Checklist de Cibersegurança para Empresas

Use este guia para verificar se sua empresa está protegida contra as principais ameaças cibernéticas. Inclui verificação de conformidade LGPD, avaliação de vulnerabilidades críticas e base para plano de ação.

50+ itens de verificação | LGPD Conformidade | ISO 27001 Boas práticas | Pentest Vulnerabilidades

O que você encontra

- ✓ 50+ itens práticos de verificação de segurança
- ✓ Checklist de conformidade LGPD
- ✓ Avaliação de vulnerabilidades críticas
- ✓ Base para plano de ação personalizado
- ✓ Referências ISO 27001 e NIST

1. Governança e LGPD

Controles de privacidade e conformidade com a Lei Geral de Proteção de Dados.

Documentação e processos

- ☐ Política de privacidade publicada e atualizada
- ☐ Registro de atividades de tratamento de dados pessoais (RATDP)
- ☐ Base legal mapeada para cada finalidade de tratamento
- ☐ Consentimento obtido quando necessário (ou base legal adequada)
- ☐ Procedimento de resposta a incidentes de segurança documentado
- ☐ Procedimento de atendimento a titulares (acesso, correção, exclusão)
- ☐ DPO indicado e contato divulgado (quando obrigatório)
- ☐ Contratos com operadores e suboperadores com cláusulas LGPD
- ☐ Avaliação de impacto à proteção de dados (RIPD) para tratamentos de alto risco
- ☐ Treinamento de conscientização em privacidade para colaboradores

Segurança da informação (ISO 27001 / NIST)

- ☐ Política de segurança da informação definida e comunicada
- ☐ Inventário de ativos de informação
- ☐ Análise de riscos realizada e documentada
- ☐ Controles de acesso (IAM) com princípio do menor privilégio
- ☐ Política de senhas forte (comprimento, complexidade, rotação)
- ☐ Autenticação multifator (MFA) em sistemas críticos
- ☐ Backup regular testado e plano de recuperação documentado
- ☐ Criptografia de dados em repouso e em trânsito
- ☐ Gestão de patches e atualizações de segurança
- ☐ Monitoramento e logs de segurança

2. Infraestrutura e aplicações

Proteção de sistemas, redes e aplicações web.

Infraestrutura

- ☐ Firewall configurado e regras revisadas periodicamente
- ☐ Segmentação de rede (isolamento de áreas sensíveis)
- ☐ VPN para acesso remoto seguro
- ☐ Proteção antivírus/EDR em endpoints e servidores
- ☐ Controle de dispositivos móveis e BYOD
- ☐ Proteção de e-mail (antispam, antiphishing)
- ☐ Gestão segura de credenciais e segredos
- ☐ Desativação imediata de acessos ao desligar colaborador

Aplicações e desenvolvimento

- ☐ Aplicações web com HTTPS obrigatório
- ☐ Validação de entrada e proteção contra injecao (OWASP)
- ☐ Gestão de dependências e vulnerabilidades conhecidas (SCA)
- ☐ Pentest ou avaliação de vulnerabilidades periódica
- ☐ Ambientes de desenvolvimento e homologação isolados
- ☐ Pipeline CI/CD com etapas de segurança

Terceiros e supply chain

- ☐ Avaliação de segurança de fornecedores críticos
- ☐ Cláusulas de segurança em contratos com terceiros
- ☐ Monitoramento de acesso de prestadores de serviço

Próximos passos: Marque os itens já implementados e priorize os pendentes por risco. Para diagnóstico personalizado, plano de ação ou pentest, entre em contato: contato@cybershieldgroup.com.br