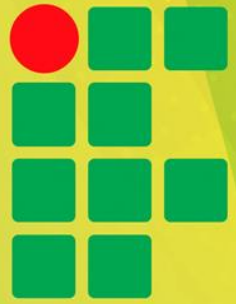
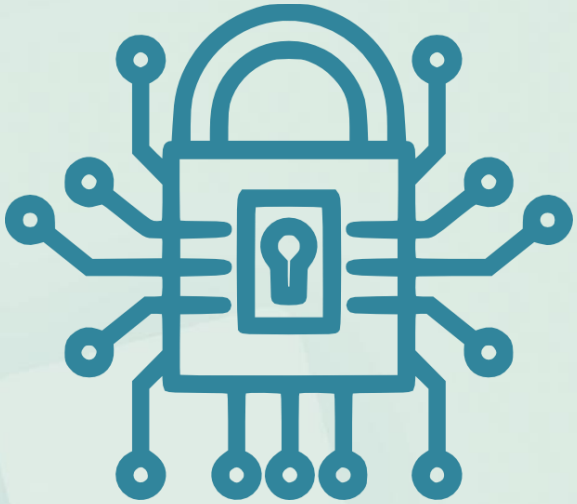


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



Introdução

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

Apresentação

Apresentação

- **Professor:** Heraldo Gonçalves Lima Junior
- **Horário:**
  - Quinta-feira (19:00-20:30)
- **Contato:**
  - heraldo.junior@ifsertao-pe.edu.br

Plano de Ensino

- **PRÉ-REQUISITOS:** Fundamentos da Computação
- **COMPETÊNCIAS:** Compreender e propor soluções para diversos tipos de situações problema na área de Segurança da Informação. Projetar políticas de Segurança da Informação.
- **HABILIDADES:** Compreender conceitos básicos inerentes à Segurança da Informação. Confecção de planos de segurança da Informação. Analisar ameaças e vulnerabilidades em sistemas. Elaborar planos de contingência para situações de risco aos ativos de TI. Conhecer táticas de defesa e ataques relativos à Segurança da Informação.

Ementa (30h)

- Princípios em segurança da informação.
- Análise de Riscos.
- Leis, normas e padrões de segurança da informação.
- Autenticação e controle de acesso.
- Aspectos tecnológicos da segurança da informação.
- Plano de continuidade do negócio.
- Boas práticas em segurança da informação.
- Norma NBR ISO/IEC 17799.
- Técnicas e algoritmos de criptografia de dados e Aplicações de segurança de dados

Bibliografia Básica

- ELEUTÉRIO, P. M. da S.; MACHADO, M. P. Desvendando a Computação Forense. São Paulo: Novatec, 2011.
- ENGEBRETSON, Patrick. Introdução ao hacking e aos testes de invasão: facilitando o hacking ético e os testes deinvasão. São Paulo: Novatec, 2014.
- MACHADO, F. N. Segurança da Informação: Princípios e Controle de Ameaças. São Paulo: Érica, 2014.
- RUFINO, N. M. de O. Segurança em redes sem fio: aprenda a proteger suas informações em ambiente Wi-Fi e Bluetooth. 4.ed. São Paulo: Novatec, 2015.

Bibliografia Complementar

- KUROSE, James F; ROSS, Keith W. Redes de computadores e a Internet: uma abordagem top-down. 5. ed. São Paulo: Pearson, 2010. 614p.
- SHIMONSKI, Robert; KINOSHITA, Lúcia Ayako. Wireshark - Guia prático: análise e resolução de problemas de tráfego de rede. São Paulo: Novatec, 2013. 167p.
- WEINDMAN, Georgia. Testes de invasão: uma introdução prática ao hacking: uma introdução prática ao hacking. São Paulo: Novatec, 2014.

Avaliações

- **Componentes:**
  - **Avaliações (AV):** 1 prova valendo 5pt.
  - **Seminários (S):** Apresentação de seminário valendo 5pt.

*As datas e temas dos seminários serão definidos ao longo da disciplina.

