1.*Gap Analysis*

A análise de lacunas, ou *gap analysis*, consiste em avaliar a diferença entre o estado atual de um sistema e o nível ideal de segurança que se deseja alcançar. No setor de TI, essa análise é essencial para entender as necessidades futuras de segurança. Embora o conceito pareça simples, o processo pode ser extremamente complexo, exigindo uma avaliação detalhada dos sistemas existentes, identificação de vulnerabilidades e planejamento de melhorias. Esse trabalho pode levar semanas, meses ou até anos para ser concluído e, normalmente, envolve diversos profissionais e departamentos dentro da organização.

Antes de iniciar a análise, é fundamental estabelecer uma linha de base, ou *baseline*, que servirá como referência para medir o progresso. Existem diversos padrões amplamente reconhecidos, como a publicação **NIST Special Publication 800-171** do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos, que define diretrizes para proteger informações não classificadas. Outra referência comum é a norma **ISO/IEC 27001**, voltada para a gestão da segurança da informação. Além dessas opções, empresas podem desenvolver seus próprios padrões personalizados de acordo com suas necessidades específicas.

A avaliação deve considerar três aspectos principais: pessoas, processos e tecnologias. A análise das pessoas inclui a verificação da experiência e qualificação dos profissionais de segurança da informação, bem como treinamentos e conhecimento das políticas de segurança da organização. Já a análise dos processos envolve a revisão de diretrizes formais, políticas de controle de acesso e procedimentos operacionais.

Durante a etapa de análise, os sistemas em operação são comparados com os requisitos da baseline, identificando falhas de segurança e oportunidades de melhoria. Esse processo pode ser estruturado de forma hierárquica, começando por categorias amplas de segurança e depois detalhando cada segmento específico. Por exemplo, no caso de controle de acesso, a análise pode incluir a verificação de registros de usuários, processos de provisionamento e revisão periódica de permissões.

Após reunir todas as informações, é elaborado um relatório detalhado que descreve a situação atual da organização, as deficiências encontradas e um plano para alcançar os objetivos estabelecidos. Esse relatório inclui gráficos e tabelas comparativas, ajudando a visualizar as áreas que necessitam de mais atenção. É comum utilizar um esquema de cores para destacar os níveis de conformidade das diferentes unidades da empresa, onde áreas em verde estão próximas do padrão desejado, amarelas necessitam de melhorias e vermelhas indicam alto risco.

A implementação das melhorias pode exigir investimentos em novas tecnologias, ajustes nos processos internos e treinamentos para a equipe. O plano de ação deve incluir estimativas de tempo e custo, além de mecanismos de controle de mudanças para garantir uma transição segura. A análise de lacunas não é um processo

único, mas sim contínuo, garantindo que a segurança evolua constantemente para atender aos desafios e ameaças em constante mudança.