

Guia de preparação EXIN ISFS ISO 27001

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.

4
capítulos por domínio

28
questões comentadas

65%
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 EXIN ISFS ISO 27001: 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 65%).

Mapa do exame

Cada prova do curso tem 40 questões e 60 minutos, no formato do exame. Referência de aprovação: 65%.

Domínio (capítulo)	Peso	Neste guia
1. Ameaças e Riscos	12,5%	17 conceitos · 16 pegadinhas
2. Controles de Segurança	52,5%	18 conceitos · 16 pegadinhas
3. Informação e Segurança	27,5%	18 conceitos · 14 pegadinhas
4. Legislação, Regulamentos e Normas	7,5%	17 conceitos · 11 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 · Ameaças e Riscos

Um raio atinge o prédio e queima equipamentos de rede. Como essa ameaça é classificada?

A. Ameaça não humana
B. Engenharia social
C. Ameaça humana intencional
D. Vulnerabilidade técnica

D2 · Ameaças e Riscos

Depois de aplicar os controles escolhidos, ainda resta uma parte do risco. Como ele é chamado e o que deve ocorrer com ele?

A. Risco zero, que dispensa novas análises no futuro
B. Risco inicial, que deve ser ignorado pela gestão
C. Risco residual, que deve ser aceito formalmente pela gestão
D. Risco transferido, que passa automaticamente ao fornecedor

D3 · Ameaças e Riscos

Um incidente causa perda de 8 mil reais por ocorrência e acontece em média uma vez a cada dois anos. Qual é a expectativa de perda anual (ALE)?

A. R$ 4.000
B. R$ 8.000
C. R$ 16.000
D. R$ 2.000

D4 · Controles de Segurança

Como deve ser o nível de verificação de antecedentes na contratação de pessoas?

A. Dispensado para cargos com acesso a dados sensíveis
B. Proporcional ao cargo, à informação acessada e aos riscos
C. Feito só depois de um incidente com a pessoa
D. Igual para todos, com investigação máxima em qualquer cargo

D5 · Controles de Segurança

Em quantos temas a ISO/IEC 27002:2022 organiza seus controles?

A. Dois: controles técnicos e controles administrativos
B. Sete, um para cada camada do modelo OSI
C. Quatro: organizacionais, de pessoas, físicos e tecnológicos
D. Catorze domínios de controle, como na edição anterior de 2013

D6 · Controles de Segurança

Após resolver um incidente de segurança, a equipe analisa as causas e atualiza procedimentos. Qual é o objetivo dessa etapa?

A. Aprender com o incidente para evitar que se repita
B. Encontrar um culpado para aplicar uma punição exemplar
C. Apagar os registros para não expor a empresa
D. Encerrar o caso sem nenhuma documentação

D7 · Informação e Segurança

Qual papel é, em geral, responsável por definir a estratégia de segurança da informação da organização como um todo?

A. O usuário final de cada departamento
B. O CISO (Chief Information Security Officer)
C. O fornecedor de antivírus contratado
D. O técnico de suporte do service desk da empresa

D8 · Informação e Segurança

Um sistema registra o valor "37,8". Na tela do enfermeiro aparece "temperatura do paciente: 37,8 °C". O que mudou?

A. A informação virou um dado bruto sem valor
B. O dado perdeu a integridade ao ser exibido
C. O dado ganhou contexto e virou informação
D. Nada, pois dado e informação são sinônimos

D9 · Informação e Segurança

Segundo a ISO/IEC 27001, o que a política de segurança da informação deve incluir?

A. A configuração detalhada de cada firewall da empresa e filiais
B. A lista de senhas dos administradores de cada sistema
C. O nome dos funcionários que já cometeram violações
D. Compromisso com os requisitos e com a melhoria contínua

D10 · Legislação, Regulamentos e Normas

Qual é o papel da norma ISO/IEC 27002?

A. Definir o vocabulário usado em todas as normas
B. Definir os requisitos para certificar o SGSI da empresa
C. Tratar da gestão da qualidade de produtos
D. Orientar a implementação dos controles de segurança

D11 · Legislação, Regulamentos e Normas

Na ISO/IEC 27001, onde estão os requisitos obrigatórios para o sistema de gestão?

A. Na introdução da norma, em notas
B. Nas cláusulas 4 a 10 do corpo da norma
C. Na norma ISO 9001, que a 27001 copia
D. No Anexo A, que lista os controles

D12 · Legislação, Regulamentos e Normas

Qual norma define os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação (SGSI)?

A. ISO/IEC 27002
B. ISO/IEC 27001
C. ISO 14001
D. ISO 9001

01

CAPÍTULO 1 · 12,5% DA PROVA

Ameaças e Riscos

Vale 12,5% da prova (cerca de 5 das 40) e é muito previsível: preciso classificar ameaças, separar ameaça, vulnerabilidade, risco e incidente, distinguir dano direto de indireto, conhecer as estratégias de risco e fazer contas simples de SLE, ARO e ALE. A prova usa a terminologia EXIN (aceitar o risco/risk bearing, neutro ao risco/risk neutral, evitar o risco/risk avoiding) misturada com as opções de tratamento ISO (modificar, reter, evitar, compartilhar), então tenho que reconhecer as duas. Como não há calculadora, as contas são simples, mas a pegadinha está na frequência: 'uma vez a cada dois anos' é ARO 0,5. Onde mais erro: confundir aceitar com neutro, e chamar multa ou perda de clientes de dano direto.

Neste capítulo

17 tópicos-chave · 16 pegadinhas · 6 macetes · 15 gatilhos · 4 questões comentadas

Tópicos-chave

Ameaça

Causa potencial de um incidente. Pode ser humana intencional (sabotagem, fraude), humana não intencional (erro, apagar uma pasta sem querer) ou não humana (raio, incêndio, inundação, tempestade).

Agente de ameaça

Quem ou o que pode concretizar a ameaça: pessoas, grupos ou eventos, como um grupo criminoso tentando invadir um banco. Conhecer motivos e capacidades ajuda a estimar a probabilidade dos riscos.

Vulnerabilidade

Fraqueza que uma ameaça pode explorar. Porta de emergência que não fecha direito é vulnerabilidade (quem entra por ela é a ameaça); software com falha conhecida e sem correção é vulnerabilidade técnica.

Risco

Surge quando uma ameaça pode explorar uma vulnerabilidade. Para determiná-lo, estima-se a probabilidade do evento e o impacto que causaria, que dependem das ameaças, das vulnerabilidades e do valor dos ativos da própria organização.

Incidente e ciclo do incidente

Incidente é a ameaça que de fato se concretizou. No ciclo, a ameaça vira incidente, que pode causar dano e exigir recuperação.

Engenharia social

Manipulação de pessoas, como alguém ligando e fingindo ser do suporte de TI para pedir a senha. O suporte legítimo não pede senhas; conscientização e verificação de identidade de quem liga reduzem o risco. Não confundir com força bruta, que tenta adivinhar senhas.

Dano direto x dano indireto

Dano direto atinge o próprio ativo: notebooks roubados, servidor e cabos queimados. Dano indireto são as consequências: perda de clientes e receita, notícia negativa, contratos não fechados e multas por descumprir lei de proteção de dados.

Proprietário do risco

Pela ISO/IEC 27001, é quem tem autoridade para gerenciar o risco. Cada risco identificado deve ter um proprietário, que decide sobre o tratamento dentro dos critérios da organização e aceita os riscos residuais.

Gestão de riscos: sequência

Identificar, analisar, avaliar e tratar os riscos, e depois monitorar. O processo é contínuo e revisto periodicamente e após mudanças relevantes. Comprar controles antes de identificar riscos inverte a ordem.

Avaliação de riscos (risk assessment)

Na ISO/IEC 27001, é formada por identificação, análise e avaliação dos riscos. A avaliação compara os riscos analisados com os critérios de aceitação para priorizar o tratamento.

Análise de riscos: objetivo e primeiro passo

O objetivo é equilibrar o custo de um incidente com o custo dos controles, para decidir o tratamento adequado. O primeiro passo costuma ser identificar os ativos e o valor deles; depois, ameaças e vulnerabilidades, e a estimativa de probabilidade e impacto. Implementar medidas e controles não é objetivo da análise de riscos; isso vem no tratamento.

Análise qualitativa x quantitativa

Qualitativa classifica em alto, médio e baixo, sem valores em dinheiro; é mais rápida e usa percepção e experiência. Quantitativa traduz riscos em valores (SLE, ARO, ALE) para comparar custo e benefício, mas é mais trabalhosa, exige dados históricos confiáveis e ainda tem estimativas.

SLE (expectativa de perda por ocorrência)

Perda esperada em uma ocorrência: valor do ativo x fator de exposição (parcela do valor perdida). Ativo de R$ 100.000 com 30% destruído dá SLE de R$ 30.000.

ARO e ALE

ARO é a taxa anual de ocorrência: uma vez a cada dois anos = 0,5; uma vez a cada quatro anos = 0,25. ALE (expectativa de perda anual) = SLE x ARO e ajuda a decidir quanto investir: um controle que custa mais que a ALE por ano precisa de outra justificativa.

Estratégias de risco na terminologia EXIN

Aceitar o risco (risk bearing): decisão consciente de não investir em controles e arcar com o prejuízo, comum quando o controle custa mais que o dano. Neutro ao risco (risk neutral): adotar medidas para que a ameaça não se manifeste ou, se ocorrer, o dano seja mínimo. Evitar o risco (risk avoiding): neutralizar a ameaça, por exemplo deixando de realizar a atividade.

Opções de tratamento de risco

Modificar (mitigar): controles para reduzir probabilidade ou impacto, como antivírus e treinamento. Reter (aceitar), evitar (encerrar a atividade, como deixar de aceitar envio de arquivos no site) e compartilhar (seguro contra ataques cibernéticos). Seguro não impede o incidente, só reduz o impacto financeiro; as opções costumam ser combinadas.

Risco residual

Parte do risco que resta depois de aplicar os controles. Deve ser aceito formalmente pela gestão (proprietários do risco) e continua sendo monitorado; não é zero nem passa automaticamente ao fornecedor.

Macetes para memorizar

💡 Cadeia do risco

Ameaça + vulnerabilidade = risco; ameaça concretizada = incidente; consequência = dano.

💡 Fórmulas

SLE = Valor x Exposição; ALE = SLE x ARO. 'Uma vez a cada N anos' → ARO = 1/N.

Estratégias EXIN

Bearing = Banca o prejuízo (sem medidas). Neutral = faz medidas. Avoiding = Abandona (neutraliza a ameaça).

Tratamento ISO

MREC: Modificar, Reter, Evitar, Compartilhar. Seguro = compartilhar; antivírus = modificar; parar = evitar.

Dano

Direto = no ativo; indireto = no negócio (clientes, imagem, multa).

Sequência da gestão de riscos

I-A-A-T-M: Identificar, Analisar, Avaliar, Tratar, Monitorar.

Tabela de memorização: não confunda

Quando é...	...e quando é
Ameaça Quem ou o que pode causar o incidente (invasor, raio, erro humano).	**Vulnerabilidade** A fraqueza explorada (porta que não fecha, software sem correção).
Dano direto Atinge o próprio ativo: equipamento roubado ou destruído.	**Dano indireto** Consequência: perda de clientes, receita, reputação, multa.
Ameaça humana intencional Houve intenção: sabotagem de ex-funcionário, fraude.	**Ameaça humana não intencional** Erro sem intenção: apagar uma pasta por engano.
Aceitar o risco (risk bearing) Não adota medidas e arca com o eventual prejuízo, de forma consciente.	**Neutro ao risco (risk neutral)** Adota medidas para a ameaça não se manifestar ou para o dano ser mínimo.
Evitar o risco Encerra a atividade que gera o risco.	**Compartilhar o risco** A atividade continua e o impacto financeiro é dividido com terceiros (seguradora).
Análise qualitativa Alto, médio e baixo, sem valores monetários; mais rápida.	**Análise quantitativa** Valores em dinheiro (SLE, ARO, ALE) para comparar custo e benefício; exige dados.

