Segurança da Informação

Competências:

- Implementar práticas e condutas de segurança da informação no ambiente de TI.

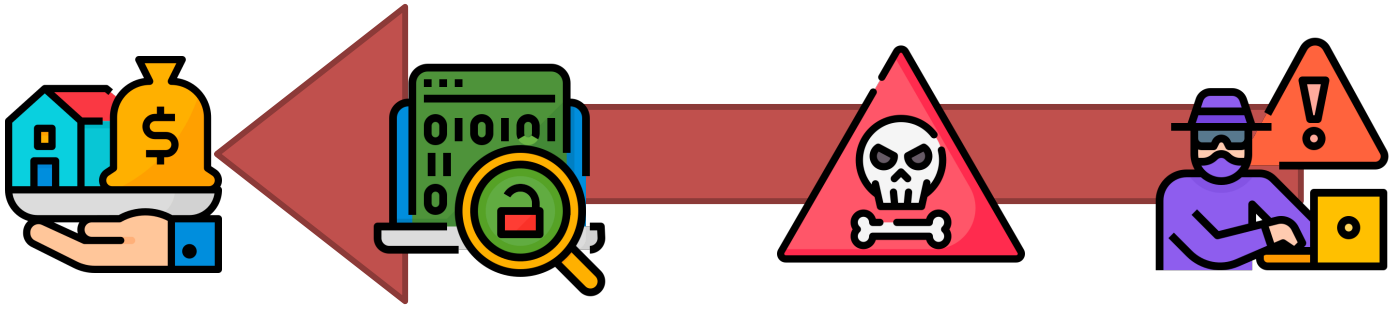
Bases Tecnológicas, científicas e instrumentais (conteúdos):

- Papéis e responsabilidades na proteção da informação;

Situação de Aprendizagem:

- Definição de Segurança.

Segurança da informação



Ativo Vulnerabilidade Ameaça Ataque

Ataques

- Duas classes: passivos e ativos
- Passivos:
  - Interceptação
    - Descoberta de conteúdo
    - Análise de tráfego
- Ativos:
  - Interrupção
  - Modificação
  - Fabricação
  - Repetição

Proteções

- São as medidas que visam livrar os ativos de situações que possam trazer prejuízo
  - Ou seja, são as medidas que são adotadas para fornecer segurança aos ativos

