere certificação de produto, extrapola o escopo, usa o logotipo da ISO ou ocorre durante suspensão: qualquer um torna o uso inadequado.

📝 **Como cai:** Gerente do programa diante de problema (falta de auditores, atrasos, auditor fraco).
Como resolver: Trate como risco ou desempenho do programa: analisar criticamente, capacitar, usar especialistas e avaliar auditores; nunca cortar tempo, terceirizar a escolha ao cliente ou criar meta de NC.

📝 **Como cai:** Requisitos para credencial PECB ou manutenção.
Como resolver: Confira anos de experiência, anos em gestão de IA e horas de auditoria; manutenção a cada ciclo de três anos com CPD e AMF.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
ano civil terminou sem supervisão e o cliente não respondeu	**Suspensão da certificação**
decisão de certificação em uma data, quando é a primeira supervisão	**No máximo 12 meses depois**
15 processos e supervisões curtas	**Rodízio cobrindo todo o escopo no ciclo**
novo sistema de IA a incluir antes da recertificação	**Auditoria especial de extensão de escopo**
empresa encerrou uma unidade	**Redução de escopo**
reclamações públicas graves sobre cliente certificado	**Auditoria especial com pouca antecedência**
recertificação adiada pelo cliente além do vencimento	**Certificação expira**
troca de organismo no meio do ciclo	**Analisar validade, relatórios anteriores e NC pendentes**

selo na embalagem 'produto selecionado por IA certificada'	**Uso inadequado: sugere certificação de produto**
site diz que todas as operações são certificadas	**Referência deve refletir o escopo certificado**
atrasos e reclamações recorrentes no programa	**Analisar criticamente e melhorar (PDCA)**
empresa passou a desenvolver modelos próprios, recertificação chegando	**Recertificação pode incluir estágio 1**
auditar fornecedores de modelos com base em contrato	**Programa de segunda parte (ISO 19011)**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Primeira supervisão em até 12 meses; depois, ao menos uma por ano civil.
- Supervisão não permitida ou NC maior sem tratamento leva à suspensão; suspenso não divulga.
- Redução tira parte do escopo; retirada tira o certificado inteiro; extensão exige auditoria especial.

Essenciais para a prova (checklist)

- ☐ Sei a sequência do processo de certificação e a duração do ciclo.
- ☐ Sei as regras de frequência das supervisões e o que elas costumam verificar.
- ☐ Sei o que a recertificação avalia e quando pode incluir estágio 1.
- ☐ Sei diferenciar suspensão, retirada, redução, extensão e expiração.
- ☐ Sei quando usar auditoria com pouca antecedência.
- ☐ Sei avaliar o uso de marcas, selos e do nome da ISO.
- ☐ Sei as responsabilidades do gerente do programa e os indicadores adequados.
- ☐ Sei os requisitos das credenciais PECB e as regras de manutenção.

Questões de revisão do capítulo

R7.1 · Domínio 7: Gestão de um programa de auditoria ISO/IEC 42001

A Locadora Via Rápida, certificada na ISO/IEC 42001, adiou duas vezes a auditoria de supervisão e o ano civil terminou sem que ela ocorresse. O organismo tentou reagendar e o cliente não respondeu. Que medida o organismo pode adotar segundo as regras de certificação?

A. Transferir a responsabilidade pela supervisão ao organismo de acreditação
B. Emitir novo certificado com validade estendida para compensar o atraso
C. Manter o certificado válido e somar a supervisão perdida à recertificação
D. Suspender a certificação, porque o cliente não permitiu a supervisão na frequência exigida

R7.2 · Domínio 7: Gestão de um programa de auditoria ISO/IEC 42001

A Startup Galáxia Dados obteve a certificação ISO/IEC 42001 para seu sistema de gestão e publicou um anúncio: 'Nossa IA de recomendação é certificada pela ISO', com o logotipo da ISO no rodapé. Como um auditor deve avaliar essa comunicação na supervisão?

A. Adequada, desde que o anúncio cite também o número do certificado e o nome do organismo
B. Adequada, porque a certificação foi emitida por um organismo de certificação acreditado
C. Inadequada, porque faltou indicar no anúncio a data de validade e o escopo do certificado emitido
D. Inadequada: a ISO não certifica nem autoriza seu logotipo, e a certificação é do sistema

R7.3 · Domínio 7: Gestão de um programa de auditoria ISO/IEC 42001

Uma empresa certificada por organismo acreditado quer usar, em sua proposta comercial, a marca do organismo de acreditação ao lado da logomarca da certificação. Qual orientação está correta?

