DOCUMENTO DE ESCOPO

Nome do Projeto: Sistema de Atendimento Flask  
Organização: Rio Brasil Terminal / iTracker  
Data: Maio/2025  
  
1. Objetivo do Sistema:  
Automatizar o registro e a coleta de informações sobre veículos, motoristas e clientes, com suporte ao upload de arquivos, por meio de um sistema web acessível internamente.  
  
2. Situação Atual (“As is”):  
Processo manual baseado em planilhas para registro e controle de dados de atendimento, com risco de erros e duplicidade.  
  
3. Situação Desejada (“To be”):  
Sistema centralizado, com campos padronizados extraídos da planilha principal, permitindo maior rastreabilidade, facilidade de busca e segurança na entrada de dados.  
  
4. Criticidade:  
Baixa a média – sistema interno de apoio a operações, sem impacto direto em operações críticas, mas relevante para integridade de registros.  
  
5. Dados Pessoais Envolvidos:  
Nome, CPF de motoristas — tratados sob a base legal de legítimo interesse com restrição de acesso.  
  
6. Recursos Necessários:  
- Servidor local ou máquina virtual Linux/Windows  
- Python 3.10+  
- Flask  
- Pandas  
- Armazenamento seguro para uploads  
  
7. ROI Esperado:  
Redução de retrabalho manual, padronização de dados, eliminação de inconsistências nas planilhas e rastreabilidade.  
  
8. Equipe Responsável:  
Desenvolvedor: Leonardo Fragoso  
TI: Equipe local de Infraestrutura  
  
9. Custo Estimado:  
Baixo (uso de tecnologias livres)

# 10. Conformidade com Política de Segurança da Informação

## Controle de Acesso

* - Autenticação obrigatória de usuários com controle de privilégios (usuário comum e administrador).
* - Restrições de acesso por sessão, expiração e logout seguro.

## Gestão de Usuários

* - Processo de cadastro via formulário protegido.
* - Redefinição de senha disponível com validação.

## Auditoria e Log

* - Geração de arquivos de log 'access.log' com registros de login, logout e ações administrativas.
* - Histórico de alterações com rastreamento de quem alterou o quê e quando (tabela 'historico' no banco de dados).

## Tratamento de Dados Sensíveis

* - Uso de hash seguro (bcrypt/werkzeug) para armazenar senhas.
* - Dados pessoais tratados conforme legítimo interesse e restritos ao ambiente interno.

## Proteção contra Upload Indevido

* - Validação e restrição de extensão dos arquivos enviados (.pdf, .jpg, etc.).
* - Salvamento em diretório seguro.

## Backup e Disponibilidade

* - Recomendação de rotina de backup automático do banco de dados SQLite e pasta 'uploads/'.

## Hospedagem Segura

* - Executado em ambiente controlado, com restrição de acesso à rede interna.
* - Possibilidade futura de uso de NGINX ou Apache como proxy reverso com HTTPS.

# 11. Próximas Etapas para Aderência Completa

* - Implementar backup automatizado e criptografado.
* - Implementar expiração automática de sessão por inatividade.
* - Avaliar uso de autenticação multifator (MFA).
* - Configurar firewall e regras de acesso por IP.
* - Registrar o sistema no inventário oficial de sistemas internos da organização.