Lista de Controlo ISO 27701

Estender o ISMS para a Privacidade

Checklist prática para autoavaliação de um PIMS alinhado com a governação de privacidade, integração com o ISMS e evidências operacionais.

Documento de trabalho para diagnóstico inicial, gap assessment e preparação de roadmap.

O que inclui

- 12 áreas críticas de controlo
- 48 perguntas práticas para diagnóstico
- Campos para estado e evidências
- Útil para CISO, DPO, IT e compliance

Como usar

- Percorra tema a tema
- Marque Sim / Parcial / Não / N/A
- Registe evidências reais
- Priorize lacunas e owners

Legenda de avaliação

Sim	Parcial	Não	N/A
Implementado e evidenciado	Existe, mas é incompleto	Não implementado	Não aplicável ao âmbito

1. Contexto, Âmbito e Partes Interessadas

#	Pergunta de controlo	Estado	Evidência / notas
1	O âmbito do PIMS está definido e alinhado com o âmbito do ISMS, incluindo serviços, processos, sistemas, localizações e categorias de dados pessoais relevantes?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	As partes interessadas internas e externas, bem como os seus requisitos de privacidade, estão identificados e revistos periodicamente?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	A organização documentou os tipos de titulares de dados, finalidades de tratamento e fluxos principais de dados pessoais incluídos no PIMS?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

#	Pergunta de controlo	Estado	Evidência / notas
4	As interfaces entre segurança da informação, privacidade, jurídico, IT, RH, marketing e procurement estão formalmente clarificadas?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

2. Liderança, Governação e Responsabilidades

#	Pergunta de controlo	Estado	Evidência / notas
1	A gestão de topo aprovou objetivos de privacidade, responsabilidades, recursos e critérios de reporte para o PIMS?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	Os papéis de controller, joint controller, processor e subprocessor estão corretamente identificados e documentados quando aplicável?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	Existe uma matriz RACI ou equivalente para privacidade, incluindo CISO, DPO, IT, owners de processo e procurement?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	As decisões relevantes de privacidade são escaladas, aprovadas e registadas de forma consistente?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

3. Inventário de Tratamentos e Mapeamento de Dados

#	Pergunta de controlo	Estado	Evidência / notas
1	A organização mantém um registo atualizado das atividades de tratamento, sistemas, categorias de dados, destinatários, retenção e bases aplicáveis?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	É possível localizar rapidamente onde os dados pessoais são recolhidos, armazenados, usados, partilhados e eliminados?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	Os fluxos de dados com terceiros, filiais, cloud providers e ferramentas SaaS estão identificados e documentados?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	As alterações significativas em sistemas ou processos desencadeiam revisão do inventário e da documentação	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____

#	Pergunta de controlo	Estado	Evidência / notas
	associada?		_____

4. Licitude, Transparência e Limitação da Finalidade

#	Pergunta de controlo	Estado	Evidência / notas
1	Cada atividade de tratamento tem finalidade definida, lógica operacional clara e fundamento devidamente documentado?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	As notices, políticas de privacidade e textos de transparência refletem o que realmente acontece nos processos e sistemas?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	A recolha de dados segue critérios de minimização e evita campos, atributos ou retenções desnecessárias?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	As alterações de finalidade, novas campanhas, novas integrações ou reutilizações de dados são revistas antes da entrada em produção?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

5. Avaliação de Risco e Privacy by Design

#	Pergunta de controlo	Estado	Evidência / notas
1	Os riscos de privacidade relacionados com pessoas singulares são avaliados com critérios claros, consistentes e proporcionais?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	Novos projetos, aplicações, integrações ou mudanças relevantes incluem privacy by design e privacy by default desde o início?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	Os requisitos de privacidade são incluídos em projetos, change management, desenvolvimento e aquisição de sistemas?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	As decisões de aceitação, mitigação ou tratamento de risco de privacidade são aprovadas e registadas com evidências?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

6. Controlos Operacionais e Segurança de Dados Pessoais

#	Pergunta de controlo	Estado	Evidência / notas

#	Pergunta de controlo	Estado	Evidência / notas
1	Os controlos de acesso a dados pessoais seguem necessidade de conhecimento, segregação de funções e revisão periódica?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	A organização protege dados pessoais em repouso, em trânsito, em cópias de segurança e em ambientes de teste ou suporte?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	Logs, monitorização e gestão de incidentes permitem detetar utilização indevida, acessos indevidos ou falhas de controlo relevantes?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	Os ambientes, contas privilegiadas e exportações de dados têm controlos adequados para reduzir risco de exposição indevida?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

