Segurança e Auditoria de Sistemas

Apresentação da disciplina

Prof. Flávio Murilo de Carvalho Leal
Centro Universitário Paraíso

Flávio Murilo de Carvalho Leal

Formação Acadêmica

- (Tecnólogo em Manutenção Industrial) – (Instituto CENTEC)
- (Especialista em Automação Industrial) – (Instituto CENTEC)
- (Especialista em Docência do Ensino Superior) – (Unileão)
- (Mestre em Desenvolvimento Regional Sustentável) – (UFCA)

Atuação Profissional

- (Modelagem preditiva de dados/Inteligência Artificial)

Outras experiências

- (Docência / Consultoria / Pesquisa)

Escaneie o QR Code e responda o formulário.

- Canal principal: AVA/E-mail institucional
- Dúvidas sobre conteúdo: Sala de aula/AVA
- Questões individuais: Documentadas por e-mail/Conversas particulares presenciais
- flavio.leal@fapce.edu.br

Objetivos da Disciplina

- Compreensão dos fundamentos de Segurança da Informação
- Análise de riscos, ameaças e vulnerabilidades
- Relação entre segurança, governança e auditoria

Competências e Habilidades Esperadas

- Postura analítica e crítica
- Capacidade de avaliação de cenários de risco
- Compreensão de responsabilidades técnicas

Componentes Avaliativos

- Avaliações formais
- Trabalhos / Estudos dirigidos
- Participação e atividades

Rubricas Essenciais

- Clareza conceitual
- Coerência técnica
- Capacidade de análise

Datas de Avaliações

- TDEs:
  - TDE1: 05/03/2026
  - TDE2: 09/04/2026
  - TDE3: 07/05/2026
  - TDE4: 28/05/2026
- AVPs:
  - AVP1: 16/04/2026
  - AVP2: 18/06/2026
- Reposição e recuperação:
  - 2^a Chamada: 25/06/2026
  - AVF: 02/07/2026

Descrição:
Realização de curso online relacionado à disciplina. (Link)

Validação:

- Certificado de conclusão
- Tema compatível com segurança / TI / auditoria
- Prazo: 05/03/2026

Quando vocês ouvem "Segurança da Informação", o que vem à mente?

Escaneie o QR Code e responda o formulário.

Quando vocês ouvem "Segurança da Informação", o que vem à mente?

Possíveis associações:

- Hackers
- Senhas
- Golpes digitais
- Vírus / Malware
- Bancos / Pix / Redes sociais

Segurança está muito mais presente do que parece.

O que é Segurança da Informação?

Segurança da Informação envolve a proteção dos **ativos informacionais** de uma organização ou indivíduo.

Ativos informacionais podem incluir:

- Dados
- Sistemas
- Código-fonte
- Infraestrutura
- Conhecimento / Pessoas

Informação possui valor → logo, precisa ser protegida.

A Tríade Fundamental (CIA)

Modelo central da Segurança da Informação:

- **Confidencialidade** → Quem pode acessar?
- **Integridade** → A informação está correta?
- **Disponibilidade** → Está acessível quando necessário?

Toda análise de segurança passa por essas três dimensões.

Proteção contra acessos não autorizados.

Exemplos:

- Dados pessoais
- Informações financeiras
- Senhas
- Documentos sigilosos

Quebra de confidencialidade não é necessariamente alteração de dados.

Garantia de que a informação não foi alterada indevidamente.

Exemplos:

- Nota acadêmica modificada
- Valor financeiro alterado
- Registro corrompido

Integridade envolve precisão, consistência e confiabilidade.

Disponibilidade

Garantia de acesso à informação ou sistema quando necessário.

Exemplos:

- Sistema fora do ar
- Ataques de negação de serviço (DoS)
- Ransomware

Disponibilidade é requisito crítico em sistemas modernos.

