

Para desenvolver o projeto de implementação e gestão de um SGSI conforme a ISO/IEC 27001, os alunos devem seguir um roteiro estruturado que abrange pesquisa, planejamento, execução e revisão. Aqui está um guia detalhado:

### 1. Pesquisa e Educação:

- **O que Pesquisar:** Norma ISO/IEC 27001, tipos de ativos de informação, ameaças à segurança, métodos de avaliação de riscos, controles de segurança recomendados.
- **Como Pensar:** Abordagem crítica para identificar quais partes da norma são mais relevantes para o contexto escolhido; considerar a aplicabilidade e eficácia dos controles de segurança.

### 2. Planejamento:

- **Definição de Escopo:** Decidir quais áreas da organização ou quais sistemas de TI serão incluídos no SGSI.
- **Papeis:** Definir líderes de projeto, responsáveis pela avaliação de riscos, implementação de controles, treinamento, monitoramento e gestão de incidentes.

### 3. Execução:

- **Avaliação de Riscos:** Identificar, analisar e avaliar riscos. Usar ferramentas como análises SWOT ou matrizes de risco.
- **Implementação de Controles:** Escolher e aplicar controles baseados na avaliação de riscos para mitigar ameaças identificadas.
- **Treinamento e Conscientização:** Organizar sessões de treinamento para todos os envolvidos, enfatizando a importância de seguir as políticas de segurança.

### 4. Monitoramento e Revisão:

- **Auditorias:** Realizar auditorias regulares para garantir a conformidade com a ISO/IEC 27001 e a eficácia dos controles implementados.
- **Gestão de Incidentes:** Estabelecer procedimentos para responder a incidentes de segurança, aprendendo com eles para melhorar o SGSI continuamente.

### 5. Uso do Jira:

- **Organização do Projeto:** Utilizar o Jira para criar epics e stories que correspondam a cada etapa do projeto, atribuindo tarefas específicas aos membros da equipe.
- **Monitoramento:** Acompanhar o progresso do projeto por meio de sprints, utilizando o quadro de Kanban ou Scrum no Jira para visualizar o fluxo de trabalho.

### Papéis dos Alunos:

- **Líder do Projeto:** Coordenação geral e comunicação entre a equipe e stakeholders.
- **Especialista em Avaliação de Riscos:** Conduz a avaliação de riscos e recomenda controles.
- **Especialista em Implementação de Controles:** Responsável por implementar os controles recomendados.

- **Oficial de Conformidade:** Garante que o projeto esteja em conformidade com a norma ISO/IEC 27001.
- **Gerente de Incidentes:** Desenvolve e implementa o plano de gestão de incidentes.