**Gerencia de Riscos**

Risco é a medida da exposição a qual o sistema computacional está sujeito. Depende de a probabilidade de uma ameaça atacar o sistema e do impacto resultante desse ataque. Sêmola (2003, p. 50), diz que risco é a **“probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios”**.

Risco é o efeito da incerteza nos objetivos, sendo normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

**Análise Qualitativa = Subjetiva!** - Depois de termos identificado os riscos do projeto, iremos realizar a análise qualitativa dos riscos. Este é o processo de priorização dos riscos para análise ou ação adicional através da avaliação e combinação de sua probabilidade de ocorrência e impacto. Neste processo, faremos uma análise subjetiva com o propósito de priorizar riscos a partir da probabilidade de impacto medida durante a análise dos riscos e, também, determinar o que precisa ser analisado quantitativamente ou não antes de ser construído o plano de resposta aos riscos.

**Análise Quantitativa = Números!** - Este é o processo de analisar numericamente os efeitos dos riscos nos objetivos gerais do projeto. Iremos considerar, por meio de análises, a exposição que o projeto tem aos riscos identificados. Para tais análises são utilizadas, em geral, simulações de cenários como a técnica de Monte Carlo. Este processo pode ser realizado com a entrada dos riscos registrados e priorizados pela análise qualitativa. Vale lembrar que os riscos a serem analisados aqui serão aqueles que podem trazer maior prejuízo ou impacto significativo ao projeto.

Uma análise quantitativa de riscos tem como objetivo **levantar dados mensuráveis — ou seja, numericamente — dos riscos envolvidos em um projeto.**

**Black box** é o tipo de teste onde o profissional não tem conhecimento algum sobre o sistema que será testado, em alguns casos o profissional tem acesso a um range de IP ou algum endereço de website que faça parte do escopo.

**White box** é quando o profissional tem total conhecimento do sistema a ser testado. Geralmente esse tipo de teste é realizado pela própria equipe interna da empresa.

**Gray box** é quando o profissional tem conhecimento parcial sobre o sistema a ser testado. É uma mistura de black box com white box e por isso geralmente é o tipo de teste mais recomendado.

**Questão:** A análise de riscos define os direitos e as responsabilidades de cada usuário em relação à segurança dos recursos computacionais que utiliza e às penalidades às quais cada um deles está sujeito**. (Errado)** - Trata-se de política de segurança e não análise de riscos.

A análise de riscos na segurança da informação é um processo que busca **identificar falhas e vulnerabilidades** que podem expor dados e informações da empresa a ameaças. Nessa análise são avaliadas configurações de redes, problemas em aplicativos, softwares que podem causar falhas futuras, etc.

A ideia é mapear todos os sistemas, programas e aplicativos que podem conter falhas e brechas de segurança. A partir das informações encontradas, é possível tomar medidas que busquem diminuir os riscos das vulnerabilidades.

**ISO 31000 – Processo**

**3. Princípios**

**b) A gestão de riscos é parte integrante de todos os processos organizacionais.**  
A gestão de riscos não é uma atividade autônoma separada das principais atividades e processos da organização. A gestão de riscos faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças.

"A análise de riscos pode ser realizada com diversos graus de detalhe, dependendo do risco, da finalidade da análise e das informações, dados e recursos disponíveis. Dependendo das circunstâncias, a análise pode ser **qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas**."

* Comunicação e consulta
* Estabelecimento do contexto (externo, interno, contexto de processo, definição de critérios de risco).
* Processo de avaliação dos riscos (identificação, análise, avaliação)
* Tratamento dos riscos (seleção de opções, preparação e implementação de planos de tratamento).
* Monitoramento e Análise crítica
* Registro do processo

A **análise de riscos** inclui:

● Identificação dos riscos

● Estimativas dos riscos

● Avaliação dos riscos

O risco de auditoria é uma função dos riscos de distorção relevante e do risco de detecção, a seguir discriminados:

* **Risco de detecção:** é o risco de que os procedimentos executados pelo auditor não detectem uma distorção potencialmente relevante, individualmente ou em conjunto com outras distorções.
* **Risco de distorção relevante:**é o risco de que as demonstrações contábeis contenham distorção relevante antes da auditoria. Consiste em dois componentes, o risco inerente e o risco de controle:
* **Risco inerente:** é a suscetibilidade de uma afirmação a respeito de uma transação, saldo contábil ou divulgação, a uma distorção que possa ser relevante, individualmente ou em conjunto com outras distorções, antes de se considerar qualquer controle preexistente;
* **Risco de controle:** é o risco de que uma distorção não seja prevenida, detectada e corrigida tempestivamente pelo controle interno da entidade.

**6.4.4 Avaliação de riscos**

O propósito da **avaliação de riscos**é apoiar decisões. A avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional. Isto pode levar a uma decisão de:

* Fazer mais nada;
* Considerar as opções de tratamento de riscos;
* Realizar análises adicionais para melhor compreender o risco;
* Manter os controles existentes.
* Reconsiderar os objetivos;

**OWASP**

**Software Assurance Maturity Model (SAMM)**  
  
Cada prática possui 3 objetivos que especificam como podem ser melhorados.  
Estabelece a noção de níveis de práticas a serem alcançadas.  
Os três níveis de cada prática geralmente correspondem a:  
  
**• 0: Ponto de partida implícito, sem prática implementada  
  
• 1: Entendimento inicial da Prática e implementação ad hoc  
  
• 2: Aumento da eficiência e/ou efetividade da Prática  
  
• 3: Domínio completo da Prática em escala**