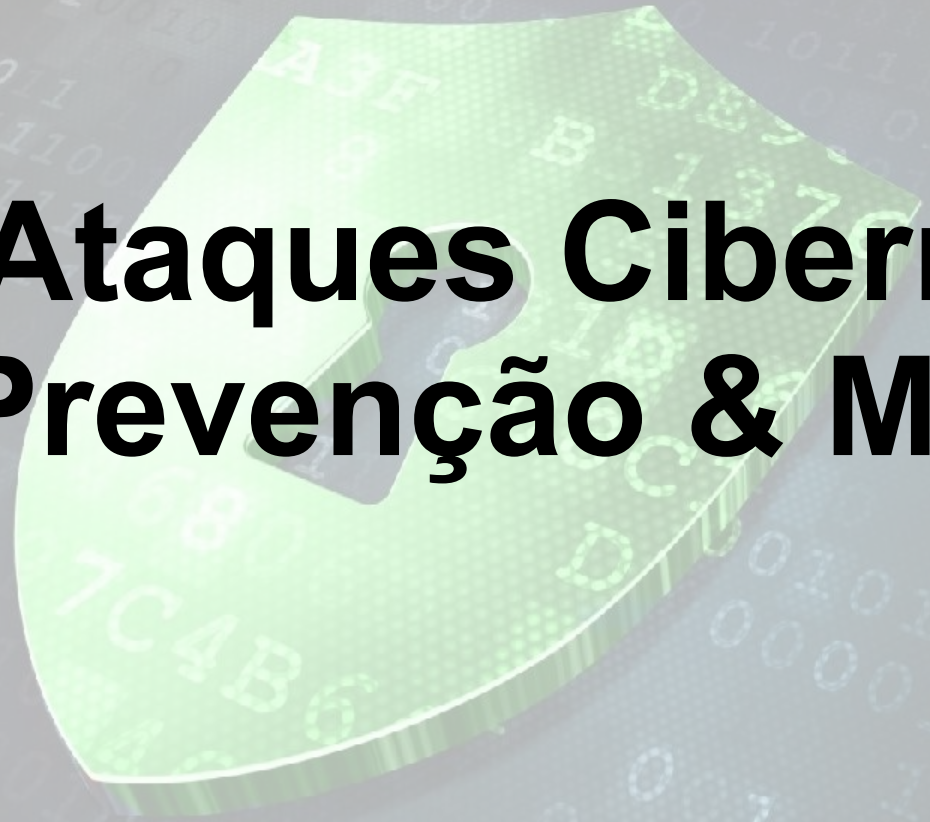


Ataques Cibernéticos, Prevenção & Mitigação

Prof. Msc. Francisco de Assis de Souza Rodrigues

UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO

🎯 Objetivos

- Compreender o que são ataques cibernéticos, suas motivações e impactos.
- Identificar os tipos mais comuns de ataques cibernéticos.
- Aprender práticas de prevenção voltadas a usuários e organizações.
- Conhecer os procedimentos de mitigação e resposta a incidentes de segurança.
- Desenvolver pensamento crítico sobre segurança da informação no contexto profissional e pessoal.

1. Introdução à Segurança da Informação e Ciberataques

✅ **Pontos principais:**

- **O que é segurança da informação?**
  - Proteção de dados e sistemas contra acesso não autorizado, uso indevido, divulgação, interrupção, modificação ou destruição.
- **Pilares da segurança da informação:**
  - **Confidencialidade** — proteger informações contra acesso não autorizado.
  - **Integridade** — garantir que as informações estejam corretas e não foram alteradas.
  - **Disponibilidade** — garantir que os sistemas e informações estejam acessíveis quando necessário.

1. Introdução à Segurança da Informação e Ciberataques

🔥 **Contextualização:**

- Ataques (ex.: vazamento de dados do governo, empresas atacadas por ransomware, hospitais paralisados).

- O impacto de um ataque vai além de perdas financeiras: afeta reputação, confiança e até vidas (hospitais, infraestruturas críticas).

1. Introdução à Segurança da Informação e Ciberataques

"Se sua senha do e-mail ou do banco vazasse hoje, qual seria o impacto na sua vida? Agora pense no impacto para uma empresa inteira."

2. Principais Tipos de Ataques Cibernéticos

🗂️ **Classificação dos ataques:**

- **Engenharia social**
- **Ataques técnicos**
- **Ataques físicos**

2. Principais Tipos de Ataques Cibernéticos

🔍 Ataques Baseados em Engenharia Social

Tipo	Descrição	Exemplos
Phishing	Envio de e-mails, SMS ou mensagens falsas para enganar o usuário e obter dados sensíveis	E-mail falso do banco pedindo atualização de senha
Spear Phishing	Phishing direcionado a uma pessoa específica	E-mail personalizado fingindo ser do RH da empresa
Vishing	Phishing por voz (telefone)	Golpes fingindo ser do suporte técnico ou banco
Smishing	Phishing via SMS ou WhatsApp	Mensagem de "seu pacote foi barrado, clique no link"

