

HIERARQUIA DE ACESSOS – SISTEMA TECHDENGUE

Resumo Executivo

Este documento define **como o acesso ao sistema Techdengue deve funcionar na prática**, para todos os atores que participam do programa: estado, URS, consórcios, municípios, prestadores de serviço e time interno da Aero/Techdengue.

Ele organiza, em um único lugar:

- Quais são os **tipos de usuários** (perfis) e em que níveis atuam (estratégico, tático, operacional ou apoio indireto);
- Que **dados cada perfil pode ver, editar, validar ou exportar**, respeitando LGPD, sigilo institucional e responsabilidades de cada ente;
- Como os acessos se conectam às **telas e módulos do sistema** (configuração, operação, monitoramento, relatórios);
- Quais são os **fluxos mínimos de governança**, como criação/alteração de usuários, revisão periódica de acessos, desligamento e tratamento de incidentes.

Para quem este documento é útil

- **Time interno da Aero/Techdengue (Produto, Operações, Dados, Suporte)**: para desenhar e configurar corretamente os perfis no sistema e orientar clientes.
- **Gestores públicos (SES, URS, Consórcios, Secretarias Municipais)**: para entender claramente o que podem e o que não podem ver/fazer dentro da plataforma.
- **Áreas de Jurídico, Compliance, Auditoria e Controle**: para verificar aderência às normas (incluindo LGPD) e às regras de financiamento/contratos.
- **Lideranças Executivas (prefeitos, secretários, diretores)**: para ter uma visão rápida de como a segurança e a governança de acesso estão estruturadas.

Como usar este documento

- Se você é **gestor municipal** ou coordena vigilância/endemias, foque principalmente nas seções **5.2 (Âmbito Municipal)** e **6.5 (Perfis Municipais)**.

- Se você atua em **URS, consórcio ou SES**, consulte as seções **3.1, 5.1** e os perfis da seção **6.3 e 6.4**.
- Se você faz parte do **time interno da Aero/Techdengue**, as seções **3.2, 4, 6.2, 7 e 8** são prioritárias.
- Se sua atuação é em **jurídico, compliance ou auditoria**, observe especialmente as seções **2.4 (Classificação de Dados), 6.7 (Perfis de Auditoria/Executivo) e 8 (Governança de Perfis)**.

Benefícios esperados

Com esta política aplicada, espera-se:

- **Maior segurança da informação**, com redução de riscos de acesso indevido ou exposição desnecessária de dados;
- **Clareza de papéis e responsabilidades**, reduzindo conflitos sobre "quem deveria enxergar o quê";
- **Padronização** na configuração de acessos entre diferentes contratos, estados, consórcios e municípios;
- **Base sólida para auditorias e prestação de contas**, com trilhas de auditoria e critérios objetivos de acesso.

Este resumo executivo pode ser utilizado como porta de entrada para apresentação a gestores e parceiros, enquanto as seções seguintes trazem o detalhamento técnico e operacional necessário para implementação no sistema.

0. Informações Gerais

- **Documento:** Política de Perfis e Hierarquias de Acesso do Sistema Techdengue
- **Versão:** 1.0 (rascunho estruturado para avaliação)
- **Responsável pelo Conteúdo:** Time Techdengue / P&D / Produto
- **Finalidade:** Definir, organizar e documentar os níveis de acesso, perfis, permissões e restrições do sistema Techdengue, incluindo as hierarquias internas da Aero e as camadas externas (SES, URS, consórcios, municípios, prestadores e demais atores).

1. Objetivo

Este documento tem como objetivo **estabelecer as diretrizes oficiais de segurança e governança de acesso** do sistema Techdengue, funcionando como

referência única para o desenho, a configuração e a manutenção de perfis, permissões e hierarquias de acessibilidade em todo o ecossistema do programa.

Mais do que apenas listar perfis, este documento busca:

- Definir de forma clara **quem pode ver o quê, onde e com qual finalidade**, considerando a posição institucional de cada ator (interno e externo);
- Explicitar como se organizam as **hierarquias internas de acessibilidade** dentro da Aero/Techdengue e entre os diferentes níveis de gestão pública (estado, URS, consórcios, municípios);
- Descrever os **perfis de acesso**, seus escopos territoriais, níveis (estratégico, tático, operacional, apoio indireto), permissões e restrições;
- Vincular os perfis às **telas, módulos e funções** do sistema, orientando o desenho técnico da solução (front-end, back-end, APIs e integrações);
- Servir como base para **auditorias, análises de conformidade e ajustes futuros** de acesso, alinhados à LGPD, às normas da saúde pública e às políticas internas da Aero.

Na prática, este documento deve apoiar:

- O time de produto e tecnologia na **configuração técnica de perfis e permissões** no sistema;
- O time de operações e relacionamento na **definição de perfis adequados para cada contrato/município/consórcio**;
- Os gestores públicos (estado, URS, consórcios, municípios) na **compreensão dos limites e responsabilidades** de cada acesso;
- As áreas de jurídico, compliance, financeiro e auditoria na **verificação de aderência** às regras de segurança da informação e de uso adequado dos dados.

O objetivo central é garantir **segurança, rastreabilidade, coerência de papéis e mínimo privilégio**, permitindo que:

- Cada usuário tenha apenas o acesso necessário para desempenhar suas funções;
- Os dados sejam protegidos contra uso indevido, exposição desnecessária ou distorção;
- As decisões tomadas a partir da plataforma tenham base em **informações confiáveis, íntegras e corretamente protegidas**.

