1.Risk analysis

Determinar níveis de risco pode variar amplamente dependendo da quantidade de variáveis envolvidas. **Uma maneira de avaliar o risco é criar uma avaliação qualitativa, que analisa fatores de risco individuais e critérios específicos para cada um**. Esse tipo de avaliação pode ser exibido de forma ampla, e um método comum é o uso de uma matriz de semáforo para indicar riscos baixos, médios ou altos.

No caso de clientes Windows legados, por exemplo, uma organização pode realizar uma avaliação e identificar um impacto médio. A taxa anualizada de ocorrência pode ser alta, representada pela cor vermelha, indicando um grande número de clientes que precisam ser atualizados. O custo de controle pode ser médio, e o risco geral, então, pode ser classificado como alto.

Outro fator a ser analisado é a presença de funcionários não treinados, que podem ter um impacto muito baixo, uma taxa anualizada média de ocorrência, um baixo custo de controle e um risco geral médio. Da mesma forma, dispositivos sem antivírus podem apresentar impacto médio, uma alta taxa anualizada de ocorrência, um custo médio de controle e um risco geral muito alto.

Esse tipo de análise qualitativa pode ser aplicado a qualquer fator de risco, permitindo uma visão geral de onde concentrar esforços para resolver problemas. No entanto, alguns riscos podem ser calculados de forma quantitativa, o que nos leva à avaliação quantitativa de risco. Esse cálculo pode começar com a **Taxa Anualizada de Ocorrência** (ARO), **que indica quantas vezes um risco pode ocorrer por ano**. Por exemplo, a probabilidade de um furacão atingir Montana é menor do que na Flórida.

Outro fator é o **Valor do Ativo** (AV), **que representa o valor de um ativo para a organização**, incluindo não apenas o custo de reposição, mas também impactos financeiros como multas e prejuízos em vendas. Além disso, há o **Fator de Exposição** (EF), **que expressa a porcentagem do valor do ativo que é perdido devido a um risco**. Se um ativo for completamente perdido, o fator de exposição será 1.0; se apenas uma parte for perdida, o valor será menor.

Com esses fatores, podemos calcular a **Expectativa de Perda Única** (SLE), **que é a perda financeira em um único evento**. Multiplicando o Valor do Ativo pelo Fator de Exposição, obtemos a SLE. Se um laptop roubado vale $1.000 e o fator de exposição é 1.0 (pois o laptop foi perdido por completo), a SLE será de $1.000.

Para estimar as perdas ao longo de um ano, calculamos a **Expectativa de Perda Anualizada** (ALE), **multiplicando a ARO pela SLE**. Se sete laptops forem roubados em um ano, e cada um tiver uma SLE de $1.000, a ALE será de $7.000. No entanto, além do custo financeiro, devemos considerar impactos adicionais, como a perda de dados confidenciais nos laptops roubados.

As avaliações de risco incluem diferentes impactos potenciais. **O impacto mais importante é sobre a vida humana**, pois pessoas não podem ser substituídas. **Depois, vem o impacto na propriedade**, incluindo prédios e equipamentos. A segurança também deve ser considerada, assim como os impactos financeiros e operacionais.

O risco pode ser analisado de acordo com sua probabilidade e a frequência com que ocorre. A probabilidade de risco pode ser expressa qualitativamente, como rara, possível ou quase certa. Já a probabilidade numérica permite associar estatísticas ao risco, muitas vezes baseadas em dados históricos.

Nem todos os riscos exigem ação imediata. Algumas organizações aceitam certos riscos como parte de sua estratégia, o que chamamos de apetite ao risco. Esse apetite pode ser descrito qualitativamente, como conservador, neutro ou expansionista. Já a tolerância ao risco representa a variação aceitável dentro desse apetite. Um exemplo prático é o limite de velocidade em rodovias. O governo define um limite legal, mas, na prática, os motoristas podem ultrapassá-lo ligeiramente sem serem multados, o que representa uma tolerância ao risco por parte da fiscalização. No entanto, essa tolerância pode diminuir em condições climáticas adversas.

Em projetos empresariais, os riscos são frequentemente documentados em um registro de riscos. Esse registro detalha os riscos associados ao projeto, identificando fatores de risco, responsáveis pela mitigação e limites aceitáveis. **Cada fator de risco pode ter um indicador-chave de risco** (KRI), **que pode incluir, por exemplo, falta de definição clara do propósito do projeto, entregáveis mal especificados ou cronograma indefinido**.

O objetivo do registro de riscos é listar esses fatores e possíveis soluções para minimizar as ameaças ao projeto. Além disso, a organização precisa equilibrar o custo da mitigação com o custo potencial do risco, garantindo que os recursos sejam alocados da melhor maneira possível.