Introdução à Segurança da Informação

Gestão de Riscos – Parte II

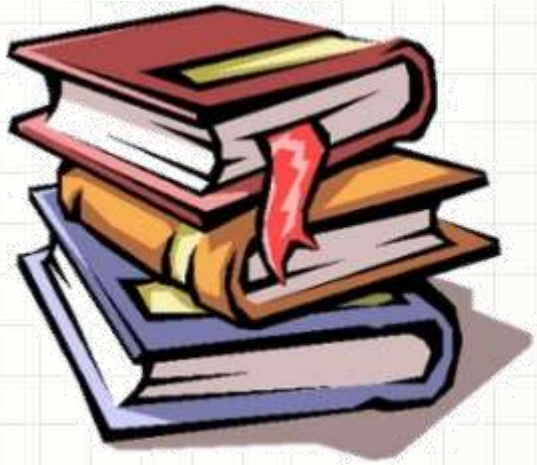
Prof. Dr. Daniel Caetano

2020 - 1

Objetivos

- Compreender como lidar com os riscos e porque e quando aceitá-los
- Perceber a necessidade de monitoramento dos riscos
- Compreender a necessidade de comunicação de riscos

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 4)
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 "DEPOIS" DA AULA 4 NO SAVA!

RETOMANDO:

RISCO E GESTÃO DE 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!

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.

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

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.

Lidando com os Riscos

Abordagens de Segurança

- Há dois tipos principais de abordagem:
  - Reativa
  - Proativa

Abordagem Reativa

- Agir quando ocorre um incidente
  - Sempre que ocorrer um incidente...
  - Verificar e agir para não voltar a acontecer

- Envolve:
  - Auditoria
  - Análise e pesquisa
  - Documentação
  - Implementação de medidas.

Abordagem Proativa

- Agir para que não haja incidentes
  - Prática diária, agir antes de acontecer
  - Para evitar que incidentes venham a acontecer

- Envolve:
  - Pesquisa de falhas
  - Análise de logs
  - Documentação
  - Implementação de medidas

Abordagens de Segurança

- Há dois tipos principais de abordag
  - Reativa
  - Proativa

- Não são excludentes!
- Ambas: mitigação de riscos futuros
  - Proativa é efetiva também para o presente
  - Reativa tende a ser mais cara no longo prazo.

Lidar com os Riscos

- Mitigar?
- É impraticável eliminar os riscos...
  - Priorizar... em função de quê?
  - Custos.
- Nosso objetivo
  - Implementar controles para...
  - Reduzir os riscos a nível **aceitável...**
  - Com mínimo impacto sobre os recursos e metas
- Significa que vamos aceitar riscos?

Aceitação de Riscos

- Há custos para mitigar riscos
- Há custos por eventuais desastres
- E se mitigar for mais caro que o desastre?
  - Podemos aceitar o risco!
- Custo “certo” x custo “duvidoso”
  - Mais fácil aceitar riscos baixos: custo “duvidoso”

	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

Mitigação de Riscos

- Etapas
  - Priorizar
  - Analisar
  - Avaliar
  - Implementar controles.

Isso se aplica inclusive a projetos de software! Prazos, Resultados!

Estratégias de Mitigação de Riscos

Estratégias de Mitigação de Riscos

- Várias estratégias
  - Escolha: metas e missão da organização

- Tipos de Estratégias
  1. Suposição de Riscos
  2. Prevenção de Riscos
  3. Limitação de Riscos
  4. Planejamento de Riscos
  5. Pesquisa e Reconhecimento
  6. Transferência de Risco

1. Suposição de Riscos

- Aceitar um risco potencial
  - Continuar operando o sistema informatizado
  - Implementar controles para diminuir o risco
    - Controlar para ficar dentro do limite
- Exemplo
  - Parar por falta de energia
    - Se gerador fora de questão, reduzir equipamentos de maneira que nobreak dê conta
  - Parar por superaquecimento
    - Sem ar-condicionado? Buscar equipamentos menos potentes.

2. Prevenção de Riscos

- Tentativa de eliminar um determinado risco
  - Eliminar sua causa
  - Eliminar sua consequência
    - Avisos prévios, sistemas alternativos
- Exemplo
  - Parar por falta de energia
    - Gerador; na falta de gerador, metodologia alternativa de trabalho.
  - Parar por superaquecimento
    - Ar condicionado. Na falta, medir temperatura e desligar equipamentos se necessário.

