Segurança da Informação

Aula 05

Análise do risco econômico para a segurança:

"Não há almoço grátis; alguém sempre paga a conta. Qual é o valor da conta da segurança para sua empresa?"

Análise do risco econômico para a segurança:

A finalidade da análise do risco econômico para a segurança é obter a medida da segurança existente em determinado ambiente.

A etapa final da análise de risco é a geração do plano de segurança da organização.

Qualquer plano de segurança deve ser montado em função da organização para a qual se aplique, como uma roupa é feita sob medida.

O enfoque de segurança para cada caso deve ter como preocupações básicas:

Evitar a ocorrência ou sinistro	→	Plano de segurança
Detectar ou combater os danos ou sinistros	→	Medidas de Segurança
Minimizar o dano, recompondo a função original	→	Plano de Contingência

Aula 05

Segurança da Informação

O plano de segurança deve preocupar-se com as medidas e procedimentos para que as falhas ou sinistros não ocorram e já prover a forma de detecção e combate através das medidas de segurança.

O plano de contingência deve servir para minimizar os efeitos ou danos ocorridos se o plano de segurança e as medidas de segurança não conseguiram evitá-las.

O plano de segurança deve sempre iniciar com a análise dos fatores que caracterizam as ameaças.

Aula 05

Segurança da Informação

Tipos de ameaças mais comuns:

Local / edifício	Fogo, raios, água, furtos/roubos, espionagem, terrorismo/sabotagem
Infra-estrutura técnica	Insuficiência de equipamentos, falhas técnicas, oscilações elétricas, falta de energia/água/combustível
Redes de comunicação	Sabotagem, espionagem, modificação, fraudes, quedas/interrupções
Software	Furtos, alterações indevidas, vírus, falta de controle de acesso

Aula 05

Segurança da Informação

Tipos de ameaças mais comuns (continuação):

Dados/ meios de armazenamento	Falhas de controle, backups insuficientes/inadequados, desmagnetização, falhas no transporte, falhas no armazenamento
Hardware	Oscilações de energia, falhas de climatização, instalações inadequadas, danos físicos

Considerações:

- relação custo benefício - não se gasta mais dinheiro em proteção do que o valor do ativo a ser protegido;
- bom senso – nos casos em que não é possível uma análise direta da relação custo/benefício, há meios indiretos de se obterem valores bem próximos dos reais.

Aula 05

Segurança da Informação

Fluxo de análise das ameaças e riscos

Ameaças

↓

Probabilidade dos riscos

↓

Peso dado ao risco

↓

Avaliação do risco

↓

Prioridades da proteção

↓

Medidas de proteção

Aula 05

Segurança da Informação

Metodologia para auxiliar na decisão dos investimentos de segurança:

- Análise dos riscos e suas conseqüências
- Estimativa das probabilidades de ocorrência
- Estimativa do dano causado pela ocorrência do incidente (vulnerabilidade)
- Cálculo de exposição ➔ (vulnerabilidade ou dano financeiro causado pela ocorrência do incidente X probabilidade de ocorrências em vezes/ano)
- Análise das medidas de proteção contra riscos
- Seleção das medidas de proteção a implementar, em função da relação custo/eficácia da segurança

Aula 05

Segurança da Informação

Probabilidade dos riscos e suas conseqüências:

RISCO = PROBABILIDADE x GRAU DAS CONSEQÜÊNCIAS

Probabilidade	
Peso	Probabilidade
1	Extremamente improvável
2	Improvável
3	Possível
4	Bem possível/ já aconteceu

x

Conseqüências	
Peso	Grau
1	Insignificante
2	Médio
3	Grande
4	Põe em perigo e existência da empresa

=

Prioridade de proteção	
Resultado obtido X Prioridades de proteção:	
0 – 2	Pouco ou nenhuma
2 – 6	Baixa
6 – 8	Média
8 – 16	Alta

Aula 05

Segurança da Informação

Análise econômico-contábil da segurança da informação

Consideramos que programas de computadores e informações são ativos porque, para sua obtenção, são necessários os três fatores clássicos de produção, conforme sua definição econômica a saber:

- **Capital** → O capital investido em informática corre os mesmos riscos de destruição, roubo, violação, fraude,... que o capital empregado em outro tipo de atividade. Esses ativos são representados por instalações, equipamentos, softwares e dados.