1.1. Mapa Mental dos Níveis de Acesso (Visão Rápida)

Para facilitar a compreensão do modelo de acesso, os níveis podem ser visualizados como um "mapa mental" em texto, onde cada camada tem um foco e um conjunto típico de atores:

- **Nível Estratégico**
 - **Quem costuma estar aqui:** Gestor Estadual SES, diretores de URS, prefeitos, secretários municipais de saúde, diretoria da Aero/Techdengue, perfis executivos e de auditoria estratégica.
 - **Foco:** visão macro do programa (estado, URS, consórcio, carteira de clientes), resultados consolidados, comparações entre regiões e períodos, suporte à tomada de decisão de alto nível.
 - **Tipo de acesso:** dashboards sintéticos, relatórios consolidados, indicadores-chave; em geral, baixa ou nenhuma edição de dados.
- **Nível Tático**
 - **Quem costuma estar aqui:** Gestores regionais de URS, gestores de consórcios, gestores municipais do programa, coordenações de vigilância epidemiológica e de endemias, time de Operações & Projetos.
 - **Foco:** transformar estratégia em planos concretos por região, consórcio ou município; acompanhar execução, ajustar prioridades, validar relatórios e conectar operação e estratégia.
 - **Tipo de acesso:** visão mais detalhada por município/contrato, acesso a planos de trabalho, relatórios intermediários, alguns poderes de configuração local e validação.
- **Nível Operacional**
 - **Quem costuma estar aqui:** agentes de campo (ACE), supervisores de equipes, operadores de drones, técnicos que alimentam dados no sistema.
 - **Foco:** execução das atividades diárias (visitas, tratamentos, voos, registros em campo), atualização de status e devolutiva direta das ações.
 - **Tipo de acesso:** telas de rotas, pontos de interesse, checklists de atendimento, registro de fotos e observações, com escopo territorial bem definido (bairro, área, rota).

- **Nível de Apoio Indireto**

- **Quem costuma estar aqui:** financeiro, faturamento, jurídico/compliance, comunicação/marketing, áreas administrativas e de apoio interno.
- **Foco:** utilizar informações agregadas do sistema para fins de faturamento, relatórios institucionais, materiais de comunicação, pareceres jurídicos e análises de conformidade.
- **Tipo de acesso:** dashboards e relatórios agregados, sem necessidade de enxergar dados sensíveis ou muito granulares (domicílios, pessoas, detalhes operacionais individuais).

Este mapa mental serve como referência rápida para validar se um pedido de acesso está coerente com o papel do usuário. Sempre que houver dúvida, deve-se perguntar: **“Este usuário precisa deste nível de detalhe para cumprir suas funções?”** – e aplicar o princípio do mínimo privilégio.

2. Escopo e Conceitos Básicos

2.1. Escopo

Esta política se aplica a todos os usuários do sistema Techdengue, incluindo, mas não se limitando a:

- Equipes internas da **Aero / Techdengue**;
- **Secretaria Estadual de Saúde (SES)** e órgãos estaduais correlatos;
- **Unidades Regionais de Saúde (URS)** e comitês técnicos regionais;
- **Consórcios Intermunicipais de Saúde (CIS)**;
- **Gestores municipais de Saúde** e equipes técnicas;
- **Equipes de campo** (agentes de endemias, operadores de drones, supervisores);
- Usuários com acesso **executivo/gerencial** (prefeitos, secretários, diretores, conselheiros, etc.);
- Perfis de **auditoria, controle interno, jurídico e financeiro**, quando aplicável.

2.2. Conceitos Básicos

- **Perfil de acesso:** conjunto de permissões e restrições atribuídas a um usuário, definindo o que ele pode visualizar, editar, aprovar, exportar e/ou administrar dentro do sistema.
- **Hierarquia de acessibilidade:** organização em níveis de acesso (estratégico, tático, operacional e apoio indireto), considerando a posição do usuário na estrutura institucional e a sensibilidade dos dados.
- **Princípio do mínimo privilégio:** cada usuário terá apenas o acesso estritamente necessário para cumprir suas atribuições, evitando acessos excessivos ou desnecessários.
- **Dados operacionais:** informações de campo (pontos de interesse, rotas, status de tratamento, registros de visita, fotos, observações etc.).
- **Dados gerenciais:** indicadores consolidados, dashboards, relatórios de acompanhamento, comparações entre períodos e áreas.
- **Dados estratégicos:** visões macro e comparativas (por URS, consórcio, estado, grupos de municípios), análises avançadas e projeções.
- **Dados sensíveis:** quaisquer dados que possam comprometer privacidade, segurança ou estratégia, como dados pessoais de usuários, endereços individualizados, coordenadas muito granulares vinculadas a pessoas físicas, informações contratuais e financeiras sigilosas.

