12. Política de Gestão de Incidentes de Segurança da Informação

A Política de Gestão de Incidentes de Segurança da Informação define procedimentos para identificação, registro, análise e tratamento de incidentes que possam comprometer a segurança das informações da organização.

Um incidente de segurança pode incluir situações como acesso não autorizado a sistemas, perda de dispositivos contendo dados, vazamento de informações, ataques cibernéticos ou qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade dos dados.

Todos os colaboradores devem estar atentos a possíveis sinais de incidentes e comunicar imediatamente qualquer suspeita aos responsáveis pela segurança da informação da organização.

Após a identificação de um incidente, é iniciado um processo de análise para avaliar sua causa, extensão e impacto potencial. Dependendo da gravidade do evento, podem ser adotadas medidas de contenção imediata para evitar a propagação do problema.

Todos os incidentes identificados devem ser registrados em sistema ou formulário específico, permitindo manter histórico das ocorrências e apoiar a melhoria contínua das práticas de segurança da informação.

Quando houver risco significativo para os titulares de dados pessoais, a organização poderá adotar medidas adicionais, incluindo comunicação aos titulares e à Autoridade Nacional de Proteção de Dados quando aplicável.

Essa política permite que a organização responda de forma rápida e organizada a eventos de segurança, reduzindo impactos e fortalecendo a proteção das informações.