Segurança da Informação e Proteção ao Conhecimento

Aula 05 – Gestão de Riscos

Prof. Dalton Martins
dmartins@gmail.com

Gestão da Informação
Faculdade de Informação e Comunicação
Universidade Federal de Goiás

Risco de segurança é uma combinação de ameaças, vulnerabilidades e impactos. Ameaças são eventos que exploram vulnerabilidades (fragilidades) e podem causar danos. O impacto é a consequência de uma vulnerabilidade ter sido explorada por uma ameaça.

No tocante à gestão de riscos, algumas definições são consideradas importantes e são apresentadas a seguir:

- A gestão de riscos compreende todas as ações tomadas para controlar os riscos em uma organização, incluindo análise/avaliação, tratamento, aceitação e comunicação dos riscos.

- A análise de riscos identifica e estima riscos, considerando o uso sistemático de informações. Engloba a análise de ameaças, vulnerabilidades e impactos, e é considerada o ponto chave da política de segurança da informação de uma organização.
- A avaliação de riscos compara o risco estimado na análise com critérios predefinidos, objetivando identificar a importância do risco para a organização.
- A aceitação de riscos engloba o levantamento do nível aceitável de riscos para uma organização de acordo com seus requisitos específicos de negócio e segurança.
- O tratamento de riscos corresponde à seleção e implementação de medidas para modificar um dado risco.

A comunicação de riscos envolve as iniciativas de divulgação dos riscos aos funcionários, dirigentes e terceiros (estes últimos, quando cabível e necessário).

Questões determinantes

- Identificar ameaças.
- Identificar impactos.
- Determinar a probabilidade de concretização de ameaças.
- Entender os riscos potenciais.
- Classificar os riscos:
  - Por nível de importância.
  - Por grau de severidade das perdas.
  - Por custos envolvidos.

Gestão de riscos

Implementar em três níveis:

- 1º nível – Tecnologia.
- 2º nível – Processos.
- 3º nível – Pessoas.

A gestão de riscos deve considerar os três níveis a seguir para sua implementação: tecnologias, processos e pessoas. A tecnologia garante a adequação técnica necessária ao tratamento adequado dos riscos; os processos asseguram que as atividades que compreendem a gestão de riscos sejam consideradas de forma sistemática; e, por fim, as pessoas, de modo que os funcionários e dirigentes identifiquem suas responsabilidades, conheçam os riscos e possam ajudar no sentido de sua redução e controle. Instrumentos como a política de segurança da informação e um código de conduta são recomendados no contexto.

Análise e avaliação de riscos

- O que proteger?
- Quais as vulnerabilidades e ameaças?
- Como analisar?
  - Análise de impacto.
  - Probabilidades de ameaça.
  - Matriz de relacionamentos.
  - Cálculo dos riscos.
  - Avaliação de riscos.

Identifica, quantifica/qualifica e prioriza os riscos de segurança da informação. Essencial para:

- Gestão de riscos.
- Proposição de medidas de segurança adequadas.

Considerações:

- Devem ser sistemáticas.
- Devem usar métodos específicos.
- Devem ser realizadas periodicamente.

Analisando os riscos

Considerar:

- Danos causados por falhas de segurança.
- Probabilidade de falhas ocorrerem.

Questões relevantes:

- O que proteger?
- Quais as vulnerabilidades e ameaças?
- Como analisar?

Resultado:

- Dados que guiam a gestão de riscos.

O que proteger?

Deve-se analisar as ameaças e vulnerabilidades antes. Ativos típicos:

- Hardware.
- Software.
- Dados.
- Pessoas.
- Documentos.
- Sistemas de informação.
- Valores intangíveis.
- Contratos etc.

Vulnerabilidades e ameaças

- Determinar as vulnerabilidades e ameaças aos ativos a proteger.
- Determinar o impacto.
- Considerar:
  - Compromisso com a informação.
  - Confidencialidade.
  - Integridade.
  - Disponibilidade.

Exemplos de ameaças típicas:

- Desastres naturais.
- Falhas no fornecimento de energia elétrica.
- Roubo.
- Ameaças programadas.
- Falhas de hardware.
- Falhas de software.
- Erros humanos.