2.3. Princípios Gerais

1. **Mínimo Privilégio** – nenhum usuário terá acesso maior do que o necessário.
2. **Separação de Funções** – sempre que possível, quem lança ou altera dados não é o mesmo que valida, aprova ou audita.
3. **Escopo Territorial Claro** – acessos sempre vinculados a recortes objetivos (estado, URS, consórcio, município, área de abrangência).
4. **Rastreabilidade** – ações críticas (edição, aprovação, exclusão, exportação maciça) devem ser registradas em logs com usuário, data, horário e contexto.
5. **LGPD e Sigilo** – priorizar sempre visões agregadas e anonimizadas, restringindo dados individualizados ao mínimo necessário.
6. **Governança de Perfis** – criação, alteração e revogação de perfis seguem fluxo definido de aprovação interna (gestores responsáveis) e registro em trilha de auditoria.

2.4. Classificação de Dados

Para fins de definição de acessos, os dados tratados no âmbito do Techdengue são classificados em três níveis principais:

1. Dados Públicos / Institucionais

- Informações que podem ser amplamente divulgadas, como: resultados agregados por estado, URS ou município, número total de hectares mapeados, percentual médio de redução de focos em áreas remapeadas, dados usados em releases, apresentações e relatórios públicos.
- Podem ser acessados por perfis estratégicos, de apoio indireto (ex.: comunicação) e, quando apropriado, por perfis externos com finalidade de transparência.

2. Dados Restritos

- Informações utilizadas para gestão e monitoramento, que não permitem identificar diretamente pessoas, mas podem expor estratégias e fragilidades operacionais, como:
 - indicadores por bairro/região;
 - consolidados por tipo de reservatório;
 - produtividade de equipes;
 - status detalhado de execução em contratos específicos.
- Devem ser acessados principalmente por perfis táticos e estratégicos vinculados à gestão do programa (municipal, regional, estadual, interno Aero/Techdengue), com **exportação controlada**.

3. Dados Confidenciais / Sensíveis

- Informações que podem identificar pessoas físicas ou expor detalhes excessivamente granulares de endereços e imóveis, bem como dados contratuais e financeiros sigilosos. Exemplos:
 - coordenadas e endereços individualizados;
 - dados pessoais de usuários (nome, e-mail, telefone, CPF, quando aplicável);
 - informações de contratos e condições comerciais não públicas.

- O acesso a esses dados deve ser **estritamente limitado** a perfis que realmente necessitem deles para cumprir obrigações legais, operacionais ou contratuais (ex.: jurídico, compliance, administradores técnicos, auditores autorizados).
- A exportação desses dados deve ser **excepcional, justificada e registrada em trilha de auditoria**.

A definição de quais telas, relatórios e funcionalidades expõem dados de cada categoria será utilizada como insumo para o desenho de perfis, filtros e níveis de exportação descritos nas seções seguintes.

3. Estrutura Institucional do Ecossistema Techdengue

Para fins de definição e gestão de acessos, o ecossistema do Techdengue é estruturado em **atores institucionais externos e áreas internas** da Aero/Techdengue.

3.1. Atores Externos

- **SES (Nível Estadual)**
 - Responsável pela coordenação da política estadual de enfrentamento às arboviroses;
 - Acompanha globalmente o programa (indicadores, cobertura, resultados, cumprimento de resoluções e programas).
- **URS / Órgãos Regionais / Comitês Técnicos**
 - Realizam a ponte entre estado e municípios;
 - Apoiam tecnicamente, monitoram a execução regional e em alguns casos protagonizam a validação técnica de ações e relatórios.
- **Consórcios Intermunicipais de Saúde (CIS)**
 - Coordenam ações e contratos para grupos de municípios;
 - Facilitam a contratação de serviços especializados e a gestão compartilhada de recursos e resultados.
- **Municípios**
 - São responsáveis pela execução direta das ações de vigilância e controle;

- Alimentam os dados no sistema, utilizam relatórios para tomada de decisão local e prestação de contas.
- **Empresas Prestadoras de Serviço com Drones (quando distintas da Aero)**
 - Executam mapeamentos aéreos e, quando aplicável, aplicações em campo;
 - Entregam dados técnicos (imagens, camadas, relatórios de voo) ao sistema, dentro do escopo contratado.

3.2. Atores Internos – Aero / Techdengue

As áreas internas da Aero/Techdengue que se relacionam direta ou indiretamente com o sistema são:

- **Produto & Tecnologia** – desenvolvimento, manutenção, parametrização técnica, performance, segurança da aplicação.
- **Operações & Projetos** – gestão da execução de serviços de campo, cronogramas, status de operações, interface com clientes.
- **Dados & BI** – consolidação, modelagem, análises, construção de dashboards e relatórios estratégicos.
- **Comercial & Relacionamento** – prospecção, gestão de carteira, renovação de contratos, relacionamento institucional.
- **Financeiro & Administrativo** – faturamento, controle de custos, indicadores de rentabilidade, análises econômico-financeiras.
- **Jurídico & Compliance** – gestão de contratos, termos de uso, políticas de privacidade, conformidade normativa, risco e LGPD.
- **Comunicação & Marketing** – uso de dados agregados e resultados para materiais institucionais, apresentações e comunicação pública.

Cada uma dessas áreas terá **níveis internos de acesso** definidos conforme sua necessidade de interação com o sistema (ver Seção 4).

4. Hierarquias Internas de Acessibilidade (Aero / Techdengue)

Esta seção formaliza o ponto central adicional: as **hierarquias internas de acessibilidade** das áreas ligadas direta e indiretamente ao sistema.

4.1. Níveis Internos de Acesso

Para padronização, adotam-se quatro níveis internos de acesso:

1. Nível Estratégico

- Visão ampla e consolidada (por estado, URS, consórcio, carteira de clientes);
- Acesso a indicadores estratégicos, comparações históricas, dashboards gerenciais completos;
- Permissões de edição geralmente restritas; foco em leitura, análise e tomada de decisão.

2. Nível Tático

- Visão detalhada por contrato, município, região ou carteira;
- Permissões de configuração de parâmetros locais, validação de relatórios, acompanhamento da operação;
- Atua como ponte entre estratégia e operação.

3. Nível Operacional

- Foco na rotina diária e execução das atividades;
- Acesso a telas de rotas, pontos de interesse, status de visitas, registros de campo;
- Permissão para lançar e atualizar dados operacionais dentro do escopo atribuído.

4. Nível de Apoio Indireto

- Áreas que não atuam diretamente no dado técnico/operacional, mas precisam de visões específicas para suas funções;
- Ex.: Financeiro (volume de operação para faturamento), Marketing (resultados consolidados para comunicação), Jurídico (relatórios para instrução de processos).
- Acesso predominantemente em **dados agregados e anonimizados**, com pouca ou nenhuma edição.

4.2. Matriz Conceitual – Áreas Internas x Níveis de Acesso

• Produto & Tecnologia:

- Estratégico (visão global do sistema, status de ambientes);

- Operacional (parametrizações técnicas, gestão de perfis e permissões, integrações).
- **Operações & Projetos:**
 - Tático (gestão de execução por cliente/região, priorização de recursos);
 - Operacional (acompanhamento de atividades de campo, consolidação de entregas).
- **Dados & BI:**
 - Estratégico (modelagem, indicadores-chave, análises multiestados/URS);
 - Tático (visões específicas por cliente, URS, consórcio ou grupos de municípios).
- **Comercial & Relacionamento:**
 - Estratégico (visão por carteira/cliente, uso de resultados para renovação e expansão);
 - Apoio Indireto (acesso a painéis gerenciais com foco em resultado, sem granularidade de dados sensíveis).
- **Financeiro & Administrativo:**
 - Apoio Indireto (indicadores de volume de operação, contratos ativos, entregas concluídas);
 - Sem acesso a detalhes pessoais ou granulares desnecessários à sua função.
- **Jurídico & Compliance:**
 - Estratégico (acesso a relatórios formais, evidências de execução, trilhas de auditoria);
 - Apoio Indireto (dados consolidados para embasar pareceres e decisões jurídicas).
- **Comunicação & Marketing:**
 - Apoio Indireto (dashboards públicos, resultados macros, cases consolidados);
 - Sem acesso a dados individualizados de imóveis ou pessoas.

4.3. Regras Gerais para Perfis Internos

- Cada colaborador interno terá um **perfil principal** associado à sua área de atuação e, quando necessário, um **perfil complementar de leitura**;
 - Perfis com acesso a dados sensíveis requerem **autorização explícita** de gestores estratégicos (por exemplo, diretoria);
 - Toda alteração de perfil (criação, modificação, revogação) deve constar em **trilha de auditoria** com data, responsável e justificativa;
 - Perfis temporários (como projetos especiais ou auditorias pontuais) devem ter **prazo de validade definido** e revisão obrigatória.
-

5. Áreas e Subáreas para Fins de Acesso no Sistema

5.1. Áreas Macro

Para organizar os acessos, o sistema utiliza as seguintes áreas macro:

- **Estadual (SES);**
- **Regional (URS / Comitês / CREA);**
- **Consórcios Intermunicipais (CIS);**
- **Municipal (Gestão, Vigilância, Endemias);**
- **Operação de Drones / Prestadores;**
- **Aero / Techdengue (Interno).**

5.2. Subáreas por Âmbito

No Âmbito Municipal:

- Gestão da Secretaria de Saúde;
- Vigilância Epidemiológica;
- Coordenação de Endemias;
- Agentes de Campo (ACE e similares).

No Âmbito Estadual/Regional:

- Coordenação Estadual de Arboviroses;
- Vigilância Epidemiológica Estadual;
- Coordenação de URS;
- Comitês Técnicos / CREA / Grupos de validação.

No Âmbito dos Consórcios:

- Gestão Administrativa do Consórcio;
- Coordenação Técnica/Operacional de Projetos.

No Âmbito Aero / Techdengue:

- Produto & Tecnologia;
- Operações & Projetos;
- Dados & BI;
- Comercial & Relacionamento;
- Financeiro & Administrativo;
- Jurídico & Compliance;
- Comunicação & Marketing.

Essas áreas e subáreas são a base para construção dos **perfis de acesso** descritos na próxima seção.

