

# Mobilidade do Futuro: um Modelo Disruptivo para São José dos Campos

Serviços Técnicos relacionados a Tecnologia da  
Informação - Relatório de acompanhamento:

Produto 5 - Suporte à Plataforma tecnológica 3

## Equipe

Coordenação: **Ciro Biderman**

Coordenação institucional: **Patricia Alencar Silva Mello**

Gestão do Projeto: **Eliana Martins de Mello Montagna**

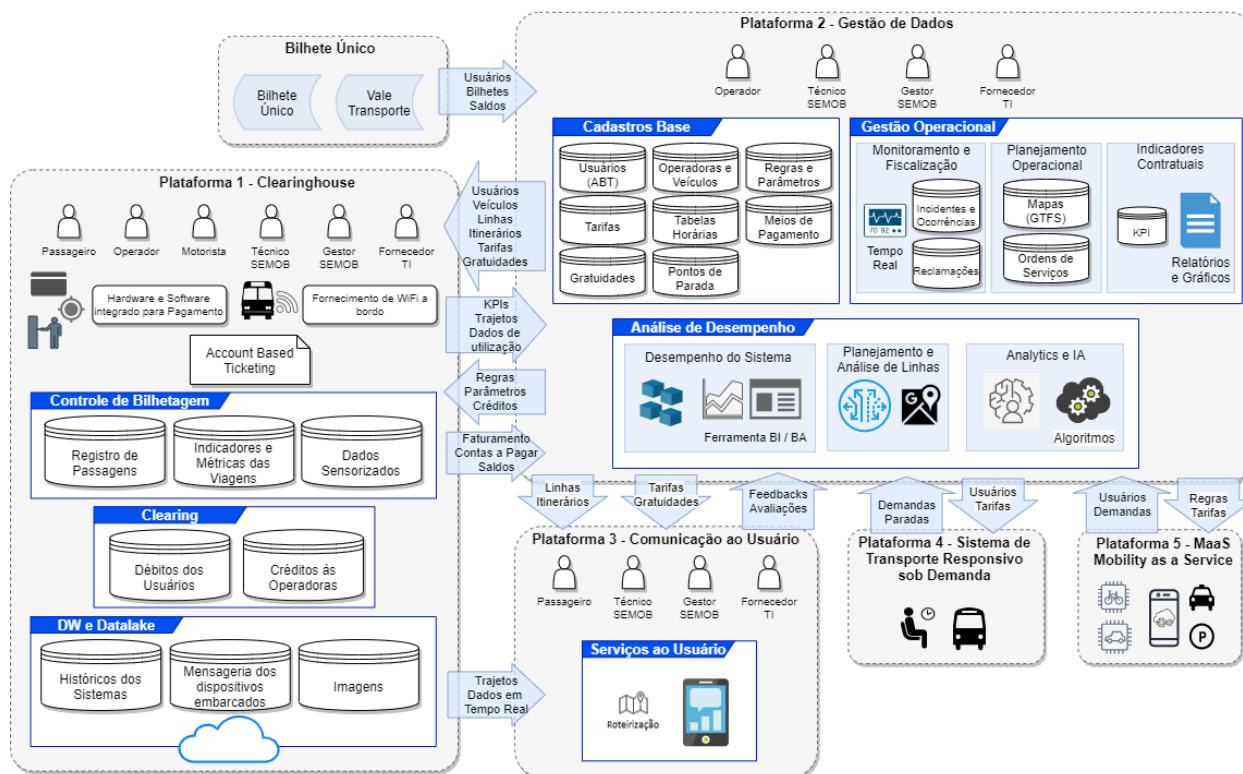
Elaboração:

**Fabricio Ricardo Perrella**

**Luiz Carlos Martinez Junior**

# Diagrama funcional dos componentes da arquitetura tecnológica

## Visão Geral das Plataformas



## Anexo técnico do Termo de Referência para Contratação

### 1 Visão Geral do Escopo da Plataforma 3

Considerando o descritivo das Plataformas Integradas de Gestão de Mobilidade Urbana inicialmente apresentado no Chamamento Público para Detalhamento Técnico das Plataformas de Mobilidade Urbana de 5 de junho de 2020, detalha-se no presente Anexo a Visão Geral da Plataforma 3 e Escopo de atuação requerido para fornecimento de serviços tecnológicos, sistemas e ferramentas de gestão apoiados por Tecnologias da Informação.