2. Principais Tipos de Ataques Cibernéticos

🔥 Ataques Técnicos

Tipo	Descrição	Exemplo
Malware	Software malicioso	Ransomware que sequestra dados
Spyware	Espionagem sem consentimento	Captura de teclas, telas, dados
Adware	Bombardeamento com anúncios	Pop-ups excessivos, redirecionamentos
Ransomware	Criptografa dados e exige resgate	Caso famoso: ataque à Colonial Pipeline
DDoS (Distributed Denial of Service)	Sobrecarga de servidores até quedas	Ataque a sites de governo ou grandes empresas

2. Principais Tipos de Ataques Cibernéticos

🔥 Ataques Técnicos

Tipo	Descrição	Exemplo
DDoS (Distributed Denial of Service)	Sobrecarga de servidores até quedas	Ataque a sites de governo ou grandes empresas
SQL Injection	Injeção de código em consultas SQL	Login com ' OR '1'='1
Cross-site Scripting (XSS)	Injeção de scripts maliciosos em páginas web	Captura de cookies, sessões de usuários
Man-in-the-Middle (MITM)	Interceptação de comunicação	Ataque em redes Wi-Fi públicas sem segurança
Zero-day Exploit	Exploração de vulnerabilidades desconhecidas pelos desenvolvedores	Ataques antes da correção oficial ser lançada

2. Principais Tipos de Ataques Cibernéticos

🚨 **Ataques a Infraestruturas**

- Ataques a sistemas SCADA, OT, IoT (Indústria, energia, saúde).
- Ex.: Ataque a uma usina elétrica ou hospital.

3. Estratégias de Prevenção

🔐 **A nível de usuário (boas práticas pessoais)**

- **Senhas fortes e exclusivas** para cada serviço.
- **Autenticação de dois fatores (2FA)** sempre que possível.
- Desconfiar de links e anexos recebidos, mesmo de conhecidos.
- Verificar a URL dos sites antes de inserir informações.

3. Estratégias de Prevenção

🔐 A nível de usuário (boas práticas pessoais)

- Manter sistemas operacionais e softwares atualizados.
- Utilizar antivírus e antimalware confiáveis.
- Usar gerenciadores de senhas (Bitwarden, 1Password).
- Cuidado com redes Wi-Fi públicas; utilizar VPN se possível.

🏢 A nível organizacional (boas práticas empresariais)

🔧 **Segurança Técnica:**

- Firewalls, IDS (Intrusion Detection System), IPS (Intrusion Prevention System).
- Criptografia de dados (em trânsito e em repouso).
- Gestão de vulnerabilidades e atualização constante de sistemas.
- Backup regular com testes de restauração.

🏢 A nível organizacional (boas práticas empresariais)

👥 Segurança Humana:

- Treinamento e conscientização dos colaboradores.
- Simulações periódicas de phishing.
- Políticas claras de segurança da informação.

🏢 A nível organizacional (boas práticas empresariais)

🗺️ **Governança e Gestão:**

- Plano de Continuidade de Negócio (PCN).
- Plano de Resposta a Incidentes.
- Auditorias e compliance (LGPD, ISO 27001).

4. Mitigação e Resposta a Incidentes

🔎 Fases de Resposta a Incidentes

Preparação

- Planos, equipes treinadas, ferramentas instaladas.

Identificação

- Monitoramento constante.
- Detectar comportamentos anômalos.

Contenção

- Isolamento rápido de máquinas ou redes afetadas.
- Minimizar o avanço do ataque.

4. Mitigação e Resposta a Incidentes

🔎 Fases de Resposta a Incidentes

Erradicação

Remoção do malware.

Aplicação de correções (patches) e mudanças necessárias.

Recuperação

Restauração dos sistemas a partir de backups.

Monitoramento pós-ataque para garantir estabilidade.

4. Mitigação e Resposta a Incidentes

🔎 Fases de Resposta a Incidentes

Lições Aprendidas

Documentação do ocorrido.

Revisão de processos e políticas.

Implementação de melhorias.

4. Mitigação e Resposta a Incidentes

🚧 Ferramentas usadas na mitigação

- SIEM (Security Information and Event Management): Splunk, IBM QRadar.
- Análise de logs: Graylog, ELK Stack (ElasticSearch, Logstash, Kibana).
- Forense digital: Autopsy, FTK.
- Monitoramento de aplicações: Sentry, Prometheus, Grafana.

Atividade Prática - Simulação de Resposta a Incidente

Cenário: A empresa XPTO sofreu um ataque de ransomware. Dados foram criptografados e há uma nota de resgate exigindo Bitcoin.

🎭 **Dividir em grupos com papéis:**

- **Equipe Técnica:** Analisar o ataque, conter e restaurar sistemas.
- **Equipe de Gestão:** Tomar decisões (pagar ou não o resgate, acionar autoridades, comunicar stakeholders).
- **Equipe de Comunicação:** Elaborar nota pública e comunicação interna.
- **Equipe Jurídica:** Avaliar aspectos legais (LGPD, notificação de vazamento).

