

RESOLUÇÃO Nº 29, DE 30 DE OUTUBRO DE 2025.

Aprova os requisitos e procedimentos para aprovação de Sistemas e Equipamentos de Bilhetagem, incluindo hardware e software, para o serviço de transporte metropolitano.

O CONSELHO DIRETOR DA AGÊNCIA REGULADORA DE SERVIÇOS PÚBLICOS DELEGADOS DO ESTADO DO CEARÁ – ARCE, no uso das atribuições que lhe conferem os artigos 8º, inciso XV, e 11 da Lei Estadual nº 12.786, de 30 de dezembro de 1997, o artigo 3º, inciso XII, do Decreto Estadual nº 25.059, de 15 de julho de 1998, de acordo com a deliberação do Conselho Diretor da ARCE:

CONSIDERANDO o disposto na Lei Estadual nº 18.628, de 18 de dezembro de 2023, que Institui o Programa VaiVem no âmbito do Serviço Regular de Transporte Metropolitano da Região Metropolitana de Fortaleza;

CONSIDERANDO o Decreto Estadual nº 35.787, de 18 de dezembro de 2023, que regulamenta o programa VaiVem Ceará no âmbito do serviço regular de transporte metropolitano, da Região Metropolitana de Fortaleza;

CONSIDERANDO as Concorrências Públicas nº 20240001/ARCE/CCC e nº 20240002/ARCE/CCC, referente à Prestação de Serviço de Transporte Intermunicipal de Pessoas do Estado do Ceará e os respectivos contratos assinados para a prestação do serviço regular e complementar;

CONSIDERANDO a necessidade de regulamentar os requisitos e procedimentos para aprovação de sistemas de bilhetagem eletrônica ou digital de maneira a garantir a segurança e integridade das informações, dados, transações e transmissões das operações realizadas no âmbito do serviço metropolitano.

RESOLVE:

Art. 1º A presente resolução estabelece os requisitos e procedimentos a serem adotados para a aprovação e homologação de sistemas e equipamentos de bilhetagem eletrônica ou digital a serem utilizados na prestação do serviço metropolitano no âmbito dos contratos oriundos das Concorrências Públicas nº 20240001/ARCE/CCC e nº 20240002/ARCE/CCC.

Parágrafo único: os requisitos técnicos e procedimentos detalhados encontram-se no Anexo Único desta resolução.

Art. 2º. Sistemas e ou equipamentos não homologados pela ARCE não poderão ser utilizados no serviço metropolitano.

§1º A utilização de equipamentos não aprovados e homologados pela ARCE implica descumprimento contratual e está sujeita as penalidades previstas em lei e nos respectivos contratos.

§2º Além das sanções e penalidades contratuais, viagens realizadas com equipamentos não homologados serão glosadas, ou seja, a ARCE não considerará sua produção para fins de pagamento e a receita auferida será considerada como receita antecipada.

Art. 3º. No caso de equipamentos e ou sistemas apresentados à ARCE para homologação que venham a ser reprovados, a ARCE, a seu critério e em requisitos considerados menos graves, poderá estabelecer prazo, não superior a 30 dias, para saneamento dos problemas.

§1º Ao fim deste prazo a transportadora deverá apresentar as soluções implementadas, toda a documentação e equipamentos, conforme o caso, para nova rodada de testes e análises visando a homologação.

§2º No caso de nova reprovação o sistema e equipamentos apresentados serão recusados pela ARCE e a transportadora terá um prazo de até 60 dias para apresentar novo sistema e equipamentos. Ao final deste prazo, caso o novo sistema e ou equipamentos não sejam apresentados para homologação, a ARCE poderá promover a extinção do contrato

Art. 4º. Durante as análises e testes para homologação, bem como, durante os prazos estabelecidos para correção de problemas ou apresentação de novos sistemas e ou equipamentos a ARCE poderá, a seu critério, autorizar temporariamente e sem exceder o estritamente necessário permitir que a transportadora utilize os sistemas e equipamentos ainda não homologados.

Art. 5º Independente da homologação de sistemas e equipamentos, a ARCE, com base nos relatórios e análises de sua auditoria técnica poderá determinar melhorias, alterações e correções, estabelecendo prazos para tanto.

Parágrafo único. O descumprimento destas determinações poderá implicar penalidades e sanções previstas em lei e nos respectivos contratos, bem como, para casos mais graves e reincidentes, na extinção do contrato.

Art. 6º As dúvidas suscitadas na aplicação desta Resolução serão resolvidas pelo Conselho Diretor desta Agência.

Art. 7º Esta Resolução entra em vigor na data de sua aprovação, sendo obrigatório que as transportadoras apresentem os equipamentos e a documentação exigida no prazo de até 10 dias úteis.

SEDE DA AGÊNCIA REGULADORA DE SERVIÇOS PÚBLICOS DELEGADOS DO ESTADO DO CEARÁ – ARCE, em Fortaleza, na data da assinatura eletrônica.

Rafael Maia de Paula
Presidente do Conselho Diretor da ARCE

Kamile Moreira Castro
Conselheira Diretora

Carlos Alberto Mendes Júnior
Conselheiro Diretor

Rachel Girão Silva
Conselheira Diretora

Aline Aguiar Albuquerque
Conselheira Diretora

ANEXO ÚNICO

1. Apresentação

Este anexo tem como objetivo apresentar os requisitos básicos a serem cumpridos pelos sistemas e equipamentos de bilhetagem eletrônica ou digital no âmbito dos contratos de prestação do serviço de transporte metropolitano regular e regular complementar a fim de fornecer um guia abrangente para fabricantes, operadores e a própria ARCE, garantindo que os equipamentos e sistemas atendam aos padrões de segurança, interoperabilidade, desempenho e qualidade exigidos para a operação eficiente e confiável dos sistemas de transporte coletivo.