6. Perfis de Acesso, Permissões e Filtros

6.1. Modelo Padrão de Descrição de Perfil

Cada perfil será documentado seguindo o modelo abaixo:

- **Nome do Perfil**
- **Atores/Áreas que Utilizam**
- **Objetivo do Perfil** (frase breve)
- **Escopo Territorial** (Estado / URS / Consórcio / Município / Área / Global)
- **Nível Interno de Acesso** (Estratégico / Tático / Operacional / Apoio Indireto)
- **Permissões de Visualização** (que tipos de dados e telas pode ver)
- **Permissões de Edição/Ação** (o que pode cadastrar, editar, aprovar, exportar)
- **Restrições Específicas** (o que explicitamente não pode ver ou fazer)
- **Observações / Justificativa** (quando necessário)

6.2. Perfis Internos – Aero / Techdengue

6.2.1. Administrador Global da Plataforma

- **Atores/Áreas:** Produto & Tecnologia.
- **Objetivo:** configurar, manter e administrar tecnicamente o sistema Techdengue.
- **Escopo Territorial:** Global.
- **Nível Interno:** Estratégico + Operacional.
- **Permissões de Visualização:**
 - Todos os módulos, telas e dados, para fins de manutenção e diagnóstico.
- **Permissões de Edição/Ação:**
 - Gerenciar cadastros de instituições (SES, URS, consórcios, municípios);
 - Criar, editar e inativar usuários;
 - Configurar perfis, parâmetros globais, integrações, indicadores base;
 - Gerenciar ambientes (produção, homologação, testes).
- **Restrições Específicas:**
 - Não registrar, em nome de órgãos públicos, decisões de gestão ou validações de natureza técnico-administrativa.

6.2.2. Suporte Técnico / Helpdesk Techdengue

- **Atores/Áreas:** Produto & Tecnologia / Suporte.
- **Objetivo:** apoiar usuários na resolução de dúvidas e problemas técnicos.
- **Escopo Territorial:** Global, acesso pontual.
- **Nível Interno:** Operacional.
- **Permissões de Visualização:**
 - Acesso temporário para visualizar o sistema “como o usuário vê”;
 - Visualização de logs técnicos e status de processamento.
- **Permissões de Edição/Ação:**
 - Ajustes pontuais de cadastros, quando autorizado;
 - Reset de senha.

- **Restrições Específicas:**
 - Não editar dados epidemiológicos ou operacionais;
 - Não exportar bases completas de dados.

6.2.3. Analista de Dados & BI (Interno)

- **Atores/Áreas:** Dados & BI.
- **Objetivo:** construir dashboards, relatórios e análises internas do programa.
- **Escopo Territorial:** Global, com foco em dados agregados.
- **Nível Interno:** Estratégico.
- **Permissões de Visualização:**
 - Acesso a bases consolidadas e anonimizadas, por município, URS, consórcio, estado e períodos;
 - Visualização de indicadores operacionais e epidemiológicos.
- **Permissões de Edição/Ação:**
 - Criação e ajuste de dashboards padrão;
 - Parametrização de visões analíticas.
- **Restrições Específicas:**
 - Acesso a dados sensíveis individuais apenas quando estritamente necessário e autorizado.

6.3. Perfis – SES e Âmbito Estadual

6.3.1. Gestor Estadual SES

- **Atores/Áreas:** Coordenação Estadual de Arboviroses / Vigilância em Saúde.
- **Objetivo:** acompanhar o panorama estadual e o cumprimento dos programas vinculados ao Techdengue.
- **Escopo Territorial:** Todo o estado.
- **Nível Interno (do ponto de vista do sistema):** Estratégico.
- **Permissões de Visualização:**
 - Dashboards consolidados por URS, consórcio, município e período;
 - Indicadores de cobertura, áreas mapeadas, focos identificados, status dos planos e relatórios.

- **Permissões de Edição/Ação:**
 - Registrar pareceres ou observações em relatórios consolidados;
 - Gerar relatórios para comitês, gabinetes e instâncias de decisão.
- **Restrições Específicas:**
 - Não editar dados de campo lançados pelos municípios;
 - Não acessar dados pessoais de usuários ou informações extremamente granulares sem necessidade.

6.3.2. Analista Estadual de Dados / Epidemiologia

- **Atores/Áreas:** Núcleos de dados e epidemiologia da SES.
- **Objetivo:** analisar comportamento epidemiológico, evolução temporal e impacto das ações.
- **Escopo Territorial:** Todo o estado.
- **Nível Interno:** Estratégico/Tático.
- **Permissões de Visualização:**
 - Séries temporais de casos, focos e indicadores;
 - Mapas de calor, comparações entre municípios, URS e regiões.
- **Permissões de Edição/Ação:**
 - Geração de relatórios e extração de bases agregadas.
- **Restrições Específicas:**
 - Não gerenciar usuários;
 - Não ajustar parâmetros operacionais de municípios ou consórcios.

6.4. Perfis – URS / Comitês / Consórcios

6.4.1. Gestor Regional URS

- **Atores/Áreas:** Coordenação da URS / Vigilância Regional.
- **Objetivo:** acompanhar execução e resultados dos municípios da sua região.
- **Escopo Territorial:** Municípios pertencentes à URS.
- **Nível Interno:** Tático.
- **Permissões de Visualização:**

- Dashboards regionais, mapas dos municípios da URS;
- Situação de planos de trabalho, execuções e relatórios municipais.
- **Permissões de Edição/Ação:**
 - Registrar pareceres regionais (sem alteração dos dados originais do município).
- **Restrições Específicas:**
 - Não alterar cadastros locais de municípios;
 - Não editar dados de campo.