- **Mão-de-obra** → O processamento de informações e as atitudes ligadas às informações ainda não podem prescindir do uso da mão-de-obra com graus variados de especialização. A mão-de-obra é o componente de custo com participação percentual mais elevada dentro de um ambiente de informações, principalmente em decorrência da constante queda de preço do hardware, em termos de unidade de informação processada pelo valor investido em equipamentos.

Aula 05

Segurança da Informação

Análise econômico-contábil da segurança da informação

- **Processos** → Temos duas classes principais de materiais em processo, a saber: o acervo de informações destinadas a confeccionar as ferramentas de processamento de informações ou sistemas de programas de aplicações ou de controle da atividade e informações relacionadas com as atividades dentro das empresas, que serão processadas pelos sistemas informatizados. Além disso, temos que ter sempre em conta que existe informação sem custo.

Aula 05

Metodologia

Ainda não existe metodologia 100% eficaz para se fazerem análises de custo/benefício.

Quase todas as metodologias existentes até o momento contemplam somente parte do problema de análise de custo/benefício ou estão mais voltadas para aspectos de destruição de informações.

O fundamental para que a metodologia funcione de forma adequada é uma avaliação correta da importância dos ativos e dos riscos a que eles estão sujeitos.

Aula 05

Fatores envolvidos na análise

A primeira coisa a ser feita no âmbito da análise de risco econômico da segurança é determinar quais fatores afetam a segurança dos ativos que serão avaliados.

São dois os principais fatores envolvidos:

- Grau de impacto da ocorrência
  → Trataremos das conseqüências que uma ocorrência danosa provocaria para a organização

- Nível de exposição à ocorrência
  → Listaremos os riscos a que cada ativo está sujeito

Aula 05

Fatores envolvidos na análise (continuação):

Grau de impacto

ALTO RISCO – a organização como um todo, ou parte importante da mesma, tem suas atividades fortemente reduzidas a curto ou médio prazo, não permitindo a continuidade normal de suas atividades, ou até mesmo pondo em risco a sobrevivência da organização.

MÉDIO RISCO – as atividades da organização, ou parte da mesma, sofrem dificuldades sérias, que acarretam prejuízos sensíveis, mas que não chegam a afetar a sobrevivência da organização como um todo.

BAIXO RISCO – as atividades da organização não são afetadas de forma significativa pela ocorrência.

Aula 05

Fatores envolvidos na análise (continuação):

Nível de Exposição

Cada atividade, processo ou produto dentro de uma organização está exposto a um certo grau de risco que lhe é inerente; os riscos existem associados a quaisquer atividades. O nível de exposição está diretamente relacionado com a probabilidade de ocorrência de um evento danoso para um determinado ativo.

É importante fazer uma avaliação o mais preciso possível do nível de exposição, caso o mesmo não possa ser reduzido ou a própria exposição eliminada, e estar preparado para suas eventuais ocorrências, de modo que sejam no máximo evitadas; mas, no caso de as mesmas virem a acontecer, é importante ter medidas de segurança prontas para serem ativadas.

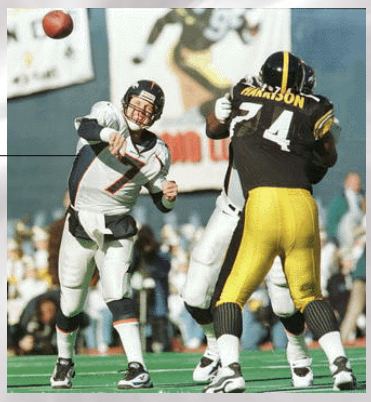
Aula 05

Segurança da Informação

Análise do Risco

- Analogia com Futebol Americano

Presidente da Organização



Aula 05

Segurança da Informação

Análise do Risco

- Analogia com Futebol Americano

Gerente responsável por sua área

Projeto de segurança

Aula 05

Segurança da Informação

Análise do Risco

- Missão do Gerente dentro da análise de risco
  - Evitar ocorrências
  - Detectar danos
  - Minimizar danos

