Projeto Integrador II

Requisitos não funcionais

Integrantes:

* Erik Figueiredo Silva
* Filipe Gabriel de Oliveira da Silva
* Gabriel Barroso dos Santos
* Jéssica Caroline Tou Soares
* Stefany Ramos Vieira

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **REQUISITOS NÃO FUNCIONAIS** | | | | | | | |
|  | | | | | | | |
|  |  |  |  |  |  |  |  |
| **Identificador:** | | RNF001 | | **Categoria:** | | Segurança | |
| **Nome:** | | Autenticação do usuário para realizar pagamento | | | | | |
| **Data de Criação** | | 31/10/2020 | | **Autor:** | | Jéssica Caroline | |
| **Data da Última alteração** | | N/A | | **Autor:** | | N/A | |
| **Versão** | | 1 | | **Prioridade:** | | Alta | |
| **Descrição:** | | O consumidor poderá escolher a forma de pagamento de sua compra que poderá ser em dinheiro no ato da entrega ou através do próprio aplicativo. O aplicativo irá permitir que o consumidor realize o pagamento de sua compra diretamente através do cartão de crédito ou débito.  O consumidor cadastra o cartão de crédito/débito na janela de configurações – pagamentos.  Todas as compras realizadas no software deverão ser verificadas no ato da realização do pagamento quando o ele for escolhido ser realizado via cartão.  Para verificação será feita a autenticação no nível da aplicação, cada consumidor deverá possuir um usuário ativo no sistema. A senha do usuário deverá ser gravada/trafegada utilizando-se criptografia.  Ao finalizar a compra e escolher o pagamento via aplicativo, a autenticação será realizada através da solicitação da digitação da senha do usuário logado.  O sistema não poderá permitir cache de senha, salvamento de senha ou qualquer outro recurso do tipo. | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **Identificador:** | | RNF002 | | **Categoria:** | | Usabilidade | |
| **Nome:** | | Simplicidade de uso geral | | | | | |
| **Data de Criação** | | 04/11/2020 | | **Autor:** | | Erik Figueiredo | |
| **Data da Última alteração** | | N/A | | **Autor:** | | N/A | |
| **Versão** | | 1 | | **Prioridade:** | | Moderada | |
| **Descrição:** | | Um novo usuário deverá ser capaz de fazer um pedido de compra de um novo produto sem nenhuma orientação prévia ou treinamento específico.  O usuário deverá receber um retorno da pesquisa de um determinado produto em um tempo máximo de 5 segundos.  Usuários devem conseguir revisar seu endereço de entrega durante todo o processo de compra.  Usuários devem conseguir alterar sua lista de compras com total facilidade até a confirmação de pagamento, sem precisar retornar várias telas para exercer tal função.  Parceiros (donos de mercados e supermercados) deverão conseguir inserir seus produtos no aplicativo após 30 minutos de treinamento.  A taxa de erros na submissão de pagamentos no ato da compra não deve exceder 10 por cento. | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| **Identificador:** | | RNF003 | | **Categoria:** | | Interoperabilidade | |
| **Nome:** | | Integração com a instituição financeira do pagador | | | | | |
| **Data de Criação** | | 08/11/2020 | | **Autor:** | | Filipe Oliveira | |
| **Data da Última alteração** | | N/A | | **Autor:** | | N/A | |
| **Versão** | | 1 | | **Prioridade:** | | Essencial | |
| **Descrição:** | | O sistema de pagamento do aplicativo deverá fazer conexão com a instituição financeira do pagador, a fim de verificar a disponibilidade de saldo na conta informada e se existe tal cartão informado no momento do pagamento feito on-line.  Para isso é necessário que se desenvolva um Web Service a fim de que se possa fazer a consulta ao banco de dados da instituição financeira para que sejam validadas todas as informações necessárias ao pagamento.  Segundo o Banco Central do Brasil (BCB), toda aplicação Web Service de consulta financeira deve ser homologada via link fornecido pelo próprio BCB (<https://scr.bcb.gov.br/wsscr>).  Protocolos de Segurança: Requisições SOAP são facilmente vulneráveis à ataques, podendo ter seu conteúdo (texto em XML) visto por terceiros. Recomenda-se que a arquitetura de transporte de transporte de requisição seja feita em HTTPS no lugar de HTTP. Toda conexão HTTPS pressupõe a existência de um certificado digital válido no servidor web com o qual a conexão é estabelecida, com isso, a validação do reconhecimento/instalação dos certificados digitas é pré-requisito para a consulto do Web Service.  Obs. : Os demais pré-requisitos e lista de possíveis erros devem ser verificados no próprio site do Banco Central do Brasil, a fim de que se cumpra todas as normas estabelecidas para o uso desse Web Service. | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| **Identificador:** | | RNF004 | | **Categoria:** | | Confiabilidade | |
| **Nome:** | | Requisitos de confiabilidade do sistema | | | | | |
| **Data de Criação** | | 05/11/2020 | | **Autor:** | | Stefany Vieira | |
| **Data da Última alteração** | | N/A | | **Autor:** | | N/A | |
| **Versão** | | 1 | | **Prioridade:** | | Essencial | |
| **Descrição:** | | O backup deve ser feito no servidor todos os dias, 2x ao dia nos horários de 10h e 20h para que possa se manter a segurança de todos os dados de cliente, motoboys e informações das empresas parceiras. Caso o backup não seja realizado, o sistema deverá apresentar uma mensagem de aviso no dia seguinte. A mensagem deverá permanecer em tela por 10 segundos sem possibilidade de ser pulada durante este tempo.  Caso ocorra erros durante processos, sistema deverá apresentar mensagem de erro em tela especificando o erro para o usuário. A mensagem deverá permanecer em tela por 5 segundos.  Ao ocorrer erros não operacionais (erros fatais), tempo de resposta maior do que o esperado ou falha de comunicação o sistema deverá fazer o procedimento de rollback, descartando updates e delets, não realizando commit. Retornando mensagem de erro em tela.  O uso de nobreaks deverá impedir a interrupção inesperada do servidor em caso de queda de energia. Caso ocorra falhas de comunicação entre o app e o servidor, sistema deverá salvar as alterações momentaneamente desde que o sistema ainda esteja aberto. | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| **Identificador:** | | RNF005 | | **Categoria:** | | Disponibilidade | |
| **Nome:** | | Aplicação de Táticas Arquiteturais de Disponibilidade | | | | | |
| **Data de Criação** | | 12/11/2020 | | **Autor:** | | Gabriel Barroso | |
| **Data da Última alteração** | | N/A | | **Autor:** | | N/A | |
| **Versão** | | 1 | | **Prioridade:** | | Essencial | |
| **Descrição:** | | A Disponibilidade refere-se a propriedade do software de estar pronto para executar uma tarefa quando solicitada, sendo assim a recuperação e/ou reparo é um aspecto importante da disponibilidade para que a interrupção de um serviço não supere um intervalo de tempo indedesejado. Sabendo isso, o uso de uma tática arquitetural permite que um erro seja reparado ou mascarado de acordo com a(o) estratégia/método escolhida(o).  Para a Detecção de um erro, podem ser usadas as táticas de *Ping/Echo*, *Heartbeat* e *Exceptions*. Na Recuperação têm-se as táticas de *Voting*, *Active Redundancy*, *Passive Redundancy*, *Spare*, *Shadow Operation*, *State Resynchronization* e *Checkpoint/Rollback*. Para a Prevenção de erros há a *Remove from Service*, *Transactions* e *Process Monitor*.  Como a Disponibilidade refere-se a propriedade do software de estar pronto para executar uma tarefa quando solicitada, por meio do uso das Táticas de Disponibilidade, falhas e erros poderão ser evitados, ou pelo menos limitarão os efeitos do erro levando até a um reparo. | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|