Após 10 min de discussão em grupo, cada grupo apresenta sua estratégia para a turma.

Reflexão

Segurança não é um produto, é um **processo contínuo**.

O elo mais fraco geralmente é o **humano**, não a tecnologia.

Segurança da informação é uma **responsabilidade compartilhada**: usuários, desenvolvedores, empresas e governo.

📖 Indicações

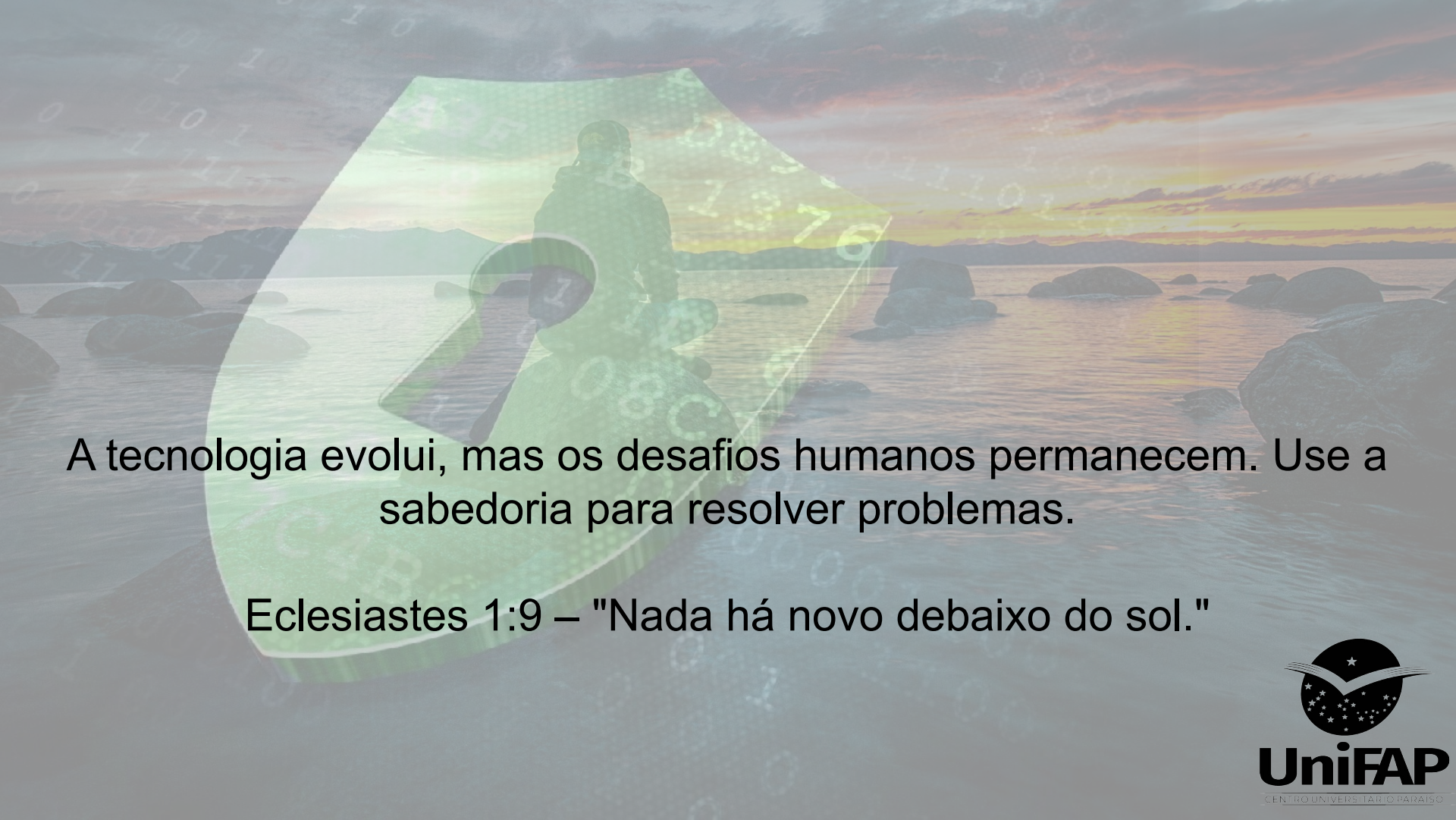
- OWASP Top 10 (https://owasp.org)
- MITRE ATT&CK Framework (https://attack.mitre.org)
- Livro: "Segurança em Redes" — William Stallings
- Documentário: "The Great Hack" (Netflix)

Bibliografia





UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO



A tecnologia evolui, mas os desafios humanos permanecem. Use a sabedoria para resolver problemas.

Eclesiastes 1:9 – "Nada há novo debaixo do sol."

UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO


OBRIGADO
Merci
Asante
Grazie
Kiitos
Obrigado
Arigato
Spasibo
Nirringrazzjak
Mamana
Kia Ora
THANK YOU
Chokrane
Terma Kasih
Multumesc
Raibh Maith Agat
Mochchakkeram
Cam on ban
Welalin
Maake
Dankon
UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO