

Guia do responsável técnico municipal

CA Informática | Monitor360APS, Hospital360 e Chamadas e-SUS

Versão 1.0 - piloto Beruri - 17/09/2026. A plataforma de Automação SaaS CA Informática está em fase de testes. Os acessos das três aplicações de Beruri estão disponíveis ao responsável municipal. A conexão técnica ao PEC de Beruri foi validada nas três aplicações por túnel privado e conta somente leitura. A voz Google e os fluxos assistenciais ainda exigem validação própria.

1. Quem configura e como começar

O município, por seu responsável técnico autorizado, cadastra as informações do PEC diretamente nas aplicações, depois do primeiro acesso. Não é necessário enviar senhas para a CA Informática por e-mail, WhatsApp ou arquivo para criar o ambiente.

A CA Informática prepara o ambiente, os acessos e a infraestrutura de integração. O município autoriza o uso dos dados, administra seu PEC e informa as credenciais nas telas protegidas. A plataforma precisa armazenar e usar esses segredos para realizar a integração; isso não elimina as responsabilidades de segurança da empresa.

1. Utilize a mensagem de entrega. Os endereços e identificadores de Beruri estão na seção 7; as senhas provisórias seguem no anexo privado do e-mail, nunca no site.
2. Entre com a credencial provisória. O assistente exige seu nome, e-mail e uma nova senha de pelo menos 12 caracteres. Ao concluir, o acesso provisório é desativado. Entre novamente com sua conta pessoal; não compartilhe a conta com a equipe.
3. Confira município e instituição. Se aparecerem dados de outra instituição, interrompa o acesso e avise o suporte.
4. Neste piloto de Beruri, a conexão PEC já foi cadastrada com autorização do proprietário. Confira a configuração salva e teste a conexão; não substitua o endereço do conector privado pelo IP público. As instruções seguintes orientam futuras alterações pelo responsável.
5. Configure a voz Google nos painéis que serão utilizados. O projeto Google, as chaves e eventuais cobranças pertencem ao município.
6. Valide a conexão e os fluxos autorizados com a equipe. As licenças emitidas em 17/09/2026 vencem em 17/10/2026. O aceite técnico será registrado separadamente; eventual ajuste da validade exige confirmação da CA Informática.

O pacote inicial contém as três aplicações. Hospedagem ou instalação de servidor PEC é um serviço separado, sob consulta à CA Informática.

2. Preparar a conexão com o PEC

Reúna estas informações com a equipe que administra o PEC. Digite-as somente na aplicação correspondente, após autenticação.

- **Host/IP:** endereço do servidor PEC acessível pela rota autorizada do SaaS. Não inclua `http://`, caminho de página ou endereço do login web.
- **Porta:** porta do PostgreSQL do PEC, confirmada pelo administrador. 5433 é um exemplo comum, não uma regra.
- **Banco de dados:** nome confirmado pelo administrador; não presume que seja `esus`.
- **Usuário e senha:** conta de integração própria, com somente leitura e permissões limitadas às consultas necessárias. Não utilizar a conta administrativa `postgres`.

Prefira contas distintas por aplicação para facilitar revogação e auditoria. A equipe do PEC deve preparar as permissões; este guia não concede acesso ao banco automaticamente.

Atenção ao endereço: localhost dentro da aplicação aponta para o próprio container. Um IP de rede interna municipal, como 192.168.x.x, exige uma rota privada ou VPN previamente configurada; preencher esse IP não cria a rota.

A CA Informática informa os requisitos de conectividade e a origem efetiva das conexões. A equipe municipal configura a rede e autoriza somente a origem/rota acordada. Não exponha o banco indiscriminadamente à internet. Proteção de transporte, certificado quando aplicável e rota devem ser validados na implantação; não há neste guia um botão de TLS presumido para todas as aplicações.

Antes de testar: confirme que o PEC está ativo, que o nome resolve na rota autorizada, que a porta está correta e que a conta possui apenas as permissões necessárias. A senha continua com o responsável municipal: o suporte pode diagnosticar horário, erro sanitizado e disponibilidade sem recebê-la.

3. Configurar o Monitor360APS

1. Acesse o Monitor360APS com a conta administrativa municipal e abra **Integração PEC**. Na versão em bancada, a rota é /integracao-pec, relativa ao endereço da aplicação.
2. Preencha **Host**, **Porta**, **Banco de dados**, **Usuário** e **Senha** com os dados autorizados do município.
3. Se houver **Modo de integração**, utilize o modo homologado para sua versão do PEC, indicado na liberação do ambiente. Não altere esse modo por tentativa.
4. Clique em **Testar com os dados do formulário** para verificar os valores digitados antes de salvar. Se houver falha, revise rede, usuário e permissões.
5. Clique em **Salvar configurações**. Em seguida use **Testar conexão** para verificar os valores efetivamente armazenados.
6. Reabra a página para confirmar host, porta e banco. Uma senha mascarada ou não reapresentada é esperada; não faça capturas contendo o segredo.
7. Somente após resultado satisfatório execute a primeira sincronização prevista para o ambiente, com o escopo municipal conferido. Verifique data de atualização e consistência dos resultados com o responsável local.

