



CERTIFICADO DIGITAL

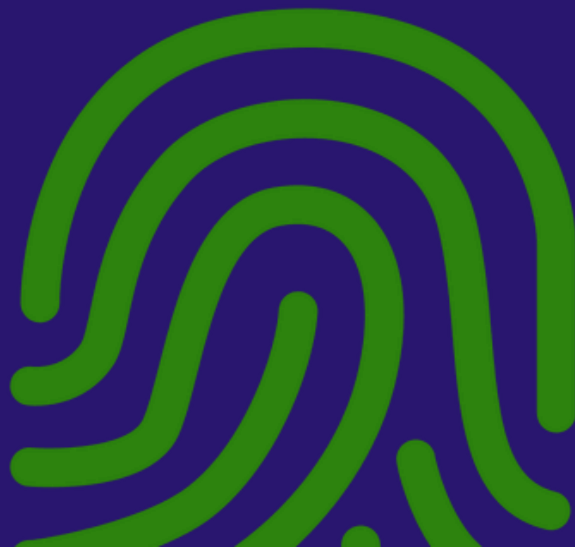
MANUAL DE EMISSÃO

Certificado Modelo A3

PARABÉNS!

Você adquiriu um Certificado Digital.

A seguir, vamos te mostrar todos os passos, divididos em três etapas, para emitir o seu certificado de forma rápida e fácil.





ETAPA 1

Preparando o seu Equipamento.

Todo o processo de emissão do seu **Certificado** é feito pelo navegador, sendo necessário apenas a instalação de alguns componentes para certificados no **Modelo A3**.

VAMOS COMEÇAR...

REQUISITOS DO SISTEMA



Vale ressaltar que a instalação da extensão será realizada **uma única vez**.

Para uma melhor experiência, sugerimos que seja utilizado um destes navegadores:

- ✓ Google Chrome
- ✓ Microsoft Edge
- ✓ Mozilla Firefox

1º PASSO

ACESSO AO PORTAL DE GERENCIAMENTO



Para acessar o Portal de Gerenciamento, você poderá clicar no botão verde, contido no e-mail que você recebeu após a validação do seu certificado, ou se preferir, [CLIQUE AQUI](#).

Pronto para iniciar a instalação do seu Certificado Digital?

Clique aqui para Emitir

Em caso de dúvidas, não deixe de entrar em contato com a Central de Atendimento da **AR SP CERTIFICADO DIGITAL DO BRASIL**:
Telefone/WhatsApp: **(11) 4862-4088**.

Nosso horário de atendimento é de segunda a sexta, das **9h00 às 17h30**.
Se preferir, também poderá entrar em contato através do nosso e-mail
vendas@spcertificadodigital.com.br



2º PASSO

IDENTIFICAÇÃO DA EXTENSÃO



Dentro do Portal de Gerenciamento, você precisará identificar se a extensão precisa ser instalada.

Se o botão *“Instalar Extensão”* estiver visível, no canto superior direito, significa que a instalação precisa acontecer. Para isso, basta clicar no botão.



3º PASSO

INICIANDO A INSTALAÇÃO DA EXTENSÃO



A partir de agora, basta seguir os passos de cada tela, começando pelo botão *"Iniciar"* .

Identificamos que você ainda não instalou a extensão SyngularID.

A extensão é necessária para **emitir** seu certificado digital com **segurança**.

Para instalar, clique no botão 'Iniciar' e siga as instruções.

[Voltar](#)

Iniciar →

4º PASSO BAIXANDO A EXTENSÃO



Ao acessar a página de instalação da extensão, clique no botão *“Usar no Chrome”*.

Em seguida, basta confirmar a instalação clicando no botão *“Adicionar Extensão”*.

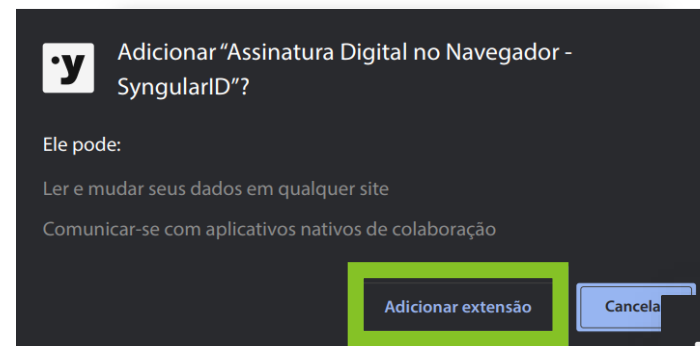
Assim que a extensão for adicionada ao navegador, feche a janela Chrome Web Store e continue a instalação.

