

## Novas Características de Segurança

---

---

*Para segurança de seu ambiente, consulte sempre o documento Guia de Implementação SiTef PCI que pode ser encontrado na pasta de instalação do SiTef ou no link <https://www.softwareexpress.com.br/distri/aplicativos/GuiaImplementacaoSiTefPCI.zip>. Ele contém as orientações de configurações do seu servidor SiTef para atender as regras do PCI PA-DSS.*

## Sumário

<b>1. INTRODUÇÃO .....</b>	<b>3</b>
<b>2. ESCOPO .....</b>	<b>3</b>
<b>3. FUNCIONAMENTO .....</b>	<b>4</b>
<b>4. ACESSO AOS CONFIGURADORES.....</b>	<b>8</b>
<b>5. VERIFICAÇÃO EM DUAS ETAPAS (OPCIONAL) .....</b>	<b>9</b>
<b>5.1 FUNCIONAMENTO .....</b>	<b>9</b>
<b>5.2 ATIVAÇÃO.....</b>	<b>9</b>
<b>5.3 INIBIÇÃO DA TELA DE OFERECIMENTO .....</b>	<b>10</b>
<b>5.4 UTILIZAÇÃO .....</b>	<b>11</b>
<b>5.5 RESET .....</b>	<b>11</b>

## 1. Introdução

Este documento descreve as novas características de configuração do SiTef que visam melhorar a segurança e a rastreabilidade das alterações realizadas nos ambientes SiTef.

## 2. Escopo

Neste primeiro momento o novo mecanismo de segurança está previsto em alguns módulos, sendo estendido posteriormente aos demais módulos do SiTef.

Nesta primeira fase estão contemplados por este novo mecanismo de segurança os seguintes dados:

- Código de Estabelecimento
- Roteamento Multibandeira

Estes controles serão também estendidos posteriormente para outros dados.

### 3. Funcionamento

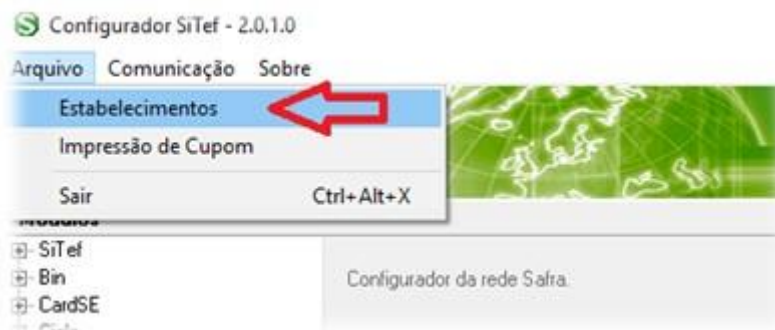
Foram criados controles para detectar que uma informação foi alterada sem a utilização do configurador apropriado e as transações que fazem uso dessa informação não serão processadas. O terminal receberá uma mensagem genérica de erro na transação e será exibida no Controle Geral do SiTef. Bastará então o administrador do ambiente verificar e confirmar/refazer a configuração desse dado via configurador para que o sistema volte a operar normalmente.

A mensagem de erro retornada para o terminal será, na maioria das vezes, “Cartão não configurado” ou “Não existe conf.” (depende da situação), pois a empresa não realizará a abertura no SiTef.