6.4.2. Validador Técnico / CREA / Comitê Regional

- **Atores/Áreas:** Comitês técnicos, CREA, grupos de validação.
- **Objetivo:** validar aderência técnica das ações executadas em relação aos parâmetros do programa.
- **Escopo Territorial:** URS ou conjunto de municípios sob sua alçada.
- **Nível Interno:** Tático/Estratégico.
- **Permissões de Visualização:**
 - Planos de trabalho municipais;
 - Relatórios consolidados de execução (hectares, áreas tratadas, focos, devolutivas).
- **Permissões de Edição/Ação:**
 - Registrar validação, reprovação ou pendências técnicas.
- **Restrições Específicas:**
 - Não editar dados operacionais;
 - Não gerenciar usuários.

6.4.3. Gestor de Consórcio Intermunicipal de Saúde

- **Atores/Áreas:** Gestão administrativa e técnica do consórcio.
- **Objetivo:** acompanhar a execução e os resultados dos municípios consorciados e dos contratos de serviços.
- **Escopo Territorial:** Municípios integrantes do consórcio.
- **Nível Interno:** Tático.

- **Permissões de Visualização:**
 - Dashboards e relatórios por município consorciado;
 - Situação de execução, número de atividades, áreas mapeadas e tratadas.
- **Permissões de Edição/Ação:**
 - Acompanhar e, quando previsto contratualmente, apoiar na elaboração de planos.
- **Restrições Específicas:**
 - Não alterar dados internos de cada município (como cadastros locais e rotas ACE).

6.5. Perfis – Município

6.5.1. Gestor Municipal do Programa / Secretário de Saúde

- **Atores/Áreas:** Gestão municipal de saúde.
- **Objetivo:** liderar a estratégia e o uso do programa Techdengue no município.
- **Escopo Territorial:** Município.
- **Nível Interno:** Tático/Estratégico.
- **Permissões de Visualização:**
 - Todos os dashboards e mapas do município (indicadores epidemiológicos, focos, áreas mapeadas, execução de campo);
 - Situação de planos, atividades, relatórios.
- **Permissões de Edição/Ação:**
 - Cadastro e edição de planos de trabalho;
 - Validação de relatórios municipais antes do envio à URS/estado;
 - Gestão de usuários municipais (criação, ajuste de perfis, inativação).
- **Restrições Específicas:**
 - Sem acesso a dados de outros municípios (salvo exceções formais).

6.5.2. Coordenador de Vigilância Epidemiológica Municipal

- **Atores/Áreas:** Vigilância Epidemiológica Municipal.

- **Objetivo:** analisar e interpretar dados epidemiológicos, cruzando-os com as ações de campo.
- **Escopo Territorial:** Município.
- **Nível Interno:** Tático.
- **Permissões de Visualização:**
 - Dados por bairro, região, período, tipo de foco;
 - Dashboards e mapas detalhados do município.
- **Permissões de Edição/Ação:**
 - Geração de relatórios e análises;
 - Registro de notas e interpretações internas.
- **Restrições Específicas:**
 - Não gerenciar usuários;
 - Não editar rotas ou parâmetros de campo.

6.5.3. Coordenador de Endemias / Supervisor de ACE

- **Atores/Áreas:** Coordenação de Endemias.
- **Objetivo:** transformar informações do sistema em ações concretas de campo.
- **Escopo Territorial:** Município (ou subconjuntos de bairros/áreas).
- **Nível Interno:** Operacional/Tático.
- **Permissões de Visualização:**
 - Mapa de pontos de interesse (PI), rotas, status de tratamento;
 - Status de visitas por agente.
- **Permissões de Edição/Ação:**
 - Planejar e atribuir rotas de ACE;
 - Ajustar prioridades de atendimento;
 - Consolidar retornos de campo (ex.: percentual de PI tratados, reincidências).
- **Restrições Específicas:**
 - Não alterar parâmetros globais do município;

- Não exportar dados em massa sem autorização.

6.5.4. Agente de Campo (ACE / Equipes)

- **Atores/Áreas:** Agentes de Endemias e similares.
- **Objetivo:** executar ações operacionais em campo, seguindo rotas e prioridades definidas.
- **Escopo Territorial:** Áreas, bairros ou rotas atribuídas.
- **Nível Interno:** Operacional.
- **Permissões de Visualização:**
 - Apenas sua rota e seus pontos designados;
 - Informações essenciais para execução (endereço, tipo de foco, orientações).
- **Permissões de Edição/Ação:**
 - Atualizar status do PI (tratado, eliminado, não localizado, impedimento etc.);
 - Registrar fotos e observações de campo.
- **Restrições Específicas:**
 - Não acessar dashboards globais ou dados de outros bairros;
 - Não gerenciar rotas ou outros usuários.

6.6. Perfis – Operadores de Drones / Prestadores

6.6.1. Operador de Drones

- **Atores/Áreas:** Empresas prestadoras ou equipes internas de operação de VANTs.
- **Objetivo:** realizar mapeamento aéreo e, quando aplicável, aplicação de produtos em campo.
- **Escopo Territorial:** Áreas geográficas vinculadas ao contrato.
- **Nível Interno:** Operacional.
- **Permissões de Visualização:**
 - Áreas designadas para voo;
 - Informações técnicas necessárias (limites, no-fly zones, orientações).

- **Permissões de Edição/Ação:**
 - Enviar dados de voo, imagens e camadas geoespaciais;
 - Registrar conclusão de atividades.
- **Restrições Específicas:**
 - Não acessar dados epidemiológicos detalhados;
 - Não gerenciar usuários ou perfis.

