

# Aula 01

Disciplina  
Segurança e Auditoria de Sistemas de Informação

Professor Gleizer B. Voss  
Turma ADS 18

# Roteiro

---

- Segurança da Informação
  - Definição;
  - Falhas;
  - Tendências;
  - Pilares norteadores;
  - Ativos envolvidos.



# Questionamento / Objetivo

---

- Segurança da Informação
  - O que são?
  - De onde vem?
  - Como se formam?
  - O que fazem?
- Proporcionar a construção de saberes aos alunos com a apresentação dos principais conceitos, relações e componentes envolvidos no processo de aplicação de práticas de Segurança da Informação.



# Conceitos Básicos

---

- *“Em um mundo onde existe uma riqueza de informação, existe frequentemente uma pobreza de atenção” (Ken Mehlman);*
- Qual o bem mais valioso de uma organização atualmente?
- Ele pode não ser aquele produzido ou um serviço prestado.

# Conceitos Básicos

---

## ***SEGURANÇA DA INFORMAÇÃO!!!***



Fonte: cisco.com

# Conceitos Básicos

---

- Informação pode ser obtida e transmitida por vários meios;
- A perda ou destruição pode gerar prejuízos imensuráveis para uma instituição;
- Não existe um ambiente 100% seguro;
- Mas o emprego de boas práticas e técnicas de segurança podem evitar danos maiores.

# Conceitos Básicos

---

- Segurança da Informação?
  - Proteção da informação contra vários tipos de ameaças;
  - Forma de manter o funcionamento do negócio e minimizar os riscos;
  - Melhorar as oportunidades de negócio;
  - Tem como propósito proteger as informações registradas, sem importar onde estejam situadas: impressas em papel, nos discos rígidos dos computadores ou até mesmo na memória das pessoas que as conhecem.

# Conceitos Básicos

---

- Segurança da Informação?
  - A Segurança da Informação (SI) é o ramo do conhecimento responsável pela preservação e descarte dos ativos de informação, seja ela pessoal ou corporativa, através da elaboração de critérios que protejam esses ativos contra o furto, roubo, perda, corrupção ou uso indevido.



# Atividade: Falhas de Segurança

---

Pesquise por falhas/incidentes de Segurança da Informação que aconteceram recentemente;  
Escolha um que julgar relevante;  
Descreva as consequências do incidente;  
Descreva o que gerou o incidente;  
Descreva a solução (ou uma possível ação que poderia ter impedido tal incidente).  
Monte uma breve apresentação (máximo 5 min) para compartilhar com os colegas.

# Conceitos Básicos

---

## Casos de Falhas de Segurança

- Em agosto de 2015, pesquisadores de segurança descobriram uma brecha que poderia afetar 95% dos dispositivos que rodam Android. A falha, batizada de "Stagefright", permitia inutilizar o smartphone com uma simples mensagem, permitindo que criminosos monitorassem áudio, vídeo e até executassem à distância uma série de tarefas.
- O Google disponibilizou patches de correção e se comprometeu a liberar as correções mensalmente, em uma tentativa de impedir que os dispositivos fiquem vulneráveis por muito tempo.

Fonte: [https://olhardigital.com.br/fique\\_seguro/noticia/5-grandes-falhas-de-seguranca-de-2015/53879](https://olhardigital.com.br/fique_seguro/noticia/5-grandes-falhas-de-seguranca-de-2015/53879)  
<https://meiobit.com/323112/android-vulnerabilidade-95-dos-aparelhos-afetados-indefensavel/>

# Conceitos Básicos

---

## Casos de Falhas de Segurança

- Em fevereiro de 2015, a base de dados da Anthem, segunda maior seguradora de saúde dos Estados Unidos, foi roubada. Nomes, datas de nascimento, IDs, endereços de e-mail e outras informações pessoais de 80 milhões de clientes foram vazados na Internet.
- Em junho, o governo dos Estados Unidos informou que o país havia sido vítima de um ataque, que teve como resultado o roubo de identidade de mais de 20 milhões de funcionários. Os ataques se repetiram ao longo de 2015, o que fez com que especialistas em inteligência afirmassem que a ameaça à segurança nacional é tão grande que seus efeitos "vão durar décadas e custar bilhões de dólares".

