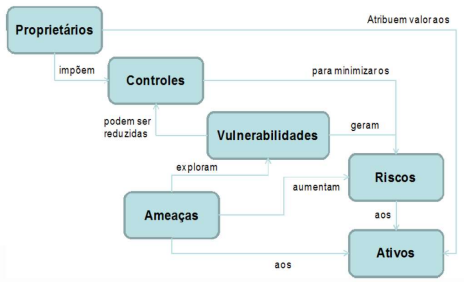
Análise de Risco

Prof. Edson Pedro Ferlin

- Objetivos
  - Apresentar as técnicas para a Análise de Risco.
- Conteúdos
  - Técnicas para avaliação do risco numa organização e os custos e benefícios associados a essa aferição
  - Identificação e descrição de métodos para determinar níveis de relevância em sistemas e processos e aproximações para desenvolver estratégias de recuperação
  - A metodologia de análise e avaliação de risco FRAAP, desenvolvida por Thomas R. Peltier

GESTÃO DE RISCO DE SEGURANÇA

É um processo sistemático da gestão organizacional que determina a aplicação equilibrada de controles de segurança nessa organização, diante do seu perfil de riscos de segurança.



Análise de Risco

A gestão dos riscos é um dos aspectos chave da norma ISO/IEC 27001, uma avaliação dos riscos é uma das exigências desta norma.

Como resultado da análise de risco, deve ser feita uma lista dos riscos identificados, classificados em ordem de gravidade para posteriormente serem tomadas medidas.

Objetivo

A análise de risco deve ser feita tendo em conta uma análise de custo-benefício, para revelar se compensa um risco ser minimizado ou transferido.

Processo de Análise de Risco

É a composição dos processos de Identificação do Risco e de Estimativa do Risco.

A identificação do risco é o processo de encontrar, listar e caracterizar os elementos ou fatores do risco.

O propósito da Estimativa do Risco é priorizar os riscos contra critérios de avaliação (estabelecidos na Definição do Contexto) e objetivos relevantes para a organização.

Estimativa do Risco

É a última etapa da fase de análise do risco, e seu objetivo é atribuir valores para as probabilidades e consequências de cada risco, usando escalas qualitativas e/ou quantitativas.

FRAAP - Facilitated Risk Analysis and Assessment Process

(**Processo Facilitado da Análise e Avaliação de Risco**)

É um processo eficiente e organizado para assegurar que as informações relacionadas à segurança dos riscos nas operações dos negócios sejam detectadas e documentadas, envolvendo a análise do sistema de acordo com a estrutura ou o segmento de atuação de cada organização.

Desenvolvido por Thomas R. Peltier

Classificação das Ameaças

(**Definições de Probabilidades no FRAAP**)

Termo	Definição
Probabilidade	Chance de que um evento irá ocorrer ou que um valor de perda específica pode ser atingido se o evento ocorrer.
Alta	Muito provável que a ameaça ocorra no próximo ano (acima de 50%).
Média	Possível que a ameaça ocorra no próximo ano (acima de 30% até 50%)
Baixa	Altamente improvável que a ameaça ocorra no próximo ano (até 30%)

Classificação das Ameaças

(**Definições para Impacto no FRAAP**)

Termo	Definição
Impacto	Uma medida da magnitude da perda ou dano no valor de um ativo da informação
Alta	Missão inteira ou negócio impactado
Média	Perda limitada à única unidade de negócio ou objetivo
Baixa	Negócio como de costume

Nível de Risco

(**Matriz de Nível de Risco no FRAAP**)

PROBABILIDADE	IMPACTO		
	Alto	Medio	Baixo
Alto	A (6)	B (5)	C (4)
Médio	B (5)	B (4)	C (3)
Baixo	C (4)	C (3)	D (2)

A - Ação corretiva tem de ser implementada;
B - Ação corretiva deve ser implementada;
C – Requer monitoramento;
D - Nenhuma ação necessária no momento.

Exemplo de Análise de Risco

Grupo de ameaças	Perguntas correspondentes	Aplicação Sim/Não	Probabilidade 1 = Baixa 2 = Média 3 = Alta	Impacto 1 = Baixo 2 = Médio 3 = Alto	Nível de risco 6 -5 (Alto) 4 (Médio) 3-2 (Baixo)
7. Vírus de computador	Qual a frequência de atualização do seu antivírus?	Sim	1	2	3 (Baixo)
	O antivírus tem algum custo financeiro?	Sim	3	2	5 (Alto)
	Certifica-se de que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação?	Sim	1	2	3 (Baixo)
8. Estações de trabalho deixadas sem vigilância	Os papéis de trabalho frequentemente são deixados à vista na mesa de trabalho?	Sim	3	2	5 (Alto)
	É costume, no ambiente de trabalho, deixar o computador ligado com as janelas abertas?	Sim	1	2	3 (Baixo)
	Os equipamentos do setor são suficientes para executar seu trabalho no SCDP?	Sim	2	2	4 (Médio)
9. Treinamento de funcionários	Recebeu orientação sobre a manutenção sigilosa de sua senha de acesso e a responsabilidade envolvida pelo mau uso dela?	Sim	2	2	4 (Médio)
	A alta administração está ciente de que a instituição precisa de um programa eficaz de segurança da informação?	Sim	2	2	4 (Médio)

Contato

eferlin@live.com

(BLOG) professorferlin.blogspot.com

(SITE) professorferlin.com.br

(YOUTUBE) ProfEdsonPedroFerlin