PROCESSO 016.797	
Folhas	Nome/Rubrica

ARTESP

AGÊNCIA DE TRANSPORTE DO ESTADO DE SÃO PAULO

Anexo IX

Termo de Referência do Sistema Integrado de Bilhetagem Eletrônica e Monitoramento (SIBEM)

ÍNDICE

1. Descrição da Arquitetura

1.1. Introdução

1.1.1. Situação Atual

A ARTESP - Agência Reguladora de Serviços Públicos Delegados de Transporte do Estado de São Paulo é uma autarquia vinculada à Secretaria Estadual de Governo do Estado de São Paulo, sendo sua atribuição regular os serviços rodoviários intermunicipais de transporte coletivo de passageiros no Estado de São Paulo no âmbito de sua competência.

O sistema de transporte rodoviário intermunicipal de passageiros é executado por meio de permissões, a empresas privadas, para a operação de linhas. Estas empresas são remuneradas por meio das tarifas cobradas, as quais são fixadas em função do coeficiente quilométrico.

O presente documento é parte do processo licitatório de concessão dos serviços rodoviários intermunicipais de transporte coletivo de passageiros.

1.1.2. Objetivo

Este Termo de Referência tem como objetivo estabelecer o escopo básico dos processos de bilhetagem e monitoramento, bem como os requisitos funcionais e técnicos estabelecidos pela ARTESP, a serem atendidos pelo SIBEM - Sistema Integrado de Bilhetagem Eletrônica e Monitoramento das Concessionárias e integrados ao Centro de Controle de Informação (CCI) da ARTESP.

1.1.3. Premissas

As Concessionárias devem fornecer todas as informações do SIBEM para a ARTESP.

As Concessionárias devem fornecer, para cada área de concessão, *logins* e senhas do SIBEM para a ARTESP. Estes usuários podem fazer consultas e downloads, com diferentes níveis de autorização, de toda e qualquer informação do SIBEM, a qualquer momento.

Todos os dados do SIBEM são armazenados pela Concessionária pelo período do contrato. Devem ficar disponíveis para consultas on-line os dados dos últimos 12 meses. Para dados

com mais de 12 meses, a Concessionária deve fornecer as informações solicitadas pela ARTESP em até 48 horas.

Os equipamentos (hardware) e softwares adquiridos pelas Concessionárias para compor o SIBEM e a integração com o CCI devem atender aos requisitos estabelecidos pela ARTESP.

As Concessionárias podem utilizar equipamentos e softwares adicionais, embarcados ou não, de forma a suportar suas aplicações proprietárias, desde que estes não contradigam ou interfiram na operação dos equipamentos básicos definidos neste instrumento e necessários para a integração com o sistema da ARTESP.

A solução de Bilhetagem Eletrônica deve utilizar Cartão Inteligente de protocolo aberto, que permita a interoperabilidade entre todas as Concessionárias para ambas as modalidades (rodoviária e suburbana), considerando o estabelecido no item 2.1.2.1. A prática do uso de mesmo Cartão Inteligente entre diferentes Concessionárias é incentivado, mas facultativo.

1.2. Sistema Integrado de Bilhetagem Eletrônica e Monitoramento

O SIBEM deve controlar e monitorar todo o transporte coletivo realizado pela Concessionária, incluindo a venda de passagens e a cobrança de tarifas.

Para facilitar o entendimento das funções do sistema, o mesmo foi dividido em módulos. Essas funções poderão ser agrupadas da maneira que for mais conveniente operacionalmente e economicamente à Concessionária. O desenvolvimento e manutenção do SIBEM, incluindo todos os seus módulos, são de responsabilidade da Concessionária.

O detalhamento das interfaces entre o SIBEM e o CCI da ARTESP será fornecido ao vencedor do processo licitatório de cada área de operação.

O SIBEM deve:

I. Cumprir solicitações da ARTESP referentes às alterações no sistema, visando atender políticas tarifárias e alterações nas regras de negócio;
II. Adquirir, instalar, manter, gerir e controlar a conectividade e a comunicação de dados entre todos os equipamentos do sistema e a ARTESP;
III. Estar aberto e disponível para auditorias a qualquer tempo, a critério da ARTESP;
IV. Capturar e arquivar todos os dados gerados pelo SIBEM.

1.2.1. Módulo de Cadastro

Consiste na identificação do usuário junto à Concessionária, onde são caracterizados o tipo de usuário e a forma de utilização do cartão, qualificando-o dentro do sistema, bem como permitindo a personalização do cartão inteligente.

Compreende:

I. Cadastramento dos usuários e empresas;
II. Controle do cadastro de beneficiários de isenções totais e parciais de tarifação no acesso ao transporte, de acordo com a legislação vigente;
III. Controle da validade das gratuidades e benefícios tarifários relacionados ao respectivo usuário;
IV. Controle e registro da associação de Cartão Inteligente ao respectivo usuário.

Os cadastros devem estar disponíveis tanto em unidades de atendimento (físicas) quanto por meio de site eletrônico da Concessionária, cabendo a escolha ao usuário. Os locais de atendimento aos usuários são de responsabilidade das Concessionárias.

1.2.1.1. Tipos de Usuários

Os usuários são classificados conforme seu uso. Nesse sentido, há quatro possíveis tipos de usuários e usos cadastráveis, listados a seguir:

I. **Comum:** é habilitado para todos, exceto os de gratuidade. Atende especialmente aos usuários que compram antecipadamente créditos monetários;
II. **Vale Transporte:** é habilitado para os empregados (beneficiários) das empresas adquirentes de Vale Transporte, no transporte suburbano;
III. **Escolar:** é habilitado para os estudantes e professores, beneficiados pela redução do valor da tarifa, conforme regramentos previstos no Anexo V – Política Tarifária, Reajuste e Revisão Tarifária;
IV. **Gratuidades:** é habilitado aos beneficiários conforme legislação vigente e regras previstas no Anexo V – Política Tarifária, Reajuste e Revisão Tarifária.

Cada usuário deve ter um único cadastro. Assim, o Módulo de Cadastro deve permitir o registro de múltiplas classificações de uso para um mesmo usuário, tal que ocorra a manutenção de um único cadastro por usuário. Usuários do tipo gratuidade não possuem

outros usos habilitados. Nesse sentido, o cadastro de demais usuários pode habilitar até três tipos de usos (vale transporte, comum e escolar).

Para viabilizar a comercialização de créditos eletrônicos de VT - Vale Transporte, deve ser realizado o cadastro dos empregadores interessados. Após efetuar o seu cadastro, cabe à empresa empregadora cadastrar os seus empregados. O vale transporte é utilizado somente na modalidade suburbana.

O estudante ou professor interessado no benefício de redução de tarifa deve requerer o benefício junto à Concessionária, conforme Anexo V – Política Tarifária, Reajuste e Revisão Tarifária.

1.2.1.2. Validade do Cadastro de Beneficiários

Os cadastros de beneficiários possuem um período de validade, com possibilidade de renovação, sendo:

I. 5 anos para o usuário gratuidade idoso;
II. 2 anos para os casos de incapacidade definitiva e aposentadoria por invalidez;
III. Pelo período indicado no parecer médico como necessário ao tratamento, limitado ao prazo máximo de 1 ano, para os casos de incapacidade temporária;
IV. 1 ano para o usuário escolar. Este valor pode ser alterado conforme regras disponíveis no Anexo V - Política Tarifária, Reajuste e Revisão Tarifária ou as que vierem a substituí-las.

Todos os períodos de validade devem ser configuráveis por meio de parâmetros do sistema.

A validade das gratuidades e benefícios tarifários é gravada nos cartões pertencentes aos respectivos usuários, sendo de responsabilidade do consórcio a validação legal (comprovação pelos usuários com as respectivas documentações) do direito ao benefício, bem como a atualização do benefício no módulo de cadastro e, consequentemente, no Cartão Inteligente do usuário. A renovação do cadastro de beneficiários deve estar disponível ao usuário em tempo hábil para que o mesmo garanta seu benefício, sem interrupções ocasionadas pelo procedimento de renovação da Concessionária.

1.2.2. Módulo de Cartões

O módulo de cartões compreende as seguintes atividades:

I. Aquisição de cartões;
II. Distribuição de cartões do sistema;
III. Controle da distribuição de Cartões Inteligentes aos usuários e às unidades de comercialização;
IV. Registro de perdas, roubos ou danificação dos cartões pelos respectivos usuários;
V. Gerenciamento das listas de Cartões Inteligentes irregulares;
VI. Emissão e controle de cartões operacionais, se utilizados;
VII. Emissão e controle de cartões de viagem unitária da modalidade suburbana;
VIII. Bloqueio e desbloqueio de cartão;
IX. Restituição de créditos remanescentes no cartão após o seu bloqueio, referentes à aplicação do sistema quando de perda, falha técnica, danificação, roubo ou furto;
X. Informação aos usuários sobre créditos disponíveis em suas contas e tempos remanescentes de validade de utilização do cartão, do cadastro de beneficiário (se for o caso) e dos créditos;
XI. Controle de estoque de cartões, de forma a garantir o atendimento aos usuários;
XII. Inicialização dos cartões, identificando-os, instalando a aplicação de transporte e alimentando a base de dados de cartões;
XIII. Emissão dos Módulos de Segurança de Acesso (SAM);
XIV. Personalização dos cartões, com foto, de acordo com as características dos diversos tipos de usuários e produtos existentes no sistema.

A estrutura do cartão deve permitir que sejam transacionados os créditos correspondentes aos diferentes tipos de tarifas vigentes.

Os Cartões Inteligentes dos usuários de categoria gratuidade e escolar, além de permitir os usos permitidos às demais categorias, servem a estes como comprovantes da sua condição de beneficiários junto à Concessionária.

1.2.2.1. Cancelamento de Cartão Inteligente

Em caso de perda, roubo, furto, falha técnica ou danificação do cartão, o mesmo pode ser cancelado junto à Concessionária, gerando um protocolo, a ser utilizado para a aquisição de um novo cartão e restituição de créditos eletrônicos existentes. Os cartões cancelados são informados de forma on-line aos veículos, atualizando a lista restritiva.

1.2.2.2. Aquisição de Cartões Inteligentes - “Viagem Unitária”

Os Cartões Inteligentes do tipo “viagem unitária” são adquiridos pelos usuários do transporte suburbano junto ao operador, utilizando o terminal de dados integrado ao validador de entrada. A tarifa é calculada de acordo com a informação das coordenadas do ponto de origem fornecidas pelo DGC (Dispositivo de Geoposicionamento e Comunicação) e com a informação do ponto de destino fornecido ao condutor. O valor deste crédito eletrônico é pago ao condutor em dinheiro e é gravado no Cartão Inteligente de viagem unitária.

Complementarmente, a Concessionária pode comercializar o Cartão Inteligente de viagem unitária em outros Pontos de Venda (PDV) da Concessionária, por meio da informação do ponto de embarque e ponto de destino do passageiro. Esta comercialização, assim como todas as demais, deve constar no SIBEM.

1.2.3. Módulo de Comercialização

Este módulo compreende as seguintes atividades:

I. Autorização e emissão dos créditos no sistema;
II. Controle dos créditos no sistema;
III. Distribuição de créditos para os PDV, cartões inteligentes e outros equipamentos e sistemas que trabalham com os créditos;
IV. Venda de créditos nos respectivos PDV;
V. Recarga e registro de operações de recarga;
VI. Débito de créditos;
VII. Disponibilização de equipamentos para consultas de saldos existentes em Cartões Inteligentes dos usuários nas bilheterias, equipamentos de autoatendimento, em loja virtual e aplicativo para dispositivos móveis;
VIII. Aquisição, instalação, manutenção e controle dos equipamentos de recarga e PDV;
IX. Gestão e controle da efetivação das cargas nos equipamentos de recarga e nos Cartões Inteligentes, decorrentes das autorizações de carregamento pré-pagos (listas de recarga);
X. Verificação de dados armazenados no Cartão Inteligente (prazo de validade, titular, classificação de uso e saldos);
XI. Transmissão de transações de recarga realizadas;

XII. Venda e reserva de passagens nos respectivos PDVs;

XIII. Atualização automática de parâmetros e versões de software dos equipamentos de venda de créditos;

XIV. Recebimento do valor da comercialização dos créditos eletrônicos e passagens, pelos meios aceitos pela Concessionária;

XV. Fornecimento de troco ao usuário (cédulas e moedas metálicas);

XVI. Fornecimento de cupom fiscal;

XVII. Eventual reembolso;

XVIII. Emissão de documentos que permitam a comprovação da realização de despesas, para fins contábeis e fiscais, de comprovação de concessão de benefícios e outros que se apliquem, quando devidos por determinação legal e solicitados pelo usuário.

