**Análise de Riscos**

**Identificação e Avaliação de Riscos:** Precisamos considerar questões como perda de dados acessa não autorizada a informações dos usuários, e possíveis interrupções no sistema que poderiam afetar os serviços da biblioteca.

**Avaliação de Vulnerabilidades:** Devemos examinar se o sistema tem falhas de segurança que poderiam permitir o acesso não autorizado ou comprometimento dos dados.

**Ameaças Potenciais:** Isso inclui desde ataques cibernéticos até roubo físico de dispositivos que contenham informações sensíveis.

* **Implementação de Medidas de Segurança**

**Implementação de Políticas de Controle de Acesso:**

Devemos estabelecer políticas claras sobre quem pode acessar o catálogo de livros, informações dos usuários e dados administrativos da biblioteca.

**Autenticação Forte:** É importante garantir que os usuários só possam acessar o sistema através de credenciais seguras, como senhas fortes ou cartões de acesso.

**Configuração de Sistemas de Detecção e Prevenção de Intrusões:** Devemos configurar sistemas de detecção de intrusões para identificar padrões suspeitos de atividade que possam indicar tentativas de acesso não autorizado.

**Prevenção de Ataques:** Isso inclui medidas como firewalls, criptografia de dados e atualizações regulares de segurança para proteger o sistema contra malware, phishing e outras ameaças cibernéticas.

**Testes de Penetração:** Devemos realizar testes regulares para identificar e corrigir quaisquer vulnerabilidades no sistema antes que elas possam ser exploradas por invasores.