APLICAÇÕES DOS CONTEÚDOS DE BASE DA UC SISTEMAS COMPUTACIONAIS E SEGURANÇA – SCS

Carolina Maria Alves Felipe – RA 824227064@ulife.com.br – Universidade São Judas Tadeu

De acordo com o conteúdo programático disponibilizado pela Universidade São Judas Tadeu, a UC de Sistemas Computacionais e Segurança tem como objetivo principal fazer com que o aluno receba e aprenda conceitos iniciais da história da computação, evolução e tendências, o funcionamento de bases numéricas (como binários, decimais, octal e hexadecimal) e a lógica de boole e portas lógicas. O aluno também aprenderá conceitos de sistemas operacionais, máquina virtual e deverá entender a função dos processadores lógicos e aritméticos. Além disso, a disciplina abordará arquitetura e organização de sistemas computadorizados, desvendando as memórias e dispositivos de armazenamento, processos e paralelismo.

Na parte de segurança, a disciplina preparará o aluno para identificar as principais ameaças existentes no uso pessoal e corporativo de sistemas computacionais e os elementos que constituem a arquitetura e a organização de computadores entendendo os aspectos relevantes de cada um deles no funcionamento e desempenho de uma máquina computacional. Ainda, o aluno deverá entender os conceitos de processos em sistemas operacionais e suas relações e deverá conhecer a importância da criptografia, seus tipos e aplicações, bem como compreender a importância da segurança da informação em redes corporativas e banco de dados.

É importante ressaltar que ao fim da disciplina o aluno deverá ser capaz de compreender, analisar os diferentes tipos de máquinas computacionais, compreender dispositivos digitais baseados em portas lógicas, descrever o comportamento do hardware em função da sua arquitetura, implementar protótipos utilizando componentes de hardwares, entender os algoritmos de criptografia, conhecer técnicas de segurança da informação, para defesas de ameaças, tanto no uso pessoal quanto corporativo de sistemas computacionais, conhecer algoritmos de escalonamento de processo, conhecer principais modos de segurança em computação em nuvem e conhecer noções de computação quântica.

O presente resumo terá por objetivo exemplificar cinco aplicações dos conteúdos de base que serão estudados na UC Sistemas Computacionais e Segurança – SCS, explicando de forma detalhada cada um. Os conceitos que serão aprofundados nesse documento são: 1. Conceito, utilização, configuração e administração de sistemas operacionais; 2. Conceito e importância Segurança da informação; 3. Cybersecurity; 4. Gestão de riscos e 5. As principais ameaças digitais.

1. Conceito, utilização, configuração e administração de sistemas operacionais

Baseado no nome da disciplina e em rápidas pesquisas, pode-se identificar sistemas operacionais como um conjunto de programas que gerenciam os recursos de hardware e software de um computador, atuando como uma interface entre o usuário e o hardware. Eles são responsáveis por controlar a execução de programas, organizar

arquivos e gerenciar processos, dispositivos de entrada e saída, além de garantir a comunicação entre componentes.

Um sistema operacional é essencial para o funcionamento de qualquer dispositivo computacional. Ele facilita a execução de programas, o acesso aos dispositivos e a interação do usuário com a máquina. A administração de sistemas operacionais envolve a manutenção e monitoramento do ambiente de operação para garantir desempenho, segurança e disponibilidade. Essas são tarefas de responsabilidade de profissionais que detém o conhecimento dessa UC. São tarefas como:

- **Monitoramento de desempenho**: Acompanhamento de uso de CPU, memória, disco e rede, com ajustes conforme necessário.
- **Atualizações e patches**: Instalação de atualizações de segurança e correções de bugs para manter o sistema seguro e eficiente.
- **Backup e recuperação**: Configuração de rotinas de backup para garantir a segurança dos dados e planos de recuperação em caso de falhas.
- **Gerenciamento de usuários**: Criação, modificação e remoção de contas de usuários, além de ajuste de permissões.
- **Segurança**: Implementação de políticas de segurança, como autenticação multifator, controle de acesso, monitoramento de logs de atividades e proteção contra malware.
- **Automação de tarefas**: Utilização de scripts e ferramentas de automação para executar rotinas de manutenção, como backups, atualizações ou ajustes de configuração.

Os sistemas operacionais são fundamentais para o funcionamento de dispositivos e para a interação entre hardware e software. A sua configuração adequada e administração são cruciais para garantir que o sistema funcione de forma eficiente, segura e que atenda às necessidades dos usuários. Cada sistema operacional pode ter nuances específicas, exigindo conhecimento técnico adequado para sua utilização e manutenção.

2. Conceito e importância Segurança da informação

Segurança da informação é conceituado como um conjunto de práticas e políticas voltadas para proteger os dados e sistemas contra ameaças, como acessos não autorizados, destruição, alteração ou roubo de informações. Ela abrange a confidencialidade, que faz com que a informação só seja acessada por pessoas autorizadas, evitando vazamentos de dados sensíveis, a Integridade, que assegura que os dados não sejam alterados ou corrompidos de forma indevida, mantendo sua precisão e consistência, a disponibilidade, para que as informações e os sistemas estejam disponíveis para os usuários autorizados sempre que necessário.

Essas práticas são essenciais para que informações pessoais, financeiras ou comerciais valiosas sejam protegidas contra roubo ou divulgação não autorizada. Para prevenir ou mitigar esses riscos de ataques como phishing, malware e ransomware se tornaram mais frequentes.

Atualmente com legislações específicas, como a LGPD no Brasil e o GDPR na Europa, obrigam as empresas a garantir a segurança dos dados de seus clientes, sob risco de multas e penalidades, sendo assim, a segurança da informação é agora uma prática legal.

Além disso, em empresas, ela será a responsável por evitar vazamentos ou violações de dados podem prejudicar a confiança dos clientes e parceiros de negócios, impactando negativamente a imagem da organização. Por isso, ao garantir a integridade e a disponibilidade dos sistemas, a segurança da informação contribui para que as operações empresariais possam continuar mesmo diante de incidentes.

Sendo assim, investir em segurança da informação é essencial para proteger tanto os dados quanto a operação de empresas, organizações públicas e indivíduos em um ambiente cada vez mais digital e interconectado.

Estudar Segurança da Informação na faculdade de TI é fundamental porque o cenário digital atual enfrenta uma crescente quantidade de ameaças cibernéticas, o que torna o conhecimento sobre proteção de dados e sistemas um pilar essencial para qualquer profissional de tecnologia.

3. Cybersecurity

Cybersecurity, em português, Cibersegurança, é o campo dedicado à proteção de sistemas, redes e dados contra os ataques cibernéticos, acessos não autorizados, destruição ou alteração de informações. Envolve o uso de tecnologias, processos e práticas para garantir a integridade, confidencialidade e disponibilidade dos ativos digitais, formando uma base essencial para qualquer infraestrutura de TI.

Cybersecurity refere-se à implementação de medidas e estratégias para proteger dados, redes e dispositivos contra ameaças cibernéticas. Esse campo é composto por diversas áreas de atuação, como:

- **Segurança de rede**: Protege redes e dados em trânsito contra invasões.
- **Segurança de sistemas**: Protege servidores e dispositivos contra acessos não autorizados.
- **Segurança da informação**: Garante que as informações sensíveis sejam protegidas e mantidas de maneira confidencial e íntegra.
- **Segurança de aplicações**: Envolve a proteção de softwares e sistemas contra vulnerabilidades durante seu desenvolvimento e uso.
- **Recuperação de desastres e continuidade de negócios**: Prepara para a recuperação rápida após incidentes que possam comprometer a infraestrutura de TI.

São benefícios da Cybersecurity a proteção contra ataques cibernéticos, minimizando a vulnerabilidade a ataques como hacking, malware e ransomware, que podem causar sérios danos financeiros e reputacionais, a proteção de informações pessoais, financeiras e confidenciais de organizações, impedindo o roubo ou o vazamento de dados, a redução de perdas financeiras ao prevenir incidentes de segurança, as empresas evitam custos associados à recuperação de dados, multas regulatórias e perda de clientes. Além disso, a presença desse tipo de segurança aumenta a confiança do cliente.

Estudar Cybersecurity na faculdade de TI é fundamental não apenas por ser uma área de conhecimento em crescimento, mas porque permite aos futuros profissionais entender, prevenir e combater ameaças que podem comprometer o funcionamento de sistemas digitais. Além de proteger dados e redes, a cibersegurança desempenha um papel crucial na proteção da sociedade digital e na promoção de um ambiente de confiança nas transações e serviços online.

4. Gestão de riscos

Gestão de Riscos é o processo de identificar, avaliar e controlar ameaças potenciais que possam impactar negativamente os objetivos de uma organização, seus ativos, reputação ou operação. Essas ameaças podem vir de diversas fontes, como financeiras, operacionais, tecnológicas ou de segurança, e o gerenciamento de riscos busca reduzir ou mitigar esses impactos para garantir a continuidade dos negócios.

O processo geralmente consiste em identificar potenciais ameaças ou eventos que possam causar problemas, seja interna ou externamente, em diferentes áreas (financeira, operacional, tecnológica, etc.). Em seguida, essas ameaças ou eventos são analisados para medir a probabilidade e o impacto de cada risco identificado. Essa avaliação ajuda a priorizar quais riscos precisam de mais atenção para que em seguida seja definido o tratamento desse risco, seja para mitigar, transferir, aceitar ou evitar o risco. Isso pode envolver implementar controles, adquirir seguros ou até mudar processos operacionais.

A gestão de riscos gera benefícios como:

1. Redução de Incertezas;
2. Melhoria na tomada de decisões;
3. Prevenção de perdas;
4. Maior resiliência organizacional;
5. Conformidade regulatória;
6. Proteção da reputação;

É uma prática essencial em diversos setores e pode ser aplicada de várias maneiras. Em empresas de TI e startups a gestão de riscos é utilizada para prevenir falhas de segurança cibernética, perda de dados e interrupções de serviços. Também é fundamental no desenvolvimento de novos produtos ou tecnologias, ajudando a evitar fracassos de projetos e perdas financeiras.

Estudar Gestão de Riscos na faculdade de TI é crucial para preparar futuros profissionais para enfrentar as incertezas que surgem na implementação e operação de sistemas de tecnologia.

Com o crescimento exponencial da dependência de tecnologia e o surgimento de novas ameaças, o conhecimento sobre como identificar, avaliar e mitigar riscos é essencial para proteger dados, sistemas e operações de qualquer organização. A gestão de riscos é uma competência altamente valorizada, que capacita os profissionais a tomar decisões informadas, proteger a organização contra perdas e garantir a continuidade dos negócios em um cenário de crescente complexidade tecnológica.

5. Ameaças digitais

As principais ameaças digitais referem-se a riscos e ataques que podem comprometer sistemas, redes, dados e informações digitais. Essas ameaças vêm se tornando cada vez mais sofisticadas e frequentes à medida que a dependência da tecnologia cresce. A segurança digital depende da identificação e mitigação dessas ameaças para proteger a integridade, a confidencialidade e a disponibilidade das informações.

As principais ameaças digitais podem ser definidas como tentativas deliberadas de causar danos a sistemas digitais, redes e dados, geralmente visando roubo, manipulação, destruição ou sequestro de informações. Essas ameaças podem ter várias origens, como hackers maliciosos, organizações criminosas, falhas técnicas, ou até mesmo erros humanos.

1. Malware (Software Malicioso);
2. Phishing;
3. Ataques DDoS (Negação de Serviço Distribuída;
4. Ransomware;
5. Spyware;
6. Ataques Man-in-the-Middle (MitM;
7. Exploits de Vulnerabilidades de Software;
8. Ataques de Engenharia Social;
9. Roubo de Identidade Digital;
10. Ataques em Cloud Computing;

Sabendo identificar e combater as Ameaças Digitais o profissional é capaz de identificar e mitigar ameaças digitais ajuda a proteger informações pessoais, financeiras e empresariais, evitando vazamentos e roubos de dados, prevenir perdas financeiras oriundas de ataques cibernéticos que podem gerar grandes prejuízos financeiros, tanto pelo roubo de dinheiro quanto pelos custos de recuperação, lidar rapidamente com ameaças digitais, evitando interrupções em seus sistemas e continuar operando sem grandes interrupções. Conhecimento para proteger dados e sistemas aumenta a confiança dos clientes e parceiros, o que é crucial para manter uma boa reputação no mercado.

Além disso, ao implementar estratégias de defesa robustas contra ameaças digitais, as organizações podem reduzir a probabilidade e o impacto de futuros ataques.

Estudar as principais ameaças digitais na faculdade de TI é uma parte essencial da formação de profissionais que estarão na linha de frente da proteção contra ataques cibernéticos. Com a rápida evolução das tecnologias e o aumento das ameaças, entender e combater esses riscos se tornou uma habilidade indispensável. As ameaças digitais não afetam apenas grandes corporações, mas também indivíduos e pequenas empresas, o que faz com que o conhecimento nesse campo seja altamente valioso em praticamente qualquer setor da economia.