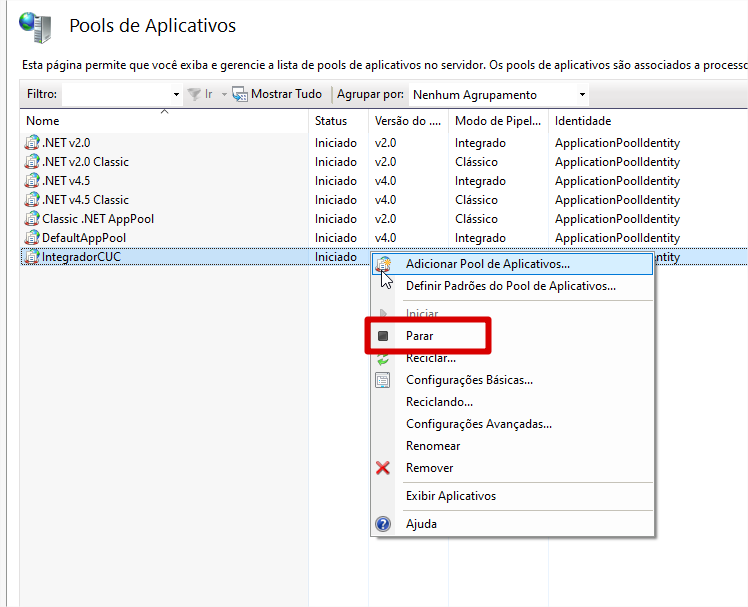
**Atualização do pacote IntegradorCUC**

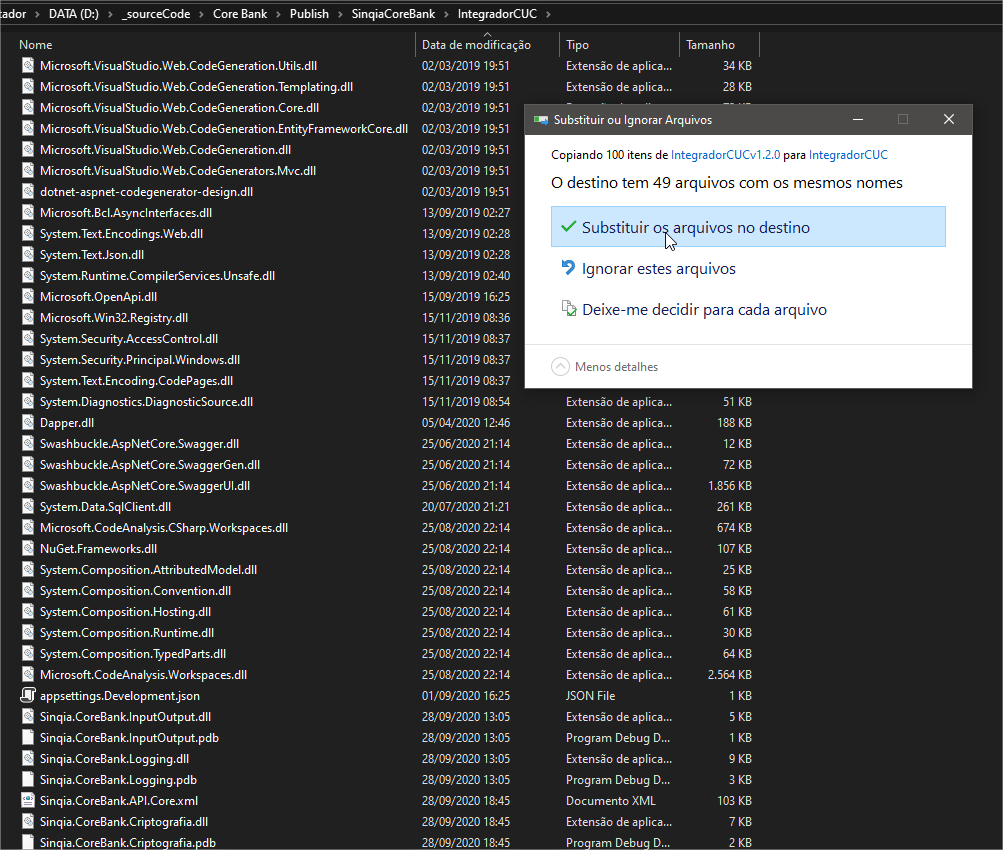
**Preparando o ambiente**

Parar os serviços no IIS para a atualização:



**Atualização dos binários**

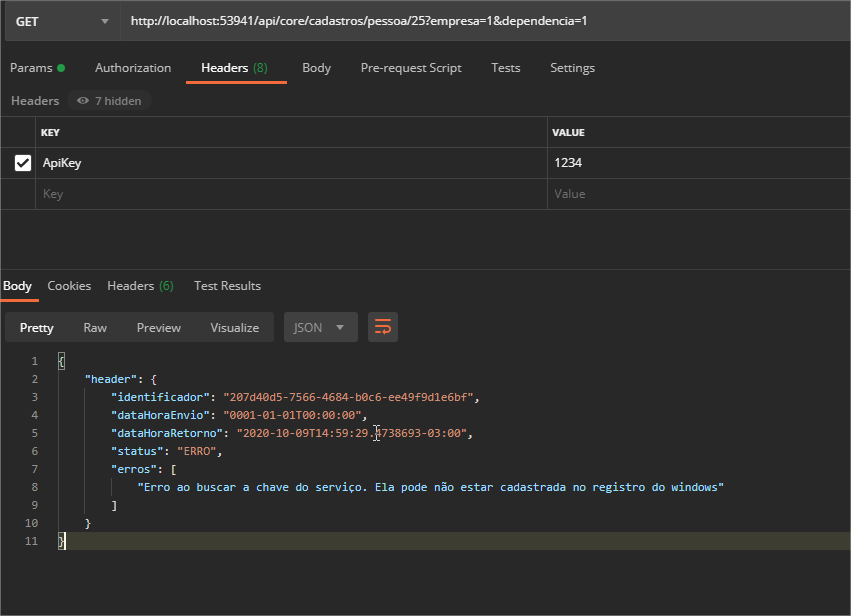
Colar os binarios do pacote na raiz do site onde está instalado a aplicação:



**Cadastro da chave de acesso**

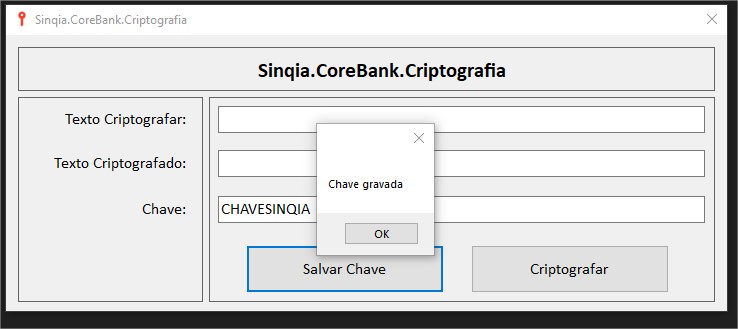
Para atualização da aplicação, ajustamos o procedimento de segurança da ferramenta para a inclusão de uma chave nas variáveis de ambiente do windows.

Caso a chave não esteja cadastrada, a mensagem abaixo será exibida:

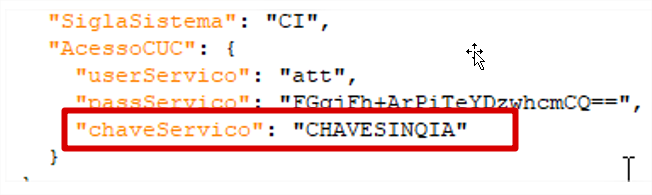


Será necessário o procedimento de armazenamento de uma chave nas variaveis de ambiente do windows a partir do utilitário de criptografia (Sinqia.CoreBank.Criptografia.exe) localizado na pasta [raiz do integrador]/ComponenteCriptografia (**abrir como administrador**):

Inserir a chave no campo “Chave” e clicar no botão “Salvar Chave”:



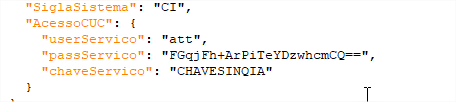
Obs.: Para facilitar, salvar a mesma chave utilizada para criptografia da senha de acesso ao CUC (apresentada na tag AcessoCUC => chaveServico), para o exemplo abaixo usei CHAVESINQIA como padrão (a mesma chave que foi feito a criptografia do campo “passServico”).



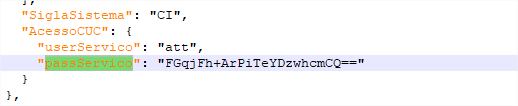
Caso queira mudar a chave, será necessário criptografar o valor do campo AcessoCUC => chaveServico novamente com a nova chave para funcionamento das integrações com o CUC.

A chave será gravada nas variáveis de sistema do windows para uso da aplicação, nesse caso, retirar a **chaveServico** do arquivo de configuração (não será necessária):

De:



Para:



**Inclusão da string de conexão**

Com a chave inserida e salva, colocar o seguinte trecho no arquivo appsettings.json:

*"ConfiguracaoBaseDataBase": {*

*"BancoUtilizado": "SQLSERVER",*

*"ConnectionStrings": [*

*{*

*"Banco": "SQLSERVER",*

*"Conexao": ""*

*}*

*]*

*},*

Na posição abaixo:



No aplicativo de criptografia, criptografar a string de conexão no formato:

**Data Source=[SERVIDOR]; User=[USUARIO]; Password=[SENHA];Initial Catalog=[DATABASE]**

Onde:

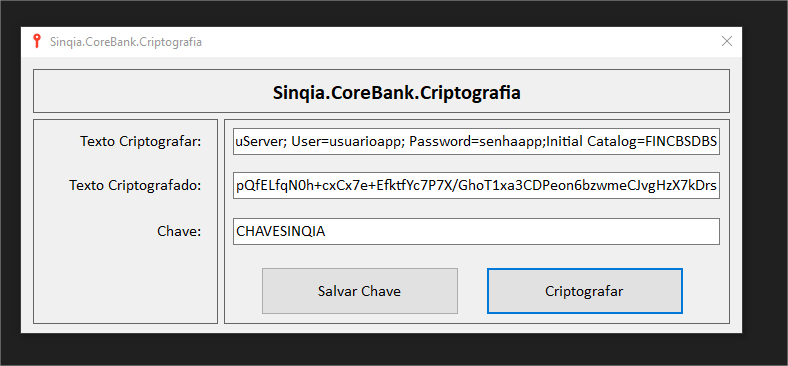
SERVIDOR = Servidor onde está localizado o banco de dados

USUARIO = Usuário do banco de dados definido para a aplicação.

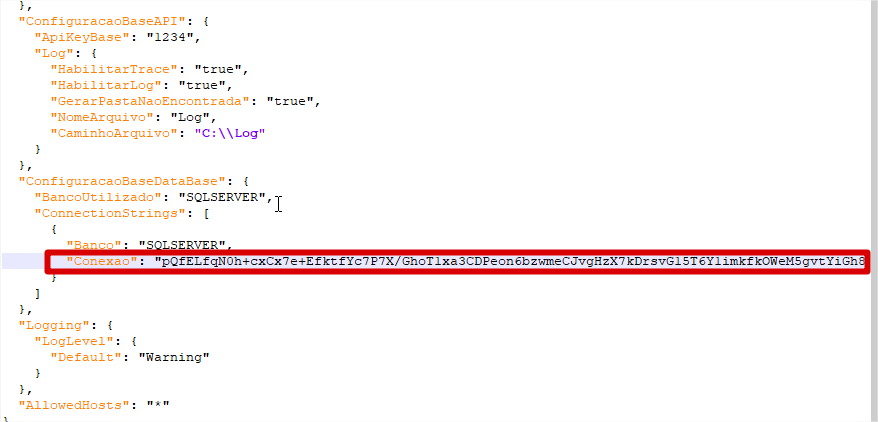
SENHA = Senha do usuário

DATABASE = Banco de dados criado para o uso da aplicação

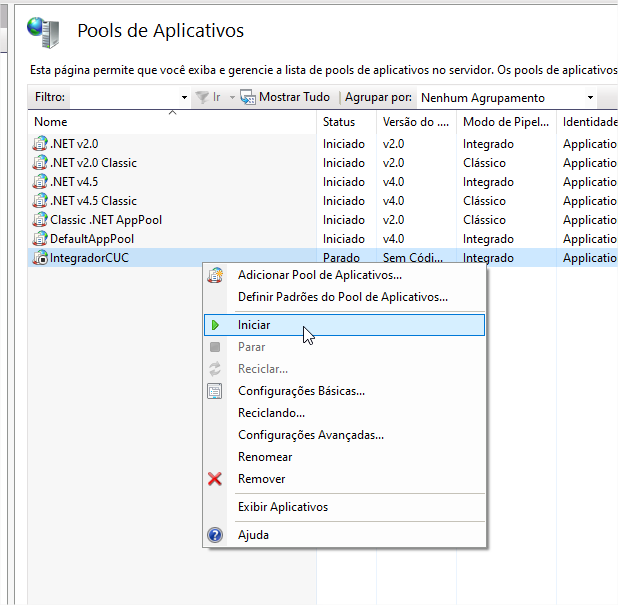
Inserir no campo texto Criptografar e clicar em criptografar para gerar a string de conexão criptografada:



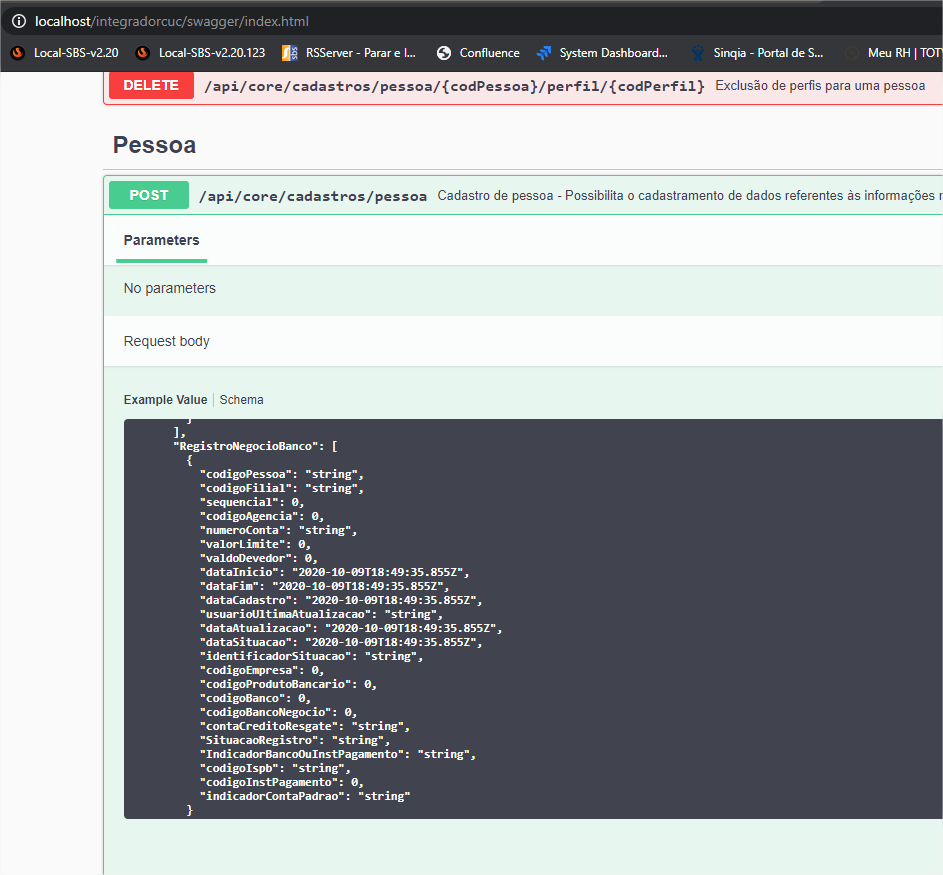
Inserir o resultado no campo " ConnectionStrings => Conexao" do appsettings.json:



Iniciar os serviços IIS novamente:



Verificar no swagger se a alteração ocorreu com sucesso abrindo a ferramenta:



Após o procedimento efetuar um teste numa chamada para ver se não houve impactos:

