serpro.gov.br

Receita Integra
Documentação Técnica

Versão do Documento – 1.0

Última Atualização - 06/02/2026

Serpro

1.Contextualização

O Receita Integra tem como objetivo padronizar, centralizar e fortalecer a governança do acesso externo às APIs e serviços disponibilizados por entes externos aos sistemas da Receita Federal.

A iniciativa busca estabelecer um modelo único de integração, promovendo maior controle, rastreabilidade, segurança e conformidade no consumo desses serviços. Para isso, foram adotados protocolos amplamente reconhecidos e consolidados no mercado, como o OAuth 2.0, utilizado para autorização segura e controle de acesso às APIs, garantindo que apenas aplicações devidamente autenticadas e autorizadas possam consumir os recursos disponibilizados.

Esse documento tem como objetivo descrever tecnicamente os aspectos técnicos e de segurança implementados, bem como as estruturas de dados envolvidas nesse compartilhamento.

1.1. Autenticação e Autorização (OAuth 2.0)

As APIs disponibilizadas utilizam o padrão OAuth 2.0, conforme a RFC 6749, com uso de Bearer Tokens (RFC 6750) e TLS (HTTPS) para proteção do transporte das informações.

O modelo adotado é o Client Credentials Flow, indicado para comunicação máquina-a-máquina (M2M), sem interação de usuário final.

Credenciais de Acesso

Cada empresa receberá um conjunto de credenciais composto por:

- client_id
- client_secret

Essas credenciais são utilizadas exclusivamente para obtenção do token de acesso junto ao Authorization Server.

Envio do Token

Após a obtenção do token, todas as chamadas devem incluir o cabeçalho HTTP:

```
Authorization: Bearer <access_token>
```

Tokens enviados fora desse padrão ou ausentes resultarão em erro de autenticação.

1.2. Ambientes

Ambiente	Authorization Server (OAuth)
Homologação	`https://h-api.receitafederal.gov.br/token`
Produção	`https://api.receitafederal.gov.br/token`

1.2.1 Controle de Acesso por Origem (ACL)

No ambiente de Homologação, o acesso à solução é adicionalmente protegido por meio de listas de controle de acesso (ACL) baseadas em endereços IP ou intervalos de IP (CIDR) de origem.

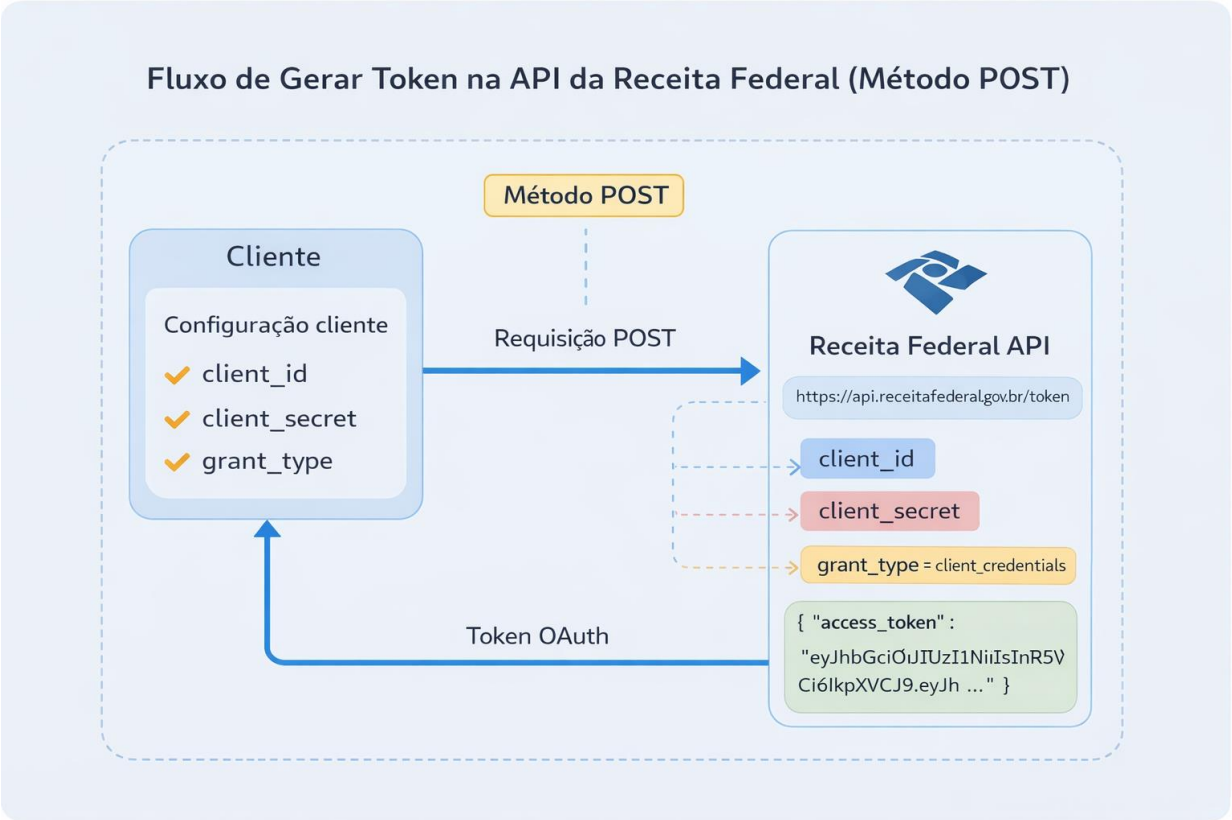
Dessa forma, para utilização da API em homologação, as empresas integradoras devem informar previamente os endereços IP ou ranges de origem a partir dos quais as requisições serão realizadas, para que possam ser devidamente cadastrados e liberados no ACL do ambiente.