A Gestão da Mobilidade Urbana foi idealizada a partir do agrupamento das usabilidades tecnológicas em cinco Plataformas distintas, a saber:

- Plataforma 1 – Clearinghouse para Serviços de Transporte
- Plataforma 2 – Sistema de Gestão de Dados do Transporte Público
- Plataforma 3 – Serviços de Comunicação com os Usuários

- Plataforma 4 – Sistema de Transporte Responsivo à Demanda
- Plataforma 5 – MaaS – Mobilidade como Serviço

Para a Plataforma 3, entende-se que ela deverá prover à SEMOB um canal de relacionamento com o usuário do transporte público que além de proporcionar a visibilidade ao usuário com relação ao fluxo e disponibilidade dos veículos nas linhas e trajetos, será um importante meio de captura de feedbacks e avaliações referentes aos serviços prestados pelas operadoras. Estas informações serão consumidas e utilizadas pela Plataforma 2 para enriquecer os dados de análise geral do Desempenho do Sistema de Transporte, adequando-o às novas realidades da mobilidade urbana e, em última análise, medir o nível de satisfação dos usuários quanto aos serviços prestados à população.

No contexto deste Edital, para fins de distinção de responsabilidades entre as Plataformas 1, 2 e 3, a Figura 1 a seguir ilustra os componentes funcionais pertinentes a cada uma das plataformas, destacando particularmente os módulos, processos e bases de dados que ficarão sob responsabilidade da Plataforma 3, bem como suas correlações com dados intercambiados entre as demais plataformas, para entendimento dos requisitos de implementação da solução.

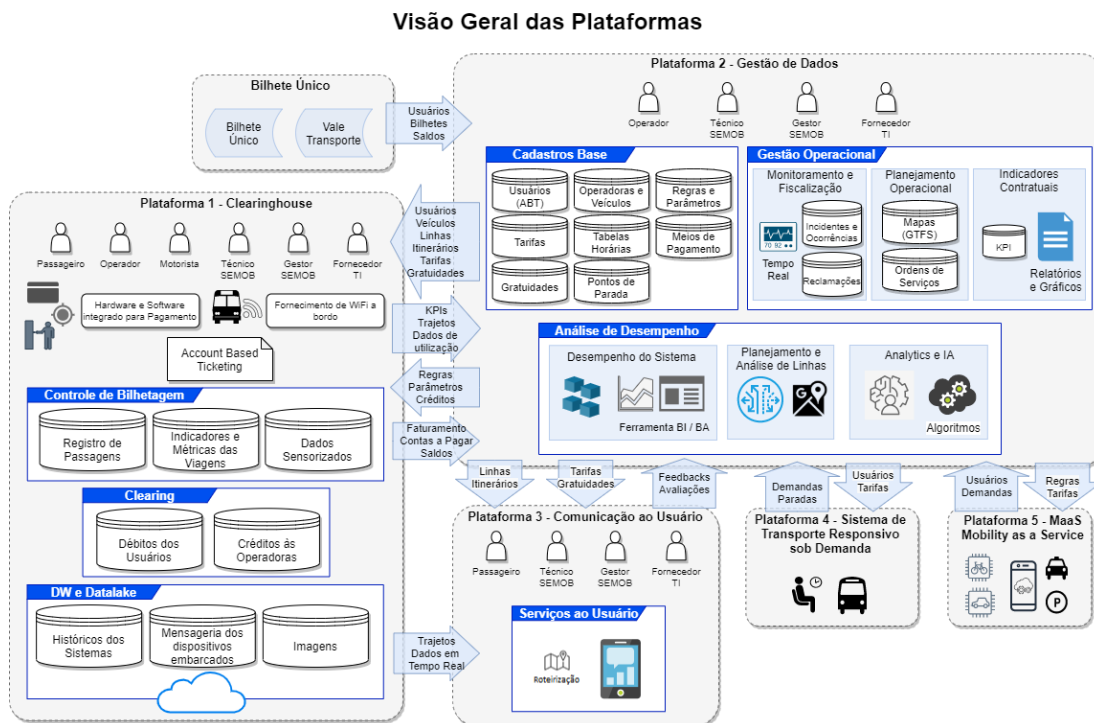


Figura 1 - Visão esquemática do Escopo da Plataforma 3

O escopo requerido para a Plataforma 3 deve contemplar o fornecimento, instalação, customizações e suporte contínuo de um **Aplicativo Móvel** como canal de **Comunicação com**

