Avaliação de Segurança do Sistema PDV

Subcaracterísticas Avaliadas:

- Confidencialidade
- Integridade
- Autenticidade
- Responsabilidade (Accountability)
- Não Repúdio (Non-repudiation)
- Disponibilidade

Detalhamento das Subcaracterísticas:

1. Confidencialidade

- **Score:** 3
- **Justificativa:** O uso de BCrypt para hash de senhas é uma prática sólida para proteger credenciais, garantindo a confidencialidade das senhas armazenadas. No entanto, a ausência de autenticação multifator (MFA) reduz a robustez da proteção contra acessos não autorizados, especialmente em casos de comprometimento de credenciais.

2. Integridade

- **Score:** 2
- **Justificativa:** A presença de campos como "lastUpdate" ajuda a rastrear modificações, mas a ausência de mecanismos robustos de versionamento de dados compromete a capacidade de manter a integridade dos dados ao longo do tempo. Além disso, a validação limitada de dados pode permitir a inserção de informações inválidas ou corrompidas, afetando a integridade dos dados.

3. Autenticidade

- **Score:** 1
- **Justificativa:** A ausência de mecanismos avançados de autenticação, como certificados digitais ou tokens JWT, limita significativamente a capacidade de verificar de forma robusta a identidade dos usuários e componentes do sistema. Isso pode facilitar a ocorrência de acessos não autorizados e comprometer a autenticidade das interações no sistema.

4. Responsabilidade (Accountability)

- **Score:** 1
- **Justificativa:** A falta de logs detalhados e ferramentas de monitoramento impede o rastreamento eficaz das ações dos usuários e dos eventos do sistema. Isso dificulta a

detecção de atividades suspeitas, a realização de auditorias e a responsabilização por ações realizadas no sistema, comprometendo a responsabilidade do sistema.

5. Não Repúdio (Non-repudiation)

- **Score:** 2
- **Justificativa:** A presença de timestamps fornece alguma evidência temporal das ações realizadas, mas sem mecanismos adicionais como assinaturas digitais ou confirmações via email/SMS, não é possível garantir de forma robusta que os usuários não possam negar suas ações. Isso limita a eficácia do não repúdio no sistema.

6. Disponibilidade

- **Score:** 1
- **Justificativa:** A ausência de planos de recuperação de desastres, balanceamento de carga e redundância compromete gravemente a disponibilidade do sistema. Em caso de falhas ou perda de dados, o sistema pode ficar indisponível por períodos prolongados, afetando operações críticas de vendas e gerenciamento.

Resumo da Avaliação de Segurança

Subcaracterística	Score
Confidencialidade	3
Integridade	2
Autenticidade	1
Responsabilidade	1
Não Repúdio	2
Disponibilidade	1

Total	**10**
Média	**1,67**

Justificativa Final

O sistema PDV apresenta uma segurança fraca com um score médio de **1,67/5**. Embora exista a utilização de hashes para senhas, muitas áreas críticas da segurança não estão adequadamente abordadas, incluindo a falta de autenticação multifator, ausência de mecanismos robustos de integridade e autenticidade, inexistência de logs detalhados e ferramentas de monitoramento, bem como a falta de medidas para garantir a disponibilidade do sistema. Essas deficiências expõem o sistema a diversos riscos de segurança que podem comprometer a confidencialidade, integridade e disponibilidade dos dados e das operações.

Recomendações para Melhoria

1. **Implementar Autenticação Multifator (MFA):**
    - **Benefício:** Adiciona uma camada extra de segurança, dificultando o acesso não autorizado mesmo que as credenciais sejam comprometidas.
    - **Como Implementar:** Integrar serviços de MFA, como autenticação via aplicativos (Google Authenticator, Authy) ou via SMS/email.
2. **Aprimorar Mecanismos de Integridade:**
    - **Benefício:** Garante que os dados permaneçam precisos e consistentes ao longo do tempo.
    - **Como Implementar:** Introduzir mecanismos de versionamento de dados e validações mais robustas tanto no lado do cliente quanto no servidor para prevenir a inserção de dados inválidos.
3. **Fortalecer a Autenticidade:**
    - **Benefício:** Assegura que apenas usuários e componentes legítimos acessem e interajam com o sistema.
    - **Como Implementar:** Utilizar autenticação baseada em tokens (como JWT) e certificados digitais para validar identidades. Implementar verificação de assinaturas digitais para transações críticas.
4. **Estabelecer Mecanismos de Responsabilidade:**
    - **Benefício:** Permite o rastreamento de ações dos usuários e facilita auditorias de segurança.
    - **Como Implementar:** Implementar sistemas de logging detalhados, utilizando ferramentas como Logback ou Log4j, e integrar soluções de monitoramento e auditoria, como ELK Stack (Elasticsearch, Logstash, Kibana) ou Splunk.
5. **Garantir Não Repúdio:**

- **Benefício:** Impede que usuários neguem ações realizadas no sistema, aumentando a confiança nas transações.
- **Como Implementar:** Adotar assinaturas digitais para transações importantes e implementar confirmações de ações via email ou SMS. Utilizar timestamps seguros para registrar operações críticas.

6. **Melhorar a Disponibilidade:**
   - **Benefício:** Garante que o sistema permaneça acessível e funcional, mesmo em caso de falhas.
   - **Como Implementar:**
     - **Redundância de Servidores:** Implementar servidores redundantes para evitar pontos únicos de falha.
     - **Balanceamento de Carga:** Utilizar balanceadores de carga (como NGINX ou HAProxy) para distribuir o tráfego e evitar sobrecarga de servidores individuais.
     - **Planos de Recuperação de Desastres:** Desenvolver e implementar planos de backup e recuperação, incluindo backups regulares do banco de dados e testes de recuperação.
     - **Uso de Contêineres e Orquestração:** Considerar o uso de contêineres (como Docker) e ferramentas de orquestração (como Kubernetes) para facilitar a escalabilidade e resiliência do sistema.
7. **Adotar Políticas de Segurança e Treinamento:**
   - **Benefício:** Estabelece diretrizes claras para a manutenção da segurança e capacita a equipe a lidar com ameaças.
   - **Como Implementar:** Desenvolver políticas de segurança abrangentes e fornecer treinamento regular para a equipe de desenvolvimento e operações sobre melhores práticas de segurança.
8. **Realizar Auditorias e Testes de Segurança Regulares:**
   - **Benefício:** Identifica vulnerabilidades e garante que as medidas de segurança estejam funcionando conforme o esperado.
   - **Como Implementar:** Contratar especialistas para realizar auditorias de segurança periódicas, testes de penetração e utilizar ferramentas automatizadas de análise de segurança.

Conclusão

A avaliação revela que o sistema PDV possui várias deficiências críticas em termos de segurança, tornando-o vulnerável a uma variedade de ameaças. É essencial implementar as recomendações acima para fortalecer a segurança do sistema, proteger dados sensíveis, garantir a integridade das operações e assegurar a disponibilidade contínua do sistema. Investir em segurança não apenas protege a organização contra riscos, mas também aumenta a confiança dos usuários e clientes no sistema PDV.