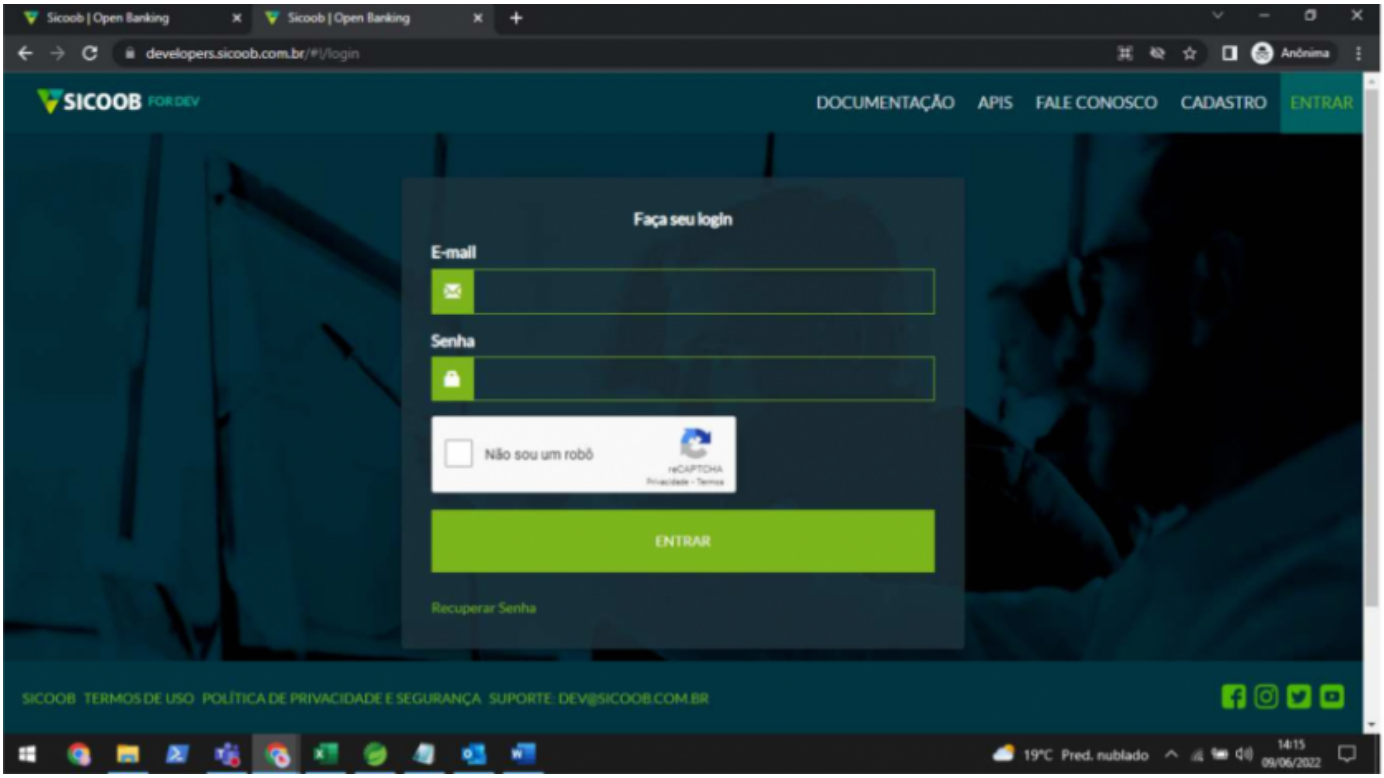
Sicoob

- Credenciais para API
- Dicas preenchimento convênio - Sicoob
- Converter certificado para .PEM

