📌 PLANEJAMENTO DAS AULAS DO CURSO DE SEGURANÇA DA INFORMAÇÃO

**Módulo 1: Introdução à Segurança da Informação (10h)**

✅ Objetivo: Apresentar conceitos fundamentais de segurança da informação e sua importância.

**Aula 1 – Fundamentos da Segurança da Informação (2h)**

📌 Conceitos básicos: Confidencialidade, Integridade, Disponibilidade (CIA).

📌 Tipos de ameaças e ataques cibernéticos (malware, phishing, ransomware).

📌 Histórico da cibersegurança e casos famosos de ataques.

**Aula 2 – Políticas e Princípios de Segurança (2h)**

📌 O que são políticas de segurança e sua importância.

📌 Princípios de defesa em profundidade.

📌 Modelos de segurança: Zero Trust, Defense in Depth, Least Privilege.

**Aula 3 – Ferramentas e Boas Práticas (3h)**

📌 Firewalls, antivírus e sistemas de prevenção/detecção de intrusão (IDS/IPS).

📌 Engenharia social e boas práticas para proteção contra ataques.

📌 Demonstração prática: análise de um ataque real (exemplo: phishing).

**Aula 4 – Atividade Prática e Discussão (3h)**

📌 Análise de um caso real de vazamento de dados.

📌 Exercícios de identificação de vulnerabilidades em cenários fictícios.

**Módulo 2: Criptografia e Segurança de Dados (10h)**

✅ Objetivo: Ensinar os princípios da criptografia e sua aplicação na proteção de dados.

**Aula 1 – Introdução à Criptografia (2h)**

📌 O que é criptografia e sua importância na segurança digital.

📌 Tipos de criptografia: simétrica vs assimétrica.

📌 Conceitos básicos: chave pública e privada, assinatura digital.

**Aula 2 – Algoritmos de Criptografia (3h)**

📌 Principais algoritmos: AES, RSA, SHA-256, ECC.

📌 Certificados digitais e SSL/TLS.

📌 Laboratório: Implementação de criptografia AES e RSA com Python.

**Aula 3 – Proteção de Dados e LGPD (2h)**

📌 Conceitos de proteção de dados e privacidade.

📌 Aplicação da criptografia em bancos de dados e armazenamento em nuvem.

📌 Exemplos de vazamentos e impacto na legislação.

**Aula 4 – Atividade Prática e Desafios (3h)**

📌 Decifrando mensagens criptografadas (atividade prática).

📌 Simulação de um ataque de força bruta a um hash MD5.

**Módulo 3: Controle de Acesso e Autenticação (10h)**

✅ Objetivo: Ensinar técnicas e mecanismos para controle de acesso seguro.

**Aula 1 – Modelos de Controle de Acesso (3h)**

📌 Controle de acesso baseado em regras (RBAC) e atributos (ABAC).

📌 Implementação de controle de acesso no Windows e Linux.

📌 Demonstração prática: configuração de permissões e ACLs.

**Aula 2 – Autenticação e MFA (3h)**

📌 Métodos de autenticação: senha, biometria, token, certificados.

📌 Implementação do Multi-Factor Authentication (MFA).

📌 Simulação: Como um atacante pode burlar autenticação fraca.

**Aula 3 – Gerenciamento de Identidade (4h)**

📌 Conceito de IAM (Identity and Access Management).

📌 Ferramentas: Active Directory (AD), Azure AD, Okta.

📌 Laboratório: Criando um grupo de usuários com controle de acesso no AD.

**Módulo 4: Gestão de Riscos e Continuidade de Negócios (10h)**

✅ Objetivo: Ensinar a identificar e mitigar riscos de segurança.

**Aula 1 – Introdução à Gestão de Riscos (3h)**

📌 Conceitos: Threat Modeling, análise de impacto, avaliação de risco.

📌 Matriz de risco: probabilidade vs impacto.

📌 Estudo de caso: análise de um ataque real e seus impactos.

**Aula 2 – Plano de Continuidade de Negócios (3h)**

📌 Desenvolvimento de um plano de continuidade.

📌 Backups e Disaster Recovery (RTO/RPO).

📌 Exercício: Criando um plano de resposta a incidentes.

**Aula 3 – Simulação Prática (4h)**

📌 Simulação de um ataque ransomware e resposta da equipe.

📌 Análise pós-incidente e melhorias no plano de continuidade.