Analisar considerando:

- Custos.
- Nível de proteção requerido.
- Facilidades de uso.

A análise de risco pode ser:

- Qualitativa.
- Quantitativa.

Tipo de dado	Classificação	Importância
Resultado clínico	Pesquisa	Alto
Pesquisa de mercado	Pesquisa	Baixo
Patentes dependentes	Proprietária	Alto
Memorandos	Administrativo	Baixo
Salários de empregados	Financeira	Médio
Característica de novo produto	Proprietária	Médio

Tabela 5.1
Exemplo para dados de determinada organização.

Análise de impactos

Pode considerar o impacto em curto e longo prazo. Exemplo de classificação:

- 0 – irrelevante.
- 1 – efeito pouco significativo.
- 2 – sistemas não disponíveis por determinado período.
- 3 – perdas financeiras.
- 4 – efeitos desastrosos, sem comprometimento dos negócios.
- 5 – efeitos desastrosos, comprometendo os negócios.

A matriz de relacionamentos é um modo simplificado de visualização das ameaças, impactos e probabilidades de acordo com o exemplo proposto, isto é, relacionando, para cada ameaça potencial na organização, seu impacto e probabilidade de ocorrência. Por exemplo, podem ser utilizadas as categorias de 0 a 5 para cada item, conforme apresentado anteriormente.

Matriz de relacionamentos

Ameaças	Impacto	Probabilidade
Erros humanos		
Instalação de hardware e software não autorizados		
Códigos maliciosos		
Bugs dos sistemas operacionais		
Invasão		
Desastres naturais		
Desastres causados por pessoas		
Falhas em equipamentos		
Sabotagem		
Grampo telefônico		
Monitoramento de tráfego na rede		
Modificação de informações		
Acesso a arquivos de senhas		
Uso de senhas frágeis		
Usuários internos praticando atos ilegais		

Exercício de fixação 4

Matriz de relacionamento

Preencha a tabela anterior de Ameaças x Impacto x Probabilidade com valores de 0 a 5 de acordo com o ambiente de TI da sua organização.

Cálculo dos riscos

- Riscos são calculados a partir da relação entre impacto e probabilidade de ocorrência.
- Considerando as propostas de classificação anteriores:
  - 0 (valor mínimo), nenhum risco.
  - 25 (valor máximo), risco altíssimo.
- Quanto maior o risco, maior a importância de se aplicar uma medida de segurança específica.

Avaliação de riscos

Modos:

- Qualitativo.
- Quantitativo.

Conhecer os impactos é relevante.

Ao avaliar riscos, procura-se uma base que sirva para efeitos de comparação; por exemplo, análise e avaliação de riscos efetuadas em épocas anteriores. O conhecimento prévio de impactos e probabilidades de riscos é sempre relevante para uma avaliação adequada e completa.

Por outro lado, há basicamente dois modos de realizar a avaliação de riscos:

- **Qualitativo** – a avaliação de riscos através da estimativa qualitativa é aquela que utiliza atributos qualificadores e descritivos para avaliar. Não são atribuídos valores financeiros. É considerada muito subjetiva. Ex: Alto, Média, Baixa, Muito Baixa.
- **Quantitativo** – a avaliação de riscos através da estimativa quantitativa é aquela que utiliza valores numéricos financeiros para cada um dos componentes coletados durante a identificação dos riscos. Ex: probabilidade de 50%; impacto: R$ 100.000,00.

Exemplo 1 – Análise de risco

Numa determinada instituição de ensino foi determinado que a área de TI realizasse um levantamento de riscos da rede administrativa em três departamentos: Engenharia, Financeiro e Administrativo. Para tanto foi utilizado como metodologia o conceito de riscos como resultado da probabilidade vezes o impacto, tendo como parâmetros qualitativos alto, médio e baixo, com pesos atribuídos a cada um para o cálculo do risco. Após realizar a etapa de análise de riscos, você realizou a avaliação dos riscos, chegando ao resultado abaixo:

Tabela 5.3
Resultado da avaliação de riscos.

