**Avaliação dos Riscos de Segurança e Privacidade**

Nome do consultor de segurança da equipe: Thyago Marques Correa

**1. Partes do projeto que exigem alterações antes da liberação**

* Autenticação e Controle de Acesso:
  + Revisão da implementação de RBAC (Role-Based Access Control) para garantir que usuários (administradores, supervisores e clientes) tenham permissões claras e segregadas (RF-02, RF-06, RF-13).
  + Validação do armazenamento seguro de senhas (hashing com algoritmos como bcrypt) e proteção contra ataques de força bruta.
* Integração com WhatsApp Business:
  + Garantir que os dados do cliente (Nome, CPF, telefone) sejam transmitidos via API segura (HTTPS) e que o WhatsApp Business utilize criptografia de ponta a ponta (RF-10).
* Validação de Dados:
  + Implementar sanitização de entradas para evitar injeções de SQL/XSS em formulários (RF-08, RF-09, RF-12).

**2. Partes do projeto que exigem revisão do design de segurança**

* Gestão de Usuários (RF-02):
  + Revisão do fluxo de cadastro/edição de usuários internos para evitar escalonamento de privilégios.
* Controle de Estoque (RF-01, RF-06):
  + Auditoria do mecanismo de atualização de estoque em tempo real (RNF-06) para evitar condições de corrida ou inconsistências.
* Catálogo Online (RF-05, RF-08):
  + Validação da exposição segura de dados (imagens, preços) e restrição de acesso a funcionalidades administrativas.
* Armazenamento de Dados (RNF-07):
  + Revisão da criptografia de dados sensíveis (CPF, telefone) em repouso e em trânsito.

**3. Partes que exigem teste de penetração externo**

* Interface Externa (Cliente Final):
  + Teste de vulnerabilidades em formulários de checkout (RF-07, RF-08) e APIs expostas (RF-10).
* Autenticação e Sessão:
  + Teste de segurança em mecanismos de login (RF-02) e gestão de sessões (ex.: fixação de sessão).
* Integração com WhatsApp Business:
  + Verificação de exposição de endpoints e manipulação de tokens de acesso.

**4. Requisitos adicionais de teste/análise de segurança**

* Testes de Segurança de Código (SAST/DAST):
  + Análise estática (SAST) para identificar vulnerabilidades no código-fonte.
  + Testes dinâmicos (DAST) para simular ataques em ambiente de staging.
* Análise de Dependências:
  + Verificação de bibliotecas de terceiros para vulnerabilidades conhecidas (ex.: OWASP Dependency-Check).
* Conformidade Legal:
  + Validação de requisitos de LGPD para coleta e armazenamento de dados pessoais (Nome, CPF, telefone).

**5. Escopo dos requisitos de teste de fuzzing**

* Campos de Entrada de Dados:
  + Fuzzing em formulários de cadastro de produtos (RF-01), checkout (RF-07) e busca (RF-09).
* APIs de Gestão de Estoque e Pedidos:
  + Teste de resiliência em endpoints de CRUD de produtos (RF-01) e atualização de estoque (RF-06).
* Upload de Imagens:
  + Validação de restrições de tipo/formato para evitar uploads maliciosos (RF-05).

**6. Classificação de Impacto de Privacidade**

Classificação: P1 (Risco Alto)

* Justificativa:
  + O sistema coleta, armazena e transmite dados pessoais sensíveis (CPF, telefone) dos clientes (RF-07, RNF-07).
  + A integração com WhatsApp Business envolve transferência de PII, exigindo conformidade com criptografia e privacidade (RF-10).
  + A ausência de mitigação adequada pode resultar em vazamento de dados ou acesso não autorizado.