2. Conceitos e definições

- **Validador Eletrônico:** Módulo eletrônico responsável pela leitura e gravação automática em cartões sem contato (Contactless Smart Cards) e pelo processamento da lógica de controle para decisão de acesso. Emite comandos de liberação ou travamento para a catraca eletromecânica.
- **Catraca Eletromecânica:** Dispositivo físico comandado pelo Validador, que autoriza ou impede a passagem do passageiro.
- **Sistema Gerenciador da Garagem (SGG):** Sistema instalado nas garagens que atua como ponte de comunicação entre os Bloqueios Eletrônicos dos ônibus e o Sistema Central da Bilhetagem
- **Sistema de Bilhetagem Eletrônica (SBE):** Sistema instalado em Data Centers em formato nuvem (pública ou privada), que controla a bilhetagem a partir das mensagens recebidas dos validadores e outros sistemas de venda, recarga, cancelamentos e outros pertencentes ao Sistema de Bilhetagem
- **Sistema de Bilhetagem Digital (SBD):** Sistema instalado em Data Centers em formato nuvem (pública ou privada), que controla a bilhetagem a partir das mensagens recebidas dos validadores e outros sistemas de venda, recarga, cancelamentos e outros pertencentes ao Sistema de Bilhetagem em tempo real.
- **Sistema de Bilhetagem Eletrônica Embarcado (SBE Embarcado):** Sistema instalado nos validadores que faz a leitura dos cartões, QR Codes e aplicativos celulares apresentados, faz interface com o SAM, verifica listas de restrição e grava nos cartões as informações de saldo e controle necessárias, é responsável pelo envio e recebimento de informações com o Data Center e tem as regras de negócio parametrizáveis do sistema
- **Sistema de Bilhetagem Digital Embarcado (SBD Embarcado):** Sistema instalado nos validadores que faz a leitura dos cartões, QR Codes e aplicativos celulares apresentados, faz interface com o SAM, verifica listas de restrição e grava no cartão informações de controle que são necessárias, sendo responsável pelo envio e recebimento de informações com o Data Center com as regras de negócio parametrizáveis do sistema

- Módulo de Segurança (SAM - Security Access Module): Módulo que armazena chaves de acesso ao cartão de forma inviolável, garantindo a segurança e autenticando as transações.
- Equipamento de Validação: Conjunto de validador e leitor de dispositivos de pagamento EMV/Contactless, homologados, configurados e acoplados para receber pagamentos.
- Leitor de Dispositivos de Pagamento: Equipamento tecnológico capaz de processar pagamentos de cartões com o padrão EMV/Contactless MIFARE Classic, MIFARE PLUS e CIPURSE
- Certificação EMV L3: Acreditação que garante que uma infraestrutura de pagamentos opera com cartões emitidos sob o padrão EMV, cumprindo integralmente com requisitos de aceitação e processamento de transações de ponta a ponta. [2]
- PCI DSS (Payment Card Industry Data Security Standard): Padrão de segurança de dados para a indústria de cartões de pagamento. [2]
- Software Base: Conjunto de instruções de programação que implementa funções complementares para o funcionamento dos equipamentos de validação no ecossistema.
- API (Application Programming Interface): Conjunto de funções, regras e procedimentos que permitem a comunicação entre diferentes programas de computador.
- SDK (Software Development Kit): Conjunto de ferramentas de desenvolvimento de software que permite a criação de aplicações.
- Centros de Concentração de Mensagens: Local para onde são destinadas as mensagens dos validadores para serem reenviadas para o Data Center. Também responsável pelo recebimento de listas de restrição e correções de código do Data Center e distribuí-las para os validadores.

3. Processo de Homologação

O processo de homologação visa garantir que os validadores e seus sistemas associados atendam aos requisitos técnicos e funcionais estabelecidos. Baseado nas referências, o processo pode ser dividido em etapas distintas:

3.1. Etapa 1: Admissão de Solicitações

Nesta fase inicial, a empresa interessada em homologar o equipamento de validação deve formalizar sua intenção. Isso envolve a submissão de uma solicitação oficial, acompanhada de toda a documentação pertinente. A entidade reguladora ARCE, será responsável por verificar se a solicitação e a documentação apresentada cumprem com todos os requisitos formais e pré-condições estabelecidas para o início do processo de homologação.

3.2. Etapa 2: Adaptação do Software Base e Provas de Laboratório

Após a admissão da solicitação, esta etapa foca na preparação técnica e nos testes em ambiente controlado. Inclui a instalação e configuração de aplicações específicas no leitor de dispositivos de pagamento e no validador. Uma bateria de testes de laboratório é então executada para verificar o cumprimento dos requisitos técnicos detalhados. Esta fase é crucial para identificar e corrigir quaisquer problemas de compatibilidade ou funcionalidade

em um ambiente simulado antes da implantação em campo. A Jiga de testes utilizada é responsabilidade da postulante.

3.3. Etapa 3: Armazenamento de dados, segurança e geração de relatórios e indicadores de controle no Data Center

Verificação do sistema que faz par com o sistema do validador, seu processamento dos dados, guarda, estrutura do Banco de Dados, segurança, e ferramentas de geração de relatórios, gestão de cancelamentos, confecção de listas de restrição e controle de indicadores de negócios, disponibilidade e de performance do sistema.

3.4. Etapa 4: Provas em Produção (Testes de Campo)

A fase final do processo de homologação envolve a realização de testes em ambiente de produção, ou seja, em condições reais de trabalho. O objetivo é avaliar o desempenho do equipamento de validação em situações operacionais diárias. Conforme o modelo, esses testes devem ser realizados em um número mínimo de veículos (e.g., cinco ônibus) e o equipamento deve funcionar ininterruptamente por um período determinado (e.g., dois meses) para uma avaliação completa de seu desempenho e confiabilidade. Nesse período será criada uma base de dados de homologação que receberá os dados vindos dos validadores e sistemas em homologação.

3.5. Etapa 5: Notificação de Resultados e Vigência da Homologação

Ao final das etapas de teste, a entidade reguladora notifica o solicitante sobre os resultados do processo de homologação. Se os resultados forem bem-sucedidos, o equipamento de validação bem como o software correspondente adquire a condição de homologado e é registrado em uma lista oficial, tornando-o apto para uso pelos operadores de transporte. Caso contrário, os equipamentos são devolvidos. A condição de homologado é mantida enquanto o funcionamento contínuo do equipamento puder ser verificado dentro do ecossistema de pagamentos.

4. Requisitos Detalhados de Hardware

Os validadores e sistemas de bilhetagem eletrônica devem aderir a rigorosos requisitos de hardware para garantir funcionalidade, durabilidade e segurança. Os requisitos a seguir são consolidados a partir das especificações da ARCE e do SBE ou SBD:

4.1. Validador Eletrônico

Os Validadores deverão ser construídos e dimensionados de maneira a suportar as condições ambientais, choques e vibrações existentes no interior dos ônibus, obedecendo ao Grau de proteção IP 56 e ao Índice de Proteção Contra Impacto (IK) igual ou superior a 7, bem como atender a todos os requisitos operacionais e funcionais especificados pela ARCE, para garantir um perfeito funcionamento em regime de trabalho contínuo. É necessário, também, que esses Validadores possam interagir com outros equipamentos embarcados via interface serial RS485.

Em relação às transações realizadas, o Validador deverá apresentar:

4.1.1. Índice de erros na contabilização de transações deverá ser inferior a 0,001% (1 erro a cada 1 milhão de transações);

4.1.2. Tempo Médio entre Falhas [Mean Time Between Failure – MTBF] deverá ser de 40.000 horas;

4.1.3. Segurança das transações utilizando o chip SAM, como mecanismo confiável para:

- a) verificação de autenticidade dos dados da mídia pelo administrador/usuário;
- b) execução de ciclo de operações seguro e completo;
- c) atualização de saldo de Crédito de Transporte e dados de viagens do Cartão de Transporte, naquelas cabíveis, mantendo integridade da mesma; e
- d) geração de assinaturas eletrônicas que autenticam as transações.

A conectividade do Validador com ambientes da Região Metropolitana de Fortaleza deverá ser realizada via chips de comunicação, GSM (4G/3G) e GPRS, ou via wifi 802.11 a/b/ac/g/n, e deverá:

- Receber vários tipos de arquivos de dados do SB, dos critérios da política tarifária e de todos os emissores de crédito associados, tais como parâmetros de listas de restrição de usuários, software do Validador e do SAM e, inclusive, arquivos contendo novas chaves do sistema, para gravação no SAM. Os arquivos recebidos deverão estar assinados eletronicamente e o Validador, através do SAM, deverá ser capaz de validá-los e interpretá-los adequadamente;
- Enviar à Central de Operações os arquivos de transações de usuários e de serviço, assinados pelo SAM do Validador, imediatamente após a sua realização no caso de o equipamento estar online ou tão logo seja possível;
- Checar a presença do módulo SAM e impedir qualquer operação caso esteja ausente;
- Executar os comandos do SAM do Validador na ordem estabelecida;
- Receber e atualizar-se com novas versões de software;
- Mediar a atualização do software do SAM;
- Permitir a atualização de chaves primárias do SAM;
- Interagir com o GPS para registrar dados georreferenciados; e
- Integrar-se a outros equipamentos mediante autenticação mútua, através do SAM, conforme a necessidade observada pela ARCE.

4.2. Sistema Gerenciador da Garagem (SGG) - Hardware

Servidor: Deve ser instalado nas garagens ou nos Centros de Concentração de Mensagens do sistema um Servidor com processamento e memória compatíveis para transmissão segura ao Data Center em Nuvem do Sistema, das informações coletadas na Frota de Ônibus que operam na referida Garagem ou se comunicam com o concentrador de serviços;

4.3. Sistema Leitor de Cartões de Bordo - Hardware

As leitoras dos cartões com circuito integrado sem contato são constituídas de interface compatível com o padrão ISO 14443 – tipo A/B, e antena RF (radiofrequência) acopladas aos circuitos lógicos do validador. O cartão deverá ser processado a uma distância de 5 (cinco) a 8 (oito) cm da face frontal do validador, onde está instalada a antena leitora.

A referida leitora deverá aceitar cartões do tipo MIFARE CLASSIC, MIFARE PLUS, DESFIRE-EV1 e CIPURSE.

5. Requisitos Detalhados de Software

Os componentes de software dos validadores e sistemas de bilhetagem eletrônica são cruciais para a funcionalidade e segurança e devem atender aos seguintes requisitos:

5.1. Validador Eletrônico - Software

O Software do Validador deverá ser modular, permitindo que futuras alterações e/ou ampliações sejam implementadas. A linguagem de programação utilizada deverá apresentar velocidade, segurança e portabilidade, sendo utilizadas aplicações que possibilitem alterações comandadas exclusivamente pelo Servidor Central do Sistema de Bilhetagem e transmitidas para os Validadores do Sistema de Bilhetagem, via internet.

Deverão ser implementadas no Software do Sistema de Bilhetagem, dentre outras, as seguintes funções:

- I.Comunicação entre Validador e Servidor nos Data Centers;
- II.Atualização da lista de restrições (Deny List) através de comunicação de internet móvel entre o Validador e o Servidor Central;
- III.Leitura e processamento de parâmetros e funcionalidades;
- IV.Processamento e validação dos meios de pagamento;
- V.Mensagens ao usuário no display;
- VI.Alarmes visuais e sonoros;
- VII.Captura, armazenamento e comunicação de dados biométricos a partir de fotos dos usuários selecionados;
- VIII.Execução de comandos de mudança do estado operacional do bloqueio; e
- IX.Geração de dados operacionais e de arrecadação que permitam extrair relatórios através de interações no Servidor do Sistema de Bilhetagem.

5.2. Câmera para Biometria Facial

Cada Validador deverá ser dotado de câmera destinada à leitura da biometria facial do usuário beneficiário de isenção e de desconto tarifário, para reconhecimento e validação da transação.

Para as categorias de usuários beneficiários de isenção e de desconto tarifário, o Validador realizará uma captura da biometria do beneficiário que utilizou o cartão para processamento posterior de reconhecimento facial.

Nos casos de exigência da biometria facial a categorias de usuários beneficiários de isenção ou desconto tarifário, a informação acerca dessa exigência da biometria facial deverá estar gravada no Cartão de Transporte ou nas listas do Validador.

Como parte integrante ou acondicionada de forma segura em gabinete externo com as mesmas características do Validador, cada Câmera para Biometria Facial deverá atender as seguintes especificações, dentre outras necessárias ao seu pleno funcionamento:

- I.Gabinete sem arestas, com cantos arredondados, vedado contra entrada de poeira e umidade, resistente a impacto e vandalismo;
- II.Lente e LEDs infravermelhos protegidos contra acesso indevido, dificultando a sua retirada. O sistema de fixação seguro deverá facilitar a substituição do equipamento;

III. Grau de proteção IP54 e Índice de Proteção Contra Impacto (IK) igual ou superior a 7. Não serão aceitas soluções que tenham conexões físicas aparentes entre os equipamentos;

IV. Geração de imagens no formato do tipo JPEG;

V. Comunicação para transferência de imagens à Central de Operações via WiFi ou através do chip 4G/ 3G, instalado na própria câmera ou no Validador. As imagens deverão ficar armazenadas na Central de Operações por 30 dias. Depois desse período, serão mantidas apenas as imagens marcadas como suspeitas, até que sejam descartadas ou guardadas definitivamente, em conformidade com Lei específica;

5.3. Sistema Operacional Embarcado

O Sistema Operacional embarcado do Validador deverá ser de tecnologia Linux ou Android, e deverá estar preparado para futuras alterações, caso sejam necessárias, além de implementar facilmente comunicações PPP com redes 3G/4G/5G e WiFi.

Esse Sistema Operacional deverá ser capaz de interfacear com os cartões SAM embarcados no próprio Validador, para a validação das transações NFC em cartões contactless e em QR code.

Os Créditos de Transporte, comprados via aplicativo móvel, referem-se a um conjunto de informações criptografadas onde nenhuma informação fica retida no aplicativo, dessa forma, através de técnicas específicas e processos de segurança, o Sistema Operacional deverá trabalhar com barreiras que impeçam a identificação de dados particulares e criptografa a comunicação entre os servidores, evitando fraudes.

Para a Segurança e Inviolabilidade dos Dados do Sistema Operacional, os dados gerados pelas transações no Validador deverão ser tratados por mecanismos de proteção contra violação, cópias e leitura.

Os dados gerados e armazenados no Validador deverão ser criptografados e só deverão ser acessíveis na Central de Operações por pessoal autorizado e credenciado.

O Sistema Operacional deverá permitir que a incorporação de novos tipos de mídia possa ser feita de maneira transparente a partir de um comando gerado pela Central de Operações, sem que seja necessária a intervenção manual ou física no Validador. Essas novas parametrizações de software, quando necessárias, serão controladas e enviadas por meio de arquivo específico criptografado, gerado pelo Sistema de Bilhetagem, após testes em ambiente de teste e homologação.

O Sistema Operacional deverá possibilitar autonomia para a ARCE ou para a contratada, que poderá alterar taxas, tarifas, formas de cobrança, através de parametrização do sistema, sem a necessidade de alteração no código do sistema embarcado e também sem necessidade de mudança de código no Sistema de Bilhetagem.

5.1.3. Módulo de Acesso Seguro

Para a operação correta do Sistema de Bilhetagem, tendo os criptogramas assinados e baseados em Módulo de Acesso Seguro [Security Access Module – SAM] padrão ISO/IEC 7816, este módulo deverá ser fornecido, juntamente com todos os equipamentos, softwares, módulos e licenças necessárias para sua inicialização e gravação de dados. Para o controle de segurança nas transações que ocorrem no validador, a operação via Módulo SAM é obrigatória, assim como sua possibilidade de expansão para integração futura com outros sistemas de bilhetagem.

A interface de comunicação do Validador deverá suportar, no mínimo, 4 slots para SAM que permitam a gravação das chaves secretas de acesso às mídias de pagamento de forma inviolável. Essas chaves, utilizadas no procedimento de autenticação mútua entre as mídias e a leitora, são transmitidas via radiofrequência, de forma criptografada, possibilitando as operações de leitura e gravação nos cartões.

O módulo SAM deve trabalhar junto com o software do Validador. O conjunto será responsável pela administração de segurança e definição de características do sistema. As regras de negócio deverão estar presentes no Sistema de Bilhetagem.

O SAM deverá ser compatível com ISO-7816 e ter formato ID-000. Deverá estar protegido contra acessos indevidos, homologado pela norma FIPS 140-2 nível 3. SBE ou SBD

Deverá utilizar um Módulo de Segurança de Hardware [Hardware Security Module – HSM], ou um dispositivo físico para proteger as chaves criptográficas, gerando, armazenando e as gerenciando. Esse dispositivo deverá fazer parte da segurança do Sistema de Bilhetagem e deve permitir: criptografar e descriptografar dados, criar assinaturas e certificados digitais, sem alterar a infraestrutura criptográfica de todos os Sistemas. Deverá ainda, utilizar certificados com os padrões de segurança FIPS 140-3.

O SAM deverá permitir:

- I. Obter chaves diversificadas para cada conta de usuário e cada tipo de dados armazenado nele, fornecendo acesso apenas aos dados que cada aplicação manipula, dependendo do perfil definido no próprio SAM, utilizando como fator de diversificação um número único atribuído ao usuário no Sistema de Bilhetagem;
- II. Verificar assinaturas eletrônicas para cada tipo de dado;
- III. Gerar novas assinaturas para novos dados da conta do usuário;
- IV. Verificar assinaturas de pacotes que contêm parâmetros, listas de restrição e novas versões de software;
- V. Assinar registros contendo informações de transações;
- VI. Assinar arquivos que devem ser enviados à Central de Operações; e
- VII. Atualizar-se automaticamente com novas versões de software recebidas.

5.4. Sistema de Bilhetagem Eletrônica ou Digital SB) – Software Central – Data Center

O Software do SB deverá ser modular, permitindo que futuras alterações e/ou ampliações sejam implementadas. A linguagem de programação utilizada deverá apresentar velocidade, segurança e portabilidade.

O SB deverá disponibilizar um conjunto de ferramentas para, de forma remota e em tempo real, viabilizar o acompanhamento, a detecção e o diagnóstico de ocorrências que causem desvios dos processos de bilhetagem na RMF, e, assim, permitir o restabelecimento da operação adequada da bilhetagem.

A plataforma do SB deverá permitir a definição de perfis de administradores para controle de acesso ao sistema, possibilitando controlar quais funcionalidades cada administrador tem ou não permissão de acesso, com respectivas autenticações e senhas individuais.

As principais funcionalidades requeridas ao SB são agrupadas em módulos apresentados a seguir.

5.4.1. Módulos do SB

- a. Módulo de Cadastramento;

- b. Módulo de Comercialização Online de Créditos de Transporte;
- c. Módulo de Rede de Revenda de Créditos de Transporte;
- d. Módulo de Segurança de Rede de Revenda de Créditos de Transporte;
- e. Módulo de Atendimento aos Usuários;
- f. Módulo Antifraude e de Reconhecimento Facial;
- g. Módulo da Central de Processamento de Dados;
- h. Módulo da Central de Operações;
- i. Módulo de Regras Tarifárias;
- j. Crédito Remanescente de Transporte
- k. Módulo de Clearing Financeiro de Recebimentos;
- l. Módulo de Relatórios.

5.4.2. Módulo de Cadastramento

Responsável pelos cadastros necessários à operacionalização do SB, com dados unificados e acessíveis em tempo real,

Cadastro de Usuários Cadastro dos usuários no sistema (usuários pagantes e usuários beneficiários de isenção e de desconto tarifário) para obtenção de Cartão de Transporte, contendo todos os dados exigidos conforme normas específicas às respectivas categorias de usuários.

5.4.3. Cadastro de Dados Operacionais

- Frota: Cadastro contendo a identificação dos ônibus e o respectivo Operador de Transporte;
- Validadores: Cadastro contendo a identificação do equipamento, identificação do SAM [Security Access Module – SAM] associado, fabricante, modelo, ano de fabricação, data de inclusão no SB, vínculo com o ônibus e com o Operador de Transporte e histórico de manutenção;
- Linhas de Transporte Público: Cadastro contendo a identificação das linhas e do respectivo Operador de Transporte;
- Operador de Transporte: Cadastro contendo a identificação da Concessionária que opera os serviços de transporte público do Sistema de Transporte da Região Metropolitana de Fortaleza; e
- Administrador do Sistema SB: Cadastro contendo a identificação das pessoas físicas autorizadas a operar nesse sistema, em seus respectivos perfis de acesso.

5.4.4. Cadastro da Venda de Créditos de Transporte

- Empresa Credenciada de Revenda de Crédito de Transporte: Cadastro contendo a identificação e a caracterização das empresas credenciadas responsáveis pela revenda de créditos de Transporte e os endereços de instalação dos equipamentos de venda e recarga;
- Comprador de vale transporte: Cadastro contendo a identificação das pessoas físicas e jurídicas, compradores de vale transporte,
- Bancos e outras entidades parceiras: Cadastro contendo informações sobre empresas especializadas na operação de transações financeiras, responsáveis pelos

clientes que utilizarão cartões bancários e similares no pagamento das tarifas diretamente nos Validadores;

- Estabelecimentos de ensino: Cadastro contendo informações sobre as instituições que oferecem cursos abrangidos na legislação que permite a concessão de desconto tarifário aos alunos matriculados; e
- Cadastro de parâmetros de operação do SB: Os cadastros de parâmetros para a venda e utilização dos Créditos de Transporte,

5.4.5. Módulo de Comercialização Online de Créditos de Transporte

- Módulo responsável pela comercialização, por meio de canais.

5.4.6. Módulo de Rede de Revenda de Créditos de Transporte:

- Módulo responsável pelo gerenciamento dos termos de credenciamento de empresas para revenda de Créditos de Transporte, assim como pelo monitoramento e controle das transações de revenda através de API [Application Programming Interface – API].

5.4.7. Módulo de Segurança de Rede de Revenda de Créditos de Transporte

- É o módulo responsável pela autorização e pela segurança de todas as transações de revenda de Créditos de Transporte, Módulo de Atendimento aos Usuários.

5.4.8. Módulo de Atendimento aos Usuários

- É o módulo responsável pelo atendimento a demandas dos usuários
- Informação e orientação em geral sobre os meios de acesso ao SB;
- Informação e orientação acerca da solução de defeitos e demais problemas que vierem a ser apresentados pelo Cartão de Transporte;
- Transferência de Créditos de Transporte a novo Cartão de Transporte devido à perda do Cartão físico;
- Disponibilização de sistema de ticketing (registro de chamados), com o objetivo de registrar todas as demandas dos usuários, por qualquer canal;
- Registro do tempo decorrido entre a notificação do problema e sua solução e do tipo de problema apresentado;
- Avaliação de satisfação do usuário atendido; Módulo Antifraude e de Reconhecimento Facial.

5.4.9. Módulo Antifraude e de Reconhecimento Facial

- É o módulo responsável pela prevenção e pela detecção de fraudes, atuando na verificação da utilização indevida dos Cartões de Transporte.
- O Reconhecimento Facial se destina a validar a biometria de usuários, beneficiários de isenções e de desconto tarifário do Sistema de Transporte Metropolitano de Fortaleza, cadastrados no BackOffice no momento do acesso aos Validadores.
- A biometria deverá ser sincronizada com o “Módulo de Cadastramento” e com o “Módulo de Atendimento aos Usuários”, de forma online, e deverá permitir o

processamento das imagens, comparando-as com a biometria de referência registrada no cadastramento. Esse processamento e sincronismo de dados deverão ser automáticos, conforme parâmetros e configurações feitas no SB.

- O Reconhecimento Facial deverá ser inteligente para aprender a identificar o usuário conforme o histórico das imagens coletadas nos Validadores, atualizando (quando couber) a imagem de referência, sem necessariamente precisar que o usuário se desloque ao Posto de Atendimento para coletar uma nova biometria.
- Ao realizar esse processamento de imagens, o SB deverá possibilitar a parametrização de um score para aprovação automática das transações, a partir da análise das imagens capturadas na operação. As transações que não atingirem o score deverão ser submetidas a uma análise humana.
- Caso, após a análise humana se identifique que uma pessoa fez uso de um benefício ao qual não é titular, o SB deve estar pronto para disparar uma Notificação ao usuário, através de e-mail, SMS ou Push Notifications e de aplicativos para dispositivos móveis. Essa Notificação deverá alertar o usuário sobre o ocorrido, convocando-o (quando couber) a comparecer a um Posto de Atendimento e cancelando provisoriamente (se assim for determinado) o Cartão de Transporte de acesso ao Sistema de Transporte Metropolitano de Fortaleza
- Caso a Notificação seja feita por e-mail, SMS ou Push Notifications, deverá ser implementado um sistema de feedback, no qual o usuário poderá clicar em um botão do tipo “Foi você mesmo?”, e recorrer do alerta, de forma a esse usuário ser verificado por um agente humano de fiscalização. Módulo da Central de Processamento de Dados

5.4.10. Módulo da Central de Processamento de Dados

- É o módulo responsável pela verificação da confiabilidade dos pacotes recebidos, descryptografia e verificação de chaves, para depois processar e enviar os dados para os respectivos módulos do SB. Esse módulo é responsável por todo o tratamento dos dados que chegarem ao Data Center, transmitidos pelos diversos ambientes sistema. Módulo da Central de Operações.

5.4.11. Módulo da Central de Operações

- Módulo responsável pela centralização da operação, monitoramento e supervisão do SB, assim como pela centralização do suporte tecnológico do Sistema, objetivando identificar, categorizar, priorizar, investigar, diagnosticar e solucionar eventuais problemas.
- Esse módulo deverá possibilitar o acompanhamento dos movimentos não previstos (a exemplo do aumento ou diminuição drástica no comportamento de um determinado agente, ou de uma determinada linha, e de perda de sinal de telecomunicação), e falhas no sistema como um todo.
- O controle de ocorrência de falhas abrange os seguintes equipamentos e aplicativos, não se limitando a:
 - o Canais de venda;
 - o Validadores;
 - o Captura da transação;

- o Transmissão de dados dos validadores;
- o Processamento das contas de usuários no BackOffice
- o Processamento do Clearing Financeiro de Recebimento.

5.4.12. Módulo de Regras Tarifárias

É o módulo responsável pela gestão da política tarifária e das regras de impedimento de utilização dos Cartões de Transporte contemplando as funcionalidades e mecanismos de integração tarifária.

5.4.13. Crédito Remanescente de Transporte

Possibilidade de se manter o crédito, ou zerar créditos que estão alocados para determinado usuário, em sua conta-corrente, por um período determinado. Exemplo: Créditos comprados há mais de 2 anos e ainda não utilizados.

5.4.14. Módulo do Clearing Financeiro de Recebimentos

- O módulo do Clearing Financeiro de Recebimentos tem a função de controlar, em tempo real, todas as viagens diárias dos usuários (usuários pagantes de tarifa integral e usuários beneficiários de isenção e de desconto tarifário), cujo pagamento seja efetuado por um dos meios de pagamento aceito pelo SB e cuja transação seja validada nos equipamentos acoplados às catracas.
- Esse módulo será o responsável pelo gerenciamento dos processos de arrecadação da Tarifa Pública, abrangendo:
 - o Gerenciar o processo de apuração de arrecadação das receitas oriundas da bilhetagem, obtidas pelos diversos canais de venda e meios de pagamentos envolvidos;
 - o Gerenciar e manter as contas gráficas dos usuários cadastrados, a fim de permitir o controle dos Créditos de Transporte efetuados para os usuários e a sua utilização nos validadores do Sistema de Transporte da Região Metropolitana de Fortaleza;
 - o Conciliar e fazer as alterações nas contas gráficas dos usuários;
 - o Identificar e tratar os indícios e as evidências de fraudes na utilização indevida de meios de pagamento de Créditos de Transporte e de acesso indevido aos serviços de transporte público, por parte dos usuários, assim como de evasão tarifária.
 - o Processar diariamente o fechamento contábil dos movimentos da bilhetagem e dos valores de remuneração da CONTRATADA e do Operador de Transporte, de acordo com as passagens apuradas em cada veículo e os valores de entrada de recursos;
 - o Efetuar eventuais reprocessamentos de fechamentos devido a problemas técnicos na transmissão dos dados e/ou falhas na leitura dos dados dentro das janelas de processamento estabelecidas;
 - o Efetuar a transferência dos valores arrecadados por meio do SB à conta centralizadora do arrecadamento;
 - o Apurar, periodicamente, a consolidação dos resultados financeiros.

