Trabalho A3

MODELOS MÉTODOS E TÉCNICAS DE ENGENHARIA DE SOFTWARE

Grupo 2:

Alex Dener de Sousa Ferreira – 321122074

João Emanuel Tavares Corrêa - 320230161

Lucas da Silva Araújo - 321120000

Vitor Henrique Ignacio Lopes - 321213584

Scrum

Dentro da metodologia Scrum, temos três papéis principais: Scrum Master, Product Owner e Equipe de Desenvolvimento. Para o nosso site, o papel de Scrum Master o papel será assumido pelo DPO (Data Protection Officer), que garantirá a conformidade com as leis de proteção de dados e facilitará a implementação efetiva do Scrum. O DPO como Scrum Master orientará a equipe no cumprimento das práticas do Scrum, removendo obstáculos, promovendo a colaboração e assegurando a transparência no processo de desenvolvimento do site. Essa abordagem permitirá a integração eficiente entre a conformidade com a LGPD e a metodologia ágil do Scrum.

O Product Owner pode ser um especialista em segurança da informação, responsável por definir e priorizar as funcionalidades, recursos e requisitos do site, levando em conta as necessidades e requisitos de segurança no ambiente digital. Esse especialista desempenhará um papel fundamental ao garantir que o site atenda aos padrões de segurança e privacidade, além de identificar e abordar adequadamente os riscos relacionados ao processamento de dados.

A Equipe de Desenvolvimento é composta por desenvolvedores web, designers, especialistas em segurança da informação, especialistas em banco de dados e especialistas em conteúdo. Essa equipe trabalhará em conjunto, seguindo as orientações do Product Owner, para criar um site seguro, funcional e atraente, aplicando as melhores práticas de desenvolvimento.

Stackholders

Dentro do projeto do site que fornece dicas de segurança na internet, os stakeholders podem incluir:

1. Clientes/Usuários: São as empresas e pessoas físicas que utilizam o site como fonte de informações e dicas de segurança na internet. Seu feedback e necessidades devem ser considerados ao desenvolver o site.

2. Proprietários do Negócio: São os responsáveis pelo projeto do site e têm interesse no seu sucesso. Eles podem ser proprietários de uma empresa ou empreendedores individuais que buscam fornecer um serviço de valor na área de segurança da informação.

3. Equipe de Desenvolvimento: Os membros da equipe de desenvolvimento têm um papel ativo no projeto. Eles estão envolvidos na construção e implementação do site, trabalhando em conjunto para alcançar os objetivos estabelecidos.

4. Especialistas em Segurança da Informação: São profissionais especializados em segurança cibernética e proteção de dados. Eles podem ser consultores externos ou membros da equipe de desenvolvimento, responsáveis por garantir que o site atenda aos mais altos padrões de segurança e privacidade.

5. Gerentes de Projeto: São responsáveis pelo planejamento, coordenação e monitoramento do projeto. Eles se envolvem na definição de metas, prazos e recursos, e garantem que o projeto seja executado de acordo com as expectativas.

6. Parceiros de Negócio: Podem incluir empresas ou organizações com as quais o projeto tem alguma forma de parceria. Isso pode envolver a colaboração em termos de marketing, divulgação ou até mesmo a contribuição de recursos técnicos.

7. Órgãos Reguladores: Em relação à LGPD, por exemplo, podem estar envolvidos órgãos reguladores que supervisionam a conformidade com as leis de proteção de dados e privacidade.

8. Fornecedores de Serviços: Podem ser empresas ou indivíduos que fornecem serviços relacionados ao projeto, como hospedagem do site, suporte técnico ou consultoria especializada.

9. Outros Stakeholders: Dependendo do contexto específico do projeto, outros stakeholders podem ser identificados, como especialistas em marketing, profissionais de comunicação, investidores ou até mesmo a sociedade em geral, que se beneficia do acesso a informações seguras na internet.

É importante envolver e gerenciar adequadamente os stakeholders ao longo do projeto, buscando atender às suas necessidades e expectativas, garantindo o sucesso do site e a satisfação de todos os envolvidos.

Técnicas de levantamento de requisitos

Técnica de levantamento de requisitos baseada em testes: A técnica de levantamento de requisitos baseada em testes é uma abordagem eficaz para identificar e documentar os requisitos de um sistema de software. Ela utiliza os testes como cenários ou casos de uso para explorar e capturar as funcionalidades e interações esperadas do sistema. Essa técnica é escolhida por várias razões. Uma das principais vantagens dessa abordagem é que ela fornece uma compreensão clara dos requisitos por meio de casos de teste concretos.

Ao criar os testes, os requisitos são identificados e especificados de forma prática e tangível. Isso ajuda a evitar ambiguidades e inconsistências na definição dos requisitos, tornando-os mais claros e compreensíveis para todos os envolvidos. Além disso, a técnica de levantamento de requisitos baseada em testes promove a validação contínua dos requisitos à medida que os testes são executados. Durante a execução dos casos de teste, é possível observar o comportamento do sistema e identificar lacunas ou requisitos não contemplados. Isso permite uma iteração rápida e contínua, ajustando e refinando os requisitos ao longo do processo de desenvolvimento. Outra razão para escolher essa técnica é a sua capacidade de envolver os stakeholders de forma ativa e colaborativa.

Os testes fornecem um contexto concreto para discussões e validação dos requisitos, permitindo que os stakeholders participem de forma mais efetiva. Isso promove uma comunicação mais clara e facilita a obtenção de um consenso sobre as necessidades e expectativas do sistema. Além disso, a abordagem baseada em testes ajuda a mitigar riscos e identificar potenciais problemas antecipadamente. Ao criar casos de teste abrangentes, é possível explorar diferentes cenários e verificar a adequação do sistema em diversas situações. Isso contribui para a detecção precoce de problemas e reduz a chance de erros ou falhas no produto final.

Backlog com mini Histórias

ID	NOME	DESCRIÇÃO	IMPORTÂNCIA	TAMANHO
1	Navegação	Como um visitante do site, eu quero poder navegar pelas seções do site para encontrar informações relevantes sobre segurança cibernética	9	5
2	Acesso à informação	Como um visitante do site, eu quero poder ler artigos informativos sobre práticas recomendadas de segurança cibernética para empresas	8	10
3	Cadastro	Como um usuário registrado, eu quero poder fazer o cadastro e login em minha conta para acessar conteúdos exclusivos	8	15
4	Notificações	Como um usuário cadastrado, eu quero receber notificações sobre atualizações em meu e-mail sobre as ultimas tendências e práticas de segurança cibernética	3	6
5	Interação	Como um usuário cadastrado, eu quero ter acesso e poder interagir em um fórum de discussões forcenido pela plataforma	6	8

Relatório de Sprints

1. Sprint 1:

- Reunião de planejamento do sprint: A equipe se reúne para identificar as funcionalidades de segurança mais importantes a serem implementadas no primeiro sprint. Isso pode incluir recursos como autenticação de usuário, gerenciamento de permissões e criptografia de dados.

- Desenvolvimento e teste: A equipe trabalha na implementação das funcionalidades identificadas durante o planejamento. Eles seguem as práticas ágeis, como desenvolvimento orientado por testes (TDD), para garantir a qualidade do código. Os testes de unidade e integração são executados regularmente para verificar a funcionalidade correta do software.

- Revisão do sprint: Ao final do sprint, a equipe realiza uma revisão com o cliente. Eles demonstram as funcionalidades desenvolvidas, explicam como cada uma contribui para a segurança do aplicativo e solicitam feedback.

- Retrospectiva do sprint: A equipe realiza uma retrospectiva para refletir sobre o sprint anterior. Eles discutem o que funcionou bem, os desafios enfrentados e quais melhorias podem ser feitas para os próximos sprints.

2. Sprint 2:

- Reunião de planejamento do sprint: Com base no feedback do cliente e nas prioridades atualizadas, a equipe define as funcionalidades a serem desenvolvidas no segundo sprint. Isso pode incluir recursos como criptografia de comunicação, monitoramento de atividades suspeitas e notificações de segurança.

- Desenvolvimento e teste: A equipe trabalha nas funcionalidades planejadas, seguindo as práticas ágeis. Eles garantem que o código esteja bem testado e a segurança seja considerada em todos os aspectos do desenvolvimento.

- Revisão do sprint: Ao final do sprint, a equipe realiza uma nova revisão com o cliente. Eles demonstram as novas funcionalidades implementadas, destacando como elas melhoram a segurança do aplicativo. Novo feedback é solicitado.

- Retrospectiva do sprint: A equipe realiza outra retrospectiva para analisar o sprint anterior e identificar oportunidades de melhoria contínua. Eles ajustam seus processos e abordagens com base nas lições aprendidas.

3. Sprint 3 e seguintes:

- O ciclo se repete para os sprints subsequentes. A equipe realiza reuniões de planejamento, desenvolvimento, teste, revisão com o cliente e retrospectiva para cada sprint.

- As funcionalidades de segurança são implementadas incrementalmente, sempre com o objetivo de entregar valor ao cliente e aprimorar a segurança do aplicativo.

- A interação com o cliente ocorre ao final de cada sprint, permitindo que eles forneçam feedback contínuo e influenciem o desenvolvimento do aplicativo.

Esse roteiro demonstra como a equipe ágil trabalha em ciclos curtos, priorizando as funcionalidades mais importantes para a segurança do aplicativo e adaptando-se às mudanças ao longo do projeto. A interação frequente com o cliente garante que suas necessidades sejam atendidas e que o aplicativo evolua de acordo com as expectativas.