Instalação da extensão:

1. Clique [aqui](#) para acessar a página da extensão.
2. Na aba que foi aberta, clique no botão 'Usar no Chrome':

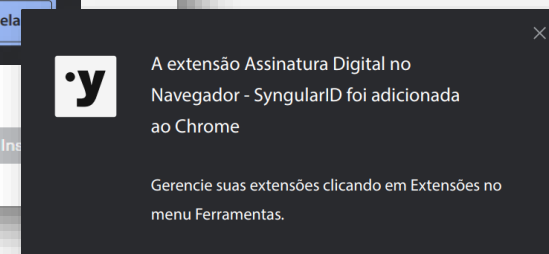


3. Confirme a instalação da extensão clicando no botão 'Adicionar extensão':



[Voltar](#)

Aguardando Ins...



5º PASSO

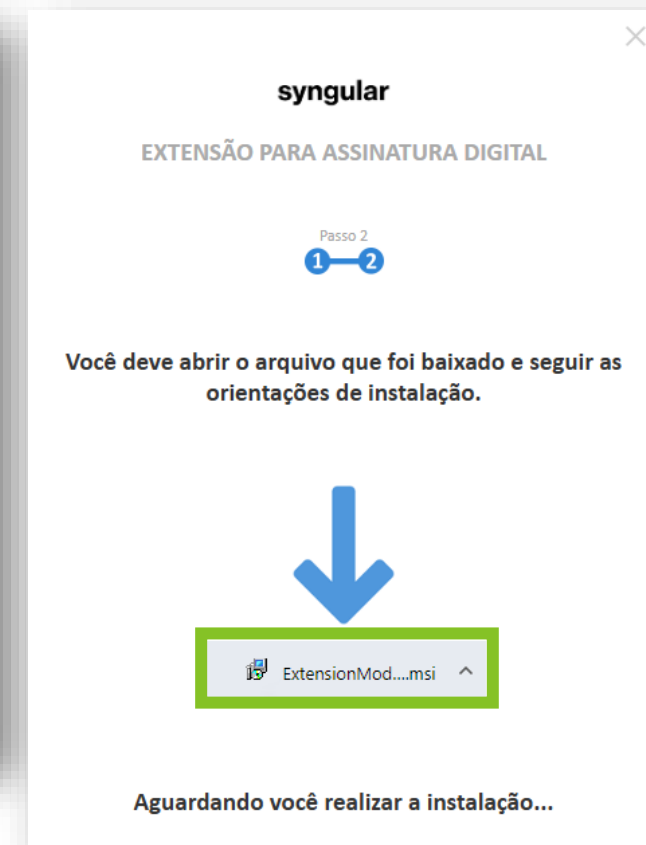
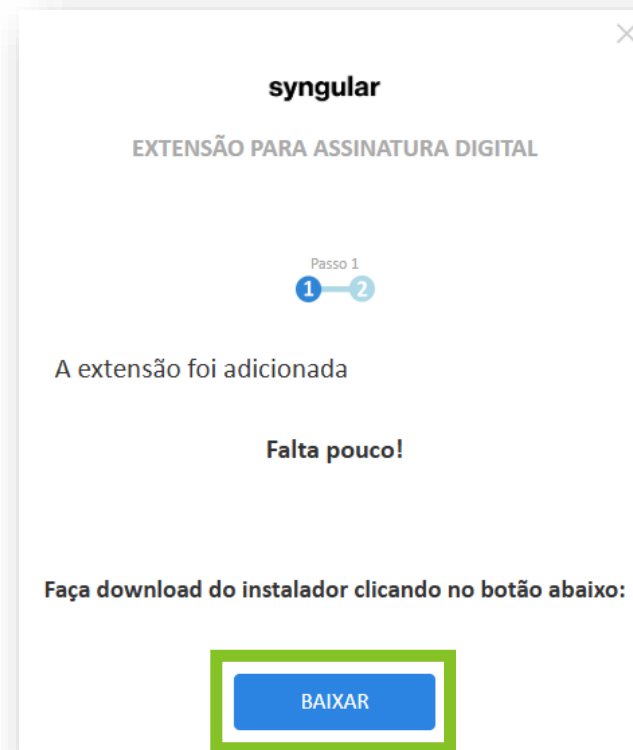
INSTALAÇÃO DO MÓDULO NATIVO



Para finalizar, é necessário instalar o Módulo Nativo.