Números que caem

Item	Valor
Peso do domínio na prova	**12,5% (cerca de 5 das 40)**
ALE	**SLE x ARO**
SLE	**Valor do ativo x fator de exposição**
ARO de uma ocorrência a cada dois anos	**0,5**

ARO de uma ocorrência a cada quatro anos	**0,25**
Exemplo: ativo de R$ 100.000 com 30% de exposição	**SLE = R$ 30.000**
Exemplo: SLE R$ 20.000 e ARO 2	**ALE = R$ 40.000**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Multa, perda de clientes ou notícia negativa são dano direto.
Como não cair: São consequências: dano indireto. Direto é o que atinge o próprio ativo.

⚠ **Alerta de prova:** Porta de emergência entreaberta é uma ameaça ou já é um dano.
Como não cair: Nenhum dano ocorreu e ela é uma fraqueza: vulnerabilidade. A ameaça é quem entraria por ela.

⚠ **Alerta de prova:** Software com falha conhecida e sem correção é uma ameaça de ataque externo.
Como não cair: Ameaça é quem ou o que explora; a falha em si é vulnerabilidade técnica.

⚠ **Alerta de prova:** O incidente é a fraqueza que a ameaça explora.
Como não cair: Fraqueza é vulnerabilidade; incidente é a ameaça que se concretizou; dano é o prejuízo depois.

⚠ **Alerta de prova:** Raio que queima equipamentos é vulnerabilidade técnica ou ameaça humana.
Como não cair: É um evento sem ação humana: ameaça não humana.

⚠ **Alerta de prova:** Ligação fingindo ser do suporte para pedir senha é ataque de força bruta.
Como não cair: Não tenta adivinhar senhas; manipula a pessoa: engenharia social.

⚠ **Alerta de prova:** Decidir não investir em controles e arcar com o prejuízo é estratégia neutra ou evitar o risco.
Como não cair: Neutro adota medidas; evitar neutraliza a ameaça. Não fazer nada, conscientemente, é aceitar (risk bearing).

⚠ **Alerta de prova:** Contratar seguro é evitar o risco ou eliminar a ameaça.
Como não cair: A atividade continua e o ataque ainda pode ocorrer; seguro é compartilhar o risco.

⚠ **Alerta de prova:** Instalar antivírus e treinar funcionários é aceitar ou compartilhar o risco.
Como não cair: Foram adotadas medidas para reduzir a probabilidade, sem transferência: é modificar (mitigar).

⚠ **Alerta de prova:** Uma vez a cada dois anos com perda de R$ 8.000 dá ALE de R$ 8.000 ou R$ 16.000.
Como não cair: ARO = 0,5, então ALE = 8.000 x 0,5 = R$ 4.000. R$ 8.000 seria uma vez por ano.

⚠ **Alerta de prova:** Na conta da ALE, R$ 20.000 por ocorrência e duas vezes por ano dá R$ 10.000 ou R$ 20.000.
Como não cair: Multiplique, não divida: 20.000 x 2 = R$ 40.000. R$ 20.000 é só o SLE.

⚠ **Alerta de prova:** Com ativo de R$ 100.000 e exposição de 30%, o SLE é R$ 70.000 ou R$ 130.000.
Como não cair: SLE = valor x fator de exposição = R$ 30.000. 70.000 é o que resta; 130.000 é soma.

⚠ **Alerta de prova:** Análise quantitativa é mais rápida e elimina a subjetividade.
Como não cair: Ela costuma ser mais trabalhosa, exige dados históricos e ainda tem estimativas; a qualitativa é que é mais rápida.

⚠ **Alerta de prova:** O risco residual é zero ou passa automaticamente ao fornecedor.
Como não cair: Sempre sobra risco; o residual é aceito formalmente pela gestão e continua monitorado.

⚠ **Alerta de prova:** A água usada para apagar um incêndio é dano direto, como o servidor queimado.
Como não cair: Para a EXIN, o dano por água do combate ao fogo é dano indireto (efeito colateral de conter o incêndio); o que o fogo destruiu (servidor, documentos, fitas de backup) é dano direto.

⚠ **Alerta de prova:** Implementar medidas e controles é um dos objetivos da análise de riscos.
Como não cair: A análise identifica ativos e valor, ameaças e vulnerabilidades e equilibra custo do incidente x custo do controle; implementar é tratamento.

Como cai na prova

📝 **Como cai:** Cálculo de SLE, ARO ou ALE com valores redondos
Como resolver: Converta a frequência em ARO (uma vez a cada 2 anos = 0,5; a cada 4 = 0,25; duas vezes por ano = 2). Multiplique SLE x ARO. Os distratores são o próprio SLE, a divisão em vez da multiplicação, a soma ou o valor que resta.

📝 **Como cai:** Cenário + 'que tipo de ameaça é essa?'
Como resolver: Houve pessoa? Se não, não humana. Se sim, houve intenção? Intencional ou não intencional. Se a pessoa foi manipulada para entregar algo, engenharia social.

📝 **Como cai:** Cenário + 'qual estratégia/opção de tratamento?'
Como resolver: Veja o que a empresa fez: nada e arca com o prejuízo (aceitar), adotou controles (neutro/modificar), parou a atividade (evitar), contratou seguro (compartilhar).

📝 **Como cai:** 'Qual destes é dano direto/indireto?' ou 'como classificar essa situação?'
Como resolver: Pergunte se é o ativo em si (direto) ou consequência para o negócio (indireto). Se nada aconteceu ainda e é uma fraqueza, é vulnerabilidade.

📝 **Como cai:** 'Qual é a sequência/etapas da gestão ou avaliação de riscos?'
Como resolver: Gestão: identificar, analisar, avaliar, tratar, monitorar. Avaliação de riscos (ISO/IEC 27001): identificação, análise e avaliação. Riscos sempre vêm antes da compra de controles.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
ex-funcionário apaga arquivos de propósito	**Ameaça humana intencional**
funcionário apaga sem querer	**Ameaça humana não intencional**
raio, incêndio, inundação, tempestade	**Ameaça não humana**
fingir ser do suporte e pedir a senha	**Engenharia social**
porta que não fecha, falha sem correção	**Vulnerabilidade**
grupo criminoso que tenta invadir	**Agente de ameaça**
custo do equipamento levado ou destruído	**Dano direto**
perda de clientes, imagem, multa após vazamento	**Dano indireto**
decide não investir e arcar com o prejuízo	**Aceitar o risco (risk bearing)**
deixa de oferecer o serviço por causa do risco	**Evitar o risco**
contrata seguro	**Compartilhar o risco**
alto, médio e baixo, sem valores em dinheiro	**Análise qualitativa**
risco que sobra depois dos controles	**Risco residual, aceito formalmente pela gestão**

quem tem autoridade para gerenciar o risco	**Proprietário do risco**
hospital, dano a pacientes é inaceitável	**Evitar o risco (risk avoiding)**

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

- ALE = SLE x ARO; 'uma vez a cada N anos' significa ARO = 1/N.
- Multa e perda de clientes são dano indireto; equipamento perdido é dano direto.
- Aceitar (risk bearing) não adota medidas; neutro adota medidas; seguro é compartilhar.
- Fraqueza é vulnerabilidade; quem explora é ameaça (agente de ameaça); ameaça concretizada é incidente.
- Risco residual é aceito formalmente pela gestão e continua monitorado.

Essenciais para a prova (checklist)

- ☐ Sei classificar uma ameaça como humana intencional, humana não intencional ou não humana.
- ☐ Sei diferenciar ameaça, agente de ameaça, vulnerabilidade, risco, incidente e dano.
- ☐ Sei separar dano direto de dano indireto em um cenário.
- ☐ Sei calcular SLE, ARO e ALE de cabeça.
- ☐ Sei diferenciar análise qualitativa de quantitativa e citar vantagens e limites de cada uma.
- ☐ Sei as estratégias EXIN (aceitar, neutro, evitar) e as opções de tratamento (modificar, reter, evitar, compartilhar).
- ☐ Sei a sequência da gestão de riscos e as etapas da avaliação de riscos na ISO/IEC 27001.
- ☐ Sei o que é proprietário do risco e risco residual.

Questões de revisão do capítulo

R1.1 · Ameaças e Riscos

Qual costuma ser o primeiro passo de uma análise de riscos?

A. Comprar os controles mais modernos disponíveis no mercado
B. Demitir quem causou o último incidente
C. Identificar os ativos e o valor deles para a organização
D. Aceitar todos os riscos para ganhar tempo

R1.2 · Ameaças e Riscos

Segundo a abordagem EXIN, qual estratégia adota medidas para que a ameaça não se manifeste ou, se ocorrer, o dano seja mínimo?

A. Concentração do risco
B. Estratégia neutra ao risco
C. Ignorância do risco
D. Aceitação do risco

R1.3 · Ameaças e Riscos

Qual é a relação entre ameaça e incidente?

A. O incidente é a fraqueza que a ameaça explora
B. O incidente é a ameaça que de fato se concretizou
C. A ameaça é o prejuízo depois que o incidente acaba
D. São a mesma coisa, com nomes diferentes

R1.4 · Ameaças e Riscos

Qual é uma vantagem da análise de riscos quantitativa em relação à qualitativa?

A. Traduz os riscos em valores para comparar custo e benefício
B. É mais rápida e mais simples de fazer que a qualitativa
C. Dispensa dados históricos e estimativas de valor dos ativos
D. Elimina a subjetividade das estimativas envolvidas

Respostas comentadas

R1.1. C) Identificar os ativos e o valor deles para a organização

Por quê: Com os ativos e seus valores, identificam-se ameaças e vulnerabilidades e estimam-se probabilidade e impacto.

✗ A) Incorreta. Vem depois da análise.
✗ B) Incorreta. Não é análise.
✗ D) Incorreta. Não é análise.

> **Dica de prova:** Análise de riscos começa pelos ativos.

R1.2. B) Estratégia neutra ao risco

Por quê: Na terminologia EXIN, as estratégias são aceitar o risco (risk bearing), ser neutro ao risco (risk neutral) e evitar o risco (risk avoiding).

✗ A) Incorreta. Não é estratégia de gestão.
✗ C) Incorreta. Não é estratégia de gestão.
✗ D) Incorreta. Aceitar não adota medidas.

> **Dica de prova:** Neutro: medidas para não ocorrer ou reduzir dano.

R1.3. B) O incidente é a ameaça que de fato se concretizou

Por quê: No ciclo do incidente, uma ameaça se transforma em incidente, que pode causar dano e exigir recuperação.

✗ A) Incorreta. Isso é vulnerabilidade.
✗ C) Incorreta. Isso é dano.
✗ D) Incorreta. São conceitos diferentes.

> **Dica de prova:** Ameaça concretizada = incidente.

R1.4. A) Traduz os riscos em valores para comparar custo e benefício

Por quê: A análise quantitativa usa valores como SLE, ARO e ALE, mas depende de dados confiáveis, que nem sempre existem.

✗ B) Incorreta. Costuma ser mais trabalhosa.
✗ C) Incorreta. Exige esses dados.
✗ D) Incorreta. Ainda há estimativas.

> **Dica de prova:** Quantitativa: valores para decidir.

02

CAPÍTULO 2 · 52,5% DA PROVA

Controles de Segurança

É o maior domínio, com 52,5% da prova (cerca de 21 das 40), então é o domínio que mais pesa no resultado. Cobre os tipos de controle (preventivo, detectivo, repressivo, corretivo, de seguro) e os quatro temas da ISO/IEC 27002:2022: organizacionais (classificação, acesso, incidentes, continuidade, auditorias), de pessoas (triagem, contratos, NDA, conscientização), físicos (anéis de proteção, entrada, ambiente, descarte) e tecnológicos (malware, rede, criptografia, logs, desenvolvimento seguro). O formato típico é um cenário com 'qual controle é esse?' ou 'o que fazer?', e os distratores costumam ser controles de outra categoria ou ações que aumentam o risco. Onde mais erro: repressivo x corretivo, autenticação x autorização, escalonamento funcional x hierárquico, e a chave certa na criptografia assimétrica.

