**Semana 2 – Pesquisa Inicial e Estruturação do Projeto**

**Atividades:**

* ***Pesquisar normas de segurança da informação (ISO 27001, LGPD).***

ISO 27001:

A ISO/IEC 27001 é uma norma internacional para a implementação de um Sistema de Gestão da Segurança da Informação. Ela estabelece um conjunto de boas práticas para garantir a proteção de dados, minimizar riscos e assegurar a continuidade do negócio.

LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018):

A LGPD é a legislação brasileira que regula o tratamento de dados pessoais por empresas e organizações, visando garantir a privacidade dos usuários.

**Normas ISO 27001:**

**Gestão de Acessos e Controles (A.9)**

Implementar autenticação forte (ex.: autenticação de dois fatores - 2FA).

Restringir acessos com base no princípio do "menor privilégio" (somente usuários autorizados podem acessar determinados dados).

Criar logs de auditoria para monitoramento de acessos e alterações.

**Proteção contra Ameaças e Vulnerabilidades (A.12)**

Usar firewalls e sistemas de detecção de intrusos (IDS/IPS).

Aplicar criptografia em dados sensíveis (como dados de cartões de crédito e senhas de clientes).

Atualizar frequentemente os softwares para corrigir vulnerabilidades.

**Normas LGPD:**

**Coleta e Tratamento de Dados (Art. 6 e 7):**

Coletar apenas os dados necessários para a finalidade informada ao usuário.

Obter **consentimento explícito** antes de armazenar dados pessoais.

**Segurança e Proteção de Dados (Art. 46 a 49):**

Adotar **medidas técnicas e organizacionais** para proteger os dados contra acessos não autorizados, vazamentos e destruição acidental.

Implementar **criptografia e anonimização** para dados sensíveis.

* ***Definir os princípios básicos de segurança para a loja virtual (Confidencialidade, Integridade, Disponibilidade - CID).***

**Confidencialidade:**

A confidencialidade assegura que apenas usuários autorizados tenham acesso às informações sensíveis da loja virtual, protegendo dados de clientes, informações financeiras e credenciais de acesso.

**Medidas/Normas para garantir a Confidencialidade:**

* Criptografia de dados sensíveis, como senhas e informações de pagamento.
* Controle de acessos assim garantindo que apenas funcionários autorizados tenham permissão para visualizar determinados dados.
* Autenticação de dois fatores (2FA) para acessos administrativos e áreas restritas.

**Integridade:**

A integridade garante que as informações da loja virtual sejam precisas, confiáveis e não alteradas indevidamente. Isso evita fraudes, modificações não autorizadas e corrupção de dados.

**Medidas para garantir a Integridade:**

* Backups periódicos para evitar perda de dados em caso de falhas.
* Registro de logs de auditoria para monitorar alterações no sistema.
* Uso de assinaturas digitais e validações para verificar a autenticidade das informações.
* Proteção contra ataques de injeção de SQL e outras técnicas que possam comprometer os dados armazenados.

**Disponibilidade:**

A disponibilidade garante que a loja virtual esteja sempre acessível e funcionando, mesmo diante de altos volumes de acessos, falhas técnicas ou ataques cibernéticos.

**Medidas para garantir a Disponibilidade:**

* Hospedagem em servidores confiáveis e escaláveis (ex.: AWS, Azure, Google Cloud).
* Proteção contra ataques DDoS, que podem derrubar o site.
* Redundância de servidores, para garantir que, se um falhar, outro assuma a operação.
* **Criar um esboço do relatório com a introdução do projeto.**

**Introdução**

O objetivo deste projeto é o desenvolvimento de uma **loja virtual** que priorize a **segurança da informação**. Considerando o crescente número de usuários acessando plataformas digitais, a proteção de dados e a integridade dos sistemas são essenciais. A nossa loja será projetada com foco na **confidencialidade**, **integridade** e **disponibilidade** dos dados dos usuários e transações realizadas.

Este relatório abordará as normas de segurança aplicáveis ao projeto, como a **ISO 27001** e a **LGPD**, e como essas normas serão implementadas para garantir a segurança e a conformidade da loja virtual.