Média

- **Média:**
  - A média (M) da disciplina será calculada como:

$$M = (AV1 \times 0.5) + (S \times 0.5)$$

Introdução

Dado x Informação x Conhecimento

- **DADOS** são os componentes básicos a partir dos quais a **informação** é criada.

Dado x Informação x Conhecimento

- **INFORMAÇÃO** são os **dados** inseridos em um contexto que é a situação que está sendo analisada.

INSTITUTO FEDERAL
Sertão Pernambucano

Dado x Informação x Conhecimento

- A partir da **informação**, vem o **CONHECIMENTO**, que permite tomar decisões adequadas, trazendo vantagem competitiva.

Quanto vale a informação?

Definição

- Para Alves (2006, p. 15), a Segurança da Informação

  "visa **proteger a informação** de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios"

Definição

- ISO/IEC,

  “como uma proteção das informações contra uma ampla gama de ameaças para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidade comerciais”

Definição

- (Sêmola, 2003, p. 9),

  "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade"

Princípios Básicos

- **CONFIDENCIALIDADE** é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las.

CONFIDENCIALIDADE

INTEGRIDADE

DISPONIBILIDADE

Princípios Básicos

- **Exemplo de Quebra:** Alguém obtém acesso não autorizado ao seu PC e lê todas as informações da sua declaração de Imposto de Renda.

CONFIDENCIALIDADE

INTEGRIDADE

DISPONIBILIDADE

Princípios Básicos

- **INTEGRIDADE** é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

CONFIDENCIALIDADE

INTEGRIDADE

DISPONIBILIDADE

Princípios Básicos

- **Exemplo de quebra:** Alguém obtém acesso não autorizado ao seu PC e altera informações da sua declaração de Imposto de Renda, antes de você enviá-la para a Receita Federal.

CONFIDENCIALIDADE

INTEGRIDADE

DISPONIBILIDADE

Princípios Básicos

- **DISPONIBILIDADE** é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que deles precisam.

CONFIDENCIALIDADE

INTEGRIDADE

DISPONIBILIDADE

Princípios Básicos

- **Exemplo de quebra:** Seu provedor sofre uma grande sobrecarga ou ataque de negação de serviço. Por conta disso, você não consegue enviar sua declaração de IR.

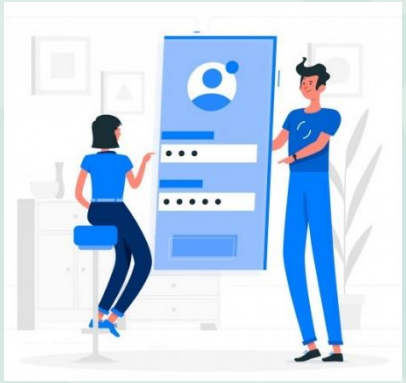
CONFIDENCIALIDADE

INTEGRIDADE

DISPONIBILIDADE

Princípios Complementares

- **AUTENTICAÇÃO:** Garantir que o usuário é de fato quem alega ser.



AUTENTICAÇÃO

NÃO-REPÚDIO

LEGALIDADE

PRIVACIDADE

AUDITORIA

Princípios Complementares

- **NÃO-REPÚDIO:** Capacidade do sistema provar quem realizou determinada ação.

AUTENTICAÇÃO

NÃO-REPÚDIO

LEGALIDADE

PRIVACIDADE

AUDITORIA

Princípios Complementares

- **LEGALIDADE:** Deve estar aderente a legislação.

AUTENTICAÇÃO

NÃO-REPÚDIO

LEGALIDADE

PRIVACIDADE

AUDITORIA

Princípios Complementares

- **PRIVACIDADE:** Capacidade de um sistema manter o usuário anônimo, sem relacionar as ações com o usuário.

AUTENTICAÇÃO

NÃO-REPÚDIO

LEGALIDADE

PRIVACIDADE

AUDITORIA

Princípios Complementares

- **AUDITORIA:** Capacidade do sistema auditar tudo que foi realizado pelos usuários, detectando fraudes ou tentativas de ataques.