- o Emitir relatórios e/ou informes ou arquivos tabulados com campos identificáveis para auditorias e controles;
 - o Fornecer suporte administrativo para os processos de BackOffice, tais como:
 - consolidação dos processamentos diários de receitas tarifárias;
 - auditoria e conciliação de entrada de valores pelos diversos meios de pagamentos;
 - envio de evidências e alertas sobre fraudes constatadas; e
 - apuração periódica de resultados financeiros da operação do SB.
 - o Fornecer suporte de Tecnologia da Informação, adequado ao processamento dos dados provenientes da apuração diária da bilhetagem, bem como o processo de transmissão e processamento dos dados para a realização dos pagamentos apontados no clearing.
 - o Providenciar monitoramento em tempo real de todas as passagens capturadas nos dispositivos móveis ou fixos de validação das transações
- Módulo de Relatórios

Todas as consultas serão em tempo real e os valores deverão estar sincronizados com as informações de quantidade de passagens de usuários. Não poderá haver a inserção manual de dados.

O total de passagens dos usuários, registrado no Módulo do Clearing Financeiro de Recebimentos, deverá ser conciliado diariamente com as movimentações de pagamentos confirmados pelo SB e pelos pagamentos em espécie

- É o módulo responsável pela geração de relatórios sobre a operação do SB, em formato de dashboards e dinâmicos, possibilitando a disponibilização por web services ou APIs e exportação dos dados em formatos comerciais CSV, XLS, XML ou TXT formatado.
- O Módulo de Relatórios deverá abranger os seguintes, mas não se limitando a:
 - o Relatório de quantitativo de usuários cadastrados, discriminado por categoria de usuário;
 - o Relatórios de quantitativo de Créditos de Transporte comercializados, discriminado por canal de venda, meio de pagamento e categoria de usuário;
 - o Relatórios de quantitativo de vales transporte comercializados, discriminado por canal de venda e meio de pagamento;
 - o IV. Relatórios de ocorrências de perdas de Cartões de Transporte, discriminadas por tipo de cartão;
 - o V. Relatórios de cancelamentos de Cartões de Transporte, discriminados por tipo de cartão;
 - o VI. Relatório de quantitativo de emissão de segunda via e de Cartões de Transporte e de reposição dos Créditos de Transporte, discriminados por tipo de cartão;

- o VII. Relatórios de não reconhecimento facial de usuários, discriminados por tipo de Cartão de Transporte;
- o VIII. Relatórios de assertividade do módulo Antifraude e Reconhecimento Facial;
- o IX. Relatório de avaliação de satisfação do usuário atendido, discriminando o tipo de problema e o tempo decorrido entre a notificação do problema e a sua solução;
- o X. Relatórios de passageiros transportados, que assegure a correta apuração do passageiro equivalente;
- o XI. Relatório de cálculo do valor a ser pago às empresas prestadoras de serviço
- o XII. Relatórios de processamento do Clearing.

5.4.15. Formas de Apresentação de Dados e Informações

- Todos os dados e informações da base de dados do SB deverão ser apresentados em forma de dashboards projetados para exibir várias visualizações conjuntas e acessados via Ambiente de Inteligência Empresarial [Business Intelligence – BI].
- Os dashboards deverão ser compostos de elementos configuráveis, tais como: mapas georreferenciados, listas, gráficos, medidores, indicadores e tabelas.
- As visualizações de dados e informações deverão ser projetadas para uso em cenários não assistidos na Central de Operações e assistidos em desktop e aplicativos mobile.

6. Testes e Validação

Os testes e a validação são etapas críticas para a homologação, garantindo que os equipamentos e sistemas funcionem conforme o esperado em diferentes cenários. Os requisitos a seguir são baseados nas especificações da ARCE e do SB:

6.1. Testes de Laboratório Conjunto Validador (SBE ou SBD)

- **Objetivo:** Verificar o cumprimento dos requisitos técnicos em um ambiente controlado.
- **Procedimento:** Instalação e configuração de aplicações no leitor de dispositivos de pagamento e no validador, seguida da execução de uma bateria de testes.
- **Requisitos:** Os testes devem abranger todas as funcionalidades e interfaces do equipamento, incluindo a leitura/escrita de cartões, comunicação com sistemas externos e processamento de lógica de controle.

6.2. Testes em Produção (Testes de Campo – SBE ou SBD Embarcado)

- **Objetivo:** Avaliar o desempenho do equipamento em condições reais de trabalho.
- **Procedimento:** Realização de testes em pelo menos 10 veículos, com o equipamento funcionando ininterruptamente por dois meses.

- Monitoramento: O desempenho e a confiabilidade do equipamento devem ser monitorados continuamente durante o período de testes em campo.
- Coleta de Dados: Coleta de dados de transações, eventos e falhas para análise posterior.

6.3. Testes de Aceitação (ARCE)

- Procedimento: Devem ser realizados testes de aceitação conforme especificado nos documentos técnicos.
- Garantias Técnicas: As garantias técnicas devem ser apresentadas e verificadas durante os testes.

6.4. Testes de Confiabilidade

- MTBF e MCBF: Verificação dos valores de MTBF (Tempo Médio Entre Falhas) e MCBF (Média de Ciclos Entre Falhas) para hardware e software, conforme os requisitos da ARCE.
- Disponibilidade: O sistema e seus componentes devem apresentar uma disponibilidade mínima de 98,5%.

6.5. Testes de Segurança

- Integridade de Dados: Testes para garantir que falhas não causem perda ou alteração de informações.
- Criptografia: Verificação da criptografia nas comunicações, especialmente entre o SAM e a interface do validador.
- Proteção Física: Avaliação da proteção física do SAM contra violações.
- Conformidade PCI DSS: Para sistemas de pagamento, conformidade com o padrão PCI DSS.

6.6. Testes de Laboratório Conjunto Validador (SBE ou SBD)

- Objetivo: Verificar o cumprimento dos requisitos técnicos em um ambiente controlado.
- Procedimento: Instalação dos sistemas em ambiente de homologação
- Integração: Integração com os equipamentos de testes instalados.
- Requisitos: Os testes devem abranger todas as funcionalidades descritas para o sistema, desde cadastros, operações de criação e cancelamento, Clearing, envio de alertas e emissão de relatórios.

6.7. Testes de Aceitação (ARCE)

- Procedimento: Devem ser realizados testes de aceitação conforme especificado nos documentos técnicos.

6.8. Testes de Confiabilidade e Performance

- Disponibilidade: O sistema e seus componentes devem apresentar uma disponibilidade mínima de 98,5%.

6.9. Testes de Segurança

- Integridade de Dados: Testes para garantir os dados só podem ser acessados por pessoas autorizadas
- Criptografia: Verificação da criptografia no armazenamento de dados
- Proteção Física: Avaliação da proteção física do Data Center / Nuvem .
- Proteção Logica – Arquitetura de proteção baseada em firewalls de última geração, estrutura de backup, DRP, aplicação de patches, atualizações de segurança, conformidade com ISO 27001, e processos ITIL e COBIT.

7. Documentação Necessária para Homologação

A documentação é um componente vital do processo de homologação, fornecendo evidências do cumprimento dos requisitos e facilitando a manutenção e o suporte. Os seguintes documentos são exigidos:

7.1. Documentação Técnica do Produto

- Manuais: Manuais completos dos sistemas incluindo procedimentos de instalação, e manuais de operação e manutenção.

7.2. Documentação para Aprovação do Sistema (ARCE)

- Certificado de Adequação Funcional de Validador Eletrônico: Documento que atesta a adequação funcional do validador.
- Autorização de Instalação: Permissão formal para a instalação dos equipamentos.
- Termo de Adequação do Layout Interno do Veículo: Documento que comprova a conformidade da instalação com o layout interno dos veículos.
- Termo de Liberação para Operação do Sistema de Bilhetagem Eletrônica ou Digital: Autorização para o início da operação do sistema.
- Termos de Aceitação do Sistema Gerenciador da Garagem: Documentos que formalizam a aceitação do SGG.
- Autorização para testes do sistema SBE ou SBD: E acesso do ambiente de homologação criado aos equipamentos em homologação e/ou produção.

7.3. Documentação para Solicitação de Homologação (Sistema de Bilhetagem)

- Solicitação de Homologação: Formulário oficial preenchido pelo solicitante.
- Evidência de Operação do Leitor: Documentação que comprova que o leitor independente que integra o validador opera com, pelo menos, outros dois modelos de validadores de diferentes fabricantes.
- Documentação de Conformidade: Evidências de conformidade com padrões como EMV L3 e PCI DSS.
- Comprovada experiência na Gestão de Bilhetagem: para operações de porte semelhante ao da Região Metropolitana de Fortaleza.

8. Manutenção e Suporte

Para garantir a continuidade e a eficiência operacional dos sistemas de bilhetagem eletrônica, são necessários requisitos claros para manutenção e suporte:

- Manutenção: Procedimentos detalhados de manutenção preventiva e corretiva devem ser definidos e seguidos.
- Sobressalentes: Disponibilidade de materiais sobressalentes para manutenção.
- Treinamento: Fornecimento de treinamento completo para operação e manutenção de hardware e software.
- Acompanhamento da Operação Assistida: Suporte e acompanhamento durante a fase inicial de operação.
- Eliminação de Pendências: Garantia de eliminação total de pendências do sistema.
- Apresentação de planos de Backup e Recuperação, DRP e gestão de mudanças.

9. Segurança

A segurança é um pilar fundamental na homologação de validadores e sistemas de bilhetagem, dada a natureza sensível das transações financeiras e dos dados de usuários. Os requisitos de segurança incluem:

- Integridade de Dados: Qualquer defeito no sistema não deve, em hipótese alguma, provocar a perda ou alteração de informações do Sistema de Bilhetagem Eletrônica.
- Criptografia: As comunicações entre o Módulo de Segurança (SAM) e o restante da interface do validador devem ser criptografadas. Os dados pessoais dos usuários de transporte devem ser guardados em Bancos de Dados criptografados.
- Proteção do SAM: O SAM deve possuir proteção física inviolável que impeça a conexão de equipamentos eletrônicos que possam violar a integridade do sistema. Qualquer violação deve causar dano permanente.
- Conformidade com Padrões de Segurança: Para sistemas de pagamento, é crucial a conformidade com padrões internacionais como EMV L3 e PCI DSS.
- Garantia Contra Fraudes: Mecanismos robustos devem ser implementados para garantir a segurança contra fraudes.