6.7. Perfis – Visualização Executiva e Auditoria

6.7.1. Visualizador Executivo (Prefeito / Secretário / Diretor / Gestores C-Level)

- **Atores/Áreas:** Lideranças políticas e executivas (município, consórcio, estado, diretoria Aero).
- **Objetivo:** acompanhar resultados de alto nível e subsidiar decisões estratégicas.
- **Escopo Territorial:** Município, consórcio, URS, estado ou carteira de clientes, conforme o cargo.
- **Nível Interno:** Estratégico.
- **Permissões de Visualização:**
 - Dashboards síntese;
 - Relatórios consolidados em PDF;
 - Comparação de períodos e cenários.
- **Permissões de Edição/Ação:**
 - Em geral, apenas geração e download de relatórios.
- **Restrições Específicas:**
 - Não editar dados operacionais;
 - Não acessar dados pessoais de usuários ou domicílios específicos.

6.7.2. Auditoria / Controle Interno

- **Atores/Áreas:** Órgãos de controle, auditorias internas/externas, compliance.
- **Objetivo:** verificar conformidade, prazos, execução e trilhas de auditoria do programa.
- **Escopo Territorial:** conforme contrato ou termo jurídico.

- **Nível Interno:** Estratégico/Tático.
 - **Permissões de Visualização:**
 - Logs de ações (quem fez o quê, quando e onde);
 - Versões de planos e relatórios;
 - Indicadores de execução e de aderência.
 - **Permissões de Edição/Ação:**
 - Registro de pareceres ou achados de auditoria.
 - **Restrições Específicas:**
 - Não editar dados primários;
 - Não alterar configurações de sistema.
-

7. Telas, Módulos e Regras de Visualização

7.1. Classificação das Telas

Para facilitar o mapeamento de acessos, as telas do sistema Techdengue são organizadas em:

1. Telas de Configuração

- Instituições (SES, URS, consórcios, municípios);
- Usuários e Perfis;
- Parâmetros globais e locais;
- Integrações e credenciais técnicas.

2. Telas de Operação

- Rotas de campo;
- Pontos de interesse (PI);
- Status de tratamento;
- Agendamento e status de voos/drones.

3. Telas de Monitoramento

- Dashboards operacionais;
- Dashboards gerenciais;

- Mapas interativos (por município, URS, consórcio, estado).

4. Telas de Relatórios

- Planos de trabalho;
- Relatórios consolidados por período;
- Relatórios específicos (por programa, contrato, projeto).

7.2. Regras Gerais de Acesso às Telas

- Cada tela estará vinculada a um **conjunto de perfis autorizados**, definido neste documento e registrado na configuração do sistema;
- Perfis operacionais terão acesso amplo às telas de operação, porém com escopo territorial limitado e filtrado (apenas sua área/rota);
- Perfis estratégicos terão acesso ampliado às telas de monitoramento e relatórios, em geral com dados agregados e consolidados;
- Perfis de apoio indireto (financeiro, marketing, jurídico) terão acesso a telas específicas com recorte em **informações relevantes à sua função**, sempre priorizando dados agregados e anonimizados;
- A exportação de dados será controlada por perfil e poderá ter níveis:
 - Exportação com dados agregados;
 - Exportação com dados sem identificação pessoal;
 - Exportação com dados completos (casos excepcionais, altamente controlados).

8. Governança de Perfis e Manutenção Contínua

8.1. Diretrizes Gerais

- A criação de novos perfis ou alteração dos existentes deverá seguir um fluxo de aprovação definido entre **gestores de produto, operação e direção**;
- Perfis com acesso a dados confidenciais/sensíveis exigem **aprovação explícita** e registro formal da justificativa;
- Todos os eventos de criação, alteração e revogação de perfis e acessos devem ser registrados em **trilha de auditoria**.

8.2. Fluxo de Criação e Alteração de Usuários

De forma geral, recomenda-se o seguinte fluxo padrão (ajustável conforme contrato ou arranjo institucional):

1. **Solicitação**

- O gestor local (ex.: Gestor Municipal, Gestor de Consórcio, Gestor de URS ou líder interno da Aero) solicita a criação ou alteração de usuário, informando:
 - Nome completo, e-mail institucional e telefone;
 - Área/setor e vínculo (município, consórcio, URS, SES, área interna da Aero);
 - Perfil de acesso desejado e justificativa;
 - Escopo territorial (município X, municípios do consórcio Y, URS Z, etc.).

2. **Validação da Solicitação**

- O gestor responsável (ex.: coordenação do contrato ou da área de operações) analisa se o perfil solicitado é compatível com as funções do usuário;
- Em caso de perfis estratégicos ou com acesso a dados sensíveis, deve haver validação adicional (ex.: direção, jurídico/compliance).

3. **Implementação no Sistema**

- O time de **Produto & Tecnologia / Suporte** realiza a criação ou alteração do usuário no ambiente de produção;
- Atribui o perfil correto, escopos territoriais e, quando aplicável, data de expiração do acesso (acessos temporários).

4. **Comunicação e Registro**

- O usuário é informado sobre seu acesso, nível de perfil e responsabilidades;
- O processo (solicitação, aprovação, execução) é registrado na trilha de auditoria do sistema ou em ferramenta dedicada (ex.: sistema de chamados).

