Checklist de preparação para a ISO/IEC 27001:2022

Marque cada ponto que a sua organização já cumpre. Os pontos por marcar mostram onde começar. Use-a como guia de autoavaliação antes de iniciar o projecto.

1. Contexto e âmbito (cláusula 4)

- ☐ Identificámos as questões internas e externas que afectam a segurança da informação.
- ☐ Identificámos as partes interessadas e os seus requisitos (clientes, reguladores, Lei n.º 22/11).
- ☐ Definimos e documentámos o âmbito do SGSI: unidades, processos, localizações e activos.

2. Liderança (cláusula 5)

- ☐ A gestão de topo aprovou o lançamento do SGSI e atribuiu os recursos necessários.
- ☐ Existe uma política de segurança da informação aprovada e comunicada.
- ☐ Os papéis e responsabilidades estão definidos, incluindo um responsável pelo SGSI.

3. Planeamento e gestão de riscos (cláusula 6)

- ☐ Definimos a metodologia de avaliação de riscos e os critérios de aceitação.
- ☐ Existe um inventário de activos de informação, cada um com responsável.
- ☐ A avaliação de riscos foi realizada e está registada.
- ☐ O plano de tratamento de riscos foi aprovado pelos responsáveis dos riscos.
- ☐ Elaborámos a declaração de aplicabilidade, com os controlos do Anexo A (93 controlos) e a justificação de cada inclusão e exclusão.
- ☐ Definimos objectivos de segurança da informação mensuráveis.

4. Suporte (cláusula 7)

- ☐ Definimos as competências necessárias e fizemos a formação correspondente.
- ☐ Existe um programa de sensibilização para todos os colaboradores.
- ☐ A informação documentada está controlada: versões, aprovação e acessos.

5. Operação (cláusula 8)

- ☐ O plano de tratamento de riscos está em execução.
- ☐ Os controlos aplicáveis estão implementados e têm evidências (acessos, cópias de segurança, fornecedores, continuidade).
- ☐ O processo de gestão de incidentes está definido e foi testado.

6. Avaliação do desempenho (cláusula 9)

- ☐ Definimos indicadores e monitorizamo-los periodicamente.
- ☐ Realizámos uma auditoria interna, por alguém independente da área auditada.
- ☐ Realizámos e registámos a revisão pela gestão.

7. Melhoria (cláusula 10)

- ☐ As não conformidades estão registadas, com causa, acção correctiva, responsável e prazo.
- ☐ Há evidência de melhoria contínua do SGSI.

8. Antes da auditoria de certificação

- ☐ Escolhemos um organismo de certificação acreditado.
- ☐ As evidências estão organizadas e a equipa está preparada para as entrevistas do auditor.

Esta checklist é um guia de preparação e não substitui a norma ISO/IEC 27001:2022 nem a avaliação feita por um organismo de certificação acreditado. A SyneraNexo prepara organizações para a certificação; a certificação é atribuída pelo organismo acreditado. Precisa de ajuda a interpretar o resultado? Escreva para geral@syneranexo.com.