Neste capítulo

18 tópicos-chave · 16 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Tipos de controle e estrutura da ISO/IEC 27002:2022

Preventivo atua antes do incidente (fechadura). Detectivo identifica (alarme, detector de fumaça, análise de logs). Repressivo contém o dano em curso (extintor). Corretivo recupera depois (restaurar backup). De seguro cobre o prejuízo financeiro (apólice). A classificação usada no ISFS também cita medidas redutivas. 93 controles em quatro temas: organizacionais, de pessoas, físicos e tecnológicos. A edição de 2022 usa atributos como tipo de controle (preventivo, detectivo, corretivo) e propriedade de segurança. Os 14 domínios eram a estrutura da edição de 2013.

Classificação e rotulagem da informação

Antes de classificar, inventariar os ativos e definir proprietários. Quem decide a classificação é o proprietário, considerando CIA e requisitos legais. O esquema costuma ter poucos níveis (público, interno, confidencial, secreto) para ser fácil de aplicar; a norma não fixa o número. A rotulagem mostra a classificação, cada nível tem regras de manuseio (ex.: confidencial só sai por e-mail cifrado) e a classificação é revista quando o valor muda.

Identificação, autenticação e autorização

Identificação diz quem é; autenticação comprova (valida a senha); autorização concede os acessos permitidos (quais pastas pode abrir). Cada pessoa deve ter identidade única para garantir responsabilização e revogação individual.

Princípios e gestão de direitos de acesso

Necessidade de conhecer (need-to-know): só quem precisa vê, como salários só para o RH da folha. Menor privilégio: só os acessos necessários à tarefa. RBAC concede acesso pelo papel/cargo. O proprietário da informação aprova o pedido e a TI executa; direitos são revisados periodicamente (mudança de área) e removidos imediatamente no desligamento.

Autenticação segura e acesso privilegiado

Senha provisória deve ser trocada no primeiro acesso. Bloqueio após tentativas erradas dificulta força bruta; MFA combina algo que você sabe, tem e é, e protege mesmo com a senha roubada. Conta de administrador só para tarefas administrativas, para limitar o dano se for comprometida, com uso registrado; acesso ao código-fonte também é controlado.

Gestão de incidentes e escalonamento

Papéis, responsabilidades e procedimentos são definidos antes do incidente. Fraquezas e eventos são relatados pelo canal definido, sem tentar explorar ou investigar sozinho; em geral o primeiro contato é o helpdesk, que avalia e escala se preciso (não se escala direto para a gestão). O registro precisa ter, no mínimo, o nome de quem relatou. O evento relatado é avaliado para decidir se é incidente; a resposta começa pela contenção (isolar a máquina da rede), depois erradicação e recuperação, preservando evidências com cadeia de custódia. No fim, aprender com o incidente para evitar repetição. Funcional: o caso vai para quem tem mais conhecimento técnico (service desk passa para a equipe de redes). Hierárquico: o caso sobe para quem tem mais autoridade, quando é preciso uma decisão de gestão (desligar o site de vendas).

Vulnerabilidades, ameaças e projetos

Correção para falha já explorada deve ser avaliada e aplicada com prioridade; sem correção, aplicam-se medidas alternativas. Inteligência de ameaças coleta e analisa informações sobre campanhas de ataque para ajustar controles. Em projetos, os requisitos de segurança entram desde o início e em todas as fases.

Continuidade de negócios (BCM, BIA, DRP) e sites de contingência

BCM mantém as atividades críticas durante e após um desastre. A BIA identifica os processos críticos e quanto tempo podem ficar parados. O plano de continuidade trata do negócio como um todo; o DRP foca em restaurar sistemas e infraestrutura de TI. Os planos são testados regularmente, e a segurança adequada deve ser mantida durante a crise. Site quente (hot site): já equipado e sincronizado, assume em minutos; mais caro e rápido. Site frio (cold site): só espaço, energia e rede, sem equipamentos; ativação pode levar dias; mais barato e lento. A escolha depende do tempo de recuperação exigido.

Auditorias e revisões

Revisões independentes, por auditores internos ou externos, verificam se a abordagem de segurança continua adequada e eficaz, em intervalos planejados ou após mudanças. Os gestores de cada área verificam regularmente o cumprimento das políticas. Testes de auditoria em produção são planejados com a gestão, com acesso somente leitura quando possível.

Controles de pessoas

Triagem (screening) antes da contratação, proporcional ao cargo, à informação acessada e aos riscos, respeitando a lei. Responsabilidades de segurança ficam nos termos e condições do contrato de trabalho, inclusive para temporários; NDA define o que é confidencial, usos, duração do sigilo e consequências. Processo disciplinar formal e conhecido antes trata violações; o dever de confidencialidade continua após a saída; trabalho remoto exige política própria. O código de conduta, aceito pelos funcionários, define o comportamento esperado; uma regra que proíbe usar o e-mail da empresa para fins pessoais fica nele.

Conscientização, educação e treinamento

Começa na integração e continua de forma periódica, com exemplos do dia a dia e conteúdo adaptado a cada função (codificação segura para desenvolvedores). Inclui reconhecer e relatar phishing, tailgating e outras formas de engenharia social, e comunicar logo a perda de crachás e tokens. Phishing simulado serve para conscientizar e medir a evolução, não para punir.

Anéis de proteção e entrada física

De fora para dentro: anel externo (terreno, cerca, iluminação, portão), prédio (portaria e recepção), espaço de trabalho (sala ou andar trancado) e objeto (cofre, armário trancado; no inglês, secure room), cada um com controles próprios. Controle de entrada física usa cartão, biometria e registro; crachás visíveis ajudam a identificar intrusos; visitantes são registrados e acompanhados; eclusa (mantrap) evita a entrada de carona; área de entrega fica separada; sala de servidores é discreta, sem placa.

Proteção de equipamentos e áreas seguras

Incêndio em sala de servidores: extinção por gás (sprinkler de água danifica). Não instalar servidor em subsolo sujeito a enchente, embaixo de tubulações ou perto de janelas. Serviços de apoio (energia, climatização) com nobreak para quedas rápidas e geradores para faltas longas; cabos de energia e dados protegidos e separados; manutenção só por técnicos autorizados e registrada. Em áreas seguras, sem fotos ou gravações sem autorização; mesa limpa e tela limpa; notebook fora da empresa nunca sem vigilância.

Mídias, descarte, proteção de dados e backup

Pendrive com informação confidencial: cifrar e controlar o uso conforme a classificação. Papel confidencial vai para fragmentadora; discos doados precisam de apagamento seguro (sobrescrita ou apagamento criptográfico) ou destruição, porque excluir ou formatar não basta. Dados fora do prazo de guarda são excluídos com segurança, inclusive backups e cópias em terceiros. Hardening troca senhas padrão e remove serviços desnecessários; gestão de capacidade monitora recursos; usuários comuns não instalam programas. Mascaramento oculta parte do dado (4111 XXXX XXXX 1234); DLP bloqueia a saída de dado sensível por e-mail, web, dispositivos e nuvem. Backup só dá garantia se a restauração for testada; contra ransomware, backups atualizados, isolados e testados. Redundância (dois servidores com failover) aumenta a disponibilidade.

Malware, phishing e spam

Worm se espalha sozinho explorando vulnerabilidades; vírus precisa de hospedeiro e ação do usuário; cavalo de Troia parece legítimo e executa funções ocultas; spyware coleta dados do usuário (keylogger é um tipo); botnet são máquinas zumbis controladas remotamente, usadas em spam e DDoS; ransomware cifra arquivos e pede pagamento. Phishing usa urgência, ameaça, link e pedido de dados. Controles: antimalware com assinaturas atualizadas, filtro antispam, filtragem web por categoria e conscientização.

Segurança de redes e registros

Firewall filtra tráfego conforme regras e separa zonas; segregação de redes isola visitantes da rede interna; VPN cifra o tráfego em Wi-Fi público; IDS detecta e alerta, IPS também bloqueia. Logs protegidos contra alteração servem como evidência; relógios sincronizados permitem correlacionar logs; monitoramento de atividades compara com uma linha de base e alerta sobre comportamento anômalo.

Criptografia

Simétrica usa a mesma chave e é rápida; o desafio é distribuir a chave com segurança, por isso a assimétrica costuma ser usada para trocá-la. Para sigilo, cifra-se com a chave pública do destinatário; para assinatura digital, o remetente assina com a própria chave privada e todos verificam com a pública dele, garantindo autenticidade e integridade (não sigilo). A autoridade certificadora da PKI emite e revoga certificados que ligam chave pública ao dono; HTTPS (TLS) protege sigilo e integridade dos dados em trânsito.

Desenvolvimento seguro

Defesa em profundidade: várias camadas (firewall, segmentação, MFA, criptografia). Codificação segura valida entradas contra injeção de SQL. Testes de segurança antes da aceitação; ambientes de desenvolvimento, teste e produção separados; gestão de mudanças com aprovação, teste, registro e plano de retorno. Dados de teste reais devem ser protegidos ou anonimizados; no desenvolvimento terceirizado, a empresa define requisitos e verifica a entrega.

Macetes para memorizar

💡 Tipos de controle na linha do tempo

Antes: Preventivo. Na hora: Detectivo (vê) e Repressivo (segura). Depois: Corretivo (conserta). Dinheiro: Seguro.

💡 Acesso em 3 passos

Quem é você? (identificação) Prove! (autenticação) O que pode? (autorização).

💡 Chaves na assimétrica

Segredo para alguém: pública DELE. Assinatura minha: privada MINHA.

💡 Anéis de proteção

Terreno → Prédio → Sala → Cofre (externo, prédio, espaço de trabalho, objeto).

💡 Escalonamento

Funcional = quem SABE mais; hierárquico = quem MANDA mais.

💡 Sites de contingência

Quente = pronto e caro; frio = vazio e barato.

Resposta a incidentes

Relatar → Avaliar → Conter → Erradicar → Recuperar → Aprender (com cadeia de custódia nas evidências).

Tabela de memorização: não confunda

Quando é...	...e quando é
Preventivo Impede que o incidente aconteça: fechadura, bloqueio de conta.	**Detectivo** Identifica o incidente: alarme da porta fora do horário, detector de fumaça, análise de logs.
Repressivo Contém o dano enquanto ocorre: extintor no princípio de incêndio.	**Corretivo** Recupera depois do dano: restaurar sistemas a partir do backup.
Autenticação Comprova que o usuário é quem diz ser (validar a senha).	**Autorização** Define o que ele pode acessar depois de autenticado (quais pastas abrir).
IDS Detecta padrões de ataque e alerta.	**IPS** Detecta e também bloqueia o ataque.
Worm Espalha-se sozinho pela rede, sem o usuário executar nada.	**Cavalo de Troia** Disfarça-se de programa legítimo e depende de o usuário instalar.
Site quente (hot site) Já equipado e sincronizado, assume em minutos; mais caro.	**Site frio (cold site)** Só espaço, energia e rede, sem equipamentos; leva dias; mais barato.
Escalonamento funcional Vai para um especialista técnico (service desk para a equipe de redes).	**Escalonamento hierárquico** Sobe para autoridade de gestão quando é preciso decidir (desligar o site de vendas).

Números que caem

Item	Valor
Peso do domínio na prova	**52,5% (cerca de 21 das 40)**
Visão geral dos controles (3.1)	**2,5%**
Controles organizacionais (3.2)	**15%**
Controles de pessoas (3.3)	**7,5%**

Controles físicos (3.4)	**10%**
Controles tecnológicos (3.5)	**17,5%**
ISO/IEC 27002:2022	**4 temas e 93 controles**
Anéis de proteção	**4 (externo, prédio, espaço de trabalho, objeto)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Extintor é corretivo porque resolve o problema.
Como não cair: Extintor contém o dano em curso: é repressivo. Corretivo recupera depois (restaurar backup).