Para isso, clique no botão "*Baixar*".

Assim que o download concluir, *execute o arquivo baixado*.



6º PASSO

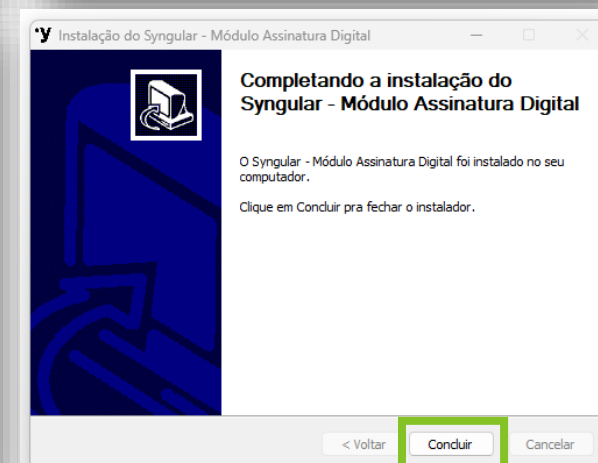
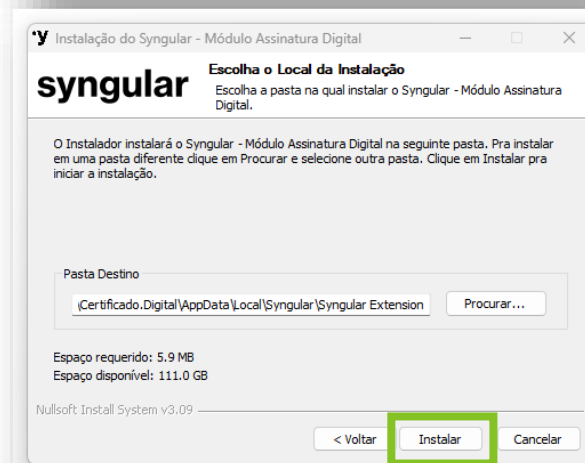
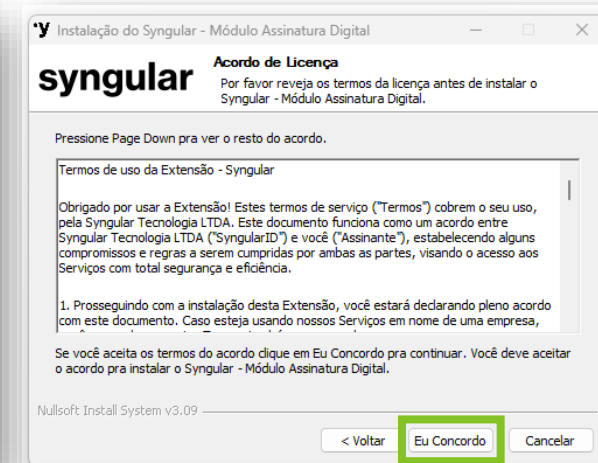
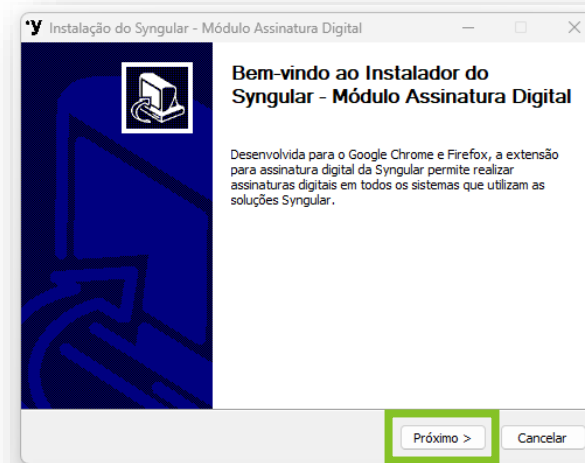
INSTALAÇÃO DO MÓDULO NATIVO



Proceda com a instalação clicando em *"Próximo"*.