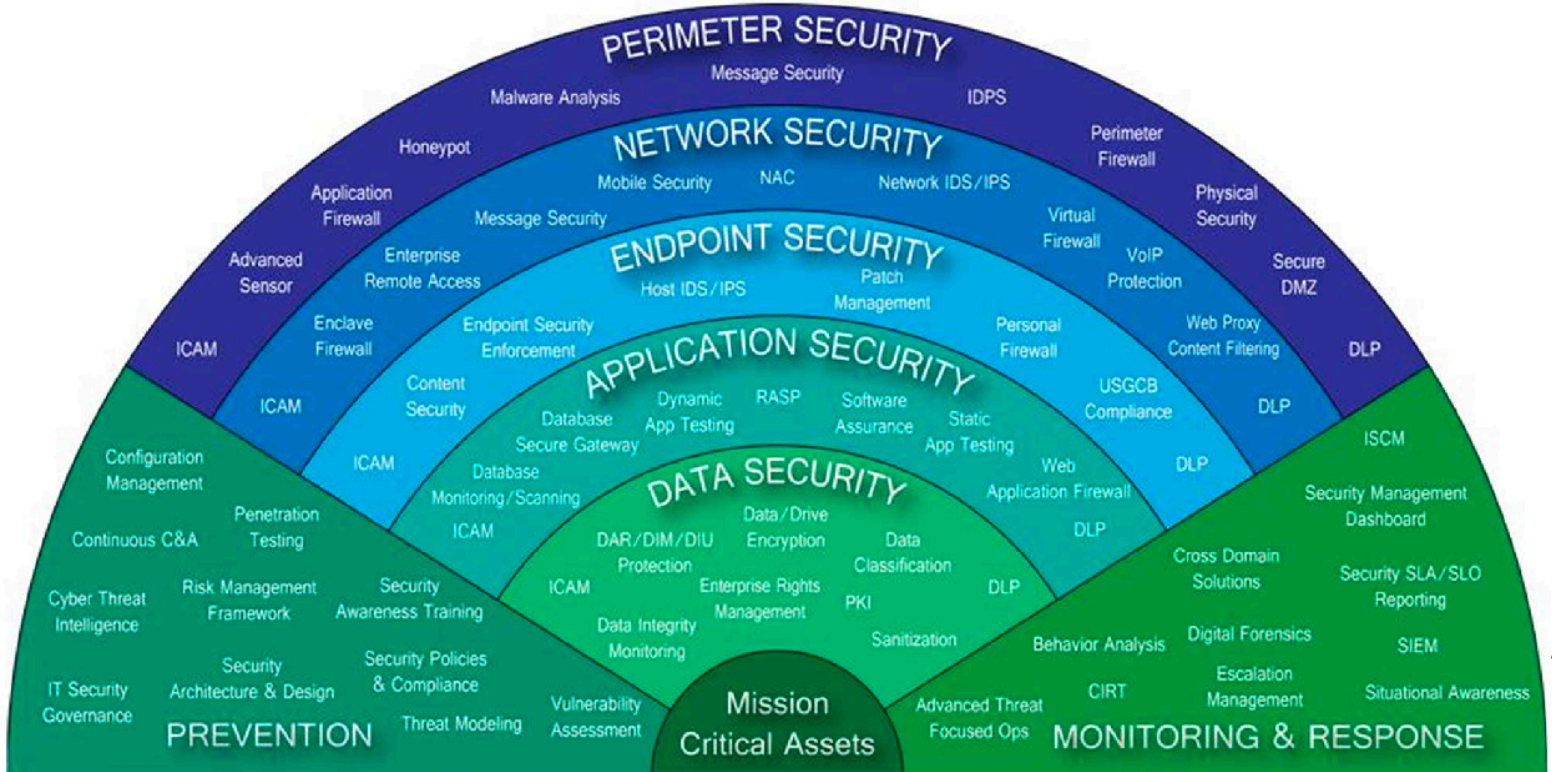
Classificação das proteções

- Lógica
  - Permissões em sistemas de arquivos
  - Firewalls
  - Perfis de usuários em aplicações
- Física
  - Portas
  - Fechaduras
  - Guardas
- Administrativa
  - Políticas
  - Normas
  - Procedimentos

Tipos de proteções

» Uma implementação eficaz de segurança se baseia na utilização de diferentes tipos de proteções

– As proteções complementam-se, sobrepondo-se e fornecendo redundância caso alguma delas falhe.



Tipos de proteções

- Preventiva
  - Impedir ou dificultar uma violação de segurança em potencial com a implantação de uma contramedida
    - Evita que incidentes ocorram
- Desencorajadora
  - Reduzir a ameaça, desencorajando a ação pelo medo ou pela dúvida
    - Desencoraja a prática de ações
- Limitadora
  - Reduzir o risco reduzindo o valor das perdas potenciais ou reduzindo a probabilidade de ocorrer a perda
    - Diminui os danos causados

Tipos de proteções

- Monitoradora
  - Monitora o estado e o funcionamento
- Detectora
  - Determinar que uma violação de segurança é iminente, está em andamento, ou que ocorreu recentemente, e assim tornar possível tomar alguma ação para reduzir a perda em potencial
    - Detecta a ocorrência de incidentes
- Reativa
  - Reage a determinados incidentes

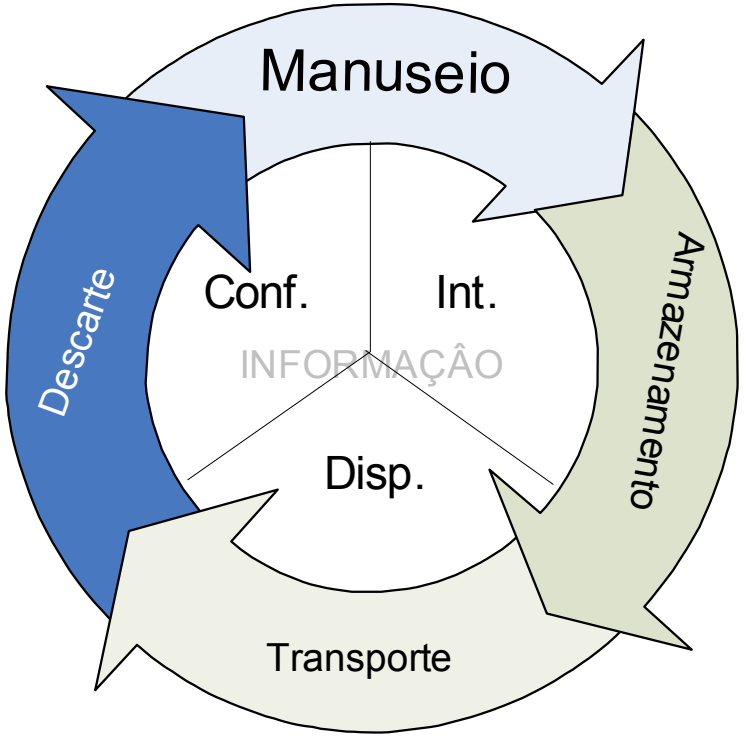
Tipos de proteções

- Corretiva
  - Alterar a arquitetura de segurança utilizada com o objetivo de eliminar ou reduzir o risco de recorrência de uma violação de segurança ou ameaça(s), tais como, eliminando a(s) vulnerabilidade(s).
    - Repara falhas existentes
- Recuperadora
  - Restaurar a um estado normal de operação do sistema, compensando uma violação de segurança, possivelmente através da eliminação ou reparação de seus efeitos.
    - Plano de contingência
    - Repara danos causados por incidentes

