**Relatório de Requisitos**

**de Segurança de Aplicação**

|  |  |
| --- | --- |
| **Empresa:** | **SOAT** |
| **Versão:** | 1.0 |
| **Data da última modificação:** | 03/07/2025 |
| **Autor:** | Vernon Araújo Corrêa Simões |

|  |
| --- |
| **Descritivo da aplicação:** |
| Criar a API, para que posteriormente o time de frontend integre a solução. O desenho da solução envolve as seguintes necessidades do negócio: • Cadastrar um veículo para venda (Marca, modelo, ano, cor, preço); • Editar os dados do veículo; • Efetuar a venda de um veículo (somente para compradores cadastrados); • Listagem de veículos à venda, ordenada por preço, do mais barato para o mais caro; • Listagem de veículos vendidos, ordenada por preço, do mais barato para o mais caro; • Cadastro de compradores. |

1. **Dados Armazenados pela Solução**

A aplicação armazena as seguintes informações no banco de dados (DynamoDB):

|  |  |
| --- | --- |
| **Entidade** | **Campos Armazenados** |
| Veículo | id, marca, modelo, ano, cor, preço, status (reservado/vendido: true ou false) |

1. **Dados Sensíveis**

Os seguintes dados são considerados sensíveis e requerem tratamento especial:

|  |  |  |
| --- | --- | --- |
| **Dado** | **Sensibilidade** | **Justificativa** |
| Cpf comprador | Alto | Identificador pessoal (PII) sujeito à LGPD |
| Nome COmprador | Alto | Identificador pessoal (PII) sujeito à LGPD |
| Informações de pagamento | Alto | Informações de pagamento de alto risco e sujeito à LGPD |

1. **Políticas de Acesso a Dados**

A aplicação aplica as seguintes **políticas de controle de acesso**, baseadas em **IAM e práticas de menor privilégio**:

|  |  |
| --- | --- |
| **Camada** | **Política de Acesso** |
| Lambda Functions | Cada função só possui permissão para acessar as tabelas e segredos necessários |
| API Gateway | Proteção por autenticação (JWT/Cognito) e autorização condicional |
| DynamoDB | Acesso apenas via Lambda (não exposto publicamente); políticas restritivas por tabela |
| Secrets Manager | Segredos acessíveis apenas pelas funções Lambda específicas |
| Logs (CloudWatch) | Acesso apenas por administradores e equipe de segurança |

1. **Políticas de Segurança da Operação**

|  |  |
| --- | --- |
| **Área** | **Ação de Segurança** |
| Logs e auditoria | Todos os acessos e alterações são registrados no CloudWatch Logs |
| Monitoramento | Alarmes configurados para falhas, picos de acesso e exceções inesperadas |
| Gerenciamento de Segredos | Credenciais criptografadas no Secrets Manager com rotação automática |
| Criptografia de Dados | DynamoDB criptografa todos os dados em repouso por padrão (KMS) |
| Proteção contra DDoS | Proteção via AWS Shield integrada ao API Gateway |
| Autenticação | Pode ser integrada ao Cognito para proteger endpoints da API |

1. **Riscos e Ações de Mitigação**

|  |  |
| --- | --- |
| **Risco Identificado** | **Ação de Mitigação** |
| Vazamento de cpf via logs ou erros | Sanitização de entradas e logs, anonimização de dados de erro |
| Acesso não autorizado à api | Uso de autenticação forte (JWT/Cognito), CORS restrito, WAF opcional |
| Elevação de privilégio em serviços internos | Aplicação do princípio do menor privilégio em todas as políticas IAM |
| Exposição indevida de segredos ou credenciais | Armazenamento em Secrets Manager com permissões limitadas |
| Perda de integridade dos dados | Uso de versionamento e logs de alteração (updated\_at) em todas as entidades |
| Ataques por automação ou scraping | Limitação de requisições no API Gateway, análise de padrões via CloudWatch |