3. Limitação de Riscos

- Limitar o risco implementando controles
  - Delimitar o “tamanho do estrago”

- Exemplo
  - Perda de dados
    - Backup periódico; pelo menos dos dados mais relevantes para a operação.
  - Incêndio
    - Sistema de reação (sprinklers, eliminação de oxigênio)
    - Sistema de delimitação (portas corta-fogo)

4. Planejamento de Risco

- Implementar processos para
  - Priorizar
  - Implementar controles
  - Manter controles
- Exemplo
  - Perda de Dados
    - Plano de recuperação de dados
    - Plano de uso de espaço disponível para backup
  - Incêndio
    - Plano de evacuação
    - Plano de combate a incêndios

5. Pesquisa e Reconhecimento

- Pesquisar sobre vulnerabilidades
  - Reconhecer a vulnerabilidade
  - Agir para corrigir a vulnerabilidade
- Exemplo
  - Invasão de equipamento computador
    - Manter softwares atualizados
    - Liberar acessos apenas pela rede interna
  - Roubo de senha por engenharia social
    - Orientar funcionários
    - Implementar mudança segura e frequente de senhas

6. Transferência de Risco

- Instrumentos Compensatórios
  - Transferir a correção para terceiros
  - Serviços ou valores
- Exemplo
  - Incêndio
    - Seguro dos equipamentos
  - Queima de equipamentos
    - Contratação de garantia com SLA adequado
    - (Service Level Agreement)

Monitoramento e Comunicação de Riscos

Evolução dos Riscos

- Os riscos não são estáticos!
  - Equipamentos envelhecem...
    - Alguns riscos aumentam!
  - Tecnologias mudam
    - Falhas são descobertas!
  - Novos hardwares, softwares, reorganizações etc.

- Monitoramento de Riscos
  - Reavaliação periódica dos riscos

Monitoramento de Riscos

- Manter atualizadas as listas de
  - Ativos
  - Vulnerabilidades
  - Controles
  - Planejamento do gerenciamento de riscos
  - Plano de Contingências
- Reavaliar critérios de risco!
- Reavaliar a priorização!

Comunicação de Riscos

- Como ter sucesso na mitigação de riscos?
  - Engajamento dos *stakeholders*
- Comunicação é essencial
  - Informes e treinamentos
  - Conhecimento das ameaças e riscos associados.

Comunicação aos Gestores

- Diretoria da empresa
  - **Relatórios e informes**
  - Liberação de verbas necessárias
  - Apoio para treinamento
  - Conhecimento dos riscos técnicos do negócio

Comunicação aos Colaboradores

- Colaboradores em geral
  - **Informes e treinamentos**
  - Compreensão em reduções de “praticidade”
  - Atenção especial a procedimentos de segurança

Comunicação à Equipe

- Colaboradores da equipe de segurança
  - **Procedimentos e treinamentos**
  - Implementação adequada das políticas
  - Evitar reprodução de erros passados
  - Reavaliação das estratégias de segurança

Sucesso na Gestão de Riscos

- Planejamento de ações e metas e...
  - Total apoio e patrocínio da alta gestão
  - Envolvimento, participação ativa e maturidade dos *stakeholders*
  - Comunicação ativa e assertiva
  - Alinhamento/gestão de conflitos nas equipes
  - Visão sistêmica da gestão de riscos (interações!)
  - Liderança e liberdade de ação da equipe de gestão de riscos.

QUESTÕES

Questão 1

- Ao chegar na empresa você descobre que a homepage da mesma está indevidamente modificada (com mensagens de ódio). Você age para contornar a situação colocando uma mensagem de “manutenção”.

a) Qual tipo de abordagem é essa?

b) Após o relatado, qual a primeira atitude?

c) Que tipo de comunicação você faria?

Questão 2

- Existem arquivos fundamentais à operação da empresa que estão armazenados em um único servidor. A perda desses dados pode ser catastrófica, então você resolve tomar uma atitude para preservá-los.

a) Qual tipo de abordagem é essa?

b) Há solução para esse problema?

c) Que tipo de comunicação você faria?

Conclusões

Resumo e Próximos Passos

- Como lidar com riscos
  - Mitigá-los até o nível aceitável
- Monitorar riscos
  - Eles são mutáveis!
- Comunicação: fundamental para o sucesso

- Ameaças e Vulnerabilidades
  - Quais são as principais?
  - Como funcionam e como reconhecê-las?
  - Como agir a respeito?

PERGUNTAS?