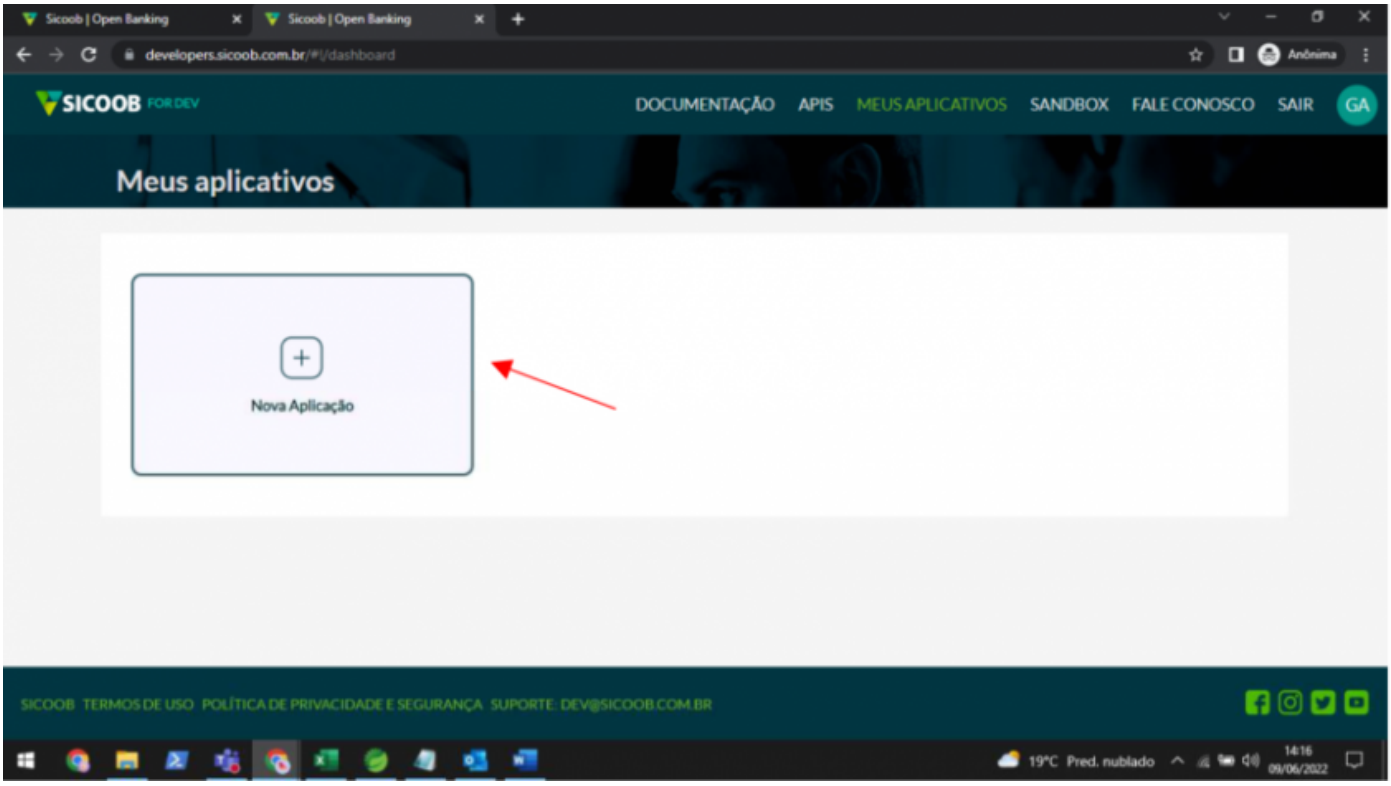
Credenciais para API

1 - Para o Cliente

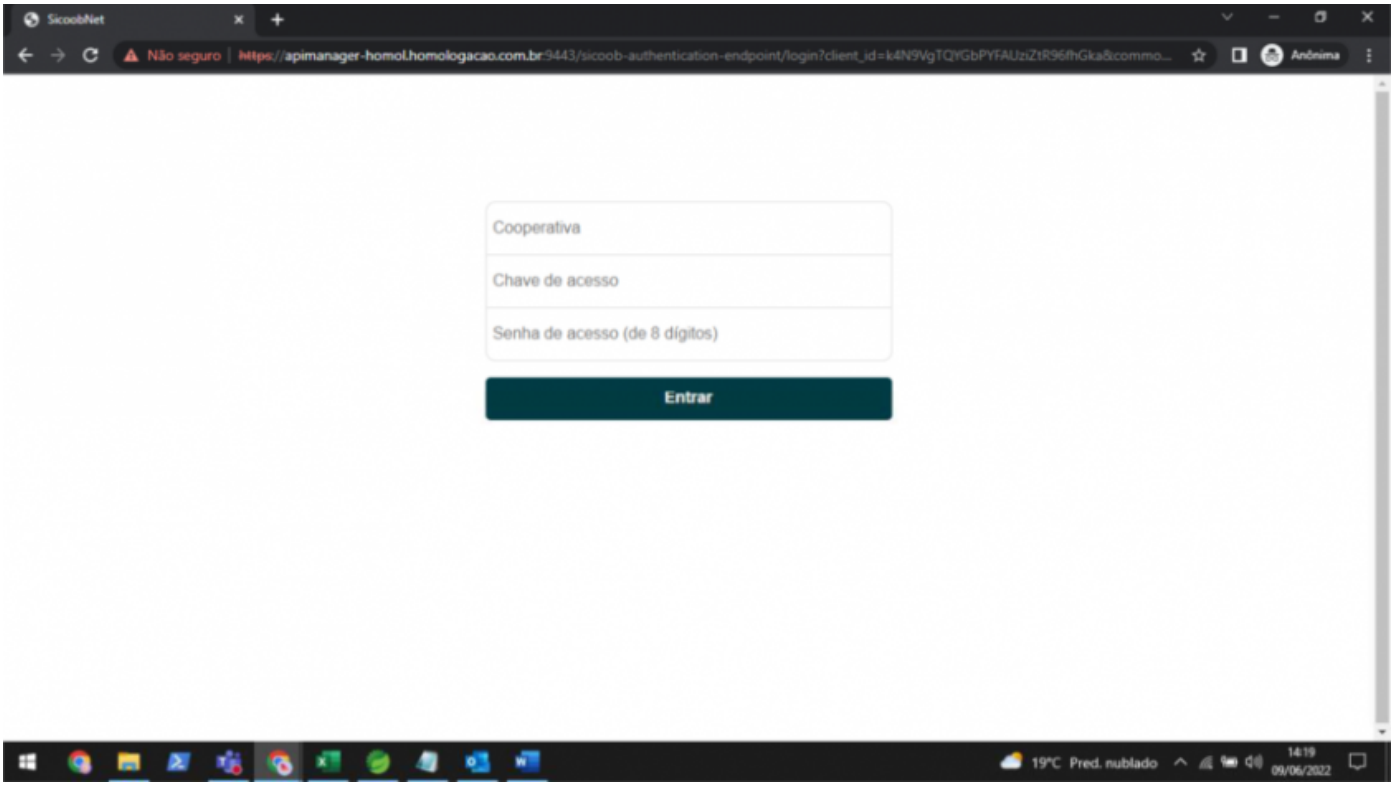
1.1 - Faça login no Portal Developers (https://developers.sicoob.com.br)



