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.

4. **Vulnerabilidades Relacionadas a Processos**

Gestão de Identidade e Acessos:
Definição: Falhas na gestão de privilégios de usuários podem permitir que pessoas não autorizadas acessem áreas críticas do sistema.
Exemplo: Funcionários com acessos elevados (administradores) que deixam as credenciais compartilhadas ou não são removidos quando deixam a empresa.
Vulnerabilidade: Falta de políticas claras de controle de acesso, como a prática de "privilégio mínimo" e o uso inadequado de senhas compartilhadas.

Segurança na Plataforma de Pagamento:
- **Definição:** Vulnerabilidades no sistema de pagamento online da loja podem permitir a interceptação de transações e dados financeiros.
- **Exemplo:** Implementação de um gateway de pagamento vulnerável a ataques ou falhas no processo de verificação de transações.
- **Vulnerabilidade:** Uso de métodos de pagamento inseguros ou falta de compliance com normas de segurança como PCI DSS (Payment Card Industry Data Security Standard).

5. Ameaças de Conformidade Legal

Violação da LGPD (Lei Geral de Proteção de Dados):
- **Definição:** Falhas no processo de coleta, armazenamento ou compartilhamento de dados pessoais dos clientes, resultando em violação da LGPD.
- **Exemplo:** Dados de clientes sendo vendidos ou usados sem o consentimento adequado, ou sem a devida proteção e anonimização.
- **Vulnerabilidade:** Falta de políticas claras de privacidade ou consentimento do cliente para coleta e processamento de dados.

Falta de Conformidade com Regulamentos de Segurança de Dados:
- **Definição:** Não seguir as melhores práticas e regulamentações do setor para proteger os dados dos clientes.
- **Exemplo:** Não seguir os requisitos de segurança obrigatórios para proteger informações sensíveis como CPF, número de cartão de crédito, etc.
- **Vulnerabilidade:** Falta de auditorias regulares ou treinamentos sobre compliance, levando a falhas na proteção dos dados dos clientes.

- **Identificação de normas, leis e regulamentações** pertinentes (ex.: ISO 27001, LGPD, marco civil da internet, políticas internas).

Etapa 3: Boas Práticas e Gestão de Risco

- **Boas práticas** recomendadas (uso de senhas fortes, políticas de backup, criptografia, antivírus, conscientização de usuários, etc.);
- **Estrutura de gestão de risco** (avaliação, tratamento e monitoramento de riscos; referências teóricas, planilhas de análise de risco);

Etapa 4: Gestão de Continuidade do Negócio

- **Noções de Plano de Continuidade de Negócio (PCN)** para o cenário:
  - ✓ Identificação de processos críticos;
  - ✓ Estratégias de recuperação;
  - ✓ Plano de contingência (procedimentos de emergência, responsáveis, comunicação etc.).

No **final do semestre**, cada grupo deve entregar um **relatório escrito** (ou um documento em formato digital) e/ou **apresentar** em sala de aula o resultado de suas análises, destacando como cada parte da ementa foi aplicada ao cenário.

2. Divisão de Responsabilidades no Grupo (4 alunos)

Embora todos contribuam para cada parte, sugere-se uma divisão clara para otimizar o trabalho:

1. **Coordenador / Editor-Chefe**
   a. Responsável por organizar prazos, tarefas e comunicação interna do grupo.
   b. Faz a integração de todos os capítulos no documento final, revisa ortografia e formatação.
   c. Também colabora na pesquisa de normas e referências (item 3.1 ou 8.3 da ementa).
2. **Analista de Ameaças e Vulnerabilidades**
   a. Foca principalmente na etapa 2 do trabalho (identificar e descrever as ameaças e vulnerabilidades do cenário).
   b. Faz a ponte entre os problemas de segurança mapeados e as soluções/boas práticas (etapa 3).
3. **Analista de Boas Práticas e Gestão de Risco**
   a. Dedica-se a levantar políticas, processos e ferramentas de segurança adequadas à organização (etapa 3).
   b. Elabora o plano de mitigação de riscos (ou seja, como tratar cada risco identificado).
4. **Analista de Continuidade de Negócios**

a. Assume a etapa 4, detalhando o Plano de Continuidade de Negócio (PCN).
b. Garante que as soluções propostas dialoguem com as práticas de segurança e gerenciamento de risco.

