ISO/IEC 27001:2022 + Amd 1:2024 Sistemas de Gestão da Segurança da Informação (SGSI)

Segurança da informação, SGSI, certificável em todo o mundo

181 requisitos. Esta norma é certificável por um organismo acreditado. Versão de 07/2026.

A norma ISO/IEC 27001 estabelece os requisitos para um sistema de gestão da segurança da informação: baseado em risco, documentado e com eficácia demonstrável. Uma avaliação face a esta norma é uma auditoria de certificação acreditada em duas fases (revisão documental e, depois, revisão de eficácia no local), seguida de auditorias de acompanhamento anuais e de recertificação ao fim de três anos.

Empresa	Data	Elaborado por

4 Contexto da organização 8

4.1-1 São determinadas e mantidas atualizadas as questões externas e internas que afetam a capacidade da organização para alcançar os resultados pretendidos do SGSI.

Como se comprova: Demonstra se através de uma análise de contexto, seja como documento autónomo, seja como secção do manual do SGSI: envolvente de mercado, situação de clientes e contratos, enquadramento legal (RGPD, NIS2), pilha tecnológica, número de colaboradores, dependência de fornecedores de nuvem. Para organizações pequenas, basta uma tabela de uma página com data e ciclo de revisão, desde que a revisão pela gestão mostre que é efetivamente atualizada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

4.1-2 A organização determinou se as alterações climáticas constituem uma questão relevante para si. A determinação é justificada, seja a resposta sim ou não.

Como se comprova: Este requisito foi introduzido pela Emenda 1:2024 e os auditores questionam especificamente sobre ele. Mantenha uma linha dedicada na análise de contexto: períodos de calor que afetam salas de servidores e disponibilidade, fenómenos meteorológicos extremos que afetam os centros de dados dos fornecedores de nuvem, estabilidade da rede elétrica. Um resultado justificado de não relevante é aceitável, uma entrada em falta não é.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

4.2-1 São determinadas as partes interessadas relevantes para o SGSI.

Como se comprova: Lista de partes interessadas que abrange clientes, colaboradores, subcontratantes e subsubcontratantes, autoridades de supervisão, seguradoras, o organismo de certificação e acionistas. Em organizações pequenas, basta uma tabela com parte, expectativa e origem da expectativa.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

4.2-2 São determinados os requisitos relevantes destas partes interessadas, incluindo eventuais requisitos relacionados com as alterações climáticas.

Como se comprova: Para cada parte, indique a origem concreta: cláusula contratual, acordo de tratamento de dados, questionário de cliente, obrigação legal. A Emenda 1:2024 acrescenta uma nota de que as partes interessadas podem ter requisitos relacionados com as alterações climáticas. Não se trata de um requisito autónomo, mas os auditores costumam levantar a questão, por exemplo em perguntas de sustentabilidade numa auditoria de fornecedores de um cliente relevante. Uma linha na tabela de partes interessadas com o resultado, incluindo nenhum requisito deste tipo, é suficiente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

4.2-3 É decidido e rastreável quais destes requisitos são tratados através do SGSI.

Como se comprova: Acrescente uma coluna à tabela de partes interessadas que remeta para a regra que trata o requisito (política, controlo, anexo contratual). Isto mostra que os requisitos não foram apenas recolhidos, mas efetivamente tratados.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

4.3-1 **O âmbito do SGSI é determinado e tem em conta as questões do ponto 4.1, os requisitos do ponto 4.2, bem como as interfaces e dependências com atividades realizadas por terceiros.**

Como se comprova: O âmbito indica locais, unidades organizacionais, produtos, sistemas e fronteiras de rede. As partes subcontratadas (alojamento, prestadores de pagamento, suporte) são descritas como interfaces com uma fronteira de responsabilidade clara. Um âmbito artificialmente reduzido que exclua processos centrais é rejeitado pelos organismos de certificação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

4.3-2 **O âmbito está disponível como informação documentada e estabelece de forma inequívoca as fronteiras do SGSI.** Documento

Como se comprova: Um documento de âmbito aprovado com versão, data e aprovação pela gestão de topo. A sua redação exata surge mais tarde no certificado, pelo que deve ser formulada com precisão e de forma a poder ser citada publicamente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

4.4-1 **O SGSI, incluindo os processos necessários e as suas interações, é estabelecido, implementado, mantido e continuamente melhorado.**

Como se comprova: Um mapa de processos ou lista de processos que ligue a gestão de risco, a gestão de incidentes, a gestão de mudanças, a auditoria e a revisão pela gestão a responsáveis e a uma periodicidade. A evidência viva importa mais do que o diagrama: registos, atas, entradas de calendário.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

5 Liderança 8

5.1-1 **A gestão de topo assume a responsabilidade pela eficácia do SGSI e assegura que a política e os objetivos são estabelecidos e são compatíveis com a orientação estratégica.**

Como se comprova: As evidências incluem aprovações assinadas da política, do âmbito e da Declaração de Aplicabilidade, atas de revisão pela gestão e decisões orçamentais documentadas. Em organizações muito pequenas, a gestão de topo é muitas vezes a mesma pessoa que o responsável pelo SGSI, o que é aceitável, mas deve ser declarado abertamente na definição de funções.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

5.1-2 **Os requisitos do SGSI estão integrados nos processos de negócio e é comunicada a importância de uma segurança da informação eficaz.**

Como se comprova: Fica melhor demonstrado quando a segurança não é uma pasta à parte: um critério de segurança na definição de concluído, uma verificação de segurança no processo de vendas ou de compras, um ponto de segurança recorrente nas atas das reuniões de equipa.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

5.1-3 **A gestão disponibiliza os recursos necessários, apoia as pessoas que contribuem para a eficácia do SGSI e promove a melhoria contínua.**

Como se comprova: Orçamento de segurança aprovado, tempo atribuído para formação, contratação de auditores externos ou de especialistas em testes de intrusão. Um registo de melhorias ou de ações com entradas ao longo de vários trimestres demonstra continuidade em vez de um esforço pontual.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

5.2-1 **É estabelecida uma política de segurança da informação adequada ao propósito da organização e que fornece um enquadramento para os objetivos de segurança da informação.** Documento

Como se comprova: Um documento de política curto e aprovado, duas a três páginas são suficientes. Indica os objetivos de proteção, o âmbito, as responsabilidades e o princípio de uma abordagem baseada em risco. Um texto genérico de modelo sem ligação ao negócio real destaca se negativamente na auditoria.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

5.2-2 **A política inclui um compromisso de satisfazer os requisitos aplicáveis e um compromisso de melhoria contínua do SGSI.** Documento

Como se comprova: Ambos os compromissos devem constar da política como frases explícitas, e são lidos palavra por palavra na auditoria da fase 1. Além disso, remeta para os processos subjacentes (registo legal, registo de melhorias).

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

5.2-3 **A política é comunicada dentro da organização e está disponível para as partes interessadas conforme apropriado.** Documento

Como se comprova: Evidência através de uma entrada na intranet ou wiki com obrigatoriedade de leitura, uma lista de verificação de integração com confirmação, ou um resumo publicado no sítio web. Uma lista de distribuição com comprovativos de receção é a prova sólida mais simples.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

5.3-1 **As responsabilidades e autoridades para funções relevantes para a segurança são atribuídas e comunicadas dentro da organização.**

Como se comprova: Uma matriz de funções (RACI) que abranja o responsável pelo SGSI, os responsáveis pelos riscos, os responsáveis pelos ativos, o coordenador de incidentes e o contacto de proteção de dados. Em equipas de uma só pessoa ou muito pequenas, atribua cada função a uma pessoa nomeada e documente abertamente a acumulação de funções resultante em vez de a esconder.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

5.3-2 **A autoridade para assegurar que o SGSI está em conformidade com a norma e para reportar o desempenho do SGSI à gestão de topo é atribuída a uma função.**

Como se comprova: Uma carta de nomeação ou descrição de funções para o responsável pelo SGSI, com uma linha de reporte explícita à gestão. A linha de reporte deve ser efetivamente evidenciada por atas de revisão pela gestão.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6 Planeamento 21

6.1.1-1 **Partindo das questões do ponto 4.1 e dos requisitos do ponto 4.2, são determinados os riscos e as oportunidades que precisam de ser tratados, de modo a que o SGSI alcance os resultados pretendidos e sejam evitados efeitos indesejados.**

Como se comprova: Um registo que liga as questões de contexto a riscos e oportunidades, mantido separadamente ou dentro do registo de riscos. O que importa é a rastreabilidade: cada questão da análise de contexto conduz visivelmente a uma avaliação ou a uma decisão justificada de não a considerar.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.1.1-2 **As ações para tratar estes riscos e oportunidades são planeadas, integradas nos processos do SGSI, e a sua eficácia é avaliada.**

Como se comprova: Plano de ação com responsável, prazo e critério de eficácia. Mantenha a avaliação de eficácia como uma coluna própria, caso contrário falta na auditoria a prova de que a ação não só foi implementada, como também verificada.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.1.2-1 **É definido e aplicado um processo de avaliação de risco de segurança da informação, que inclui critérios de aceitação de risco e critérios para a realização das avaliações de risco.** Documento

Como se comprova: Uma política de gestão de risco com escalas de probabilidade e impacto, uma matriz de risco definida e um limiar de aceitação claro. O limiar deve ser um número ou uma zona, não uma expressão como ao nosso critério.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.1.2-2 **O processo assegura que avaliações de risco repetidas produzem resultados consistentes, válidos e comparáveis.**

Como se comprova: Demonstrado através de uma metodologia fixa com escalas definidas e da comparação entre duas versões de avaliação: mesmos riscos, mesma lógica de classificação, diferenças explicáveis. Uma versão datada do registo de riscos do ano anterior é aqui a evidência mais forte.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.1.2-3 **São identificados riscos de segurança da informação para detetar a perda de confidencialidade, integridade e disponibilidade dentro do âmbito, e é atribuído um responsável a cada risco.**

