Slides 01

- **Planeamento**
  - Desenho de uma solução que responda aos requisitos, num contexto normativo
    - Sem falhas
    - Todos os estados de funcionamento são previstos
    - Não existem estados que fujam à lógica pretendida
- **Desenvolvimento**
  - Implementação de uma solução que responda ao design, sem outros modos de funcionamento
    - Sem erros que comprometam a execução correta
  - Desenvolvimento de software envolve testes de forma a se obter uma solução que faça o pretendido e apensa o pretendido
- **Execução**
  - Execução do código tal como foi escrito e com todos os processos previstos
  - Ambiente controlado, não manipulável, não observável
  - Sem a existência de comportamentos anómalos, introduzidos pelo ambiente onde executa

---

- **Pessoas e parceiros**
  - Comportamentos dos sujeitos não possui um impacto negativo na solução
    - Existem normas que definem qual o comportamento correto
    - Possuem comportamentos para distinguir quais os comportamentos corretos e incorretos
    - Possuem os incentivos para manter o comportamento
    - Quando comprometidos ou desviantes, as ações têm um impacto limitado
- **Análise e auditoria**
  - Identificar aspetos desviantes
    - Falhas, erros, comportamentos
  - Identificar o risco de a solução ser desviada
    - Exposição a possíveis atacantes
    - Incentivos para que seja desviada
    - Potenciais atores
  - Identificar o impacto dos desvios
    - Perda total dos dados?
    - Disrupção?
    - Custo de Operação?

- **Facetas**
- Facetas da segurança são interligadas e indissociáveis

    - **Defensiva**: foca-se na manutenção da previsibilidade
    - **Ofensiva**: foca-se na violação da previsibilidade
        - Pode ter intuito malicioso/criminoso
        - Pode ter intuito de validação da solução
    - Outras:
        - **Engenharia reversa**: recuperação de design a partir do produto
        - **Forense:** identificar ações passadas e recuperar informação
        - **Recuperação de desastres:** minimizar impacto
        - **Auditoria:** validar o cumprimento com certas premissas
- **CIA**
    - **Confidencialidade**: Informação só pode ser acedida por um grupo restrito de sujeitos
        - Cifrar informação
        - Usar senhas de acesso (fortes)
        - Sistemas de Identificação e Autenticação
        - Firewalls, Grupos de segurança
        - Portas, Paredes robustas
        - Pessoal de Segurança
        - Formação das pessoas
    - **Integridade**: Informação mantém-se inalterada
        - Controlos de integridade (sínteses)
        - Backups
        - Controlos de Acesso
        - Dispositivos de armazenamentos robustos
        - Processos de verificação de informação
    - **Disponibilidade**: Informação mantém-se disponível
        - Backups
        - Planos de recuperação de desastres
        - Redundância
        - Virtualização
        - Monitorização
- **Privacidade**: como é tratada a informação pessoal
    - Recolha
    - Processamento
    - Armazenamento
    - Partilha de informação
    - Eliminação
        - Controlos de acesso
        - Transparência dos processos
        - Cifras
        - Controlos de integridade e de autenticidade
        - Registos
- **Objetivos da Segurança**
    - **Defesa contra catástrofes**
        - Fenómenos naturais

        - Temperatura anormal, relâmpagos, picos de energia, inundações, radiação, etc.
    - **Degradação dos sistemas informáticos físicos**
        - Setores degradados
        - Falha da fonte de alimentação
        - Erros em células da RAM ou SSD
        - Etc.
    - **Defesa contra falhas e erros comuns**
        - Falhas de energia
        - Falhas internas aos sistemas operativos
            - Blue Screen
        - Erros no software / Erros nas comunicações
    - **Defesa contra as atividades não autorizadas (adversários)**
        - Iniciados por alguém "de dentro", ou "de fora"
    - **Tipos de atividades não autorizadas**
        - Acesso a informação
        - Alteração de informação
        - Utilização de recursos
            - CPU, memória, rede, etc
        - Negação de serviço (DoS)
        - Vandalismo
            - Interferência do funcionamento normal, sem benefício direto para o atacante

---

- **Domínios de Segurança**
    - Domínios podem ser organizados de forma plana ou hierárquica
    - Interações entre domínios são normalmente controladas
- **Políticas de Segurança**
    - Conjunto de orientações relativas à segurança que regem um domínio
    - Exemplos:
        - Só é possível aceder a serviços web
        - Pessoas têm de se identificar para entrar
    - Definem o poder de cada sujeito
        - Princípio do privilégio mínimo: cada sujeito só tem acesso ao essencial para as suas funções
    - Definem procedimentos de segurança
    - Definem requisitos mínimos de segurança dos sistemas
        - Níveis de segurança
        - Grupos de segurança
        - Autorizações e autenticação correspondentes
    - Definem estratégias de defesa e de resposta
    - Definem o que é legal / ilegal
        - Modelo baseado numa lista de negações
            - Proíbem-se algumas coisas