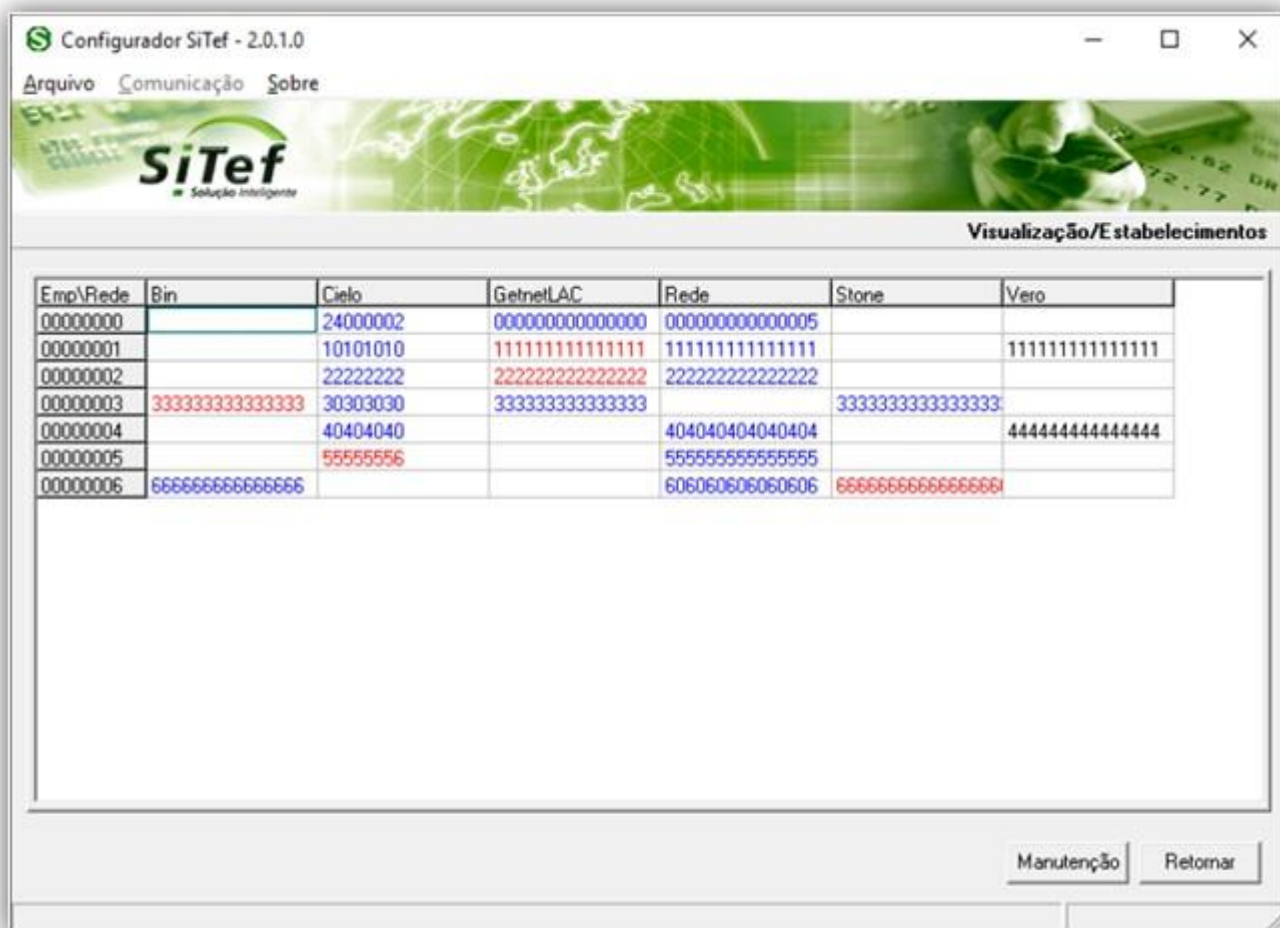
- Exemplo de alteração do código de estabelecimento por outros meios que não seja o Configurador do SiTef:  
Se a configuração de código de estabelecimento for alterada para uma determinada loja por outros meios que não seja o Configurador do SiTef as transações para a mesma serão interrompidas, onde será apresentada uma mensagem de alerta no Console do Controle Geral como na imagem abaixo:



Para ter uma visão global dos Códigos de Estabelecimentos que podem estar inválidos, deve-se acessar o Configurador do SiTef e selecionar a opção **Arquivo -> Estabelecimentos**.

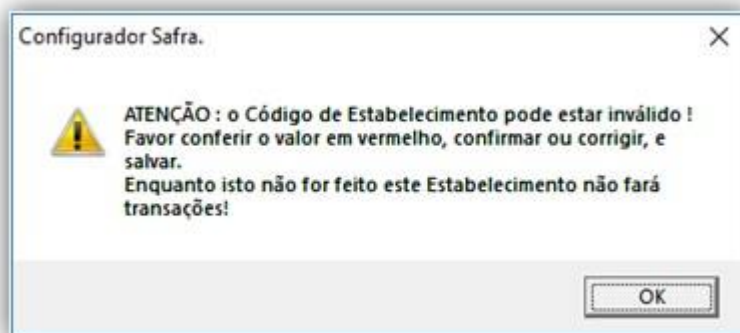


Será apresentada a tela a seguir.



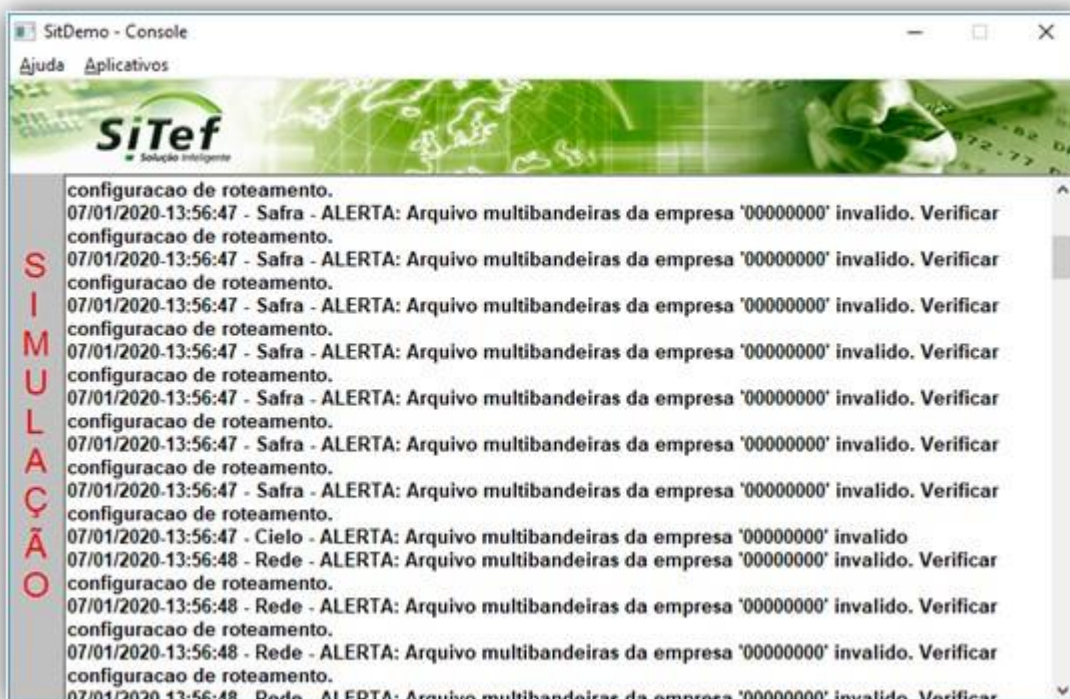
Os estabelecimentos em vermelho indicam que devem ser verificados.

Ao acessar o Configurador do SiTef e selecionar a adquirente e a empresa que foi alterado o código de estabelecimento será apresentado a mensagem:

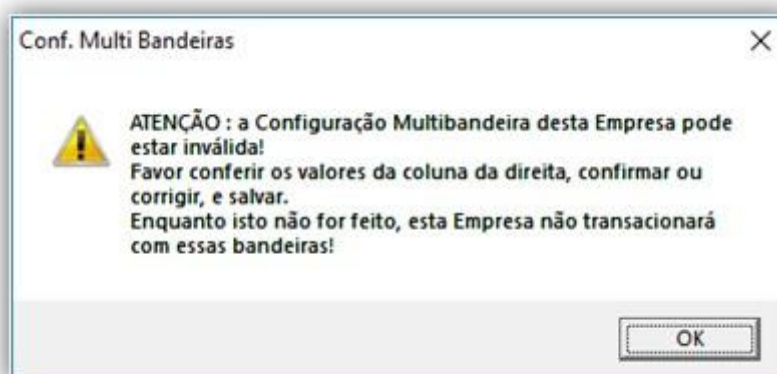


Somente após validar o código de estabelecimento, salvar a configuração e reiniciar o serviço do SiTef, as transações para esta empresa voltarão a funcionar.

- Exemplo de alteração do roteamento por outros meios que não seja o configurado MultiBandeiras:  
Se a configuração de roteamento for alterada por outros meios que não seja o Configurador Multibandeira, além da transação ser interrompida será apresentado o alerta no Console do Controle Geral.



Ao acessar o Configurador do Multibandeiras será apresentada a mensagem a seguir.

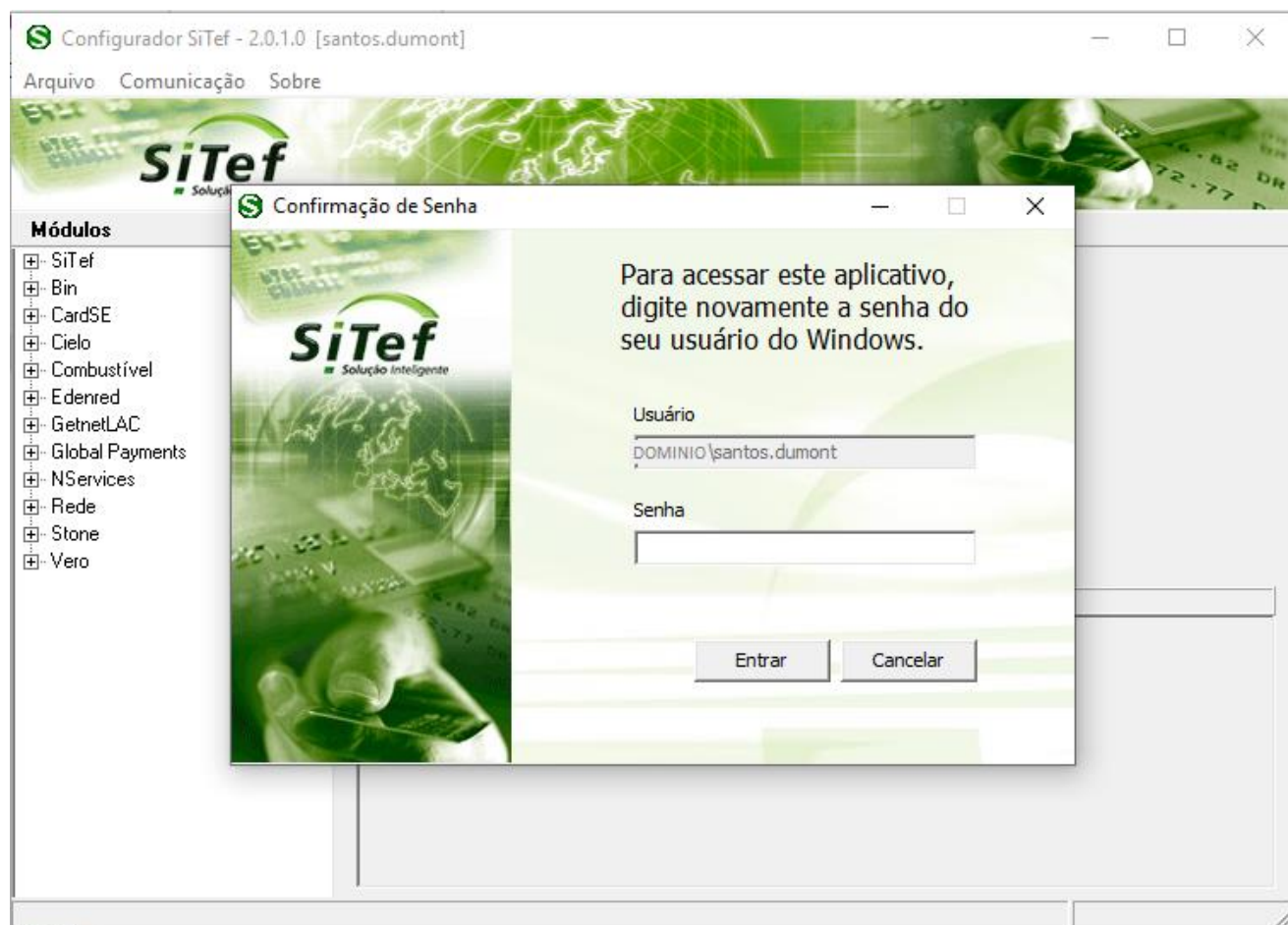


Neste caso, será necessário validar a configuração e somente após salvar e reiniciar o serviço do SiTef as transações voltaram a funcionar.



## 4. Acesso aos Configuradores

Como se sabe, o controle de acesso aos configuradores do SiTef é feito através dos usuários e grupos do Windows. No acesso ao configurador é verificado se o usuário do Windows logado na máquina tem permissão para utilizá-lo. Embora a senha do usuário tenha sido validada no momento da autenticação do usuário no login no Windows, foi incluída uma verificação adicional quando o usuário acessar os configuradores locais, solicitando novamente a senha do seu usuário do Windows:





## 5. Verificação em Duas Etapas (Opcional)

### 5.1 Funcionamento

Os Configuradores do SiTef passam a suportar também a Verificação em Duas Etapas para autenticação do usuário. Nesse tipo de autenticação, além do fornecimento da senha (primeira etapa da verificação) será solicitado também um Token que é obtido através do smartphone do usuário (segunda etapa da verificação). Este Token é gerado pelo aplicativo “Google Authenticator” e funciona como uma senha dinâmica que é mudada a cada utilização.

O processo de Verificação em Duas Etapas (também conhecido como Autenticação de Dois Fatores) tem como base a utilização de dois fatores diferentes para confirmar a autenticidade do usuário: uma informação que só ele sabe (a senha) e algo que só ele possui (o dispositivo pessoal que gera o Token).

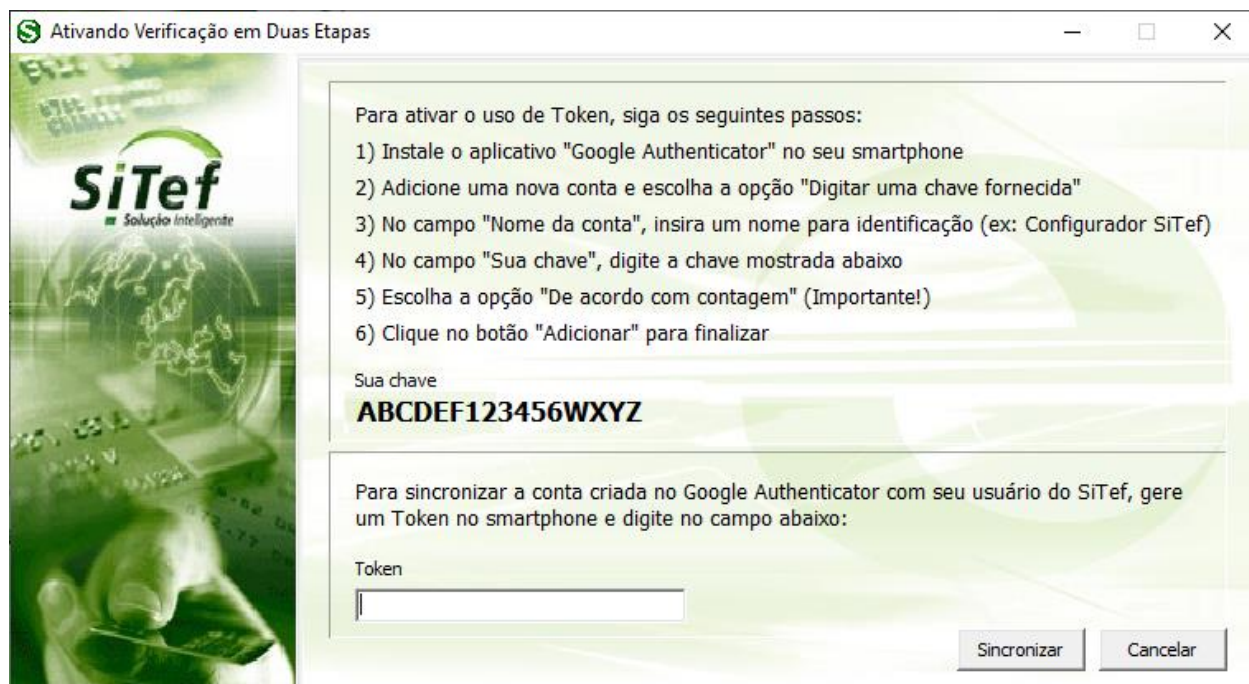
### 5.2 Ativação

Se o usuário não tiver configurado ainda a Verificação em Duas Etapas, ao fazer login será mostrada a tela abaixo oferecendo a ativação dessa segurança adicional:



Se o usuário responder que não quer ativar o uso do Token, ele poderá continuar utilizando o Configurador normalmente, e esta tela de opção continuará sendo mostrada toda vez que ele acessar o configurador novamente.

Caso ele aceite ativar a utilização do Token, será explicado ao usuário como configurar e ativar o uso do Token:



**Ativando Verificação em Duas Etapas**

Para ativar o uso de Token, siga os seguintes passos:

- 1) Instale o aplicativo "Google Authenticator" no seu smartphone
- 2) Adicione uma nova conta e escolha a opção "Digitar uma chave fornecida"
- 3) No campo "Nome da conta", insira um nome para identificação (ex: Configurador SiTef)
- 4) No campo "Sua chave", digite a chave mostrada abaixo
- 5) Escolha a opção "De acordo com contagem" (Importante!)
- 6) Clique no botão "Adicionar" para finalizar

Sua chave  
**ABCDEF123456WXYZ**

Para sincronizar a conta criada no Google Authenticator com seu usuário do SiTef, gere um Token no smartphone e digite no campo abaixo:

Token

Sincronizar Cancelar

O usuário deverá instalar em seu smartphone o aplicativo "Google Authenticator" conforme as instruções acima, gerar um Token no celular pelo aplicativo, digitá-lo no campo indicado e clicar em "Sincronizar".

#### Observações:

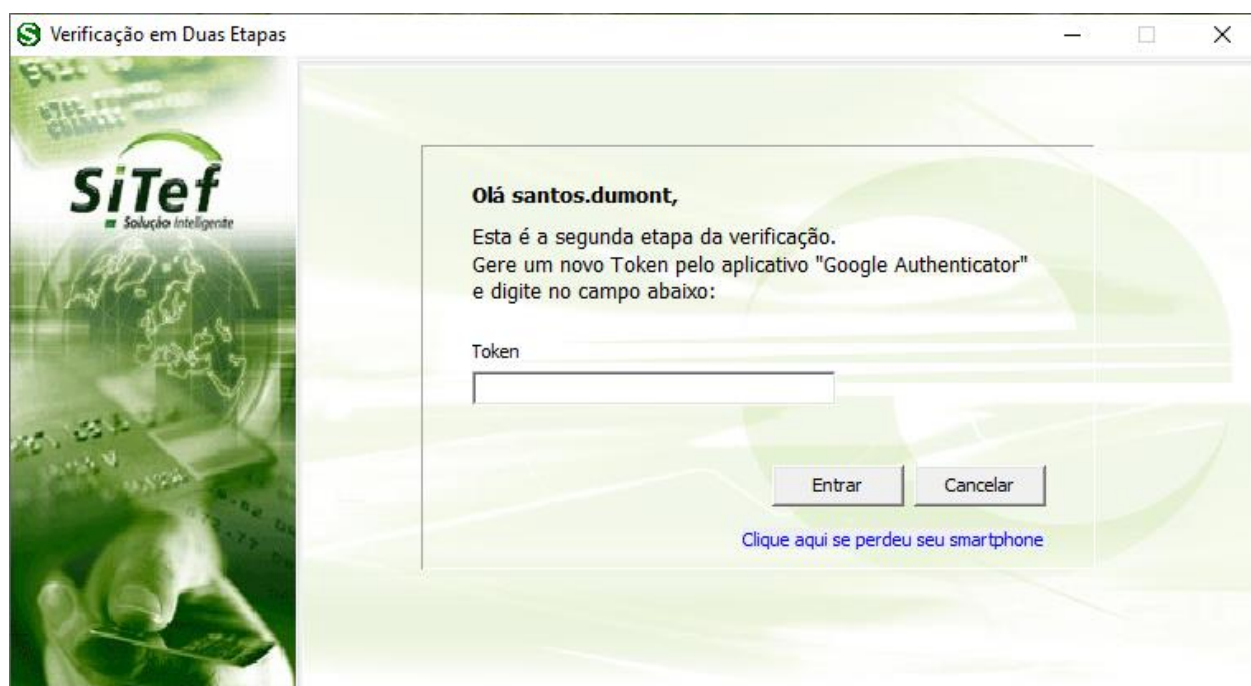
- A chave gerada pelo SiTef para ser introduzida no aplicativo "Google Authenticator" é única. A cada vez que esta tela for mostrada, será gerada uma nova chave.
- Cada usuário Administrador do SiTef deverá fazer sua própria configuração e ativação da Verificação em Duas Etapas (que terão chaves distintas), cada um com seu smartphone.
- Uma vez feita a sincronização, a chave utilizada nunca mais será mostrada, nem no SiTef nem no aplicativo do smartphone, por razões de segurança.
- Caso o usuário necessite realizar o reset do processo de verificação em duas etapas, ou seja, cadastrar uma nova conta no aplicativo "Google Authenticator" e sincronizar novamente com o SiTef, deverá entrar em contato Equipe de Suporte da Software Express e solicitar o reset do token.

### 5.3 Inibição da tela de oferecimento

Enquanto não ativar a Verificação em Duas Etapas, toda vez que acessar o configurador será oferecida a ativação. Caso não deseje mesmo utilizar essa segurança adicional e não quiser mais que essa tela fique aparecendo, é possível inibir a tela através do menu **Arquivo->Autenticação->Verificação em Duas Etapas** e desabilitar.

## 5.4 Utilização

Se tudo estiver correto, a Verificação em Duas Etapas será ativada para esse usuário e nos próximos acessos ao configurador, após a solicitação da senha, será solicitada a digitação do Token para completar o acesso:



## 5.5 Reset

Em caso de inconsistências ou perda do smartphone, será necessário resetar o Token. Para isso é necessário entrar em contato com o nosso Suporte, via e-mail: [suporte@softwareexpress.com.br](mailto:suporte@softwareexpress.com.br) ou pelo telefone (11) 3170-5353.