Como se comprova: Registo de riscos que remete para ativos ou processos, os três objetivos de proteção e um responsável pelo risco nomeado. O responsável pelo risco deve ter autoridade para aceitar o risco; em organizações pequenas este é normalmente o diretor geral.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.1.2-4 **Os riscos identificados são analisados: são determinadas as consequências potenciais, a probabilidade realista e o nível de risco resultante.**

Como se comprova: Colunas para impacto, probabilidade e nível de risco resultante, cada uma com uma justificação breve. Uma frase de fundamentação por risco evita o achado de auditoria mais comum, nomeadamente números sem derivação.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.1.2-5 **Os riscos são comparados com os critérios de aceitação e priorizados para tratamento.**

Como se comprova: O registo de riscos deve mostrar quais os riscos que se situam acima do limiar de aceitação e por que ordem serão tratados. Uma vista ordenada ou uma coluna de prioridade são suficientes.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.1.2-6 **O processo de avaliação de risco está disponível como informação documentada.** Documento

Como se comprova: A própria metodologia é um documento obrigatório, não apenas o seu resultado. Uma política aprovada com versão e data de aprovação, ligada a partir do índice de documentos do SGSI.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.1.3-1 **Para cada risco acima do limiar de aceitação, é selecionada uma opção de tratamento adequada (reduzir, evitar, transferir ou aceitar).**

Como se comprova: Uma coluna de opção de tratamento no registo de riscos. Quando um risco é aceite, registe a justificação e a aprovação formal do responsável pelo risco; quando é transferido, indique o contrato ou a apólice de seguro.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6.1.3-2 **São determinados todos os controlos necessários para implementar as opções de tratamento de risco escolhidas.**

Como se comprova: Formule os controlos de forma concreta e verificável, com um responsável e um prazo. Remeter para trabalho técnico já em curso (implementação de MFA, teste de cópia de segurança) é aceitável desde que aponte para um registo ou para um elemento de configuração.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6.1.3-3 **Os controlos determinados são comparados com os controlos do Anexo A para verificar que nenhum controlo necessário foi omitido.**

Como se comprova: A comparação é um passo próprio e rastreável, não um subproduto. Evidenciada por uma coluna de correspondência no registo de riscos que remete para os números do Anexo A, mais atas datadas da comparação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6.1.3-4 **Existe uma Declaração de Aplicabilidade (DdA). Esta avalia individualmente todos os 93 controlos do Anexo A, indica a aplicabilidade com justificação para cada controlo, o estado de implementação, e a justificação para cada exclusão.** Documento

Como se comprova: A DdA é o documento obrigatório central e o mapa de toda a auditoria. Deve estar completa: os controlos não aplicáveis também surgem com uma justificação, nunca como uma linha em branco. Colunas recomendadas: número do controlo, título, aplicável sim ou não, justificação, estado de implementação, referência à política ou evidência, ligação ao risco. A versão e a aprovação pela gestão são obrigatórias, porque a DdA é confrontada com a realidade em cada auditoria de vigilância.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6.1.3-5 **É produzido um plano de tratamento de risco que reúne controlos, responsabilidades, prazos e recursos necessários.** Documento

Como se comprova: Pode ser uma folha numa base de cálculo de riscos ou um quadro de projeto. O que conta é que os prazos sejam realistas e que os prazos incumpridos tenham sido visivelmente reagendados, porque é exatamente isso que o auditor verifica.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6.1.3-6 **O plano de tratamento de risco é aprovado pelos responsáveis pelos riscos, e os riscos residuais remanescentes são formalmente aceites por eles.** Documento

Como se comprova: Assinatura, aprovação eletrónica ou uma decisão datada em ata. Uma linha na ata da revisão pela gestão que remeta para a versão do registo é suficiente, desde que a versão seja inequívoca.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6.1.3-7 **O processo de tratamento de risco está disponível como informação documentada.** Documento

Como se comprova: Normalmente coberto no mesmo documento de política da avaliação de risco. O fluxo desde a avaliação, passando pela seleção da opção, até à aceitação do risco residual deve estar descrito.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6.2-1 **São estabelecidos objetivos de segurança da informação para as funções e níveis relevantes, coerentes com a política e mensuráveis sempre que possível.**

Como se comprova: Uma folha de objetivos com três a seis objetivos, cada um com um indicador, um valor de partida, um valor alvo e um prazo. Exemplo: percentagem de sistemas com MFA elevada de 80 para 100 por cento até ao final do trimestre. Objetivos sem um número contam como não mensuráveis.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.2-2 **Os objetivos têm em conta os requisitos de segurança da informação aplicáveis, bem como os resultados da avaliação de risco e do tratamento de risco.**

Como se comprova: Acrescente uma coluna de origem à folha de objetivos: de que risco, que requisito de cliente ou que obrigação legal deriva o objetivo. Isto evita objetivos que pareçam arbitrários.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.2-3 **Os objetivos são monitorizados, comunicados e atualizados conforme necessário.**

Como se comprova: Acompanhamento trimestral do progresso na folha de objetivos, mais comunicação à equipa, por exemplo uma nota breve na wiki ou um ponto na ordem de trabalhos da reunião de equipa. Versões históricas demonstram que as atualizações acontecem.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.2-4 **Os objetivos de segurança da informação estão disponíveis como informação documentada.** Documento

Como se comprova: Basta um documento de objetivos aprovado e datado. Pode fazer parte da revisão pela gestão, mas tem de existir aí como secção própria e recuperável.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.2-5 **Para cada objetivo é planeado o que será feito, que recursos são necessários, quem é responsável, quando será concluído e como os resultados serão avaliados.**

Como se comprova: Estes cinco pontos são individualmente verificáveis e são pedidos individualmente na auditoria. Configure os como cinco colunas na folha de objetivos, e a conformidade fica visível de imediato.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

6.3-1 **Quando a organização determina que são necessárias alterações ao SGSI, essas alterações são realizadas de forma planeada.**

Como se comprova: Evidenciado por pedidos de alteração, atas ou registos que mostrem o motivo, a avaliação de impacto, a aprovação e a implementação. Motivos típicos em organizações pequenas: mudança de fornecedor de nuvem, novos locais, a primeira contratação.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7 Apoio 15

7.1-1 **São determinados e disponibilizados os recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI.**

Como se comprova: Uma rubrica orçamental de segurança, licenças de ferramentas (gestor de palavras passe, MDM, plataforma de registos), dias pessoa planeados para a manutenção do SGSI e serviços de auditoria externa. Uma fatura ou uma aprovação orçamental prova isto mais depressa do que qualquer texto.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7.2-1 **É determinada a competência necessária das pessoas cujo trabalho afeta o desempenho da segurança da informação.**

Como se comprova: Matriz de competências ou perfis de função que listam o conhecimento exigido por função, por exemplo desenvolvimento seguro para programadores, gestão de incidentes para o coordenador. Em equipas muito pequenas, basta uma linha por pessoa.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

7.2-2 **A competência é assegurada com base em educação, formação ou experiência adequadas.**

Como se comprova: Certificados, comprovativos de cursos, currículos ou experiência prática documentada. A autoformação é aceitável se for evidenciada, por exemplo por registos de conclusão de cursos em linha ou por testes internos de conhecimento aprovados.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

7.2-3 **Quando existem lacunas de competência, foram tomadas ações para as colmatar e a eficácia dessas ações foi avaliada.**

Como se comprova: Plano de formação com comparação entre previsto e realizado e uma verificação de eficácia, por exemplo uma pontuação de teste, uma taxa de cliques numa simulação de phishing ou observação no posto de trabalho. A verificação de eficácia é frequentemente esquecida e é um achado menor clássico.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

7.2-4 **Está disponível informação documentada adequada como evidência de competência.** Documento

Como se comprova: Uma pasta de competências ou de formação por pessoa, com evidências e datas. Em organizações pequenas, basta uma pasta com registos em PDF guardados mais uma tabela de resumo.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

7.3-1 **As pessoas que trabalham dentro do âmbito têm conhecimento da política de segurança da informação.**

Como se comprova: Confirmação na integração e após cada alteração à política, com data e versão. Uma funcionalidade de confirmação de leitura na wiki ou uma lista assinada são suficientes.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

7.3-2 **As pessoas conhecem o seu próprio contributo para a eficácia do SGSI e os benefícios de um melhor desempenho da segurança da informação.**

Como se comprova: Materiais de formação e listas de presenças nas quais a ligação ao trabalho da própria pessoa é visível. Os auditores entrevistam diretamente os colaboradores, pelo que a formação deve usar exemplos concretos do dia a dia em vez de citações abstratas da norma.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

7.3-3 **As pessoas conhecem as consequências do incumprimento dos requisitos do SGSI.**

Como se comprova: Indique as consequências nos diapositivos de formação e nas instruções de trabalho e ligue-as ao processo do ponto A.6.4. Mesmo organizações sem colaboradores devem cobrir isto para prestadores e trabalhadores independentes através dos respetivos contratos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

7.4-1 **É determinada a comunicação interna e externa relevante para o SGSI: o que é comunicado, quando, com quem e por que meio.**

Como se comprova: Uma matriz de comunicação com linhas como incidente de segurança para clientes, notificação à autoridade de supervisão no prazo de 72 horas, relatório de estado mensal para a gestão. É a base da comunicação de crise e é revista após cada incidente.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7.5.1-1 **O SGSI inclui a informação documentada exigida pela norma, bem como a informação documentada que a organização determinou ser necessária para a eficácia do SGSI.** Documento

Como se comprova: Um índice de documentos que lista todos os documentos do SGSI com finalidade, responsável, versão e local de armazenamento. Mostra que os documentos obrigatórios estão completos e é o ponto de entrada mais rápido para o auditor.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7.5.2-1 **Ao criar e atualizar documentos, são asseguradas a identificação, o formato e o suporte adequados, e os documentos são revistos e aprovados quanto à sua adequação.**

Como se comprova: Um cabeçalho de documento uniforme com título, versão, data, autor e aprovador. Em ambientes baseados em Git, as revisões de pull request com aprovação satisfazem o requisito de revisão e aprovação, desde que o histórico seja imutável.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7.5.3-1 **A informação documentada está disponível e adequada para utilização onde e quando é necessária.**

Como se comprova: Um local de armazenamento central acessível a todos os que a ele têm direito, com função de pesquisa. Testável por amostragem: qualquer instrução de trabalho deve ser encontrável em menos de um minuto.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7.5.3-2 **A informação documentada é adequadamente protegida, em particular contra perda de confidencialidade, utilização indevida e perda de integridade.**

Como se comprova: Direitos de acesso baseados em funções aos documentos do SGSI, controlo de versões com histórico, proteção de escrita para versões aprovadas e cópia de segurança do repositório de documentos. A evidência da cópia de segurança é a parte mais frequentemente esquecida.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7.5.3-3 **São regidas a distribuição, o acesso, a recuperação, o armazenamento, o controlo de alterações, bem como a retenção e o destino final da informação documentada.**

Como se comprova: Uma regra breve de controlo de documentos com prazos de retenção e regras de eliminação. Deve ser conciliada com obrigações legais (direito comercial, direito fiscal, RGPD) e é a base dos pontos A.5.33 e A.8.10.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7.5.3-4 **A informação documentada de origem externa necessária para planear e operar o SGSI é identificada e controlada.**

Como se comprova: Uma lista de documentos externos com versão e origem: normas, textos legais, guias de reforço de fornecedores, documentação de segurança da nuvem, acordos de tratamento de dados. Sem referência de versão, o controlo não pode ser demonstrado.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

8 Operação 8

8.1-1 **Os processos necessários para cumprir os requisitos de segurança da informação e para implementar as ações da secção 6 são planeados, implementados e controlados, e são estabelecidos critérios para esses processos.**

Como se comprova: Um manual de operações ou procedimentos operacionais com critérios claros, por exemplo o tempo máximo para implementar correções críticas, critérios de aprovação para implantações, limiares de alerta. Critérios sem números não têm valor na auditoria.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

8.1-2 **Está disponível informação documentada na medida necessária para dar confiança de que os processos foram realizados conforme planeado.** Documento

Como se comprova: Registos operacionais como evidência: histórico de registos, execuções do pipeline de integração contínua, relatórios de correções, registos de cópias de segurança, revisões de acesso. Estes registos são a prova efetiva de eficácia na auditoria da fase 2.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

8.1-3 **As alterações planeadas são controladas e as consequências de alterações não intencionais são analisadas; sempre que necessário, os efeitos adversos são mitigados.**

Como se comprova: Um processo de gestão de mudanças com aprovação e um caminho de reversão, ligado ao ponto A.8.32. Para alterações não intencionais (configuração incorreta, elevação de privilégios acidental), documente o incidente e evidencie a correção.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

8.1-4 **São determinados e controlados os processos, produtos e serviços fornecidos externamente que são relevantes para o SGSI.**

Como se comprova: Uma lista de fornecedores com criticidade, referência contratual e estado da evidência (o certificado ISO 27001 do fornecedor, relatório SOC 2, acordo de tratamento de dados). Para organizações pequenas, esta é a maior alavanca, porque a maior parte das TI já funciona externamente.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

8.2-1 **As avaliações de risco são realizadas em intervalos planeados e sempre que ocorram alterações ou incidentes significativos, tendo em conta os critérios estabelecidos.**

Como se comprova: Um ritmo (tipicamente anual), mais motivos definidos para avaliações não programadas. Evidenciado por versões datadas do registo de riscos e entradas no calendário ou no sistema de registos.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

8.2-2 **Os resultados das avaliações de risco são retidos como informação documentada.** Documento

Como se comprova: Versões históricas do registo de riscos com datas, não apenas o estado atual. Sobrescrever o ficheiro torna impossível provar a evolução; o controlo de versões no sistema de ficheiros ou em Git resolve isto.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

8.3-1 **O plano de tratamento de risco é implementado.**

Como se comprova: Compare o plano com a realidade: ações concluídas com data de implementação e um elemento concreto (configuração, política, contrato). As ações em aberto precisam de uma justificação documentada e de um novo prazo alvo.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

8.3-2 **Os resultados do tratamento de risco são retidos como informação documentada.** Documento

Como se comprova: Relatórios de estado ou ações encerradas com referência à evidência. O registo por si só é suficiente se cada linha tiver uma data de conclusão e uma ligação à evidência.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

9 Avaliação do desempenho 21

9.1-1 **É determinado o que precisa de ser monitorizado e medido, incluindo os processos e controlos de segurança da informação.**

Como se comprova: Uma folha de indicadores com um número gerível de medidas sólidas: pendência de correções, cobertura de MFA, tempo de resolução de incidentes, resultado do último teste de restauro, achados em aberto. Alguns indicadores que são efetivamente recolhidos valem mais do que uma lista de desejos extensa.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

9.1-2 **Os métodos de monitorização, medição, análise e avaliação são definidos e produzem resultados válidos.**

Como se comprova: Documente a fonte de dados e o cálculo de cada indicador, por exemplo uma exportação do detetor de vulnerabilidades ou do relatório do fornecedor de identidade. A rastreabilidade da fonte é o cerne da validade.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

9.1-3 **É definido quando e por quem são realizadas a monitorização e a medição, e quando os resultados são analisados e avaliados.**

Como se comprova: Acrescente colunas de periodicidade e responsável à folha de indicadores. Um compromisso recorrente no calendário para a avaliação prova a regularidade melhor do que qualquer descrição.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

9.1-4 **Os resultados da monitorização e da medição são retidos como informação documentada.** Documento

Como se comprova: Avaliações arquivadas, painéis exportados ou uma folha de indicadores mantida como série temporal. Uma vista em tempo real sem histórico não satisfaz o requisito.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

9.1-5 **O desempenho da segurança da informação e a eficácia do SGSI são avaliados com base nos resultados da medição.**

Como se comprova: Uma avaliação escrita, não apenas números: tendência, causas, necessidade de ação. Este texto de avaliação é, ao mesmo tempo, um contributo para a revisão pela gestão.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

9.2.1-1 **São realizadas auditorias internas em intervalos planeados, que fornecem informação sobre se o SGSI está em conformidade com os requisitos próprios da organização e com os requisitos da norma, e se está efetivamente implementado.**

Como se comprova: Antes da auditoria de certificação, tem de estar concluído pelo menos um ciclo completo de auditoria interna que abranja todo o âmbito. Sem isso, a certificação está fora de alcance; este é um dos obstáculos mais comuns em primeiras certificações.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

9.2.2-1 **É planeado, estabelecido e mantido um programa de auditorias, que define periodicidade, métodos, responsabilidades, requisitos de planeamento e relato, e que tem em conta a importância dos processos em causa e os resultados de auditorias anteriores.**

Como se comprova: Um programa de auditorias plurianual que abrange todas as secções e todos os controlos aplicáveis ao longo do ciclo de certificação, com maior frequência para as áreas críticas. Uma tabela simples que abranja três anos é inteiramente suficiente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.2.2-2 **São definidos os critérios e o âmbito de auditoria para cada auditoria.**

Como se comprova: Um plano de auditoria por data com os critérios (a norma, as políticas internas, os contratos) e um âmbito claro. Um plano de auditoria de uma página por auditoria é suficiente e serve também de base para o relatório.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.2.2-3 **Os auditores são selecionados e as auditorias são conduzidas de forma a assegurar objetividade e imparcialidade. Ninguém audita o seu próprio trabalho.**

Como se comprova: A independência é aqui o obstáculo difícil: quem escreveu as políticas e configurou os sistemas não pode auditá-las. Em organizações muito pequenas, isto significa quase sempre um auditor interno externo, por exemplo um consultor contratado ou um colega de uma empresa parceira; um contrato de auditoria mais a declaração de independência do auditor são a evidência. Só em equipas suficientemente grandes é que a função pode rodar internamente para uma pessoa sem responsabilidade pela área auditada, e isso tem então de ficar demonstrado na matriz de funções.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.2.2-4 **Os resultados da auditoria são reportados à gestão relevante.**

Como se comprova: Um relatório de auditoria com achados, não conformidades, recomendações e uma lista de distribuição, mais evidência da entrega à gestão, por exemplo um ponto em ata ou uma entrega por correio eletrónico datada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.2.2-5 **É retida informação documentada sobre o programa de auditorias e os resultados das auditorias.** Documento

Como se comprova: Mantenha o programa de auditorias, os planos de auditoria, os relatórios de auditoria e as ações resultantes num único local. A ligação entre um achado e uma ação corretiva (secção 10.2) deve ser visível de ponta a ponta.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.1-1 **A gestão de topo revê o SGSI em intervalos planeados para assegurar a sua contínua pertinência, adequação e eficácia.**

Como se comprova: Pelo menos anualmente e agendada antes da auditoria externa. Mesmo em organizações muito pequenas tem de haver atas datadas e assinadas, mesmo quando a gestão e o responsável pelo SGSI são a mesma pessoa.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.2-1 **A revisão pela gestão tem em conta o estado das ações de revisões pela gestão anteriores.**

Como se comprova: A ata começa com uma tabela de seguimento das decisões do ano anterior e o seu estado atual. Sem esta referência retrospetiva, a revisão conta como incompleta.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.2-2 **A revisão pela gestão tem em conta as alterações nas questões externas e internas relevantes para o SGSI, incluindo aspetos relevantes das alterações climáticas.**

