
Análise de Riscos em SegInfo

Pós-graduação em Redes
Prof. Frederico Sauer

Análise de Riscos

- Administrar SegInfo é o processo de conhecer, avaliar, reagir e aceitar um nível de Risco, que deve ser mantido em todo o ciclo de vida da Informação
- A probabilidade da ocorrência de um IS é a mesma de uma Ameaça explorar uma Vulnerabilidade, causando Impacto

Conceitos fundamentais

- A questão não é apenas definir os riscos existentes, e sim gerenciar um nível de risco aceitável
- Questões-chave
 - Os riscos foram identificados ?
 - Os riscos foram definidos por prioridades ?
 - Foram tomadas ações para reduzir a probabilidade do risco tornar-se um IS ?
 - Há Plano de Contingências para os riscos ?
 - Como será monitorada a eventual ocorrência do IS ?
 - Quem é responsável pelo gerenciamento do nível de risco ?

Por quê não se Gerencia o Risco ?

- Pessoas acham que, apesar do risco, o IS não ocorrerá com elas;
- Não há tempo disponível para o gerenciamento do nível de risco;
- Excesso de auto-confiança considerando que poder-se-á recuperar em caso de IS;
- Pessoas não gostam de gerenciar riscos.

Fases da Administração do Risco

- Avaliação (Análise) de Riscos
 - Identificação, dimensionamento do nível e priorização dos riscos
- Gerenciamento dos Riscos
 - Redução do nível de probabilidade da ocorrência de um IS;
 - Investimento nas ações de contingência
 - Designação de um gerente

Riscos de SegInfo

- Riscos Físicos – catástrofes, acidentes, sabotagens, acessos indevidos
- Riscos Tecnológicos – bugs, vírus, worms, invasões, destruição e alteração lógica de dados
- Riscos Humanos – ignorância, displicência, vingança, ganância,

Riscos Físicos

- Todos os perímetros de segurança estão definidos e adequadamente protegidos ?

Riscos Tecnológicos

- Todos os sistemas (Software básico e Aplicações) foi testado e está atualizado quanto às vulnerabilidades conhecidas ?
- São usadas adequadamente ferramentas de mitigação de ameaças ?

Riscos Humanos

- Há estratégia de capacitação e disseminação de cultura de SegInfo ?
- Há mecanismos de desestímulo e monitoração de comportamentos indevidos ?

Modalidades de Análise

- Qualitativa – apenas considera os Impactos resultantes de um IS, de forma subjetiva e genérica – Matriz de Classificação
- Quantitativa – mais abrangente, avalia numericamente os aspectos da probabilidade de um IS ocorrer e seus impactos – Ferramentas especializadas (Decision Tree, Simulações)

Análise Qualitativa

- Probabilidade de ocorrência do IS

Prob	Ameaças ou Oportunidades					
MA	M	M	A	MA	MA	
A	B	M	M	A	MA	
M	B	M	M	A	A	
B	MB	B	M	M	A	
MB	MB	MB	B	M	M	
	MB	B	M	A	MA	
	Impacto					

100%		Probabilidade	Muito alta	100%
	Provável	alta	Alta	85%
		Probabilidade	Média	
50%		média		35%
	Improvável	Probabilidade	Baixa	15%
0%		baixa	Muito baixa	0%

Análise Qualitativa

- Avaliação Qualitativa (exemplo)

Classificação	Probabilidade	Impacto
Alta	É muito provável que o evento de Risco ocorra	Impactos irreversíveis
Média	É provável que o evento de Risco ocorra	Impactos significativos
Baixa	É improvável que o evento de Risco ocorra	Impactos absorvíveis

Aspectos do Impacto

- Prejuízo Tangível:
 - Valor intrínseco da Informação
 - Comprometimento do Sigilo
 - Recuperação ou até Reconstrução de dados
 - Perdas de clientes, oportunidades, multas
- Prejuízo Intangível
 - Comprometimento da imagem da empresa ou de um produto

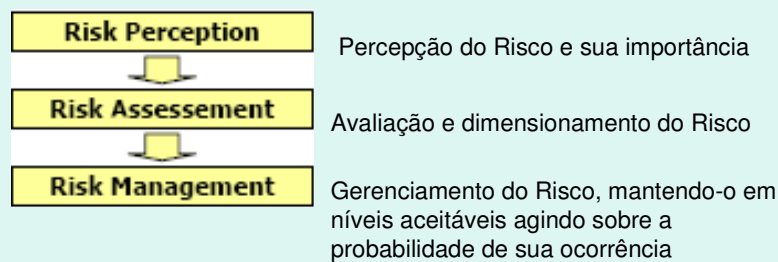
Aspectos do Impacto

- Circunstâncias agravantes ou atenuantes
 - Ameaças
 - Vulnerabilidades
 - Mecanismos de Segurança existentes
- Probabilidade de ocorrer um determinado IS
 - Dados históricos (desejado)
 - Sensibilidade do Analista