Segurança da Informação

SEGURANÇA DA INFORMAÇÃO

CONFIDENCIALIDADE | INTEGRIDADE | DISPONIBILIDADE



Segurança da Informação

Segurança da Informação protege a Informação de um grande número de ameaças, de forma a garantir a continuidade do negócio, minimizar os danos e maximizar o retorno do investimento e as oportunidades de negócio.

Classificação dos ativos

- Ativos podem ser:
  - Tangíveis
    - Informações impressas ou digitais
    - Impressoras
    - Móveis de escritório
  - Intangíveis
    - Imagem de uma empresa
    - Confiabilidade de um órgão
    - Marca de um produto

Propriedades da segurança da Informação

"Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas."

ISO/IEC ABNT NBR 27002:2005.

Definições e Termos

CONFIDENCIALIDADE:

Propriedade de que a informação não esteja disponível para pessoas, entidades ou processos não autorizados.

- Uso de criptografia e senhas são exemplos de recursos que visam à confidencialidade. Em geral são recursos que escondem ou encobrem os usuários.

INTEGRIDADE:

Propriedade de proteger a exatidão e a completeza de ativos.

• Recursos que permitem que se saiba se a informação foi, ou não, alterada, como o ***Hash***, são necessários para que se ofereça essa garantia.

Definições e Termos

DISPONIBILIDADE:

Propriedade de tornar acessível e utilizável sob demanda, por fontes autorizadas.

- Recursos como ***geradores de energia***, ***computadores de "reserva"*** são importantes para esse objetivo.

Ameaças à confidencialidade

- Exemplos de problemas são:

  - Acesso não autorizado;
  - Vulnerabilidades do ***login/password*** (p.ex. partilha de ***passwords***);
  - Intercepção não autorizada da informação em trânsito (p.ex. ***sniffing***);
  - Gestão não controlada da informação.

Ameaças à integridade

- Exemplos de problemas são:

  - Erros no software;
  - Mau funcionamento de equipamento;
  - Erros operacionais (e.g. na introdução de dados);
  - Vírus que corrompem a informação.

Ameaças à disponibilidade

» Exemplos de problemas são:

- Falhas nos equipamentos ou serviços de rede (p.ex. ao nível do hardware/software, falhas de energia, erros/bugs);
- Erros no manuseamento do sistema;
- Causas naturais (incêndios, inundações);
- Recursos insuficientes para o correto funcionamento do software;
- Quando ocorrem ataques propositados para impedir o funcionamento normal do sistema (p.ex. DOS-Denial of Service attacks, SPAM).

5 pilares da Segurança da Informação

- Frequentemente a literatura faz referência aos ***cinco pilares*** da segurança da informação

- Além da tríade CID, ainda inclui a ***Autenticidade*** e o ***Não repúdio***.

Autenticidade:

Propriedade de assegurar as veracidades do emissor e do receptor de informações trocadas.

- Recursos como ***senhas***, ***biometria***, ***assinatura digital*** e ***certificação digital*** são usados para esse fim.

Não repúdio

Não repúdio (Irretratabilidade):

Garantia de que o autor de uma informação não poderá negar falsamente a autoria de tal informação.

- Autenticidade e Integridade juntas garantem o Não-Repúdio;
- Condição necessária à validade jurídica das informações digitais.
- Recursos como o ***uso de criptografia*** são usados para esse fim.

Resumo: Definições e Termos

- **Confidencialidade**:
  - propriedade de que a informação não esteja disponível para pessoas, entidades ou processos não autorizados;
- **Integridade**:
  - propriedade de proteger a exatidão e a completeza de ativos;
- **Disponibilidade**:
  - propriedade de tornar acessível e utilizável sob demanda, por fontes autorizadas;
- **Autenticidade**:
  - propriedade de assegurar as veracidades do emissor e do receptor de informações trocadas;
- **Não repúdio**:
  - Não Repúdio (Irretratabilidade): é a garantia de que o autor de uma informação não poderá negar falsamente a autoria de tal informação;
- **Legalidade**:
  - Trata-se do embasamento legal;
- **Confiabilidade**:
  - Garantir que um sistema vai se comportar segundo o esperado e projetado.