
# Segurança em Sistemas de Informação

**Prof. Me. Luis Gonzaga de Paulo**

# Gestão de Riscos

- Abordagem Reativa
- Abordagem Proativa
- Análise Quantitativa
- ROI
- Matriz P x I

# Abordagem Reativa

- Ação a partir da ocorrência do incidente:
  - Proteger a vida e garantir a segurança das pessoas;
  - Conter os danos;
  - Avaliar os danos;
  - Determinar a causa dos danos;
  - Corrigir os danos;
  - Analisar o resultado e atualizar os planos e controles.

# Abordagem Proativa

- Prevenção contra o incidente:
  - Identificar os ativos;
  - Calcular os possíveis  danos de um incidente;
  - Identificar as vulnerabilidades;
  - Planejar e atuar para minimizar o risco de incidentes;
  - Implementar e manter os controles apropriados.

# Análise Quantitativa

- Calcular valores numéricos (objetivos)
- Estimar:
  - O valor real de cada ativo em termos do custo de substituição;
  - Custo associado à perda de produtividade ou resultados;
  - Custo representado pela reputação ou marca;
  - O valor geral do ativo para a organização;
  - O impacto financeiro imediato da perda do ativo;
  - O impacto indireto nos negócios causado pela perda do ativo;
  - Outros valores comerciais diretos ou indiretos.

# Análise Quantitativa

- Expectativa de perda única (EPU):
  - É a quantidade total de receita perdida em uma única ocorrência do risco;
- Taxa de ocorrência anual (TOA):
  - É o número de vezes que se espera que o risco ocorra durante o ano
  - Intervalo de 0% (nunca) a 100% (sempre);
- Expectativa de perda anual (EPA):
  - É a quantidade de dinheiro que se perderá em um ano se nada for feito para atenuar o risco;
  - É calculada multiplicando-se EPU x TOA.

# Análise Quantitativa

Exemplo 1:

- Um site de e-commerce é suportado por um conjunto de servidores (farm), e opera 24 horas por dia, sete dias por semana.

- O site fatura $2.000,00 por hora, gerando uma receita aproximada de $17.520.000,00 por ano.

- O histórico de incidentes que resultam em paradas aponta para uma média de 06 (seis) horas por ano.

# Análise Quantitativa

Calculando:

Taxa de ocorrência anual (**TOA**):

= 06 horas por ano (ou 0,000685)

Expectativa de perda anual (**EPA**):

= $2.000,00 x 6 = $12.000,00

Ou

= $17.520.000,00 x 0,000685 = $12.000,00

# Análise Quantitativa

Exemplo 2:

- O mesmo site de e-commerce é suportado por uma *web farm* cujo valor é de $150.000,00.

- Um incêndio pode destruir até 25% dos equipamentos antes de ser controlado.

- Qual é a expectativa de perda única (EPU)?

# Análise Quantitativa

## EPU – Site de e-commerce:

- Web Farm de $150.000
- Incêndio destrói 25%
- EPU: $150.000 x 0,25 = $37.500

## TOA

- Probabilidade da ocorrência de um incêndio uma vez a cada dez anos
- TOA: 1 ÷ 10 = 0,1

## EPA

- $37.500 x 0,1 = $ 3.750

# Análise Quantitativa

## Exemplo 3

– Uma Empresa de e-commerce com faturamento anual bruto de $10 milhões e margem de lucro em torno de 5%, mantém seus sistemas em um único datacenter próprio, junto a um de seus centros de distribuição à margem da rodovia Régis Bittencourt, próximo ao rio Ribeira do Iguape. A empresa usa o serviço de logística dos Correios e algumas transportadoras, cujos sistemas são integrados (B2B). A região é conhecida por secas prolongadas, quando incêndios devastam grandes áreas de pastagens á margem do rio, sendo que na última ocorrência, há cerca de vinte anos, cerca de 25% do CD foi destruído. É conhecida também a ocorrência de inundações durante os períodos de cheia do rio, sendo que a última ocorrência, há dez anos, resultou em perdas equivalentes a 5% do faturamento.

# Análise Quantitativa

| Descrição do Risco | Expectativa de Perda Única - EPU | Taxa de Ocorrência Anual - TOA | Expectativa de Perda Anual - EPA | Comentário |
|---|---|---|---|---|
| Incêndio que reduz 25% do faturamento anual | 2.500.000,00 | 5% | 125.000,00 | A cada 20 anos |
| Alagamento que reduz 5% do faturamento anual | 500.000,00 | 10% | 50.000,00 | A cada 10 anos |
| Falha de energia prolongada - 20 ocorrências de 01 hora de duração. | 22.831,05 | 100,00% | 22.831,05 | Todo ano |
| Defeito em equipamento que reduz 1% do faturamento anual | 100.000,00 | 20% | 20.000,00 | A cada 5 anos |

# Resultados

- Valores monetários atribuídos aos ativos;
- Uma lista abrangente de ameaças significativas;
- A probabilidade de ocorrência de cada ameaça;
- A possível perda para a empresa com base em cada ameaça ao longo de doze meses;
- Informações para a tomada de decisão sobre salvaguardas, controles e ações a serem implantados.

# Retorno do Investimento (ROI)

É calculado com base em:

- EPA antes do controle
- EPA após o controle
- Custo anual do controle

**ROI:**

(EPA antes do controle) – (EPA após o controle) – (custo anual do controle)

# Retorno do Investimento (ROI)

Exemplo 4:

- A EPA associada ao risco de um ataque desativar um servidor da Web é de $ 12.000.
- Após a salvaguarda sugerida ter sido implementada, a EPA é avaliada em $ 3.000.
- O custo anual de manutenção e operação da salvaguarda é de $ 650
- O retorno do investimento em segurança é de $ 8.350 por ano:

$ 12.000 - $ 3.000 - $ 650 = $ 8.350.

# Matriz P x I

| Item | Risco | Probabilidade | Impacto |
|---|---|---|---|
| #1 | Acesso às informações da base de dados | Alta | Alto |
| #2 | Roubo de identidade / credenciais do usuário | Baixa | Alto |
| #3 | Interrupção da aplicação durante operação crítica | Alta | Alto |
| #4 | Interrupção da aplicação durante operação crítica | Baixa | Alto |
| #5 | Interrupção da aplicação durante operação crítica | Baixa | Alto |
| #6 | Uso impróprio dos recursos do ambiente | Média | Baixo |

# Matriz P x I

| | | Probabilidade | | | | |
|---|---|---|---|---|---|---|
| | | Muito Baixa | Baixa | Média | Alta | Muito Alta |
| Impacto | Muito Alto | | | | | |
| | Alto | | #2, #4, #5 | | #1, #3 | |
| | Médio | | | | | |
| | Baixo | | | #6 | | |
| | Muito Baixo | | | | | |