**SENAI – ADS**

Gabriell Rodrigues dos Santos

**TRABALHO**

**Segurança da Informação e Ciberameaças na Era Digital**

Ferraz de Vasconcelos

13 de maio de 2025

**Introdução à Segurança da Informação**

A segurança da informação é o conjunto de práticas, políticas e tecnologias voltadas à proteção de dados contra acessos não autorizados, destruição, modificação ou divulgação indevida.

* Dados são registros brutos, sem interpretação ex: números, nomes.
* Informações são dados organizados que fazem sentido e geram conhecimento.

A tríade da segurança da informação (CID) representa os três pilares básicos:

* Confidencialidade: garantir que somente pessoas autorizadas tenham acesso à informação.
* Integridade: assegurar que a informação não seja alterada indevidamente.
* Disponibilidade: garantir o acesso à informação sempre que necessário.

**Ameaças e Tipos de Ataques Digitais**

Os ataques digitais podem ser realizados de diversas formas:

* Engenharia social: manipulação psicológica para obter informações sensíveis.
* Phishing: e-mails falsos que induzem o usuário a fornecer dados sigilosos.
* Ataques por força bruta: tentativa automática de diversas combinações de senha até descobrir a correta.

Malware: softwares maliciosos como:

Vírus: Malware que se anexa a arquivos ou programas e se espalha quando esses são executados.

* Precisa da ação do usuário para se propagar.
* Pode danificar arquivos, deixar o sistema lento ou apagar dados.
* Exemplo: vírus em anexos de e-mail ou pen drives.

Trojan: Malware que se disfarça de programa legítimo para enganar o usuário.

* Não se replica sozinho.
* Permite controle remoto, roubo de dados ou instalação de outros malwares.
* Exemplo: RATs (acesso remoto), Trojans bancários.

Spyware: Programa espião que coleta informações do usuário sem permissão.

* Rastreia navegação, senhas, dados bancários e hábitos online.
* Pode exibir propagandas (adware) ou capturar tudo que o usuário digita (keylogger).
* Exemplo: spyware embutido em softwares falsos ou downloads suspeitos.

Ransomware: Malware que sequestra dados e exige resgate (normalmente em criptomoedas).

* Criptografa arquivos da vítima.
* Muito usado contra empresas e órgãos públicos.
* Exemplo: WannaCry, REvil.
* Prevenção: backup, antivírus e cautela com links.

Worm: Tipo de malware que se espalha automaticamente pela rede, sem necessidade de ação do usuário.

* Usa falhas de segurança para se replicar.
* Pode sobrecarregar sistemas e redes.
* Exemplo: worms que se espalham por e-mail ou por falhas no Windows.

Ataques a redes:

* Man-in-the-middle: interceptação de comunicação.
* DoS/DDoS: sobrecarga de servidores.
* Spoofing: falsificação de identidade digital.

**Hackers x Crackers**

**Hackers**

Definição: Pessoa com grande conhecimento em informática, redes e sistemas, que usa habilidades para explorar, melhorar ou testar tecnologias.

Intenção

* Ajuda empresas a encontrar falhas e corrigir vulnerabilidade.
* Promove inovação, liberasse de informação e segurança digital.

**Crackers**

Definição:Pessoa que usa conhecimento técnico para fins maliciosos ou ilegais, como invadir sistemas, roubar dados ou causar prejuízo.

Intenção

* Prejudicar pessoas ou organizações
* Roubar informações, aplicar golpes, quebrar proteções
* Espalhar malwares

Tipos de hackers:

* White Hat: hackers éticos que ajudam a proteger sistemas.
* Black Hat: hackers maliciosos.
* Grey Hat: atuam entre os dois extremos.

Casos famosos:

* Kevin Mitnick (ex-hacker que se tornou consultor de segurança).
* Ataques do grupo Anonymous.

**Ferramentas de Proteção**

Para proteger-se no ambiente digital, é essencial utilizar ferramentas como:

* Antivírus e antispyware: detectam e eliminam malwares.
* Firewall: controla o tráfego entre a rede interna e externa.
* Autenticação em dois fatores: adiciona uma camada extra de segurança no login.
* Criptografia de dados: codifica informações para que apenas o destinatário correto as leia.
* Backup e políticas de recuperação de desastres: garantem a continuidade dos serviços após incidentes.

**Casos Reais de Ciberataques**

* Ransomware em órgãos públicos: Em 2020, o STJ (Superior Tribunal de Justiça) foi vítima de um ataque de ransomware, paralisando suas atividades por dias.
* Facebook/Cambridge Analytica: milhões de dados de usuários foram utilizados sem consentimento para manipulação política.
* Vazamento de dados no Brasil: em 2021, dados de mais de 220 milhões de brasileiros (incluindo falecidos) foram expostos na internet.

**Boas Práticas para o Usuário**

* Criar senhas seguras: misturar letras maiúsculas, minúsculas, números e símbolos.
* Cuidado com links e e-mails suspeitos: verificar remetente e não clicar em links desconhecidos.
* Comportamento seguro em redes sociais: evitar expor dados pessoais e localização em tempo real.
* Educação digital nas empresas: promover treinamentos e conscientização sobre segurança cibernética.