1.Risk management

A maioria das organizações possui algum nível de **gestão de riscos**, permitindo identificar ameaças potenciais antes que se tornem problemas maiores. À medida que a organização cresce, os riscos aumentam proporcionalmente, tornando essencial a identificação e mitigação desses desafios. **A gestão de riscos avalia tanto ameaças internas quanto externas, qualificando os riscos para determinar quais demandam atenção prioritária**.

Existem diferentes formas de realizar uma **avaliação de riscos**. Algumas empresas fazem isso apenas uma vez, geralmente atrelado a um projeto específico. Por exemplo, antes de adquirir outra empresa, pode-se realizar um estudo para entender os riscos envolvidos. Da mesma forma, ao implementar novas tecnologias, um levantamento pode ser feito para avaliar os impactos dessa mudança.

Outras empresas adotam uma abordagem **contínua**, incluindo avaliações de risco como parte do **processo de controle de mudanças**. Cada alteração feita nos sistemas passa por uma análise de risco, garantindo que as modificações não criem vulnerabilidades inesperadas.

Além disso, há avaliações de risco **ad hoc**, ou seja, realizadas para um propósito específico. Um exemplo disso seria um CEO que retorna de uma conferência e descobre um novo tipo de ataque que afetou outras empresas. Para entender se a organização está vulnerável, uma avaliação temporária pode ser feita exclusivamente para essa ameaça. Normalmente, esse tipo de análise envolve a criação de um comitê, que elabora um relatório detalhado para a liderança e é desfeito assim que o estudo é concluído.

Algumas organizações adotam um **cronograma fixo** para avaliações de risco, realizando-as a cada três, seis ou doze meses. Dependendo da estrutura da empresa, essas avaliações podem ser feitas **internamente** ou por **terceiros especializados**, garantindo uma análise mais imparcial.

Além disso, certos setores exigem avaliações de risco **obrigatórias** para atender a normas regulatórias. Empresas que armazenam **dados de cartões de crédito**, por exemplo, devem realizar avaliações periódicas conforme exigido pelo **PCI DSS (Payment Card Industry Data Security Standard)**, garantindo que suas práticas de segurança atendam aos padrões da indústria.