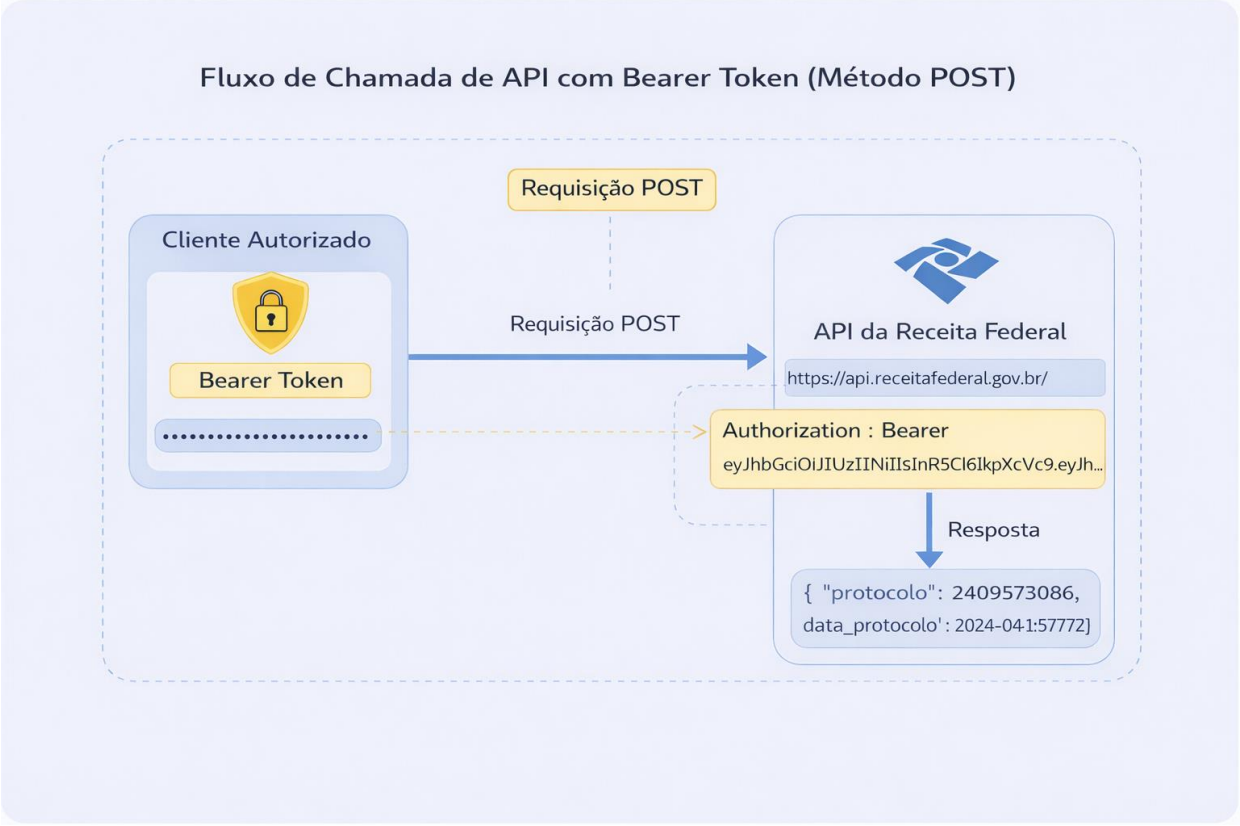
Requisições originadas de endereços não autorizados no ACL serão bloqueadas, independentemente da validade das credenciais OAuth 2.0 utilizadas.

Em caso de qualquer alteração nos IPs ou ranges previamente informados, a empresa integradora deverá comunicar a mudança de forma antecipada, permitindo a atualização do ACL e evitando indisponibilidades no acesso à solução.

No ambiente de Produção, não está configurado ACL explícito por restrição de IP de origem. O controle de acesso é realizado exclusivamente por meio dos mecanismos de autenticação e autorização previstos no OAuth 2.0, associados às credenciais específicas de cada empresa e aos respectivos escopos autorizados.

1.3. Diagrama


Fluxo de Gerar Token na API da Receita Federal (Método POST)
Método POST
Cliente
Configuração cliente
client_id
client_secret
grant_type
Requisição POST
Receita Federal API
https://api.receitafederal.gov.br/token
client_id
client_secret
grant_type = client_credentials
{ "access_token" : "eyJhbGciOiJIUzI1NiIsInR5V Ci6IkpXVCJ9.eyJh ..." }
Token OAuth


Fluxo de Chamada de API com Bearer Token (Método POST)
Requisição POST
Cliente Autorizado
Bearer Token
Requisição POST
API da Receita Federal
https://api.receitafederal.gov.br/
Authorization : Bearer eyJhbGciOiJIUzIINiIIsInR5CI6IkpXcVc9.eyJh...
Resposta
{ "protocolo": 2409573086, data_protocolo' : 2024-04-1:57772]

1.4. Tabela de Erros

A solução adota códigos de status HTTP padronizados para sinalização de erros, os quais podem ser retornados tanto pela camada de gerenciamento de APIs (API Gateway) quanto pelos serviços backend, conforme o estágio de processamento da requisição.

Código HTTP	Descrição	Possível Causa
400	Bad Request	Requisição malformada ou parâmetros inválidos
401	Unauthorized	Token de acesso ausente, inválido ou expirado
403	Forbidden	Token válido, porém sem escopo ou permissão para acesso ao recurso
404	Not Found	Endpoint inexistente ou recurso não disponível
429	Too Many Requests	Limite de requisições excedido, conforme políticas de rate limit configuradas
500	Internal Server Error	Erro interno durante o processamento da requisição

1.5. Aspectos de Segurança

O acesso às APIs é protegido por meio do protocolo OAuth 2.0, utilizando o fluxo client_credentials, garantindo autenticação segura entre sistemas (machine-to-machine).

A obtenção do token de acesso ocorre exclusivamente via método HTTP POST, sobre conexão HTTPS, assegurando a confidencialidade e integridade das credenciais de autenticação. O Bearer Token emitido possui validade inicialmente configurada para 60 (sessenta) minutos e deve ser encaminhado em todas as requisições subsequentes no cabeçalho HTTP Authorization, no formato:

Authorization: Bearer <token>

Essa abordagem evita a exposição de informações sensíveis em URLs ou corpos de mensagens. Antes de processar qualquer requisição, a API realiza a validação completa do token, incluindo verificação de assinatura, prazo de expiração e escopos autorizados.

Como resposta às requisições válidas, a API retorna exclusivamente um identificador de protocolo, não expondo dados sensíveis no payload de resposta.

Recomenda-se que o gerenciamento de credenciais e tokens seja realizado exclusivamente em ambientes de backend, com adoção de cofres seguros (secret vaults), controle de acesso restrito e políticas de rotação periódica de credenciais, em conformidade com as boas práticas de segurança da informação e normas vigentes.