        - O resto é permitido
    - Modelo baseado numa lista de permissões
        - Proíbe-se tudo
        - Algumas coisas são permitidas
- **Mecanismos de Segurança**
    - Mecanismos implementam as políticas no domínio
    - Exemplos:
        - Autenticação
        - Cifras
        - Filtragem
        - Auditorias
- **Exemplo**
    - **Política:** Sistemas devem ser resilientes
    - **Mecanismos**: Equipamentos/ ligações duplicadas, arquitetura

---

- **Controlos de segurança**
    - Controlos são todos e quaisquer aspetos que permitam evitar, detetar, neutralizar ou minimizar o risco
    - Controlos incluem políticas e mecanismos, mas também normas e leis e processos
- **Tipos de controlos**
    - Físicos
    - Técnicos
    - Administrativos

- **Prevenção realista**
    - Assumir que não existe segurança perfeita
    - Focar nos eventos mais prováveis
    - Considerar custo e receitas
    - Considerar todos os domínios e entidades
    - Considerar impacto
        - À luz da CIA
    - Considerar custo e tempo de recuperação
    - Caracterizar os atacantes
    - Assumir que o sistema vai ser comprometido
        - Ter planos de recuperação

- **Computadores conseguem fazer muitos estragos num curto espaço tempo**
- **O número de vulnerabilidades aumenta sempre**
- **Redes permitem novos mecanismos de atacante**

- **Atacantes podem construir cadeias de ataque complexas**

- **Utilizadores não possuem noção do risco**
- **Utilizadores são desleixados**
    - Tomam riscos
    - Não querem saber
    - Não estimam o risco de forma adequada

- **Principais fontes de vulnerabilidades**
    - Aplicações hostis ou erros em aplicações
    - Utilizadores
        - Ignorantes
        - Falsa noção de segurança
        - Hostis
    - Administração deficiente
        - A configuração por omissão raramente é a mais segura
        - Restrições de Segurança vs Operações Flexíveis
        - Exceções a indivíduos
    - Comunicações sobre ligações não controladas/conhecidas

- **Políticas de Segurança em sistemas distribuídos**
    - Domínios de segurança
    - Gateways de segurança
    - Conjunto de controlos para validação
- **Defesa em Perímetro**
    - Proteção contra atacantes externos
    - Assume que os utilizadores internos são confiáveis e partilham políticas
    - Utilização doméstica ou em pequenas organizações
    - Limitações:
        - Não protege contra atacantes internos
- **Defesa em profundidade**
    - Proteção contra atacantes externos e internos
    - Assume domínios bem definidos sobre todos os aspetos
    - Limitações:
        - Necessária uma coordenação entre controlos
        - Custo
        - Necessidade de treino, alteração de processos e auditorias

- **Sistemas Operativos Confiáveis**
  - Níveis de segurança, certificação
  - Ambientes de execução segura
  - Máquinas virtuais
- **Firewalls e Sistemas de segurança**
  - Controlo de tráfego entre redes
  - Monitorização
- **Comunicações seguras / VPNs**
  - Canais seguros sobre redes públicas / inseguras
  - Extensão segura das redes da organização
- **Autenticação**
- **Entidades de certificação / PKI**
  - Gestão de chaves públicas e certificados
- **Cifra de ficheiros e dados em sessões**
  - Privacidade/ confidencialidade de dados transmitidos e armazenados
- **Deteção de intrusões**
- **Inventariação de vulnerabilidades**
- **Testes de Penetração**
- **Monitorização de conteúdos**
- **Administração da segurança**
  - Desenvolvimento de políticas de segurança
  - Aplicação das políticas de forma distribuída
  - Co-administração (equipas externas)
- **Resposta a Incidentes / Seguimento em tempo real**

- **Zero Trust**
  - **Modelo de defesa sem perímetros**
    - Não existe confiança intrínseca por entidades serem internas
  - **Modelo recomendado para novos sistemas**
    - Antigos sistemas deverão migrar
    - Sistemas legados requerem instalação de novos níveis de segurança
- **Zero Trust - Princípios**
  - Conhecer a arquitetura
  - Conhecer entidades
  - Validar comportamentos e saúde de dispositivos e serviços
  - Usar políticas para autorizar pedidos
  - Autenticar e autorizar as intenções
  - Monitorizar utilizadores, dispositivos e serviços
  - Não confiar em nenhuma rede, nem mesmo a própria
  - Usar serviçoes desenvolvidos para Zero Trust

- **Cibersegurança é limitada por aspetos económicos, operacionais e logísticos**
- **Cibersegurança resume-se a construir e aplicar uma estratégia, co um orçamento e num contexto operacional legal**