É importante ressaltar que a **responsabilidade** é para efeito de organização, mas o grupo deve trabalhar **colaborativamente**, revisando e dando suporte a todos os capítulos.

3. Caminhos para Resolução do Projeto

Abaixo, um roteiro geral de como o grupo pode conduzir o trabalho ao longo do semestre:

1. **Escolha do Cenário e Planejamento Inicial (Semanas 1-2)**
    a. Discutir ideias de empresas/organizações fictícias ou reais.
    b. Delimitar o tamanho, a área de atuação e o tipo de informação crítica manipulada.
    c. Definir a divisão de papéis (coordenador, analistas etc.).
2. **Coleta de Informações e Fundamentação Teórica (Semanas 3-6)**
    a. Pesquisar referências nos livros e materiais indicados (bibliografia básica e complementar).
    b. Coletar dados para identificar ativos de TI, serviços, possíveis ameaças e vulnerabilidades.
    c. Iniciar a escrita do *rascunho* da Etapa 1 (contexto e princípios) e da Etapa 2 (ameaças e vulnerabilidades).
3. **Análise de Riscos e Propostas de Boas Práticas (Semanas 7-10)**
    a. Com base na lista de vulnerabilidades, identificar o nível de risco (ex.: probabilidade x impacto).
    b. Elaborar políticas de segurança e boas práticas alinhadas às normas pertinentes.
    c. Registrar tudo em um formato claro (tabelas, fluxos, diagramas).
4. **Desenvolvimento do Plano de Continuidade e Consolidação (Semanas 11-13)**
    a. Criar um esboço do PCN, incluindo identificação de processos críticos e estratégias de resposta.
    b. Revisar se o PCN abrange as ameaças/vulnerabilidades principais já levantadas.
    c. Incluir aspectos de governança (quem faz o quê em caso de incidentes, contatos de emergência etc.).
5. **Finalização e Apresentação (Semanas 14-15)**
    a. Revisar e padronizar o documento final.
    b. Preparar uma **apresentação** (slides, pôster ou seminário) para compartilhar as principais conclusões.
    c. Destacar lições aprendidas e sugestões para evoluir o plano no futuro.

4. Recomendações de Sucesso

- **Organização e Cronograma**: Utilizar ferramentas de gestão de projetos (ex.: Trello, Microsoft Planner ou Google Planilhas) para acompanhar o andamento das tarefas.
- **Pesquisa e Referências**: Apoiar-se sempre em materiais confiáveis, como os livros de bibliografia básica (CABRAL & CAPRINO, HINTZBERGEN et al., STANEK) e complementar (BARRETO & BRASIL, GALVÃO, MANOEL, STALLINGS, VANCIM).
- **Validação do Trabalho**: Conversar com o professor, apresentar rascunhos e receber feedback periódico para ajustes.
- **Clareza e Qualidade**: Garantir que o relatório final seja objetivo, coerente e apresente exemplos práticos onde possível.
- **Ética e Contribuição de Todos**: O trabalho em grupo exige divisão de tarefas e colaboração. Cada membro deve produzir conteúdo original, evitar plágio e contribuir ativamente.

Cronograma de apresentações

- **Início oficial do projeto** em 10/03, conforme solicitado;
- Aulas às segundas-feiras, das 19h30 às 21h30;
- Feriados/ausências já previstos (03/03 – Carnaval; 21/04 – Tiradentes);
- Prazo para encerramento do semestre em 15/06.