AUTENTICAÇÃO

NÃO-REPÚDIO

LEGALIDADE

PRIVACIDADE

AUDITORIA

O que proteger?

Ativos

- Qualquer elemento que tenha valor para a organização [ISO27002];
- Os ativos fornecem suporte aos processos de negócios, portanto devem ser protegidos. Todo elemento utilizado para armazenar, processar, transportar, armazenar, manusear e descartar a informação, inclusive a própria.

Categorias de Ativos

- Os ativos podem ser classificados / agrupados de diversas formas:
  - Informações; Hardware; Software; Ambiente Físico; Pessoas;
  - Lógico; Físico Humano;
  - Equipamentos; aplicações, usuários, ambientes, informações e processos;

Vulnerabilidades

- **Fragilidade** de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças [ISO 27002];
- As vulnerabilidades devem ser gerenciadas (identificadas e corrigidas);

Tipos de Vulnerabilidades

- **Físicas:** Instalação predial, controle de acesso, data center, etc. Tudo que envolve controle de acesso às instalações do ambiente corporativo.

Tipos de Vulnerabilidades

- **Naturais:** Desastres como incêndios, quedas de energia, etc. Para tudo o que pode tirar o seu ambiente de produção do funcionamento adequado, a pergunta que deve ser feita é: existe um plano de contingência?

Tipos de Vulnerabilidades

- **Humanas:** Falta de treinamento e alinhamento com as políticas de segurança da empresa, vandalismo e até mesmo sabotagem. Um colaborador descontente pode, sim, ser uma ameaça.

Tipos de Vulnerabilidades

- **Hardware:** Depreciação do ativo, má instalação, etc. Tudo o que envolve um ativo ou item de configuração que pode causar indisponibilidade do acesso ao ambiente de produtividade da empresa.

Tipos de Vulnerabilidades

- **Software:** Um software ou sistema operacional desatualizado pode causar grande impacto aos negócios.

Ameaças

- **Causa potencial** (agente) de um incidente indesejado, que pode resultar em dano para um sistema ou organização [ISO 27002];
- A segurança da informação precisa prover mecanismos para impedir que as ameaças explorem as vulnerabilidades;

Tipos de Ameaças

- **Naturais:** que são as decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.

Tipos de Ameaças

- **Involuntárias:** são as ameaças inconscientes, quase sempre causadas pelo desconhecimento, como acidentes, erros, falta de energia, entre outros.

Tipos de Ameaças

- **Voluntárias:** são as ameaças propositais, causadas por agentes humanos, como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador e incendiários.

Evento de Segurança da Informação

- Uma **ocorrência identificada de um estado de sistema**, serviço ou rede, indicando uma **possível violação da política de segurança** da informação ou falha de controles que possa ser relevante para a segurança da informação [ISO 27000:2009].

Evento de Segurança da Informação

- Um simples ou uma série de **eventos de segurança da informação** indesejados ou inesperados, que tenham uma **grande probabilidade** de comprometer as operações de negócios e **ameaçar a segurança da informação** [ISSO 27000:2009].

Controles

- Medidas de segurança são práticas, procedimentos e mecanismos utilizados para a proteção de ativos;
- Esses controles podem: (a) impedir que as ameaças explorem as vulnerabilidades, (b) reduzir o surgimento de vulnerabilidades e (c) minimizar o impacto dos incidentes de segurança da informação;