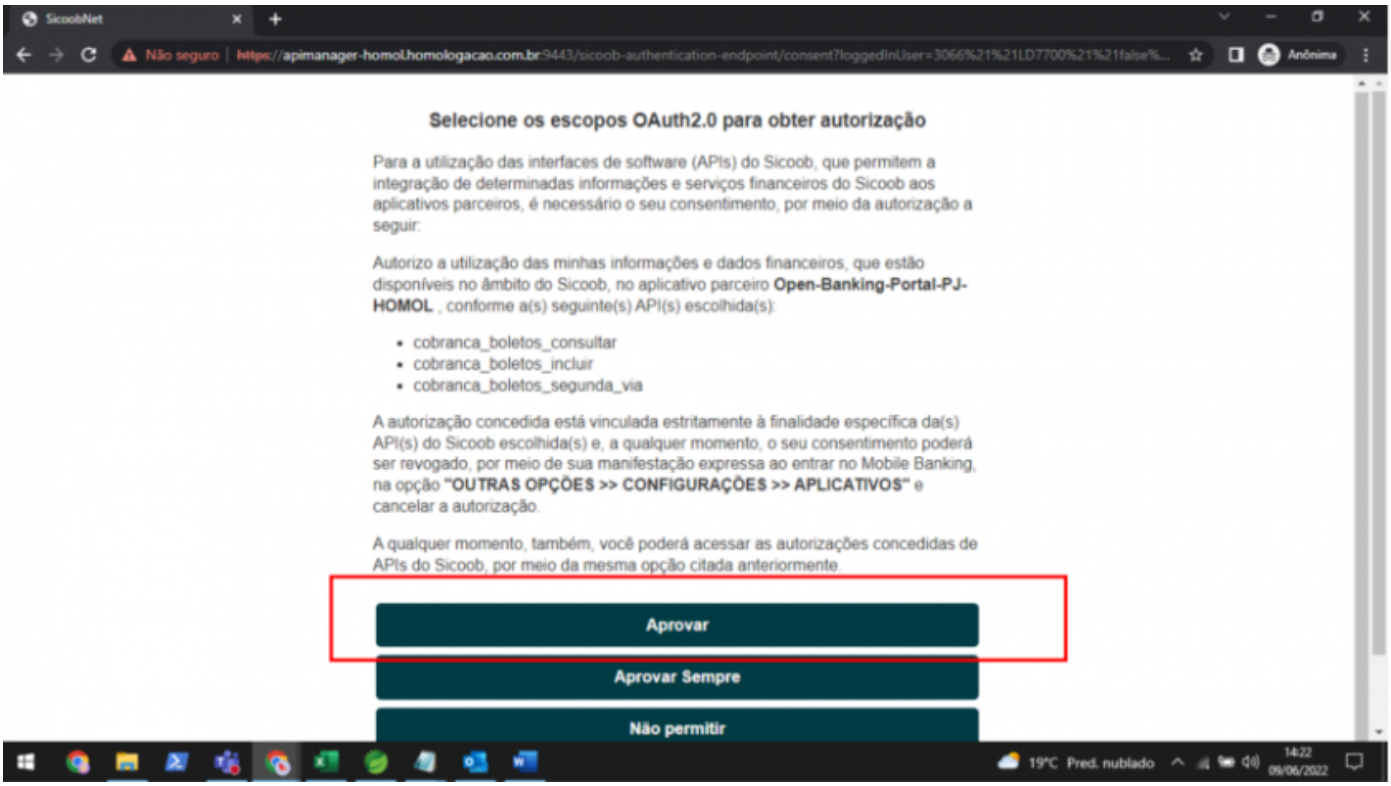
1.2 - Criar uma nova aplicação



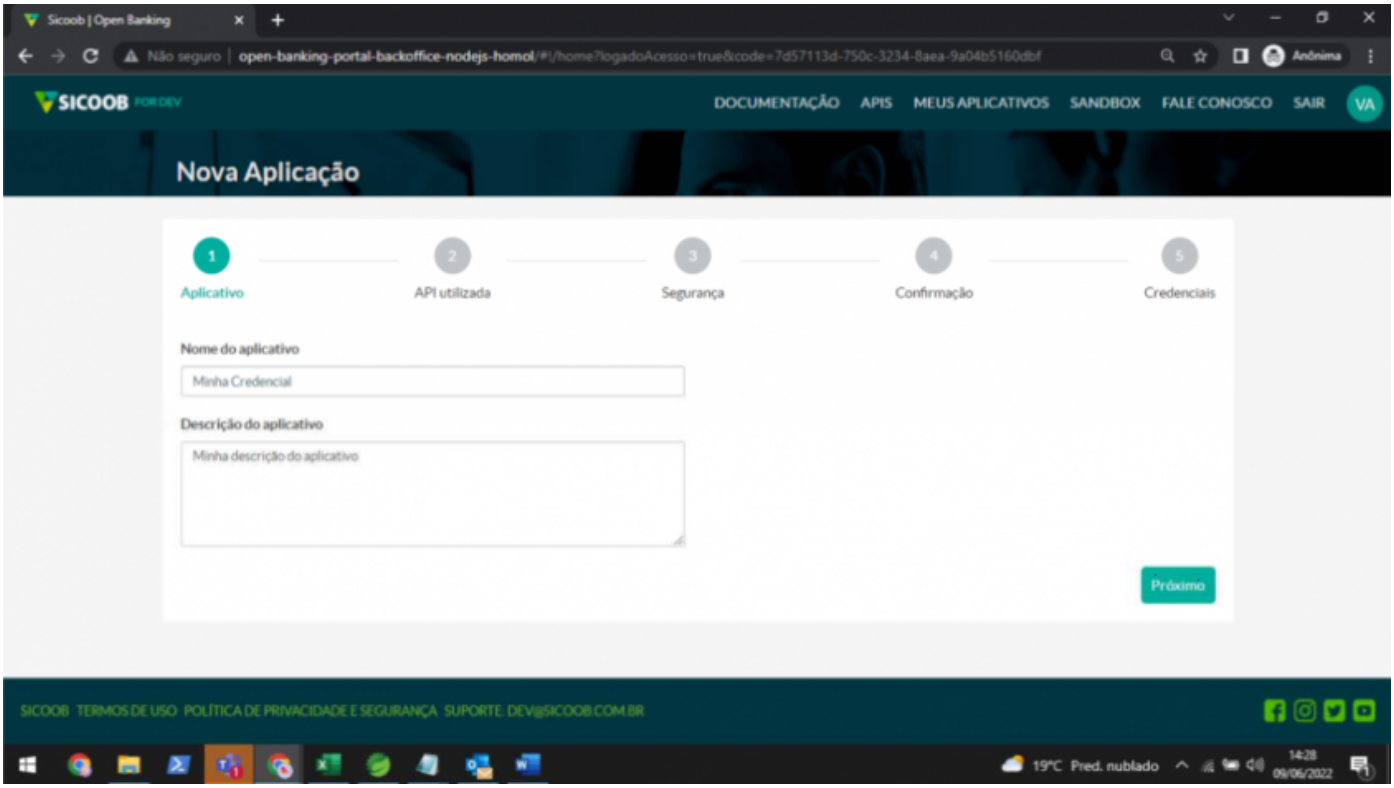
1.3 - Efetuar login com credencial SicoobNet



