## Etapa 1: Contexto e Princípios de Segurança da Informação

**Descrição do Cenário:**
O cenário escolhido é uma **loja virtual** de venda de cursos com atuação nacional. A plataforma oferece uma variedade de cursos online em diversas áreas do conhecimento, incluindo áreas técnicas, pessoais e corporativas. A loja virtual não só gerencia transações financeiras de clientes, mas também armazena dados pessoais e históricos de atividades dos alunos, além de proteger o conteúdo dos cursos oferecidos. O ambiente exige uma segurança robusta para garantir que os dados dos alunos, as transações financeiras e o conteúdo digital dos cursos estejam protegidos contra acessos não autorizados e danos.

**Inventário Básico de Recursos de TI:**

1. **Hardware:**
   - Servidores para hospedagem da plataforma de cursos e bancos de dados.
   - Equipamentos de backup e dispositivos de redundância (servidores de backup, NAS).
   - Equipamentos de trabalho, como computadores, notebooks e dispositivos móveis usados pela equipe de suporte, administradores e gerentes
   - Dispositivos de segurança de rede, como firewalls e roteadores.

2. **Software:**
   - Plataforma de e-commerce para venda de cursos (interface de usuários, portal do aluno e gestão do conteúdo).
   - Sistemas de pagamento integrados com gateways de pagamento seguros.
   - Ferramentas de monitoramento de rede, firewalls e antivírus.
   - Sistema de gerenciamento de aprendizagem (LMS) para controle dos cursos e dos dados dos alunos.

3. **Redes:**
   **-** Conexões de rede de alta capacidade, com redundância e failover.
   - VPN para conexões remotas seguras para funcionários ou prestadores de serviços.
   - Certificados SSL/TLS para garantir a segurança das transações online e proteção de dados sensíveis.

4. **Dados Sensíveis:**
   - Dados pessoais dos clientes (nome, e-mail, CPF, endereço, dados bancários).
   - Histórico de compras de cursos e registros de participação.
   - Conteúdo de cursos e materiais protegidos por direitos autorais.

**Principios de segurança:**

## Etapa 2: Ameaças, Vulnerabilidades e Normas de Segurança

1. **Ameaças Técnicas:**

**Malware**:
- **Definição**: Software malicioso que pode infectar sistemas, roubar informações, danificar dados e comprometer o funcionamento da loja.
- **Exemplo**: Vírus, trojans ou ransomware que infectam o sistema de pagamento ou os servidores da loja, comprometendo dados financeiros dos clientes.
- **Vulnerabilidade**: Falhas nos sistemas de defesa, como falta de antivírus,

**Phishing**:
- **Definição:** Ataques de engenharia social em que criminosos tentam enganar usuários para que forneçam informações pessoais, como login, senha e dados financeiros.
- **Exemplo:** E-mails fraudulentos ou mensagens de SMS que simulam a loja, solicitando que o cliente forneça suas credenciais de pagamento ou acesso.
- **Vulnerabilidade:** Falta de conscientização de usuários sobre as práticas de phishing ou ausência de autenticação de dois fatores (2FA) para verificar a identidade dos clientes.

**Injeção de SQL (SQL Injection)**:
- **Definição:** Exploração de falhas em um banco de dados onde um atacante insere comandos SQL maliciosos para acessar ou manipular dados sensíveis.
- **Exemplo:** O atacante pode obter acesso a dados de clientes, como nome, endereço e histórico de compras.
- **Vulnerabilidade:** Falta de validação de entrada no formulário de login ou falta de criptografia dos dados no banco de dados.

**Cross-Site Scripting (XSS)**:
- **Definição:** Exploração de falhas em sites que permitem a execução de scripts maliciosos no navegador do usuário.
- **Exemplo:** Inserção de código malicioso em campos de comentário ou chat ao vivo que rouba credenciais do cliente.
- **Vulnerabilidade:** Ausência de sanitização de entradas de usuários, permitindo o armazenamento e execução de scripts maliciosos.

**Falta de Criptografia de Dados Sensíveis**:
- **Definição:** Dados sensíveis, como informações de pagamento ou dados pessoais, não são protegidos adequadamente.
- **Exemplo:** Transações financeiras ou dados de login transmitidos em texto simples ou armazenados sem criptografia.
- **Vulnerabilidade:** Uso de protocolos inseguros (HTTP ao invés de HTTPS) ou falta de criptografia de dados no banco de dados.

2. **Ameaças Físicas e Operacionais:**

**Acesso Físico Não Autorizado**:
- **Definição:** Acesso indevido aos servidores ou instalações que hospedam o sistema da loja virtual.
- **Exemplo:** Funcionários com privilégios inadequados acessando dados sensíveis de clientes.

- **Vulnerabilidade:** Falta de controle de acesso físico e monitoramento em locais sensíveis.

**Interrupções no Serviço** (Ex.: DDoS):
- **Definição:** Ataques de negação de serviço distribuída (DDoS) que sobrecarregam servidores e deixam a loja indisponível para os clientes.
- **Exemplo:** Os atacantes enviam um volume massivo de tráfego para derrubar a loja online.
- **Vulnerabilidade:** Falta de proteção contra DDoS, como sistemas de mitigação de tráfego ou CDNs (Content Delivery Networks).

3. **Ameaças de Engenharia Social:**

**Engenharia Social**:
- **Definição:** Manipulação de indivíduos para que revelem informações confidenciais, como senhas ou dados de acesso ao sistema.
- **Exemplo:** Um atacante se passa por um funcionário de TI e solicita informações de login de administradores do site ou dados bancários de clientes.
- **Vulnerabilidade:** Falta de treinamento adequado para os funcionários, resultando em descuido ao lidar com informações sensíveis.

**Spear Phishing**:
- **Definição:** Ataques direcionados a funcionários ou clientes específicos, com o objetivo de coletar dados confidenciais ou realizar fraudes financeiras.
- **Exemplo:** Um atacante finge ser um fornecedor ou parceiro comercial da loja e envia um e-mail com um link ou anexo malicioso.
- **Vulnerabilidade:** Falta de vigilância e ceticismo por parte dos funcionários e clientes quanto a e-mails suspeitos.