⚠ **Alerta de prova:** Restaurar backup após ataque é preventivo ou detectivo.
Como não cair: O ataque já aconteceu e nada é detectado; restaurar é corretivo.

⚠ **Alerta de prova:** Apólice contra incêndio é medida preventiva ou repressiva.
Como não cair: Não evita nem combate o fogo; cobre o prejuízo: é medida de seguro.

⚠ **Alerta de prova:** Verificar quais pastas o usuário pode abrir é autenticação.
Como não cair: Autenticação confirma quem é; o que pode acessar é autorização.

⚠ **Alerta de prova:** Para mandar uma mensagem sigilosa, cifra-se com a chave privada do remetente.
Como não cair: Chave privada do remetente serve para assinar. Sigilo: chave pública do destinatário.

⚠ **Alerta de prova:** Assinatura digital garante o sigilo do conteúdo.
Como não cair: Assinatura não cifra; garante autenticidade do autor e integridade do conteúdo.

⚠ **Alerta de prova:** A autoridade certificadora guarda as chaves privadas dos usuários.
Como não cair: A chave privada fica com o dono; a autoridade certificadora emite e revoga certificados.

⚠ **Alerta de prova:** Criptografia simétrica é mais lenta que a assimétrica.
Como não cair: Costuma ser mais rápida; o desafio dela é distribuir a mesma chave com segurança.

⚠ **Alerta de prova:** A ISO/IEC 27002 organiza os controles em 14 domínios ou exige exatamente quatro níveis de classificação.
Como não cair: 14 domínios era a edição de 2013; a de 2022 tem 4 temas e 93 controles. A norma não fixa o número de níveis de classificação.

⚠ **Alerta de prova:** Sprinklers de água comuns são a melhor proteção contra incêndio na sala de servidores.
Como não cair: Água danifica os equipamentos; o adequado é extinção por gás.

⚠ **Alerta de prova:** Ao perceber uma fraqueza ou malware, o funcionário deve testar, investigar sozinho ou formatar a máquina.
Como não cair: Relatar pelo canal definido o quanto antes, sem explorar; testar pode causar dano e destruir evidências.

⚠ **Alerta de prova:** Na resposta a malware, reinstalar o sistema na hora é o primeiro passo.
Como não cair: Primeiro conter (isolar o computador da rede), preservando evidências; depois erradicação e recuperação.

⚠ **Alerta de prova:** Triagem deve ser igual para todos, com investigação máxima em qualquer cargo.
Como não cair: A verificação é proporcional ao cargo, à informação acessada e aos riscos, e respeita a lei.

⚠ **Alerta de prova:** O acesso de quem foi demitido pode ser removido na próxima revisão anual ou após 30 dias.
Como não cair: Remoção imediata, no momento do desligamento; a revisão periódica serve para mudanças de área.

⚠ **Alerta de prova:** Transferir a equipe para um escritório reserva (stand-by arrangement) depois de um incêndio é medida corretiva.
Como não cair: É medida repressiva: limita o dano. No ciclo do incidente, fica entre o incidente e o dano; a recuperação vem depois.

⚠ **Alerta de prova:** 'Anel do meio' (middle ring) é um dos anéis de proteção.
Como não cair: Os quatro anéis são externo, prédio, espaço de trabalho e objeto (no inglês, secure room); anel do meio não existe.

Como cai na prova

📝 **Como cai:** Cenário + 'que tipo de controle é esse?' (preventivo, detectivo, repressivo, corretivo, de seguro)
Como resolver: Coloque a medida na linha do tempo do incidente: impede antes, percebe, contém durante, recupera depois ou paga o prejuízo. Elimine pelo critério: não impede, não detecta, não contém, não recupera.

📝 **Como cai:** Cenário + 'qual controle está sendo aplicado?' com nomes da ISO/IEC 27002
Como resolver: Identifique o tema do cenário (pessoas, físico, tecnológico, organizacional). Os distratores quase sempre são controles de outro tema ('é controle físico', 'é controle de pessoas'), então elimine os que não combinam.

📝 **Como cai:** 'O que o funcionário/organização deve fazer?' diante de situação de risco
Como resolver: Elimine toda alternativa que aumenta o risco (emprestar crachá, desligar antivírus, esperar, ignorar, apagar evidências). Sobra a que relata, controla, registra ou remove acesso de imediato.

📝 **Como cai:** Malware ou ataque descrito por comportamento
Como resolver: Leia o verbo: espalha sozinho (worm), finge ser útil (Troia), espiona (spyware), controla máquinas (botnet), cifra e cobra (ransomware), urgência com link (phishing).

📝 **Como cai:** Criptografia: 'qual chave?' ou 'o que garante?'
Como resolver: Defina o objetivo: sigilo usa a pública do destinatário; assinatura usa a privada do remetente e garante autor e integridade; TLS protege dados em trânsito, não os guardados no disco.

📝 **Como cai:** Anéis de proteção: 'qual anel?'
Como resolver: Localize o elemento de fora para dentro: área ao redor (externo), edifício e recepção (prédio), sala ou andar (espaço de trabalho), cofre ou armário (objeto). Rede lógica não é anel físico.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
alarme, detector de fumaça, análise de logs	**Controle detectivo**
extintor, limitar o dano em curso	**Controle repressivo**
restaurar a partir do backup	**Controle corretivo**
apólice, cobrir prejuízo	**Medida de seguro**
só a equipe que processa a folha vê os salários	**Necessidade de conhecer (need-to-know)**
acessos concedidos pelo cargo (analista financeiro, vendedor)	**RBAC**
duas portas em sequência, uma só abre após a outra fechar	**Eclusa (mantrap) contra entrada de carona**
cerca, iluminação, portão / recepção / sala trancada / cofre	**Anel externo / prédio / espaço de trabalho / objeto**

senha padrão do fabricante e serviços desnecessários ativos	**Gestão de configuração (hardening)**
dígitos do meio ocultos em dados de teste	**Mascaramento de dados**
bloqueia envio de números de cartão para e-mail externo	**DLP (prevenção de vazamento de dados)**
se espalha sozinho / parece legítimo / coleta senhas / máquinas zumbis / cifra e pede resgate	**Worm / cavalo de Troia / spyware / botnet / ransomware (backup isolado e testado)**
processos críticos e quanto tempo podem ficar parados	**BIA (análise de impacto nos negócios)**
validar entradas contra injeção de SQL	**Codificação segura**

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

- Extintor é repressivo; restaurar backup é corretivo; alarme é detectivo; fechadura é preventiva; apólice é seguro.
- Sigilo: chave pública do destinatário. Assinatura: chave privada do remetente (autor + integridade, sem sigilo).
- Acesso de quem sai é removido imediatamente; quem decide classificação e aprova acesso é o proprietário.
- Diante de fraqueza ou suspeita: relatar logo pelo canal definido, nunca testar ou investigar sozinho.
- Backup só vale se a restauração for testada; contra ransomware, backup isolado.

Essenciais para a prova (checklist)

☐ Sei classificar uma medida como preventiva, detectiva, repressiva, corretiva ou de seguro.

☐ Sei os 4 temas da ISO/IEC 27002:2022 e encaixar um controle no tema certo.

☐ Sei diferenciar identificação, autenticação e autorização, e need-to-know, menor privilégio e RBAC.

☐ Sei a ordem da resposta a incidentes e a diferença entre escalonamento funcional e hierárquico.

☐ Sei a diferença entre BCM, BIA e DRP, e entre site quente e site frio.

☐ Sei os controles de pessoas: triagem proporcional, contrato, NDA com duração, processo disciplinar, deveres após a saída.

☐ Sei localizar um controle físico no anel certo e citar controles de entrada, ambiente e descarte.

☐ Sei distinguir worm, vírus, cavalo de Troia, spyware, botnet e ransomware.

☐ Sei qual chave usar para sigilo e para assinatura, o papel da autoridade certificadora e o que o TLS protege.

☐ Sei a função de firewall, VPN, segregação de redes, IDS/IPS, DLP, mascaramento, logs e sincronização de relógios.

Questões de revisão do capítulo

R2.1 · Controles de Segurança

Os resultados trimestrais eram confidenciais até serem divulgados oficialmente ao mercado. O que deve acontecer com a classificação depois da divulgação?

A. Ser apagada, pois informação pública não é ativo
B. Ser revista, pois o valor e o sigilo mudaram
C. Continuar confidencial, pois a classificação nunca muda
D. Ser elevada a secreta, para evitar novos vazamentos

R2.2 · Controles de Segurança

Após cinco tentativas de senha erradas, a conta do usuário é bloqueada por alguns minutos. Qual ataque esse controle dificulta?

A. Furto de notebooks no aeroporto
B. Inundação da sala de servidores
C. Ataque de força bruta às senhas
D. Falha de energia no centro de dados

R2.3 · Controles de Segurança

Uma arquitetura usa firewall, segmentação de rede, MFA e criptografia em camadas. Qual princípio de engenharia segura ela aplica?

A. Segurança por obscuridade
B. Ponto único de controle
C. Confiança implícita na rede interna
D. Defesa em profundidade

R2.4 · Controles de Segurança

Qual tema deve fazer parte do programa de conscientização em segurança da informação?

A. Como compartilhar senhas de forma rápida
B. Como desativar o antivírus para ganhar desempenho
C. Como burlar o bloqueio de sites da empresa
D. Como reconhecer e relatar incidentes, como phishing

Respostas comentadas

R2.1. B) Ser revista, pois o valor e o sigilo mudaram

Por quê: Manter informação superclassificada gera custo desnecessário; subclassificá-la gera risco. A revisão deve ser prevista.

✗ A) Incorreta. Informação pública continua sendo ativo.
✗ C) Incorreta. A classificação pode mudar.
✗ D) Incorreta. Não faz sentido após a divulgação.

> **Dica de prova:** Valor mudou: revisar a classificação.

R2.2. C) Ataque de força bruta às senhas

Por quê: Procedimentos de login seguros também incluem MFA, mensagens de erro que não revelam detalhes e registro de tentativas.

✗ A) Incorreta. Não tem relação.
✗ B) Incorreta. Não tem relação.
✗ D) Incorreta. Não tem relação.

> **Dica de prova:** Bloqueio por tentativas: contra força bruta.

R2.3. D) Defesa em profundidade

Por quê: Se uma camada falhar, as outras continuam protegendo; esse é um dos princípios de arquitetura segura da ISO/IEC 27002.

✗ A) Incorreta. Não é o princípio aplicado.
✗ B) Incorreta. É o oposto.
✗ C) Incorreta. É o oposto.

> **Dica de prova:** Camadas de proteção: defesa em profundidade.

R2.4. D) Como reconhecer e relatar incidentes, como phishing

Por quê: O programa também trata de políticas, senhas, mesa limpa, uso de dispositivos, trabalho remoto e proteção de dados pessoais.

✗ A) Incorreta. Aumenta o risco.
✗ B) Incorreta. Aumenta o risco.
✗ C) Incorreta. Aumenta o risco.

> **Dica de prova:** Conscientização: reconhecer e relatar.

03

CAPÍTULO 3 · 27,5% DA PROVA

Informação e Segurança

Este é o alicerce da prova e vale 27,5% (cerca de 11 das 40): diferença entre dado e informação, o triângulo CIA (confidencialidade, integridade, disponibilidade), responsabilização e auditabilidade, SGSI e PDCA, política de segurança, papéis e segurança com fornecedores. Quase tudo cai como cenário curto do dia a dia: aconteceu algo com a informação e eu preciso dizer qual aspecto foi afetado ou qual controle está sendo aplicado. Onde eu mais erro é quando a informação está incompleta (é integridade, não disponibilidade) ou atrasada (é disponibilidade, não integridade). Também preciso lembrar que a política dá direção e compromissos, nunca configuração de firewall ou lista de senhas. E que nenhuma resposta certa promete risco zero: a meta é sempre risco aceitável.