Os pontos de venda (PDV) e as operações realizadas nos mesmos para cada serviço (rodoviário ou suburbano) devem seguir as operações mínimas obrigatórias definidas na tabela a seguir:

Pontos de Venda (PDV)	Operações Mínimas Suportadas	Serviço
Bilheterias	Comercialização de créditos eletrônicos	Rodoviário e Suburbano
	Comercialização de passagens	Rodoviário
Equipamentos de autoatendimento	Comercialização de créditos eletrônicos	Rodoviário e Suburbano
	Comercialização de passagens	Rodoviário
Loja virtual (site)	Comercialização de créditos eletrônicos	Rodoviário e Suburbano
	Reserva de passagens	Rodoviário
Aplicativo para dispositivos móveis	Comercialização de créditos eletrônicos	Rodoviário e Suburbano
	Reserva de passagens	Rodoviário
Terminal de dados	Comercialização de cartões de viagem unitária	Suburbano
Equipamento de venda embarcada*	Comercialização de passagens	Rodoviário

* O equipamento de venda é obrigatório apenas para optantes por venda embarcada, conforme item 1.2.4.3.4.

Quando o Bilhete de Passagem Eletrônico (BP-e), instituído pelo Ajuste SINIEF nº 1 de 2017, ou outro documento fiscal eletrônico que venha a ser instituído tiver seu uso autorizado pela Secretaria da Fazenda do Estado de São Paulo, a comercialização de passagens do serviço rodoviário passa a ser obrigatória também por meio da loja virtual e aplicativo para dispositivos móveis, cancelando-se a função de reserva de passagens.

Os meios de pagamento mínimos disponibilizados nos PDV são os definidos na tabela a seguir:

Pontos de Venda (PDV)	Meios de Pagamento Mínimos
Bilheterias	Cartão de débito, cartão de crédito, créditos de Cartão Inteligente e em dinheiro
Equipamentos de autoatendimento	Cartão de débito, cartão de crédito, créditos de Cartão Inteligente e em dinheiro
Loja virtual (site)	Cartão de crédito
Aplicativo para dispositivos móveis	Cartão de crédito
Terminal de dados	Dinheiro
Equipamento de venda embarcada	Meios de pagamentos a serem propostos pela Concessionária, observada a minimização de transações em dinheiro*

* Conforme item 1.2.4.3.4, a solução proposta para venda embarcada será avaliada no Projeto Inicial.

A oferta de meios de pagamento além dos mínimos definidos, inclusive opções não listadas por ventura aceitas pela Concessionária, podem ser disponibilizados nos PDV.

1.2.3.1. Créditos Eletrônicos

1.2.3.1.1. Vendas de Créditos Eletrônicos

Existem os seguintes tipos de Vendas de Créditos eletrônicos:

I. Para usuários “comum” e “escolar” (conforme classificação disponível no item 1.2.1.1): compra de créditos eletrônicos realizada pelo próprio usuário;
II. Para empresas adquirentes de Vale Transporte – VT: compra de créditos eletrônicos realizada pela empresa empregadora.

As transações de vendas de créditos eletrônicos e vendas de passagens em papel devem ser armazenadas na memória não volátil dos terminais de venda e equipamentos de autoatendimento.

Os equipamentos assistidos e de autoatendimento devem realizar o processo de recarga de créditos mediante autorização de um elemento seguro, que disponha de créditos para transferência aos cartões inteligentes. O Cartão Inteligente constante na lista restritiva não pode ser recarregado.

O dispositivo de segurança e de armazenamento de créditos pode ser:

I. O HSM instalado no CCO da Concessionária, acessível on-line pelo equipamento através de rede de comunicação com o Servidor de Recarga do SIBEM; ou
II. O SAM instalado no equipamento, enquanto existir saldo disponível de créditos para distribuição.

Todos os equipamentos que operam créditos devem ter um chip SAM instalado que permita realizar com segurança as funções de acesso e atualização de dados dos Cartões Inteligentes.

A Carga do Cartão Inteligente com créditos eletrônicos deve ser realizada com auxílio do HSM (recarga on-line) ou do chip SAM (recarga off-line);

Para distribuição de créditos off-line, isto é, através do chip SAM, os equipamentos instalados nas unidades de comercialização devem realizar operações on-line de abastecimento de créditos, acessando, via rede de comunicação, o Servidor de Recarga do SIBEM.

1.2.3.1.2. Restituição de Créditos Eletrônicos no Cartão Inteligente

Para os cartões cancelados e que possuam saldo, a partir do momento em que o usuário efetuou o cancelamento junto ao sistema da concessionária, o sistema deve calcular o saldo a ser restituído, deixando este valor disponível para ser gravado em novo cartão ou ser diretamente restituído para o cliente.

Ao final do período de um ano sem que ocorra qualquer movimentação no cartão, os clientes devem ser informados que possuem saldo e que, salvo realização de movimentação, o mesmo será revertido à ARTESP.

1.2.3.1.3. Controle de Saldos

Para cada Cartão Inteligente deve ser mantido no SIBEM uma conta corrente contendo todas as viagens-utilização (débitos), as recargas realizadas (créditos) e o saldo atualizado. Todos os registros de viagens-utilização e recargas realizadas devem ser verificados, quanto à sua autenticidade, e armazenados em banco de dados do SIBEM, acompanhados da assinatura eletrônica que os autentica.

Em decorrência do Cartão Inteligente do usuário cadastrado no sistema eventualmente possuir saldo negativo, esse é compensado na próxima recarga.

A Concessionária deve arcar com o saldo negativo não recuperado em recarga.

A Concessionária deve informar à ARTESP o saldo de créditos eletrônicos em Cartões Inteligentes em poder dos usuários.

1.2.3.2. Passagens Rodoviárias

1.2.3.2.1. Vendas de Passagens

A Concessionária deve consultar o SIBEM, verificando a disponibilidade de poltrona nas datas e horários solicitados pelo usuário e disponíveis para viagens, considerando as reservas existentes.

Na emissão da passagem, deve ser impresso um número sequencial único fornecido pelo HSM-SAM, que identifica esta transação.

A transação de venda ou reserva de passagens da modalidade rodoviária, quando da utilização de cartão inteligente para armazenamento de créditos eletrônicos correspondentes aos bilhetes adquiridos, deve estar dentro do processo de Segurança do SIBEM, tendo acesso às chaves de escrita e leitura do cartão e obtendo a assinatura da transação de venda através do HSM (se a transação for realizada on-line, com o equipamento conectado ao Servidor de Recarga do SIBEM) ou SAM (se a transação for off-line, desconectado do

Servidor de Recarga do SIBEM), atendendo os requisitos de autenticidade, integridade e confiabilidade.

1.2.3.2.2. Devolução (Cancelamento) de Passagens

O usuário, conforme previsto no Anexo III – Regulamento Complementar dos Serviços, pode efetuar a devolução da passagem para a concessionária, recebendo o valor pago pela mesma de acordo com a Lei. 11.975, de julho de 2009, ou a que vier substituí-la.

1.2.3.2.3. Troca de Passagens

Assim como é permitida a devolução de uma passagem, respeitando os limites de prazos estabelecidos, também é possível efetuar a troca da passagem.

Para tal, deve ser efetuado o cancelamento da passagem atual e então deve ser emitida uma nova passagem para o usuário, utilizando as transações normais de cancelamento e venda de passagem.

1.2.3.2.4. Reserva de Passagens

Todo o processo de controle de reserva de passagens é de responsabilidade e controle exclusivo das Concessionárias. A reserva deve ser realizada no SIBEM, de modo que seja verificada a disponibilidade de poltrona nas datas e horários solicitados pelo usuário e a poltrona reservada não esteja disponível em consultas de reserva e venda posteriores.

1.2.3.2.5. Descontos promocionais

Quando a passagem for vendida com descontos promocionais concedidos pelas Concessionárias, deve ser informado no SIBEM o valor efetivamente praticado.

1.2.3.2.6. Loja Virtual ou Agências de Viagens

Todo o processo de controle de reserva de passagens pela Loja Virtual ou Agências de Viagens é de responsabilidade e controle da Concessionária.

1.2.4. Módulo de Validação e Acesso

O módulo de validação e acesso compreende nas atividades e equipamentos de cobrança de tarifa e validação de acesso, deve ser projetado de forma a prover as atividades:

I. Garantir ao usuário o acesso e o pagamento de tarifas quando este não dispuser do cartão;
II. Os validadores instalados devem ser equipamentos com leitores de cartão inteligente, programados para debitar os valores monetários correspondentes tendo por base as tarifas em vigor. Em particular, devem permitir a concessão das gratuidades e dos descontos de beneficiários e impedir a liberação do validador quando o cartão estiver inserido na lista de cartões inválidos devendo, para tanto, que o validador esteja apropriado das informações e parametrizações necessárias;
III. As transações de viagens realizadas (débito da tarifa nos Cartões Inteligentes) pelos validadores devem ser armazenadas na memória não volátil do validador;
IV. Os validadores devem registrar todas as operações;
V. A inclusão de Cartões Inteligentes na lista restritiva deve ser realizada de forma on-line.
VI. A atualização/troca de dados e software entre o Sistema e os validadores deve ser realizada remotamente pelo Sistema, sem a necessidade de intervenção manual no local onde estejam instalados e que atendam às exigências de segurança quanto à transmissão de dados;
VII. Deve ser mantido o controle dos validadores, principalmente em relação aos riscos de fraudes e falhas desses equipamentos;
VIII. Fornecimento de Cartão Inteligente para viagem unitária na modalidade Suburbana;
IX. Adquirir, instalar, manter e controlar os validadores para utilização nos veículos;
X. Adquirir, instalar, manter, gerir e controlar as barreiras de ônibus;
XI. Adquirir, instalar, manter, gerir e controlar os DGCs - Dispositivos de Geoposicionamento e Comunicação, utilizados nos veículos;
XII. Prover rede de interligação dos equipamentos embarcados com o SIBEM;
XIII. Adquirir, instalar, manter, gerir e controlar os contadores de passageiros;
XIV. Instalar dois validadores nos veículos suburbanos, um junto ao acesso e outro junto à saída;

XV. Ler e processar as informações contidas no Cartão Inteligente, indicando ao usuário a validade ou problemas existentes no Cartão Inteligente, mediante um visor de informações (display);

XVI. No caso de uso de barreira, acionar o controle da barreira permitindo ou não a liberação do usuário segundo o resultado do processamento do Cartão Inteligente;

XVII. No caso de uso de barreira, manter ativa a liberação, após considerar válida a liberação e cancelá-la automaticamente somente após a passagem do usuário pela barreira, sendo que a liberação não poderá ser cancelada por quaisquer outros motivos, inclusive por mudança de estado operacional;

XVIII. No caso de uso de barreira, evitar que o direito de viagem de um Cartão Inteligente válido seja cancelado pela utilização incorreta por parte do usuário imediatamente anterior, como, por exemplo, por movimentação incompleta da barreira (curso parcial);

XIX. Apresentar informação pictográfica de existência de alarme e passagem sujeita a fiscalização;

XX. Apresentação de informação visual e acústica de rejeição do Cartão Inteligente, indicação de passagem liberada, de valor debitado, de saldo, solicitação de reapresentação do cartão e outras;

XXI. Deve ser feita verificação periódica, automática e rápida da versão do software executável;

XXII. Os validadores devem suportar operação ininterrupta 24 horas por dia, todos os dias do ano;

XXIII. O validador deve gravar as informações referentes a outros eventos como:

a) Transações individualizadas de cada Cartão Inteligente, contendo no mínimo as seguintes informações: número lógico do Cartão Inteligente, tipo de Cartão Inteligente, data e hora da transação, prefixo do veículo, ligação, modalidade (rodoviária ou suburbana), tipo de transação (débito ou gratuidade), ponto de origem, ponto de destino, tipo de tarifa, valor debitado, assinatura da transação;

b) Cartões Inteligentes irregulares, com código do motivo da recusa;

c) Ocorrências de falhas durante a operação;

d) Cartões Inteligentes cancelados por constarem na lista restritiva;

e) Horários de início e fim de serviços e meias viagens;

f) Cartões Inteligentes bloqueados.

As transações de usuários e de serviço realizadas no validador devem ser enviadas ao DGC, para que este as encaminhe ao CCO de maneira on-line. As informações geradas na validação devem ser armazenadas em backup nos próprios validadores, com capacidade equivalente a 7 dias de operação, que posteriormente são transmitidos para o banco de dados das garagens e, por fim, transmitidos para a central de operações, atendendo as exigências de segurança.

O processo da transação deve prevenir colisão de informações de mais de um cartão que eventualmente esteja dentro do campo de ação da interface do validador, com suspensão da transação e prevenção de débitos indevidos, inclusive por repetição de leitura/gravação do cartão, antes que haja autorização de acesso/saída do usuário.

Quando diferentes categorias e tipos de créditos coexistirem no mesmo cartão do sistema, este deve obedecer ao critério de parametrização estabelecido no Projeto Inicial.

O software executável do validador deve ser auditável, ou seja, depois de instalado e em funcionamento nos validadores, deve ser possível verificar, mediante comparação com cópia autenticada, se houve qualquer alteração no software executável em operação.

A concessionária deve manter controle de todos os validadores e dos módulos de segurança de acesso (chips SAM) neles instalados, responsabilizando-se pelos riscos de fraudes, falhas e disponibilidade no uso desses equipamentos.

Nos validadores são registrados os parâmetros do sistema, a estrutura tarifária e a lista restritiva (cartões irregulares) para evitar a utilização de Cartões Inteligentes com irregularidades.

1.2.4.1. Utilização dos Cartões Inteligentes

1.2.4.1.1. Comum, Vale Transporte e Escolar

O Cartão Inteligente é apresentado no validador existente na entrada do veículo, sendo registrado no cartão o ponto de origem correspondente à coordenada levantada pelo DGC (Dispositivo de Geoposicionamento e Comunicação).

No ponto de destino, identificado pela apresentação do Cartão Inteligente e por meio da coordenada obtida com o auxílio do DGC, o validador de saída efetuará o cálculo da tarifa que é debitada no cartão do usuário, comparando o ponto de origem com o ponto de destino.

1.2.4.1.2. Viagem Unitária

Para os usuários que não possuem o seu Cartão Inteligente, é utilizado um cartão de viagem unitária, no qual o usuário informa o seu destino ao condutor que registra esta informação no sistema. O sistema calcula o valor da passagem que é paga pelo passageiro ao condutor e grava o direito a esta viagem no cartão de viagem unitária, que é entregue ao passageiro.

No destino, o usuário encosta o cartão no validador de saída que efetua a validação do ponto de destino onde foi apresentado o cartão e o ponto de destino informado pelo o usuário no momento da entrada no veículo.

Se o valor da passagem paga corresponde ao trecho da viagem, o equipamento de recolhimento de cartões recebe o cartão de viagem unitária e a saída é liberada.

Se o valor no cartão de viagem unitária é menor que o valor correspondente ao trecho de viagem, o passageiro deve pagar o valor complementar ao condutor, que atualiza as informações e possibilita a apresentação e recolhimento do cartão viagem unitária, com a respectiva liberação de saída.

1.2.4.1.3. Gratuidades

Os usuários que possuem direito à gratuidade, tais como idosos, pessoas com deficiência, possuem um Cartão Inteligente especial, personalizado e com data de validade, de acordo com o tipo de gratuidade.

Para os usuários que não possuam o Cartão Inteligente próprio e apresentem a identidade para validação da condição de idoso, deve o condutor informar a situação à concessionária e promover a entrada do usuário ao veículo.

1.2.4.2. Processos do Suburbano

Nos processos de Inicialização de Serviço, Abertura de Serviço e Fechamento de Serviço, a autenticidade da identificação do funcionário deve ser verificada e registrada no SIBEM. A cargo da Concessionária, esses processos podem ser automatizados, a fim de diminuir atividades sob responsabilidade manual de seus funcionários e aumentar taxa de entrada de dados.

A tecnologia utilizada deve estar proposta no Projeto Inicial para avaliação e validação da ARTESP.

1.2.4.2.1. Inicialização de serviço

O processo de associação de um determinado veículo a uma linha, quando do início de operação ou mudança durante a operação, deve ser realizada por um funcionário da Concessionária.

1.2.4.2.2. Abertura de Serviço

No início de um turno de operação por um condutor, o mesmo deverá efetuar o seu *login* e informar ao sistema o início da operação (saída da garagem) e/ou do turno.

No instante em que o veículo é ligado, todos os componentes embarcados são sincronizados, possibilitando assim o início da operação.

1.2.4.2.3. Fechamento de Serviço

No final de um turno de operação por um condutor, o mesmo deve efetuar o seu *login* e informar o final de uma operação (retorno para a garagem) e/ou do turno.

1.2.4.3. Processos do Rodoviário

Nos processos de Abertura de Viagem, Abertura do Embarque, Fechamento do Embarque, Embarque de Passageiros Durante a Viagem e Fechamento de Viagem, a autenticidade da

identificação do funcionário deve ser verificada e registrada no SIBEM. A cargo da Concessionária, esses processos podem ser automatizados, a fim de diminuir atividades sob responsabilidade manual de seus funcionários e aumentar taxa de entrada de dados.

A tecnologia utilizada deve estar proposta no Projeto Inicial para avaliação e validação da ARTESP.

1.2.4.3.1. Abertura de Viagem

Uma vez estacionado o ônibus na plataforma de embarque (inicial de partida), o condutor efetua a abertura de viagem, identificando assim o início do embarque.

1.2.4.3.2. Abertura do Embarque

Durante o processo de embarque, os passageiros são contados e registrados. Deve ser tratada pela Concessionária a contabilização de usuários embarcados em garagens, antes dos terminais rodoviários.

1.2.4.3.3. Fechamento do Embarque

Uma vez identificado pelo condutor que o processo de embarque foi completado, é efetuado o fechamento do embarque.

1.2.4.3.4. Embarque de Passageiros Durante a Viagem

É tolerado o embarque durante a viagem. Caso a Concessionária tenha interesse em realizar venda embarcada, a venda e o embarque devem ser registrados no SIBEM. O equipamento de venda embarcada, o processo desta venda e o registro no SIBEM devem ser propostos no Projeto Inicial para avaliação e validação da ARTESP. Um dos quesitos de avaliação é a proposição de soluções que minimizem transações em dinheiro.

1.2.4.3.5. Fechamento de Viagem

Uma vez que a viagem tenha sido completada, o condutor efetua o fechamento da viagem.

1.2.4.4. Contagem de Passageiros

Em todo ponto de parada, são contabilizados os passageiros que entraram no veículo e os passageiros que saíram, gerando um evento que é enviado ao CCO da Concessionária.

Para a modalidade suburbana, estas informações são obtidas dos validadores de entrada e saída do veículo.

1.2.5. Módulo de Atendimento e Informação ao Usuário

O módulo de Atendimento e Informação ao Usuário deve realizar:

I. Registro de consultas, denúncias, reclamações e sugestões por parte dos usuários;
II. Implantar e operar serviço de atendimento ao público.

1.2.5.1. Ouvidoria e Sistema de Atendimento e Informação ao Usuário

A concessionária deve implantar, operar e manter, uma Ouvidoria em consonância com a Lei Estadual nº 10.294, de 20/04/1999, e demais normas legais e infra-legais vigentes, incluindo respectivas regulamentações e normas da ARTESP relacionadas à matéria, sem prejuízo da previsão contratual acerca da implantação de Ouvidoria.

Além disso, deve implantar, operar e manter um sistema de atendimento e informação ao usuário (SAC), nos termos do estabelecido no contrato de concessão, recebendo as comunicações dos usuários por todos os meios de comunicação gratuitamente inclusive a partir de telefones celulares, referentes a consultas; denúncias; reclamações; sugestões; elogios; pedidos de informações; cadastramentos; registro de perdas, registro de roubos e danificação de Cartões Inteligentes; e pedidos de bloqueios e cancelamento de Cartões Inteligentes.

1.2.6. Módulo de Comunicação com Usuário

A comunicação nos terminais rodoviários é realizada com os equipamentos descritos no item 2.3.4. O mesmo conteúdo deve estar disponível em site e em dispositivos móveis, por meio de um aplicativo. Nesses mesmos ambientes devem estar presentes ainda as informações do transporte suburbano.

A entrega das informações de comunicação com o usuário nos terminais deve vir da *web*, de uma fonte centralizada.

A Concessionária deve adquirir, instalar, manter, gerir e controlar os displays, que serão utilizados nos terminais rodoviários.

1.2.6.1. Geração de Informações

Para os displays do Sistema de Informação (Rodoviárias e Terminais), a Concessionária deve apresentar as informações atualizadas, contendo no mínimo:

I. Próximas partidas (horário e plataformas de embarque);
II. Próximas chegadas (horário e plataformas de desembarque);
III. Acontecimentos extraordinários que afetem as viagens, como atrasos, acidentes, entre outros que por ventura ocorram.

1.2.6.2. Consulta de Informações

A Concessionária deve disponibilizar a consulta de informações sobre os serviços rodoviários intermunicipais de transporte coletivo de passageiros, entre elas:

I. Ligações e itinerários;
II. Horários;
III. Tarifas.

Essas informações devem estar disponíveis em vários canais:

I. Sítio eletrônico - Internet;
II. Equipamentos de autoatendimento;
III. Bilheterias;
IV. Central de atendimento (inclusive por telefone);
V. Aplicativo para dispositivos móveis.

1.2.7. Módulo de Integração

1.2.7.1. Rede de Comunicação de Dados

A concessionária deve dimensionar, implantar, operar e manter todas as redes de comunicações, físicas ou não, de transferência de dados, comandos e informações entre todos os componentes do SIBEM, sendo no mínimo:

I. Entre os equipamentos instalados nas unidades de comercialização, nas unidades de atendimento ao usuário e o CCO.

Estas redes de comunicação devem ter características de confiabilidade e disponibilidade que possibilitem pelo menos a realização on-line das seguintes operações:

a) Transmissão de todas as transações de venda de créditos pendentes de envio por parte dos equipamentos;

b) Recebimento das novas versões de parâmetros e software para atualização por parte dos equipamentos;

c) Abastecimento de créditos para distribuição off-line nos equipamentos.

II. Entre os equipamentos instalados nos veículos e o CCO.

Estas redes de comunicação deverão ter características de confiabilidade e disponibilidade que possibilitem a realização on-line das seguintes operações:

a) Transmissão de todas as transações de utilização de créditos e monitoramento de frota, pendentes de envio, por parte dos equipamentos;

i O embarque e o desembarque dos passageiros devem ser registrados e transmitidos ao SIBEM;

ii Posicionamento e informações sobre o veículo (coordenadas GPS), em intervalos de tempo de no máximo 2 minutos, que pode ser parametrizado.

b) Recebimento das novas versões de parâmetros e software para atualização por parte dos equipamentos.

III. Entre o CCO e os equipamentos de informação ao usuário.

Estas redes de comunicação devem ter características de confiabilidade e disponibilidade que possibilitem o acesso on-line ao CCO por parte dos equipamentos, para obtenção de informações operacionais para atualização das informações aos usuários.

IV. Entre o CCO da concessionária e o CCI da ARTESP.

As Concessionárias devem enviar dados ao CCI da ARTESP. O envio de dados deve ser on-line e ter características de confiabilidade e disponibilidade. Com especial atenção para:

a) Transmissão de todas as transações de venda de créditos, utilização de créditos e monitoramento de frota, pendentes de envio, procedentes dos equipamentos instalados em unidades de comercialização e dos equipamentos embarcados nos veículos;

b) Abastecimento de créditos para distribuição off-line nas unidades de comercialização. Os custos das transmissões de dados serão arcados pela concessionária;

c) Informações sobre linhas inter e intra área, veículos, horários, trajeto, número de passageiros por veículo, manutenções, localização por GPS dos veículos (geoposicionamento) e status dos veículos junto à ARTESP (em termos de cadastro, vistorias e fiscalizações).

Além da transmissão dos dados, a Concessionária deve fornecer *logins* e senhas do respectivo CCO para a ARTESP. Estes *logins* devem ter acesso à visualização e download de todas as informações.

1.2.7.2. Envio de Informações para o CCO

Em intervalos de tempo pré-estabelecidos (parametrizado = 2 minutos), o DGC deve enviar as informações para o CCO da concessionária:

I. Posicionamento do veículo;
II. Alarmes;
III. Abertura de portas;
IV. Velocidade instantânea.

Os componentes requisitados e seus detalhamentos são passíveis de atualização, conforme as necessidades de monitoramento identificadas pela ARTESP.