A. A marca de acreditação só pode aparecer na embalagem dos produtos com IA
B. O uso deve seguir as regras do organismo de certificação e da acreditação
C. O uso é livre, pois a acreditação é pública e qualquer pessoa pode citá-la
D. O uso exige autorização da ISO, que controla as marcas de acreditação

R7.4 · Domínio 7: Gestão de um programa de auditoria ISO/IEC 42001

Um auditor do organismo que certifica a Fintech Cofre Seguro quer levar para casa, em pendrive pessoal, cópias dos registros da auditoria com amostras de dados de clientes. Como a gestão do programa de auditoria trata esses registros?

A. Registros enviados ao organismo de acreditação para guarda centralizada e segura
B. Registros de uso livre, pois pertencem ao auditor que os coletou
C. Registros com acesso controlado e proteção conforme a confidencialidade
D. Registros descartados ao fim de cada auditoria para evitar vazamentos

Respostas comentadas

R7.1. D) Suspender a certificação, porque o cliente não permitiu a supervisão na frequência exigida

Por quê: A suspensão torna a certificação temporariamente inválida; se a situação não for resolvida no prazo definido, o organismo pode retirar a certificação ou reduzir o escopo.

✗ A) Incorreta. Organismos de acreditação não realizam supervisões de clientes certificados.
✗ B) Incorreta. Atrasos do cliente não geram extensão de validade.
✗ C) Incorreta. A supervisão deve ocorrer ao menos uma vez por ano civil; acumulá-la na recertificação não é permitido.

> **Dica de prova:** Supervisão não realizada no ano civil por causa do cliente = suspensão.

R7.2. D) Inadequada: a ISO não certifica nem autoriza seu logotipo, e a certificação é do sistema

Por quê: A ISO informa que não realiza certificação, não emite certificados e não permite o uso do seu logotipo em conexão com certificação. O uso de marcas e referências à certificação é verificado pelo organismo nas supervisões.

✗ A) Incorreta. Citar o número do certificado não corrige a atribuição à ISO, o uso do logotipo nem a sugestão de certificação de produto.

✗ B) Incorreta. Mesmo com organismo acreditado, a mensagem é enganosa: atribui a certificação à ISO e a apresenta como certificação do produto.

✗ C) Incorreta. A falta de data não é o problema central; o anúncio é enganoso pela atribuição à ISO e pelo uso indevido do logotipo.

> **Dica de prova:** ISO não certifica: 'certificado pela ISO' e logotipo da ISO são indevidos.

R7.3. B) O uso deve seguir as regras do organismo de certificação e da acreditação

Por quê: O handbook cobra conhecimento de requisitos de uso de marcas; o organismo verifica nas supervisões se o cliente controla o uso de documentos e marcas de certificação.

✗ A) Incorreta. Marcas de certificação de sistema de gestão não devem aparecer em produtos de modo a sugerir certificação de produto.

✗ C) Incorreta. Marcas não são de uso livre; há condições para evitar declarações enganosas.

✗ D) Incorreta. A ISO não controla marcas de acreditação nem autoriza seu uso.

> **Dica de prova:** Marcas de certificação e acreditação seguem as regras dos donos das marcas.

R7.4. C) Registros com acesso controlado e proteção conforme a confidencialidade

Por quê: O handbook cobra a proteção da integridade, disponibilidade e confidencialidade dos registros de auditoria e as boas práticas de gestão desses registros no programa.

✗ A) Incorreta. O organismo de acreditação não guarda registros de auditorias de clientes.

✗ B) Incorreta. Os registros pertencem ao processo do organismo e são confidenciais.

✗ D) Incorreta. Registros precisam ser retidos para demonstrar o processo e apoiar decisões e auditorias futuras.

> **Dica de prova:** Registros de auditoria: retidos, protegidos e com acesso controlado.