Para entender riscos, precisamos distinguir:

- **Ativo** → O que tem valor
- **Ameaça** → O que pode causar dano
- **Vulnerabilidade** → Fraqueza explorável
- **Risco** → Probabilidade de perda

Exemplo de Risco

Cenário:

- Ativo → Dados bancários
- Ameaça → Phishing
- Vulnerabilidade → Usuário despreparado
- Risco → Perda financeira

Risco surge da combinação entre ameaça e vulnerabilidade.

Ameaça vs Vulnerabilidade

Pergunta clássica:

Uma senha fraca é ameaça ou vulnerabilidade?

Resposta correta:
Vulnerabilidade → Fraqueza que pode ser explorada.

Grande parte dos incidentes de segurança envolve pessoas.

- Engenharia social
- Erros operacionais
- Má configuração
- Excesso de confiança

Tecnologia forte + comportamento frágil = risco elevado.

Exemplos comuns:

- Vazamento de dados
- Sistemas indisponíveis
- Sequestro de informações (ransomware)
- Fraudes digitais

Perguntas importantes:

- Qual ativo foi afetado?
- Qual dimensão da CIA foi violada?

Segurança não é etapa final.

- Deve nascer no projeto
- Decisões arquiteturais impactam riscos
- Erros de modelagem geram vulnerabilidades

Não existe sistema seguro mal projetado.

Exemplos frequentes:

- Validação inadequada de entradas
- Autenticação fraca
- Controle de acesso incorreto
- Exposição excessiva de dados

Considere um sistema web simples com login e senha.

Questões:

- Quais ativos precisam ser protegidos?
- Que tipos de ataques podem ocorrer?
- Onde podem existir vulnerabilidades?

Segurança envolve múltiplas dimensões:

- Tecnologia
- Pessoas
- Processos
- Gestão de riscos
- Decisões organizacionais

Não é apenas um problema técnico.

Por que olhar para o histórico?

A Segurança da Informação não surgiu pronta.

Ela evoluiu em resposta a:

- Mudanças tecnológicas
- Novos modelos de uso de sistemas
- Incidentes e ataques relevantes
- Demandas legais e regulatórias

Grande parte das práticas atuais nasceu de crises e falhas reais.

Era dos Mainframes (décadas de 1960–1970)

Ambientes centralizados e altamente controlados.

- Computadores isolados
- Acesso físico restrito
- Segurança focada em controle de acesso

Principais preocupações:

- Quem pode usar o sistema
- Proteção contra uso indevido interno

Time-Sharing e Multiusuários

Surgimento de múltiplos usuários no mesmo sistema.

- Compartilhamento de recursos computacionais
- Necessidade de isolamento lógico
- Fortalecimento de autenticação e permissões

Nasce a importância de:

- Controles de acesso
- Perfis e privilégios

Sistemas deixam de ser isolados.

- Comunicação entre máquinas
- Novos vetores de ataque
- Surgimento de ameaças remotas

Segurança passa a envolver:

- Proteção de comunicação
- Confiança entre sistemas

1988 – Worm de Morris

Marco fundamental na história da segurança.

- Primeiro worm de grande impacto na Internet
- Exploração automática de vulnerabilidades
- Sistemas indisponíveis em larga escala

Consequências:

- Consolidação da área de segurança
- Criação de equipes de resposta a incidentes (CERT)

Popularização dos PCs e Vírus (anos 1990)

Computação descentralizada.

- Crescimento de malware
- Disseminação via disquetes e softwares
- Usuário final torna-se alvo crítico

Fortalecimento de:

- Antivírus
- Políticas de uso

Explosão de conectividade.

- Sistemas expostos globalmente
- Surgimento de ataques web
- Crescimento de fraudes digitais

Evolução de:

- Firewalls
- Criptografia
- Segurança de aplicações

Incidentes passam a gerar impactos financeiros e legais.