Neste capítulo

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

Tópicos-chave

Dado x informação

Dado é fato bruto, sem contexto (a sequência 20251231). Informação é dado com contexto e significado (o prazo de entrega é 31/12/2025). O mesmo dado gera informações diferentes conforme o contexto e quem interpreta; milhões de registros de vendas agregados em um relatório por região viram informação para a diretoria. Quem recebe define o valor: a fatura gerada a partir de milhões de transações de uma operadora é informação para o cliente.

Informação como ativo e seu valor

A informação é ativo porque tem valor e pode ser perdida, roubada ou alterada; deve ser inventariada, ter proprietário e proteção proporcional ao valor. O valor é dado pela importância para os processos de negócio, não pela idade, tamanho do arquivo ou número de cópias. O valor muda com o tempo: uma previsão de vendas é muito sensível antes da divulgação e perde parte do valor depois.

Formas da informação e sistema de informação

A informação existe em sistemas, papel, mídias e na fala (gerentes discutindo uma aquisição no elevador vazam informação). Sistema de informação é o conjunto de pessoas, processos, dados e tecnologia, incluindo arquivos em papel e meios de comunicação, e não só software ou servidores.

Gestão e análise da informação; ciclo de vida

O foco da gestão da informação é garantir que o valor da informação seja aproveitado (como ela é obtida, usada, compartilhada e descartada). A análise da informação serve para entender como ela flui entre áreas, sistemas e pessoas. O ciclo de vida tem criação, armazenamento, uso, compartilhamento, arquivamento e descarte; no descarte a preocupação principal é a destruição segura.

Segurança da informação (definição EXIN)

É a preservação da confidencialidade, integridade e disponibilidade da informação, em qualquer forma: digital, papel ou falada. Antivírus e firewall são controles, não a definição. A meta realista é reduzir os riscos a um nível aceitável, conforme o apetite a risco, e não chegar a risco zero.

Confidencialidade

Garante que a informação seja acessível só a quem tem autorização e necessidade de conhecer. Cai em cenários como planilha de salários enviada para a empresa inteira, documentos esquecidos na impressora do corredor e disco cifrado em notebook furtado. Controles típicos: criptografia, impressão com liberação por crachá, mesa limpa.

Integridade

É a exatidão, completude e validade da informação. Preço alterado por engano, pedido gravado sem endereço e verificação de hash de arquivo baixado são integridade. Controles: validação de entrada e de preenchimento, aprovação de alterações, controle de versões com edição restrita a autorizados.

Disponibilidade

A informação deve estar acessível no momento em que é necessária; inclui pontualidade e continuidade. Site fora do ar por DDoS, relatório que chega depois da reunião e prontuário em emergência médica são disponibilidade. Controles excessivos (três aprovações e duas senhas para abrir um relatório) também prejudicam a disponibilidade; backup em outro prédio a protege.

Não repúdio

Impede que alguém negue ter feito uma ação. Depende de mecanismos confiáveis de autenticação e registro, como assinatura digital e logs protegidos. Cenário clássico: o cliente nega o pedido, mas a transação tem a assinatura digital dele.

Responsabilização (accountability)

É responder pelos próprios atos. Para responsabilizar alguém por uma ação em um sistema é preciso identificação única do usuário e registro das ações. Senha compartilhada, login genérico, acesso anônimo ou logs desativados impedem saber quem agiu.

Auditabilidade

É a capacidade de ser verificado. Registrar quem aprovou cada pagamento, quando e com base em quê torna o processo auditável. Para uma organização certificada na ISO/IEC 27001, auditabilidade permite provar a terceiros que os controles funcionam; ela não substitui a análise de riscos nem garante ausência de incidentes.

SGSI (sistema de gestão de segurança da informação)

Parte da gestão que trata a segurança com base em riscos, com políticas, processos, papéis, recursos e melhoria contínua, geralmente no ciclo PDCA. A implantação começa definindo escopo e limites, considerando contexto, partes interessadas e interfaces com terceiros. Os resultados da avaliação de riscos, o escopo, a política e a declaração de aplicabilidade são informação documentada exigida; não conformidade exige corrigir e tratar a causa.

Ciclo PDCA no SGSI

Plan: definir escopo, política e objetivos. Do: implementar os controles. Check: monitorar, medir e auditar a eficácia dos controles. Act: corrigir não conformidades e melhorar. O ciclo se repete continuamente.

Evento x incidente; due diligence x due care

Incidente é um evento indesejado com chance real de prejudicar o negócio; um login com senha errada é só evento. Due diligence é o esforço contínuo de investigar e entender riscos e obrigações; due care é agir, adotando as medidas razoáveis que uma organização prudente adotaria.

Política de segurança da informação

Dá direção e apoio da gestão à segurança; é aprovada pela alta direção, comunicada aos funcionários e às partes externas relevantes e revisada em intervalos planejados e após mudanças importantes. Pela ISO/IEC 27001, inclui compromisso com os requisitos e com a melhoria contínua e os objetivos de segurança (ou a estrutura para defini-los). Temas como acesso, criptografia, backup e uso aceitável ganham políticas específicas por tema, alinhadas à geral.

Papéis e responsabilidades

O CISO define a estratégia de segurança; gerente ou oficial de segurança (ISM, ISO) atuam no nível tático e operacional. O proprietário do ativo responde pela proteção ao longo do ciclo de vida e pode delegar tarefas, não a responsabilidade. A direção exige que todos apliquem a segurança, e o gestor de cada departamento garante o cumprimento no dia a dia; segregação de funções separa tarefas conflitantes, como cadastrar fornecedor e aprovar pagamento.

Segurança com fornecedores

Antes de contratar, avaliar os controles do fornecedor (questionários, certificações, auditorias). O contrato prevê requisitos de segurança, direito de auditar, notificação de incidentes, controle de subcontratados (que recebem os mesmos requisitos) e devolução ou destruição segura da informação ao final, com confirmação. Depois da contratação, monitorar o cumprimento; em nuvem, definir a divisão de responsabilidades (responsabilidade compartilhada).

Outros controles organizacionais deste domínio

Contato com autoridades: saber antes de qualquer incidente como e quando acionar polícia e autoridade de proteção de dados. Contato com grupos de interesse especial: fóruns e associações para alertas e boas práticas. Uso aceitável: regras documentadas sobre e-mail, internet e equipamentos. Devolução de ativos no desligamento (notebook, crachá) e regras e acordos para transferência segura de informação a parceiros. PII é qualquer informação que identifique uma pessoa; senha é informação de autenticação, não PII.

Macetes para memorizar

💡 Triângulo CIA

C = quem VÊ; I = está CERTO e COMPLETO; D = está LÁ na HORA. Pergunte: vazou, mudou ou sumiu/atrasou?

💡 Dado x informação

Dado + contexto = informação. Sem contexto, é só dado.

💡 PDCA

Planeja (escopo, política), Faz (implementa), Checa (mede e audita), Age (corrige e melhora).

💡 Due diligence x due care

Diligence = Descobrir; Care = Cuidar (agir).

💡 Accountability x auditabilidade

Accountability = Alguém responde (ID único + log). Auditabilidade = dá para comprovar.

💡 Fornecedores

Avaliar → Contratar com requisitos e direito de auditoria → Monitorar → Devolver ou destruir. Subcontratado herda os requisitos.

💡 Política

Direção aprova, todos que aplicam recebem, revisa no calendário e na mudança.

Tabela de memorização: não confunda

Quando é...	...e quando é
Dado Fato bruto sem contexto, como 20251231 ou 37,8 soltos no sistema.	**Informação** O mesmo dado com contexto e significado, como 'temperatura do paciente: 37,8 °C' ou um relatório consolidado para decisão.

Integridade A informação está errada, alterada ou incompleta (preço errado, pedido sem endereço), mas o sistema funciona.	**Disponibilidade** A informação está correta, mas não chega a quem precisa quando precisa (site fora do ar, relatório atrasado, controles excessivos).
Confidencialidade A informação foi vista por quem não devia (e-mail para todos, papel na impressora); os valores não mudaram.	**Integridade** O conteúdo mudou ou ficou incompleto; nada foi divulgado. Hash e controle de versões protegem integridade, não sigilo.
Responsabilização (accountability) Responder pelos atos; exige ID único e logs para atribuir a ação a uma pessoa.	**Auditabilidade** Poder ser verificado por terceiros; exige registros completos e protegidos que sirvam de evidência.
Due diligence Investigar e conhecer riscos e obrigações, de forma contínua.	**Due care** Agir para proteger, adotando as medidas razoáveis de uma organização prudente.
Evento Ocorrência sem impacto provável, como um login com senha errada.	**Incidente** Evento indesejado com chance real de prejudicar o negócio, como várias tentativas seguidas de invasão.
Contato com autoridades Contatos prontos com polícia e autoridade de proteção de dados para responder a incidentes e cumprir prazos legais.	**Contato com grupos de interesse especial** Participação em fóruns e associações profissionais para trocar alertas e boas práticas.

Números que caem

Item	Valor
Peso do domínio na prova	**27,5% (cerca de 11 das 40)**
Conceitos relativos à informação (1.1)	**10%**
Aspectos de confiabilidade (1.2)	**7,5%**
Segurança da informação na organização (1.3)	**10%**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Disco cifrado em notebook furtado protege a disponibilidade.
Como não cair: Criptografia protege a confidencialidade; os dados continuam perdidos para a empresa. Disponibilidade exige backup.

⚠ **Alerta de prova:** Pedido gravado sem endereço é falha de disponibilidade ou de autenticidade.
Como não cair: O sistema funcionou e o cliente foi identificado; informação incompleta é integridade.

⚠ **Alerta de prova:** Relatório que chega depois da reunião é problema de integridade.
Como não cair: Os números estão certos; faltou pontualidade, que faz parte da disponibilidade.

⚠ **Alerta de prova:** Exigir três aprovações e duas senhas prejudica a confidencialidade.
Como não cair: A confidencialidade foi reforçada; quem sofre é a disponibilidade. Os aspectos precisam ser equilibrados.

⚠ **Alerta de prova:** Catálogo de preços público não precisa de nenhuma proteção, ou só de confidencialidade.
Como não cair: Informação pública também tem valor: precisa estar correta e acessível, então integridade e disponibilidade.

⚠ **Alerta de prova:** Backup em outro prédio protege a confidencialidade porque fica escondido.
Como não cair: O objetivo principal é a disponibilidade caso o local principal seja destruído; a cópia é que precisa de proteção física e criptografia.

⚠ **Alerta de prova:** A verificação de hash protege a confidencialidade do arquivo.
Como não cair: O hash não esconde o conteúdo; ele detecta alteração, então protege a integridade.

⚠ **Alerta de prova:** Capacidade, redundância ou portabilidade aparecem como aspectos de confiabilidade.
Como não cair: Os aspectos de confiabilidade são confidencialidade, integridade e disponibilidade; esses outros termos são distratores.

⚠ **Alerta de prova:** A política de segurança deve trazer a configuração dos firewalls ou a lista de senhas dos administradores.
Como não cair: Política dá direção, compromissos e objetivos; detalhe técnico vai para procedimentos e senhas nunca entram em documento de política.

⚠ **Alerta de prova:** A política aprovada vale para sempre ou só é revisada quando o auditor exige.
Como não cair: Revisão em intervalos planejados e após mudanças importantes no negócio, na lei, na tecnologia ou nos riscos.

⚠ **Alerta de prova:** Basta comunicar a política à diretoria que a aprovou ou aos auditores.
Como não cair: Ela precisa chegar a quem a aplica: funcionários e partes externas relevantes, de forma acessível e compreensível.

⚠ **Alerta de prova:** Senha é exemplo de PII.
Como não cair: Senha é informação de autenticação. PII é o que identifica uma pessoa: nome, CPF, e-mail, foto e combinações de dados.

