

Gerenciamento de Risco

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br



Gestão de Segurança

Roteiro

- Conceitos básicos
- Importância da Informação
 - utilidade, valor, validade, classificação
- Riscos
 - Análise
 - Identificação
 - Gerência
- Estudo de caso

Marcos Laureano

2





Gestão de Segurança

Risco

- Uma expectativa de perda expressada como a probabilidade de que uma ameaça em particular poderá explorar uma vulnerabilidade com um possível prejuízo
- Uma medida da incerteza associada aos retornos esperados de investimentos
- Não é ruim por definição, o risco é essencial para o progresso e as falhas decorrentes são parte de um processo de aprendizado.

Marcos Laureano

3



Avaliação ou Análise de Risco

- Um processo que identifica sistematicamente
 - recursos valiosos de sistema
 - ameaças a aqueles recursos
 - quantifica as exposições de perda
 - recomenda como alocar recursos às contramedidas no para minimizar a exposição total

Gerenciamento de Riscos

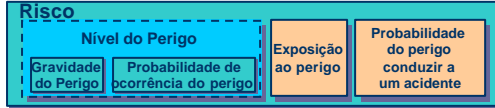
- O processo de identificar, de controlar, os eventos incertos, eliminando ou minimizando os que podem afetar os recursos de sistema
- Uma das ferramentas mais poderosas no gerenciamento de riscos é o conhecimento
- Indica os caminhos e as informações que devem ser protegidas
 - disponibilidade, integridade, confidencialidade, ...

Cenário Atual

- O risco não é um novo problema ou uma nova terminologia
- Os seres humanos sempre tiveram de enfrentar (ou encarar) os riscos no seu meio ambiente

Risco e Perigo

- O perigo tem duas importantes características
 - a gravidade (algumas vezes denominada de dano)
 - probabilidade da ocorrência
- A gravidade é definida como o pior acidente possível de ocorrer
- A probabilidade de ocorrência pode ser especificada quantitativamente e qualitativamente



7

Importância da Informação

- Qual a utilidade da Informação ?
 - Lembrar dos fins: suporte, estratégia, ...
- Qual o valor da Informação ?
 - Avaliação pessoal do dono da informação
- Qual a validade da Informação ?
 - Deve possuir um período de validade
- Quem é o responsável pela manutenção da classificação da informação ?
 - O criador é responsável pela classificação inicial

8

Vale a pena proteger tudo ?

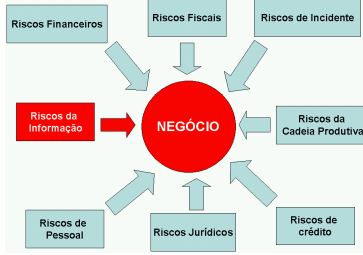
- Segurança requer investimentos
- Pode-se utilizar o ROI - *Return on Investment*
 - Não existe um modelo unificado
- Conhecimento do Negócio
 - Este é o ponto chave de qualquer gerenciamento de riscos



9

Proteger contra o quê ?

- O objetivo da segurança da informação é protegê-la contra riscos
- O objetivo é proteger a informação, não o ativo que a contém



Como proteger uma informação ?

- Identificação dos Riscos
 - que o negócio está sujeito
- Quantificação dos Riscos
 - impacto sobre o negócio
- Tratamento dos Riscos
 - medidas para mitigar o risco
- Monitoração dos Riscos
 - acompanhamento do risco

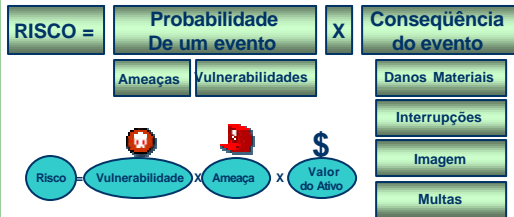
Requisitos básicos para Gerência

- Objetivos do Negócio
 - Especificação clara do objetivo
- Riscos
 - Identificação dos riscos para cada objetivo de negócio
- Ações
 - Ações para cada risco identificado

A Análise

- A análise de risco consiste em um processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios.

Análise de Risco

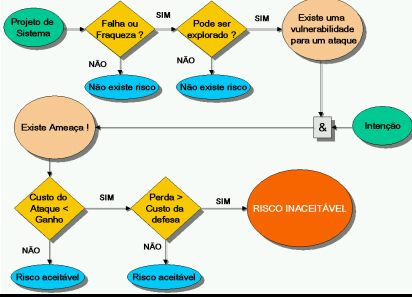


- Conhecer o risco é ganhar mobilidade.
- Segurança é risco tendendo a zero.

Análise de Risco

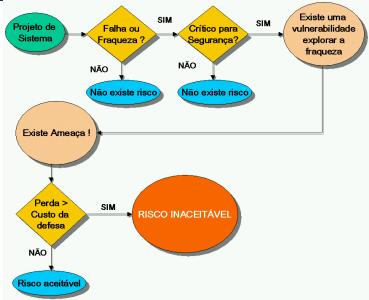
1. Por que fazer uma análise de risco ?
 1. Indicações que os planos se concretizem
2. Quando fazer uma análise de riscos ?
 1. Sempre, antecedendo um investimento
3. Quem deve participar da análise de riscos ?
 1. Especialistas em análise de riscos e no negócio da empresa
4. Quanto tempo o projeto deve levar ?
 1. deve ser realizada em tempo mínimo

Roteiro para Identificar Riscos



Marcos Laureano

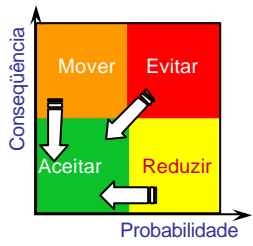
Roteiro para Identificar Riscos



Marcos Laureano

Finalizando

- Qualquer investimento deve ter objetivo
 - A análise de riscos serve para direcionar investimentos de segurança
- Não existe segurança 100%
 - Segurança é risco tendendo a zero
 - Se você não puder medir o risco, você não poderá reduzi-lo.
- A Gerência de Riscos (PMI) pode (deve) ser utilizado como referência



Marcos Laureano

Então...

- Dúvidas ??
- Perguntas ??
- Comentários ??
