**SISTEMAS COMPUTACIONAIS E SEGURANÇA - SCS**

**PRÁTICA 00 - PROF CALVETTI**

**CONTEÚDOS DE BASE QUE SERÃO UTILIZADOS NA UC SISTEMAS COMPUTACIONAIS E SEGURANÇA - SCS**

****

***1. Segurança em Redes de Computadores:***Um dos principais conteúdos abordados em SCS envolve a segurança de redes. Isso inclui a proteção de dados em trânsito através da criptografia e a implementação de firewalls para filtrar tráfego malicioso. A segurança em redes é essencial em empresas, para garantir que informações sensíveis, como dados de clientes ou informações financeiras, não sejam interceptadas durante a transmissão.

***2. Controle de Acesso e Autenticação:***Esse tema abrange a implementação de políticas de controle de acesso, que definem quem tem permissão para acessar determinados recursos de um sistema. Técnicas como autenticação multifatorial (MFA) e autenticação biométrica são cada vez mais comuns em sistemas bancários e plataformas digitais, garantindo que apenas usuários autorizados possam acessar informações confidenciais.

***3. Segurança de Dados em Aplicações Web:***Sistemas de segurança para aplicações web protegem contra ataques como injeção SQL, cross-site scripting (XSS) e cross-site request forgery (CSRF). Essas práticas de segurança são fundamentais em plataformas de e-commerce, por exemplo, onde é necessário proteger informações pessoais e dados de pagamento dos usuários

***4. Monitoramento de Sistemas e Detecção de Intrusos:***A disciplina aborda a importância do monitoramento contínuo de sistemas e redes para identificar atividades suspeitas, como tentativas de acesso não autorizadas ou comportamentos anômalos. Softwares de detecção de intrusos (IDS) e sistemas de prevenção de intrusos (IPS) são usados em ambientes corporativos para detectar e reagir a possíveis ameaças antes que causem danos.

***5. Segurança em Dispositivos Móveis:***Com o crescimento do uso de smartphones e tablets, a proteção de dispositivos móveis se tornou uma área crucial dentro da segurança de sistemas computacionais. As práticas abordadas incluem criptografia de dados, uso de senhas fortes e políticas de atualização de software para mitigar vulnerabilidades. Empresas que adotam o modelo de "bring your own device" (BYOD) precisam garantir a segurança dos dispositivos móveis de seus funcionários para proteger suas redes.