DIA DA PROVA

Estratégia de prova

A prova PECB ISO/IEC 42001 Lead Auditor tem 80 questões de múltipla escolha com 3 alternativas e uma correta, isoladas e em cenários com 5 questões cada, em 3 horas, com nota mínima de 70%. Mais da metade (55%) mede avaliação, ou seja, julgar o que o auditor deve fazer num caso concreto, e não decorar texto. O pensamento é sempre o do auditor imparcial: a evidência manda, o auditor não presta consultoria, quem decide a certificação é o organismo e a conformidade é responsabilidade do cliente. Os distratores costumam ser respostas 'simpáticas' (agradar o cliente, ganhar tempo) ou radicais (encerrar a auditoria, cancelar o certificado, registrar NC por precaução). Na CertiProf I42001LA o raciocínio é o mesmo, com 40 questões de 4 alternativas, 60 minutos e nota mínima de 80%.

Como responder

✓ Como a prova PECB é de livro aberto (cópia impressa da ISO/IEC 42001, material do curso e anotações pessoais), prepare um índice próprio com as cláusulas 4 a 10, os temas do Anexo A e as regras da 17021-1 para achar rápido, mas não dependa de consultar tudo.

✓ Use as 3 horas a seu favor: com 80 questões, dá pouco mais de 2 minutos por questão; leia o cenário uma vez com atenção e responda as 5 questões dele em sequência.

✓ Em cada alternativa, pergunte 'isso se apoia em evidência?' e 'isso é papel do auditor?'; elimine as que mudam constatação sem evidência ou que fazem o auditor corrigir, redigir ou indicar solução.

✓ Desconfie das justificativas do auditado nas alternativas: ninguém reclamou, o modelo funciona bem, já corrigimos, é do fornecedor, a política foi aprovada em 2023. Quase sempre são a pegadinha.

✓ Quando a pergunta for 'qual requisito está em foco', procure o centro da falha e escolha a cláusula mais direta; descarte as que só tangenciam o tema.

✓ Entre uma resposta extrema (encerrar a auditoria, cancelar o certificado) e uma que comunica, registra e segue o processo formal, prefira a segunda, salvo risco imediato que exige comunicação sem demora.

✓ Revise ao final as questões de definição (combinada x conjunta, robustez x resiliência, verificação x validação), que são as que mais se trocam por desatenção.

✓ Se a prova não for no seu idioma nativo, lembre que o handbook prevê 30 minutos adicionais, a pedido, para provas de nível Lead.

Erros que derrubam candidatos

✗ Aceitar declaração do gerente ou do diretor como evidência suficiente.

✗ Registrar NC sem evidência verificável, ou classificar tudo como maior por cautela.

✗ Achar que o auditor-líder concede a certificação ou que a ISO certifica empresas.

✗ Confundir auditoria combinada, conjunta e integrada, e primeira, segunda e terceira parte.

✗ Tratar como oportunidade de melhoria um controle que a própria organização definiu e não cumpre.

✗ Achar que todos os controles do Anexo A são obrigatórios ou que o Anexo A pode ser ignorado.

✗ Confundir redução com retirada e somar supervisão perdida à recertificação.

Na semana da prova

- ☐ Refaça as provas práticas cronometradas e anote em qual domínio você erra mais; o Domínio 5 pesa 23,75% e o Domínio 3 pesa 20%.
- ☐ Monte e imprima o índice das cláusulas 4 a 10, dos Anexos A a D e das regras de ciclo de certificação (supervisão, suspensão, redução, retirada) para consulta rápida.
- ☐ Releia os sete princípios de auditoria e os princípios da 17021-1 e associe cada um a um exemplo de violação.
- ☐ Revise a família de normas de IA (22989, 23053, 23894, 38507, 42005, 42006) e os termos da 22989 que mais se confundem.
- ☐ Confira as regras do dia da prova: chegar ou estar presente pelo menos 30 minutos antes, materiais permitidos e equipamentos proibidos.
- ☐ Na véspera, revise só as seções 'lembrar' e 'pegadinhas' de cada domínio e durma bem.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. Domínio 1: Princípios e conceitos fundamentais de um sistema de gestão de IA

▸ termos e conceitos de IA, terminologia → **ISO/IEC 22989**

▸ framework de sistema de IA que usa aprendizado de máquina → **ISO/IEC 23053**

▸ orientação para gerir riscos de IA e integrá-los à organização → **ISO/IEC 23894**

▸ conselho, o que supervisionar ao autorizar o uso de IA → **ISO/IEC 38507 (governança)**

▸ quando avaliar impacto, escopo, responsabilidades e registro da avaliação → **ISO/IEC 42005**

⚠ A única referência normativa é a ISO/IEC 22989:2022; a 27001 está só na bibliografia.

⚠ A ISO não certifica, não emite certificado e não permite seu logotipo associado a certificação; quem certifica é o organismo de certificação.

⚠ A norma vale para qualquer organização que desenvolve, fornece ou usa IA; desenvolver modelo próprio não é condição.

2. Domínio 2: Requisitos do sistema de gestão de IA

▸ questões internas e externas, papel frente aos sistemas de IA → **4.1 Contexto**

▸ limites vagos do AIMS, documento não disponível → **4.3 Escopo**

▸ política aprovada, mas as áreas usam IA sem passar pelo AIMS → **5.1 Integração dos requisitos aos processos de negócio**

▸ ninguém sabe quem aprova a colocação em produção → **5.3 Papéis, responsabilidades e autoridades**

▸ objetivo 'melhorar a IA', sem medida, dono nem prazo → **6.2 Objetivos de IA**

⚠ Usam-se os necessários conforme os riscos, com exclusões justificadas, e podem existir controles próprios.

⚠ Ele é a referência para a seleção de controles e não pode ser desconsiderado; exclusões precisam de justificativa na SoA.

⚠ Todos os riscos identificados e seus controles devem se refletir na SoA.

3. Domínio 3: Conceitos e princípios fundamentais de auditoria

▸ auditor tem ações do fornecedor auditado → **Independência comprometida**

▸ comentou detalhes do cliente em evento ou colou documento em chatbot público → **Confidencialidade**

▸ concluiu 'adequado' só com o relato do gerente → **Abordagem baseada em evidência**

▸ pouco tempo e vários sistemas para escolher → **Abordagem baseada em risco: maior impacto primeiro**

▸ mesmo tempo para sistema crítico e chatbot de perguntas frequentes → **Devido cuidado profissional: redistribuir tempo**

⚠ A classificação segue a evidência; pressão comercial se registra e se informa ao organismo.

⚠ Mantenha o texto fiel à evidência e explique os processos de contestação.

⚠ Testemunho é evidência fraca sozinho: corrobore com registros ou observação.

4. Domínio 4: Preparação de uma auditoria ISO/IEC 42001

▸ equipe experiente em 42001, mas sem conhecimento do setor → **Incluir especialista técnico**

▸ pessoa do auditado marca entrevistas e dá acesso às áreas → **Guia**

▸ representante do banco quer acompanhar → **Observador acordado antes, sem interferir**

▸ milhares de registros de cada tipo no período → **Plano de amostragem com critérios e tamanhos**

▸ 25 sistemas e três dias de supervisão → **Priorizar por risco, impacto, mudanças e histórico**

⚠ A auditoria precisa cobrir o escopo pedido; leve a questão ao organismo.

⚠ Objeção justificada é avaliada e, se procedente, o auditor é substituído.

⚠ Consultoria recente (dois anos) impede a designação para aquele cliente.

5. Domínio 5: Condução de uma auditoria ISO/IEC 42001

‣ nenhum sistema teve riscos identificados e não há critérios de risco → **NC maior: falha sistêmica**

‣ um analista recém-contratado sem evidência de competência, demais completos → **NC menor (7.2)**

‣ requisito atendido e ideia que reduziria perdas → **Oportunidade de melhoria sem prescrever solução**

‣ registro alterado à mão, sem identificar quem, quando e por quê → **Integridade dos registros e controle de alterações (7.5)**

‣ versão em uso sem identificação nem aprovação → **7.5 Controle de informação documentada**

⚠ Ausência de incidentes e bom desempenho não demonstram que o controle definido é executado.

⚠ Controle definido no AIMS é critério; não cumprir é NC.

⚠ Processos providos externamente continuam sob controle e responsabilidade da organização.

6. Domínio 6: Encerramento de uma auditoria ISO/IEC 42001

‣ diretor pede o certificado no mesmo dia → **Equipe recomenda; organismo decide por quem não auditou**

‣ duas NC menores e decisão pendente → **Analisar e aceitar o plano do cliente**

‣ NC maior e cliente diz que resolveu → **Verificar correção e ação corretiva (documentos ou visita)**

‣ pessoa que não participou analisa relatório e recomendação → **Revisão independente para decisão imparcial**

‣ diretor discorda da constatação e não há acordo → **Registrar a divergência e encaminhar ao organismo**

⚠ Quem auditou não decide; a decisão é do organismo por pessoas que não participaram.