- Fraudes eletrônicas
- Manipulação de informações
- Falhas de controle interno

Auditoria de sistemas torna-se essencial para:

- Verificar controles
- Avaliar riscos

Escândalos corporativos e exigências legais.
Exemplos relevantes:

- SOX (Sarbanes–Oxley)
- ISO/IEC 27001
- LGPD

Segurança deixa de ser apenas técnica → torna-se estratégica.

Ameaças tornam-se mais sofisticadas.

- APTs (ameaças persistentes avançadas)
- Ransomware
- Vazamentos massivos

Exigem:

- Monitoramento contínuo
- Gestão de riscos
- Resposta a incidentes

Mudança radical de paradigma.

- Perímetro difuso
- Dependência de terceiros
- Compartilhamento de responsabilidades

Surgem novos modelos:

- Zero Trust
- Segurança baseada em identidade

Segurança evolui reativamente e continuamente.

- Novas tecnologias → novos riscos
- Novos ataques → novos controles
- Novos cenários → novas abordagens

Não existe segurança definitiva — apenas gestão contínua de riscos.

Por que olhar para o histórico?

A Segurança da Informação não surgiu pronta.

Ela evoluiu em resposta a:

- Mudanças tecnológicas
- Novos modelos de uso de sistemas
- Incidentes e ataques relevantes
- Demandas legais e regulatórias

Grande parte das práticas atuais nasceu de crises e falhas reais.

Era dos Mainframes (décadas de 1960–1970)

Ambientes centralizados e altamente controlados.

- Computadores isolados
- Acesso físico restrito
- Segurança focada em controle de acesso

Principais preocupações:

- Quem pode usar o sistema
- Proteção contra uso indevido interno

Surgimento de múltiplos usuários no mesmo sistema.

- Compartilhamento de recursos computacionais
- Necessidade de isolamento lógico
- Fortalecimento de autenticação e permissões

Nasce a importância de:

- Controles de acesso
- Perfis e privilégios

Sistemas deixam de ser isolados.

- Comunicação entre máquinas
- Novos vetores de ataque
- Surgimento de ameaças remotas

Segurança passa a envolver:

- Proteção de comunicação
- Confiança entre sistemas

1988 – Worm de Morris

Marco fundamental na história da segurança.

- Primeiro worm de grande impacto na Internet
- Exploração automática de vulnerabilidades
- Sistemas indisponíveis em larga escala

Consequências:

- Consolidação da área de segurança
- Criação de equipes de resposta a incidentes (CERT)

Popularização dos PCs e Vírus (anos 1990)

Computação descentralizada.

- Crescimento de malware
- Disseminação via disquetes e softwares
- Usuário final torna-se alvo crítico

Fortalecimento de:

- Antivírus
- Políticas de uso

Explosão de conectividade.

- Sistemas expostos globalmente
- Surgimento de ataques web
- Crescimento de fraudes digitais

Evolução de:

- Firewalls
- Criptografia
- Segurança de aplicações

Incidentes passam a gerar impactos financeiros e legais.

- Fraudes eletrônicas
- Manipulação de informações
- Falhas de controle interno

Auditoria de sistemas torna-se essencial para:

- Verificar controles
- Avaliar riscos

Escândalos corporativos e exigências legais.
Exemplos relevantes:

- SOX (Sarbanes–Oxley)
- ISO/IEC 27001
- LGPD

Segurança deixa de ser apenas técnica → torna-se estratégica.

Ameaças tornam-se mais sofisticadas.

- APTs (ameaças persistentes avançadas)
- Ransomware
- Vazamentos massivos

Exigem:

- Monitoramento contínuo
- Gestão de riscos
- Resposta a incidentes

Mudança radical de paradigma.

- Perímetro difuso
- Dependência de terceiros
- Compartilhamento de responsabilidades

Surgem novos modelos:

- Zero Trust
- Segurança baseada em identidade

Segurança evolui reativamente e continuamente.

- Novas tecnologias → novos riscos
- Novos ataques → novos controles
- Novos cenários → novas abordagens

Não existe segurança definitiva — apenas gestão contínua de riscos.