

Checklist para verificação de Política de Proteção de Dados Pessoais

As normas ABNT NBR ISO/IEC 27001:2013, 27002:2013 e 27701:2019 fornecem diretrizes para gestão de segurança da informação e sua relação com a proteção de dados pessoais, levando em consideração os ambientes de risco das organizações. Essas normas foram projetadas para serem usadas como referência na seleção e na implementação de controles de segurança da informação e proteção de dados pessoais comumente aceitos.

De acordo com o item 5.1 da ABNT NBR ISO/IEC 27701:2019 c/c o item 5.2 da ABNT NBR ISO/IEC 27001:2013 e o item 5.1 da ABNT NBR ISO/IEC 27002:2013, a alta direção deve estabelecer um conjunto de políticas de segurança da informação, entre as quais sugere-se uma política de proteção de dados pessoais. Este *checklist* para verificação de POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS foi definido conforme as diretrizes para implementação relacionadas nos referidos itens.

--> Checklist para verificação de POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

#	Verificar se	S/N	Observações/ evidências
1	<u>Existe</u> uma política de proteção de dados pessoais (ou instrumento normativo equivalente) formalmente estabelecida		
2	A política de PD foi <u>publicada</u> para as partes interessadas (públicos interno e externo)		
3	A política de PD é <u>assinada pela alta direção</u> , refletindo o comprometimento em satisfazer os requisitos legais aplicáveis relacionados com a proteção de dados pessoais		
4	A política de PD prevê a <u>relação com outros normativos</u> associados (e.g. Política de Segurança da Informação)		
5	A política de PD regulamenta os <u>agentes de tratamento</u> no âmbito da organização		
6	A política de PD define <u>gestores e estruturas</u> , atribuindo-lhes <u>papeis e responsabilidades</u> pela proteção de dados pessoais		
7	A política de PD <u>abrange e é aplicável aos fornecedores</u> da organização (que tratem dados pessoais)		
8	A política de PD regulamenta os <u>principais aspectos</u> para a proteção de dados pessoais na organização (tratando, no mínimo, das hipóteses de tratamento de dados pessoais utilizadas, do exercício dos direitos dos titulares, das transferências e compartilhamentos de dados e da interação com a ANPD)		
9	A política de PD prevê a necessidade de <u>comunicação/conscientização</u> aos interessados		
10	A política de PD prevê a sua <u>revisão periódica</u> ou quando ocorrerem mudanças significativas		