⚠ O cliente apresenta plano com causa, correção e ação corretiva, que o organismo analisa e aceita.

⚠ NC maior exige verificar correção e ação corretiva antes de decidir.

7. Domínio 7: Gestão de um programa de auditoria ISO/IEC 42001

‣ ano civil terminou sem supervisão e o cliente não respondeu → **Suspensão da certificação**

‣ decisão de certificação em uma data, quando é a primeira supervisão → **No máximo 12 meses depois**

‣ 15 processos e supervisões curtas → **Rodízio cobrindo todo o escopo no ciclo**

‣ novo sistema de IA a incluir antes da recertificação → **Auditoria especial de extensão de escopo**

‣ empresa encerrou uma unidade → **Redução de escopo**

⚠ Supervisão é ao menos anual por ano civil; cliente que não permite pode ter a certificação suspensa.

⚠ A primeira supervisão ocorre em no máximo 12 meses após a decisão.

⚠ Supervisões não precisam ser auditorias completas; o ciclo cobre o escopo.

GABARITO

Respostas do diagnóstico

D1. C) Previsibilidade → revise o capítulo 1

Por quê: Previsibilidade, explicabilidade e transparência são características de confiabilidade que ajudam partes interessadas a confiar nos sistemas de IA.

✗ A) Incorreta. Explicabilidade é expressar os fatores que influenciaram um resultado.

✗ B) Incorreta. Heteronomia é operar sob controle ou supervisão externa.

✗ D) Incorreta. Imputação é substituir dados ausentes por estimativas.

> **Dica de prova:** Suposições confiáveis sobre a saída = previsibilidade.

D2. C) Rede neural recorrente, como a LSTM → revise o capítulo 1

Por quê: A 22989 distingue redes feed forward (informação em um só sentido), convolucionais (convolução) e recorrentes (usam o passo anterior), como a LSTM.

✗ A) Incorreta. A rede convolucional usa convolução em pelo menos uma camada e é muito usada em imagens.

✗ B) Incorreta. Árvore de decisão não é rede neural.

✗ D) Incorreta. Máquina de vetores de suporte é algoritmo de ML que busca margens máximas, não rede neural.

> **Dica de prova:** Dados sequenciais = rede recorrente (LSTM).

D3. C) Porque é IA estreita: focada em tarefas definidas → revise o capítulo 1

Por quê: A nota da definição de AGI observa que o termo é muitas vezes usado em sentido mais forte, de sistemas capazes de realizar todas as tarefas que um humano realiza.

✗ A) Incorreta. Geração de texto não define um sistema especialista, que se baseia em conhecimento de especialistas.

✗ B) Incorreta. A norma define termos; não proíbe classificações.

✗ D) Incorreta. AGI não se define pela técnica usada, mas pela amplitude de tarefas.

> **Dica de prova:** Tarefa específica = IA estreita; ampla gama de tarefas = IA geral.

D4. D) Orienta a implementação dos controles; não exige justificar seu uso na SoA → revise o capítulo 2

Por quê: A PECB descreve os Anexos: A (controles de referência), B (orientação de implementação), C (objetivos e fontes de risco) e D (uso em diferentes setores).

✗ A) Incorreta. O Anexo A continua sendo a referência de objetivos de controle e controles.

✗ B) Incorreta. O Anexo B não lista setores proibidos.

✗ C) Incorreta. Requisitos de organismos estão na 17021-1 e na 42006.

> **Dica de prova:** Anexo B = como implementar os controles.

D5. A) Riscos e controles devem se refletir na declaração → revise o capítulo 2

Por quê: A nota 1 da definição lembra que a organização pode não precisar de todos os controles do Anexo A ou pode ir além deles, com controles próprios.

✗ B) Incorreta. A nota exige que os riscos identificados e seus controles apareçam na declaração.
✗ C) Incorreta. A organização pode ter controles além do Anexo A.
✗ D) Incorreta. Não há exceção setorial.

> **Dica de prova:** Todo risco identificado e seu controle aparecem na SoA.

D6. C) Objetivos e política, riscos e oportunidades, confiabilidade da IA e fornecedores → revise o capítulo 2

Por quê: A introdução também diz que o AIMS deve ser integrado aos processos e à estrutura de gestão da organização.

✗ A) Incorreta. Esses processos podem usar IA, mas não são os exemplos citados.
✗ B) Incorreta. Esses processos de RH não são os exemplos citados.
✗ D) Incorreta. Esses processos de apoio não são os exemplos citados.

> **Dica de prova:** Processos cruciais: objetivos, riscos, confiabilidade da IA e fornecedores.

D7. C) Processo sistemático, independente e documentado → revise o capítulo 3

Por quê: A 42001 tem definição semelhante e observa que a auditoria pode ser interna (primeira parte) ou externa (segunda ou terceira parte) e combinada.

✗ A) Incorreta. Auditoria é sistemática e documentada, não informal.
✗ B) Incorreta. Inspeção de código pode ser técnica de verificação, mas não define auditoria.
✗ D) Incorreta. A independência é parte da definição; autoavaliação não é auditoria.

> **Dica de prova:** Auditoria = sistemática, independente e documentada.

D8. B) Registrar a constatação conforme a evidência encontrada → revise o capítulo 3

Por quê: Imparcialidade é a presença de objetividade; o auditor permanece justo e sem viés, sensível a influências sobre o próprio julgamento.

✗ A) Incorreta. Transferir o registro para evitar desconforto não é atitude objetiva.
✗ C) Incorreta. O propósito da empresa não altera a classificação técnica.
✗ D) Incorreta. Prazo informal antes do registro distorce a constatação.

> **Dica de prova:** Simpatia pelo auditado não muda a constatação.

D9. A) Auditoria conjunta → revise o capítulo 3

Por quê: A 17021-1 usa o mesmo conceito: auditoria conjunta é quando duas ou mais organizações auditoras cooperam para auditar um único cliente.

✗ B) Incorreta. Segunda parte é feita por parte interessada, como cliente.

✗ C) Incorreta. Combinada é a auditoria de dois ou mais sistemas de gestão em um único auditado.

✗ D) Incorreta. Auditoria interna é feita pela própria organização ou em seu nome.

> **Dica de prova:** Duas organizações auditoras juntas = auditoria conjunta.

D10. B) Incluir um especialista técnico na equipe → revise o capítulo 4

Por quê: Na seleção da equipe, considera-se a competência necessária para atingir os objetivos; quando falta conhecimento específico, inclui-se especialista técnico, que atua sob a direção de um auditor.

✗ A) Incorreta. Reduzir o escopo para contornar falta de competência compromete os objetivos da auditoria.

✗ C) Incorreta. Depender do relato do auditado não substitui a competência da equipe para avaliar evidências.

✗ D) Incorreta. A competência necessária deve ser assegurada na formação da equipe, antes da auditoria.

> **Dica de prova:** Falta conhecimento do setor = especialista técnico (não atua como auditor).

D11. A) Um plano de amostragem com critérios e tamanhos → revise o capítulo 4

Por quê: O Anexo A da ISO 19011:2026 trata de amostragem e de preparação de documentos de trabalho.

✗ B) Incorreta. Constatações dependem da evidência coletada.

✗ C) Incorreta. A seleção da amostra é da equipe auditora.

✗ D) Incorreta. Documentos de trabalho não devem restringir a auditoria.

> **Dica de prova:** Preparar plano de amostragem com critérios, sem engessar.

D12. A) A ISO/IEC 42001, a informação documentada do AIMS e requisitos legais aplicáveis → revise o capítulo 4

Por quê: Critérios de auditoria são o conjunto de requisitos usado como referência; podem incluir políticas, procedimentos, requisitos legais, obrigações contratuais e normas.

✗ B) Incorreta. Preferências do auditor não são critérios.

✗ C) Incorreta. Metas de vendas e orçamento não são critérios de auditoria do AIMS.

✗ D) Incorreta. Avaliação de desempenho de RH não é critério da auditoria do AIMS.

> **Dica de prova:** Critérios: norma + documentos do AIMS + requisitos legais aplicáveis.

Agora, treine no formato real

Faça as 6 provas completas do curso ISO 42001 Lead Auditor: 480 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de PECB. As questões são inéditas e não reproduzem a prova real.