Introdução à Segurança da Informação

Gestão de Riscos – Parte I

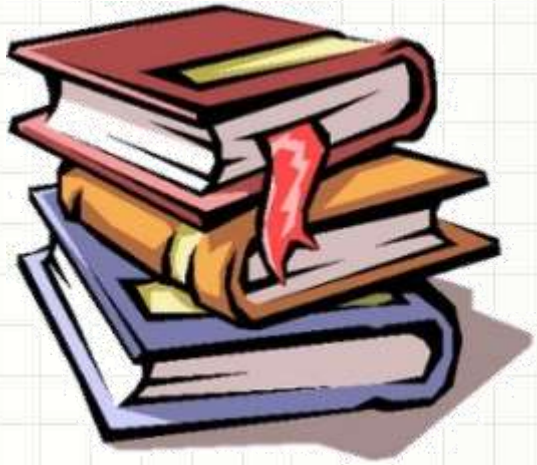
Prof. Dr. Daniel Caetano

2020 - 1

Objetivos

- Compreender os conceitos de risco, ameaça, vulnerabilidade e desastre
- Compreender os aspectos que envolvem riscos e a percepção dos mesmos
- Aplicar a análise e avaliação dos riscos.

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 3)
Material Didático	Gestão de Segurança da Informação, Cap 4.
Leitura Adicional	https://www.esab.edu.br/wp-content/uploads/monografias/nara-suely-oliveira-bandeira.pdf (Monografia)

LEMBRETE: CONSULTAR O "ANTES" DA AULA 4 NO SAVA!

RETOMANDO:

SEGURANÇA FÍSICA X LÓGICA E CICLO DE VIDA DA INFORMÃÇÃO

Aspectos Lógicos x Físicos

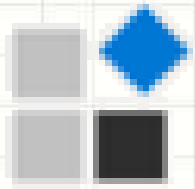
Não existe segurança lógica

sem segurança física

Ciclo de Vida da Informação

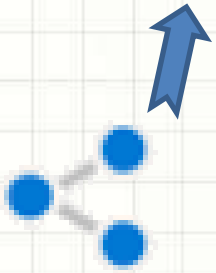
Criar, importar ou modificar dados

Detectar dados



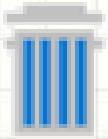
Classificar e Rotular Dados

Proteger os dados com base em Política de Segurança



Enviar, compartilhar e mover dados

Monitorar Dados



Reter, expirar e deletar dados

Risco? Que Risco?

Ameaça, vulnerabilidade e desastre

- Definindo alguns termos...
  - Ameaça
    - Qualquer ocorrência que possa provocar perda

  - Vulnerabilidade
    - Elementos que expõem às ameaças

  - Desastre
    - Impacto de uma força externa que ocasiona perda ou prejuízo; não precisa ser destruidor!

Ameaça, vulnerabilidade e desastre

- Exemplos
  - Ameaças
    - Existência de potenciais invasores com interesse nas informações que mantemos
    - Funcionários insatisfeitos com acesso ao banco de dados
  - Vulnerabilidades
    - Uma versão antiga de *webserver* com falha conhecida
    - Código PHP mal elaborado que permita *injection*
  - Desastres
    - *Furto* das informações confidenciais de nosso banco de dados
    - *Deleção* do banco de dados como um todo

O que é Risco?

- Risco é uma probabilidade de...
  - Ameaças e vulnerabilidades...
  - Levarem a desastres

- Em geral, define-se risco como sendo:

$$risco = ameaças \,.\, vulnerabilidades$$

- Em outras palavras...
  - Se não houver ameaças ou vulnerabilidades...
  - ... Não haverá riscos.

Inevitabilidade dos Riscos

- Riscos são inevitáveis
  - Investidores comprando ações
  - Cirurgiões realizando operações
  - Engenheiros projetando pontes
  - Empresários abrindo negócios
  - Etc...

- Mas gerenciá-los é estratégico:
  - Precisam ser minimizados ou mitigados...
  - Já que não temos como eliminá-los totalmente

A Gestão de Riscos

Gestão de Riscos

- Gestão de Riscos é:
  - Processo para identificar, mensurar e planejar passos para reduzir um determinado risco a níveis aceitáveis pela organização
- Já vimos que a informação é estratégica
  - Fundamental realizar análise de riscos voltada aos ativos de informação
  - Determinar quais riscos podem afetar a entrega de produtos ou serviços
  - É preciso conhecer os requisitos de negócio!

Objetivos da Gestão de Risco

- Fornecer subsídios para:
  - A segurança efetiva dos sistemas de TIC – processamento, armazenagem e transmissão de dados
  - Base sólida para a tomada de decisão – execução de orçamento e investimentos em tecnologias para minimizar riscos
  - Possibilidade de equilíbrio entre custos de proteção e desempenho dos sistemas

Gestão de Riscos (PMBOK)

- Segundo o PMBOK
  - Processos sistemáticos de identificação, análise e avaliação dos riscos e no estabelecimento de respostas adequadas
- Processos envolvidos
  - Planejar o gerenciamento de riscos
  - Identificar os riscos (iterativamente!)
  - Analisar qualitativamente os riscos (probab. x impacto)
  - Análise quantitativamente os riscos
  - Planejar as respostas aos riscos (e responsáveis)
  - Monitorar os riscos (acompanhar e identificar novos)

Análise e Avaliação de Riscos

Avalição de Riscos

- Passos para a avaliação
  - Caracterização do ambiente e sistemas
  - Identificação das ameaças
  - Identificação das vulnerabilidades
  - Análise de controles de segurança
  - Determinação da probabilidade
  - Análise de impacto
  - Determinação do risco
  - Recomendação dos controles
  - Documentação dos resultados.

