Ameaças e Riscos

Gerenciamento de Riscos

- Processo que transformação
  - De uma ameaça em risco
- Medidas de segurança
- Processo contínuo
  - Identificados
  - Examinados
  - Reduzidos a um nível aceitável

Análise de Riscos

- Serve para:
  - Como ferramenta para Gestão de Riscos
  - Determinar se as ameaças são relevantes
  - Identificar riscos associados
  - Garantir que as medidas de segurança sejam implantadas
  - Evita gastos desnecessários em medidas de segurança
  - Ajuda a conhecer os conceitos de segurança
  - Avaliar corretamente os riscos
- Objetivos
  - Identificar os bens e os seus valores
  - Determinar as vulnerabilidades e ameaças
  - Determinar quais as ameaças se tornarão um risco
  - Determinar um equilíbrio entre os custos
- Tipo
  - Quantitativo
    - Baseado no impacto
    - Baseado na perda financeira
    - Baseado na probabilidade da ameaça tornar-se um incidente
  - Qualitativo
    - Baseado nos cenários
    - Baseado nas situações
    - Baseado nos sentimentos
- Medidas de Redução de Riscos
  - Objetivo
    - Reduzir a chance do evento ocorrer
    - Minimizar as consequências
  - Tipos
    - Detecção
    - Repressão
    - Correção
    - Seguros
    - Aceitação
- Tipos de Ameaças
  - Humanas
  - Não Humanas
- Tipos de Danos
  - Danos diretos
  - Danos indiretos
  - Expectativa de Perda Anual (ALE – Annual Loss Expectancy)
  - Expectativa de Perda Única (SLE – Single Loss Expectancy)
- Tipos de Estratégia de Risco
  - Carregar o Risco (Aceitar)
  - Neutralizar o Risco
  - Evitar o Risco
- Diretrizes para implementar medidas de segurança
  - ISO/IEC 27001:2013 especifica os requisitos para
    - Estabelecer
    - Implementar
    - Operar
    - Monitorar
    - Rever
    - Manter
    - Melhorar
  - ISO/IEC 27002:2013 lidam com um padrão de aspectos
    - Organizacionais
    - Processuais
    - Físicas
    - Lógicas