Limites do acesso: os recursos de instalação encontrados na bancada, como usuário administrativo temporário e aplicação de permissões padrão no PEC, não fazem parte do procedimento municipal SaaS. A versão liberada deverá restringi-los. Não informe senha administrativa do PEC nessas opções.

Se o teste de conexão passar, mas a sincronização falhar, não aumente permissões para administrador. Envie ao suporte o nome da aplicação, horário e mensagem de erro sem dados pessoais. A conta pode precisar de uma permissão específica de leitura ou de compatibilidade com a versão do PEC.

4. Configurar Hospital360 e Chamadas e-SUS

Hospital360

1. Entre no Hospital360 e abra **Configuração e-SUS PEC** (/conexao_pec.php na bancada).
2. Na seção **Banco de dados e-SUS PEC**, preencha Host, Porta, Banco, Usuário e Senha.
3. Clique em **Salvar configurações** e depois em **Testar e-SUS PEC**. Confirme que o teste se refere ao PEC municipal.
4. Valide o fluxo de consulta autorizado antes de importar dados ou iniciar utilização assistencial. Um teste de conexão não comprova sozinho a homologação clínica do sistema.

Não altere a seção **Banco de dados Hospital**: trata-se do banco interno mantido pela CA Informática. Na versão SaaS, essa alteração deve ser restrita ao operador da plataforma. O painel de chamadas integrado usa a integração do Hospital360; sua voz Google é configurada separadamente, conforme a próxima página.

Chamadas e-SUS independente

1. Entre na aplicação e abra **Configurações** (/configuracoes na bancada). Autentique-se com a credencial administrativa fornecida para esse ambiente.
2. Escolha a aba **PEC**. Preencha Host, Porta, Banco de dados, Usuário e Senha do banco.
3. Use **Testar conexão** e **Salvar PEC**. Depois teste novamente a configuração salva. Use **Reconectar** se a tela solicitar restabelecer a sessão após a alteração.
4. Confira as unidades autorizadas e faça um teste controlado do painel, do som e dos dispositivos previstos para a unidade.

Chamadas independente e painel integrado do Hospital360 são componentes distintos. Configurar um não significa que o outro recebeu a mesma chave Google ou as mesmas preferências de voz.

5. Criar e cadastrar a chave de voz Google

Nas versões analisadas, o campo de voz recebe uma **chave de API**. Não cole um token OAuth temporário nem um arquivo JSON de conta de serviço. O código atual dos painéis faz a síntese de voz no servidor usando essa chave.

1. Entre no [Google Cloud Console](#) com a conta institucional autorizada. Crie ou selecione um projeto do município, vincule o faturamento aprovado e ative **Cloud Text-to-Speech API** em **APIs e serviços > Biblioteca**. [Preparação oficial](#).
2. Em **APIs e serviços > Credenciais**, escolha **Criar credenciais > Chave de API**. Nas restrições de API, permita somente **Cloud Text-to-Speech API**. Para chamadas feitas pelo servidor, use restrição por **endereços IP**, com a origem pública de saída confirmada pela CA Informática. Não use o IP do computador municipal nem restrição de site/navegador. Salve e guarde a chave em local protegido. [Gerenciar e restringir chaves](#).
3. Recomendamos uma chave identificada para o Chamadas e outra para o Hospital360, permitindo revogação independente. A CA Informática informará a origem de saída antes desse cadastro; não presuma que todo endereço de entrada do site seja também a saída.
4. **Chamadas independente**: em Configurações, localize **Credenciais Google TTS** na área de voz do painel. Use **Trocar**, insira a chave, confirme em **OK** e faça o teste de voz disponível.
5. **Painel do Hospital360**: abra as configurações do painel integrado (/configuracoes na bancada), com permissão de gerenciamento do painel. Localize **Credenciais Google TTS**, salve a chave e faça o teste Google TTS.
6. Use uma frase fictícia, por exemplo: “Senha de teste, dirigir-se à sala um”. Confira o áudio no dispositivo de exibição. Nunca publique a chave em prints, manuais ou chamados de suporte.

O texto enviado para síntese é processado pelo Google. O município deve definir o conteúdo permitido e considerar esse serviço no seu tratamento de dados. Evite nomes e informações clínicas quando a identificação por senha for suficiente.

Configure alertas de orçamento no projeto. Alertas **não interrompem automaticamente os gastos**. A cobrança depende do uso e da categoria de voz; não há promessa de gratuidade neste pacote. [Orçamentos e alertas e preços Google TTS](#).

6. Validar, solucionar e manter

- **Tempo esgotado ou conexão recusada:** confirme host, porta, disponibilidade, VPN/rota e firewall. Não resolva abrindo o banco para qualquer IP.
- **Falha de autenticação:** revise usuário e senha no painel da aplicação. Não envie a senha ao suporte.
- **Permissão negada ou tabela ausente:** confirme as permissões específicas de leitura e a compatibilidade da versão do PEC.
- **Erro Google 403:** confira API ativada, faturamento, restrições da chave e origem pública efetiva. Não remova permanentemente todas as restrições como solução.
- **Erro Google 429:** consulte cotas e uso no projeto municipal antes de repetir várias tentativas.
- **Teste concluído, mas sem som na TV:** confira volume, saída de áudio e permissão de reprodução do navegador/dispositivo.

Checklist antes de iniciar os 30 dias

1. Endereços HTTPS, instituição e administrador conferidos.
2. PEC configurado pelo município em cada aplicação necessária; conexão salva testada.
3. Escopo de leitura, unidades e resultados conferidos pelo responsável municipal.
4. Voz e dispositivos testados; contas e cobranças Google sob controle municipal.
5. CA Informática confirmou a homologação do ambiente, os backups e o procedimento de suporte; município registrou o aceite e recebeu as datas do teste.

Troca de responsável ou credencial: revise acessos, substitua senhas/chaves na aplicação, teste a nova configuração e só então revogue a credencial anterior. Em suspeita de vazamento, revogue imediatamente e acione o suporte. Não reutilize a chave de outro município.

Suporte: **WhatsApp (92) 99158-0637**, [abrir conversa com o suporte](#), ou **contato@cainformatica.com.br**. Se encontrar um erro, tire um print e envie pelo WhatsApp, informando aplicação, município, horário e o que estava fazendo. Antes de enviar, oculte nomes e dados de pacientes, senhas, tokens e outras informações sensíveis. Não encaminhe prontuários ou o anexo de acessos ao suporte. Configurar pessoalmente os segredos não impede tecnicamente todo acesso administrativo à hospedagem; acessos excepcionais devem obedecer às regras de autorização e auditoria do serviço.

Referência de versão: telas, código e primeiro acesso das três aplicações conferidos em 17/09/2026; instruções Google consultadas na mesma data. A validação do acesso não substitui os testes da integração municipal.

7. Endereços e primeiro acesso de Beruri

Município: Beruri/AM. **Código IBGE:** 1300631. Este anexo é específico deste ambiente.

Página de entrada: beruri.cainformatica.com.br.

- **Hospital360:** [abrir Hospital360](#). Identificador provisório: beruri@hospital360.local.
- **Monitor360APS:** [abrir Monitor360APS](#). Identificador provisório: beruri@monitor360aps.local.
- **Chamadas e-SUS:** [abrir configurações do Chamadas](#). Identificador provisório: beruri@painel.local.

Esses identificadores não são caixas de e-mail. Cada aplicação possui senha provisória própria e administração independente. A senha está no anexo privado entregue pela CA Informática; não encaminhe esse anexo para grupos ou chamados de suporte.

1. Abra o endereço da aplicação e digite o identificador e a senha correspondente.
2. Na tela **Crie seu acesso pessoal**, informe seu nome completo, seu e-mail pessoal ou institucional e uma senha exclusiva. Confirme a senha. Não reutilize a provisória.
3. Conclua o cadastro e faça novo login com seu e-mail e a nova senha. O identificador provisório deixa de funcionar.
4. Repita nas outras aplicações contratadas. Somente depois configure a integração com o PEC e a voz, conforme as seções anteriores.

Acesso individual: as credenciais provisórias servem para o responsável criar o próprio perfil. Depois, cadastre os profissionais nas opções de usuários de cada aplicação. Não compartilhe sua senha pessoal com toda a equipe.

Conectividade de Beruri: a integração PEC utiliza um túnel cifrado exclusivo. Nas três aplicações, o host técnico é /run/ca-pec, porta 5433, banco esus, usuário esus_leitura; a senha já está salva nos locais privados e não integra este guia. Esse caminho funciona somente neste ambiente SaaS. Não é endereço web nem um IP público. As redes dos containers continuam isoladas; o túnel permite somente a conexão ao PEC de Beruri. Google TTS ainda depende da chave institucional e da liberação/teste de saída específica.

Prazo e testes: este material orienta o primeiro acesso. As licenças emitidas vencem em 17/10/2026; o aceite técnico ainda deve ser registrado. Não presuma renovação automática da licença. Caso encontre um erro em qualquer aplicação, envie um print sem informações sensíveis ao WhatsApp (92) 99158-0637. Sugestões de melhoria também são bem-vindas.