Modalidades de Risco

- Risco Negativo – mais óbvio, representa situações de prejuízo ou dano (impacto iminente)
- Risco Positivo – Aquele com potencial de trazer ganhos adicionais, mas também impactos – PMI: Oportunidade
 - Ex.: o batedor de penalty
 - Ex.: Adoção do Linux (desconhecido) em substituição ao software proprietário (dominado) para as soluções de segurança

Tratamento do Risco



Risk Perception



Risk Assessment

- Várias técnicas focadas em PROJETOS, mas inadequadas para PROCESSOS, como a PMI
- Apesar disso, como as instituições operam com orçamentos para exercícios financeiros, permitem a avaliação dos custos de cada solução e o somatório de seu montante

Risk Management

- Riscos Negativos
 - Eliminar
 - Eliminar a probabilidade da ocorrência de impactos através de controles agressivos
 - Aceitar
 - Absorver, ativa ou passivamente os impactos
 - Ativamente – elabora-se um PLCont
 - Passivamente – não faz nada
 - Mitigar (Controlar)
 - Ações objetivas no sentido de minimizar os impactos na ocorrência de um IS
 - Transferir
 - Terceirizar a atividade impactante ou fazer seguro

Risk Management

- Riscos Positivos (Oportunidades)
 - Ignorar
 - Descartar sua implementação
 - Melhorar
 - Ações objetivas para aumentar a probabilidade da ocorrência e o impacto (positivo)
 - Provocar
 - Buscar a causa e provocá-la (probabilidade 100%)

Planilha de *Risk Assessment*

- Conceitos Básicos:
 - Custo de um Projeto
 - Dimensionamento do Investimento em um PN em um período (despesas, custo fixo e custo variável)
 - Ameaças e Vulnerabilidades
 - Oportunidades – Riscos positivos
 - Valor Esperado – custo intrínseco da ocorrência de um IS, de acordo com o impacto e a sua probabilidade de ocorrer
 - Valor Esperado do Projeto – Valor Base referente ao PN + Valor Esperado dos Riscos → Custo das ações de Tratamento

Planilha de *Risk Assessment*

- Prioridades
 - Nunca há tempo e recursos para Controle do Risco de TODAS as ameaças simultaneamente
 - Usa-se a priorização par-a-par

Riscos					Frequência
Risco 1	Risco 1				1
Risco 2	2	Risco 2			3
Risco 3	1	2	Risco 3		0
Risco 4	4	2	4	Risco 4	2

Trabalho - 1ª Parte

- 1. Analisar as informações existentes sobre o caso.
- 2. Façam um BrainStorming
 - Produzam uma Lista de Riscos de SegInfo para o PN Selecionado, a mais extensa possível (mínimo de 10 riscos, sendo 2 positivos).
 - Considerar Riscos positivos E negativos;
- 3. Analisem as descrições dos Riscos – ajustem com Causa e Consequência
- 4. Façam a categorização dos Riscos
- 5. Transcrevam para a ferramenta SegInfo.xls
- 6. Revejam e aprovem os Riscos identificados e categorizados na equipe

Trabalho - 2ª Parte

- Agora que os riscos estão identificados, é necessário analisá-los quanto à sua probabilidade de ocorrência e o seu impacto.
- Utilizando a ferramenta SegInfo.xls:
 - 1. Identificar a abordagem de análise a ser utilizada (qualitativa/ quantitativa) e seus motivos para esta seleção;
 - 2. Calcular o Valor Esperado para cada Risco;
 - 3. Calcular os Valores Esperados para o projeto;
 - 4. Classifiquem os Riscos por ordem de importância;
 - 5. Decidam quais Riscos serão tratados e quais não serão;

Trabalho - 3ª Parte

- Agora que vocês já identificou, quantificou e priorizou os riscos, sua equipe precisa elaborar estratégias específicas de reação a estes riscos.
- Utilize a ferramenta SegInfo.xls:
 - 1. Analise cada Risco e decida pela Reação
 - 2. Avalie o custo da Reação
 - 3. Compare o custo da Reação contra o Valor Esperado original
 - 4. Decida o que a Reação provoca em termos de:
 - a) Probabilidade
 - b) Impacto
 - 5. Avalie o Novo Valor Esperado, contra o Custo da Reação e contra o Valor Esperado Original
 - 6. Decida se esta relação é coerente
 - 7. Analise o Valor Esperado após as Reações e tome a decisão sobre o orçamento do PN.

Conclusão

- **Ao final do trabalho, questione-se:**
 - Você está se antecipando aos riscos?
 - Você está acompanhado os riscos?
 - Os riscos mitigados foram contingenciados de maneira suficiente?
 - Os riscos aceitos podem ser tolerados?
 - Os resultados do plano de contingência foram satisfatórios?
 - Os contornos realizados geraram resultados eficazes?
 - É necessária a tomada de alguma ação extra?
 - Todos os *stakeholders* estão cientes dos riscos, das responsabilidades e das ações?
 - Todos os *stakeholders* estão sendo informados das atualizações?
 - Você está estimulando a Gerência de Riscos em todos os níveis?
 - Você está anotando lições aprendidas?
 - O processo está sendo seguido?
 - Os canais de comunicação estão abertos?