1.4 - Aprovar termos de autorização

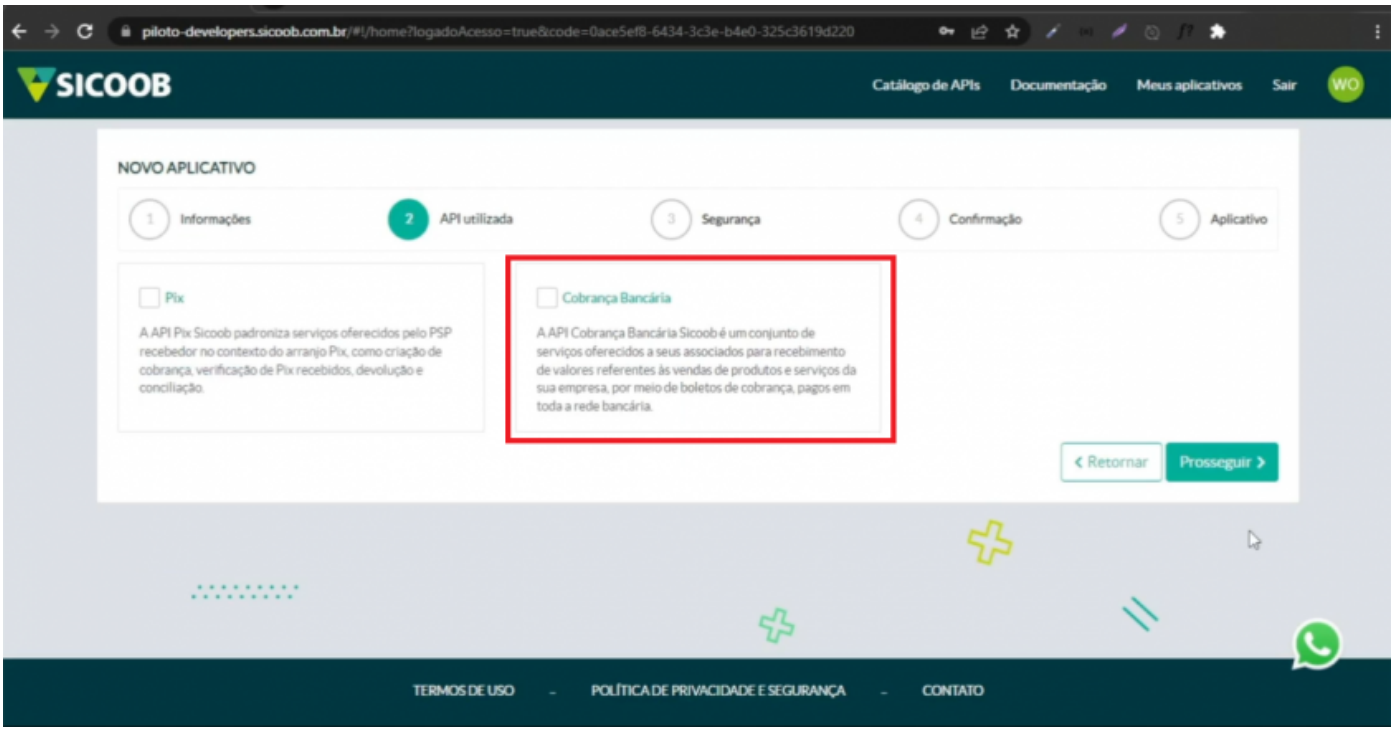


1.5 - Preencher dados iniciais da aplicação (Nome e descrição) e clicar em próximo