**o Usuário do Transporte Público**, baseado em modelos de referência como o *Mobility Data Specification* (MDS) mantido pela *Open Mobility Foundation* (OMF), capaz de:

- 1) Capturar feedbacks, críticas e sugestões dos usuários a respeito dos veículos, itinerários e pontos de paradas
- 2) Capturar avaliação sobre as condições de manutenção dos veículos da frota, qualidade dos serviços prestados pelas empresas operadoras dos serviços de transporte e qualidade da condução dos motoristas
- 3) Disponibilizar informações em tempo real sobre as linhas, com base nos posicionamentos georreferenciados da frota e do próprio usuário, permitindo visualizar a estimativa de chegada de uma ou mais linhas em um determinado ponto de parada.
- 4) Garantir comunicação segura e em completo alinhamento com os requerimentos da Lei Geral de Privacidade de Dados (LGPD).

A seguir detalham-se os requisitos específicos sob o Escopo da Plataforma 3.

## **2 Detalhamento dos Requisitos**

### **2.1 Sistema de Comunicação com o Usuário do Transporte Público**

#### **2.1.1 Identificação do Usuário**

Por definição todos os feedbacks e avaliações devem ser seus autores identificados, com isso, é requisito do sistema que os usuários façam o login para ter acesso às funcionalidades, podendo criar um usuário específico para a plataforma ou fazer uso de credenciais já existentes em contas como o Google ou Facebook.

A gestão destas informações dentro da Plataforma 3 deve seguir os requisitos estabelecidos pela Lei Geral de Privacidade de Dados (LGPD) sobre tudo quanto ao desejo do usuário de ter seus dados pessoais esquecidos, ou seja, ter seus dados excluídos seguramente da plataforma.

#### **2.1.2 Captura de feedbacks, críticas e sugestões**

O sistema deve permitir que o usuário do transporte público envie feedbacks críticas e ou sugestões de maneira rápida e fácil, após se identificar. O formulário de registro destes feedbacks, críticas e ou sugestões em texto livre deve permitir que o usuário especifique os elementos relacionados a viagem através do preenchimento dos campos que identifiquem o veículo, a linha e o itinerário da viagem, assim como o momento em que ocorreu a viagem, de forma automática através da leitura de um QRCode presente no veículo ou de forma manual.

O sistema deve capturar automaticamente as informações de geoposicionamento do usuário assim como data e hora do registro do feedback, críticas e ou sugestões.

#### **2.1.3 Captura de Avaliações**

O sistema deve permitir que o usuário do transporte público envie avaliações com relação à viagem efetuada de maneira rápida e fácil, após se identificar. O formulário de registro desta avaliação deve permitir que o usuário especifique os elementos relacionados a viagem através do preenchimento dos campos que identifiquem o veículo, a linha e o itinerário da viagem, assim como o momento em que ocorreu a viagem, de forma automática através da leitura de um QRCode presente no veículo ou de forma manual.

O sistema deve capturar automaticamente as informações de geoposicionamento do usuário assim como data e hora do registro da avaliação.

#### **2.1.4 Registro de Denúncias e Ocorrências de Emergência**

O sistema deve permitir que o usuário efetue um registro de denúncia ou ocorrências de emergência, mesmo sem estar autenticado no aplicativo, afim de manter o anonimato diante de um evento crítico em que a lei permita tal condição, como por exemplo, denunciar um assédio ou violência dentro do transporte público ou em suas mediações.

O sistema deve capturar automaticamente as informações de geoposicionamento do usuário assim como data e hora do registro do evento.

### 2.1.5 Monitoramento de Linhas e Trajetos

O sistema deve permitir que o usuário do transporte público devidamente identificado consiga ter acesso as informações sobre os veículos, linhas e trajetos próximas a posição georreferenciada de seu dispositivo através de pesquisas abertas ou com base na lista de favoritos e preferências previamente salvas pelo próprio usuário em seu perfil de acesso.

Esta funcionalidade deve ser apresentada para o usuário de duas formas:

- 1- Lista de opções, apresentando as informações de identificação dos veículos, linhas, previsão de chegada e distância relativa à posição do dispositivo do usuário
- 2- Objetos sobre um mapa georreferenciado com símbolos identificando o usuário, pontos de parada e veículos, com as informações dispostas de forma simples e clara sobre estimativas de chegadas e distância.

### 2.2 Interfaces sistêmicas e integrações de dados

Para a Plataforma 3, deverão ser previstas no mínimo as seguintes integrações com a Plataforma 2 através das APIs descrita no Edital da Plataforma 2, para os seguintes propósitos:

Propósito	Entidades Relacionadas	Frequência
Recebimento de dados em tempo real sobre os itinerários, trajetos e percurso das linhas de interesse do usuário	Itinerário Linha Veículo Operadora Registro de Estado (GPS e sensores)	Online
Recebimento de dados sobre linhas, partidas e pontos de paradas para efeito de planejamento de rotas por parte dos usuários	Itinerário Linha Operadora Registro de Estado (GPS e sensores) Registro da Viagem	Online
Envio de feedbacks, críticas e sugestões dos usuários a respeito dos veículos, itinerários e pontos de paradas	Itinerário Linha Motorista Operadora Registro do Chamado com GPS (Feedback, crítica ou sugestão) Usuário Veículo	Online

<p>Envio de avaliação sobre as condições de manutenção dos veículos da frota, qualidade dos serviços prestados pelas empresas operadoras dos serviços de transporte e qualidade da condução dos motoristas</p>	<p>Itinerário Linha Motorista Operadora Registro do Chamado com GPS (Avaliação) Usuário Veículo</p>	<p>Online</p>
<p>Envio de denúncias ou ocorrências de emergência de forma anônima ou não</p>	<p>Itinerário Linha Registro do Chamado com GPS (Sinistro) Usuário (não obrigatório) Veículo</p>	<p>Online</p>

### **3 Disposições Gerais para o fornecimento dos serviços**

#### **1.1 Suporte Técnico contínuo**

É requerido que o fornecedor descreva detalhadamente na Proposta Técnica toda e quaisquer atividades de suporte técnico contínuo como parte das atribuições do fornecedor na contratação dos serviços. Entende-se que o projeto de implantação dos componentes se dará nos primeiros meses da contratação e será necessário disponibilizar uma equipe para monitoração e suporte contínuo pós-implantação dos componentes da solução.

#### **1.2 Modelo de Operação**

Em função da natureza dos serviços prestados e do tempo de vigência do contrato, é requerido que o fornecedor descreva detalhadamente na Proposta Técnica o modelo de operação que será adotado para monitoração, suporte contínuo, correção de defeitos e eventuais manutenções necessárias nos componentes da solução técnica durante o projeto de implantação e ao longo do contrato.

#### **1.3 Adequação da Solução à LGPD**

A solução proposta deve contemplar a implementação de medidas de segurança física, técnica e organizacional adequadas de acordo com a Lei Geral de Proteção de Dados Lei nº 13.709/18. As medidas de segurança da Operadora da Solução devem, em particular, evitar que os Dados Pessoais Processados sejam:

- acidental ou ilegalmente destruída, perdida ou alterada;
- divulgado ou disponibilizado sem autorização; ou
- de outra forma processado em violação da LGPD.

A Operadora da Solução deve garantir que todos os Dados Pessoais Processados em nome do Controlador sejam mantidos separados de forma segura de quaisquer outros Dados Pessoais Processados pela Operadora.

A Operadora deve, mediante solicitação, fornecer ao Controlador documentação suficiente para permitir ao Controlador demonstrar que as medidas de segurança técnicas e organizacionais apropriadas foram implementadas e que a Operadora está agindo em conformidade com este Contrato de Processamento de Dados e a legislação vigente.



A Operadora deve implementar medidas de segurança técnicas e organizacionais apropriadas de acordo com a LGPD incluindo as seguintes precauções adicionais:

- Organização de segurança com responsabilidades claras;
- Política de segurança da informação e política de privacidade;
- Controle de acesso a sistemas e dados;
  - Tanto o uso autorizado quanto as tentativas de uso não autorizado de sistemas devem ser registrados;
  - A documentação deve ser mantida por pelo menos trinta e seis meses;
- Controle de acesso físico a edifícios e equipamentos utilizados para Processamento de Dados Pessoais;
- Proteção contra vírus, filtros de spam e firewalls de próxima geração (nível de aplicativo e rede) conforme apropriado;
- Processo regular de gerenciamento de vulnerabilidade, seguido por um processo de reforço de segurança e aplicação de *patches* para software e configurações de sistema de processamento de dados pessoais;
- Registro de todas as operações críticas do sistema, de preferência com mecanismo de correlação inteligente que consolida os registros e fornece gerenciamento proativo de incidentes;
- Processos e monitoramento de violação de segurança;
  - As violações de segurança devem ser documentadas e a documentação mantida por pelo menos três meses;
- Ferramenta de rastreabilidade que gerencie o ciclo de vida dos dados nas Bases de Dados sistêmicas e analíticas;
- Processo de backup / restauração para todos os sistemas críticos e testes de restauração;
- Uso de software autorizado e licenciado desenvolvido sob um ciclo de vida de desenvolvimento de software no qual a segurança é um princípio básico incorporado em cada fase deste ciclo de vida;
- Um processo de gerenciamento de mudança adequado garantindo a segurança e integridade dos dados pessoais processados em nome do Controlador;

- Treinamento e educação em segurança da informação e dados pessoais;
- Criptografia de dados na comunicação entre os sistemas da plataforma 1 e demais sistemas integrados a ela;
  - Os dados confidenciais devem ser sempre criptografados em trânsito e em repouso, incluindo protocolos e técnicas utilizados;
- Mascaramento dos dados descritos nas especificações de implementação das soluções para garantia e anonimização de dados pessoais e/ou sensíveis;
- Um processo de sanitização de dados adequado e certificado para exclusão segura de dados, apoiando o Método de Limpeza de Dados DoD 5220.22-M (com pelo menos 3 rodadas) ou melhor, mediante solicitação do Controlador ou exigência da legislação vigente;
- Certificação de conformidade com as melhores práticas e padrões de segurança relevantes e capacidade de fornecer relatórios de auditoria independente sobre os últimos, como ISO27k, ISAE 3402 tipo 2, SOC 2, SSAE 18, PCIDSS Nível 1).

#### 1.4 Finalidades Específicas dos Tratamentos de Dados

**A Solução proposta deve** atender às finalidades específicas dos tratamentos e tipos de dados tratados de acordo com sua solução. Caso haja outras finalidades não específicas e que sejam necessárias à solução apresentada, é obrigatório descrever a finalidade e os dados pessoais que serão impactados naquela finalidade. A tabela a seguir destaca as Finalidades e Dados inicialmente previstos:

**Tabela 1 - Modelo de Finalidades Específicas e Dados Necessários**

Finalidade	Operações	Periodicidade	Dados necessários	Tratamento
Validação das passagens	coleta de dados	a cada marcação do bilhete na catraca do pré-embarque ou do veículo	Identificador do veículo / validador Identificador da viagem / sentido trajeto Identificador do	Dados serão coletados no equipamento validador para transmissão em rede protegida e

			bilhete / cartão Identificador do usuário Valor da tarifa Tipo de Gratuidade, caso aplicada Latitude / Longitude Data / Hora	dados criptografados ao Sistema de Controle da Bilhetagem, mantidos durante um período de 10 anos
	compartilhamento de dados com o meio de pagamento para verificar a possibilidade de débito	toda vez que houver passagem de bilhete ou cartão que requeira autorização da empresa de meio de pagamento	Identificador do bilhete / cartão Identificador do usuário Valor da tarifa Data / Hora	Dados serão coletados no equipamento validador para transmissão em rede protegida e dados criptografados à administradora do meio de pagamento
	recebimento de dados do meio de pagamento	toda vez que houver passagem de bilhete ou cartão que requeira autorização da empresa de meio de pagamento	Identificador do bilhete / cartão Identificador do usuário Data / Hora	Autorização do pagamento será retornada pela administradora do meio de pagamento ao equipamento validador
	registro da passagem	a cada marcação do bilhete na catraca do pré-embarque ou do veículo	Identificador do veículo / validador Identificador da viagem / sentido trajeto Identificador do bilhete / cartão Identificador do usuário Valor da tarifa Tipo de Gratuidade, caso aplicada Latitude / Longitude Data / Hora	Dados serão coletados no equipamento validador para transmissão em rede protegida e dados criptografados ao Sistema de Controle da Bilhetagem, mantidos durante um período de 10 anos

