UC- SISTEMAS COMPUTACIONAIS E SEGURANÇA
Maria Eduarda Medeiro Porto 824144948
ORIENTADOR: Robson Calvetti

PRÁTICA 00 e 01- Introdução

ATIVIDADE 1- Introdução

”Dê outros exemplos, no mínimo 5 (cinco), de aplicações dos conteúdos de base que serão estudados na UC Sistemas Computacionais e Segurança – SCS, explicando cada um deles”

1. Criptografia

A criptografia é a prática de proteger a confidencialidade, integridade e autenticidade das informações usando algoritmos de criptografia para transformar dados de texto simples em texto cifrado ilegível. No contexto do SCS, a criptografia é usada para proteger a transmissão de dados pela Internet, proteger informações confidenciais e garantir a autenticidade das mensagens.

As aplicações de criptografia incluem:

-Transações on-line seguras (por exemplo, serviços bancários on-line, comércio eletrônico)
-Assinaturas digitais e autenticação
-Protocolos de comunicação seguros (por exemplo, HTTPS, SSH)
-Criptografia de dados para armazenamento e transmissão
-Gerenciamento de direitos digitais (DRM)

2. Proteção de dados

A proteção de dados refere-se às medidas tomadas para impedir o acesso, utilização, divulgação, modificação ou destruição não autorizada de dados sensíveis. No SCS, a proteção de dados é crucial para garantir a confidencialidade, integridade e disponibilidade dos dados.

As aplicações de proteção de dados incluem:

-Mecanismos de controle de acesso (por exemplo, senhas, biometria)
-Sistemas de backup e recuperação de dados
-Mascaramento de dados e anonimato
-Sistemas de prevenção contra perda de dados (DLP)
-Conformidade com regulamentos de proteção de dados (por exemplo, GDPR, HIPAA)

3. Políticas e Normas de Proteção de Dados

As políticas e normas de proteção de dados são diretrizes e regulamentos que as organizações devem seguir para garantir o tratamento seguro de dados sensíveis. Na SCS, estas políticas e normas são essenciais para prevenir violações de dados e garantir a conformidade com os requisitos regulamentares.

As aplicações de políticas e normas para proteção de dados incluem:

-Desenvolvimento de políticas e procedimentos de proteção de dados
-Conformidade com regulamentos de proteção de dados (por exemplo, GDPR, HIPAA)
-Programas de treinamento e conscientização de funcionários
-Planos de resposta a incidentes e recuperação de desastres
-Monitoramento e auditoria contínua das práticas de proteção de dados

4. Ameaças e vulnerabilidades

Ameaças e vulnerabilidades referem-se aos riscos e fraquezas potenciais que podem comprometer a segurança dos sistemas e dados informáticos. No SCS, compreender as ameaças e vulnerabilidades é crucial para identificar e mitigar potenciais riscos de segurança.

As aplicações de ameaças e vulnerabilidades incluem:

-Avaliação de riscos e gerenciamento de vulnerabilidades
-Modelagem de ameaças e simulação de ataque
-Teste de penetração e verificação de vulnerabilidades
-Planos de resposta a incidentes e recuperação de desastres
-Monitoramento e auditoria contínuos da segurança do sistema

5. Segurança de rede e Internet

A segurança da rede e da Internet refere-se às medidas tomadas para proteger as redes de computadores e os sistemas conectados à Internet contra acesso, uso, divulgação, modificação ou destruição não autorizados. No SCS, a segurança da rede e da Internet é essencial para prevenir ataques cibernéticos e garantir a confidencialidade, integridade e disponibilidade dos dados.

As aplicações de segurança de rede e Internet incluem:

-Firewalls e sistemas de detecção de intrusão
-Redes privadas virtuais (VPNs) e protocolos de comunicação seguros
-Segmentação de rede e controle de acesso
-Camada de soquete seguro (SSL) e segurança da camada de transporte (TLS)
-Monitoramento de rede e resposta a incidentes

6. Análise de Riscos

A análise de risco é o processo de identificar, avaliar e priorizar possíveis riscos de segurança para sistemas e dados de computador. No SCS, a análise de risco é crucial para identificar e mitigar potenciais riscos de segurança.

As aplicações de análise de risco incluem:

-gerenciamento de vulnerabilidades
-Modelagem de ameaças e simulação de ataque
-Priorização de riscos e estratégias de mitigação
-Conformidade com regulamentos de gestão de risco (por exemplo, ISO 27001)
-Monitoramento e auditoria contínuos da segurança do sistema