1.2.7.3. Integração entre ARTESP e Concessionária

O processo de integração entre ARTESP e concessionárias dar-se-á por meio da troca segura de informações entre a Concessionária e o CCI da ARTESP, utilizando canais seguros de comunicação. É obrigação da concessionária garantir a comunicação entre o CCI da ARTESP e as informações do CCO. A integração das informações operacionais do SIBEM ao CCI da ARTESP deve ser on-line. A integração dessas informações deve estar prevista no Projeto Inicial.

1.2.8. Módulo de Monitoramento

A Concessionária deve implantar o Centro de Controle Operacional (CCO), com no mínimo os seguintes componentes:

I. Registro das Ocorrências Operacionais;
II. Ouvidoria e Sistema de Atendimento e Informação ao Usuário;
III. Monitoramento das Viagens.

Em relação ao monitoramento das viagens, o CCO deve apresentar em uma única tela o mapa do Estado de São Paulo com localização dos veículos operacionais de toda a frota, linhas realizadas (rota, número da linha, origem e destino), identificação dos veículos (placa), identificação do condutor (nome e foto), viagens em andamento, horários programados de partida e chegada, horários efetivos de partida e chegada, status da documentação, dados de GPS (geoposicionamento do veículo, deslocamento, velocidade atual e velocidade média horária) e demais informações provenientes de equipamentos embarcados (como transações de créditos e contagem de passageiros). Deve, ainda, mostrar a identificação da viagem, lista de passageiros com nomes e documento de identificação, discriminados por tipo de cadastro (conforme item 1.2.1.1).

O CCO deve operar 24 horas ininterruptamente.

Os componentes requisitados e seus detalhamentos são passíveis de atualização, conforme as necessidades de monitoramento identificadas pela ARTESP.

1.3. Segurança

A Segurança é responsável pela geração e verificação da assinatura digital que garante a segurança dos créditos eletrônicos, das informações (transações) e dos cartões do sistema.

Compreendem atividades de segurança: adquirir, instalar e manter os Módulos de Segurança de Acesso (chips SAM) nos equipamentos definidos neste Termo de Referência.

1.3.1. Geração, Armazenamento e Transporte de Chaves Primárias

As chaves primárias constituem a base do sistema de segurança de bilhetagem eletrônica. São utilizadas para derivar as chaves de acesso ao cartão e em todos os algoritmos de criptografia usados nos processos de segurança. Devido ao alto custo computacional dos algoritmos de criptografia assimétricos, são adotados chaves e algoritmos de criptografia simétricos, como o AES.

As chaves devem ser geradas em ambiente seguro, utilizando hardware dedicado (HSM) que garanta a proteção das chaves. Neste processo, as chaves nunca podem trafegar em aberto. Portanto, o processo de geração precisa ser feito por inteiro dentro deste hardware.

Outro requisito importante que deve cumprir o sistema de segurança a ser apresentado pela concessionária é o transporte seguro das chaves do HSM para o SAM, no processo de inicialização deste último. As chaves não podem trafegar abertas (*cleartext*) pela rede, nem serem expostas a nenhuma aplicação, em momento algum.

Para tal, é necessário criar uma chave de transporte dentro do HSM, a partir de um procedimento que utilize duas ou mais frases secretas, em poder de pessoas diferentes, para geração da chave de transporte. Utilizando as mesmas frases secretas é possível, na inicialização do SAM, usando o mesmo algoritmo, gerar e armazenar nele a mesma chave de transporte.

1.3.2. Certificação de Créditos

A rede on-line utiliza um Serviço de Recarga On-line ou Servidor de Créditos, que atua como “ponte” entre o HSM, no papel de Certificador de Créditos e o terminal de venda ou terminal de recarga. O HSM terá como missão permitir a transferência segura de créditos para o cartão do usuário.

O HSM deve permitir a execução da seguinte sequência de operações:

I. Autenticar a solicitação de transferência de créditos: o terminal de venda enviará uma solicitação “carimbada” pelo SAM de PDV, de forma que o HSM possa confiar na origem do pacote. Esta assinatura terá o número de série do SAM como fator de diversificação. O pacote terá ainda contadores de transações do SAM para impedir fraude de repetição de pacotes;
II. Produzir e assinar criptograma de crédito para recarga e atualização de dados da última recarga do cartão, que tenha como único destino possível o cartão cujos dados foram recebidos na solicitação de crédito anterior;
III. Gerar e assinar registro de transação de crédito on-line, que deve ser inserido no banco de dados pelo Servidor de Créditos, para garantir rastreabilidade do processo;
IV. Calcular chave de escrita para atualização de dados no cartão do usuário;
V. Enviar pacote de crédito “carimbado” pelo HSM, contendo chave de escrita, que possa ser interpretado apenas pelo solicitante do crédito: o SAM instalado no equipamento que emitiu a solicitação.

Os créditos a serem transferidos para o cartão do usuário também poderão ser procedentes do SAM instalado no equipamento de venda de créditos.

O módulo SAM se abastecerá de créditos através de uma transação on-line que ocorre através do Serviço de Recarga On-line, que acessa o repositório de créditos do HSM para transferir os mesmos ao SAM e, assim, possibilita a sua distribuição *offline*.

Nesta modalidade de recarga o SAM executa a mesma sequência de operações descrita anteriormente para o HSM.

1.3.3. Fiscalização de Transações de Viagem

No papel de Fiscalizador de Transações de Viagem originadas nos validadores, o HSM instalado no CCO da Concessionária deve ser capaz de garantir a validação de cada uma das transações de viagem recebidas no Sistema Central de Processamento. Todos os dados da transação recebida, incluída a assinatura, devem ser armazenados no banco de dados, o que permite guardar um registro íntegro que pode ser auditado a qualquer momento. O hardware e a modelagem da aplicação do HSM devem garantir o tempo de resposta considerando altos volumes de transação.

1.3.4. Fiscalização de Transações de Créditos

No papel de Fiscalizador de Transações de Crédito originadas nos terminais de venda, o HSM do SIBEM deve ser capaz de garantir, com alto desempenho, a validação de cada uma das transações de crédito realizadas nesses terminais. Devido ao alto volume, o HSM deve apresentar os níveis de serviço requeridos para conferência destas assinaturas.

1.3.5. Certificação de Arquivos

Todas as listas, arquivos de parâmetros, arquivos de software para o validador, terminais de venda e terminais de recarga e SAMs devem ser assinados pelo HSM instalado no CCO da Concessionária, no papel de Certificador de Arquivos.

1.3.6. Geração e armazenamento de crédito

A geração de crédito deve ser realizada em ambiente controlado e seguro. Os atores principais deste processo são dois elementos de hardware, o Cartão para Geração de Créditos e o Repositório de Crédito, que executam aplicações com acesso a serviços criptográficos localizados em cada dispositivo.

O Cartão para Geração de Créditos deve ser um Cartão Inteligente com contato, compatível com ISO 7816. É um cartão de propriedade exclusiva do responsável pela geração de crédito, que armazena a senha solicitada neste processo.

O Repositório de Crédito deve ser um dispositivo seguro, FIPS 140-2 nível 3, para o qual pode ser utilizado o próprio HSM descrito anteriormente.

Para poder efetuar a geração do crédito deve ser estabelecido um canal de comunicação seguro entre o Cartão e o Repositório, em que ambos os participantes se autenticam mutuamente e, após esta autenticação, os dados passam a trafegar criptografados. Usando algoritmos de criptografia assimétricos, como o RSA, o crédito gerado em uma determinada origem, o Cartão para Geração de Créditos, pode ser depositado apenas no destino que iniciou a “conversa” com ele, o Repositório de Créditos, pois neste canal uma mensagem cifrada procedente de um deles somente pode ser decifrada pelo outro elemento.

1.3.7. Transferência de Crédito do HSM para o SAM de PDV

Com o objetivo de garantir maior disponibilidade nas redes de recarga, devendo manter os mesmos níveis de segurança, o SAM do PDV pode armazenar créditos eletrônicos, que serão transferidos para o Cartão Inteligente do usuário, quando da realização de cargas.

O SAM deve manter armazenado um determinado valor de créditos eletrônicos (saldo) armazenado (parametrizado), utilizado na carga dos Cartões Inteligentes. Quando este saldo atingir um determinado valor (parametrizado), a aplicação de vendas de créditos efetua uma solicitação de transferência on-line de créditos eletrônicos da aplicação do HSM para o SAM, utilizando o protocolo ISO-8583.

A condição estabelecida para que a aplicação do HSM realize a transferência dos créditos eletrônicos solicitados é o envio para o HSM, de todas as transações de carga realizadas. A aplicação HSM deve realizar a conciliação do saldo do SAM com os valores utilizados nas cargas.

A aplicação do HSM deve gerar um registro que identifica a transação de *log* de transferência de créditos eletrônicos para o SAM. Esta transação deve ser assinada. Como mínimo, o *log* de transferência deve conter os seguintes campos:

I. NSU (Número sequencial único) da transação;
II. Identificação do SAM;
III. Valor da transação de transferência;
IV. Saldo anterior do SAM (antes da transferência);
V. Data da transferência;
VI. Saldo atual do SAM (após a transferência).

Para assegurar a rastreabilidade deste processo, a aplicação executada no servidor deve armazenar no banco de dados, para cada transação, um registro, chamado *log* de transferência de créditos eletrônicos, contendo informações anteriores, além da própria assinatura do *log*.

A geração da assinatura do *log* de transferência é atribuição apenas da aplicação do HSM.

1.3.8. Transferência de Crédito do SAM para Cartões de Usuário

O processo de recarga de créditos eletrônicos nos cartões dos usuários requer de um elemento de segurança no POS ou PDV, o SAM de PDV, de um Certificador de Créditos (HSM) e de um Repositório de Crédito que garanta a transferência segura do crédito armazenado nele para o cartão do usuário.

Com o objetivo de garantir maior disponibilidade nas redes de recarga, devendo manter os mesmos níveis de segurança, o SAM do PDV poderá armazenar créditos eletrônicos, que serão transferidos para o Cartão Inteligente do usuário, quando da realização de recargas no Cartão Inteligente.

Neste processo, o SAM é responsável pelo fornecimento do valor do crédito eletrônico pela geração das assinaturas dos novos dados do cartão, pois na transação modificam-se tanto o saldo quanto os dados de recarga do cartão. As novas assinaturas e a própria chave de acesso para escrita dos novos dados assinados são fornecidas pelo SAM.

A recarga somente pode ser realizada se confirmada a integridade do cartão antes da operação, o que deve ser feito pelo SAM.

A aplicação do SAM deve reunir em um registro que identifica a transação, chamado *log* de recarga, as informações que a caracterizem e deve gerar uma assinatura para esse conjunto de dados. Como mínimo, o *log* de recarga deve conter os seguintes campos:

I. Tipo de cartão (comum, estudante, VT);
II. Tipo de carteira creditada (comum ou especial);
III. NSU (Número sequencial único) da transação;
IV. Número do cartão;
V. Valor da transação;
VI. Contador de viagens;
VII. Contador de recarga;
VIII. Data da recarga;
IX. Data da compra do crédito (diferente do campo anterior em caso de créditos pré-pagos);
X. Saldo do cartão.

Para assegurar a rastreabilidade deste processo, a aplicação executada no servidor deve armazenar no banco de dados, para cada transação, um registro, chamado *log* de recarga, contendo informações anteriores, além da própria assinatura do *log*.

A transferência de créditos do SAM para o cartão do usuário segue a mesma sequência de operações descrita anteriormente.

1.4. Contingência

A concessionária deve desenvolver um plano de contingência do SIBEM, considerando as diretrizes abaixo relacionadas e submetê-lo à apreciação e aprovação da ARTESP no Projeto Final. O plano de contingência, após aprovado, deve ser implementado junto com o SIBEM.

O plano de contingência do SIBEM deve prever todas as ações e medidas para pronta realização, com vistas a assegurar a continuidade dos processos nos casos de ocorrência anormal com perda ou deterioração nos serviços, cujas consequências possam provocar prejuízos ou sérios danos a pessoas ou a bens patrimoniais da própria concessionária, dos usuários, da ARTESP ou de terceiros.

Tudo que apresenta potencial de gerar uma ocorrência anormal deve constar no plano de contingência do SIBEM, com respectivas ações e medidas preventivas.

O plano de contingência deve, também, definir as responsabilidades, estabelecer organização para atender a uma emergência e conter informações detalhadas sobre as características da ocorrência anormal. Deve ser desenvolvido curso entre os funcionários da concessionária com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais (planejamento de riscos e de recuperação de desastres).

Deve, ainda, descrever as medidas a serem tomadas, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos, como perdas de dados, informações e de receitas, sanções governamentais e problemas judiciais.

Seus itens devem estar documentados e a atualização desta documentação deve ser feita sempre que necessário. Testes periódicos no plano também são necessários para verificar se o processo continua válido. O detalhamento das medidas deve ser o necessário e suficiente para a sua rápida execução.

O plano de contingência deve conter:

I. Identificação dos riscos e definição de cenários possíveis de falha para cada um dos processos críticos, levando em conta a probabilidade de ocorrência de cada falha, provável duração dos efeitos, consequências resultantes e os limites máximos aceitáveis de permanência da falha, sem a ativação da respectiva medida de contingência;
II. Identificação das medidas para cada falha, ou seja, listagem das medidas a serem postas em prática, caso a falha aconteça, incluindo comunicação à própria concessionária, aos usuários, à ARTESP e até mesmo à imprensa;
III. Definição das ações necessárias para operacionalização das medidas cuja implantação dependa da aquisição de recursos físicos ou humanos;
IV. Implantação de alguma forma de monitoramento que possibilite a rápida atuação em casos anormais, com critérios claros de ativação do plano.

Os funcionários da concessionária devem estar familiarizados com o plano, visando evitar hesitações ou perdas de tempo que possam causar maiores problemas em situação de crise.

A concessionária é a responsável por todo eventual prejuízo gerado pela falta da contingência, ou pelo atraso de sua implementação.

A concessionária deve descrever como executará os serviços quando ocorrerem contingências envolvendo quaisquer dos processos, como por exemplo: ataques de intrusão, constatação de fraudes, usos indevidos do sistema, quebra de segurança dos cartões, módulos de segurança de acesso (chips SAM), chaves privadas, criptografia, senhas, software, ocorrência de paralisações de funcionários, etc.

Deve, ademais, prever redundâncias para manter os níveis de serviço no que se refere a:

I. Confiabilidade e disponibilidade das redes de comunicações;

II. Confiabilidade e disponibilidade dos servidores do CCO da concessionária;
III. Confiabilidade e disponibilidade dos HSMs instalados no CCO da concessionária;
IV. Confiabilidade e disponibilidade dos equipamentos instalados nas unidades de comercialização e nos veículos.

O Sistema deve conter uma análise de suas vulnerabilidades, uma lista de possíveis ameaças associadas a essas vulnerabilidades, uma análise dos riscos operacionais associados a cada uma dessas ameaças, bem como um plano de mitigação de riscos operacionais.

Os principais eventos de risco operacional são:

I. Fraudes internas;
II. Fraudes externas;
III. Demandas trabalhistas e segurança deficiente do local de trabalho;
IV. Práticas inadequadas relativas a clientes, produtos e serviços;
V. Danos a ativos físicos próprios ou em uso pela instituição;
VI. Eventos que acarretam a interrupção das atividades da instituição;
VII. Falhas em sistemas de tecnologia da informação;
VIII. Falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição.

O gerenciamento do risco operacional deve prever:

I. Identificação, avaliação, monitoramento, controle e mitigação do risco operacional;
II. Documentação e armazenamento de informações referentes às perdas associadas ao risco operacional;
III. Elaboração, com periodicidade mínima anual, de relatórios que permitam a identificação e correção tempestiva das deficiências de controle e de gerenciamento do risco operacional;
IV. Realização, com periodicidade máxima anual, de testes de avaliação dos sistemas de controle de riscos operacionais implementados;
V. Elaboração e disseminação da política de gerenciamento de risco operacional ao pessoal da instituição, em seus diversos níveis, estabelecendo papéis e responsabilidades, bem como as dos prestadores de serviços terceirizados;

VI. Existência de plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional;
VII. Implementação, manutenção e divulgação de processo estruturado de comunicação e informação;
VIII. Estrutura de gerenciamento do risco operacional capacitada a identificar, avaliar, monitorar, controlar e mitigar os riscos, inclusive decorrente de serviços terceirizados.

Os procedimentos de contingência devem incluir:

I. Manutenção de backup regular das bases de dados;
II. Manutenção de um “site de contingência” sempre atualizado;
III. Backup do servidor e suas configurações (Imagens) completas e atualizadas de servidores vitais para o funcionamento (principalmente os que requerem muito tempo para reconstituição);
IV. Manutenção de senhas em local seguro, mas de fácil acesso às pessoas autorizadas no caso de uma emergência;
V. Profissionais preparados para atuação imediata;
VI. Hardware redundante.

Além disso, o SIBEM deve ser dotado de recursos que permitam:

I. Contingência de energia elétrica desejável de pelo menos 2 horas, para o funcionamento dos equipamentos de recarga de Cartões Inteligentes instalados nas bilheterias de terminais e rodoviárias;
II. Contingência de comunicação com o CCO da concessionária para o funcionamento dos equipamentos de recarga de Cartões Inteligentes instalados nas bilheterias de terminais e rodoviárias;
III. Rápida troca de chaves ou algoritmos de criptográficos dos HSMs e Módulos de Segurança de Acesso (SAM), no caso de quebra da segurança.

1.5. Parâmetros do Sistema

Cada Concessionária deve manter as tabelas de parametrização no seu sistema SIBEM.

Após aprovação da solicitação, a Concessionária efetua a atualização em seu sistema SIBEM, o qual deve estar sempre atualizado (sincronizado) com as mesmas informações existentes no CCI da ARTESP, quais sejam:

I. **Veículos:** contendo todas as características funcionais dos veículos, tais como lotação máxima, área, tipo de veículo, ano de fabricação;
II. **Ligações:** contendo todas as ligações com seus respectivos atributos, tais como pontos de parada e respectivas coordenadas GPS, extensões, horários etc.;
III. **Tarifas:** contendo todos os valores de tarifas correspondentes às ligações ou trechos das ligações com tarifas diferenciadas;
IV. **Equipamentos:** contendo todos os dados dos equipamentos, tais como tipo, marca, modelo, identificação, fornecedor, veículo instalado (equipamentos de bordo), localização, identificação do SAM.

1.6. Níveis de Serviço

O projeto, a implantação, a operação e a manutenção do SIBEM devem ser desenvolvidos de forma que atendam os níveis de serviço descritos no Anexo IV – Índices de Desempenho do Serviço.

Além disso, devem ser registrados e medidos nos equipamentos, sistema e infraestrutura (rede) do SIBEM:

I. Toda vez que ocorrer uma falha;
II. O tempo total para recuperação.

Com base nos dados capturados são estabelecidos valores para o cálculo do tempo médio entre falhas (MTBF) e o tempo médio para reparação (MTTR), que são acompanhados pela ARTESP.

O SIBEM da Concessionária deve atender os requisitos de:

I. Alta confiabilidade;
II. Alta disponibilidade;
III. Alta confidencialidade.

Devem ser garantidos níveis de desempenho compatíveis com o exigido para o desempenho operacional do SIBEM, cabendo salientar a sua grande influência perante a população.

Nível de Serviço do SIBEM: os equipamentos devem estar em operação em 99,999% (noventa e nove vírgula novecentos e noventa e nove por cento) do tempo, ou seja, admite-se apenas a inoperância de até 8,760 horas ao ano.

Caso ocorra indisponibilidade ou mudanças não planejadas no SIBEM, a notificação ao usuário deve ocorrer em até quinze minutos após a identificação automática ou não do problema, como exemplifica a tabela a seguir:

Objeto	Verificar	Método de Coleta
Cluster de Servidores	Disponibilidade	Ativo ou Inativo
Servidores Web	Disponibilidade	Teste dos serviços Monitoramento do uso
Rede interna do CCO	Disponibilidade	Serviço de Echo (PING)
Banco de Dados	Disponibilidade	Query no database

No caso de manutenção planejada, os usuários devem ser informados com os seguintes prazos: uma semana antes, um dia antes e uma hora antes da alteração.

As bases de dados necessárias para o armazenamento de todas as informações e aplicações do SIBEM, tais como cartões Inteligentes, cadastros, transações de viagens, vendas de créditos eletrônicos e outras, bem como as bases utilizadas na administração da segurança do SIBEM (arquivos de chaves dinâmicas e certificados), devem ser mantidas em segurança, com manutenção de backups de acordo com as melhores práticas do setor.

As bases de dados devem ser armazenadas em memórias redundantes de alta confiabilidade e com capacidades suficientes de acordo com as necessidades legais e de informação de cada concessionária.

Todas as informações contidas nas bases de dados devem ser protegidas contra modificações não autorizadas nos diversos níveis de autorização sempre acompanhadas das assinaturas que certificam tais informações como fidedignas, de forma a permitir verificações de autenticidade em eventuais processos de auditoria.

1.7. Auditoria

O SIBEM deve possuir rotinas automáticas de auditorias que validem a integridade de todos seus processos, como por exemplo, a consistência do saldo de um Cartão Inteligente com a sua movimentação de débito e crédito.

As rotinas de auditoria devem definir mecanismos automáticos e procedimentos associados que registrem todas as atividades importantes do SIBEM.

Algumas características destas rotinas são:

I. Registro de atividades relevantes, isto é, quaisquer atividades que possam potencialmente estar relacionadas com algum tipo de ataque;
II. O esquema de auditoria deve causar o menor impacto possível sobre as rotinas normais do SIBEM, não causando impacto significativo em desempenho e disponibilidade;
III. A informação de auditoria deve ser armazenada de maneira uniforme e com facilidade de acesso na consulta e interpretação;
IV. A informação de auditoria deve ser protegida contra ataques;
V. A identificação e a autenticação estão relacionadas às rotinas de auditoria. O SIBEM deve ser capaz de identificar corretamente a entidade responsável por operação registrada;
VI. O SIBEM deve manter uma base de dados sobre operações realizadas e respectivas participações de entidades, permitindo o exame específico das ações de uma ou mais entidades. Os dados da base de dados do SIBEM devem estar sempre acompanhados de assinaturas criadas em tais operações, que certificam a autenticidade desses dados. Essas assinaturas devem ser geradas com auxílio de HSMs (*Hardware Security Module*) instalados no CCO das concessionárias.

A ARTESP irá definir procedimentos específicos de auditoria, cabendo a concessionária corrigir e se adequar aos problemas encontrados nas auditorias. Além disso, a concessionária deve:

I. Transmitir e permitir à ARTESP, total acesso e controle dos dados e informações armazenados;
II. Capturar e arquivar todos os dados gerados pelo SIBEM;
III. Conceder acesso on-line e controle total da ARTESP ao banco de dados de bilhetagem, que possibilite à obtenção de informações referentes à operação do transporte, emissão, comercialização e compensação dos créditos eletrônicos previamente autorizados e emitidos no SIBEM. Deve ser disponibilizado canal de comunicação que garanta acessos a relatórios básicos, bem como a extração de quaisquer informações disponíveis no banco de dados, que é definido no Projeto Inicial;
IV. Pelo *login* e senha do SIBEM fornecido à ARTESP, esta pode consultar e fazer download de toda e qualquer informação do SIBEM, a qualquer momento;
V. Permitir à ARTESP auditar o código fonte e executáveis dos sistemas que fazem parte do SIBEM.

2. Equipamentos

Todos os equipamentos utilizados, independentemente das especificações técnicas mínimas presentes neste Termo de Referência, devem seguir as legislações, normas e regulamentos a eles relacionados.

2.1. Equipamentos de Segurança

2.1.1. HSM - *Hardware Security Module*

É um dispositivo de hardware que permite o armazenamento seguro das chaves primárias e a execução de algoritmos de *hashing*, criptografia simétrica e assimétrica com alto desempenho.

A concessionária deve utilizar um sistema de segurança baseado no uso de HSMs, detalhando fabricante, algoritmos de criptografias suportados, índices de desempenho e facilidades de escalabilidade.

O HSM deve ser um equipamento tipo *appliance*, com interface para conexão em rede local. Deverá também estar capacitado para:

I. Gerar de forma segura as chaves primárias do sistema de segurança (um ou mais lotes caso necessário).
II. Proteger as chaves primárias geradas. O HSM precisa cumprir com rigorosas exigências de segurança para garantir que as chaves fiquem protegidas sob “lacre” inviolável, jamais possam ser acessadas por nenhum tipo de invasão nem exportadas em aberto. Em caso de tentativa de invasão, o HSM deve destruir as chaves e parâmetros críticos de segurança;
III. Gerar e verificar assinaturas de *logs* de transações usando as chaves primárias geradas;
IV. Gerar e verificar assinaturas de arquivos usando uma das chaves primárias geradas. Os arquivos de parâmetros, de listas de restrição e de software devem ser assinados pelo HSM;
V. Hospedar e proteger a aplicação criptográfica que contém as funções de segurança do sistema. Deve garantir que não seja possível realizar alterações indevidas na aplicação, *debug* ou decompilação para engenharia reversa e que somente aplicações devidamente autorizadas possam ser colocadas ou atualizadas no interior do HSM;
VI. Realizar backup das chaves primárias e recuperar tais chaves apenas em hardware do mesmo tipo, sem exposição das chaves em aberto em qualquer canal de comunicação ou para qualquer aplicação fora do HSM;
VII. Executar funções de criptografia simétricas e assimétricas em hardware, com altíssimo desempenho;
VIII. Gerar chaves de acesso diversificadas para os cartões do usuário usando as chaves primárias geradas;
IX. Autenticar qualquer aplicação que deseje utilizar os serviços do HSM mediante mecanismos seguros de autenticação mútua;
X. Servir como repositório de crédito;

XI. Permitir hospedar várias aplicações criptográficas, com chaves e repositórios de créditos independentes, garantindo a não interferência entre aplicações.

Para garantir a proteção das chaves e parâmetros críticos de segurança, o HSM a ser oferecido pela concessionária deve ser certificado pela norma FIPS 140-2 nível 3. O certificado FIPS (*Federal Information Processing Standards*) é oferecido pelo *National Institute of Standards and Technology* (NIST) e especifica as exigências de segurança que devem ser preenchidas pelas soluções de criptografia. O certificado FIPS 140-2 nível 3 garante que o hardware está protegido contra:

I. Violação física do equipamento;
II. Desligamento da rede de alimentação por tempos acima do normal;
III. Acessos de usuários não autorizados;
IV. Tráfego de chaves.

A tecnologia adotada para o HSM deve permitir uma fácil e rápida escalabilidade, que permita, em um prazo máximo de 48 h, aumentar a capacidade de processamento do HSM, executando nesse período os seguintes processos:

I. Instalação e configuração do HSM;
II. Replicação segura de chaves primárias;
III. Instalação e configuração de servidores criptográficos para acesso e utilização da nova capacidade de processamento.

2.1.2. Geração, armazenamento e transporte de chaves primárias

2.1.2.1. SAM

O Módulo de Segurança de Acesso - SAM (*Secure Access Module*) é um dispositivo de hardware utilizado para proteger o acesso ao Cartão Inteligente, disponibilizar algoritmos de criptografia e regular o comportamento das aplicações que manipulam esses cartões.

O SAM deve ser compatível com ISO-7816 e ter formato ID-000. Deve estar protegido contra acessos indevidos, homologado pela norma FIPS 140-2 nível 3. Essa proteção faz se necessária, pois o SAM, em um modelo de segurança com criptografia simétrica, como o utilizado no Sistema de Bilhetagem, armazena as chaves primárias do sistema e os algoritmos que permitem executar operações criptográficas utilizando essas chaves.

O SAM deve permitir, em equipamentos como validadores, DGCs e dispositivos de venda de créditos:

I. Obter chaves diversificadas para cada cartão 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 o número de série do cartão;
II. Verificar assinaturas eletrônicas para cada tipo de dado;
III. Gerar novas assinaturas para novos dados do cartão;
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 ao sistema central;
VII. Atualizar-se automaticamente com novas versões de software recebidas.

É importante também ressaltar que o SAM a ser adotado deve permitir armazenar separadamente várias aplicações, cada uma com seu conjunto de chaves, para garantir interoperabilidade segura entre diferentes gestores do sistema de transporte. O SAM deve permitir a separação física das chaves e aplicações de cada gestor e a atribuição individualizada de permissões para obtenção de chaves de acesso aos cartões emitidos pelos outros gestores, conforme critérios utilizados na criação do SAM.

Cada chip produzido deve ter a garantia de procedência e identificador único, determinando inclusive o fabricante.

Os chips SAMs são especializados, sendo no mínimo os seguintes:

I. SAM para inicialização do chip
II. SAM para operação de crédito
III. SAM para operação de débito
IV. SAM com operação de crédito e débito

Este procedimento vai garantir os padrões de qualidade, segurança e o protocolo aberto definido pela ARTESP. Todo chip produzido deve ter um identificador único que permita o rastreamento do fabricante e do próprio chip.

2.1.2.2. Máquina de Estados

O módulo SAM deve ser capaz de controlar o fluxo das aplicações instaladas nos equipamentos do Sistema de Bilhetagem. Para tal o SAM utiliza uma máquina de estados, que força as aplicações a executar regras de negócio específicas, em determinada ordem, e define as transições de estado que garantam um fluxo seguro de operações.

Cada tipo de SAM tem sua própria máquina de estado, para executar as operações próprias em uma sequência segura. Cada operação da máquina de estado no SAM deve gerar um código *hash* de estado derivado dos dados utilizados na operação, que serve de entrada na próxima fase do processo.

Segue uma típica ordem de execução que deve ser utilizada como guia para implementação:

I. Fornecer chaves de acesso de leitura ao cartão, com base no número de série;
II. Verificar assinatura eletrônica de todos os dados do cartão. Se for detectado qualquer problema de integridade, retornar ao estado inicial da máquina de estados;
III. Gerar assinaturas eletrônicas para os novos dados do cartão, utilizando como referência para validação os dados atuais e os novos dados. Esta operação dependerá do tipo de SAM, que definirá os níveis de acesso aos diferentes tipos de dados do cartão;
IV. Gerar assinatura de registro da transação, conforme o tipo de operação.

2.1.3. Utilização de itens de segurança

Os equipamentos devem utilizar itens de segurança para assinar a realização de ações ou ler dados encriptados no cartão, conforme tabela abaixo:

	Ação	Equipamento	Segurança mínima
Rodoviário e Suburbano	Inicialização Cartão	Cartão	SAM
	Venda de Crédito	Terminal de Venda e Equipamento de Autoatendimento	SAM
	Recarga	Equipamento de Recarga, Terminal de Venda e Equipamento de Autoatendimento	SAM
	Armazenamento de Crédito	Equipamento de Recarga, Terminal de Venda e Equipamento de Autoatendimento	HSM ou SAM
	Ler e verificar dados do cartão inteligente (prazo, validade, saldos e autenticidade)	Validador, Equipamento de Recarga, Terminal de Venda, Equipamento de Autoatendimento e Aplicativo para dispositivos móveis	SAM
	Registro de Bloqueio do Cartão	Validador, Equipamento de Recarga, Terminal de Venda e Equipamento de Autoatendimento	SAM
	Atualizar-se com versões e parâmetros	Validador, Equipamento de Recarga, Terminal de Venda, Equipamento de Autoatendimento, DGC, Terminal de Dados e Contador	HSM ou SAM
	Eventos de monitoramento	DGC	SAM ou Serial
Rodoviário	Reserva	Loja virtual (site) e Aplicativo para dispositivos móveis	HSM ou SAM
	Venda Passagem	Terminal de Venda e Equipamento de Autoatendimento	HSM ou SAM
	Troca de Passagem	Terminal de Venda	HSM ou SAM
	Contagem de Passageiros	Contador de Passageiros	SAM
	Abertura de Viagem	A definir pela Concessionária	SAM

	Ação	Equipamento	Segurança mínima
	Embarque	A definir pela Concessionária	SAM
	Fechamento de Embarque	A definir pela Concessionária	SAM
	Desembarque	A definir pela Concessionária	SAM
	Fechamento da Viagem	A definir pela Concessionária	SAM
Suburbano	Ler e verificar dados do cartão de viagem unitária (saldos e autenticidade)	Terminal de Dados	SAM
	Registro de Bloqueio do Cartão de viagem unitária	Terminal de Dados	SAM
	Débito de Viagem	Validador	SAM
	Envio das informações do validador ao DGC	Validador	SAM
	Pagamento de valor complementar da passagem unitária	Terminal de Dados	SAM
	Entrada de idoso apresentando a identidade	Validador	SAM
	Registro de entrada e saída	Validador	SAM
	Inicialização de Serviço	A definir pela Concessionária	SAM
	Abertura de Serviço	A definir pela Concessionária	SAM
	Fechamento de Serviço	A definir pela Concessionária	SAM

2.2. Equipamentos Embarcados

2.2.1. Comuns ao Suburbano e Rodoviário

2.2.1.1. Validadores

O validador tem como função principal verificar se o cartão apresentado pelo usuário o autoriza a realizar a viagem. Para tal, o validador deve checar a autenticidade do cartão através do módulo SAM e, posteriormente, efetuar a transação de débito no cartão do usuário.

O resultado da transação deve ser informado no display do validador, com sinais luminosos e com sinais sonoros diferenciados.

Caso seja do interesse da Concessionária, o validador pode ser utilizado para os procedimentos de inicialização, abertura e fechamento de serviço suburbano e ainda na abertura de viagem, abertura e fechamento de embarque, embarque de passageiros durante a viagem e fechamento da viagem do serviço rodoviário.

2.2.1.1.1. Requisitos dos Equipamentos

Para poder operar no Sistema de Bilhetagem os validadores devem possuir os seguintes requisitos mínimos:

I. Leitor de cartão eletrônico sem contato, compatível com ISO 14.443 A e B, distância máxima de operação de 100 mm;
II. Pelo menos um soquete disponível ID-000 para o chip SAM, e interface de comunicação em estado operacional com este dispositivo;
III. Uma porta de comunicação RS-485 disponível para interface com dispositivo de Geoposicionamento e comunicação, ou placa de GPS e modem para chip 4G integrado;
IV. Microprocessador com função de *boot loader* para atualização de software;
V. Memória volátil para execução de programas;
VI. Memória não volátil suficiente para armazenamento de parâmetros e *logs* de transações e operações realizadas;
VII. Display de caracteres de duas ligações para interface com os usuários e o operador;

VIII. Sinal luminoso verde para indicar transação de usuário bem-sucedida;
IX. Sinal luminoso vermelho para indicar algum erro ou restrição para uso do cartão do usuário;
X. Sinal sonoro (*buzzer*) para indicar resultado da transação de forma diferenciada;
XI. Mecanismo por radiofrequência para coleta de arquivos e atualização de parâmetros e software; Interface de manutenção;
XII. Tempo médio de processamento de débitos do cartão no validador inferior a 400 milissegundos, limitada a 800 milissegundos em 0,001% das passagens.

2.2.1.1.2. Interface com Outros Sistemas

O validador deve estar preparado para receber vários tipos de arquivos de dados do SIBEM: parâmetros de listas de restrição, software do validador e do SAM e, inclusive, arquivos contendo novas chaves do sistema, para gravação no SAM. Os arquivos recebidos vêm assinados eletronicamente e o validador, através do SAM, deve ser capaz de validá-los e interpretá-los adequadamente.

2.2.1.1.3. Requisitos de Software

As operações mínimas dos validadores são:

I. Checar a presença do módulo SAM e impedir qualquer operação caso esteja ausente;
II. Executar os comandos da máquina de estados do SAM de validador na ordem estabelecida;
III. Receber e se atualizar com novas versões de software;
IV. Mediar a atualização do software do SAM;
V. Permitir a atualização de chaves primárias do SAM;
VI. Interagir com o módulo de Geoposicionamento e comunicação para produzir dados georreferenciados e enviar resumo de dados de bilhetagem;
VII. Viabilizar a migração dos cartões do sistema atual para o novo, quando aplicável;
VIII. Integrar-se a outros equipamentos mediante autenticação mútua, com suporte do SAM;
IX. Tempo máximo da transação com cartão de usuário inferior a 800 ms, envolvendo acesso ao cartão e as funções do SAM.

2.2.1.2. Dispositivo de Geoposicionamento e Comunicação - DGC

O dispositivo de geoposicionamento e comunicação (DGC) permite a obtenção de coordenadas geográficas do veículo para geração de informações georreferenciadas. O DGC pode ser um equipamento único ou estar integrado a outro equipamento embarcado. Nesse caso, é opcional a presença de um equipamento DGC de uso exclusivo.

Este dispositivo é dotado de um módulo SAM ou de um identificador serial único que se comporta como módulo SAM, se o DGC estiver integrado a outro equipamento embarcado. O software que controla o funcionamento deste dispositivo deve interagir com o SAM para reconhecer a autenticidade de outros dispositivos conectados a ele e para gerar pacotes de informação assinados, que certifiquem a origem e qualidade destas informações.

Por meio do DGC é realizado o envio de eventos (mensagens) programados e pré-definidos de forma on-line ao SIBEM. O DGC permite o envio de informações de bilhetagem, procedentes do validador, e de passageiros que embarcaram e desembarcaram procedentes do contador de passageiros.

2.2.1.2.1. Requisitos do Equipamento

Para poder operar no Sistema de Bilhetagem os DGCs devem possuir os seguintes requisitos mínimos:

I. Meio de comunicação com equipamentos embarcados;
II. Microprocessador, podendo atuar em modo *polling* ou requisição, com função de *boot loader* para atualização de software;
III. Memória volátil para execução de programas;
IV. Memória não volátil suficiente para armazenamento de parâmetros e *logs* de transações e operações realizadas;
V. Modem GSM *quadriband* com capacidade para duas operadoras de celular;
VI. Controlador GPS e antena embarcada interna;
VII. Compatível com GPS;
VIII. Mínimo de 32 canais de aquisição;
IX. Supervisão de antena integrada;
X. Bateria backup;

XI. Protocolo NMEA 2.3 ou superior;
XII. Interface de manutenção.

2.2.1.2.2. Interface com Outros Sistemas

O DGC deve estar preparado para receber do SIBEM arquivos de configuração, de software do equipamento, os arquivos recebidos são assinados eletronicamente e o DGC deve ser capaz de validá-los e interpretá-los adequadamente.

Do DGC são enviadas ao CCO mensagens de posicionamento, assinadas pelo SAM ou identificadas pelo número serial, se integrado a outro equipamento embarcado.

O DGC também responde pelo envio ao CCO de resumos de transações procedentes do validador, bem como de informações de contagens apuradas pelo contador de passageiros.

O DGC deve enviar coordenadas de GPS aos dispositivos instalados nos ônibus que precisam desta informação para geração de eventos georreferenciados relacionados à sua operação, como o validador e o contador de passageiros.

2.2.1.2.3. Requisitos de Software

O software do DGC possui os seguintes requisitos:

I. Checar a presença do módulo SAM e impedir qualquer operação caso esteja ausente, exceto se integrado a outro equipamento embarcado;
II. Receber e se atualizar com novas versões de software;
III. Permitir a atualização de chaves primárias do SAM;
IV. Interagir com o validador e o contador de passageiros usando protocolo de comunicação a ser definido;
V. Enviar pacotes periódicos de posicionamento que contenham o identificador serial do equipamento, latitude, longitude e hora correspondente à posição, velocidade, direção e validade da informação GPS;
VI. Comunicar-se a outros equipamentos, mediante autenticação mútua, com suporte do SAM, exceto ao equipamento que estiver integrado.

2.2.2. Exclusivos do Suburbano

2.2.2.1. Barreira Eletrônica

A barreira eletrônica, destinada à instalação embarcada para o controle em ônibus suburbano, a partir da liberação feita pelo validador eletrônico de Cartões Inteligentes, deve possuir:

I. Grande resistência a vibrações e impactos constantes;
II. Trava comutadora, para liberar mecanicamente a saída em situações de falha de liberação do validador e situações de emergência.

Em linhas suburbanas multi-tarifas, pode a concessionária configurar a sua frota com duas barreiras, uma no embarque e outra no desembarque, desde que não restrinja o acesso aos cadeirantes e as normas vigentes.

2.2.2.2. Dispositivo de Reconhecimento Facial

A instalação de um dispositivo de reconhecimento facial junto ao validador de entrada para que seja realizada a identificação de fraudes no uso de cartões é permitida. Caso a instalação do dispositivo seja do interesse da Concessionária, a política de privacidade do mesmo deve ser avaliada e aprovada pela ARTESP.

2.2.2.3. Equipamento de Recolhimento

Deve ser instalado um equipamento para o recolhimento de cartões inteligentes do tipo “viagem unitária” junto à saída.

2.2.2.4. Terminal de Recarga

O terminal de recarga é destinado à transferência de créditos eletrônicos para o Cartão Inteligente.

Para tal, o terminal de recarga deve checar se constam recargas pendentes no cartão do usuário e, em caso positivo, efetuar a transação de crédito correspondente. O resultado da transação deve ser exibido no display do terminal de recarga, com sinais luminosos e sinais sonoros diferenciados.

O terminal de recarga deve estar disponível em todos os ônibus suburbanos. O prazo para finalização da instalação desse equipamento em toda a frota suburbana é de 12 meses, contados a partir do início da implantação do SIBEM.

2.2.2.5. Terminal de Dados

A entrada de dados é realizada por meio de um teclado, conectado ao validador, instalado próximo ao condutor.

2.2.2.5.1. Requisitos do Equipamento

O terminal de dados deve possuir os seguintes requisitos mínimos:

I. Display;
II. Sinal luminoso verde para indicar transação bem-sucedida;
III. Sinal luminoso vermelho para indicar erro;
IV. Sinal sonoro (*buzzer*) para indicar resultado da transação de forma diferenciada;
V. Interface de manutenção.

2.2.2.5.2. Interface com Outros Sistemas

O terminal de dados deve estar preparado para receber do SIBEM arquivos de configuração e de software do próprio terminal de dados. Os arquivos recebidos vêm assinados eletronicamente e o terminal de dados, por meio do SAM instalado no validador, deve ser capaz de validá-los e interpretá-los adequadamente.

2.2.2.5.3. Requisitos de Software

As operações mínimas dos terminais de dados são:

I. Checar a comunicação com equipamentos que estejam integrados;
II. Receber e se atualizar com novas versões de parâmetros e software.

2.2.3. Exclusivo do Rodoviário

2.2.3.1. Contador de Passageiros

O contador de passageiros é um dispositivo instalado nos ônibus para fiscalizar a entrada e saída de passageiros.

Este equipamento também deve ser dotado de um módulo SAM. O software que controla o funcionamento deste dispositivo deve interagir com o SAM para reconhecer a autenticidade de outros dispositivos conectados a ele e para gerar pacotes de informação assinados, que certifiquem a origem e qualidade destas informações.

2.2.3.1.1. Requisitos do Equipamento

Para poder operar dentro do Sistema de Bilhetagem, os contadores de passageiros devem possuir os seguintes requisitos mínimos:

I. Precisão de 92%;
II. Módulo de captura e processamento digital;
III. Comunicação com DGC;
IV. Microprocessador com função de *boot loader* para atualização de software;
V. Memória não volátil suficiente para armazenamento de parâmetros e *logs* de transações e operações realizadas;
VI. Interface de manutenção;
VII. *International Protection Marking*: 50 (IP-50).

2.2.3.1.2. Interface com Outros Sistemas

O contador de passageiros deve estar preparado para receber do SIBEM arquivos de configuração e de software do próprio equipamento. Os arquivos recebidos vêm assinados eletronicamente e o contador de passageiros, comunicando-se com o SAM de DGC, é capaz de validá-los e interpretá-los adequadamente.

Do contador de passageiros devem ser enviados ao CCO os registros de contagens realizadas, assinados pelo SAM de DGC.

Para geração de eventos de contagens georreferenciados, o contador de passageiros deve obter do DGC as coordenadas de GPS.

2.2.3.1.3. Requisitos de Software

O software do contador de passageiros deve ser capaz de:

I. Identificar e contabilizar passageiros, permitindo contagem bidirecional e registrando em memória os eventos de contagem georreferenciados e assinados pelo SAM de DGC;
II. Apresentar alta performance para execução dos processos de aquisição, identificação do alvo e processamento de imagens;
III. Permitir o reconhecimento individual de passageiros mesmo quando trafegando em grupos na região de detecção;
IV. Checar a comunicação com o módulo SAM do DGC e impedir qualquer operação caso houver falha na comunicação;
V. Executar os comandos respeitando a sequência da máquina de estados do SAM de DGC;
VI. Receber e se atualizar com novas versões de software;
VII. Mediar a atualização do software do SAM;
VIII. Permitir a atualização de chaves primárias do SAM;
IX. Interagir com o DGC usando protocolo de comunicação a ser definido.

2.3. Equipamentos Não Embarcados

2.3.1. Cartões Inteligentes

A tecnologia adotada para o Sistema de Bilhetagem compreende a utilização de cartões sem contato (Cartão Inteligente *contactless*) com circuito integrado. Para os sistemas que já estão em operação é requisito indispensável a adoção desta tecnologia, para garantir a implantação do Sistema de Bilhetagem objeto desta licitação.

Cada tipo de dado do cartão é protegido com chaves dedicadas (diferentes uma da outra). Isto permite conceder permissões de acesso aos dados do cartão conforme o perfil da aplicação que os utiliza.

2.3.1.1. Requisitos do equipamento

É necessário que o cartão inteligente tenha ao menos espaço suficiente para armazenar os seguintes dados:

I. Número sequencial do cartão;
II. Data da emissão ou migração do cartão;
III. Tipo do cartão;
IV. Validade do cartão;
V. Tipo de usuário e identificação de usuário para o caso de cartões personalizados;
VI. Restrições de uso, por período e por faixa horária;
VII. Contadores de uso para verificação das restrições anteriores;
VIII. Contadores de integração;
IX. Dados referentes à última transação de crédito do cartão: código do terminal de venda, do SAM, da rede credenciada, do crédito realizado, data;
X. Saldo financeiro disponível para consumo;
XI. Dados referentes à última transação de débito do cartão: código do validador, do SAM, da Concessionária transportadora, da ligação, do veículo, tarifa, latitude e longitude, data e hora;
XII. Assinaturas eletrônicas.

Em caso de sistemas em operação, o cartão em uso deve ter configurações de acesso que possibilitem:

I. Ler dados da aplicação atual;
II. Gravar dados do novo sistema em setores disponíveis;
III. Modificar chaves e perfil de acesso aos novos dados.

2.3.1.2. Requisitos de Segurança

O sistema de segurança a ser adotado no SIBEM, no que se refere aos cartões de padrão aberto, deve possuir as seguintes características:

I. Utilizar chaves de acesso diversificadas pelo número serial do cartão, que é único conforme especificação do fabricante do chip. Esta medida de segurança impede a clonagem de cartões no caso da quebra das chaves de algum cartão de usuário;

II. Separar em arquivos diferentes tipos de dados diferentes (emissão, restrições de uso, viagens, recargas, saldos), para permitir a concessão de permissões de acesso diferenciadas;

III. Para cada tipo de perfil de usuário deve-se utilizar chaves dedicadas (diferentes umas das outras). Isto permite conceder permissões de acesso e interações aos dados do cartão conforme o perfil da aplicação que os utiliza. Exemplo: o validador utiliza um SAM que concede acesso para alterar o saldo e viagens; o terminal de venda utiliza um SAM que garante acesso de escrita para arquivos de recarga e saldo; o terminal de consulta utiliza um SAM que garante acesso de leitura do saldo e das últimas viagens realizadas;

IV. Utilizar assinaturas eletrônicas como certificados de integridade dos dados. Isto garante que os dados continuem protegidos, mesmo na hipótese de quebra de chaves. As assinaturas eletrônicas também devem ser diversificadas em função do número serial do cartão. Isto permite adotar estratégias de tipificação de assinaturas, de acordo com o tipo de dados a ser assinado;

V. Utilizar condições de acesso que permitam trocas de chaves e das próprias condições de acesso;

VI. Usar contadores de decremento que impeçam a fraude de espelhamento (cópia de imagem *mirror* do cartão previamente armazenada);

VII. Chip resistente a ataques de DPA (Análise diferencial do consumo de energia) e DFA (Análise diferencial de falhas), que ofereça AES-MAC para garantir a integridade da sequência de comandos de AES-ENC para garantir a confidencialidade na transmissão de dados;

VIII. Compatibilidade com a criptografia dos atuais sistemas para garantir uma migração suave;

IX. O envio de dados cifrados deve ser feito alterando-se a chave de sessão a cada envio de comando, evitando a utilização da chave para próximos comandos na possibilidade da chave ser quebrada.

As chaves e algoritmos que permitem gerar as assinaturas eletrônicas não devem fazer parte das aplicações do sistema, devem estar protegidos nos SAMs, apresentados anteriormente neste documento.

2.3.1.3. Utilização do Cartão Eletrônico

Ao utilizar seu cartão, o usuário recebe informações do validador de três formas: um anunciador sonoro, um display gráfico e um sinalizador com duas posições luminosas nas cores verde e vermelha.

O sinalizador visual, no caso do validador do sistema suburbano, orienta o usuário sobre o resultado do processamento de seu cartão:

I. A luz verde autoriza o embarque ou desembarque do usuário;
II. A luz vermelha no validador de entrada indica problema no cartão (exemplo: crédito negativo, cartão cancelado, etc.) e não valida o processo de registro de abertura de viagem;
III. A luz vermelha no validador de saída indica problema no cartão ou, no caso de usuário eventual crédito insuficiente.

O display fornece mensagens aos usuários sobre o estado atual do seu cartão (valor debitado, saldo remanescente, data de validade, etc.), a razão da recusa ou do problema com o cartão e mensagens para o pessoal de manutenção (tipo de falha, erros de transmissão, etc.).

O validador emite, associado à sinalização visual acima descrita, um sinal sonoro, nas seguintes situações:

I. Cartão não validado pela regra de negócio;
II. Cartões Gratuito ou Escolar validado com sucesso;
III. Cartões comum ou VT validado com sucesso.

Ao ser aproximado do validador, o cartão do usuário pode apresentar as seguintes condições:

I. **Cartão Válido:** quando é aproximado da zona de leitura do validador o cartão é processado e o usuário é informado, pelo display, sobre o valor debitado e o saldo (ou

tempo de validade para gratuidades) remanescente. Debitado o valor correspondente, o usuário afasta o cartão da zona de leitura e acende-se a luz verde;

II. **Cartão não Válido, sem Crédito, com Créditos Insuficientes:** quando é aproximado da zona de leitura, o cartão é processado, acende-se a luz vermelha, soa um sinal sonoro, e o usuário é informado pelo display do motivo da recusa do cartão;

III. **Cartão Incluso na Lista de Cartões Cancelados:** quando é aproximado da zona de leitura, o cartão é processado, acende-se a luz vermelha, soa um sinal sonoro, e o usuário é informado pelo display do motivo da recusa do cartão. No cartão é gravado um código de cancelamento, que impede a utilização daquele cartão novamente.

2.3.2. Terminal de Venda

O terminal de venda é um dispositivo que está presente nas bilheterias. Ele permite a comercialização de passagens e créditos eletrônicos. O terminal permite a recarga de créditos por meio de transações on-line, tanto de créditos pré-pagos (recarga por lista no servidor) como de créditos pagos no ato da recarga.

O terminal deve estar preparado também para realizar recargas off-line, sem conexão com o Servidor de Recarga On-line. Neste tipo de recarga o terminal deve interagir com o SAM de PDV, que age como repositório e certificador de créditos na transação.

O SAM possui um estoque de créditos eletrônicos. Esse estoque deve ser monitorado pelo terminal de venda e, caso necessário, deve ser efetuada uma transação on-line de abastecimento de créditos, isto é, uma transferência do Repositório de Crédito (HSM) para o SAM de PDV.

2.3.2.1. Requisitos do equipamento

O terminal de venda fixo deve possuir os seguintes requisitos mínimos:

I. Leitor de cartão eletrônico sem contato, compatível com ISO 14.443 A e B, distância máxima de operação de 100 mm;

II. Pelo menos um soquete disponível ID-000 para o chip SAM, e interface de comunicação em estado operacional com este dispositivo;

III. Microprocessador com função de *boot loader* para atualização de software;

IV. Memória volátil para execução de programas;

V. Memória não volátil suficiente para armazenamento de parâmetros e *logs* de transações e operações realizadas;
VI. Display de caracteres de duas ligações para interface com os usuários e o bilheteiro;
VII. Impressora térmica para emissão de comprovantes de venda;
VIII. Interface de comunicação com o Sistema Central: Ethernet ou GSM/GPRS.

2.3.2.2. Interface com outros Sistemas

Para realizar as operações on-line de recarga de cartões de usuário e de transferência de crédito para o SAM de PDV, o terminal de venda deve se conectar a uma rede on-line. Do lado do servidor, as recargas serão autorizadas por meio do Servidor de Recarga On-line, que implementa um protocolo baseado na norma ISO-8583.

A rede de distribuição de créditos deve fornecer um Serviço Concentrador, que é responsável pelo gerenciamento dos terminais de venda e age como intermediário entre esses terminais e o Servidor de Recarga On-line.

Cada rede de distribuição, ou seja, cada Serviço Concentrador da Rede possui um número limitado de conexões com o Serviço de Recarga On-line da Concessionária.

2.3.2.3. Requisitos de Software

As redes de distribuição de crédito devem observar alguns requisitos relativos à implementação do software que controla os terminais de venda. Estes requisitos são:

I. Checar a presença do módulo SAM e impedir qualquer operação caso esteja ausente;
II. Executar os comandos da máquina de estados do SAM de PDV na ordem estabelecida;
III. Receber e se atualizar com novas versões de software;
IV. Mediar a atualização do software do SAM;
V. Permitir a atualização de chaves primárias do SAM;
VI. Viabilizar a migração dos cartões do sistema atual para o novo, quando aplicável;
VII. Assinar as operações realizadas por meio do módulo SAM.

2.3.3. Equipamento de Autoatendimento

Equipamentos de autoatendimento devem ser instalados pela Concessionária, no mínimo nos terminais rodoviários dos 56 polos regionais em que ela opera.

Os equipamentos de autoatendimento permitem a venda auto assistida de recargas de cartões inteligentes e passagens rodoviárias.

O equipamento de autoatendimento deve permitir a recarga de créditos por meio de transações on-line, quando estiver conectado ao Servidor de Recarga On-line, e off-line, quando não estiver.

Na transação off-line o equipamento de autoatendimento deverá interagir com o SAM de PDV instalado nele, que age como repositório e certificador de créditos na transação.

O SAM de PDV possui um estoque de créditos eletrônicos. Esse estoque deve ser monitorado pelo equipamento de autoatendimento e, caso necessário, deve ser efetuada uma transação on-line de abastecimento de créditos, isto é, uma transferência do Repositório de Crédito (HSM) para o SAM.

A venda de passagens rodoviárias deve ser on-line e sincronizada entre os diversos pontos e modos de venda, para que seja impossibilitada a venda de um mesmo assento. Deve ser registrada no SIBEM a venda das passagens rodoviárias.

2.3.3.1. Requisitos do Equipamento

Os equipamentos de autoatendimento devem atender os seguintes requisitos de funcionamento e arquitetura:

I. Portas frontais independentes para acesso a rolo de impressora e cofre de cédulas e moedas;
II. Antivandalismo;
III. Arquitetura da eletrônica baseada em computador industrial;
IV. Monitor touch screen;
V. Dispositivo de Áudio polifônico com capacidade de executar locuções;
VI. Impressora térmica, com sistema de corte automático;
VII. Fácil mecanismo de troca de papel;

VIII. Introdução de cédulas e moedas pela parte frontal;

IX. Aceitar todas as cédulas e moedas vigentes no Brasil. Aceitação de futuras cédulas e moedas mediante reconfiguração;

X. Taxa de aceitação de cédulas e moedas superior a 95%;

XI. Taxa de rejeição de moedas fraudulentas superior a 98%;

XII. Cofre de arrecadação de fácil retirada, com mecanismo de autofechamento automático e sensores;

XIII. Leitor de cartão eletrônico sem contato, compatível com ISO 14.443 A e B, distância máxima de operação de 100 mm;

XIV. Pelo menos um soquete disponível ID-000 para o chip SAM, e interface de comunicação em estado operacional com este dispositivo;

XV. *International Protection Marking*: 53 (IP-53);

XVI. Mecanismos de monitoramento remota;

XVII. Conectividade Ethernet e GPRS;

XVIII. Modem GSM *quadriband* com capacidade para duas operadoras de celular.

2.3.3.2. Interface com outros Sistemas

Para realizar as operações on-line de recarga de cartões de usuário e de transferência de crédito para o SAM de PDV, o equipamento de autoatendimento deve se conectar a uma rede on-line. Do lado do servidor, as recargas serão autorizadas por meio de um serviço no Servidor de Recarga On-line, que implementa um protocolo baseado na norma ISO-8583.

Os equipamentos de autoatendimento se conectam ao Servidor de Recarga On-line por meio do Serviço Concentrador da rede de distribuição de créditos, da mesma forma que ocorre com os terminais de venda.

Na venda de passagens rodoviárias, o equipamento de autoatendimento deve efetivar a operação em servidor centralizado.

2.3.3.3. Requisitos de Software

Os equipamentos de autoatendimento devem possuir as características mínimas:

I. Interação com os dispositivos e periféricos de validação de notas, moedas e Cartões Inteligentes;

II. Executar as operações de crédito de cartões, de modo on-line e off-line em contingência do mesmo modo que os Pontos de Venda Fixos.

2.3.4. Equipamentos de Informação ao Usuário

Os equipamentos de informação ao usuário fornecem informações sobre o serviço rodoviário. Esses equipamentos devem ser instalados, no mínimo, nos terminais rodoviários dos 56 polos regionais em que a concessionária opera, em locais de alta circulação dos terminais.

2.3.4.1. Requisitos mínimos

I. TVs de 50 polegadas;
II. Entradas de vídeo VGA e HDMI;
III. Resolução mínima: Full HD (1920 x 1080 pixels);
IV. Cores: 16,8 milhões de cores;
V. Sistemas de cor: NTSC, PAL-M;
VI. Caixa de Proteção com tela antirreflexo.

3. Cronograma de Implantação

O processo de implantação deve ocorrer no prazo máximo de 27 meses a ordem de início de operação.

O cronograma prevê a entrega de dois artefatos relacionados ao desenvolvimento do projeto de implantação do SIBEM, que serão validados pela ARTESP:

I. **Projeto Inicial:** especificação macro dos módulos, processos, integrações e equipamentos do SIBEM, e cronograma preliminar de atividades, análise, desenvolvimento, testes e implantação. Deve conter:
   a) Modelo, especificação técnica e estimativa da quantidade de equipamentos que serão adquiridos;
   b) Sistemas que serão adquiridos, desenvolvidos ou reaproveitados, os seus módulos e macro funcionalidades;

c) Cronograma para desenvolvimento do Projeto Final e de implantação do SIBEM;

d) Itens deste termo de referência explicitamente requisitados para serem entregues no Projeto Inicial.

II. **Projeto Final:** especificação técnica detalhada dos módulos, processos, integrações e equipamentos do SIBEM, e cronograma detalhado de atividades, análise, desenvolvimento, testes e implantação. Deve conter:

a) Equipamentos testados e aprovados, que serão adquiridos;

b) Detalhamento dos processos dos módulos do sistema;

c) Apresentar a análise do sistema pronta: telas, equipamentos, processos, funcionalidades e especificação técnica;

d) Cronograma preciso para aquisição e instalação dos equipamentos, desenvolvimento e implantação do SIBEM;

e) Tecnologias que serão utilizadas, banco de dados e arquitetura detalhada;

f) Itens deste termo de referência explicitamente requisitados para serem entregues no Projeto Final.

No Projeto Inicial e Projeto Final devem constar os itens presentes e também os não presentes neste documento, mas que são necessários no Sistema.

Etapa	Prazo Máximo	Atividade	Responsável
Apresentação do Projeto Inicial	**3 meses após ordem de início de operação**	Desenvolvimento e apresentação do Projeto Inicial.	Concessionária
Avaliação do Projeto Inicial	3 semanas após Apresentação do Projeto Inicial	Avaliação do Projeto Inicial, com formulação de parecer (Aprovação ou Reprovação).	ARTESP
* Revisão do Projeto Inicial	2 semanas após Avaliação do Projeto Inicial	Apresentação do Projeto Inicial revisado considerando o parecer da ARTESP.	Concessionária
* Reavaliação do Projeto Inicial	2 semanas após Revisão do Projeto Inicial	Reavaliação do Projeto Inicial revisado pela Concessionária, com formulação de parecer (Aprovação ou Reprovação).	ARTESP
Apresentação do Projeto Final	**12 meses após ordem de início de operação**	Desenvolvimento e apresentação do Projeto Final.	Concessionária
Avaliação do Projeto Final	3 meses após Apresentação do Projeto Final	Avaliação do Projeto Final, com formulação de parecer (Aprovação ou Reprovação).	ARTESP
** Revisão do Projeto Final	3 semanas após Avaliação do Projeto Final	Apresentação do Projeto Final revisado considerando o parecer da ARTESP.	Concessionária
** Reavaliação do Projeto Final	5 semanas após Revisão do Projeto Final	Reavaliação do Projeto Final revisado pela Concessionária, com formulação de parecer (Aprovação ou Reprovação).	ARTESP
Implantação	**27 meses após ordem de início de operação**	SIBEM implantado em toda a área de operação da Concessionária.	Concessionária

* Etapa cíclica que ocorre nos casos de reprovação do Projeto Inicial.

** Etapa cíclica que ocorre nos casos de reprovação do Projeto Final.