O foco aqui está nas **entregas / apresentações** relativas ao andamento do projeto, que será desenvolvido ao longo das semanas, integrado aos conteúdos da disciplina.

Visão Geral do Cronograma de Apresentações

Data	Atividade / Entrega
10/03	**Início do Projeto** - Orientações gerais sobre o trabalho - Formação de grupos (4 alunos) - Definição preliminar dos papéis (coordenador, analistas etc.)
17/03	Aula regular (continuação dos conteúdos); grupos trabalham no projeto internamente (sem apresentação formal).
24/03	**Apresentação 1** (curta) - **Proposta do cenário** escolhido (empresa/instituição fictícia ou real) - Justificativas e delimitação do escopo (quais ativos/dados são críticos).
31/03	Aula regular; grupos utilizam para avançar nas pesquisas.
07/04	Aula regular; aprofundamento teórico (conforme ementa).
14/04	**Apresentação 2** - **Mapeamento de ameaças e vulnerabilidades** inicial - Referência a normas pertinentes (ISO 27001, LGPD, etc.) - Discussão das principais descobertas até o momento.

21/04	**Feriado (Tiradentes) – Sem aula.**
28/04	**Apresentação 3** - **Propostas de boas práticas** (controle de acesso, senhas, backups, criptografia etc.) - Diretrizes iniciais para **gestão de risco** (métodos de classificação e tratamento).
05/05	Aula regular; grupos trabalham no refinamento do projeto.
12/05	Aula regular; foco em conteúdos complementares e dúvidas.
1G/05	**Apresentação 4** - **Rascunho do Plano de Continuidade de Negócio (PCN)** - Demonstração de como o PCN cobre as vulnerabilidades e riscos já levantados.
26/05	Aula regular; consolidação dos resultados e preparo final.
02/06	**Apresentação Final** - **Entrega do trabalho completo** (documento) - Exposição dos resultados (slide ou seminário) para a turma, com o resumo das etapas: • Cenário, ameaças, normas e boas práticas • Gestão de risco e PCN - Espaço para perguntas e debate.
0G/06	Reservado para eventuais complementos ou ajustes finais (caso necessário) e possíveis revisões do conteúdo geral da disciplina.
15/06	Encerramento oficial do semestre.

Detalhes Complementares

1. **Distribuição dos Papéis**: Reforçar, no dia 10/03, quem será o coordenador/editor-chefe do grupo e quem ficará responsável pelos tópicos de (a) ameaças e vulnerabilidades, (b) boas práticas e gestão de risco e (c) continuidade de negócio.
2. **Formato das Apresentações**:
    a. As “Apresentações Curtas” (24/03, 14/04, 28/04, 19/05) podem ter de 10 a 15 minutos, focando em **resultados parciais** ou **dúvidas específicas**.
    b. A “Apresentação Final” (02/06) terá tempo maior (sugerido 15-20 minutos por grupo) para mostrar a visão integrada do trabalho.
3. **Relatório / Documento Final**:
    a. Deve consolidar todas as partes (cenário, ameaças, normas, boas práticas, gestão de risco, plano de continuidade).
    b. Pode ser entregue em formato PDF, com padronização de fontes, tabelas, diagramas, sempre citando as **bibliografias básica e complementar** quando necessário.
4. **Integração com o Conteúdo da Disciplina**:

    a. A cada tópico da ementa visto em aula (princípios, vulnerabilidades, normas, etc.), os grupos atualizam seu projeto.
    b. Dessa forma, teoria e prática avançam juntas.
5. **Uso do Tempo em Sala**:
    a. Entre as datas de apresentação, os grupos têm aulas regulares para absorver novos conteúdos e usar parte do tempo para discussão/progressão interna do projeto.
    b. É aconselhável que o professor dedique **alguns minutos** em cada encontro para esclarecer dúvidas e acompanhar o progresso dos grupos.