Medidas Organizacionais

- Gerenciamento de Continuidade de Negócio
  - Continuidade
  - Desastres
  - DRP
  - Locais Alternativos
    - Local Alternativo
    - Site Redundante
    - Hot site sobre demanda
  - Testando o BCP
  - Medidas Pessoais
- Segurança dos Recursos Humanos
  - Antes da admissão
  - Gerente é o responsável pela correta descrição das atribuições
  - Durante o emprego assegurar que cumpram com as responsabilidades
  - Pessoal
    - Acordo de Não Divulgação
    - Contratantes
    - Arquivos Pessoais
    - Conscientização da Segurança
    - Acesso
- Política de Segurança
  - Hierarquia
    - Regulamento
    - Procedimentos
    - Orientações
    - Normas
  - Avaliando a Política com o ciclo PDCA
    - Plan ou Planejar (Desenho do ISMS)
    - Do ou Fazer (Implementar o ISMS)
    - Check ou Verificar (Monitorar e Verificar o ISMS)
    - Act ou Ajuste (Manter e Ajustar o ISMS)
  - Configurando um ISMS
    - Definir um framework
    - Compreende pelo menos 11 domínios da ISO/IEC 27002:2013
  - Os 18 domínios do ISO/IEC 27002:2013
    - 0 – Introdução sobre Norma
    - 1 – Escopo do conteúdo da Norma
    - 2 – Referências Normativas
    - 3 – Termos e Definições sobre Segurança da Informação
    - 4 – Estrutura da Norma
    - 5 - Políticas de Segurança da Informação
    - 6 – Segurança da Informação Organizacional
    - 7 – Segurança de Recursos Humanos, inclusa recentemente na edição 2013
    - 8 – Gerenciamento de Ativos
    - 9 – Controle de Acesso
    - 10 - Criptografia
    - 11 – Segurança Ambiental e Física
    - 12 – Segurança Operacional
    - 13 – Segurança da Comunicação
    - 14 – Manutenção, Desenvolvimento e Aquisição de Sistemas
    - 15 – Relacionamento com Fornecedores
    - 16 – Gerenciamento de Incidentes de Segurança da Informação
    - 17 – Aspectos de Segurança da Informação do Gerenciamento de Continuidade de Negócio
    - 18- Conformidade
  - Acompanhamento
    - Periódico
    - Permissão do conselho para modificação
  - A Organização para empresas:
    - Pequenas
    - Médias
    - Grandes
- Gerenciando a Comunicação e os Processos Operacionais
  - Gestão de Mudanças
  - Segregação de Funções
  - Criação de ambientes
    - Desenvolvimento
    - Teste
    - Homologação
    - Produção
  - Gestão de Serviços de Terceiros
  - Proteção
    - Malware
      - Phishing
      - Spam
    - Definição
      - Vírus
        - Exemplos
          - Brain
          - Chernobyl
        - Medidas
          - Scanner de vírus no servidor de correio e PCs
          - Tema vírus incluso em uma campanha
          - Tema faz parte da política de SI
          - Formas de notificação de incidentes
          - Procedimento de acompanhamento.
      - Worm
        - Exemplos
          - Melissa
          - I Love You
          - Happy99
          - Blaster
          - Storm Worm
        - Medidas
          - Scanner no servidor de correio e PCs
          - Ferramenta de monitoramento de rede.
          - Incluso em uma campanha de sensibilização
          - Tema faz parte da política de SI
          - Notificação de incidentes
          - Procedimento de acompanhamento
      - Trojan
        - Exemplos
          - BackOrifice
          - Netbus
        - Medidas
          - Scanner no servidor de correio e PCs
          - Ferramenta de monitoramento de rede.
          - Incluso em uma campanha de sensibilização
          - Tema faz parte da política de SI
          - Notificação de incidentes
          - Procedimento de acompanhamento
          - Firewall pessoal
      - Hoax
        - Exemplos
          - Good times
          - Pen Pal
        - Medidas
          - Scanner no servidor de correio e PCs
          - Incluso em uma campanha de sensibilização
          - Tema faz parte da política de SI
          - Notificação de incidentes
      - LogicBomb
      - Spyware
        - Medidas
          - Garantir a atualização constante dos softwares
          - Scanners que fazem a varredura do registro do Windows
          - Firewall pessoal
          - Incluso na campanha de sensibilização
          - Tema faz parte da política de SI
          - Notificação de incidentes
          - Procedimento de acompanhamento
      - Botnets / StormWorm
        - Medidas
          - Garantir a atualização constante dos softwares
          - Scanners que fazem a varredura do registro do Windows
          - Firewall pessoal
          - Incluso na campanha de sensibilização
          - Tema faz parte da política de SI
          - Notificação de incidentes
          - Procedimento de acompanhamento
          - Ferramentas de Monitoramento
      - Rootkit
        - Medidas
          - Garantir a atualização constante dos softwares
          - Scanners que fazem a varredura do registro do Windows
          - Firewall pessoal
          - Incluso na campanha de sensibilização
          - Tema faz parte da política de SI
          - Notificação de incidentes
          - Procedimento de acompanhamento
          - Ferramentas de detecção de Rootkits escondidos
  - Backup e Restore
  - Gerenciamento de Segurança de Rede
    - Intranet
    - Extranet
    - VPN
  - Manuseio de Mídia
    - Publicação não autorizada
    - Alteração
    - Deleção ou destruição
    - Interrupção das atividades empresariais
  - Equipamento Móvel
    - Procedimentos para a manipulação de informações
  - Troca de Informação
    - Mensagens Eletrônicas
    - Sistemas de informações empresariais
  - Serviços para e-commerce
  - Informações publicamente disponíveis