Fonte: [https://olhardigital.com.br/fique\\_seguro/noticia/5-grandes-falhas-de-seguranca-de-2015/53879](https://olhardigital.com.br/fique_seguro/noticia/5-grandes-falhas-de-seguranca-de-2015/53879)

# Conceitos Básicos

---

## Casos de Falhas de Segurança

- Na espionagem realizada pela NSA no EUA e desmascarada pelo ex-agente Edward Snowden, ficou evidente que estamos sendo vigiados e que qualquer conversa por telefone ou por e-mail podem ser facilmente interceptadas por governos e crackers do mal.

Fonte: <https://analistati.com/tendencias-em-seguranca-da-informacao-para-2017-um-ano-critico/>

- **7 ataques hacker que entraram para a história**

<https://canaltech.com.br/video/top-tech/7-ataques-hacker-que-entraram-para-a-historia-top-tech-10404/>

# Conceitos Básicos

---


## **5 grandes vazamentos de dados no Brasil**

1. Cadastros de chaves PIX
2. Operação Deepwater
3. Vazamentos de dados no Ministério da Saúde
4. Netshoes
5. Vazamentos de dados da Enel em Osasco

<https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022>

# Conceitos Básicos

globo.com | g1 | ge | gshow | globoplay

ASSINE JÁ  GLEIZER VOS

MENU

g1

ECONOMIA

🔍 BUSCAR

## Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber

Número é maior do que a população do país, estimada em 212 milhões, porque inclui dados de falecidos. Informações expostas incluem CPF, nome, sexo e data de nascimento, além de uma tabela com dados de veículos e uma lista com CNPJs. Origem dos dados ainda é desconhecida.



NOTÍCIAS

VÍDEOS

CORONAVÍRUS

EDITORIAS

SUORTE

OD SEGURANÇA

Nós do **Olhar Digital** e nossos parceiros utilizamos *cookies*, *localStorage* e outras tecnologias semelhantes para personalizar conteúdo, análise de tráfego e melhorar sua experiência neste site, de acordo com nossos **Termos de Uso e Privacidade**. Ao continuar navegando, você concorda com essas condições.

## Brasil é o 6º país com mais vazamentos de dados no planeta, aponta levantamento

Por **Ronnie Mancuzo**, editado por **Acsa Gomes**

🕒 17/03/2022 10h48, atualizada em 18/03/2022 21h30

<https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>

# Conceitos Básicos

---

## Principais Falhas em Segurança

- Inexistência de uma estrutura de políticas, normas e procedimentos.
- A gestão do controle de acesso permite uma identificação para uso comum.
- Inexistência de gestor da informação.
- Planos de continuidade que são apenas belos documentos.

Fonte: <https://www.fiap.com.br/2016/05/09/dez-falhas-em-seguranca-da-informacao/>

# Conceitos Básicos

---

## Principais Falhas em Segurança

- Registros de ações realizadas inexistentes ou com pouco tempo de guarda.
- Cópias de segurança: definição da informática.
- Inexistência de um gestor do processo de segurança.
- Não existência de uma gestão de risco.
- Desalinhamento da segurança com o negócio.
- Usuário: pouco treinamento e conscientização.

Fonte: <https://www.fiap.com.br/2016/05/09/dez-falhas-em-seguranca-da-informacao/>



# Conceitos Básicos

---

## 8 previsões de cibersegurança para 2019

Vaporworms, Disrupção Global da Internet e Rogue IA Chatbots. Confira o que esperar para os próximos meses:

- 1) Surgimento de Malware worms “Vaporworms” ou Fileless
- 2) Internet será mantida como refém
- 3) Ataques cibernéticos em escala no nível de Estado forçam um tratado de ciber segurança da NU
- 4) Chatbots conduzido por IA
- 5) Um grande Hack biométrico será o começo do fim da autenticação de único fator
- 6) Estado-Nação receberão ataques do tipo “Fire Sale”, da ficção à realidade
- 7) Blackouts causados por hackers focados em Serviços Públicos e Sistemas de Controle Industriais
- 8) Uma rede WPA3 Wi-Fi será invadida usando uma das seis categorias de ameaça Wi-Fi

Fonte: <https://itforum365.com.br/8-previsoes-de-cibserguranca-para-2019/>

# Conceitos Básicos

---

**Confira 7 previsões sobre cibersegurança até 2020, segundo o Gartner.**

- 1) Inteligência artificial
- 2) Vulnerabilidades
- 3) Testes de penetração
- 4) Gestão inteligente da informação
- 5) Falhas
- 6) Nuvem
- 7) Programas de segurança da informação

Fonte: <https://www.cbsi.net.br/2017/07/confira-7-previsoes-sobre-ciberseguranca-ate-2020.html>

<https://www.portnet.com.br/previsoes-de-seguranca-da-informacao-para-alem-de-2020/>

# Conceitos Básicos

---

2020 / 2021

- Aumento na variedade de malwares e sofisticação dos ataques cibernéticos;
- Mais foco em ataques a dispositivos móveis;
- Aplicativos de rastreamento e venda de dados à terceiros;
- Golpes direcionados a games e produtores de conteúdos;
- Ciberataques direcionados à educação.
- Infestações de redes domésticas;
- Inteligência Artificial, como uma arma de desinformação.

Fonte: <https://blog.starti.com.br/previsoes-2021/>

# Conceitos Básicos

## Previsões globais de cibersegurança para 2022:

- Notícias falsas/Fake News 2.0 e o retorno de campanhas de desinformação
- Ataques cibernéticos à cadeia de suprimentos continuarão a crescer e os governos enfrentarão o desafio
- Os ataques à cadeia de suprimentos se tornarão mais comuns e os governos começarão a estabelecer regulamentações para lidar com esses ataques e proteger as redes
- A “guerra fria” cibernética se intensificará
- As violações de dados serão em maior escala e mais caras

# Conceitos Básicos

## Previsões de cibersegurança de tecnologias para 2022:

- Os ataques de malware móvel aumentarão à medida que mais pessoas usam carteiras digitais e plataformas de pagamento
- A criptomoeda se tornará um ponto focal para ataques cibernéticos em todo o mundo
- Os atacantes aproveitarão as vulnerabilidades dos microsserviços para lançar ataques em grande escala
- A tecnologia Deepfake será uma arma para ataques
- As ferramentas de penetração continuarão a aumentar

# Conceitos Básicos

## Previsões de ciberataques no Metaverso para o segundo semestre de 2022:

- O ransomware se tornará um ecossistema muito mais fragmentado
- Cadeias de infecção de e-mails mais diversificadas
- O hacktivismo continuará a evoluir
- Ataques contínuos em redes blockchain descentralizadas com os primeiros ataques esperados no Metaverso

<https://www.checkpoint.com/press-releases/check-point-sofware-mid-year-security-report-reveals-42-global-increase-in-cyber-attacks-with-ransomware-the-number-one-threat/>

# Conceitos Básicos

## Tendências de cibersegurança para 2024:

- Recursos dos reguladores estarão sob pressão;
- Conselhos embarcando na segurança cibernética;
- Organizações começam a avaliar sua infraestrutura quanto à prontidão quântica.

<https://securityleaders.com.br/seguranca-sera-guiada-por-novas-politicas-nacionais-em-2024-preveem-especialistas/>

# Tendências de cibersegurança para 2024:

1. **Maior Foco na IA e Machine Learning em Cibersegurança;**
2. **Importância Crescente da Segurança IoT;**
3. **Expansão do Trabalho Remoto e Implicações de Cibersegurança;**
4. **A ascensão da computação quântica e o seu impacto na cibersegurança;**
5. **Evolução dos ataques de *phishing*;**
6. **Foco melhorado na segurança móvel;**
7. **Segurança Zero Trust;**
8. **Lacuna de competências de cibersegurança e educação;**
9. **Blockchain e Cibersegurança;**
10. **Seguros de cibersegurança tornando-se *mainstream*.**

<https://www.splashtop.com/pt/blog/cybersecurity-trends-and-predictions-2024#:~:text=Em%202024%2C%20a%20IA%20e,os%20sistemas%20de%20detec%C3%A7%C3%A3o%20precoce.>



# Conceitos Básicos

- **Pilares da Segurança**
- **C**onfidencialidade;
- **I**ntegridade;
- **D**isponibilidade;
- Autenticidade;
- Não repúdio.



# Conceitos Básicos

---

- **Confidencialidade**
- Diz respeito ao direito de acesso;
- A informação deve estar acessível apenas para quem tem direito de acesso;
- Empregos de medidas de segurança para evitar acesso não autorizado;
- Quando uma informação é acessada por uma pessoa não-autorizada, ocorre um incidente na segurança da informação por quebra de confidencialidade.

# Conceitos Básicos

---

- **Confidencialidade**
- Exemplos:
  - Informações de operação policial;
  - Senha da conta bancária;
  - Gabarito da prova;
  - Listão de aprovados no vestibular;
- Técnicas como a Criptografia e a Esteganografia são utilizadas para aumentar a confidencialidade de uma informação.

# Conceitos Básicos

---

- **Confidencialidade**
- O primeiro passo para proteger a confidencialidade das informações é através do estabelecimento do grau de sigilo;
- Que é uma graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem permissões de acesso.

# Conceitos Básicos

---

- **Confidencialidade**
- O grau de sigilo faz parte de um importante processo de segurança de informações, a classificação da informação;
- Um exemplo de graus de sigilo pode ser:
  - Confidencial;
  - Restrito;
  - Sigiloso;
  - Público.

# Conceitos Básicos

---

- **Integridade**
- Diz respeito à sua exatidão;
- É garantido quando a informação acessada está completa, sem alterações e portanto confiável;
- A informação deve ser somente alterada por pessoas e/ou ativos autorizados;
- Também pode ser necessário em situações que demandem alteração legítima.

# Conceitos Básicos

---

- **Integridade**
- Exemplos:
  - Plano de viagem;
  - Dados preenchidos em um cheque;
  - Conteúdo de um edital;
  - Prescrição de um medicamento;
- Uma técnica muito utilizada para a garantia da Integridade é o uso de funções Hash.

# Conceitos Básicos

---

- **Integridade**
- A quebra de integridade ocorre quando a informação é corrompida, falsificada ou indevidamente alterada;
- Uma informação poderá ser alterada de várias formas, tanto em seu conteúdo quanto no ambiente:
  - Alterações do conteúdo dos documentos – quando são realizadas inserções, substituições ou exclusões de parte de seu conteúdo.
  - Alterações nos elementos que oferecem suporte à informação – quando são realizadas alterações na estrutura física e lógica onde a informação está armazenada.



# Conceitos Básicos

---

- **Disponibilidade**
- Devem garantir que a informação esteja disponível;
- Sempre que for necessário, os usuários devem ter o direito de acesso à ela;
- Causas: podem ser as mais diversas, desde a falta de luz, incêndios, sabotagens até vírus, ataques computacionais, congestionamentos, etc;
- Solução: o uso de no-breaks, a manutenção dos backups e o espelhamento de discos (RAID).

# Conceitos Básicos

---

- **Disponibilidade**
- **Exemplos**
  - Extrato bancário;
  - Dados gerenciais de tomada de decisão;

# Conceitos Básicos

---

- **Autenticidade**
- Diz respeito à certeza da origem da informação;
- Deve ser garantido que a informação é resultante de uma fonte confiável e que não foi alvo de mutação ao longo de sua transmissão;
- Técnicas como o uso de senhas, biometria, tokens e certificados digitais podem ser utilizados para tornar autêntico o acesso às informações.

# Conceitos Básicos

---

- **Autenticidade**
- Exemplos:
  - Página Web do banco;
  - CRV para transferência do proprietário;
  - Atestado médico.

# Conceitos Básicos

---

- **Não repúdio/Irretratabilidade**
- Garantia que o autor de uma determinada ação não possa negar tal ação;
- É preciso garantir que sejam utilizados meios que possam identificar que há um equívoco na ação do autor.

# Conceitos Básicos

---

- **Não repúdio/Irretratabilidade**
- Notificação judicial;
- Notificação extrajudicial;
- Acesso a um determinado ambiente crítico (biometria).

# Conceitos Básicos

---

- A Confidencialidade é dependente da Integridade, pois se a Integridade de um sistema for perdida, os mecanismos que controlam a Confidencialidade não são mais confiáveis;
- A integridade é dependente da Confidencialidade, pois se alguma informação confidencial for perdida (senha de administrador do sistema) os mecanismos de integridade podem ser desativados.

# Conceitos Básicos

- **Ativos:**
- A própria informação;
- Infraestrutura física;
- Tecnologia da Informação;
- Pessoas.



Fonte: <https://italodiego.files.wordpress.com/2012/10/seguranc3a7a.png>



# Conceitos Básicos

---

- **Cenários de Segurança:**
- Segurança Física;
- Pessoas;
- Segurança na Tecnologia da Informação;
- Aspectos Legais;

# Conceitos Básicos

---

- **Segurança Física:**
- Desabamento
  - Total ou parcial;
- Explosão
  - Proposital ou acidental;
- Incêndio
  - Espontâneo, provocado ou acidental;
- Inundação
  - Natural ou em situações ambientais específicas;

# Conceitos Básicos

- **Segurança Física:**
- Barreiras e Controle de Acesso Físico;
- Identificação dos funcionários e visitantes;
- Equipamentos e Comunicações;
- Salas com acesso restrito;



Fonte: [http://www.activesolutionsrj.com.br/novosite/wp-content/uploads/2011/04/AS\\_acessob.jpg](http://www.activesolutionsrj.com.br/novosite/wp-content/uploads/2011/04/AS_acessob.jpg)

# Conceitos Básicos

- **Pessoas:**
- Falta de conhecimento;
- Agir com intenção de prejudicar;
- Negligência;
- Exemplos;



Fonte: <http://placas-digimetta.com.br/dinamic3/midia/?im=site/catalogo/1756/placa-pessoas-autorizadas.jpg>

# Conceitos Básicos

---

- **Pessoas:**
- Terrorismo: ação de agressão ao patrimônio empresarial com a utilização de violência extrema;
- Sequestros: ação de intimidação física concretizada contra pessoas físicas ou bens de extrema importância;
- Roubos e furtos: supressão de bens materiais;
- Fraudes: ações de modificação, com consequente obtenção de vantagem pelo agente agressor;
- Sabotagens: modificação de máquinas, equipamentos, instalações das organizações;
- Espionagem industrial: captação não autorizada de ativos intangíveis organizacionais.

# Conceitos Básicos

---

- **Pessoas:**
- Engenharia Social;
- Como tornar possível a indução de uma pessoa a atuar segundo seu desejo;
- **Objetivos:**
  - Espionagem;
  - Obter informações privilegiadas e/ou confidenciais;
  - Roubo de senhas;
  - Diversão.

# Conceitos Básicos

---

- **Pessoas:**
- Engenharia Social;
- Pessoas podem ser vulneráveis a este tipo de ação:
  - Autoridade;
  - Reciprocidade;
  - Ambição;
  - Curiosidade;
  - Carência afetiva;
  - Etc.



Fonte: <http://ultradicadas.net/wp-content/uploads/2016/05/engenharia-social-ataques.jpg>

# Conceitos Básicos

---

- **Aspectos Legais:**
- Uso de recursos de TI para fins pessoais;
- Uso malicioso de recursos;
- Problemas causados pelos funcionários podem afetar as empresas no meio judicial.



Fonte: [https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRnsP09tgenLSW6CUE8EeP0plsN\\_mSWxoOMqjkSHcRRrqPGwGjz](https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRnsP09tgenLSW6CUE8EeP0plsN_mSWxoOMqjkSHcRRrqPGwGjz)



# Conceitos Básicos

---

- **Aspectos Legais:**
- “Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados” (Art. 1o. 9.609/98 - Lei do Software)

# Conceitos Básicos

---

- **Aspectos Legais:**
- Pirataria de Usuário Final: ocorre quando os usuários fazem cópias adicionais do software sem autorização;
- Venda Não Autorizada: a pirataria de revendedor ocorre quando um revendedor sem escrúpulos distribui múltiplas cópias de um único pacote de software original a diferentes clientes.

# Conceitos Básicos

---

- **Aspectos Legais:**
- Pirataria pela Internet: softwares originais disponibilizados pelos fabricantes são replicados ilegalmente em sites piratas;
- Cracking: ocorre quando se consegue acesso ilegal a softwares protegidos.

# Conceitos Básicos

---

- **Aspectos Legais:**
- **Spamming:** é o envio indiscriminado de e-mail não solicitado para muitos usuários da Internet, sendo a tática favorita dos remetentes de massas de propagandas não solicitadas ou junk e-mail;
- **Flaming:** prática de enviar mensagens de e-mail extremamente críticas, detrativas e muitas vezes vulgares (flame mail) para outros usuários na Internet ou serviços on-line.

# Conceitos Básicos

---

- **Segurança na Tecnologia da Informação:**
- Evolução gigante no uso de sistemas de informação;
- Aumento dos riscos:
  - Vírus;
  - Acesso não autorizado;
  - Invasão de sistemas;
  - Entre outros.
- Difusão da Internet;
- Aumento do número de vulnerabilidades;

# Conceitos Básicos

---

- **Segurança na Tecnologia da Informação:**
- Complexidade dos ataques aumentou;
- Busca pelo poder e reconhecimento;
- Alto conhecimento técnico.

# Conceitos Básicos

---

- **Segurança na Tecnologia da Informação:**
- Cracker: responsáveis pelos maiores danos e fraudes;
- Hacker: muito utilizado em organizações para testar seus sistemas de segurança;
- Phreakers: equipamentos eletrônicos;
- Carders: cartões de crédito;
- Script Kiddie: cracker inexperiente, usa ferramenta de terceiros e códigos prontos;
- Atacantes Internos: usam informações internas.

# Conceitos Básicos

---

- **Tipos de Ataque - Vírus**
- Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador;
- O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.



# Conceitos Básicos

---

- **Sistemas de detecção de intrusões (IDS)**
- Software capazes de detectar atividades suspeitas;
- Utiliza-se de padrões conhecidos de comportamento de intrusos;
- Podem analisar o tráfego interno e externo;
- Tipos de análise de tráfego
  - Signature detection;
  - Behaviour detection;
  - Protocol anomaly detection.

# Conceitos Básicos

---

- **Golpes na Internet (Discussão)**
- Furto de identidade;
- Fraude de antecipação de recursos;
- Phishing;
- Pharming;
- Golpes de comércio eletrônico;
- Boatos.

Fonte: <https://cartilha.cert.br/golpes/>



# Conceitos Básicos

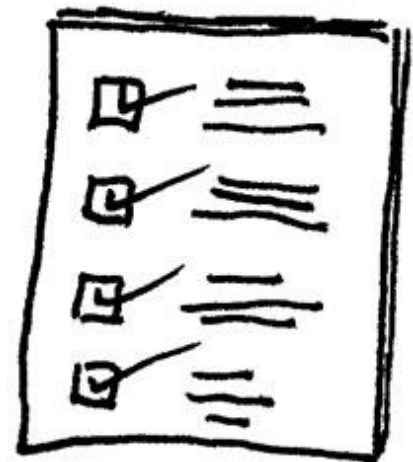
---

- **Boas práticas**
- Mantenha os programas instalados com as versões mais recentes;
- Use mecanismos de proteção;
- Use as configurações de segurança já disponíveis;
- Cuidado ao manipular arquivos;
- Proteja seus dados;
- Instalação de aplicativos;
- Cuidado com seu PC e de terceiros;
- Rede e Dispositivos Móveis.

# Resumo da Aula

---

- Segurança da Informação;
- Pilares norteadores;
- Brechas de Segurança;
- Aspectos envolvidos na Segurança.



# Referências Bibliográficas

---

- 1 Fórum de Excelência Pública 2012 – Boas práticas de Segurança da Informação;
- Softwares de Segurança da Informação. Jorge Procópio da Costa Novo. Curso Técnico em Manutenção e Suporte em Informática;

<https://cve.mitre.org/>

# Próxima aula

---

- Conceitos básicos;
- Norma BS 7799;
- Norma ISO/IEC 17799;
- Norma ISO/IEC 13335;

# Atividade 01

---

1. Para que serve a Segurança da Informação?
2. Cite os 5 princípios básicos da Segurança da Informação?
3. Cite principais falhas de segurança em uma empresa.
4. Quais são os aspectos a serem considerados em Segurança?
5. O que é um Cracker, Hacker e Phreakers?
6. O que é um IDS e seus tipos de análise?

# Proposta de atividade avaliativa

## Seminário

---

1. Escolher um tema/artigo nos anais do SBSEG (Últimos 5 anos)
2. Realizar a leitura;
3. Preparar uma apresentação para os colegas
4. Apresentações
5. Discussão sobre as apresentações

Anais SBSEG:

<https://sol.sbc.org.br/index.php/sbseg/issue/archive>



# Roteiro para a Apresentação

- Apresentação simples 5 a 6 slides com título;
- Autores/Instituição;
- Resumo com contextualização;
- Objetivos;
- Conceitos básicos envolvidos;
- Principais resultados;
- Conclusões;

- Vinicius (2022) - Ataques automatizados de Engenharia Social com o uso de Bots em Redes Sociais Profissionais
- Jorge (2022) - Gerenciamento Descentralizado de Identidades para Cidades Inteligentes baseado na tecnologia Blockchain
- Alice (2011) - Rumo à caracterização de Disseminação Ilegal de Filmes em redes BitTorrent
- Arthur (2019) - Gatos virtuais: detectando e avaliando os impactos da mineração de criptomoedas em infraestrutura pública
- Carlos (2021) - Subversão de perímetro criptográfico e alteração de dados na Urna Eletrônica Brasileira
- Erik (2023) - Impacto da Criptografia na Camada de Transportes
- João (2023) - Uma abordagem para detecção automática de fraudes em Aplicativos de Mensagens Instantâneas
- Samara (2021) - Protegendo redes de canais de pagamento sem fio
- Thiago (2023) - Explorando o RSSI na Geração de Chaves para LoRaWAN
- Yuri (2022) - Blockchain aplicado à rastreabilidade da cadeia produtiva do cacau da Amazônia
- Juliandro (2023) - Extração e análise de Indicadores de Comprometimento (IoCs) em Fóruns da Dark Web