1.Risk management strategies

Uma organização pode adotar diversas estratégias para lidar com riscos. Uma dessas estratégias é a **transferência do risco**, **que significa passar a responsabilidade para outra entidade**. Um exemplo comum é a contratação de um seguro de segurança cibernética.

Outra abordagem é a **aceitação do risco**, que é a estratégia mais comum. **A empresa decide aceitar o risco sem medidas adicionais, o que pode incluir a concessão de isenções de políticas internas**. Por exemplo, se um equipamento essencial para a produção usa um sistema operacional Windows, mas o fabricante não permite atualizações, a empresa pode aprovar uma isenção desde que o equipamento não esteja conectado à rede.

Em alguns casos, a empresa pode criar **exceções às políticas de segurança**. Se uma política exige que todas as máquinas sejam atualizadas em até três dias após um patch ser lançado, mas esse patch causa falhas em um software crítico, a empresa pode adiar a atualização até que o problema seja resolvido.

Outra estratégia é **evitar o risco**, **eliminando completamente a possibilidade de que ele ocorra**. Isso pode ser feito, por exemplo, evitando o uso de determinadas tecnologias que apresentem vulnerabilidades.

Também é possível **mitigar o risco**, **reduzindo seu impacto por meio de medidas de segurança**. Se há preocupação com ameaças vindas da internet, a organização pode investir em um firewall de próxima geração para minimizar os riscos.

Dado que uma empresa pode ter dezenas ou até centenas de riscos para monitorar, é essencial contar com um **relatório de riscos**, **que documenta e acompanha todos os riscos identificados, bem como as estratégias adotadas para lidar com eles**. Esse relatório é frequentemente consultado pela alta administração para embasar decisões de negócios, investimentos e estratégias de mitigação. Ele é atualizado constantemente e inclui tanto riscos críticos quanto riscos emergentes que precisam ser considerados no planejamento estratégico da organização.