8.3. **Revisão Periódica de Acessos**

- Recomenda-se que, ao menos **uma vez por semestre**, sejam revisados:
 - Usuários ativos por contrato/instituição;

- Perfis atribuídos a cada usuário;
 - Usuários sem acesso recente (por exemplo, sem login há mais de 90 dias).
- A revisão deve resultar em:
 - Revogação de acessos desnecessários;
 - Ajuste de perfis excessivamente amplos;
 - Atualização de usuários que mudaram de função.

8.4. Desligamento e Encerramento de Vínculo

Em situações de desligamento de colaborador ou encerramento de contrato com instituição/município, o processo mínimo recomendado é:

1. Notificação Interna

- A área responsável (RH, Gestão de Contratos ou equivalente) informa o time de Produto & Tecnologia / Suporte sobre o desligamento ou encerramento.

2. Revogação de Acesso

- Desativar usuários vinculados à instituição/município ou colaborador desligado;
- Revogar credenciais de integração específicas, quando existirem.

3. Registro

- Registrar data, hora, responsável e motivo da revogação;
- Quando aplicável, guardar evidências em dossiês de contrato ou de pessoa.

8.5. Tratamento de Incidentes de Acesso

Em caso de incidente real ou suspeito envolvendo acessos (ex.: uso indevido, compartilhamento de login, exportação de dados sem autorização), recomenda-se o seguinte procedimento mínimo:

1. Resposta Imediata

- Bloqueio imediato ou redução do perfil do usuário envolvido;
- Suspensão temporária de exportações mais sensíveis, se necessário.

2. Análise

- Levantamento de logs e contexto (o que foi feito, quando, de onde);
- Identificação dos dados possivelmente afetados e dos impactos.

3. Registro Formal

- Registro do incidente em canal oficial (ex.: sistema de segurança da informação, registro interno de incidentes);
- Notificação às áreas envolvidas (Produto, Operações, Jurídico/Compliance, cliente, quando aplicável).

4. Medidas Corretivas

- Ajuste de perfis, políticas e fluxos, se necessário;
- Orientação/retreinamento dos usuários;
- Adoção de controles adicionais (ex.: reforço de MFA, limitação de exportações, alertas automáticos).

9. Anexo I – Modelo de Ficha de Perfil de Acesso

Nome do Perfil:

Atores/Áreas que Utilizam:

Objetivo do Perfil:

Escopo Territorial:

Nível Interno de Acesso:

Permissões de Visualização:

- ☐ Dados operacionais
- ☐ Dados gerenciais
- ☐ Dados estratégicos
- ☐ Dados sensíveis (justificar)

Permissões de Edição/Ação:

- ☐ Configuração de parâmetros
- ☐ Gestão de usuários
- ☐ Edição de dados operacionais
- ☐ Validação/aprovação de planos/relatórios
- ☐ Exportação de dados

Restrições Específicas:

Observações / Justificativa do Acesso:

10. Anexo II – Matriz de Perfis x Ações (Versão Conceitual)

A tabela abaixo serve como referência conceitual para o time de produto/tecnologia e para as áreas de operação e contrato na hora de configurar os perfis no sistema. Ela pode ser detalhada em planilha ou ferramenta própria, com nível de granularidade maior.

Linhas (exemplos de ações principais):

1. Visualizar dashboard estadual consolidado.
2. Visualizar dashboards por URS.
3. Visualizar dashboards por município.
4. Visualizar mapa de pontos de interesse (PI) de um município.
5. Visualizar rota atribuída a um agente.
6. Editar plano de trabalho municipal.
7. Validar relatório municipal antes do envio à URS/estado.
8. Registrar parecer técnico (CREA/comitê).
9. Cadastrar/editar usuários de um município.
10. Exportar dados agregados por município.
11. Exportar dados agregados por URS/consórcio.
12. Exportar dados com granularidade de endereço/PI.
13. Enviar dados de voo de drone.
14. Editar rotas de ACE.
15. Atualizar status de PI em campo.
16. Visualizar trilha de auditoria (logs de ações).
17. Gerenciar instituições (criar/editar SES, URS, consórcios, municípios).
18. Gerenciar perfis globais e parâmetros do sistema.

Colunas (principais perfis):

- Administrador Global da Plataforma (Aero)
- Suporte Técnico / Helpdesk Techdengue
- Analista de Dados & BI (Interno)
- Gestor Estadual SES

- Analista Estadual de Dados / Epidemiologia
- Gestor Regional URS
- Validador Técnico / CREA / Comitê Regional
- Gestor de Consórcio Intermunicipal de Saúde
- Gestor Municipal do Programa / Secretário de Saúde
- Coordenador de Vigilância Epidemiológica Municipal
- Coordenador de Endemias / Supervisor de ACE
- Agente de Campo (ACE / Equipes)
- Operador de Drones
- Visualizador Executivo
- Auditoria / Controle Interno

Em uma implementação prática (como planilha ou módulo interno), para cada combinação **Ação x Perfil** deverá ser indicado, por exemplo:

- ✓ – Ação permitida;
- ✕ – Ação não permitida;
- △ – Ação permitida em condições específicas (ex.: mediante justificativa ou em ambiente restrito).

Essa matriz é dinâmica e deve ser atualizada conforme a evolução do sistema, surgimento de novos perfis ou mudanças nos contratos e programas.