**Matriz SWOT**

| **CADASTRO DE USUÁRIOS** | **FORÇAS**  1. São necessárias poucas informações.  2. Validador de senhas fortes.  3. Validação de contas via email.  4. Interface intuitiva.  5. Todos os campos são validados em tempo real. | **FRAQUEZAS**  1. O cadastro não pode ser feito através de uma conta do Google.  2. Mesma pessoa pode fazer vários cadastros.  3. O cadastro não pode ser feito de forma offline.  4. Validação de senha forte pode impedir que o usuário utilize uma senha que ele está acostumado  5. Nada garante que o usuário forneça informações reais. |
| --- | --- | --- |
| **OPORTUNIDADES**  1. Gerador de senhas fortes.  2. Cadastro do login com email ou telefone.  3. Cadastro do usuário com alguma rede social.  4. Cadastro de nickname para interação entre perfis.  5. Foto de perfil. | **AMEAÇAS**  1. Perda de informações decorrente de uma desconexão com a internet.  2. Criação de usuários falsos.  3. Falha ao enviar informações para API.  4. Descumprir a lei LGPD.  5. Múltiplos cadastros decorrentes de um robô. |

| **ROBÔS QUE BUSCAM INFORMAÇÕES** | **FORÇAS**  1. Minimização de tempo.  2. Diminuição de custos.  3. Maior probabilidade de acertos.  4. Verificações em múltiplos sites em tempo real.  5. Gera alertas ao encontrar inconsistência | **FRAQUEZAS**  1. Risco de informação incoerente.  2. Necessita de programação específica para cada padrão.  3. Não é totalmente automático  4. Necessita de validações finais humanas. |
| --- | --- | --- |
| **OPORTUNIDADES**  1. Auto restart em caso de falhas.  2. Automatização completa do processo de mineração de dados.  3. Atualização automática ao encontrar informações novas.  4. Plano de backup em caso de sites offline.  5. Utilização de inteligência artificial para identificar novos padrões de layout. | **AMEAÇAS**  1. Sites fora do ar.  2. Sites inconsistentes.  3. Mudança brusca de layout.  4. Falta de centralização de informações.  5. Sites bloquearam os robôs. |

| **LOGIN** | **FORÇAS**  1. Autenticação em duas etapas com email  2. Salvar a sessão do usuário.  3. Redefinição de senha.  4. Layout intuitivo.  5. Acesso completo ao sistema. | **FRAQUEZAS**  1. Sem verificação se é um robô que está logando.  2. Dependência de conexão com internet.  3. Não conseguir fazer login com as redes sociais. |
| --- | --- | --- |
| **OPORTUNIDADES**  1. Palavra chave para ajudar a lembrar a senha.  2. Login automático com rede social.  3. Conseguir olhar a senha que está sendo digitada.  4. Login com a digital.  5. uso de reCAPTCHA. | **AMEAÇAS**  1. Risco de vazamento de informações.  2. Risco de invasão de conta.  3. Inconsistência com API.  4. Servidor offline. |