Ministério da Economia

Documento Relatório de Teste

Prova de Conceito - TaxiGov

Ministério da Economia
Diretoria de Tecnologia da informação - DTI
Coordenação-Geral de Sistemas

Versão 2.1

Sumário

1 Controle de Revisão

Data	Versão	Descrição	Autor	Área
26/07/2020	1.0	Elaboração do documento	Leonardo Oliveira	Fábrica de Teste
13/07/2020	2.0	Novo ciclo de testes, alteração nas sessões 6.3.2.1 e 6.4.2.1	Leonardo Oliveira	Fábrica de Teste
17/08/2020	2.1	Adicinada sessão Conclusão		

2 Identificação da Demanda

Número da OS:	012	**Sistema/Módulo:**	TaxiGov
Líder do Projeto:	Wellington Palmeira	**Analista de Teste:**	
Dono do Produto:	Luis Guilherme Izycki		

3 Finalidade

O objetivo deste é sintetizar os resultados obtidos na execução dos serviços de Teste e Qualidade de Software relativos à Prova de Conceito para contratação de transporte terrestre ou agenciamento/intermediação de transporte terrestre dos servidores, empregados e colaboradores a serviço dos órgãos e entidades da Administração Pública Federal – APF.

4 Escopo

Os serviços de teste e qualidade compreendem a execução das seguintes atividades para a soluções tecnológica apresentada pelo CONTRATADA, com o objetivo de identificação de possíveis falhas e defeitos, em conformidade com o processo licitatório e os itens de avaliação elencados no Anexo E do Termo de Referência:

- Requisitos de Acessibilidade
- Requisitos de Funcionalidade
- Requisitos de Disponibilidade
- Requisitos de Segurança

Soluções apresentadas:

Web: https://portal.huby.com.br/

Mobile

IOS

https://apps.apple.com/br/app/99-carro-particular-e-t%C3%A1xi/id553663691

IPA fornecido pela CONTRATADA

Android

https://play.google.com/store/apps/details?id=com.taxis99&hl=pt_BR

APK baixado da Google Store

4.1 Não Escopo

Não se aplica.

5 Recursos Necessários

5.1 Recursos Humanos

Responsável	Papel	Responsabilidades
Leonardo Gonçalves de Oliveira	Coordenador de Operações	Responsável pela coordenação dos testes e andamento do projeto
Rodrigo Teixeira Pimentel	Especialista em Teste	Responsável pela execução dos testes funcionais previstos para o projeto
Emerson Santos Pereira	Especialista em Automação	Responsável pela execução dos testes não funcionais previstos para o projeto
Anderson Araújo Alves	Especialista em Segurança	Responsável pela execução dos testes de segurança do projeto
Luiz Henrique Cavalcante Wurli	Especialista em Segurança	Responsável pela execução dos testes de segurança do projeto

6 Resultados Obtidos

6.1 Requisitos de Acessibilidade

Esta atividade compreende na avaliação dos seguintes itens:

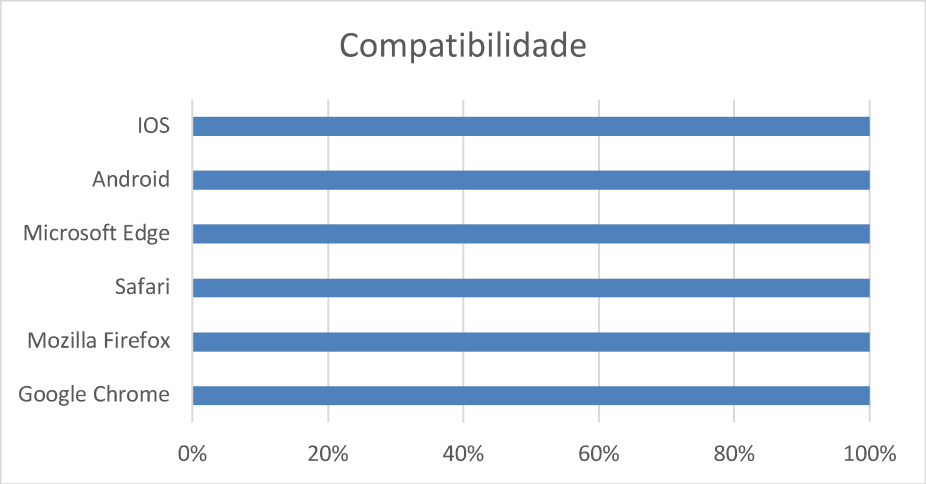
- Acesso à solução solução tecnológica por meio de aplicação web compatível com Google Chrome
- Acesso à solução solução tecnológica por meio de aplicação web compatível com Mozilla Firefox
- Acesso à solução solução tecnológica por meio de aplicação web compatível com Safari
- Acesso à solução solução tecnológica por meio de aplicação web compatível com Microsoft Edge
- Acesso à solução solução tecnológica por meio de aplicação web compatível com Android
- Acesso à solução solução tecnológica por meio de aplicação web compatível com IOS

Tipo de avaliação: Conformidade

Estratégia de teste: Verificação manual

Status: Aprovado

Item Avaliado	Versão	Resultado
Google Chrome	84.0.4147.89	OK
Mozilla Firefox	78.0.2	OK
Apple Safari	13.1.2	OK
Microsoft Edge	84.0.522.40	OK
Android	6.14.2	OK
IOS	13.6	OK



6.2 Requisitos de Funcionalidade

Esta atividade compreende na avaliação dos seguintes itens:

- Acesso à solução solução tecnológica por meio de login e senha pessoal
- Cadastramento de órgãos e entidades na solução tecnológica por meio da aplicação web
- Cadastramento de unidades administrativas na solução tecnológica por meio da aplicação web
- Cadastramento de gestores e usuários na solução tecnológica por meio da aplicação web
- Solicitação de serviço por meio da aplicação web e do aplicativo mobile
- Acompanhamento de solicitações de serviço e de atendimentos em andamento, por meio da aplicação web e do aplicativo mobile, incluindo imagem geoprocessada do percurso
- Cancelamento de solicitações de serviço por meio da aplicação web e do aplicativo mobile
- Consultas e relatórios com informações sobre solicitações de serviço e atendimentos

Tipo de avaliação: Conformidade

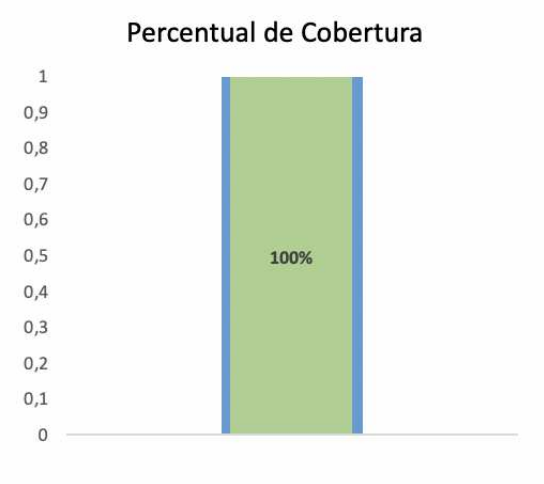
Estratégia de teste: Verificação manual

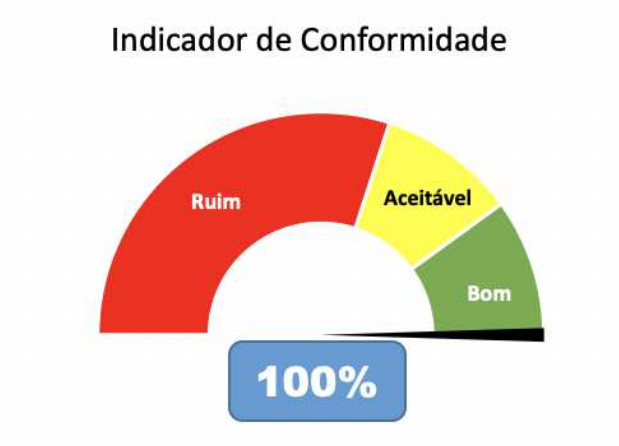
Status: Aprovado

Item Avaliado	Chrome	Firefox	Edge	Safari	Android	IOS
Acesso à solução solução tecnológica por meio de login e senha pessoal	OK	OK	OK	OK	OK	OK
Cadastramento de órgãos e entidades na solução tecnológica por meio da aplicação web	OK	OK	OK	OK	OK	OK
Cadastramento de unidades administrativas na solução tecnológica por meio da aplicação web	OK	OK	OK	OK	OK	OK

Cadastramento de gestores e usuários na solução tecnológica por meio da aplicação web	OK	OK	OK	OK	OK	OK
Solicitação de serviço por meio da aplicação web e do aplicativo mobile	OK	OK	OK	OK	OK	OK
Acompanhamento de solicitações de serviço e de atendimentos em andamento, por meio da aplicação web e do aplicativo mobile, incluindo imagem geoprocessada do percurso	OK	OK	OK	OK	OK	OK
Cancelamento de solicitações de serviço por meio da aplicação web e do aplicativo mobile	OK	OK	OK	OK	OK	OK
Consultas e relatórios com informações sobre solicitações de serviço e atendimentos	OK	OK	OK	OK	OK	OK

Funcionalidade	Ciclo	Cobertura	Qualidade	Resultados da Execução					Incidentes por Gravidade				
				Planejados	Com Defeito	Com Sucesso	Bloqueados	Não Executados	Crítico	Alto	Médio	Baixo	Melhoria
Web	1	100%	100%	36	0	36	0	0	0	0	0	0	0
Mobile	1	100%	100%	16	0	16	0	0	0	0	0	0	0
Total Geral:		**100%**	**100%**	**52**	**0**	**52**	**0**	**0**	**0**	**0**	**0**	**0**	**0**





6.3 Requisitos de Disponibilidade

Esta atividade compreende na avaliação dos seguintes itens:

- Disponibilidade da solução tecnológica mínima de 96% (noventa e seis porcento) do período de tempo utilizado para aplicação da PoC
- Desempenho medido por tempo de resposta (RESPONSE TIME TESTING) correspondente a até 5 segundos para 25 solicitações de serviços (corridas) na aplicação web.
- Desempenho medido por tempo de resposta (RESPONSE TIME TESTING) correspondente a até 5 segundos para 25 solicitações de serviços (corridas) no aplicativo mobile

6.3.1 Disponibilidade de 96%

[redacted]Web

Tipo de avaliação: Automatizada

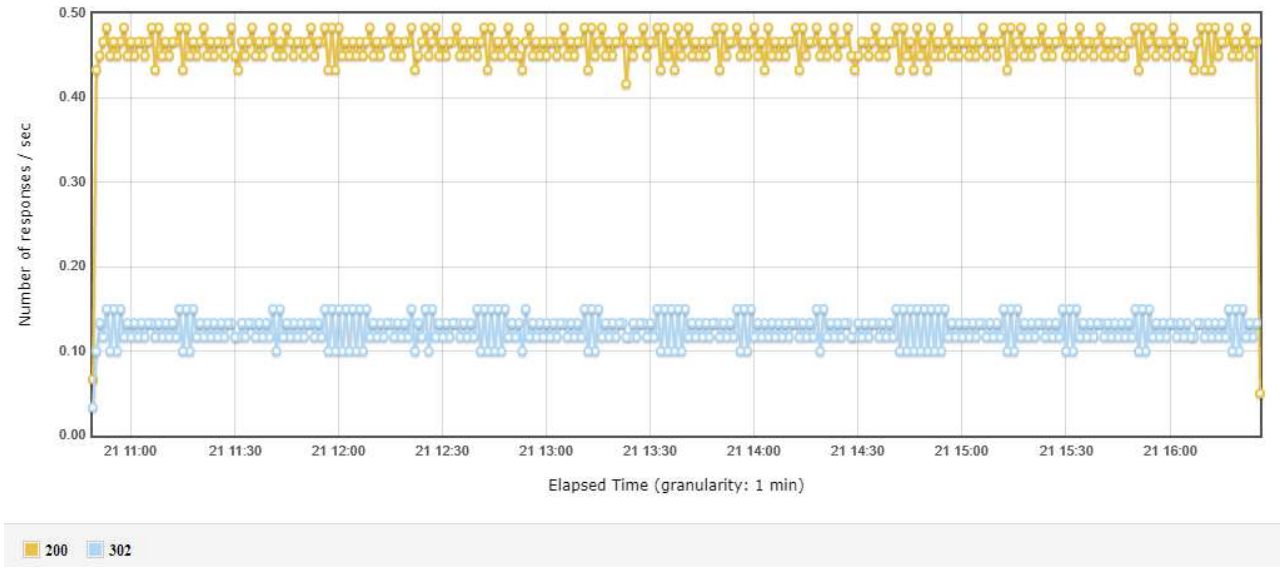
Estratégia de teste: Script de disponibilidade

Tempo de Execução: 05:37

Status: Aprovado

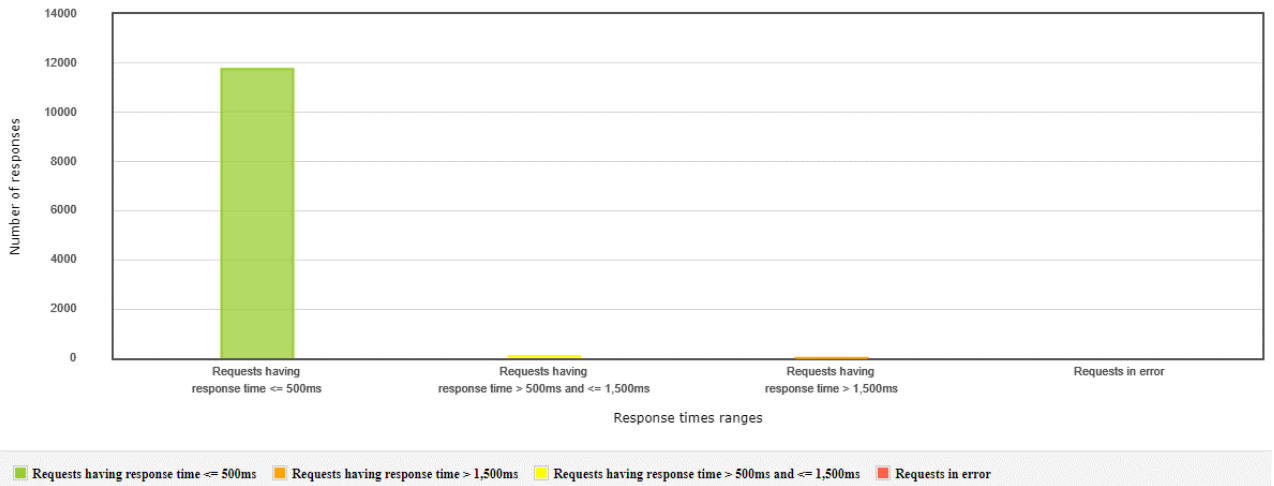
Códigos por Segundo

O relatório de tempo de resposta por tempo de execução exibe dados sobre o comportamento das páginas/requisições durante o tempo de execução do teste de uma forma gráfica. Apresentando de uma maneira bem simples todos os valores recuperados tanto para cima quanto para baixo:



Visão Geral do Tempo de Resposta

Este gráfico representa a distribuição das requisições nas faixas de tempo de resposta definidas:



[redacted] Mobile

Tipo de avaliação: Automatizada

Estratégia de teste: Script de disponibilidade

Tempo de Execução: 02:00

Status: Aprovado

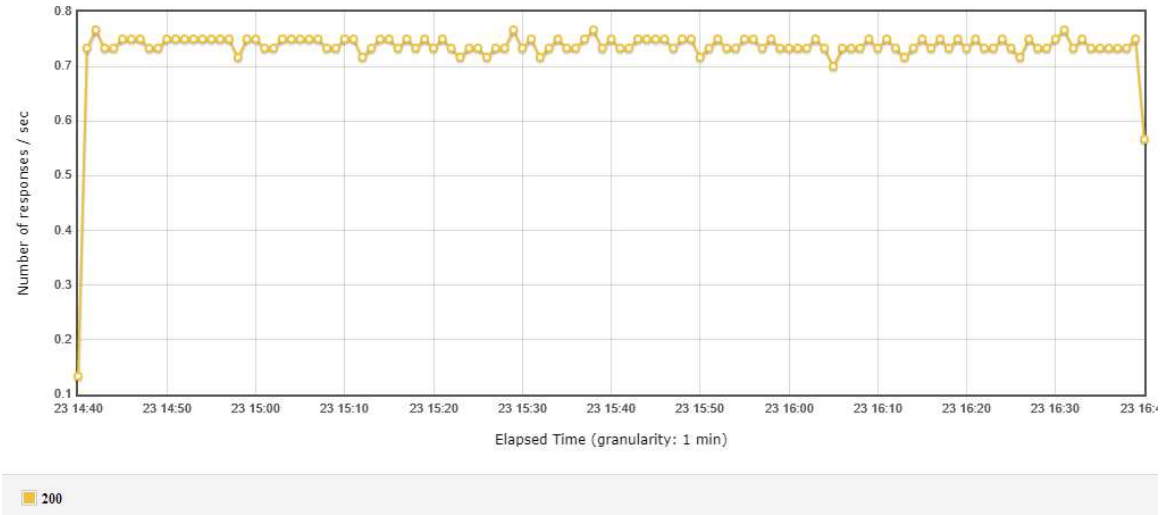
A execução foi realizada utilizando a API Recuperar Usuários, onde foram coletados os resultados abaixo:

Resultado Geral

Requisições	Execução		Tempos de Resposta		
Nome	Amostras	% de Erro	Média	Min.	Max
Mobile	5327	0.00%	1,048	0,953	3,199
Recuperar Usuários	5327	0.00%	1,048	0,953	3,199

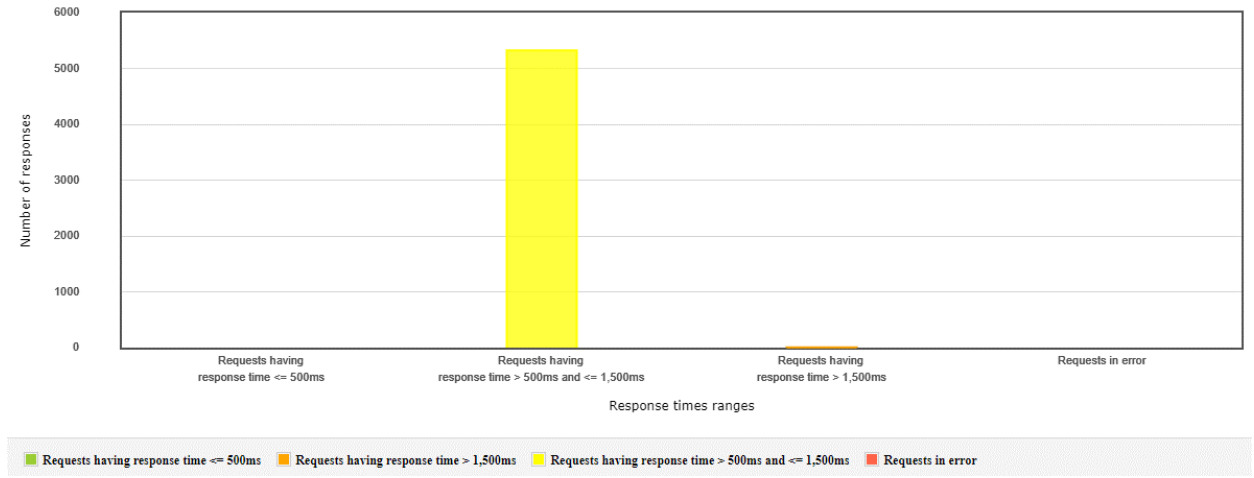
Códigos por segundo

O relatório de tempo de resposta por tempo de execução exibe dados sobre o comportamento das páginas/requisições durante o tempo de execução do teste de uma forma gráfica. Apresentando de uma maneira bem simples todos os valores recuperados tanto para cima quanto para baixo:



Visão Geral do Tempo de Resposta

Este gráfico representa a distribuição das requisições nas faixas de tempo de resposta definidas:



6.3.2 Desempenho – 25 corridas

[redacted]Web

Tipo de avaliação: Automatizada

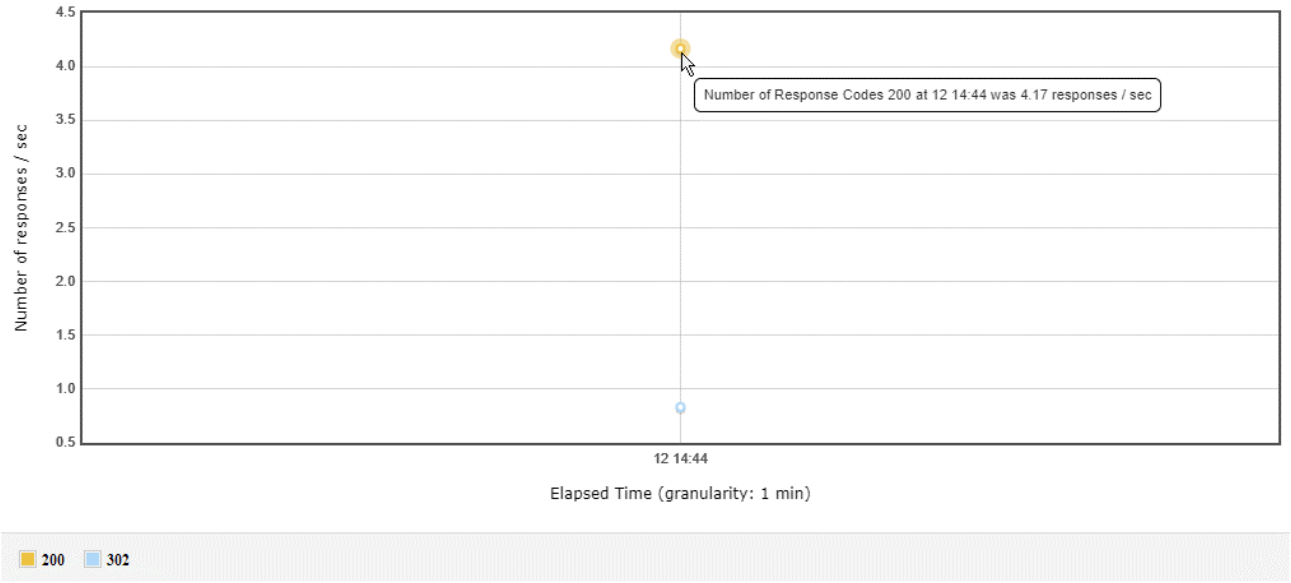
Estratégia de teste: Script de desempenho

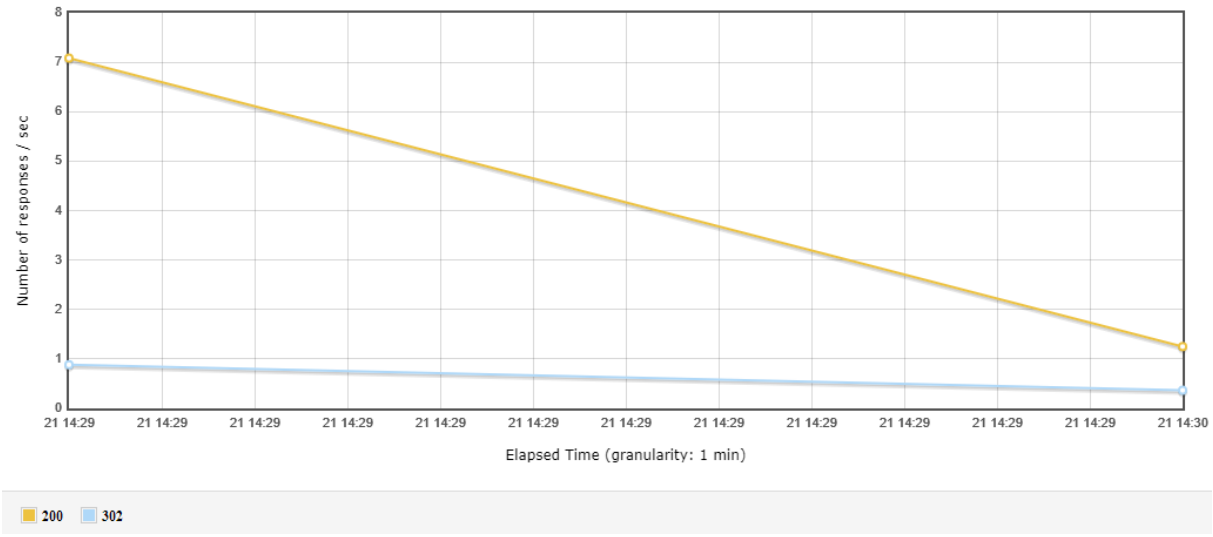
Tempo da requisição: 3,9 segundos

Status: Aprovado

Códigos por Segundo

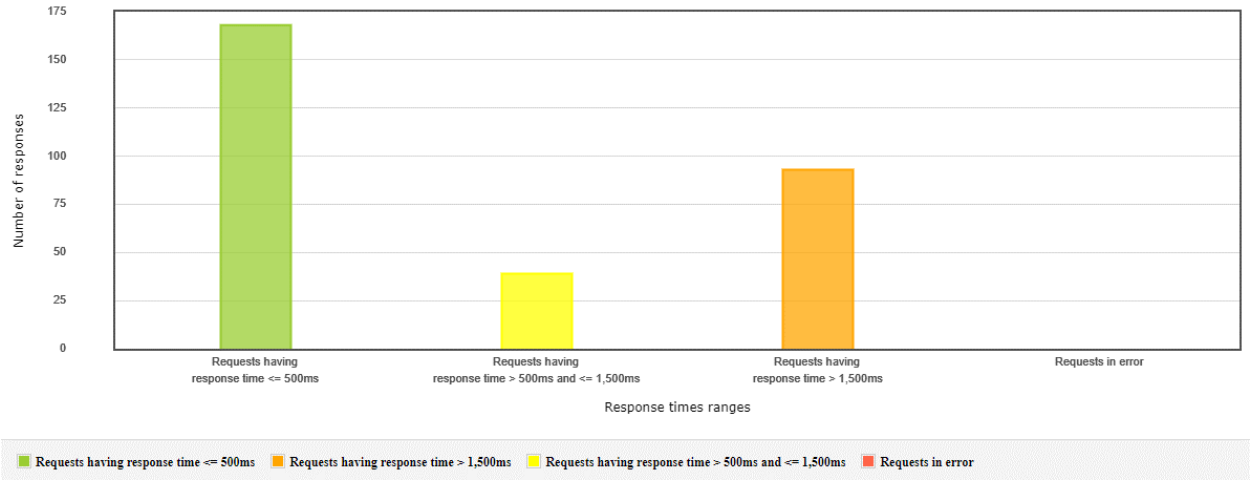
O relatório de tempo de resposta por tempo de execução exibe dados sobre o comportamento das páginas/requisições durante o tempo de execução do teste de uma forma gráfica. Apresentando de uma maneira bem simples todos os valores recuperados tanto para cima quanto para baixo:



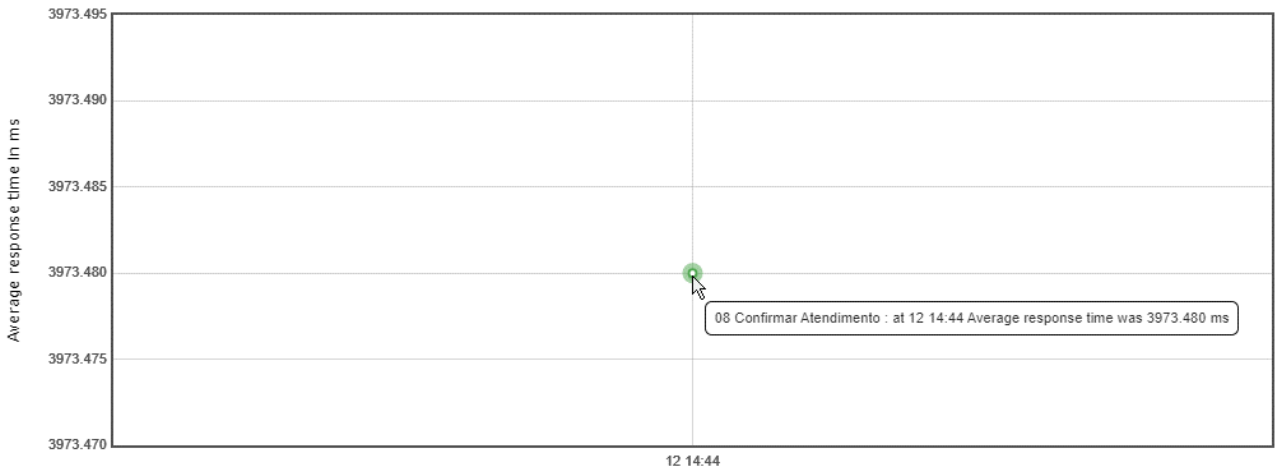


Visão Geral do Tempo de Resposta

Este gráfico representa a distribuição das requisições nas faixas de tempo de resposta definidas.



Este gráfico representa o tempo de resposta médio durante a execução do teste:



[redacted] Mobile

Tipo de avaliação: Automatizada

Estratégia de teste: Script de desempenho

Tempo da requisição: 3,7 segundos

Status: Aprovado

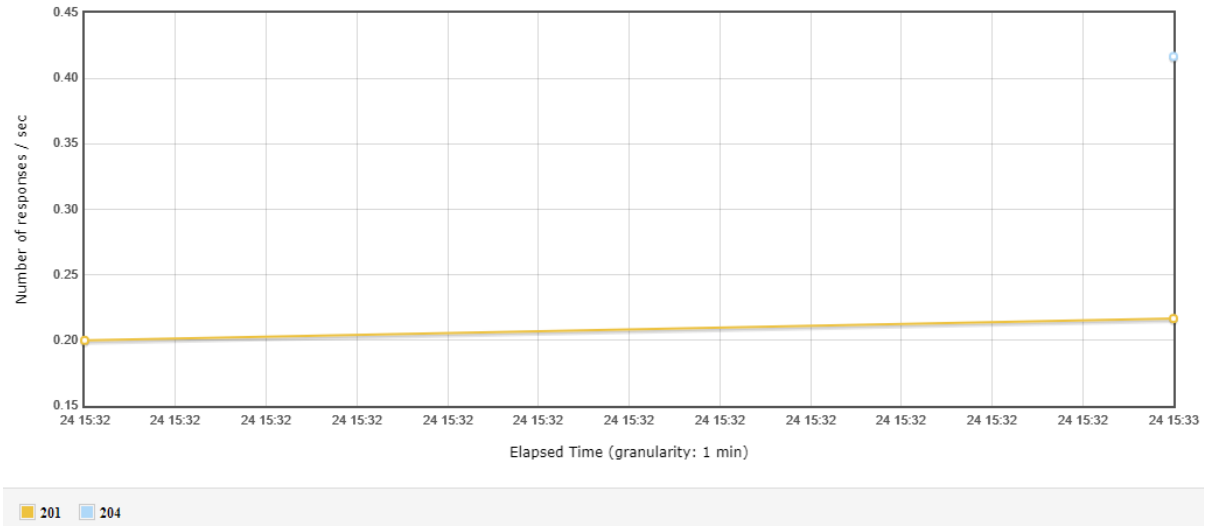
A execução foi realizada utilizando a API Ride, onde foram coletados os resultados abaixo:

Resultado Geral

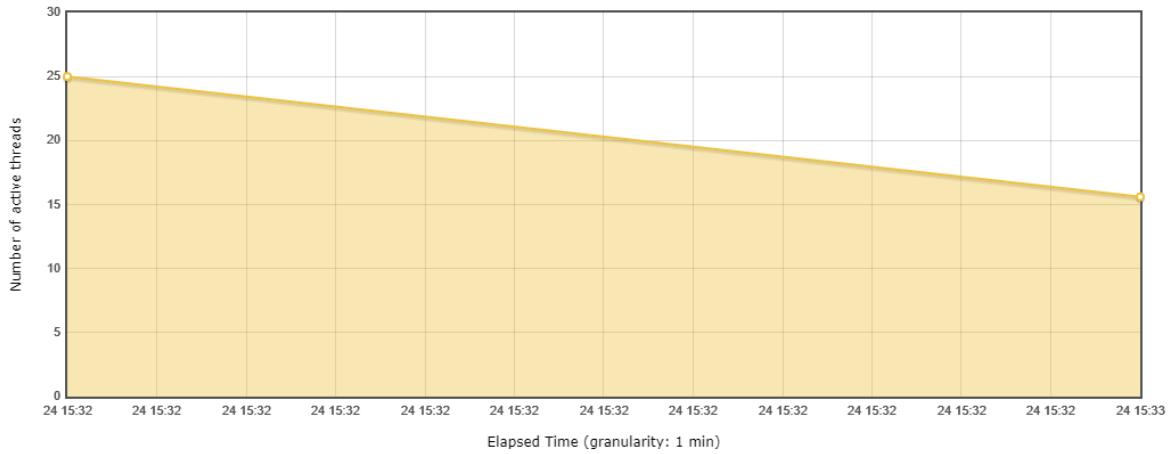
Requisições	Execução		Tempos de Resposta		
Nome	Amostras	% de Erro	Média	Min.	Max
Solicitar Corrida	25	0.00%	3,732	3,162	4,270
Cancelar Corrida	25	0.00%	1,322	1,138	1,579

Códigos por segundo

O relatório de tempo de resposta por tempo de execução exibe dados sobre o comportamento das páginas/requisições durante o tempo de execução do teste de uma forma gráfica. Apresentando de uma maneira bem simples todos os valores recuperados tanto para cima quanto para baixo:

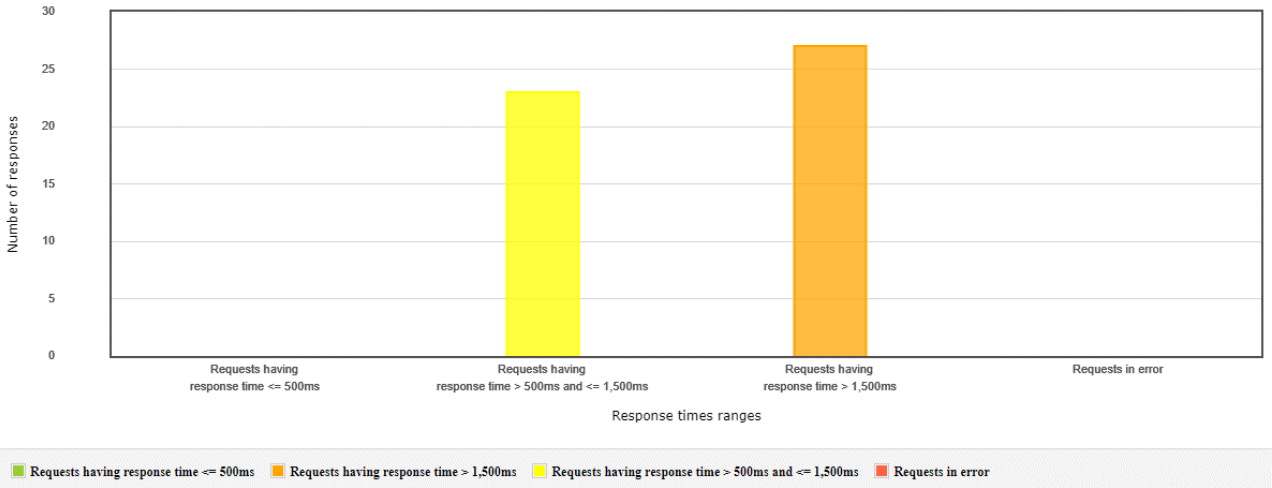


Usuários ativos ao longo do tempo



Visão Geral do Tempo de Resposta

Este gráfico representa a distribuição das requisições nas faixas de tempo de resposta definidas



6.4 Requisitos de Segurança

Esta atividade compreende na avaliação dos seguintes itens:

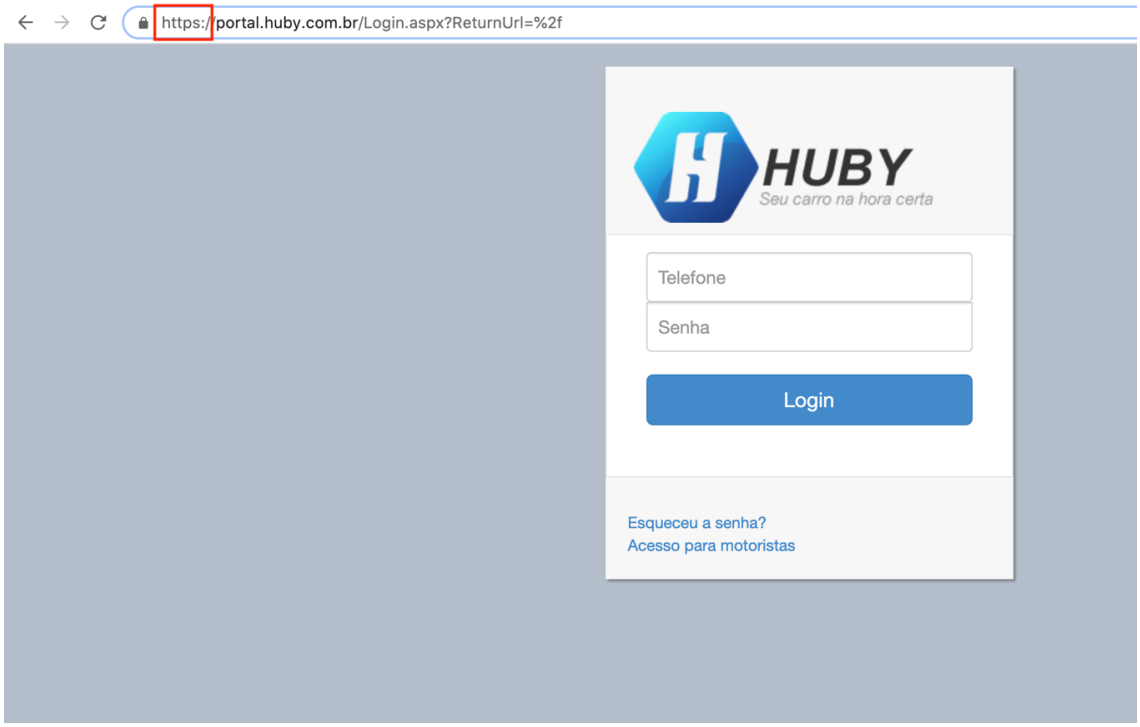
- Site de hospedagem da solução tecnológica com certificado SECURE SOCKETS LAYER
- Solução tecnológica resistente a CROSS-SITE REQUEST FORGERY
- Solução tecnológica resistente a CROSS-SITE SCRIPTING
- Solução tecnológica resistente a INJECTION
- Acesso às funcionalidades da solução tecnológica de acordo com perfis de usuários

6.4.1 Hospedagem

Tipo de avaliação: Conformidade

Estratégia de teste: Verificação manual

Status: Aprovado



6.4.2 Segurança Injection e Cross-site

[redacted]Web

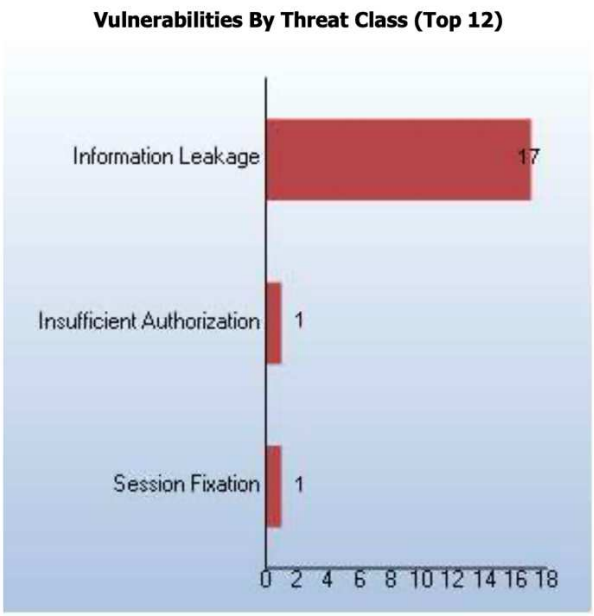
Tipo de avaliação: Automatizada

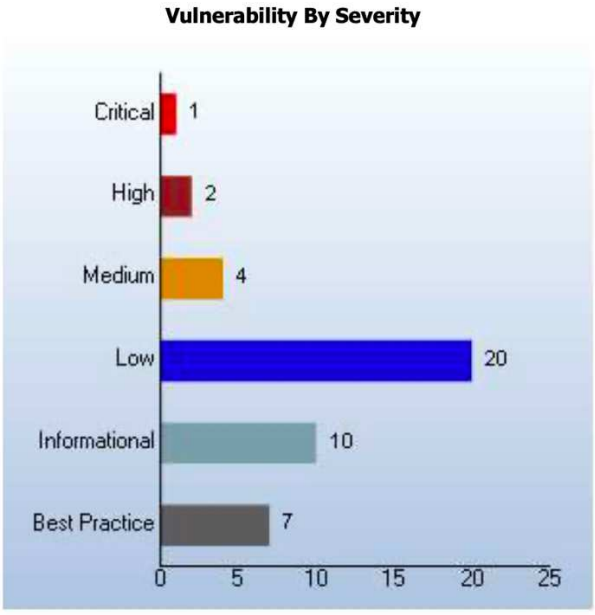
Estratégia de teste: Validação de segurança

Status: Reprovado

Resumo de Inconsistências identificadas na avaliação de Segurança

Tipo	Quant. de Defeitos por Gravidade						Total defeitos
	Impeditiva	Crítica	Alta	Média	Baixa	Muito Baixa	Erros
Segurança	0	5	6	3	50	0	64





Erros corrigidos

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
11285	Insecure Transport: Weak SSL Cipher	Critical	Yes	Fail	1
5665	Insecure Deployment: Unpatched Application	Critical	Yes	Pass	-
5663	phpBB2 Local File Include Vulnerability	Critical	Yes	Pass	-
5658	SQL Injection	Critical	Yes	Pass	-
5207	Cross-Site Scripting: Reflected	Critical	Yes	Pass	-
11293	Cross-Frame Scripting	High	Yes	Pass	-

INJECTION

Falhas de injeção, especialmente de injeção SQL, são comuns em aplicativos Web. A injeção ocorre quando os dados fornecidos pelo usuário são enviados para um intérprete como parte de um comando ou consulta. Os dados hostis do invasor enganam o intérprete e o forçam a executar comandos não pretendidos ou a alterar dados.

Nenhuma vulnerabilidade encontrada

CROSS-SITE SCRIPTING

Falhas XSS ocorrem sempre que um aplicativo inclui dados não confiáveis em uma nova página da Web sem validação ou escape adequado ou atualiza uma página da Web existente com dados fornecidos pelo usuário usando uma API do navegador que pode criar HTML ou JavaScript. O XSS permite que os invasores executem scripts no navegador da vítima, o que pode sequestrar sessões do usuário, desfigurar sites, redirecionar o usuário para sites mal-intencionados, etc.

Nenhuma vulnerabilidade encontrada

Erros encontrados de acordo com o escopo da POC

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
10963	Cross-Site Request Forgery	Medium	Yes	Fail	4

Avaliação de segurança do código contra técnicas de exploração de vulnerabilidades:

CROSS-SITE REQUEST FORGERY

A falsificação de solicitação entre sites (CSRF) é um tipo de ataque que ocorre quando um site, email, blog, mensagem instantânea ou programa mal-intencionado faz com que o navegador da web do usuário execute uma ação indesejada em um site confiável quando o usuário é autenticado. Um ataque CSRF funciona porque as solicitações do navegador incluem automaticamente todos os cookies, incluindo os de sessão. Portanto, se o usuário estiver autenticado no site, ele não poderá distinguir entre solicitações legítimas e falsificadas.

4 vulnerabilidades encontradas

Páginas:

https://portal.huby.com.br:443/Login.aspx
https://portal.huby.com.br:443/CancelarAtendimento.aspx?id=fLOFzn0o2tswdKa2%2f9MshQ%3d%3d
https://portal.huby.com.br:443/Master/Main.aspx
https://portal.huby.com.br:443/relatorio_usuarios.aspx

[redacted] Mobile

6.4.2.2.1 Android

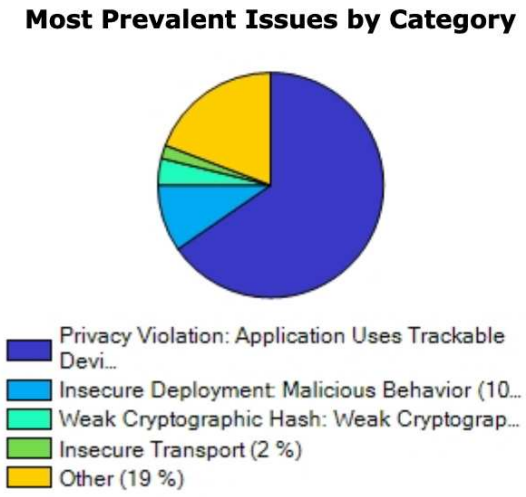
Tipo de avaliação: Automatizada

Estratégia de teste: Validação de segurança

Status: Aprovado

Resumo de Inconsistências identificadas na avaliação de Segurança

Tipo	Quant. de Defeitos por Gravidade						Total defeitos
	Impeditiva	Crítica	Alta	Média	Baixa	Muito Baixa	Erros
Segurança	0	0	0	1	38	0	39



Rating	Category	Test Type	
Medium	Weak Encryption: Weak Code-signing Certificate	Mobile	1
Low	Android Bad Practices: Encryption Secret Held in Static Field	Mobile	1
Low	Insecure Transport	Mobile	1
Low	Privacy Violation: Application Uses Trackable Device Identifiers	Mobile	34
Low	Weak Cryptographic Hash: Weak Cryptography	Mobile	2

Avaliação de segurança do código contra técnicas de exploração de vulnerabilidades:

CROSS-SITE REQUEST FORGERY

A falsificação de solicitação entre sites (CSRF) é um tipo de ataque que ocorre quando um site, email, blog, mensagem instantânea ou programa mal-intencionado faz com que o navegador da web do usuário execute uma ação indesejada em um site confiável quando o usuário é autenticado. Um ataque CSRF funciona porque as solicitações do navegador incluem automaticamente todos os cookies, incluindo os de sessão. Portanto, se o usuário estiver autenticado no site, ele não poderá distinguir entre solicitações legítimas e falsificadas.

Nenhuma vulnerabilidade encontrada

CROSS-SITE SCRIPTING

Falhas XSS ocorrem sempre que um aplicativo inclui dados não confiáveis em uma nova página da Web sem validação ou escape adequado ou atualiza uma página da Web existente com dados fornecidos pelo usuário usando uma API do navegador que pode criar HTML ou JavaScript. O XSS permite que os invasores executem scripts no navegador da vítima, o que pode sequestrar sessões do usuário, desfigurar sites, redirecionar o usuário para sites mal-intencionados, etc.

Nenhuma vulnerabilidade encontrada

INJECTION

Falhas de injeção, especialmente de injeção SQL, são comuns em aplicativos Web. A injeção ocorre quando os dados fornecidos pelo usuário são enviados para um intérprete como parte de um comando ou consulta. Os dados hostis do invasor enganam o intérprete e o forçam a executar comandos não pretendidos ou a alterar dados.

Nenhuma vulnerabilidade encontrada

6.4.2.2.2 IOS

Tipo de avaliação: Automatizada

Estratégia de teste: Validação de segurança

Status: Reprovado

Binário apresentado para o teste de segurança encontra-se corrompido.

6.4.3 Perfis

Tipo de avaliação: Conformidade

Estratégia de teste: Verificação manual

Status: Aprovado

Item Avaliado	Versão	Resultado
Perfil Gestor Master	Visualiza todas as funcionalidades do sistema. Visualiza as corridas, reclamações do centro de custo e de todos os usuários e departamentos.	OK
Perfil Gestor Secundário	Visualiza todas as funcionalidades do sistema, exceto o relatório de auditoria. Visualiza somente as corridas, reclamações, usuários do seu departamento.	OK
Perfil Colaborador	Visualiza somente as funcionalidades de corrida, reclamações, rede credenciada e relatório de corridas finalizados somente de seu usuário.	OK

7 Referências

Evidências e Relatórios completos encontram-se disponíveis no repositório GIT do Ministério da Economia.

Link: https://git.economia.gov.br/rsi/rsi/-/tree/master/TAXIGOV

8 Resultado

Foi realizada um nova rodada de teste no dia 12/08/2020 referente aos itens que foram reprovados: Performance para a solução web, segurança para solução web e mobile IOS, segue parecer da nova análise:

Performance

Web
Foi realizado uma nova verificação após ajustes realizados pela Contratada, a solução tecnológica apresentou tempo de resposta menor que na primeira rodada de testes da POC, na requisição referente à Solicitar Corrida, onde consta média de 3,9 segundos. Logo em conformidade com os requisitos da prova de conceito que sugere o tempo médio de 5 segundos.

Segurança

Web
A solução tecnológica possui vulnerabilidades de gravidade média que têm baixo impacto e alta probabilidade de exploração, possibilitando que dados fornecidos pelo usuário sejam enviados para um intérprete através do navegador com chamada automática com os cookies de sessão, estes problemas representam um risco moderado de segurança para uma aplicação.

Mobile - IOS
Foi encaminhado pela Contratada um novo link para download do arquivo IPA e realizada mais uma (1) tentativa de execução, não foi possível validar a segurança da solução, o arquivo fornecido continua corrompido.

9 Conclusão

Após análise de qualidade da solução tecnológica apresentada pela CONTRATADA referente a Prova de Conceito do processo licitatório para contratação de transporte terrestre - TaxiGov, percebe-se que a solução apresentada não está de acordo com alguns critérios definidos no Item “4 Escopo” deste documento e Anexo E do Termo de Referência.

Diante do exposto, informamos que a solução apresentada não passou nos teste e continua com problemas e em desconformidade com os requisitos estabelecidos.

Leonardo Gonçalves de Oliveira
Coordenador de Projetos
RSI - Informática