Matriz de Risco de Segurança e Cibersegurança

Projeto: Furniture AI

Aviso de Concurso: №21/C16-i02/2025 **Vouchers para Startups – Novos produtos digitais/ tecnológicos**

Identificação do Beneficiário

Nome: Eduard Izgorodin
NIF: 311880517
CAE: 62020 - Atividades de consultoria em informática

Análise de Riscos e Medidas de Mitigação

R3: Má conceção e configuração de plataformas

Especificação do risco: Má conceção e configuração da plataforma de IA para design de móveis que pode levar a vulnerabilidades, ameaçando a segurança dos dados dos utilizadores e a propriedade intelectual dos fabricantes.

Medidas de mitigação:

- **M1:** Desenvolvimento de plano de risco detalhado com foco na proteção dos dados dos utilizadores e documentação de produção
- **M3:** Especificações de cibersegurança desenvolvidas e auditadas por especialistas antes do lançamento do projeto piloto
- **M6:** Exigência de credenciação de segurança para todos os fornecedores que trabalhem no projeto
- **M7:** Desenvolvimento de ações de auditoria de cumprimento do RGPD e de cibersegurança regularmente
- **M13:** Utilização de sistemas com fator de dupla autenticação para todos os utilizadores da plataforma

R4: Interferência de terceiros

Especificação do risco: Considerando que a plataforma conterá dados de produção valiosos e propriedade intelectual, existe o risco de acesso não autorizado por terceiros.

Medidas de mitigação:

- **M1, M3:** Criação e atualização regular do plano de segurança com ajuda de especialistas em cibersegurança
- **M4:** Articulação operacional e técnica com o Centro Nacional de Cibersegurança para consultas

- **M6:** Implementação de requisitos rigorosos de segurança para todas as integrações com serviços de terceiros
- **M9:** Implementação de sistemas de backup e redundância para todos os dados críticos
- **M13:** Implementação de sistema de monitorização de segurança para deteção de atividades suspeitas

R6: Não cumprimento das disposições do RGPD

Especificação do risco: Como o sistema processará dados dos utilizadores, incluindo plantas de espaços e preferências de design, existe o risco de violação das disposições do RGPD.

Medidas de mitigação:

- **M5:** Identificação do Encarregado de Proteção de Dados (EPD) e implementação de políticas de processamento de dados pessoais
- **M7:** Desenvolvimento de ações de auditoria regular de cumprimento do RGPD e requisitos de privacidade
- **M13:** Implementação de medidas técnicas que garantam o processamento seguro de dados pessoais

R8: Dependência de fornecedores específicos

Especificação do risco: O uso de tecnologias proprietárias pode criar dependência de determinados fornecedores ("vendor lock-in"), limitando a flexibilidade e escalabilidade da solução.

Medidas de mitigação:

- **M10:** Desenvolvimento de arquitetura com foco em padrões abertos e APIs que garantam a interoperabilidade com diferentes sistemas de fabricantes de móveis

R10: Requisitos técnicos de cibersegurança insuficientes

Especificação do risco: Requisitos técnicos de cibersegurança insuficientes ou incorretos podem criar vulnerabilidades na plataforma de IA.

Medidas de mitigação:

- **M1, M3:** Desenvolvimento de requisitos abrangentes de segurança com a participação de especialistas
- **M6, M7:** Implementação de verificações e auditorias regulares da segurança do sistema
- **M9:** Implementação de estratégia multinível de proteção de dados com backup
- **M13:** Implementação de métodos modernos de proteção, incluindo criptografia de dados e autenticação segura

R12: Software desatualizado

Especificação do risco: O uso de componentes sem atualizações de segurança atuais pode criar vulnerabilidades no sistema.

Medidas de mitigação:

- **M2:** Formação regular da equipe de desenvolvedores em questões de cibersegurança

- **M3:** Implementação de procedimentos de verificação de segurança para todos os componentes do sistema
- **M9:** Criação de sistema de monitorização e atualização de todos os componentes de software
- **M12:** Promoção de mecanismos de atualização automática através da utilização de soluções cloud by default

Medidas adicionais de segurança para o projeto Furniture AI

1. **Proteção de propriedade intelectual:** Implementação de medidas especiais para proteger algoritmos de IA e documentação de produção contra acesso não autorizado

2. **Segurança de dados dos clientes:** Implementação de segregação rigorosa de dados de diferentes fabricantes de móveis que utilizam nossa plataforma

3. **Proteção contra ataques a modelos de IA:** Desenvolvimento de mecanismos de proteção contra tentativas de manipulação de recomendações de IA ou extração de dados de treinamento

4. **Segurança na integração com sistemas de produção:** Implementação de protocolos seguros para integração da nossa plataforma com equipamentos de produção

5. **Formação dos utilizadores:** Desenvolvimento de programa de formação sobre uso seguro da plataforma para designers de móveis e fabricantes

Declaração

Eu, abaixo assinado, declaro que as informações fornecidas nesta Matriz de Risco de Segurança e Cibersegurança são verdadeiras e que implementarei todas as medidas de mitigação descritas para garantir a segurança e conformidade do projeto Furniture AI.

Mais declaro que estou ciente das minhas responsabilidades em matéria de segurança da informação e proteção de dados, conforme exigido pelo Regulamento Geral sobre a Proteção de Dados (RGPD) e outras leis e regulamentos aplicáveis.

Eduard Izgorodin

Data:17-03-2025