Caracterização do Ambiente

- Permitir identificar limitações operacionais, computacionais, de informação etc.
- Inventariar
  - Equipamentos
  - Sistemas
  - Informações
  - Serviços (suporte, garantias etc.)
  - Pessoas
- Identificar sua criticidade

Identificação das Ameaças

- Históricos de incidentes de segurança
  - Estatísticas da empresa ou fontes externas
- Tipos de ameaças
  - Naturais (terremoto, enchente, incêndio etc...)
  - Humanas (dolosos, imperitos, imprudentes ou negligentes)
  - Ambientais (falta de energia, poluição etc...)

Identificação de Vulnerabilidades

- Falhas ou fraquezas de segurança
- Listas de verificação
  - Falhas de software e hardware
- Outros métodos
  - Testes e simulações
  - Teste de invasão de sistemas
  - Auditoria de código
  - ...

Análise de Controles

- Avaliar controles existentes
  - Controles para minimizar ou eliminar chance de ameaça
  - Adequados, ineficazes, insuficientes ou injustificáveis
- Informações podem ser obtidas através de:
  - Análise de documentos dos processos de gestão de segurança
  - Averiguação da efetividade dos controles existentes.

Análise de Probabilidades

- Produção de índice indicativo da chance de uma ameaça se tornar um desastre
  - Alta: existe uma ameaça evidente e nenhum controle preventivo efetivo
  - Média: existe uma ameaça evidente, mas há controles efetivos em ação
  - Baixa: a ameaça é desmotivada e há controles efetivos em ação
- Considerar experiências passadas
  - Estatísticas históricas de ocorrências
  - Fatores climáticos e geográficos
  - Situações que poderiam levar a erros humanos

Análise de Impactos

- Determinar impacto e valor do sistema para a organização
- Inicia-se com:
  - Missão do sistema
  - Criticidade do sistema de dados
  - Sensibilidade dos dados do sistema
- Identificar o impacto...
  - Caso a ameaça “tenha sucesso”
  - Integridade, disponibilidade e confidencialidade
- Qualitativa x Quantitativa

Determinação do Risco

- Avaliar:
  - A possibilidade de exploração da vulnerabilidade
  - O impacto ao negócio devido a evento adverso
  - Efetividade de controles para reduzir os riscos.
- Tabela conforme ABNT (notas 0 a 8)

	PROBABILIDADE DO CENÁRIO DE INCIDENTE	MUITO BAIXA (MUITO IMPROVÁVEL)	BAIXA (IMPROVÁVEL)	MÉDIA (POSSÍVEL)	ALTA (PROVÁVEL)	MUITO ALTA (FREQUENTE)
IMPACTO NO NEGÓCIO	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Recomendações de Controle

- Sugerir novos controles para mitigar riscos
- Considerar:
  - Efetividade de opções recomendadas
  - Legislação e regulamentação
  - Política organizacional
  - Impacto operacional
  - Segurança e confiabilidade.

Documentação dos Resultados

- Documentação e armazenamento
  - Estabelecer uma base de conhecimento
  - Apoiar novas políticas e procedimentos

- Não se busca apontar erros
  - Indicar os riscos inerentes
  - Justificar investimentos
  - Reduzir potenciais perdas e danos

QUESTÕES

Questão 1

O Gerenciamento de Riscos é um processo que tem como objetivo dar subsídios à organização realizar sua missão institucional, de forma a: (leia as asserções e assinale a alternativa correta)

I. Possibilitar a segurança efetiva dos sistemas de Tecnologias de Informação e Comunicação.

II. Criar uma base sólida para a tomada de decisões.

III. Permitir aos gestores equilibrarem seus custos de proteção e desempenho dos sistemas de informação.

a) Somente a asserção I está correta.

b) Somente a asserção II está correta.

c) Somente a asserção III está correta.

d) As asserções I e II estão corretas.

e) As asserções I, II e III estão corretas.

Questão 2

Existem alguns passos sequenciais para avaliar os riscos. Sobre estes passos, assinale a alternativa incorreta.

a) Caracterização do ambiente.

b) Identificação de ameaças.

c) Identificação de vulnerabilidades.

d) Implementação de correções.

e) Determinação de probabilidades.

Conclusões

Resumo e Próximos Passos

- Ameaça, vulnerabilidade e riscos
- Gestão de riscos
- Análise e Avaliação de Riscos
  - Várias etapas!

- Tratamento dos riscos
  - Mitigação
  - Aceitação
  - Comunicação
  - Monitoramento

PERGUNTAS?