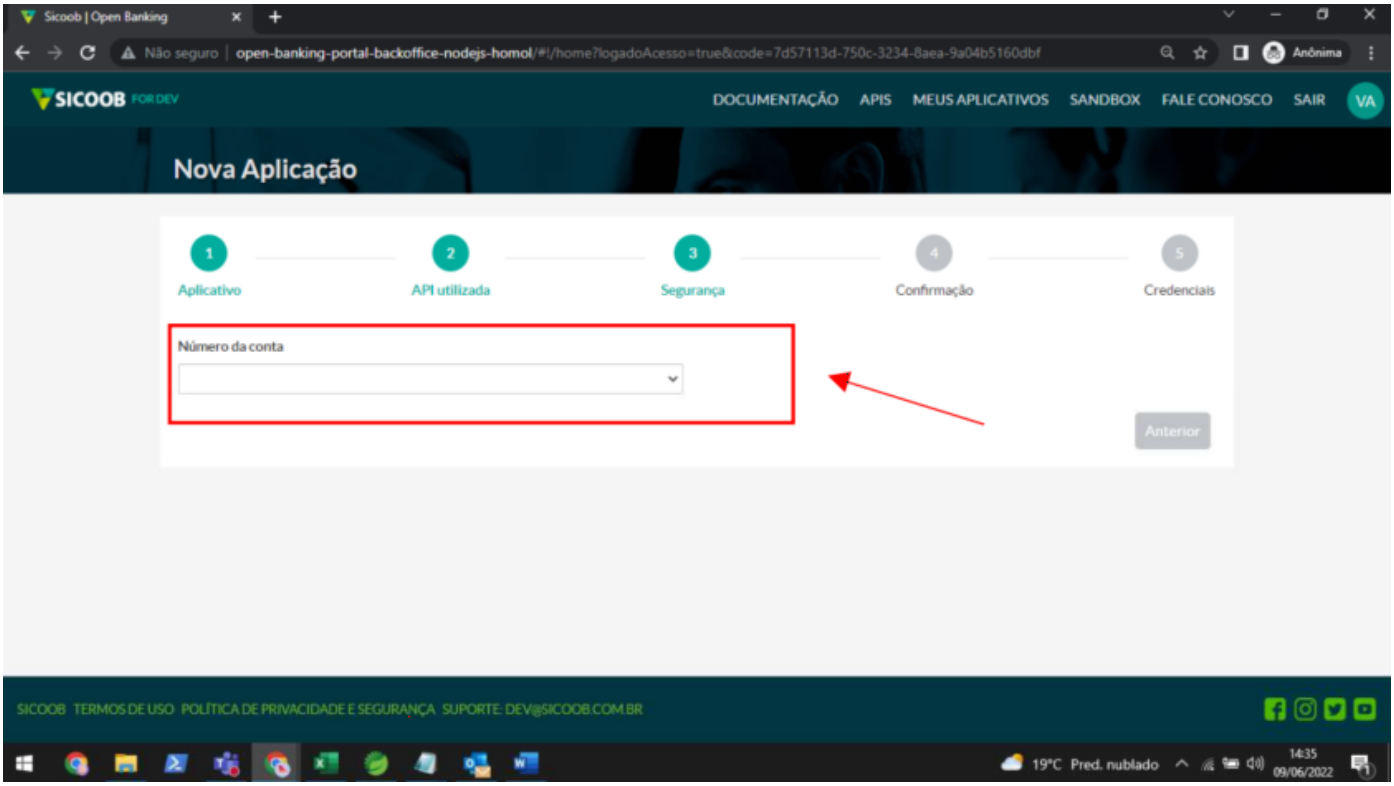


1.6 - Selecione a API Utilizada

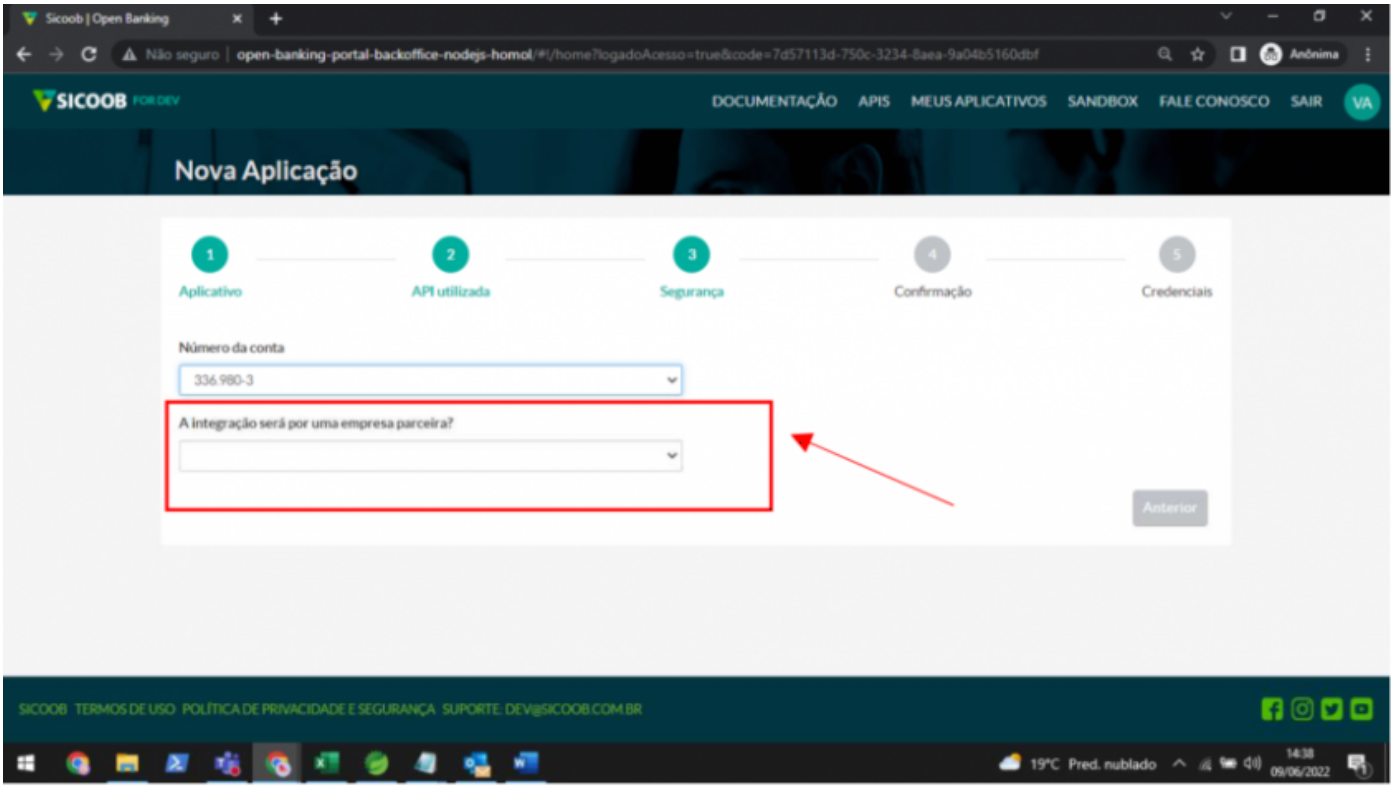
Em nosso caso é a opção "Cobrança Bancária".



1.7 - Selecione o "Número da Conta" para qual a credencial está sendo vinculada



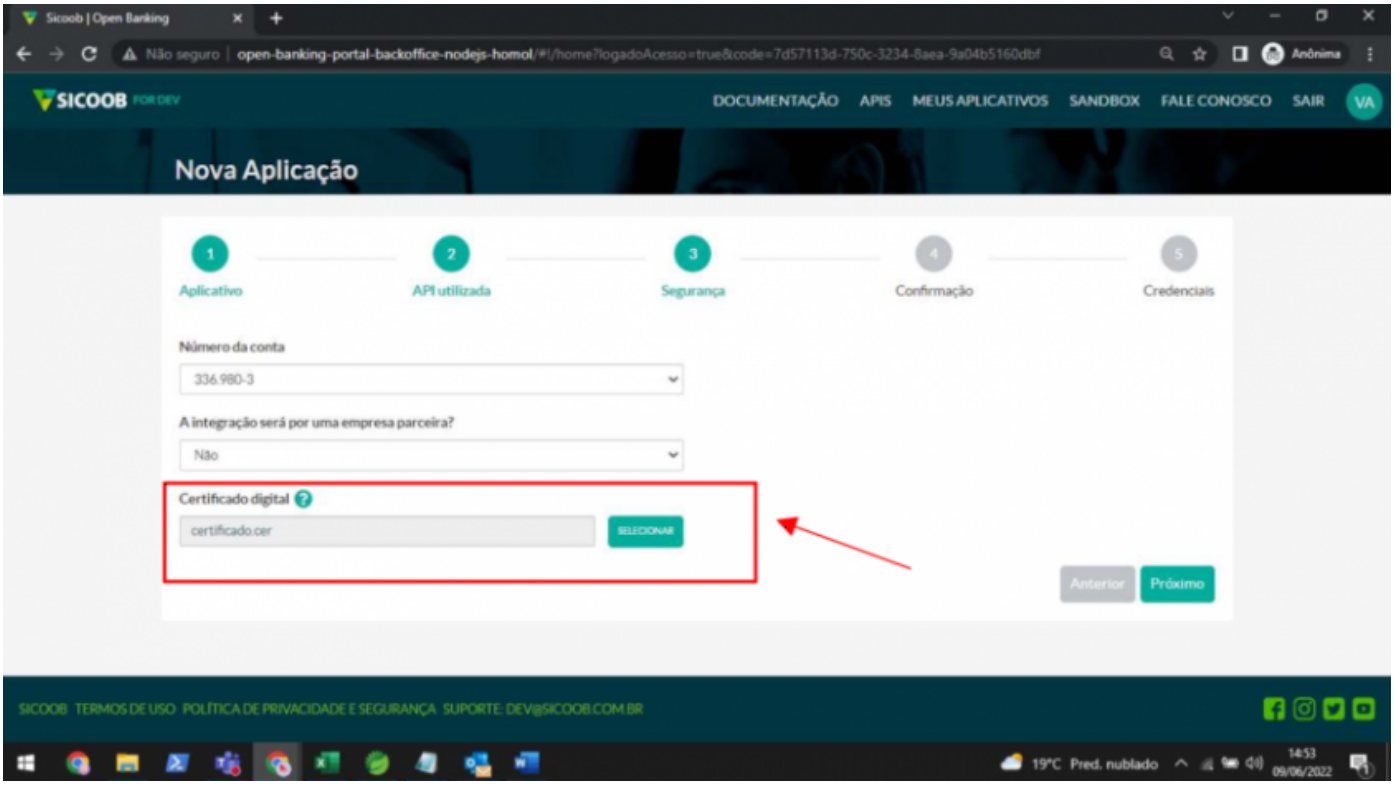
1.8 - Opção "A integração será por uma empresa parceira?" marcada como **NÃO**



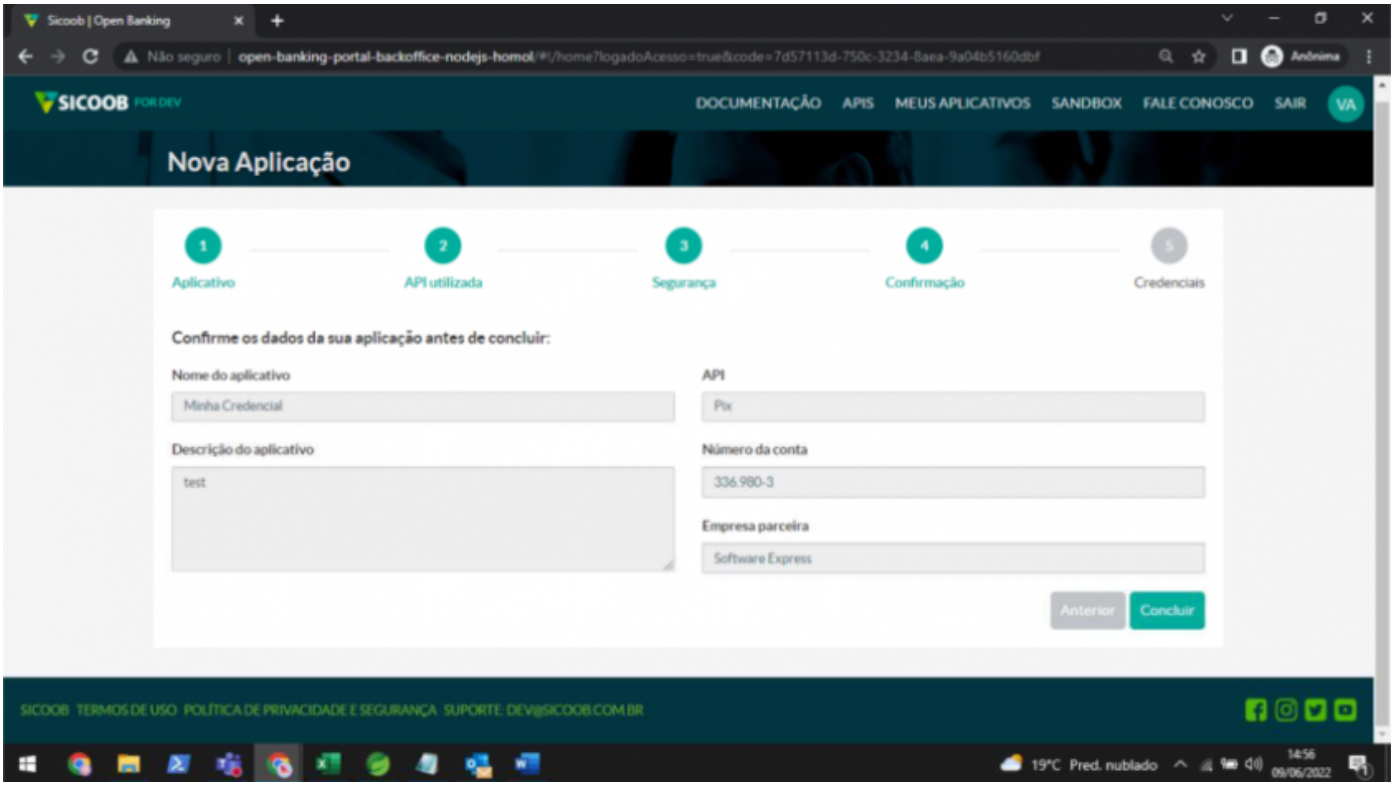
1.9 - Selecione um certificado A1 válido em formado .PEM

O certificado deve ser emitido para o CNPJ do cedente e deve estar em formato .PEM.

Clique aqui para mais informações sobre gerar o certificado nesse formato.

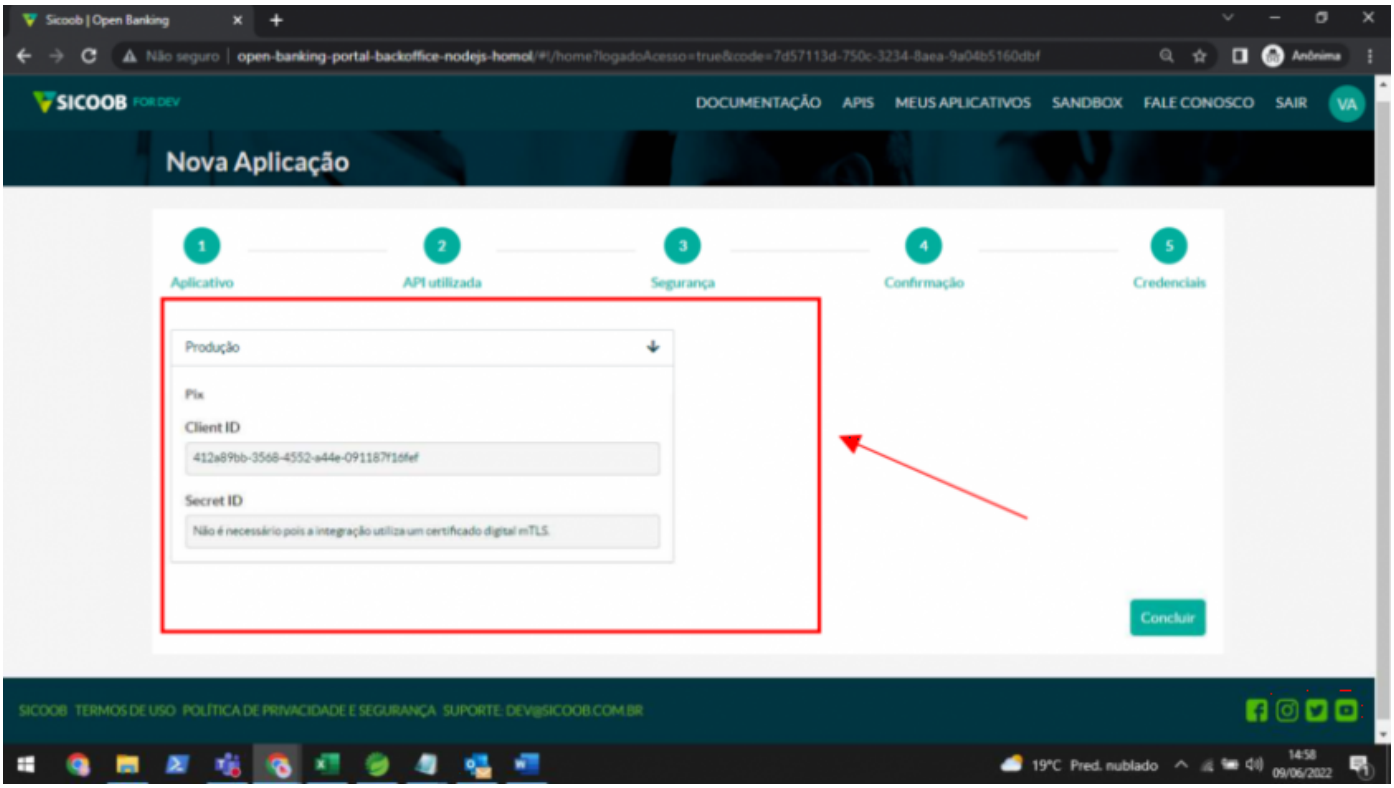


1.10 - Confirme os dados



Caso esteja tudo certo, clique em concluir, dessa forma a credencial para o WebService foi

gerado com sucesso, disponibilizando a **Client ID** que o **MsysGestor** precisa para emitir os boletos.



2 - Para a Microsys

> No MsysGestor, preencher da seguinte forma:
>
> **Certificado digital:** Realizar o upload do certificado A1 para o sistema Microsys.
>
> **Tipo webservice**: Informar **V2.2**.
>
> **API ID:** Informar com o campo **Client - ID** disponibilizado pelo banco.

Referência

https://atendimento.tecnospeed.com.br/hc/pt-br/article_attachments/10402422907799/Open-Banking-Sicoob-_-Manual-para-Credenciais-

API.pdf

https://atendimento.tecnospeed.com.br/hc/pt-br/articles/104023541034 47-Utilizando-o-registro-via-Web-Service-com-o-Sicoob-V2-

Dicas preenchimento convênio - Sicoob

As informações abaixo são dicas para auxiliar o cadastro dos dados bancários, é de suma importância que todo e qualquer dado seja confirmado com o banco.

Cadastro de conta corrente

Campo	**Dica**
Tipo	Informar o **tipo** da conta. **Pode ser "Conta corrente" ou "Conta poupança".**
Banco	Informar o código do banco de acordo com a FEBRABAN. **Para Sicoob deverá ser o código 756.**
Número da conta	Informar o **número da conta.** campo composto por **até 7 dígitos + DV da conta**. Exemplo: **1234567-8**
Agência	Informar a **agência** mantenedora da conta. Este campo é composto por **4 dígitos + DV da agência**. Exemplo: **1234-5**
Código beneficiário	Informar o **código do beneficiário com o DV** conforme informado pelo banco. Exemplo: **123456**

Cadastro de convênio

Campo	**Dica**
CNAB	Layout adotado pelo banco. **Pode ser "240" ou "400"**
Número	Neste campo pode ser informado o **código do beneficiário com o DV.** Exemplo: **1234567**
Descrição	Campo de texto para controle interno e identificação do convênio.
Número da carteira	Informar o **Número da carteira** de acordo com o repassado pelo banco. Pode ser: **1**- Simples Com Registro **3**- Garantia Caucionada
Código Carteira	Campo opcional, preencher em caso de exigência bancária.
Número contrato	Campo opcional, preencher em caso de exigência bancária. **Normalmente o valor preenchido no Número de Contrato é o mesmo informado no Código do beneficiário.**
N° remessa reinicia diariamente	Para Sicoob, está opção **pode** ser marcada como "**True**".
Número da remessa	Caso a opção "**N° remessa reinicia diariamente**" for "**Não**", deve ser informado o número da remessa atual.
Tipo webservice	Para Sicoob, marcar a opção **V2.2**

Referência

https://atendimento.tecnospeed.com.br/hc/pt-br/articles/360015260973-Sicoob

Converter certificado para .PEM

A API do Sicoob utiliza o certificado digital para autenticar as informações, porém o certificado digital utilizado pelo Sicoob é feito somente com a chave publica.

O certificado A1 utilizado para emissão de NF-es, contém tanto a chave publica como a chave privada, que em hipótese alguma deve ser compartilhada. Por isso que deve-se converter o certificado existente em um novo certificado em formato **.PEM,** o qual vai conter somente a chave publica.

Requisitos

1. OpenSLL - Precisamos dele para rodar alguns comandos.
2. GitBash - Terminal utilizado para escrever os comandos.

1 - Extração da chave publica do certificado A1

Caso o usuário tenha o certificado A1 na máquina:

1. crie uma nova pasta e copie o certificado dentro.
2. Abra o **GitBash** nesta pasta
3. Rode o seguinte comando:

```
openssl pkcs12 -in 'caminhodocertificadoarquivo.pfx' -nokeys -out 'caminhodocertificadocertificatename
```

> Lembre de alterar as seguintes informações:
> **caminhodocertificadoarquivo:** Inclua o caminho completo com o nome e a extensão .pfx do certificado A1. Exemplo: 'C:\certificado\NomeDoCertificado.pfx'.
> **caminhodocertificadocertificatename:** Inclua o caminho completo com o nome e a extensão .pem de onde será salvo o novo certificado. Exemplo: 'C:\certificado\NomeDoNovoCertificado.pem'

2 - Verifique se a chave pública foi vinculada corretamente

Antes de enviar o novo certificado **.pem** na API do Sicoob, abra o certificado em um editor de texto de sua preferência.

O conteúdo do certificado deve ser apenas assim:

```
-----BEGIN CERTIFICATE-----MIIHPjCCBSagAwIBAgIIaEshCShhC1wwDQYJKoZIhv...-----END CERTIFICATE-----
```

Com um conteúdo iniciado com "BEGIN CERTIFICATE" e finalizado com "END CERTIFICATE".

Caso o conteúdo contenha as tags "BEGIN RSA PRIVATE KEY" e " END RSA PRIVATE KEY", quer dizer que a **chave privada** do certificado foi compartilhada junto no **.pem**.
Nesse caso o certificado **NÃO** deve ser vinculado. **Sendo necessário realizar o procedimento novamente.**

Referências

https://developers.sicoob.com.br/#!/documentacao?section=seguranca&item=certificado-digital

https://atendimento.tecnospeed.com.br/hc/pt-br/article_attachments/10402422907799/Open-Banking-Sicoob-_-Manual-para-Credenciais-API.pdf