7. Gestão de Terceiros e Processors

#	Pergunta de controlo	Estado	Evidência / notas
1	Existe due diligence para fornecedores que tratam dados pessoais, incluindo medidas técnicas, organizativas e histórico de conformidade?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	Os contratos com processors incluem instruções documentadas, confidencialidade, subcontratação, incidentes e apoio a direitos dos titulares?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	A organização revê regularmente sub-processors, serviços cloud, integrações externas e alterações relevantes de risco?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	Existe evidência de acompanhamento de fornecedores críticos, incluindo avaliações, reuniões, planos de ação ou follow-up?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

8. Retenção, Eliminação e Qualidade dos Dados

#	Pergunta de controlo	Estado	Evidência / notas
1	Os períodos de retenção estão definidos por categoria de dados, finalidade, obrigação legal e necessidade operacional?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	Existem mecanismos práticos para eliminação, anonimização ou bloqueio quando os dados deixam de ser necessários?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	A organização testa ou verifica se os calendários de retenção são realmente executados nos sistemas?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	Há critérios para correção, atualização e qualidade dos dados pessoais relevantes para o negócio e para os titulares?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

9. Direitos dos Titulares de Dados

#	Pergunta de controlo	Estado	Evidência / notas

#	Pergunta de controlo	Estado	Evidência / notas
1	Existe processo documentado para receção, avaliação, resposta e fecho de pedidos de acesso, retificação, apagamento e outros direitos aplicáveis?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	A organização consegue localizar dados pessoais por sistema, processo e terceiro dentro de prazos razoáveis?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	As equipas sabem quando um pedido pode ser satisfeito, limitado, recusado ou escalado para avaliação adicional?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	Os pedidos e respostas são registados com evidência suficiente para demonstrar consistência e cumprimento?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

10. Gestão de Incidentes e Violação de Dados

#	Pergunta de controlo	Estado	Evidência / notas
1	O processo de incident response distingue claramente incidentes de segurança e potenciais violações de dados pessoais?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	Existe avaliação estruturada do impacto sobre titulares, critérios de severidade e decisão documentada sobre notificação?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	As equipas de segurança, privacidade, jurídico e comunicação sabem quando e como colaborar num incidente relevante?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	São mantidos registos de incidentes, causas, ações corretivas, lições aprendidas e follow-up?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

11. Competência, Formação e Consciencialização

#	Pergunta de controlo	Estado	Evidência / notas
1	Os colaboradores recebem formação adequada ao seu papel em matéria de privacidade, segurança e tratamento de dados pessoais?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	As equipas com maior exposição — RH, IT, marketing, suporte, vendas e procurement — recebem formação reforçada ou específica?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	Existe evidência de participação, eficácia, reciclagem periódica e atualização do conteúdo formativo?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	Os temas de privacidade são incluídos em onboarding, mudança de funções e campanhas de sensibilização contínuas?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

12. Monitorização, Auditoria e Melhoria Contínua

#	Pergunta de controlo	Estado	Evidência / notas

#	Pergunta de controlo	Estado	Evidência / notas
1	A organização definiu indicadores de desempenho para o PIMS, como direitos dos titulares, retenção, incidentes, terceiros e ações corretivas?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
2	O programa inclui auditorias internas, revisões pela gestão e acompanhamento formal de não conformidades e melhorias?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
3	As evidências do PIMS estão organizadas e acessíveis para clientes, auditorias internas, avaliações de fornecedores e due diligence?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____
4	Existe um plano realista de melhoria contínua para reforçar integração entre ISO 27701, ISO 27001 e requisitos legais aplicáveis?	☐ Sim ☐ Parcial ☐ Não ☐ N/A	_____ ____ _____ ____

Pacote mínimo de evidências sugerido

Use esta página para validar se o PIMS consegue demonstrar controlo de forma prática e auditável.

Evidência	Existe?
Âmbito do PIMS e interfaces com o ISMS	☐ Sim ☐ Parcial ☐ Não
Políticas de privacidade, retenção, gestão de terceiros e incidentes	☐ Sim ☐ Parcial ☐ Não
Registo de atividades de tratamento e mapeamento de dados	☐ Sim ☐ Parcial ☐ Não
Matriz de papéis: controller / processor / owners / DPO / CISO	☐ Sim ☐ Parcial ☐ Não
Critérios e registos de privacy by design e gestão de risco	☐ Sim ☐ Parcial ☐ Não
Contratos e avaliações de processors e sub-processors	☐ Sim ☐ Parcial ☐ Não
Registos de pedidos de titulares, incidentes e ações corretivas	☐ Sim ☐ Parcial ☐ Não
Indicadores, auditorias internas e revisão pela gestão	☐ Sim ☐ Parcial ☐ Não

Próximo passo recomendado: atribuir um owner por tema, recolher evidências, priorizar lacunas e definir um plano de implementação faseado.

Precisa de apoio para transformar esta checklist num programa real? Fale com a iCompliance.eu.