

Issues Authenticator	
Plano de Testes	Versão 2.0.0

Issues Authenticator Plano de Testes

Versão <2.0.0>

Issues Authenticator	
Plano de Testes	Versão 2.0.0

Histórico de Revisão

Data	Versão	Descrição	Autor
22/10/2017	1.0.0	Definição da introdução e estratégia de teste	Equipe Cascavel
04/11/2017	2.0.0	Atualização do Plano de Testes	Equipe Cascavel

Issues Authenticator	
Plano de Testes	Versão 2.0.0

Sumário

Introdução	4
Finalidade	4
Escopo	4
Definições, Acrônimos, e Abreviações	4
Referências	4
Visão geral	4
Estratégia de Teste	4
Teste Funcional	4
Prazo para realização	4
Recursos necessários	5
Requisitos a serem testados	5
Casos de Teste	5
Resultados dos Testes	5

Issues Authenticator	
Plano de Testes	Versão 2.0.0

Plano de Testes

1. Introdução

1.1 Finalidade

Este documento tem por finalidade especificar o plano de teste para o sistema Issues Authenticator.

1.2 Escopo

O escopo deste documento está restrito ao teste das funcionalidades do sistema Issues Authenticator. Qualquer alteração em outros sistemas não fará parte do escopo deste documento, sendo este restrito a orientação aos teste do sistema Issues Authenticator.

1.3 Definições, Acrônimos, e Abreviações

ESE - Engenharia de Software Experimental.

1.4 Referências

Título	Versão	Data	Onde pode ser obtido
Plano de Projeto - Issues Authenticator	1.4	01/11/2017	Moodle
Lista de Requisitos - Issues Authenticator	1.4	28/10/2017	Moodle
Casos de Uso - Issues Authenticator	1.3	29/10/2017	Moodle

1.5 Visão geral

Os itens que seguem serão conforme a seguir: Item 2 - discorre sobre a estratégia de testes a ser implementada para o sistema Issues Authenticator, Item 2.1 e seus subsequentes - Lista e identifica os tipo de teste a serem feitos, Item 2.1.1 - especifica os prazos para realização, vislumbrando em que momentos esse tipo de teste vai ser realizado, Item 2.1.2 - lista os recursos necessários para o teste sejam humanos, de software ou de hardware, Item 2.1.3 - lista os requisitos a serem testados, identificando quais requisitos do sistema serão submetidos a esse tipo de teste, item 2.1.4 - lista os casos de teste, descrevendo cenários de teste com dados de entrada e o resultado que é esperado com esses dados. Por fim, o item 3 especifica o resultado obtido após a execução dos testes e as ações tomadas.

2. Estratégia de Teste

Os tipos de testes que serão feitos são:

- testes funcionais

2.1 Teste Funcional

A versão 1.0.0 deste documento está contemplando os testes funcionais para a Sprint 1 do sistema Issues Monitoring, sendo este plano atualizado conforme o decorrer do projeto.

2.1.1 Prazo para realização

Data	Descrição
31/10/2017	Teste do Sistema Pré-Release 1
14/11/2017	Teste do Sistema Pré-Release 2

Issues Authenticator	
Plano de Testes	Versão 2.0.0

01/12/2017	Teste do Sistema Pré-Release 3
------------	--------------------------------

2.1.2 Recursos necessários

Humanos: Um projetista de testes e um testador.

Hardware: Um smartphone com especificações técnicas compatíveis ao software.

Autorização: Acesso autorizado aos laboratórios do ESE.,

Software: O sistema desenvolvido deverá estar previamente instalado e sua versão precisa estar previamente definida e alinhada com o plano de testes.

2.1.3 Requisitos a serem testados

Serão testados os seguintes requisitos:

Código	Descrição
RF01	O sistema deve avisar ao Issues Monitoring que o usuário entrou em um laboratório.
RF02	O sistema deve avisar ao Issues Monitoring que o usuário saiu de um laboratório.
RF03	O sistema deve ser capaz de capturar a intensidade do sinal
RF04	O sistema deve ser capaz de identificar a geolocalização do usuário.
RF05	O sistema deve permitir a configuração das preferências ambientais do usuário.
RF06	O sistema deve enviar as novas configurações das preferências ambientais ao Issues Monitoring.
RF07	O sistema deve receber notificações enviadas pelo Issues Monitoring.
RF08	O sistema deve exibir as mensagens previamente recebidas do Issues Monitoring.
RF09	O sistema deve associar o usuário do Issues Authenticator ao seu respectivo cadastrado no Issues Monitoring.
RF10	Cada cópia do sistema deve possuir um ID único para ser identificado pelo Issues Monitoring.
RF11	O sistema deve permitir a desassociação dos dados que foram armazenados para as autenticações.
RF12	O sistema deve retornar para o usuário uma mensagem sobre o sucesso ou a falha das solicitações.
RF13	O sistema deve avisar o usuário não cadastrado da necessidade de um cadastro prévio.

2.1.4 Casos de Teste

Anexo - Documento de Casos de Teste

Issues Authenticator	
Plano de Testes	Versão 2.0.0

3. Resultados dos Testes

Este capítulo será preenchido quando os testes forem executados.