

GP

PITCH



JUSTIFICATIVAS
Passado

- Crescimento dos vazamentos de dados expõe credenciais de usuários.
- Falta de conhecimento dificulta a adoção de medidas preventivas.

**PRODUTO**

- Site que verifica se e-mail, senha e nome de usuário vazaram.



STAKEHOLDERS

Externos &
Fatores Externos

- Usuários finais preocupados com segurança digital.
- Comunidade de segurança e empresas.



PREMISSAS

1. O site não armazenará informações sensíveis dos usuários.
2. O projeto usará tecnologias de código aberto sempre que possível.
3. As APIs utilizadas devem ser bem documentadas e seguras.
4. O suporte técnico básico deve estar disponível via e-mail ou chat para usuários.
5. A plataforma deve permitir futuras integrações com outros serviços de segurança.



RISCOS

1. Não armazenar informações sensíveis pode limitar funcionalidades e dificultar auditorias.
2. Uso de código aberto pode trazer vulnerabilidades e depender de terceiros para suporte.
3. APIs externas podem ser comprometidas ou sofrer mudanças inesperadas, afetando o sistema.
4. Suporte via e-mail ou chat pode ser insuficiente para alta demanda ou problemas complexos.
5. Integrações futuras podem gerar incompatibilidades e expor o sistema a novos riscos.



OBJ SMART

- Criar uma plataforma web para consulta de credenciais vazadas e exibição de relatórios, desenvolvendo um MVP em 3 meses e a versão final em 5 meses.



REQUISITOS

- Permitir busca por e-mail, nome de usuário e senha.
- Notificar usuários sobre novos vazamentos identificados.
- Exibir detalhes sobre os vazamentos encontrados.



EQUIPE

- DEV: Guilherme de Abreu
- PO: Gustavo Flores
- Gerente: Kaique Fernandes



GRUPOS DE ENTREGAS

- 1.Canva
- 2.Modelos de Negócio Requisitos
- 3.Lista de Serviços
- 4.Contrato de Serviços
- 5.Componentes de Serviço
- 6.Estratégias de Teste
- 7.Plano de Gerenciamento

LINHA DO TEMPO

1. Canva (01/03)
2. Modelos de Negócio Requisitos (01/03 - 08/03)
3. Lista de Serviços (08/03 - 12/04)
4. Contrato de Serviços (08/03 - 12/04)
5. Componentes de Serviço (08/03 - 12/04)
6. Estratégias de Teste (12/04 - 10/05)
7. Plano de Gerenciamento (10/05 - 24/05)



BENEFÍCIOS
Futuro

- Aumento da segurança digital e prevenção de ataques.
- Serviço acessível para usuários e empresas.
- Serviço gratuito
- Incentivo à adoção de boas práticas de segurança digital.



RESTRIÇÕES

- Tempo para desenvolvimento
- Sem coleta de dados pessoais dos usuários
- Atualizações apenas a cada semestre
- Qualquer mudança crítica precisa ser aprovada pelo gerente do projeto
- Não haverá versão offline da plataforma



CUSTOS

- Equipe
- Infraestrutura (Cloud, banco de dados, domínio, equipamentos, APIs)
- Licenças