Gerente responsável por sua área

Projeto de segurança

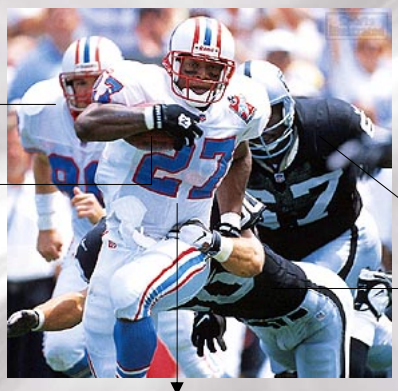
Aula 05

Segurança da Informação

Análise do Risco

- Ampliando a Visão do Gerente

Stakeholders



Projeto de Segurança

Fatores de Risco

Gerente responsável por sua área

Aula 05

Segurança da Informação

Análise do Risco

- Ampliando (ainda mais) a Visão do Gerente

Aula 05

Segurança da Informação

Análise do Risco

Stakeholders

• Pessoas, grupos ou organizações, envolvidos ativamente no projeto que podem ganhar ou perder (poder e/ou dinheiro) com seu resultado

Principais stakeholders

- Gerente do projeto (e sua equipe)
- Executivo patrocinador
- Cliente

Fatores de Risco

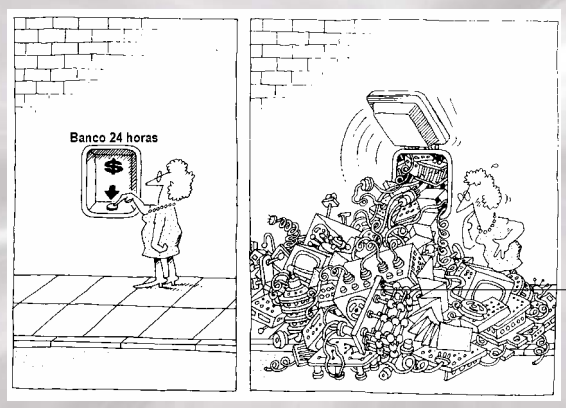
"É a probabilidade de que qualquer variável associada a um projeto possa assumir valores, dentro da sua distribuição normal de valores, que possam diminuir, ou eliminar por completo, as chances de sucesso do projeto".

Aula 05

Segurança da Informação

Análise do Risco

- Por que o assunto vem recebendo atenção ?



Fatores de Risco

Aula 05

Segurança da Informação

Análise do Risco

Análise de risco é garantia de sucesso ?

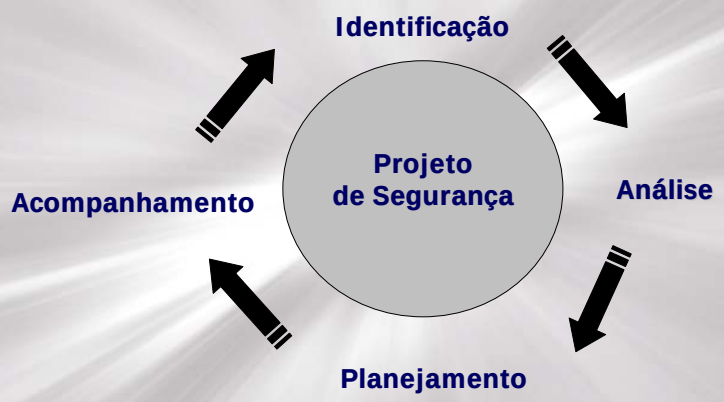
X

É sim, se você conhecer bem seus fatores de risco!
A forma mais eficiente de se efetuar análise de custo/benefício é fazer com que os usuários finais de casa sistema de informação avaliem o valor das mesmas para a organização.

Aula 05

Segurança da Informação

Análise do Risco



Aula 05

Segurança da Informação

Análise do Risco

Fase de Identificação

- Identificação dos Stakeholders
- Lista de Fatores de Risco
- Brainstorm

Análise

- Impacto de fatores de risco sobre o projeto
- Priorização de fatores de risco

Aula 05

Análise do Risco

Planejamento

- Atribuição de responsabilidades
- Planos de contenção (redução do risco)
- Planos de contingência (diminuir o estrago)

Acompanhamento

- Monitoramento do fator de risco
- Acionamento dos planos de contenção e contingência

Segurança da Informação

Termino da Aula 05