Remuneração da Concessionária de Transporte	validação e registro dos trajetos percorridos para consumo de bilhetagem	diariamente ao final da operação em cada veículo utilizado	Latitude / Longitude de início da viagem Latitude / Longitude de término da viagem Quilometragem percorrida Identificador do veículo / AVL Data / Hora de início da viagem Data / Hora de término da viagem Quantidade de passageiros transportados	Dados dos validadores e do veículo serão transmitidos em rede protegida e criptografados ao Sistema de Clearing, mantidos durante um período de 10 anos
Verificação de lotação dos veículos nas viagens, para efeito de Fiscalização e Controle Operacional do serviço prestado pela Concessionária de Transporte	coleta via sensores de porta	a cada entrada e saída de passageiros no veículo	Identificador do veículo Latitude / Longitude da parada Quantidade de passageiros embarcados na parada Quantidade de passageiros desembarcados na parada Data / Hora da parada	Dados dos sensores de porta serão transmitidos em rede protegida e criptografados ao Sistema de Controle da Bilhetagem, mantidos durante um período de 30 dias
	coleta via imagens na câmera salão	a cada 3 minutos	Identificador do veículo Data / Hora da captura da imagem Quantidade de passageiros contados na imagem Latitude / Longitude	Imagens serão tratadas para descaracterizar os rostos dos indivíduos, mantidos durante um período de 30 dias
	expurgo dos dados	a cada 30 dias	todos os dados coletados via sensores de porta e via imagens na câmera salão,	Dados serão removidos da base de dados dos sistemas de controle

			como discriminados acima	
Controle de fraude no uso dos bilhetes	captura da imagem da face do passageiro para efeito de gratuidades e benefícios (meia passagem ou gratuidade estudantil, idosos, aposentados, PCD etc.)	a cada marcação do bilhete na catraca do veículo	Identificador do bilhete / cartão Identificador do Usuário Momento do evento Regra aplicada Data / Hora Latitude / Longitude Identificador do validador / veículo Imagem facial	Dados e imagem facial serão enviados criptografados em rede protegida ao Sistema de Clearing para reconhecimento facial e verificação das evidências da fraude no uso do bilhete, mantidos por um período de 30 dias
	captura da imagem da face do passageiro para efeito de aplicação das regras tarifárias e regras de integração	a cada marcação do bilhete na catraca do veículo	Identificador do bilhete / cartão Identificador do Usuário Momento do evento Data / Hora Identificador do validador / veículo Imagem facial	Dados e imagem facial serão enviados criptografados em rede protegida ao Sistema de Clearing para reconhecimento facial e verificação das evidências da fraude no uso do bilhete, mantidos por um período de 30 dias
Aplicação de obrigatoriedades legais (Vale Transporte)	coleta e registro do uso do VT	a cada marcação do bilhete na catraca do veículo	Identificador do Usuário Momento do evento Data / Hora Identificador do validador / veículo	Dados serão coletados no equipamento validador para transmissão em rede protegida e dados criptografados ao Sistema de Controle da Bilhetagem, mantidos durante um período de 10 anos

Planejamento operacional	armazenamento dos dados históricos da bilhetagem	diariamente ao final da operação	Identificador da viagem / sentido trajeto Tipo de Gratuidade, caso aplicada Latitude / Longitude Data / Hora Perfil do usuário (gênero, faixa etária e raça)	Dados serão consolidados e anonimizados pelo Sistema de Controle da Bilhetagem e armazenados de forma protegida e criptografados em um Data Warehouse por um período de 10 anos
Oferta de serviço Premium de Wi-Fi a bordo	identificação dos usuários conectados ao serviço de Wi-Fi	sempre que o passageiro conectar-se ao serviço de Wi-Fi a bordo dos veículos	Identificador do usuário Identificador do veículo Identificador do roteador Data / Hora de início da conexão Data / Hora de término da conexão Velocidade média de tráfego de dados (downstream) Latitude / Longitude	Dados de quantidade de usuários conectados, velocidade e tempo de conexão serão mensurados com a finalidade de comercialização de serviço Premium de Wi-Fi, mantidos por um período de 1 ano
Encerramento ou distrato do contrato	transferência dos dados à SEMOB	no caso de término do período contratual ou distrato durante o período de vigência	todos os dados registrados nas bases de dados dos Sistemas de Controle da Bilhetagem, Clearing, Data Warehouse e Datalake, incluindo os dados discriminados acima nesta tabela	As bases de dados e os arquivos de backup dos dados serão armazenados e transferidos à SEMOB, incluindo as senhas de administração para estas bases de dados
	eliminação e descarte dos dados	no caso de término do período contratual ou distrato durante o período de vigência	todos os dados registrados nas bases de dados dos Sistemas de Controle da	As bases de dados e os arquivos de backup dos dados serão eliminados lógica e fisicamente

			Bilhetagem, Clearing, Data Warehouse e Datalake, incluindo os dados discriminados acima nesta tabela	dos dispositivos de hardware, sendo descartados de forma segura e apropriada os meios físicos utilizados para arquivamento
--	--	--	--	--