⚠ **Alerta de prova:** Nuvem é segura por natureza, então basta confiar no provedor.
Como não cair: A responsabilidade continua com a empresa: requisitos no contrato, monitoramento e divisão de responsabilidades definida.

⚠ **Alerta de prova:** O objetivo da gestão de segurança é chegar a risco zero.
Como não cair: Risco zero é impossível e inviável; a meta é reduzir os riscos a um nível aceitável, com controles proporcionais.

Como cai na prova

📝 **Como cai:** Cenário de incidente seguido de 'qual aspecto da confiabilidade foi afetado?'
Como resolver: Pergunte o que aconteceu com a informação: foi vista por quem não devia (C), ficou errada ou incompleta (I) ou não estava acessível na hora certa (D). Descarte de cara termos que não são aspectos, como capacidade, redundância e portabilidade.

📝 **Como cai:** 'Qual controle está sendo aplicado?' com nomes de controles da ISO/IEC 27002
Como resolver: Ache o verbo-chave do cenário (participar de fóruns, contatar autoridades, separar funções, definir regras de uso) e associe ao controle. Os distratores costumam ser controles de outra categoria (técnico, físico, de pessoas).

📝 **Como cai:** 'Quem é responsável por...?' ou 'Quem deve aprovar...?'
Como resolver: Política: alta direção aprova. Estratégia de segurança: CISO, que traduz a estratégia definida pela direção geral. Proteção do ativo e sua classificação: proprietário. Cumprimento no dia a dia: gestor da área. Fornecedor, auditor, visitante e estagiário costumam ser distratores.

📝 **Como cai:** 'Qual é a diferença entre X e Y?' (dado/informação, evento/incidente, accountability/auditabilidade)
Como resolver: A certa traz definições curtas e distintas. Elimine 'são sinônimos', leituras contábeis dos termos e critérios absurdos como suporte (papel x digital) ou pessoas x máquinas.

📝 **Como cai:** Fornecedor ou nuvem: 'como garantir a segurança?'
Como resolver: Escolha a alternativa que mantém o controle com a organização (requisitos no contrato, direito de auditoria, monitoramento). Erradas dispensam controles, confiam cegamente ou entregam senhas.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
site fora do ar, DDoS, informação chegou atrasada, emergência médica	**Disponibilidade**
enviado para toda a empresa, papéis esquecidos na impressora, notebook cifrado furtado	**Confidencialidade**
valor alterado por engano, registro incompleto, hash comparado com o publicado	**Integridade**
cliente nega o pedido, mas há assinatura digital	**Não repúdio**
registrar quem aprovou, quando e com base em quê	**Auditabilidade**
senha compartilhada, login genérico, acesso anônimo	**Perda de responsabilização; exigir ID único + logs**
sequência de números sem nenhum contexto	**Dado (não informação)**
a mesma pessoa cadastra fornecedores e aprova pagamentos	**Segregação de funções**
fóruns e associações profissionais para trocar alertas	**Contato com grupos de interesse especial**
já sabe como e quando contatar polícia e autoridade de proteção de dados	**Contato com autoridades**
fornecedor usa subcontratados	**Subcontratados recebem os mesmos requisitos (cadeia de fornecimento)**
contrato com fornecedor encerrado	**Devolução ou destruição segura, com confirmação**
implantar o SGSI, o que definir primeiro	**Escopo e limites do sistema de gestão**
regras sobre e-mail, internet e equipamentos corporativos	**Uso aceitável da informação e dos ativos**

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

- Informação incompleta é integridade; informação atrasada é disponibilidade.
- Segurança da informação = preservar confidencialidade, integridade e disponibilidade, em qualquer forma (digital, papel, fala).
- Política: aprovada pela alta direção, comunicada a quem aplica, revisada em intervalos planejados e após mudanças.
- Responsabilizar exige identidade única + registro das ações; senha compartilhada destrói isso.
- A meta é risco aceitável, nunca risco zero.

Essenciais para a prova (checklist)

- ☐ Sei classificar um exemplo como dado ou informação pelo contexto.
- ☐ Sei apontar o aspecto CIA afetado em cenários de vazamento, alteração, dado incompleto, atraso e indisponibilidade.
- ☐ Sei diferenciar responsabilização, auditabilidade e não repúdio.
- ☐ Sei as quatro fases do PDCA e o que acontece no Check.
- ☐ Sei o que entra e o que não entra na política de segurança, quem aprova e quando revisar.
- ☐ Sei os papéis de CISO, proprietário do ativo, direção e gestor da área.
- ☐ Sei as etapas da segurança com fornecedores: avaliar, contratar com requisitos, monitorar, devolver ou destruir.
- ☐ Sei diferenciar evento de incidente e due diligence de due care.
- ☐ Sei por onde começa a implantação de um SGSI e o que a ISO/IEC 27001 exige diante de uma não conformidade.

Questões de revisão do capítulo

R3.1 · Informação e Segurança

Quais elementos compõem um sistema de informação?

A. O software de gestão comprado de um fornecedor
B. Os servidores e os computadores da empresa
C. Pessoas, processos, dados e tecnologia juntos
D. Os cabos de rede e a conexão com a internet

R3.2 · Informação e Segurança

Quem responde pela proteção adequada de um ativo de informação ao longo do seu ciclo de vida?

A. A empresa que fabricou o servidor onde o ativo fica
B. O auditor externo contratado uma vez por ano
C. Qualquer pessoa que tenha acesso de leitura ao ativo
D. O proprietário designado do ativo

R3.3 · Informação e Segurança

A equipe de segurança participa de fóruns e associações profissionais para trocar alertas e boas práticas. Qual controle está sendo aplicado?

A. Mascaramento de dados pessoais
B. Processo disciplinar dos funcionários da empresa
C. Proteção de registros contábeis
D. Contato com grupos de interesse especial

R3.4 · Informação e Segurança

Por que a informação deve ser tratada como um ativo da organização?

A. Porque tem valor e pode ser perdida, roubada ou alterada
B. Porque só a informação em papel precisa de proteção
C. Porque aparece no balanço contábil como bem imóvel da empresa
D. Porque o fornecedor de TI é dono da informação

Respostas comentadas

R3.1. C) Pessoas, processos, dados e tecnologia juntos

Por quê: Sistemas de informação incluem também arquivos em papel, meios de comunicação e as pessoas que usam a informação.

✗ A) Incorreta. É só uma parte do sistema.
✗ B) Incorreta. Deixa de fora pessoas e processos.
✗ D) Incorreta. É só infraestrutura.

> **Dica de prova:** Sistema de informação: pessoas + processos + dados + tecnologia.

R3.2. D) O proprietário designado do ativo

Por quê: O proprietário garante que o ativo esteja inventariado, classificado e protegido, podendo delegar tarefas, mas não a responsabilidade.

✗ A) Incorreta. Não é o responsável.
✗ B) Incorreta. Não é o responsável.
✗ C) Incorreta. Não é o responsável.

> **Dica de prova:** Ativo protegido: responsabilidade do proprietário.

R3.3. D) Contato com grupos de interesse especial

Por quê: Esses grupos ajudam a manter o conhecimento atualizado e a receber alertas antecipados sobre ameaças e vulnerabilidades.

✗ A) Incorreta. É controle técnico.
✗ B) Incorreta. É controle de pessoas.
✗ C) Incorreta. É outro controle.

> **Dica de prova:** Fóruns de segurança: grupos de interesse.

R3.4. A) Porque tem valor e pode ser perdida, roubada ou alterada

Por quê: Ativos de informação devem ser inventariados, ter proprietário e receber proteção proporcional ao valor.

✗ B) Incorreta. Vale para qualquer forma.
✗ C) Incorreta. Não é esse o motivo.
✗ D) Incorreta. A organização é a responsável.

> **Dica de prova:** Informação tem valor: é ativo.

04

CAPÍTULO 4 · 7,5% DA PROVA

Legislação, Regulamentos e Normas

É o menor domínio, 7,5% da prova (cerca de 3 das 40), mas são pontos quase garantidos se eu decorar qual norma faz o quê. Preciso separar bem ISO/IEC 27000 (vocabulário), 27001 (requisitos e certificação), 27002 (orientação dos controles) e 27005 (riscos), além de normas e referências vizinhas: 27017, 27701, 22301, PCI DSS e NIST CSF. Do lado legal, cai exemplo de legislação: GDPR, NIS2, crimes informáticos, propriedade intelectual, proteção de registros e leis de criptografia. As alternativas erradas costumam ser normas de outro assunto (ISO 9001, ISO 14001, ITIL, PMBOK) ou a norma vizinha da família 27000. Onde mais erro é trocar 27001 por 27002.

Neste capítulo

17 tópicos-chave · 11 pegadinhas · 5 macetes · 12 gatilhos · 4 questões comentadas

Tópicos-chave

ISO/IEC 27000

Traz a visão geral e o vocabulário usados nas demais normas de segurança da informação. Define termos como ativo, ameaça, vulnerabilidade e risco, usados de forma consistente em toda a família.

ISO/IEC 27001

Define os requisitos para estabelecer, implementar, manter e melhorar um SGSI. É a norma usada na certificação, feita por um organismo acreditado que audita o SGSI contra seus requisitos.

Cláusulas 4 a 10 e Anexo A da ISO/IEC 27001

Os requisitos obrigatórios do sistema de gestão estão nas cláusulas 4 a 10, que seguem a estrutura harmonizada das normas de sistemas de gestão ISO (o que facilita integrar SGSI, qualidade e outros). O Anexo A lista os controles de referência.

Declaração de aplicabilidade (SoA)

Documento que indica quais controles do Anexo A foram aplicados ou excluídos, com justificativa. Liga o resultado do tratamento de riscos aos controles escolhidos e é revisada nas auditorias.

ISO/IEC 27002

Orienta a implementação dos controles de segurança, detalhando como aplicar os controles do Anexo A da 27001. A edição de 2022 organiza 93 controles em quatro temas: organizacionais, de pessoas, físicos e tecnológicos. Orienta, mas não certifica.

ISO/IEC 27005

Traz orientações específicas para a gestão de riscos de segurança da informação. Apoia a aplicação dos requisitos de risco da ISO/IEC 27001, sem ser certificável.

ISO/IEC 27017 e ISO/IEC 27018

A 27017 traz controles de segurança específicos para serviços de nuvem, complementando a 27002 para provedores e clientes. A 27018 trata de dados pessoais na nuvem.

ISO/IEC 27701

Estende a ISO/IEC 27001 para incluir a gestão da privacidade da informação. Acrescenta requisitos e controles para controladores e operadores de dados pessoais.

ISO 22301

Norma de sistemas de gestão da continuidade de negócios. Complementa a segurança da informação, ajudando a manter atividades críticas durante interrupções.

PCI DSS

Padrão do setor de cartões que lojas que processam pagamentos com cartão precisam seguir. É exigido por contrato pelas bandeiras e adquirentes e define controles para proteger dados de titulares de cartão.

NIST Cybersecurity Framework

Referência publicada pelo NIST dos Estados Unidos que organiza a cibersegurança nas funções Governar, Identificar, Proteger, Detectar, Responder e Recuperar. É voluntário e pode ser usado junto com a ISO/IEC 27001.

GDPR e leis de proteção de dados

O Regulamento Geral sobre a Proteção de Dados (GDPR) é a legislação europeia que exige proteger dados pessoais com medidas técnicas e organizativas adequadas. Leis como o GDPR e a LGPD tornam a segurança da informação uma obrigação legal quando há dados pessoais. Para cumprir uma lei de proteção de dados, o primeiro passo é traduzi-la em uma política interna de privacidade.

Diretiva NIS2

Diretiva da União Europeia que amplia obrigações de cibersegurança e notificação de incidentes para entidades essenciais e importantes. Exige gestão de riscos, medidas de segurança, notificação de incidentes e responsabilização da direção em vários setores.

Crimes informáticos

Acesso não autorizado a um sistema e cópia de dados configuram crime previsto na legislação de crimes informáticos, não uma simples violação de licença. Leis de crimes cibernéticos, como a Convenção de Budapeste e leis nacionais, tratam de invasão, fraude e dano a sistemas; acesso indevido já é ilícito mesmo sem apagar nada.

Direitos de propriedade intelectual

Instalar software em mais máquinas do que a licença permite viola direitos de propriedade intelectual e pode gerar multas e processos. A organização deve controlar licenças e instalações.

Proteção de registros

Controle da ISO/IEC 27002 que trata de obrigações legais de guarda, como manter notas fiscais pelo prazo exigido. Registros devem ser protegidos contra perda, destruição, falsificação e acesso não autorizado, conforme requisitos legais e do negócio.

Requisitos legais em vários países

A organização deve identificar e manter atualizados os requisitos legais, regulamentares e contratuais de cada país em que atua. Ao enviar notebooks com discos criptografados ao exterior, é preciso verificar as leis locais sobre uso e exportação de criptografia.

Macetes para memorizar

💡 Família 27000

27000 = dicionário; 27001 = exige (requisitos, certifica); 27002 = explica os controles; 27005 = riscos.

💡 Normas vizinhas

27017 = nuvem; 27018 = dados pessoais na nuvem; 27701 = privacidade; 22301 = continuidade.

Distratores fora do tema

9001 = qualidade; 14001 = meio ambiente; ITIL = serviços; PMBOK = projetos. Se aparecerem, quase sempre estão erradas.

Estrutura da 27001

Requisito nas cláusulas 4 a 10; controle no Anexo A; escolha justificada na SoA.

NIST CSF

Governar, Identificar, Proteger, Detectar, Responder, Recuperar; uso voluntário, pode ser combinado com a ISO/IEC 27001.

Tabela de memorização: não confunda

Quando é...	...e quando é
ISO/IEC 27001 Requisitos do SGSI e base da certificação.	**ISO/IEC 27002** Orientação para implementar os controles; orienta, mas não certifica.
ISO/IEC 27000 Visão geral e vocabulário da família.	**ISO/IEC 27005** Orientação para a gestão de riscos de segurança da informação, sem ser certificável.
Cláusulas 4 a 10 Onde estão os requisitos obrigatórios do sistema de gestão.	**Anexo A** Lista de controles de referência, escolhidos e justificados na declaração de aplicabilidade.
ISO 22301 Gestão da continuidade de negócios.	**ISO/IEC 27701** Extensão da 27001 para gestão da privacidade (dados pessoais).
NIST Cybersecurity Framework Referência voluntária com as funções Governar, Identificar, Proteger, Detectar, Responder e Recuperar.	**PCI DSS** Padrão do setor de cartões, exigido por contrato pelas bandeiras e adquirentes.
Legislação (GDPR, NIS2) Obrigação legal imposta por lei ou regulamento.	**Norma (ISO 9001, ISO/IEC 27001)** Padrão adotado pela organização; a ISO 9001 é de qualidade e não é legislação.

Números que caem

Item	Valor
Peso do domínio na prova	**7,5% (cerca de 3 das 40)**
Legislação e regulamentos (4.1)	**2,5%**

Normas (4.2)	**5%**
Requisitos obrigatórios da ISO/IEC 27001	**Cláusulas 4 a 10**
Controles da ISO/IEC 27002:2022	**93, em 4 temas**
Funções do NIST Cybersecurity Framework	**Governar, Identificar, Proteger, Detectar, Responder, Recuperar**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** A ISO/IEC 27002 é a norma de certificação do SGSI.
Como não cair: Certificação é contra a ISO/IEC 27001; a 27002 só orienta os controles.

⚠ **Alerta de prova:** A ISO/IEC 27001 define o vocabulário de todas as normas.
Como não cair: Vocabulário e visão geral são da ISO/IEC 27000; a 27001 traz os requisitos.

⚠ **Alerta de prova:** Os requisitos obrigatórios da 27001 estão no Anexo A.
Como não cair: O Anexo A lista controles de referência; os requisitos estão nas cláusulas 4 a 10.

⚠ **Alerta de prova:** A 27001 copia os requisitos da ISO 9001.
Como não cair: Ela tem requisitos próprios; só segue a mesma estrutura harmonizada das normas de sistemas de gestão.

⚠ **Alerta de prova:** ISO/IEC 27005 é certificável.
Como não cair: A 27005 apoia os requisitos de risco da 27001, mas não é certificável.

⚠ **Alerta de prova:** A norma de sistema de gestão da continuidade de negócios é a ISO/IEC 27002 ou a 27000.
Como não cair: Sistema de gestão da continuidade é a ISO 22301. A 27002 traz controles ligados à continuidade (5.29 e 5.30), mas não é a norma desse sistema de gestão.

⚠ **Alerta de prova:** Nuvem ou privacidade são cobertas pela ISO 22301, 9001 ou 14001.
Como não cair: Nuvem: ISO/IEC 27017. Privacidade sobre a 27001: ISO/IEC 27701. 22301 é continuidade, 9001 qualidade, 14001 meio ambiente.

⚠ **Alerta de prova:** Funções Governar, Identificar, Proteger, Detectar, Responder e Recuperar são do PCI DSS ou da 27701.
Como não cair: São do NIST Cybersecurity Framework; PCI DSS é para dados de cartão.

⚠ **Alerta de prova:** A ISO 9001 ou um contrato de licença são exemplos de legislação de proteção de dados.
Como não cair: Norma e contrato não são legislação; o exemplo europeu é o GDPR.

⚠ **Alerta de prova:** Invadir um sistema e copiar dados é só violação de contrato de licença, ou é permitido se nada for apagado.
Como não cair: Acesso indevido já é ilícito: configura crime previsto na legislação de crimes informáticos.

⚠ **Alerta de prova:** ITIL ou PMBOK tratam das obrigações de cibersegurança e notificação de incidentes na UE.
Como não cair: Isso é a Diretiva NIS2; ITIL trata de serviços e PMBOK de projetos.

Como cai na prova

📝 **Como cai:** 'Qual norma trata de X?'
Como resolver: Associe a palavra-chave à norma (vocabulário, requisitos, controles, riscos, nuvem, privacidade, continuidade, cartão). Elimine normas de outro assunto (9001, 14001) e depois a vizinha da família 27000.

📝 **Como cai:** 'Qual é o papel da norma X?'
Como resolver: A certa descreve a função exata; as erradas descrevem a função de outra norma da família ('isso é a 27000', 'isso é a 27001').

📝 **Como cai:** Cenário legal: 'qual requisito legal está sendo violado?' ou 'o que esse ato configura?'
Como resolver: Identifique o objeto: software sem licença (propriedade intelectual), guarda de documentos (proteção de registros), invasão (crime informático), dados pessoais (GDPR), criptografia no exterior (leis locais).

📝 **Como cai:** Estrutura da certificação 27001
Como resolver: Requisitos nas cláusulas 4 a 10; controles no Anexo A; aplicados ou excluídos com justificativa na declaração de aplicabilidade; certificação por organismo acreditado.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
visão geral e vocabulário	**ISO/IEC 27000**

requisitos do SGSI, certificação reconhecida internacionalmente	**ISO/IEC 27001**
orientar a implementação dos controles	**ISO/IEC 27002**
gestão de riscos de segurança da informação	**ISO/IEC 27005**
controles específicos para serviços de nuvem	**ISO/IEC 27017**
estender a 27001 para privacidade	**ISO/IEC 27701**
sistema de gestão da continuidade de negócios	**ISO 22301**
loja que processa pagamentos com cartão	**PCI DSS**
controles do Anexo A aplicados ou excluídos, com justificativa	**Declaração de aplicabilidade**
software instalado em mais máquinas do que a licença	**Direitos de propriedade intelectual**
lei exige guardar documentos por um prazo	**Proteção de registros**
notebooks criptografados enviados a outro país	**Leis locais sobre uso e exportação de criptografia**

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

- 27001 certifica (requisitos); 27002 orienta (controles); 27000 é vocabulário; 27005 é risco.
- Requisitos da 27001 nas cláusulas 4 a 10; controles no Anexo A; escolha justificada na declaração de aplicabilidade.
- 22301 continuidade, 27017 nuvem, 27701 privacidade, PCI DSS cartões, NIST CSF funções de Governar a Recuperar.
- Norma (ISO 9001) não é legislação; GDPR e NIS2 são.

Essenciais para a prova (checklist)

☐ Sei o papel de cada uma: ISO/IEC 27000, 27001, 27002 e 27005.

☐ Sei onde ficam os requisitos e os controles da ISO/IEC 27001 e o que é a declaração de aplicabilidade.

☐ Sei associar nuvem, privacidade, continuidade e cartões à norma ou padrão certo.

☐ Sei as funções do NIST Cybersecurity Framework (Governar, Identificar, Proteger, Detectar, Responder, Recuperar).

☐ Sei dar exemplos de legislação: GDPR, NIS2, crimes informáticos, propriedade intelectual, proteção de registros.

☐ Sei distinguir legislação de norma e reconhecer distratores como ISO 9001, ISO 14001, ITIL e PMBOK.

Questões de revisão do capítulo

R4.1 · Legislação, Regulamentos e Normas

Uma empresa quer uma certificação de segurança da informação reconhecida internacionalmente. Em qual norma ela deve se basear?

A. ISO/IEC 27002
B. ISO/IEC 27001
C. ISO/IEC 27005
D. ISO/IEC 27000

R4.2 · Legislação, Regulamentos e Normas

Uma loja que processa pagamentos com cartão precisa seguir qual padrão do setor de cartões?

A. PCI DSS
B. ISO 14001
C. ISO 9001
D. ITIL 4

R4.3 · Legislação, Regulamentos e Normas

Qual norma traz controles de segurança da informação específicos para serviços de nuvem?

A. ISO/IEC 27017
B. ISO 14001:2015
C. ISO 9001:2015
D. ISO 22301:2019

R4.4 · Legislação, Regulamentos e Normas

Qual norma estende a ISO/IEC 27001 para incluir a gestão da privacidade da informação?

A. ISO 14001:2015
B. ISO/IEC 27701
C. ISO 9001:2015
D. ISO 22301:2019

Respostas comentadas

R4.1. B) ISO/IEC 27001

Por quê: A certificação é feita por um organismo acreditado, que audita o SGSI contra os requisitos da ISO/IEC 27001.

✗ A) Incorreta. Orienta, mas não certifica.
✗ C) Incorreta. Orienta a gestão de riscos.
✗ D) Incorreta. Traz o vocabulário.

> **Dica de prova:** Certificação: ISO/IEC 27001.

R4.2. A) PCI DSS

Por quê: O PCI DSS é exigido por contrato pelas bandeiras e adquirentes, e define controles para proteger dados de titulares de cartão.

✗ B) Incorreta. Trata de meio ambiente.
✗ C) Incorreta. Trata de qualidade.
✗ D) Incorreta. Trata de gestão de serviços.

> **Dica de prova:** Dados de cartão: PCI DSS.

R4.3. A) ISO/IEC 27017

Por quê: A ISO/IEC 27017 complementa a 27002 para provedores e clientes de nuvem; a ISO/IEC 27018 trata de dados pessoais na nuvem.

✗ B) Incorreta. Trata de meio ambiente.
✗ C) Incorreta. Trata de qualidade.
✗ D) Incorreta. Trata de continuidade.

> **Dica de prova:** Nuvem: ISO/IEC 27017.

R4.4. B) ISO/IEC 27701

Por quê: A ISO/IEC 27701 acrescenta requisitos e controles para controladores e operadores de dados pessoais.

✗ A) Incorreta. Trata de meio ambiente.
✗ C) Incorreta. Trata de qualidade.
✗ D) Incorreta. Trata de continuidade.

> **Dica de prova:** Privacidade sobre a 27001: ISO/IEC 27701.

DIA DA PROVA

Estratégia de prova

São 40 questões de múltipla escolha em 60 minutos, sem consulta e sem equipamentos eletrônicos, com aprovação em 65% (26 acertos). O exame cobra os níveis 1 e 2 da taxonomia de Bloom: lembrar definições e entender como aplicá-las, então a maioria é um cenário curto do dia a dia seguido de 'qual aspecto foi afetado', 'qual controle é esse' ou 'o que fazer'. As alternativas erradas costumam ser de outra categoria (controle físico quando o cenário é técnico), de outro conceito vizinho (repressivo x corretivo, 27001 x 27002) ou claramente aumentam o risco. Algumas têm só três alternativas. A terminologia segue a ISO/IEC 27001/27002:2022 e o vocabulário próprio da EXIN, como risk bearing, risk neutral e anéis de proteção.

Como responder

✓ Ritmo: 60 minutos para 40 questões dá 1,5 minuto por questão; responda as de definição em segundos e guarde tempo para cenários e cálculos.

✓ Meta realista: 26 acertos aprovam. Controles de Segurança vale 52,5% (cerca de 21 questões); dominar esse domínio é o caminho mais curto.

✓ Em cenário de confiabilidade, pergunte: vazou (confidencialidade), mudou ou ficou incompleto (integridade), não estava acessível na hora (disponibilidade).

✓ Em 'qual controle é esse?', identifique o tema do cenário (organizacional, pessoas, físico, tecnológico) e elimine os distratores de outro tema.

✓ Em 'o que fazer?', elimine primeiro toda alternativa que aumenta o risco (emprestar crachá, esperar, ignorar, apagar evidências, desligar antivírus).

✓ Para tipos de controle, posicione a medida na linha do tempo do incidente: antes (preventivo), percebe (detectivo), contém (repressivo), recupera (corretivo), paga (seguro).

✓ Cálculos sem calculadora: converta a frequência em ARO (a cada 2 anos = 0,5) e multiplique pelo SLE; confira se não escolheu o próprio SLE.

✓ Desconfie de alternativas com absolutos como 'risco zero', 'nunca', 'vale para sempre' ou 'são sinônimos'.

Erros que derrubam candidatos

✗ Confundir integridade com disponibilidade em informação incompleta ou atrasada.

✗ Chamar extintor de corretivo ou restauração de backup de repressiva.

✗ Trocar autenticação por autorização, ou a chave pública do destinatário pela privada do remetente.

✗ Achar que a ISO/IEC 27002 é a norma certificável no lugar da 27001.

✗ Classificar multa ou perda de clientes como dano direto.

✗ Confundir aceitar o risco (sem medidas) com estratégia neutra (com medidas) ou seguro com evitar.

✗ Escolher a ação 'proativa' de testar uma fraqueza ou investigar sozinho em vez de relatar pelo canal definido.

Na semana da prova

- ☐ Revise os pares que mais confundem: repressivo x corretivo, IDS x IPS, worm x cavalo de Troia, site quente x frio, escalonamento funcional x hierárquico.
- ☐ Refaça os cálculos de SLE, ARO e ALE até sair de cabeça, incluindo frequências como 'uma vez a cada quatro anos'.
- ☐ Memorize a tabela de normas: 27000, 27001, 27002, 27005, 27017, 27701, 22301, PCI DSS e NIST CSF.
- ☐ Faça provas cronometradas de 40 em 60 minutos e revise cada erro pela explicação das alternativas erradas.
- ☐ Na véspera, repasse só gatilhos e macetes, sem conteúdo novo, e confirme que vai fazer a prova sem consulta e sem equipamentos eletrônicos.

REVISÃO FINAL

Folha de cola

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

1. Ameaças e Riscos

‣ ex-funcionário apaga arquivos de propósito → **Ameaça humana intencional**

‣ funcionário apaga sem querer → **Ameaça humana não intencional**

‣ raio, incêndio, inundação, tempestade → **Ameaça não humana**

‣ fingir ser do suporte e pedir a senha → **Engenharia social**

‣ porta que não fecha, falha sem correção → **Vulnerabilidade**

⚠ São consequências: dano indireto. Direto é o que atinge o próprio ativo.

⚠ Nenhum dano ocorreu e ela é uma fraqueza: vulnerabilidade. A ameaça é quem entraria por ela.

⚠ Ameaça é quem ou o que explora; a falha em si é vulnerabilidade técnica.

2. Controles de Segurança

‣ alarme, detector de fumaça, análise de logs → **Controle detectivo**

‣ extintor, limitar o dano em curso → **Controle repressivo**

‣ restaurar a partir do backup → **Controle corretivo**

‣ apólice, cobrir prejuízo → **Medida de seguro**

‣ só a equipe que processa a folha vê os salários → **Necessidade de conhecer (need-to-know)**

⚠ Extintor contém o dano em curso: é repressivo. Corretivo recupera depois (restaurar backup).

⚠ O ataque já aconteceu e nada é detectado; restaurar é corretivo.

⚠ Não evita nem combate o fogo; cobre o prejuízo: é medida de seguro.

3. Informação e Segurança

‣ site fora do ar, DDoS, informação chegou atrasada, emergência médica → **Disponibilidade**

‣ enviado para toda a empresa, papéis esquecidos na impressora, notebook cifrado furtado → **Confidencialidade**

‣ valor alterado por engano, registro incompleto, hash comparado com o publicado → **Integridade**

‣ cliente nega o pedido, mas há assinatura digital → **Não repúdio**

‣ registrar quem aprovou, quando e com base em quê → **Auditabilidade**

⚠ Criptografia protege a confidencialidade; os dados continuam perdidos para a empresa. Disponibilidade exige backup.

⚠ O sistema funcionou e o cliente foi identificado; informação incompleta é integridade.

⚠ Os números estão certos; faltou pontualidade, que faz parte da disponibilidade.

4. Legislação, Regulamentos e Normas

‣ visão geral e vocabulário → **ISO/IEC 27000**

‣ requisitos do SGSI, certificação reconhecida internacionalmente → **ISO/IEC 27001**

‣ orientar a implementação dos controles → **ISO/IEC 27002**

‣ gestão de riscos de segurança da informação → **ISO/IEC 27005**

‣ controles específicos para serviços de nuvem → **ISO/IEC 27017**

⚠ Certificação é contra a ISO/IEC 27001; a 27002 só orienta os controles.

⚠ Vocabulário e visão geral são da ISO/IEC 27000; a 27001 traz os requisitos.

⚠ O Anexo A lista controles de referência; os requisitos estão nas cláusulas 4 a 10.

GABARITO

Respostas do diagnóstico

D1. A) Ameaça não humana → revise o capítulo 1

Por quê: Ameaças não humanas incluem raios, incêndios, inundações e tempestades; controles incluem para-raios, supressores de surto e redundância.

✗ B) Incorreta. Não envolve manipulação de pessoas.

✗ C) Incorreta. Não houve ação humana.

✗ D) Incorreta. É um evento, não uma fraqueza.

> **Dica de prova:** Raio: ameaça não humana.

D2. C) Risco residual, que deve ser aceito formalmente pela gestão → revise o capítulo 1

Por quê: Os proprietários dos riscos aprovam o plano de tratamento e aceitam os riscos residuais, que continuam sendo monitorados.

✗ A) Incorreta. Risco zero não existe.

✗ B) Incorreta. Não deve ser ignorado.

✗ D) Incorreta. Não é transferido automaticamente.

> **Dica de prova:** O que sobra: risco residual aceito.

D3. A) R$ 4.000 → revise o capítulo 1

Por quê: Uma vez a cada dois anos significa ARO de 0,5; o controle que custar mais que a ALE por ano precisa de outra justificativa.

✗ B) Incorreta. Seria uma vez por ano.

✗ C) Incorreta. Seria duas vezes por ano.

✗ D) Incorreta. Não corresponde à frequência.

> **Dica de prova:** ALE = SLE x ARO (0,5).

D4. B) Proporcional ao cargo, à informação acessada e aos riscos → revise o capítulo 2

Por quê: A verificação deve respeitar leis trabalhistas e de privacidade, e pode ser refeita quando a pessoa muda para uma função mais sensível.

✗ A) Incorreta. É o contrário.

✗ C) Incorreta. Deve ser feito antes.

✗ D) Incorreta. Deve ser proporcional.

> **Dica de prova:** Triagem proporcional ao risco.

D5. C) Quatro: organizacionais, de pessoas, físicos e tecnológicos → revise o capítulo 2

Por quê: A edição de 2022 também usa atributos, como tipo de controle (preventivo, detectivo, corretivo) e propriedade de segurança.

✗ A) Incorreta. Não é a estrutura da norma.
✗ B) Incorreta. Não é a estrutura da norma.
✗ D) Incorreta. Era a estrutura de 2013.

> **Dica de prova:** 27002:2022: 4 temas, 93 controles.

D6. A) Aprender com o incidente para evitar que se repita → revise o capítulo 2

Por quê: O conhecimento obtido com incidentes deve fortalecer os controles e melhorar a resposta futura.

✗ B) Incorreta. Não é o objetivo principal.
✗ C) Incorreta. Destruiria evidências.
✗ D) Incorreta. Perde o aprendizado.

> **Dica de prova:** Pós-incidente: aprender e melhorar.

D7. B) O CISO (Chief Information Security Officer) → revise o capítulo 3

Por quê: Em organizações maiores, o CISO define a estratégia; o gerente ou o oficial de segurança da informação (ISM, ISO) atuam nos níveis tático e operacional.

✗ A) Incorreta. Tem outras responsabilidades.
✗ C) Incorreta. Não define a estratégia.
✗ D) Incorreta. Atua no nível operacional.

> **Dica de prova:** Estratégia de segurança: CISO.

D8. C) O dado ganhou contexto e virou informação → revise o capítulo 3

Por quê: O mesmo dado pode gerar informações diferentes conforme o contexto e quem o interpreta.

✗ A) Incorreta. O caminho é o inverso.
✗ B) Incorreta. Nada foi alterado.
✗ D) Incorreta. São conceitos diferentes.

> **Dica de prova:** Dado + contexto = informação.

D9. D) Compromisso com os requisitos e com a melhoria contínua → revise o capítulo 3

Por quê: A política também deve trazer objetivos de segurança ou a estrutura para defini-los, e estar adequada ao propósito da organização.

✗ A) Incorreta. É detalhe técnico.
✗ B) Incorreta. Não deve constar.
✗ C) Incorreta. Não deve constar.

> **Dica de prova:** Política: compromissos + objetivos.

D10. D) Orientar a implementação dos controles de segurança → revise o capítulo 4

Por quê: A edição de 2022 organiza 93 controles em quatro temas: organizacionais, de pessoas, físicos e tecnológicos.

✗ A) Incorreta. Isso é a ISO/IEC 27000.
✗ B) Incorreta. Isso é a ISO/IEC 27001.
✗ C) Incorreta. Isso é a ISO 9001.

> **Dica de prova:** 27002: guia dos controles.

D11. B) Nas cláusulas 4 a 10 do corpo da norma → revise o capítulo 4

Por quê: As cláusulas seguem a estrutura harmonizada das normas de sistemas de gestão ISO, o que facilita integrar SGSI, qualidade e outros sistemas.

✗ A) Incorreta. A introdução não traz requisitos.
✗ C) Incorreta. A 27001 tem requisitos próprios.
✗ D) Incorreta. O Anexo A lista controles de referência.

> **Dica de prova:** Requisitos: cláusulas 4 a 10.

D12. B) ISO/IEC 27001 → revise o capítulo 4

Por quê: A ISO/IEC 27001 é a norma de requisitos usada na certificação; a 27002 detalha como aplicar os controles do seu Anexo A.

✗ A) Incorreta. Traz orientações sobre controles.
✗ C) Incorreta. Trata de gestão ambiental.
✗ D) Incorreta. Trata de gestão da qualidade.

> **Dica de prova:** Requisitos do SGSI: 27001.

Agora, treine no formato real

Faça as 6 provas completas do curso EXIN ISFS ISO 27001: 240 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 EXIN. As questões são inéditas e não reproduzem a prova real.