Área	Probabilidade de ocorrer		Impacto caso ocorra		Risco = P x I	
	Avaliação	Peso	Avaliação	Peso	Peso	Avaliação
Departamento de Engenharia	Média	2	Médio	2	4	Médio
Departamento Administrativo	Média	2	Baixo	1	2	Baixo
Departamento Financeiro	Média	2	Alto	3	6	Alto

Critério de Probabilidade		Peso
Alta	Tem ocorrido com frequência mensal	3
Média	Ocorreu pelo menos uma vez nos últimos seis meses	2
Baixa	Não existe registro/ histórico de ocorrência	1

Tabela 5.4
Critério de probabilidade utilizado.

Critério Impacto		Peso
Alto	Caso ocorra irá causar grandes prejuízos financeiros	3
Médio	Na ocorrência seus prejuízos causarão impacto financeiro de até R$ 10 mil	2
Baixo	Na ocorrência seus prejuízos não causarão impacto financeiro	1

Tabela 5.5
Critério de impacto utilizado.

Risco	
Alto	>4
Médio	>2 e <=4
Baixo	<=2

Figura 5.6
Critério de risco utilizado.

Exemplo 2 – Análise de risco

Numa determinada instituição da área de ensino foi determinada que a área de TI realizasse um levantamento de riscos da rede administrativa em três departamentos: Engenharia, Financeiro e Administrativo. Para tanto foi utilizada uma metodologia desenvolvida por uma consultoria que calcula os riscos da instituição através de uma fórmula que se utiliza de parâmetros como criticidade, disponibilidade, confidencialidade entre outros. Após realizar a etapa de análise de riscos, você realizou a avaliação dos riscos, chegando ao resultado abaixo:

Tabela 5.7
Resultado da avaliação de riscos.

Área	Criticidade da rede	Disponibilidade da rede	Confidencialidade da rede	Importância da rede	EO	ED	RR
Departamento de Engenharia	2	3	1	6	0,1	0,3	3,8
Departamento Administrativo	2	3	2	12	0,5	0,5	3
Departamento Financeiro	2	3	3	18	0,3	0,3	8,8

Valores para Criticidade, Disponibilidade e Confidencialidade	
Qual a criticidade desta rede para o negócio da área? Qual a importância do requisito Disponibilidade ou Confidencialidade para a segurança da rede na área?	
Alta	3
Média	2
Baixa	1

Tabela 5.8
Valores dos critérios para Criticidade, Disponibilidade e Confidencialidade.

Valores de EO e ED	
Muito baixo	0,1
Baixo	0,3
Moderado	0,5
Alto	0,7
Muito Alto	0,9

Tabela 5.9
Valores para evitar a ocorrência e a degradação.

Convenções		
IR	Importância da rede.	Qual a importância da rede para os negócios?
EO	Evitar a ocorrência.	Qual a probabilidade atual de evitar a ocorrência.
ED	Evitar a degradação.	Qual a possibilidade atual de evitar a degradação.
RR	Risco relativo	IR*[(1-EO)*(1-ED)] Cálculo do risco nesta metodologia.

Tabela 5.10
Convenções utilizadas.

Para o exemplo apresentado, o ativo analisado é a rede da organização. Como pode ser visto, algumas convenções foram utilizadas para mapear a importância de serviços específicos de segurança, tais como disponibilidade, integridade e confidencialidade em uma análise, e na outra apenas a probabilidade e o impacto. Ao final, o resultado expresso foi gerado a partir da proposta para a medição de riscos naquela organização.

Determina os critérios para indicar se um risco é aceitável. Aspectos a considerar:

- Requisitos legais e de segurança.
- Objetivos organizacionais.
- Custo x benefício.

Exercício

- Faremos uma análise de risco da rede da FIC para a realidade do curso de Gestão da Informação. Para isso, reflita sobre:
  - Que elementos organizacionais serão analisados;
  - Que critério de avaliação será utilizado;
  - Quais os valores de referência dos critérios;
  - Qual fórmula de cálculo do risco.