1. Proposta Geral do Projeto

Cada grupo (composto por 4 alunos) deverá **selecionar** (ou criar) um cenário de uma empresa ou instituição que necessite de um **Plano Básico de Segurança da Informação**. Esse cenário pode ser:

- Uma pequena ou média empresa de tecnologia,
- Uma loja virtual,
- Uma organização governamental ou não governamental,
- Qualquer ambiente que utilize sistemas computacionais e manipule dados sensíveis.

A partir desse cenário, o grupo deverá **desenvolver**:

1. **Análise de ameaças e vulnerabilidades** do ambiente;
2. **Normas e boas práticas** aplicáveis;
3. **Políticas de gestão de risco**;
4. **Recomendações de continuidade de negócio** (plano de contingência básico).

Esses pontos correspondem aos **tópicos essenciais** da ementa (princípios de segurança, ameaças e vulnerabilidades, normas, boas práticas, gestão de risco e continuidade de negócios).

2. Estrutura Sugerida do Trabalho

Para contemplar toda a ementa, o trabalho pode ser organizado em **quatro grandes etapas** (ou capítulos), com cada integrante focando em uma área principal. Entretanto, é fundamental que todos colaborem em cada etapa, mesmo que um membro seja o responsável principal.

Etapa 1: Contexto e Princípios de Segurança da Informação

- **Descrição do cenário** (empresa/organização escolhida);
- **Inventário básico** de recursos de TI (hardware, software, redes, dados sensíveis);
- **Princípios de segurança** aplicados (confidencialidade, integridade e disponibilidade - CID).

Etapa 2: Ameaças, Vulnerabilidades e Normas de Segurança

- **Mapeamento de possíveis ameaças e vulnerabilidades** no cenário escolhido (ex.: malware, phishing, engenharia social, falhas de configuração etc.);

- **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.

3. 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.

4. 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.

5. 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.