A unidade curricular (UC) Sistemas Informáticos e Segurança (SCS) abrange os fundamentos da compreensão e aplicação de sistemas informáticos, centrando-se nos fundamentos do seu funcionamento e nos desafios de segurança a eles associados. Este conteúdo tem uma variedade de aplicações práticas em áreas como desenvolvimento de software, gerenciamento de rede, administração de sistemas e segurança de rede. Aqui estão algumas aplicações possíveis do conteúdo abordado:

Integrantes Do Grupo:

Otavio Paiva/ RA: 824147017
Gabriel Prietro/ RA: 824142064
Eduardo Baptistella/ RA: 824147595

1. Arquitetura do sistema computacional:
Desenvolvimento de Sistemas e Aplicativos: Compreender como funciona um sistema de computador, incluindo sua arquitetura, é fundamental para o desenvolvimento de aplicativos eficientes. Compreender a arquitetura impacta diretamente na otimização do sistema para melhor desempenho e eficiência de recursos.
Incorporado e IoT: Muitos dispositivos modernos, como sensores e dispositivos de Internet das Coisas (IoT), são baseados em arquiteturas de sistemas de computação específicas. O conhecimento arquitetônico ajuda a projetar e otimizar esses dispositivos.

2. Sistema operacional e gerenciamento de recursos:
Gerenciamento de sistemas e infraestrutura: O estudo de sistemas operacionais, suas capacidades e gerenciamento de recursos (memória, processamento e armazenamento) para gerenciar com eficácia servidores, data centers e infraestrutura em nuvem.
Desenvolvimento de software: Compreender o gerenciamento de processos, threads e alocação de recursos no nível do sistema operacional é fundamental para a criação de aplicativos mais poderosos e eficientes.

3. Rede de computadores:
Construção e manutenção de redes: além de implementar soluções de rede seguras, compreender os protocolos de rede, o roteamento e a comunicação entre sistemas é fundamental para criar e gerenciar redes corporativas.
Segurança de Rede: A aplicação de práticas de segurança de rede, como firewalls, VPNs (redes virtuais privadas) e criptografia, depende de um profundo conhecimento dos protocolos e arquitetura de rede.

4. Criptografia e segurança de dados:
Proteção de dados confidenciais: O uso de criptografia para proteger dados armazenados ou em trânsito é uma aplicação direta do conhecimento de segurança de dados e é fundamental em áreas como finanças, saúde e comércio eletrônico.
Autenticação e controle de acesso: Ferramentas de segurança como autenticação multifator (MFA), sistemas de autorização e criptografia de senha são fundamentais para garantir a integridade e confidencialidade dos dados.

5. Segurança em Sistemas Computacionais:
Prevenção de Ataques Cibernéticos: Compreender os diferentes tipos de ameaças, como malware, phishing e ataques DDoS (Negação de Serviço Distribuída), possibilita a adoção de estratégias defensivas eficazes, incluindo antivírus, detecção de intrusos e sistemas de monitoramento.
Análise Forense e Resposta a Incidentes: Após a ocorrência de um incidente de segurança, é fundamental realizar uma análise forense para apurar como o ataque se deu e quais ações corretivas devem ser adotadas. Esse tipo de análise requer um conhecimento aprofundado em sistemas computacionais e segurança.

6. Virtualização e Computação em Nuvem:
Infraestrutura de TI e Cloud Computing: Dominar a virtualização de sistemas e a computação em nuvem possibilita a construção de ambientes adaptáveis e escaláveis para executar aplicativos, armazenar informações e realizar backups, com ênfase em alta disponibilidade e segurança.
Automação e Orquestração de Recursos: O emprego de containers (como o Docker) e sistemas de orquestração (como o Kubernetes) torna o uso de recursos computacionais mais eficiente, sendo crucial para empresas que lidam com grandes volumes de dados ou que oferecem serviços em larga escala.

7. Segurança em Sistemas Distribuídos:
Desenvolvimento de Sistemas Seguros: Sistemas distribuídos apresentam frequentes vulnerabilidades a ataques por causa de sua estrutura descentralizada. Por isso, é essencial investigar técnicas de segurança específicas para esses ambientes, como protocolos de consenso e estratégias de tolerância a falhas, para desenvolver sistemas robustos.
Blockchain e Criptomoedas: A segurança nas redes distribuídas é fundamental para as tecnologias de blockchain e criptomoedas, que se baseiam em algoritmos de consenso e criptografia sofisticada para assegurar a integridade e a proteção das transações.

8. Administração de Vulnerabilidades e Redução de Riscos:
Testes de Penetração (Pentesting): A execução de testes de segurança com o intuito de detectar vulnerabilidades em redes e sistemas requer um entendimento minucioso da estrutura desses sistemas e das formas como as falhas podem ser exploradas.

Diretrizes de Segurança e Governança: É fundamental que empresas e organizações implementem políticas de segurança bem definidas e eficazes, que vão desde o controle de acesso até a aderência a normas e regulamentos, como o GDPR.
9. Defesa Contra Ameaças Avançadas:
Inteligência Artificial e Aprendizado de Máquina na Segurança: A implementação de inteligência artificial e machine learning para identificar padrões de ataque e bloquear ameaças em tempo real está se tornando fundamental em sistemas de segurança de alta sofisticação.
Redes Neurais na Identificação de Intrusões: As redes neurais têm a capacidade de reconhecer comportamentos anômalos dentro dos sistemas, facilitando a detecção de possíveis ataques de maneira mais eficiente do que as abordagens convencionais.