Como se comprova: Um ponto próprio na ordem de trabalhos que remete para a análise de contexto atualizada. As alterações climáticas não são referidas explicitamente no texto desta secção (a Emenda 1:2024 altera apenas os pontos 4.1 e 4.2), mas entram aqui através das alterações nas questões do ponto 4.1, e os auditores esperam encontrá-las. Mesmo um resultado de não relevante, sem alteração, deve constar da ata.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.2-3 **A revisão pela gestão tem em conta as alterações nas necessidades e expectativas das partes interessadas relevantes para o SGSI.**

Como se comprova: Novos requisitos de clientes provenientes de contratos e questionários de segurança, novas obrigações legais, requisitos do organismo de certificação. Registe-os como uma lista com origens na ata.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.2-4 **A revisão pela gestão tem em conta o retorno sobre o desempenho da segurança da informação, incluindo não conformidades e ações corretivas, resultados de monitorização e medição, resultados de auditoria e o cumprimento dos objetivos de segurança da informação.**

Como se comprova: Trate estes quatro blocos como pontos separados na ordem de trabalhos, caso contrário um deles acabará por faltar na ata. Anexe a folha de indicadores, o relatório de auditoria e a folha de objetivos como anexos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.2-5 **A revisão pela gestão tem em conta o retorno das partes interessadas.**

Como se comprova: Reclamações de clientes com uma dimensão de segurança, resultados de auditorias de clientes, comunicações do canal de denúncias, retorno de prestadores de serviços. Registe na ata mesmo quando a conclusão é que não foi recebido nenhum.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.2-6 **A revisão pela gestão tem em conta os resultados da avaliação de risco e o estado do plano de tratamento de risco.**

Como se comprova: Anexe o registo de riscos atual e o estado de implementação do plano de tratamento, com confirmação explícita da aceitação do risco residual pelos responsáveis pelos riscos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.2-7 **A revisão pela gestão tem em conta oportunidades de melhoria contínua.**

Como se comprova: Um ponto na ordem de trabalhos com ideias de melhoria concretas e uma decisão sobre cada uma. As ideias aceites passam para o registo de melhorias como entradas com prazos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.3-1 **Os resultados da revisão pela gestão incluem decisões sobre oportunidades de melhoria contínua e sobre qualquer necessidade de alterações ao SGSI.**

Como se comprova: A ata termina com uma secção de decisões: decisão, responsável, prazo. Atas sem decisões são um achado na auditoria, porque falta então o efeito de liderança.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9.3.3-2 **É retida informação documentada como evidência dos resultados da revisão pela gestão.** Documento

Como se comprova: Ata assinada com data, participantes, elementos de entrada, avaliação e decisões. É um dos primeiros documentos que um organismo de certificação pede na fase 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

10 Melhoria 7

10.1-1 **A pertinência, a adequação e a eficácia do SGSI são continuamente melhoradas.**

Como se comprova: Um registo de melhorias alimentado por várias fontes (auditorias, incidentes, ideias, desvios de indicadores) com progresso visível ao longo do tempo. A continuidade ao longo de vários meses é a prova, não o número de entradas.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

10.2-1 **Quando ocorre uma não conformidade, a organização reage a ela: controla-a e corrige-a, e lida com as consequências.**

Como se comprova: Um relatório de não conformidade com uma ação imediata e uma data. As origens são auditorias internas, auditorias externas, incidentes e observações da operação diária; todas elas alimentam o mesmo registo.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

10.2-2 **É avaliado se é necessária ação para eliminar as causas, de modo a que a não conformidade não se repita nem ocorra noutro local; isto inclui verificar se existem ou poderiam ocorrer não conformidades semelhantes.**

Como se comprova: Documente a análise de causa raiz, por exemplo com os 5 Porquês ou o diagrama de Ishikawa, mais uma declaração explícita sobre a aplicabilidade a outros sistemas ou processos. O passo da aplicabilidade é o que mais frequentemente é omitido.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

10.2-3 **São implementadas quaisquer ações corretivas necessárias e a sua eficácia é analisada.**

Como se comprova: Para cada ação, registe a data de implementação, o elemento de evidência e uma análise de eficácia posterior com data própria. Dois campos de data por linha são a forma mais simples de não perder a análise de eficácia.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

10.2-4 **Sempre que necessário, são feitas alterações ao SGSI em resultado da não conformidade.**

Como se comprova: Se uma não conformidade tiver origem numa lacuna de uma política, do registo de riscos ou da DdA, a alteração tem de ficar visível aí. Uma referência da não conformidade para a versão de documento atualizada fecha a cadeia.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

10.2-5 **As ações corretivas são adequadas aos efeitos das não conformidades encontradas.**

Como se comprova: Uma classificação de gravidade no registo, da qual resulte evidente a proporcionalidade da ação. Nem trivialidades tratadas como um projeto, nem desvios graves respondidos com um mero correio eletrónico de lembrete.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

10.2-6 **É retida informação documentada sobre a natureza das não conformidades, as ações tomadas em resposta e os resultados das ações corretivas.** Documento

Como se comprova: Um registo de não conformidades e ações corretivas com colunas para natureza, causa, ação, responsável, prazo e resultado da análise de eficácia. É evidência obrigatória e é solicitado em todas as auditorias de vigilância.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5 Anexo A: Controlos organizacionais 37

A.5.1 **Políticas de segurança da informação: São definidas uma política de segurança da informação abrangente e políticas específicas por tema, aprovadas pela gestão, comunicadas e revistas em intervalos planeados e sempre que ocorram alterações significativas.** Documento

Como se comprova: Um conjunto de políticas com versão, data de aprovação e próxima data de revisão, mais evidência de confirmação de leitura. Para organizações pequenas, basta uma política quadro e um punhado de políticas temáticas (acesso, criptografia, trabalho remoto, incidentes).

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.2 **Funções e responsabilidades de segurança da informação: As funções e responsabilidades de segurança da informação são definidas e atribuídas de acordo com as necessidades da organização.**

Como se comprova: Uma matriz de funções com nomes, substitutos e tarefas. Em organizações muito pequenas, indique abertamente onde várias funções se acumulam numa só pessoa e ligue isto aos controlos compensatórios do ponto A.5.3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.3 **Segregação de funções: As funções e áreas de responsabilidade destinadas a controlar-se mutuamente não são exercidas por uma única pessoa. O objetivo é que ninguém possa iniciar, aprovar e ocultar uma alteração por conta própria.**

Como se comprova: Em organizações pequenas, a segregação total é estruturalmente impossível; uma afirmação genérica de conformidade desmorona-se de imediato na entrevista de auditoria. O que se sustenta é uma análise honesta: quais as combinações de funções que são críticas (desenvolver e lançar, conceder direitos e utilizá-los, iniciar e aprovar pagamentos), quais delas recaem numa só pessoa, e que controlos compensatórios se aplicam. Abordagens comprovadas são registos de auditoria imutáveis acessíveis a um terceiro, MFA em contas privilegiadas, portas de controlo automatizadas na integração contínua e proteção de ramos em vez da revisão a quatro olhos, uma revisão periódica de registos por uma pessoa externa, e aprovação separada para pagamentos. Mantenha a análise e os controlos compensatórios como um documento próprio e datado, e ligue-o a partir da DdA.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.4 **Responsabilidades da gestão: A gestão exige que todo o pessoal aplique a segurança da informação em conformidade com as políticas e procedimentos estabelecidos.**

Como se comprova: Um compromisso nos contratos de trabalho e de prestação de serviços, confirmação de leitura das políticas na integração, e lembretes regulares por parte da gestão. Evidência: declarações de compromisso assinadas e atas de reunião.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.5 **Contacto com autoridades: São mantidos contactos adequados com as autoridades relevantes, que podem ser contactadas quando necessário.**

Como se comprova: Uma lista de contactos com a autoridade de proteção de dados competente, a polícia ou a unidade de cibercrime, o ponto nacional de comunicação de cibersegurança e, quando aplicável, os canais de comunicação do NIS2. Registe os prazos (como as 72 horas do RGPD) diretamente na lista.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.6 **Contacto com grupos de interesse específico: São mantidos contactos com grupos de interesse específico, fóruns de segurança e associações profissionais.**

Como se comprova: Filiações, alertas subscritos (CERT nacional, feeds de fornecedores), participação em grupos de interesse específico. Uma prova simples: uma lista de subscrições mais um exemplo de como um alerta conduziu a uma ação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.7 **Informação sobre ameaças: É recolhida e analisada informação sobre ameaças à segurança da informação, para dela derivar ações adequadas.**

Como se comprova: Novidade na edição de 2022. Exequível para organizações pequenas: subscrever alertas do CERT nacional e alertas de fornecedores, e depois realizar uma revisão mensal breve com uma decisão de relevância e registos dela derivados. A evidência é a análise, não a subscrição.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.8 **Segurança da informação na gestão de projetos: A segurança da informação está integrada na gestão de projetos, independentemente do tipo de projeto.**

Como se comprova: Pontos de segurança na lista de verificação do projeto: necessidades de proteção, revisão de risco, verificação de proteção de dados, aprovação de segurança antes do arranque em produção. Em equipas ágeis, fixe-os como pontos permanentes na definição de pronto e na definição de concluído.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.9 **Inventário de informação e de outros ativos associados: É criado e mantido um inventário de informação e de outros ativos associados, com responsáveis nomeados.**

Como se comprova: Um inventário de ativos que abrange equipamento, software, serviços de nuvem, repositórios de dados, domínios e contas, cada um com um responsável e as suas necessidades de proteção. Em organizações pequenas, pode ser reunido automaticamente a partir de uma exportação do MDM, de uma lista de licenças e da consola de nuvem; uma data atual é obrigatória.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.10 **Utilização aceitável de informação e de outros ativos associados: São identificadas, documentadas e implementadas regras para a utilização aceitável e o tratamento de informação e de outros ativos associados.** Documento

Como se comprova: Uma política de utilização aceitável para equipamentos, redes, contas de nuvem e ferramentas de IA, com confirmação de leitura. Os dispositivos pessoais e os serviços de IA externos devem ser cobertos explicitamente, porque é aí que ocorre a maior parte das fugas de informação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.11 **Devolução de ativos: Quando uma relação de trabalho termina ou é alterada, é regida e confirmada por escrito a devolução de todos os equipamentos, chaves, contas e documentos atribuídos.**

Como se comprova: Uma lista de verificação de saída com comprovativo de devolução de portátil, tokens, chaves, certificados e suportes de armazenamento, mais a desativação da conta no mesmo dia. Isto aplica-se igualmente a trabalhadores independentes e estagiários.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.12 **Classificação da informação: A informação é classificada de acordo com as suas necessidades de proteção em termos de confidencialidade, integridade, disponibilidade e requisitos legais.**

Como se comprova: Um esquema simples com três ou quatro níveis (público, interno, confidencial, estritamente confidencial) e regras de tratamento concretas por nível. Registe a atribuição no inventário de ativos ou no registo das atividades de tratamento.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.13 **Rotulagem da informação: O nível de classificação é reconhecível no próprio documento, ficheiro ou mensagem, de modo a que os destinatários saibam como o tratar sem terem de perguntar.**

Como se comprova: Rotulagem no cabeçalho do documento, no nome do ficheiro, no assunto do correio eletrónico ou através de etiquetas de sensibilidade no pacote de escritório na nuvem. Evidência através de amostras de documentos efetivamente rotulados, não apenas através da regra.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.14 **Transferência de informação: Estão implementadas regras, procedimentos e acordos para a transferência de informação dentro da organização e com terceiros.**

Como se comprova: Uma regra que indica que canal é permitido para que nível de classificação: correio eletrónico cifrado ou uma sala de dados para conteúdo confidencial, sem envio através de aplicações de mensagens pessoais. Sustente as transferências confidenciais com acordos de confidencialidade.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.15 **Controlo de acesso: São estabelecidas e implementadas regras para controlar o acesso físico e lógico à informação e a outros ativos associados, com base nos requisitos de negócio e de segurança.**

Como se comprova: Uma política de controlo de acesso que segue os princípios da necessidade de conhecer e do privilégio mínimo, com um mapeamento de funções para direitos. Evidência através da configuração real de direitos no fornecedor de identidade, não apenas através da política.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.16 **Gestão de identidades: É gerido o ciclo de vida completo das identidades.**

Como se comprova: Um processo desde a criação, passando pela alteração, até à desativação, idealmente centralizado num fornecedor de identidade com início de sessão único. Sem contas de grupo partilhadas; quando tecnicamente inevitável, nomeie a conta, justifique-a e registe a sua utilização.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.17 **Informação de autenticação: A atribuição e a gestão da informação de autenticação são controladas por um processo de gestão que exige que as pessoas a tratem corretamente.**

Como se comprova: Um gestor de palavras passe como ferramenta obrigatória, uma política de qualidade de palavras passe e MFA, acesso inicial seguro e um procedimento de reposição com verificação de identidade. Evidência através de capturas de ecrã da configuração e do relatório do gestor de palavras passe.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.18 **Direitos de acesso: Os direitos de acesso são atribuídos, revistos, alterados e removidos de acordo com a política de controlo de acesso.**

Como se comprova: Uma revisão periódica de acessos, pelo menos anual, com resultado documentado por conta e evidência dos direitos removidos. A remoção no dia da saída é um ponto que os auditores gostam de seguir através de um caso concreto.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.19 **Segurança da informação nas relações com fornecedores: São definidos e implementados processos e procedimentos para gerir os riscos de segurança decorrentes da utilização de produtos e serviços de terceiros.**

Como se comprova: Uma lista de fornecedores com um nível de criticidade e a profundidade de avaliação. Para fornecedores críticos, obtenha evidências (certificado ISO 27001, relatório SOC 2) em vez de realizar auditorias próprias, o que é a única via realista para organizações pequenas.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.20 **Tratamento da segurança da informação nos acordos com fornecedores: São acordados com cada fornecedor os requisitos de segurança relevantes, estabelecidos nos contratos.**

Como se comprova: Um anexo contratual de segurança da informação com deveres de notificação de incidentes, regras sobre subsubcontratantes, obrigações de eliminação e direitos de auditoria. Para serviços padrão, os termos do fornecedor mais um acordo de tratamento de dados são suficientes, desde que o seu conteúdo tenha sido revisto e documentado.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.21 **Gestão da segurança da informação na cadeia de fornecimento de TIC: São definidos e implementados processos para gerir os riscos de segurança na cadeia de fornecimento de tecnologias de informação e comunicação.**

Como se comprova: Isto abrange as dependências de software e os próprios subfornecedores dos fornecedores. Na prática: uma lista de materiais de software (SBOM) ou lista de dependências, verificações automatizadas de pacotes vulneráveis na integração contínua, e obtenção de software apenas através de canais assinados ou oficiais.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.22 **Monitorização, revisão e gestão de alterações de serviços de fornecedores: As alterações aos serviços dos fornecedores são regularmente monitorizadas, revistas e geridas.**

Como se comprova: Uma revisão anual de fornecedores que analisa incidentes, relatórios de disponibilidade e validade de certificados, mais um canal para os anúncios de alterações do fornecedor. Registe o resultado como uma nota breve por fornecedor.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.23 **Segurança da informação na utilização de serviços de nuvem: São estabelecidos processos para adquirir, utilizar, gerir e cessar serviços de nuvem, em conformidade com os requisitos de segurança.**

Como se comprova: Novidade na edição de 2022 e o controlo central para organizações pequenas assentes na nuvem. Evidência através de uma política de nuvem com um processo de aprovação para novos serviços, um modelo de responsabilidade partilhada documentado por serviço, definições de reforço, e uma estratégia de saída que inclua a devolução de dados e a confirmação de eliminação.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.24 **Planeamento e preparação da gestão de incidentes de segurança da informação: São planeados e estabelecidos os processos, funções e responsabilidades para a gestão de incidentes.** Documento

Como se comprova: Um plano de resposta a incidentes com o percurso de comunicação, funções, níveis de escalonamento, contactos fora de horas e modelos de comunicação. Realista para equipas pequenas: uma página, mas praticada.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.25 **Avaliação e decisão sobre eventos de segurança da informação: Os eventos de segurança são avaliados e é tomada uma decisão sobre se devem ser classificados como incidentes de segurança da informação.**

Como se comprova: Critérios de triagem com uma matriz de gravidade e um registo de eventos no qual também constam os eventos descartados, com justificação. A separação entre evento e incidente tem de ser visível no registo.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.26 **Resposta a incidentes de segurança da informação: Os incidentes são tratados de acordo com os procedimentos documentados.**

Como se comprova: Processos de incidentes com uma cronologia, as ações tomadas, as pessoas envolvidas e a decisão de encerramento. Se ainda não ocorreu nenhum incidente real, um exercício de simulação documentado é a melhor evidência disponível.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.27 **Aprendizagem a partir de incidentes de segurança da informação: O conhecimento obtido a partir de incidentes é utilizado para reforçar os controlos de segurança.**

Como se comprova: Uma análise pós-incidente sem atribuição de culpa, com análise de causa raiz e ações derivadas, ligada ao registo de melhorias e, quando necessário, ao registo de riscos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.28 **Recolha de evidências: É regido o modo como os vestígios relacionados com um evento de segurança são identificados, preservados e retidos, de forma a permanecerem utilizáveis mais tarde.**

Como se comprova: Um procedimento breve de preservação de evidências: não reconstruir sistemas prematuramente, preservar imagens e registos, documentar a cadeia de custódia. Para organizações pequenas, basta definir o nível de gravidade a partir do qual é chamado um prestador de perícia forense externo, juntamente com os respetivos contactos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.29 **Segurança da informação durante uma interrupção: A organização planeia como a segurança da informação é mantida a um nível adequado durante uma interrupção.**

Como se comprova: As disposições de emergência não podem desligar a segurança. Documente que a MFA, o registo de eventos e as restrições de acesso também se aplicam em funcionamento de contingência, e que as contas de emergência (contas de break-glass) estão lacradas, documentadas e são revistas posteriormente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.30 **Prontidão das TIC para a continuidade de negócio: A prontidão das TIC é planeada, implementada, mantida e testada com base nos objetivos de continuidade de negócio e nos requisitos de continuidade das TIC.**

Como se comprova: Novidade na edição de 2022. Evidência através de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO) definidos por sistema crítico, um procedimento de recuperação e pelo menos um teste documentado por ano. Um teste de restauro bem sucedido, com data e duração, é a evidência isolada mais forte.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.31 **Requisitos legais, estatutários, regulamentares e contratuais: São identificados, documentados e mantidos atualizados os requisitos relevantes e a abordagem para os cumprir.** Documento

Como se comprova: Um registo legal que abrange o RGPD, o direito das telecomunicações, o direito comercial e fiscal, e, quando aplicável, o NIS2 ou regras específicas do setor, cada um com a regra que o implementa e a data de revisão. Uma revisão anual é suficiente, mas tem de estar datada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.32 **Direitos de propriedade intelectual: São implementados procedimentos adequados para proteger os direitos de propriedade intelectual.**

Como se comprova: Um inventário de licenças do software em utilização, uma verificação das licenças de código aberto no produto (um verificador de licenças na integração contínua) e uma regra para o tratamento de código de terceiros e código gerado. Evidência: o relatório de licenças da compilação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.5.33 **Proteção de registos: Os registos de negócio e de evidência são armazenados de modo a que não se possam perder, não possam ser alterados sem deteção e não possam cair em mãos erradas, e isto aplica-se durante todo o período de retenção.**

Como se comprova: Um calendário de retenção com os prazos legais, armazenamento resistente a adulteração, acesso restrito e cópia de segurança. Para registos relevantes para efeitos fiscais, indique explicitamente os prazos de retenção legais, pois os auditores gostam de verificar isso especificamente.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.34 **Privacidade e proteção de dados pessoais: São identificados e cumpridos, em conformidade com a legislação aplicável, os requisitos de privacidade e de proteção de informação pessoal identificável.**

Como se comprova: Registo das atividades de tratamento, acordos de tratamento de dados, um conceito de eliminação, um processo para os direitos dos titulares dos dados e, quando exigido, uma avaliação de impacto sobre a proteção de dados. Ligar isto ao SGSI através de uma lista de ativos partilhada evita manter tudo em duplicado.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.35 **Revisão independente da segurança da informação: A abordagem da organização à gestão da segurança da informação é revista de forma independente em intervalos planeados e sempre que ocorram alterações significativas.**

Como se comprova: Evidenciado pela auditoria interna realizada por um auditor independente, por testes de intrusão externos ou pela própria auditoria de certificação. Independente significa não realizada pela pessoa responsável pela área em revisão.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.36 **Conformidade com políticas, regras e normas de segurança da informação: É revista regularmente a conformidade com as políticas de segurança próprias da organização e com as regras aplicáveis.**

Como se comprova: Verificações de conformidade com data e resultado, por exemplo uma verificação de configuração face à sua própria base de reforço, amostragem da rotulagem de documentos, verificações automatizadas de políticas na nuvem. Os desvios alimentam o registo de ações corretivas.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.5.37 **Procedimentos operacionais documentados: Os procedimentos operacionais das instalações de processamento de informação são documentados e disponibilizados às pessoas que deles necessitam.** Documento

Como se comprova: Procedimentos operacionais para cópia de segurança e restauro, implantação, administração de utilizadores, aplicação de correções e gestão de incidentes. Curto e atual vale mais do que extenso e desatualizado; uma data da última alteração por procedimento é obrigatória.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.6 Anexo A: Controlos relativos às pessoas 8

A.6.1 **Verificação de antecedentes: Os candidatos que irão trabalhar para a organização são previamente verificados, dentro dos limites da lei e de forma proporcional às necessidades de proteção; para funções sensíveis, a verificação é repetida durante o vínculo.**

Como se comprova: Sem colaboradores, este controlo pode ser justificado como atualmente não aplicável, mas o procedimento para o caso de uma contratação deve ainda assim ser definido e registado na Declaração de Aplicabilidade como planeado. Um âmbito exequível: verificação de identidade, currículo e referências, mais certificados; verificação de registo criminal apenas quando as necessidades de proteção o justifiquem e a lei o permita. Exija o mesmo padrão a trabalhadores independentes e prestadores através dos respetivos contratos, caso contrário a lacuna abre-se exatamente aí.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.6.2 **Termos e condições de trabalho: Os acordos contratuais estabelecem as responsabilidades de segurança da informação do pessoal e da organização.**

Como se comprova: Uma cláusula de segurança no contrato de trabalho ou de prestação de serviços, que remete para as políticas aplicáveis. Para trabalhadores independentes, a mesma cláusula no contrato de prestação de serviços, mais um acordo de confidencialidade.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.6.3 **Sensibilização, educação e formação em segurança da informação: O pessoal e as partes externas relevantes recebem sensibilização e formação adequadas, bem como atualizações regulares sobre as políticas da organização.**

Como se comprova: Formação anual com evidência de presença e data, complementada por simulações de phishing com uma taxa de cliques avaliada. Mesmo trabalhadores independentes a título individual precisam de evidência da sua própria formação contínua, por exemplo comprovativos de cursos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.6.4 **Processo disciplinar: Existe um processo formal e comunicado para tomar medidas contra pessoas que tenham violado as políticas de segurança.**

Como se comprova: Sem colaboradores, isto pode ser justificado como atualmente não aplicável, mas o processo tem ainda assim de estar definido para o caso de uma contratação; apenas a sua aplicação caduca, não a regra. O que é exigido é uma escala de respostas graduada e comunicada (conversa, repreensão, advertência formal, despedimento), em conformidade com o direito do trabalho e as regras de representação dos trabalhadores. Para prestadores, reflita o nível de sanção no contrato, por exemplo uma cláusula penal ou um direito de rescisão.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.6.5 **Responsabilidades após a cessação ou alteração do vínculo: As responsabilidades e deveres de segurança que permanecem válidos após a cessação ou uma alteração de função são definidos, aplicados e comunicados às pessoas envolvidas.**

Como se comprova: Uma lista de verificação de saída com remoção de direitos, devolução de ativos, transição de funções, e um lembrete explícito das obrigações de confidencialidade que se mantêm. Um registo assinado da entrevista de saída é a evidência mais simples.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.6.6 **Acordos de confidencialidade ou de não divulgação: É determinado quem tem de assinar um acordo de confidencialidade. O conteúdo corresponde às necessidades de proteção da informação, os acordos são assinados, arquivados e revistos regularmente para se manterem atuais.**

Como se comprova: Acordos de confidencialidade assinados para colaboradores, trabalhadores independentes, prestadores de serviços e estagiários, com um período de subsistência. Uma tabela de resumo com contraparte, data e validade torna a carteira auditável.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.6.7 **Trabalho remoto: São implementadas medidas de segurança quando as pessoas trabalham fora das instalações da organização e, nesse contexto, acedem a informação da organização.**

Como se comprova: Uma política de teletrabalho e trabalho remoto com requisitos de cifragem de disco, bloqueio de ecrã, Wi-Fi seguro, utilização de VPN ou acesso de confiança zero, filtros de privacidade e proibição de utilizar dispositivos pessoais sem aprovação. Evidência através do relatório de conformidade do MDM para os dispositivos finais.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.6.8 **Comunicação de eventos de segurança da informação: Existe um mecanismo através do qual as pessoas podem comunicar atempadamente eventos de segurança observados ou suspeitos.**

Como se comprova: Um canal de comunicação claramente divulgado (caixa de correio, canal de conversação, número de telefone) com a garantia de ausência de sanções para comunicações de boa fé. Evidência: o volume de comunicações no registo de eventos; um registo permanentemente vazio é um sinal de alerta na auditoria.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7 Anexo A: Controlos físicos 14

A.7.1 **Perímetros de segurança física: São definidos e utilizados perímetros de segurança para proteger áreas que contêm informação e instalações de processamento de informação.**

Como se comprova: Uma descrição dos perímetros com um esquema ou fotografias: edifício, escritório, bastidor de servidores. Num escritório em casa, o perímetro é a divisão de trabalho fechada à chave ou, na sua falta, um armário fechado à chave; descreva-o em vez de o omitir.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.2 **Entrada física: As áreas seguras são protegidas por controlos de entrada e pontos de acesso adequados.**

Como se comprova: Um registo de chaves ou cartões com entrega e devolução, e uma regra de visitantes com acompanhamento e registo. Se for utilizado um espaço de coworking ou um centro de dados, tome os controlos de entrada do operador como evidência e assegure-os contratualmente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.3 **Segurança de escritórios, salas e instalações: É concebida e implementada a segurança física de escritórios, salas e instalações.**

Como se comprova: Portas com fechadura, proteção de janelas no rés-do-chão, nenhum ecrã confidencial visível a partir do exterior, sem sinalética da empresa em áreas sensíveis. Uma descrição breve mais uma fotografia são suficientes como evidência.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.4 **Monitorização da segurança física: As instalações são continuamente monitorizadas quanto a acessos físicos não autorizados.**

Como se comprova: Novidade na edição de 2022. As opções são um sistema de alarme, detetores de movimento, videovigilância ou registos de entrada. A videovigilância tem de ser verificada quanto à conformidade com a proteção de dados; num escritório em casa, a alternativa justificada é uma combinação de um sistema de alarme, uma divisão fechada à chave e a constatação de que ali não são mantidos servidores sensíveis.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.5 **Proteção contra ameaças físicas e ambientais: Está implementada proteção contra ameaças físicas e ambientais, como catástrofes naturais e danos intencionais ou não intencionais.**

Como se comprova: Uma análise de incêndio, água, calor, falha de energia e arrombamento, juntamente com as medidas implementadas (detetores de fumo, extintores, nenhum equipamento sob tubagens de água, cópia de segurança armazenada noutro local). É aqui que se liga a determinação sobre alterações climáticas do ponto 4.1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.6 **Trabalho em áreas seguras: São concebidas e implementadas medidas para o trabalho em áreas seguras.**

Como se comprova: Regras para a sala de servidores ou áreas de elevada confidencialidade: sem acesso de terceiros sem supervisão, sem gravações com câmaras ou dispositivos móveis, registo do trabalho realizado. Se não existirem áreas seguras, isso pode ser justificado remetendo para uma operação exclusivamente em nuvem.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.7 **Secretária limpa e ecrã limpo: São definidas e cumpridas regras de secretária limpa quanto a papéis e suportes amovíveis, e de bloqueio de ecrãs.**

Como se comprova: Isto aplica-se integralmente também no escritório em casa e, por isso, não deve ser declarado não aplicável. Evidenciado por uma regra breve (guardar documentos fechados à chave, bloqueio de ecrã após cinco minutos, sem notas autocolantes com credenciais), mais o bloqueio tecnicamente imposto através da política de dispositivos, cuja configuração pode ser exportada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.8 **Localização e proteção de equipamento: O equipamento é localizado de forma segura e protegido.**

Como se comprova: Colocação afastada de vias de passagem e áreas públicas, sem visibilidade a partir do exterior, proteção contra calor e humidade, cadeados de cabo para dispositivos móveis. Uma descrição breve dentro da política de escritório em casa ou de escritório é suficiente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.9 **Segurança de ativos fora das instalações: Os ativos localizados fora das instalações são protegidos.**

Como se comprova: Em organizações pequenas, trata-se principalmente do portátil, do smartphone e de suportes externos, e isso não pode ser argumentado como inaplicável. Evidência: cifragem de disco imposta, limpeza remota ativada através do MDM, uma regra contra deixar dispositivos em veículos e contra a utilização de redes públicas sem VPN, mais um percurso de comunicação de perdas. O relatório de conformidade do MDM que mostra o estado de cifragem por dispositivo é a evidência isolada mais sólida.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.10 **Suportes de armazenamento: Os suportes de armazenamento são geridos ao longo de todo o seu ciclo de vida, em conformidade com o esquema de classificação e os requisitos de tratamento, desde a aquisição, passando pela utilização e transporte, até à eliminação.**

Como se comprova: Isto aplica-se mesmo ao trabalho puramente móvel, porque existem pens USB, discos externos e suportes de cópia de segurança. Evidência: um registo de suportes, suportes cifrados, uma proibição tecnicamente imposta de suportes amovíveis não aprovados, armazenamento seguro num local fechado à chave, e transição para o ponto A.7.14 no fim da vida útil.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.11 **Serviços de apoio: As instalações de processamento de informação são protegidas contra falhas dos serviços de apoio, em particular o fornecimento de energia.**

Como se comprova: Quando os servidores são operados internamente, uma fonte de alimentação ininterrupta com um teste documentado. Numa configuração exclusivamente em nuvem, a evidência é a referência aos compromissos do fornecedor, mais uma regra sobre como continuar a trabalhar durante uma falha local de energia ou de internet (partilha de ligação móvel, local alternativo).

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.12 **Segurança da cablagem: A cablagem de energia, dados e comunicações é protegida contra interceção, interferência e danos.**

Como se comprova: Quando a cablagem é própria, proteção contra danos e contra acesso não autorizado a painéis de distribuição. Em pequenos escritórios e escritórios em casa, a justificação é sucinta, mas tem de ser dada: o router e as tomadas de rede não são acessíveis ao público, as portas não utilizadas estão desativadas.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.13 **Manutenção de equipamento: O equipamento é mantido corretamente para assegurar a disponibilidade, integridade e confidencialidade da informação.**

Como se comprova: Um plano de manutenção ou estado de suporte do fabricante por dispositivo, e uma regra para reparações realizadas por terceiros (remover primeiro o suporte de armazenamento ou limpar os dados, e estabelecer um acordo de confidencialidade com o prestador). Acompanhe as datas de fim de suporte no inventário de ativos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.7.14 **Eliminação ou reutilização segura de equipamento: Antes de um dispositivo com capacidade de armazenamento ser transmitido, vendido ou abatido, é verificado e registado que nele já não é possível reconstruir dados protegidos nem software licenciado.**

Como se comprova: Isto também se aplica no escritório em casa e a dispositivos pessoais retirados de serviço que foram utilizados para trabalho. Evidência: um registo de limpeza por dispositivo com número de série, data e método (apagamento criptográfico em SSD cifrados, sobrescrita, destruição física), ou um certificado de destruição de um prestador. Para dispositivos cifrados, a destruição documentada da chave é suficiente, desde que o procedimento esteja descrito.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8 Anexo A: Controlos tecnológicos 34

A.8.1 **Dispositivos finais de utilizador: É protegida a informação armazenada, processada ou acessível através de dispositivos finais de utilizador.**

Como se comprova: Uma base de reforço por sistema operativo, gestão centralizada através de MDM, cifragem de disco, atualizações automáticas e bloqueio de ecrã. O relatório de conformidade do MDM, com um estado por dispositivo, evidencia tudo isto de uma só vez.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.2 **Direitos de acesso privilegiado: A atribuição e a utilização de direitos de acesso privilegiado são restringidas e geridas.**

Como se comprova: Uma lista de todas as contas de administrador com justificação, contas de administração separadas não utilizadas para o trabalho diário, MFA imposta, elevação limitada no tempo sempre que possível, e revisão periódica. Em organizações pequenas, este é o controlo compensatório mais importante para o ponto A.5.3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.3 **Restrição de acesso à informação: O acesso à informação e a outros ativos associados é restringido de acordo com a política de controlo de acesso estabelecida.**

Como se comprova: Um conceito de autorização baseado em funções e grupos, em vez de concessões individuais, evidenciado por uma exportação das associações a grupos. Reveja regularmente as ligações de partilha pública no armazenamento em nuvem e deixe-as caducar.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.4 **Acesso ao código-fonte: O acesso de leitura e escrita ao código-fonte, às ferramentas de desenvolvimento e às bibliotecas de software é adequadamente gerido.**

Como se comprova: Permissões de repositório por função, ramos principais protegidos, revisões impostas ou verificações de estado impostas, sem envio direto para o ramo principal. Evidência através da configuração de proteção de ramos e da lista de membros da organização.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.5 **Autenticação segura: São implementadas tecnologias e procedimentos de autenticação segura, com base nas restrições de acesso e na política específica do tema.**

Como se comprova: MFA para todos os acessos externos e todas as contas de administrador, métodos resistentes a phishing (chaves de acesso, FIDO2) sempre que possível, e bloqueio após tentativas falhadas. Evidência através do relatório de cobertura de MFA do fornecedor de identidade.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.6 **Gestão de capacidade: São monitorizados o armazenamento, a capacidade de processamento, a largura de banda e as licenças, e a procura é ajustada com antecedência suficiente para que os estrangulamentos nunca ameacem a disponibilidade.**

Como se comprova: Monitorização do armazenamento, da carga de processamento, das quotas de licenças e dos orçamentos de nuvem, com alertas de limiar. Em organizações pequenas, basta um alerta de utilização de disco e de limites de custo, mais uma revisão anual de capacidade.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.7 **Proteção contra software malicioso: As defesas técnicas contra software malicioso estão ativas e atualizadas, e as pessoas que utilizam os dispositivos estão suficientemente formadas para não comprometerem essas defesas.**

Como se comprova: Proteção ativa de dispositivos finais com uma vista de estado centralizada, um filtro de correio que inspeciona anexos e ligações, e uma regra contra a execução de software não aprovado. O relatório de estado datado da solução de proteção é a evidência direta.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.8 **Gestão de vulnerabilidades técnicas: A organização informa-se ativamente sobre vulnerabilidades na tecnologia que utiliza, decide para cada achado qual é o grau de exposição, e fecha a lacuna dentro de prazos definidos ou justifica uma resposta diferente.**

Como se comprova: Gestão de vulnerabilidades com uma fonte (detetor, verificação de dependências na integração contínua, alertas de fornecedores), uma classificação de gravidade e prazos definidos por nível, por exemplo crítico dentro de 7 dias. Evidência: relatórios de verificação de vários momentos que mostram a diminuição dos achados em aberto.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.9 **Gestão de configuração: São estabelecidas, documentadas, implementadas, monitorizadas e revistas as configurações de equipamento, software, serviços e redes, incluindo as configurações de segurança.**

Como se comprova: Novidade na edição de 2022. Evidência através de configurações de base documentadas (bases de reforço) e da sua imposição, idealmente como infraestrutura como código em controlo de versões ou através de perfis de MDM. A deteção de desvios e uma comparação periódica de configuração completam o quadro.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.10 **Eliminação de informação: A informação armazenada em sistemas de informação, em dispositivos e em suportes de armazenamento é eliminada quando deixa de ser necessária.**

Como se comprova: Novidade na edição de 2022, estreitamente ligada ao RGPD. Evidência através de um conceito de eliminação com prazos de retenção por categoria de dados, políticas de retenção tecnicamente implementadas em serviços de nuvem e bases de dados, e registos de eliminação. As cópias de segurança e os arquivos de registos também precisam de um prazo de retenção.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.11 **Mascaramento de dados: É aplicado mascaramento de dados de acordo com a política específica sobre controlo de acesso e com os requisitos de negócio e legais.**

Como se comprova: Novidade na edição de 2022. Na prática: sem dados de produção em ambientes de teste e desenvolvimento, mas antes dados anonimizados ou sintéticos; pseudonimização em análises; mascaramento de números de conta e credenciais em registos e interfaces de suporte. Evidência através do script ou procedimento que gera os dados de teste.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.12 **Prevenção de fuga de dados: São aplicadas medidas de prevenção de fuga de dados a sistemas, redes e dispositivos que processam, armazenam ou transmitem informação sensível.**

Como se comprova: Novidade na edição de 2022. Realista em organizações pequenas: controlo das ligações de partilha no armazenamento em nuvem, bloqueio de suportes amovíveis não aprovados, regras contra o reencaminhamento para caixas de correio pessoais, verificações sobre a introdução de dados confidenciais em serviços de IA externos, e deteção de segredos no código-fonte. Evidência através da configuração e da revisão das ocorrências.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.13 **Cópia de segurança da informação: Existem cópias de segurança de dados, software e sistemas de acordo com uma regra definida (âmbito, frequência, retenção, localização), e o respetivo restauro é efetivamente testado em intervalos regulares.**

Como se comprova: Uma política de cópias de segurança com frequência, retenção e uma cópia externa seguindo o princípio 3-2-1, cifragem das cópias de segurança, e proteção contra sobrescrita por ransomware (cópias de segurança imutáveis). O que é decisivo é o teste de restauro documentado, com data e resultado, porque uma cópia de segurança não testada conta como inexistente na auditoria.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.14 **Redundância das instalações de processamento de informação: As instalações de processamento de informação são implementadas com redundância suficiente para cumprir os requisitos de disponibilidade.**

Como se comprova: A redundância tem de corresponder aos objetivos de disponibilidade, não ao máximo possível. Evidência através de uma descrição de arquitetura com instâncias ou zonas redundantes, equipamento de reserva, e uma decisão justificada sobre onde a redundância está deliberadamente ausente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.15 **Registo de eventos: As atividades relevantes para a segurança deixam um vestígio. Os registos são produzidos, retidos, protegidos contra alteração e efetivamente analisados, não apenas recolhidos.**

Como se comprova: No mínimo, registe inícios de sessão e tentativas falhadas, alterações de permissões, ações administrativas e acessos a dados confidenciais. Os registos são protegidos contra alteração e têm um prazo de retenção definido; em organizações pequenas, os registos imutáveis são, ao mesmo tempo, a compensação para a segregação de funções em falta prevista no ponto A.5.3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.16 **Atividades de monitorização: As redes, sistemas e aplicações são monitorizados quanto a comportamentos anómalos, e são tomadas ações adequadas para avaliar potenciais incidentes de segurança.**

Como se comprova: Novidade na edição de 2022. Exequível sem uma equipa de segurança própria: alertas do fornecedor de identidade sobre deslocações impossíveis e séries de tentativas falhadas, alertas da plataforma de nuvem sobre despesas invulgares ou alterações de permissões, reencaminhados para uma caixa de correio monitorizada com um tempo de resposta definido. Evidência através das regras de alerta, mais exemplos de alertas tratados.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.17 **Sincronização de relógios: Todos os sistemas que registam eventos obtêm a sua hora a partir de uma fonte definida e fiável, de modo a que os eventos possam ser colocados na ordem correta entre sistemas.**

Como se comprova: Configuração de NTP em servidores e dispositivos finais, e um fuso horário uniforme nos registos (idealmente UTC). Sem hora sincronizada, a reconstrução de um incidente ao abrigo do ponto A.5.28 não se sustenta; um extrato de configuração é suficiente como evidência.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.18 **Utilização de programas utilitários privilegiados: A utilização de programas utilitários capazes de se sobrepor às proteções do sistema é restringida e rigorosamente controlada.**

Como se comprova: Uma lista de ferramentas de administração aprovadas, restrição dos direitos de administrador local, controlo de aplicações (lista de permissões) sempre que possível, e registo da utilização. Evidência: a política mais a configuração da gestão de direitos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.19 **Instalação de software em sistemas operacionais: São implementados procedimentos e medidas para gerir de forma segura a instalação de software em sistemas operacionais.**

Como se comprova: Apenas software aprovado proveniente de fontes fiáveis, instalação através de distribuição centralizada ou de um gestor de pacotes, um caminho de reversão e retenção da versão anterior. Evidência através da lista de aprovação e dos registos de implantação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.20 **Segurança das redes: As redes e os dispositivos de rede ativos têm um responsável nomeado, uma configuração reforçada e um conjunto de regras rastreável que define que tráfego é sequer permitido.**

Como se comprova: Um conjunto de regras de firewall que segue o princípio de negação por defeito, portas abertas documentadas com justificação, uma configuração de Wi-Fi segura, e credenciais predefinidas alteradas nos dispositivos de rede. Evidência através de uma exportação do conjunto de regras e de uma verificação externa de portas.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.21 **Segurança dos serviços de rede: São identificados, implementados e monitorizados os mecanismos de segurança, os níveis de serviço e os requisitos de gestão dos serviços de rede.**

Como se comprova: Para cada serviço de rede em utilização (VPN, DNS, correio, CDN), documente os compromissos de segurança e a configuração própria, incluindo a cifragem em trânsito e os compromissos de nível de serviço do fornecedor. Evidência: uma vista geral da configuração, mais o contrato ou a descrição do serviço.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.22 **Segregação de redes: A rede é dividida em zonas, de modo a que serviços, grupos de utilizadores e sistemas com diferentes necessidades de proteção não consigam alcançar-se mutuamente sem filtragem.**

Como se comprova: Segmentos de rede ou VLAN separados para convidados, administração e produção; na nuvem, contas ou redes virtuais separadas com grupos de segurança. Num escritório em casa, a implementação exequível é uma rede ou VLAN separada para dispositivos de trabalho, mantida à parte de dispositivos pessoais e tecnologia doméstica inteligente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.23 **Filtragem web: O acesso a sítios web externos é gerido para reduzir a exposição a conteúdo malicioso.**

Como se comprova: Novidade na edição de 2022. Alcançável com pouco esforço através de um serviço de DNS com filtragem ou da filtragem web incluída na proteção de dispositivos finais, com categorias bloqueadas e registo dos pedidos bloqueados. Evidência através da configuração do filtro e de um extrato de relatório.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.24 **Utilização de criptografia: É definido de forma vinculativa onde é aplicada a cifragem, com que algoritmos, e como as chaves são geradas, armazenadas, rodadas e destruídas ao longo de todo o seu ciclo de vida.** Documento

Como se comprova: Uma política de criptografia com algoritmos aprovados e comprimentos mínimos de chave, cifragem em trânsito (TLS) e em repouso, mais um procedimento de gestão de chaves que abrange geração, armazenamento, rotação e destruição. Evidência através da política, mais a configuração do serviço ou cofre de chaves.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.8.25 **Ciclo de vida de desenvolvimento seguro: São estabelecidas e aplicadas regras para o desenvolvimento seguro de software e sistemas.**

Como se comprova: Uma descrição do processo de desenvolvimento com pontos de contacto de segurança por fase: requisitos, conceção, implementação, testes, lançamento, operação. Para equipas pequenas, basta uma página que remeta para as portas de controlo concretas na integração contínua e para a obrigação de revisão.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.8.26 **Requisitos de segurança de aplicações: Os requisitos de segurança para aplicações são identificados, especificados e aprovados durante o desenvolvimento e a aquisição.**

Como se comprova: Requisitos de segurança como pontos explícitos na lista de requisitos ou como uma lista de verificação reutilizável, orientada por exemplo por normas comuns de verificação de segurança de aplicações. Evidência através de registos ou documentos de requisitos com uma dimensão de segurança.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.8.27 **Princípios de arquitetura e engenharia de sistemas seguros: São estabelecidos, documentados e aplicados às atividades de desenvolvimento princípios de engenharia de sistemas seguros.**

Como se comprova: Princípios documentados como o privilégio mínimo, a defesa em profundidade, predefinições seguras, minimização de dados e uma abordagem de confiança zero, juntamente com a sua aplicação visível em esquemas de arquitetura ou registos de decisão.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.8.28 **Codificação segura: São aplicados princípios de codificação segura no desenvolvimento de software.**

Como se comprova: Novidade na edição de 2022. Evidência através de regras de codificação vinculativas, análise estática de código e deteção de segredos como portas de controlo obrigatórias na integração contínua, utilização de bibliotecas verificadas, e revisões de código documentadas. Onde a segregação de funções é impossível, portas de controlo automatizadas impostas substituem a revisão a quatro olhos; justifique isto e evidencie-o com a configuração do pipeline.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.8.29 **Testes de segurança em desenvolvimento e aceitação: São definidos e implementados processos de testes de segurança dentro do ciclo de vida de desenvolvimento.**

Como se comprova: Testes de segurança automatizados no pipeline (verificações de dependências, análise estática e dinâmica), mais um teste de intrusão periódico quando as necessidades de proteção são elevadas. Evidência através de relatórios de teste datados e do acompanhamento dos achados.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

A.8.30 **Desenvolvimento subcontratado: As atividades de desenvolvimento subcontratadas são dirigidas, monitorizadas e revistas.**

Como se comprova: Quando o desenvolvimento é subcontratado, estabeleça os requisitos de segurança no contrato, assegure a titularidade do código e o direito de revisão, e realize revisões de código e testes de segurança antes da aceitação. Sem desenvolvimento subcontratado, a não aplicabilidade tem de ser justificada de forma coerente na DdA.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.31 **Separação de ambientes de desenvolvimento, teste e produção: Os ambientes de desenvolvimento, teste e produção são separados e protegidos.**

Como se comprova: Contas, projetos ou espaços de nomes separados, credenciais separadas e conjuntos de dados separados. Em combinação com o ponto A.8.11, assegure que nenhum dado de produção acaba em ambientes que não sejam de produção. Evidência através da vista geral dos ambientes e da atribuição de direitos.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.32 **Gestão de mudanças: As alterações às instalações de processamento de informação e aos sistemas de informação estão sujeitas a procedimentos de gestão de mudanças.**

Como se comprova: Um processo de gestão de mudanças com pedido, avaliação de impacto, testes, aprovação, implementação e um caminho de reversão. Em equipas de desenvolvimento, um pipeline de pull request com verificações impostas e implantações registadas satisfaz este ponto, desde que o histórico seja imutável.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.33 **Informação de teste: A informação de teste é adequadamente selecionada, protegida e gerida.**

Como se comprova: O princípio: sem dados pessoais reais em sistemas de teste. Quando isso é inevitável, documente a aprovação, o mascaramento, a restrição de acesso e a eliminação após o teste. Evidência através do conceito de dados de teste e dos registos de eliminação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

A.8.34 **Proteção dos sistemas de informação durante testes de auditoria: Os testes de auditoria que envolvem acesso a sistemas operacionais são planeados e acordados com a gestão, para evitar perturbações na operação.**

Como se comprova: Um acordo de auditoria com uma janela temporal, um âmbito, acesso apenas de leitura sempre que possível, registo do acesso de auditoria e aprovação pela gestão. Isto também se aplica aos testes de intrusão: uma autorização de teste por escrito, com uma janela temporal e um contacto de emergência, é a evidência.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação