ISO REPORTS GLOBAL

Checklist ISO 27001:2022

Sistema de Gestão de Segurança da Informação — Verificação Completa

Este checklist cobre as cláusulas 4-10 da ISO 27001:2022 e os controles do Anexo A (93 controles em 4 temas). Para cada item: (I) Implementado | (NI) Não Implementado | (P) Parcial | (NA) Não Aplicável — justificar na SoA.

4–6. Contexto, Liderança e Planejamento do SGSI

Fundação do sistema: compreender o ambiente, comprometer a liderança e planejar a gestão de riscos.

- [ ] 4.1/4.2 — O contexto interno/externo e as partes interessadas relevantes para segurança da informação foram determinados?
- [ ] 4.3 — O escopo do SGSI está definido e documentado com interfaces e dependências entre atividades e serviços?
- [ ] 5.1 — A alta direção demonstra liderança: aprova política, assegura recursos e lidera revisões do SGSI?
- [ ] 5.2 — A política de segurança da informação está documentada, comunicada internamente e disponível a partes interessadas?
- [ ] 6.1.2 — Um processo de avaliação de riscos de SI está definido, com critérios de aceitação e critérios para realizar avaliações?
- [ ] 6.1.2 — Os riscos de SI foram identificados e avaliados quanto à probabilidade e impacto, com responsáveis designados?
- [ ] 6.1.3 — Os tratamentos de risco foram selecionados (mitigar, aceitar, transferir, evitar) e um Plano de Tratamento de Riscos elaborado?
- [ ] 6.1.3 — A Declaração de Aplicabilidade (SoA) foi elaborada listando todos os controles do Anexo A com justificativas?
- [ ] 6.2 — Os objetivos de segurança da informação são mensuráveis, monitorados e consistentes com a política de SI?

Anexo A — Tema 5: Controles Organizacionais (37 controles)

Controles relacionados a políticas, papéis, processos organizacionais e gestão de ativos de informação.

- [ ] A.5.1 — Políticas de segurança da informação: documentadas, aprovadas pela direção, comunicadas e revisadas periodicamente?
- [ ] A.5.2 — Papéis e responsabilidades de segurança da informação definidos e atribuídos?
- [ ] A.5.9 — Inventário de ativos de informação e outros ativos associados criado e mantido?
- [ ] A.5.10 — Uso aceitável de ativos de informação: política documentada e comunicada?
- [ ] A.5.12 — Classificação da informação: esquema de classificação definido e aplicado?
- [ ] A.5.14 — Requisitos de SI incluídos em acordos com fornecedores e prestadores de serviços?
- [ ] A.5.15 — Controle de acesso baseado em necessidade de negócio (princípio do menor privilégio)?
- [ ] A.5.23 — Segurança no uso de serviços de nuvem: política e controles para aquisição e uso de cloud?
- [ ] A.5.24/25/26 — Gestão de incidentes: classificação, relatórios, resposta e aprendizado documentados?
- [ ] A.5.29 — Plano de continuidade de negócios considera requisitos de segurança da informação?
- [ ] A.5.36 — Conformidade com políticas de SI: procedimentos de revisão e verificação implementados?

Anexo A — Temas 6, 7 e 8: Pessoas, Físico e Tecnológico

Controles de pessoas (8), segurança física (14) e controles tecnológicos (34).

- [ ] A.6.1 — Triagem/verificação de antecedentes de funcionários e contratados conforme leis aplicáveis?
- [ ] A.6.2 — Termos e condições de emprego incluem responsabilidades de SI (acordo de confidencialidade)?
- [ ] A.6.3 — Treinamento em conscientização de segurança da informação realizado regularmente?
- [ ] A.6.5 — Processo para retorno de ativos e revogação de acessos no desligamento está implementado?
- [ ] A.7.1 — Perímetros de segurança física definidos para proteger áreas com informações e ativos críticos?
- [ ] A.7.2 — Controles de acesso físico em vigor (cartões, biometria, câmeras, registros de acesso)?
- [ ] A.7.6 — Política de mesa limpa e tela limpa implementada e verificada?
- [ ] A.8.1 — Dispositivos de usuário final (notebooks, smartphones) protegidos com política de endpoint?
- [ ] A.8.2 — Direitos de acesso privilegiado limitados, monitorados e revisados periodicamente?
- [ ] A.8.5 — Autenticação segura: MFA implementada para sistemas críticos e acesso remoto?
- [ ] A.8.7 — Proteção contra malware: antivírus/EDR atualizado e centralizado em todos os endpoints?
- [ ] A.8.8 — Gestão de vulnerabilidades técnicas: processo de identificação, avaliação e remediação?
- [ ] A.8.12 — Prevenção de vazamento de dados (DLP): controles para dados sensíveis em trânsito/em uso?
- [ ] A.8.15 — Logs de eventos gerados, protegidos e revisados para sistemas críticos?
- [ ] A.8.24 — Criptografia usada para proteger dados sensíveis em repouso e em trânsito?

7–10. Apoio, Operação, Avaliação e Melhoria

Verificar a operação do SGSI, medição de desempenho, auditorias e melhoria contínua.

- [ ] 7.2 — Competências em SI das pessoas responsáveis são determinadas, asseguradas e documentadas?
- [ ] 7.4 — Comunicações internas e externas relevantes para o SGSI estão determinadas?
- [ ] 7.5 — Informação documentada exigida pelo SGSI está criada, mantida e controlada?
- [ ] 8.1 — Os processos do SGSI são operados e controlados conforme planejado?
- [ ] 8.2 — Avaliações de riscos de SI são realizadas em intervalos planejados ou quando ocorrem mudanças significativas?
- [ ] 8.3 — O Plano de Tratamento de Riscos está implementado e as evidências são mantidas?
- [ ] 9.1 — O desempenho e a eficácia do SGSI são monitorados e medidos com indicadores definidos?
- [ ] 9.2 — Auditorias internas do SGSI são realizadas conforme programa planejado?
- [ ] 9.3 — A alta direção analisa criticamente o SGSI incluindo desempenho, riscos, NC e oportunidades de melhoria?
- [ ] 10.1 — Não conformidades de SI são tratadas, causas raiz investigadas e ações corretivas documentadas?
- [ ] 10.2 — A organização promove melhoria contínua do SGSI com base em medições, auditorias e análises críticas?