Ataques

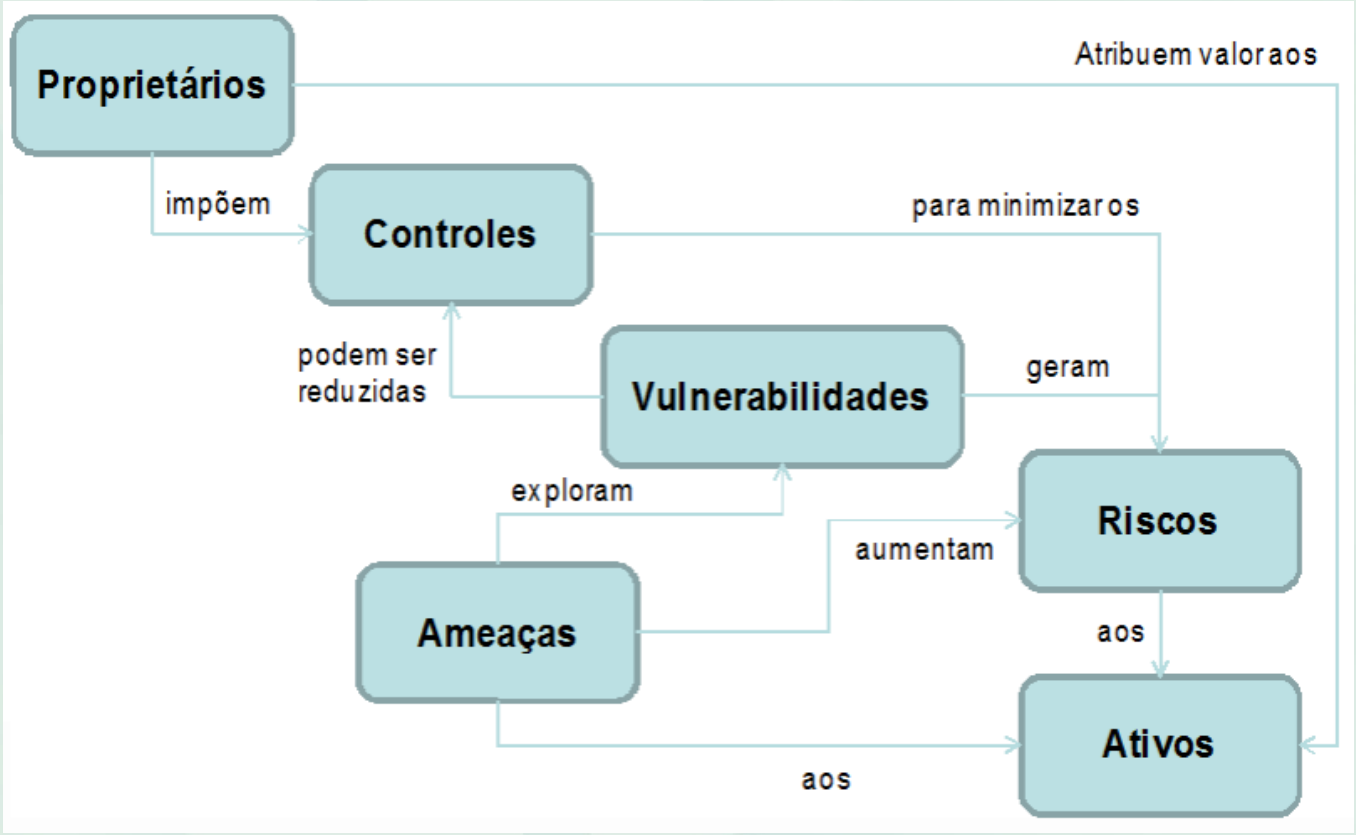
- "evento decorrente da exploração de uma vulnerabilidade por uma ameaça." (Beal, 2008)

Tipos de Ataques

- **Passivos**: São aqueles que não interferem no conteúdo do recurso que foi atacado, como por exemplo, observação e conhecimento de informações armazenadas nos sistemas institucionais ou análise de tráfego de uma rede.
- **Ativos:** Prejudicam diretamente o conteúdo do recurso atacado, modificando e eliminando informações.

Incidente

- Eventos de segurança indesejados que violem algum dos principais aspectos da segurança da informação (Confiabilidade, integridade, disponibilidade, dentre outros).


Proprietários
Atribuem valor aos
impõem
Controles
para minimizar os
podem ser reduzidas
Vulnerabilidades
geram
exploram
Riscos
aumentam
Ameaças
aos
Ativos
aos

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano