- **Kauê Soares Dos Santos - 824117267**
- **Leonardo Macedo Camargo - 82422817**
- **Luiz Washington de Jesus Muraro - 824148694**
- **Lucas Felipe Monteiro Suarez - 824138683**
- **George Geronimo Menezes Ferreira - 824148488**

”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”

Gerenciamento de Identidade e Acesso em Nuvem

Explicação: O Gerenciamento de Identidade e Acesso em Nuvem (ou IAM, na sigla em inglês para Identity and Access Management) é um conjunto de práticas e ferramentas utilizadas para garantir que apenas pessoas autorizadas possam acessar recursos e serviços em ambientes de nuvem.

Exemplo: Nas plataformas de computação em nuvem, o gerenciamento de identidade e acesso (IAM) permite definir quem pode acessar quais recursos e com quais permissões. Isso envolve a implementação de autenticação multifator e regras de permissão específicas para assegurar que os dados e serviços só sejam acessados por usuários e sistemas devidamente autorizados.

Monitoração e Detecção de Intrusos em Redes Corporativas

Explicação: A Monitoração e Detecção de Intrusos em Redes Corporativas refere-se a um conjunto de práticas e tecnologias destinadas a identificar e responder a atividades suspeitas ou maliciosas dentro de uma rede corporativa.

Exemplo: tentativas de invasão ou atividades maliciosas. Ao identificar essas anomalias, o IDS alerta a equipe de segurança, permitindo uma resposta rápida e mitigação de possíveis danos.

Segurança em Sistemas de Votação Eletrônica

Explicação:A Segurança em Sistemas de Votação Eletrônica refere-se ao conjunto de práticas, tecnologias e políticas aplicadas para proteger sistemas de votação eletrônica contra fraudes, manipulações e falhas.

Exemplo: Sistemas de votação eletrônica utilizam criptografia e assinaturas digitais para garantir que os votos sejam registrados de forma segura e que não possam ser alterados. Além disso, a tecnologia de blockchain pode ser usada para criar um registro transparente e imutável das transações, assegurando a integridade do processo eleitoral e evitando fraudes.

Segurança em Transações de Criptomoedas

Explicação: A segurança em transações de criptomoedas é crucial para proteger a integridade, confidencialidade e autenticidade das transações realizadas em redes de criptomoedas.

Exemplo: As criptomoedas operam em um ambiente digital descentralizado, diferentes mecanismos de segurança são implementados para evitar fraudes, roubos e outras ameaças.

Análise de Risco e Gestão de Segurança da Informação

Explicação: Analisar e gerenciar riscos é um processo contínuo para identificar e avaliar ameaças potenciais à segurança da informação. Estudar como realizar avaliações de risco, criar matrizes de risco e implementar medidas de mitigação ajuda a proteger os ativos da organização de forma proativa, ajustando as políticas e controles de segurança conforme necessário.

Exemplo: Realização de avaliações de risco para identificar e mitigar potenciais ameaças e vulnerabilidades.

Segurança Física e Ambiental

Explicação: A segurança não se restringe ao digital; a proteção física dos recursos computacionais é igualmente importante. Estudar e implementar controles como câmeras de segurança, sistemas de controle de acesso e monitoramento de temperatura e umidade em centros de dados ajuda a proteger contra danos físicos e acessos não autorizados.

Exemplo: Implementação de controles físicos e ambientais em centros de dados, como sistemas de controle de acesso físico e monitoramento ambiental.

Forense Digital

Explicação: A forense digital é a aplicação de técnicas científicas e analíticas para investigar incidentes cibernéticos e crimes digitais. Isso inclui a coleta, preservação e análise de evidências digitais para descobrir como ocorreu um ataque, quem foi o responsável e quais dados foram comprometidos.

Exemplo: Análise de logs e rastros digitais para entender como um ataque foi realizado, identificar os responsáveis e determinar quais dados ou sistemas foram comprometidos.

Arquitetura de Sistemas Computacionais

Explicação: Compreender a arquitetura de sistemas permite projetar servidores que possam lidar eficientemente com grandes volumes de tráfego e dados. Isso envolve o balanceamento de carga, o uso de clusters e a otimização de recursos para garantir alta disponibilidade e desempenho

Exemplo: Design e otimização de arquiteturas de servidores para suportar aplicações de alta demanda.

Avaliação e Gestão de Risco de Terceiros

Explicação: Terceiros que acessem dados ou sistemas podem representar um risco. Estudar e implementar processos para avaliar e gerenciar esses riscos ajuda a proteger contra possíveis vulnerabilidades introduzidas por parceiros e fornecedores.

Exemplo: Avaliação de riscos associados a fornecedores e terceiros que têm acesso a sistemas e dados da organização.

Segurança em Ambientes de Desenvolvimento e Teste

Explicação: Ambientes de desenvolvimento e teste podem ser alvos de ataques ou inadvertidamente expor dados sensíveis. Estudar e aplicar práticas de segurança para proteger esses ambientes ajuda a garantir que a segurança não seja comprometida durante o desenvolvimento e teste.

Exemplo: Implementação de controles de segurança em ambientes de desenvolvimento e teste para proteger dados e sistemas.

Segurança em Internet das Coisas (IoT)

Explicação: A segurança em IoT abrange a proteção de dispositivos conectados à internet, como sensores, câmeras, e dispositivos inteligentes. Devido à sua natureza distribuída e muitas vezes limitada em capacidade de processamento, garantir a segurança desses dispositivos é crucial para evitar ataques como sequestro de dispositivos (botnets) ou roubo de dados.

Exemplo: Implementação de protocolos de segurança para proteger dispositivos domésticos, como câmeras de segurança, termostatos inteligentes e sistemas de iluminação, contra ataques e invasões.

Engenharia Social e Segurança da Informação

Explicação: A engenharia social é a manipulação psicológica de pessoas para realizar ações ou divulgar informações confidenciais. Ensinar os usuários a reconhecer e resistir a técnicas de engenharia social, como phishing, é uma aplicação crítica na segurança da informação.

Exemplo: Realização de simulações de phishing para testar a resiliência dos funcionários e identificar vulnerabilidades que precisam ser corrigidas.

Segurança em DevOps (DevSecOps)

Explicação: DevSecOps integra práticas de segurança ao longo do ciclo de vida de desenvolvimento de software, desde o planejamento até a implementação e

manutenção. Isso inclui automação de testes de segurança e integração contínua de controles de segurança, garantindo que o software seja seguro desde o início.

Exemplo: Implementação de pipelines CI/CD que integram verificações automáticas de segurança, como análise de código estática, testes de penetração automatizados e gerenciamento de vulnerabilidades.

Resiliência Cibernética

Explicação: Resiliência cibernética refere-se à capacidade de uma organização de se preparar, responder e se recuperar de incidentes cibernéticos. Isso inclui a implementação de estratégias que permitem manter a continuidade dos negócios e minimizar os impactos de ataques ou falhas de segurança.

Exemplo: Desenvolvimento de planos de continuidade que garantam a operação ininterrupta dos serviços críticos, mesmo em caso de incidentes cibernéticos graves.

Segurança de Sistemas Operacionais

Explicação: práticas e técnicas empregadas para proteger um sistema operacional contra ameaças, ataques e acessos não autorizados. O sistema operacional (SO) é o software fundamental que gerencia o hardware do computador e fornece serviços para outros softwares, tornando-o um alvo crítico para ataques.

Exemplo: Atualizações de segurança do Windows para corrigir vulnerabilidades conhecidas.Sistema de permissões no Linux que usa chmod e chown para gerenciar o acesso a arquivos e diretórios.