Leia o acordo de licença e clique em *"Eu Concordo"*.

Em seguida, clique em *"Instalar"* e posteriormente em *"Concluir"*.



7º PASSO

CONCLUSÃO DA 1ª ETAPA



Que bom! Você chegou ao final do processo de instalação de todos os componentes necessários para emitir o seu certificado.

Clique em "*Voltar à tela Inicial*".

Tudo certo!

Todos os componentes foram instalados com sucesso!

Agora é só emitir o seu certificado digital **Syngular** :)

Voltar à tela inicial



ETAPA 2

Instalando seu Certificado.

Agora que os componentes necessários para a emissão do seu certificado foram instalados, vamos mostrar como instalar o seu **Certificado Digital**, no dispositivo adquirido.

1º PASSO

ACESSANDO O PORTAL DE GERENCIAMENTO



O Certificado Digital, no modelo A3, é emitido dentro de uma mídia criptográfica, token ou Smartcard. Conecte a mídia ao dispositivo e acesse novamente o Portal de Gerenciamento através do e-mail recebido ou, se preferir, [CLIQUE AQUI](#).

Agora, clique em *“Emitir”*, no Menu Superior ou no botão *“Emitir certificado”*, localizado no centro da tela.

Uma nova página será aberta para o preenchimento dos dados solicitados.



2º PASSO

BUSCANDO DADOS NO E-MAIL



Logo após a validação do seu Certificado, seja de forma presencial ou através da videoconferência, você recebeu um e-mail informando que o certificado está pronto para ser instalado. É o mesmo e-mail que você utilizou para acessar o Portal de Gerenciamento, no 1º passo.

Você precisa de dois dados contidos nesse e-mail: o seu *CPF* e o *Protocolo*.



Seu Certificado Digital está pronto para ser instalado!

Olá, **CLIENTE SP CERTIFICADO DIGITAL**, o seu certificado está pronto para ser emitido, ou seja, pronto para ser instalado.

DADOS DO CERTIFICADO

Solicitante: Cliente SP Certificado Digital

E-mail: cliente@spcertificado.digital

CPF: 123.456.789-10

Protocolo: 2BQ-8AM2-RWV

3º PASSO

PREENCHIMENTO DOS DADOS



Agora, digite o código do *"Protocolo"* e o número do *"CPF"* , retirados do e-mail no passo anterior.

Após digitar os dados, clique no botão *"Próximo"* .



Informe seus dados para começar.

Protocolo	2BQ-8AM2-RWV	✓
CPF	123.456.789-10	✓

[Voltar](#)

4º PASSO

AUTORIZAÇÃO DE ACESSO



Um Pop-up será aberto para que você autorize o acesso aos certificados disponíveis.

Basta clicar em *"Autorizo"* .



syngular

Pedido de Acesso

O site **emissao.spcertificadodigital.com.br** solicita acesso aos seus certificados digitais. Você autoriza?

Você pode gerenciar este acesso clicando no botão da Extensão.

Não autorizo

Autorizo

5º PASSO

RECONHECIMENTO DO DISPOSITIVO



Antes de prosseguir com os próximos dados, você precisa verificar se a mídia foi reconhecida.

Se ela estiver instalada corretamente, será identificada automaticamente no campo "*Dispositivo Token/ Smartcard*".

Caso o campo fique em branco, significa que sua mídia não está sendo reconhecida pela máquina, sendo por falta de driver ou por estar desconectada.


Selecione o dispositivo de armazenamento da mídia.

Insira seu código de emissão.

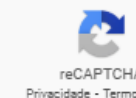
Dados da Solicitação

Tipo:	Certificado do tipo PF A3 – Videoconferência
Emitido por:	AC SyngularID Multipla
Nome:	Cliente SP Certificado Digital
CPF:	123.456.789-10
Protocolo:	2BQ-8AM2-RWV

Insira seu código aqui

* Dispositivo Token/Smartcard:
ACS CCID USB Reader 0 - G&D Sm@rtCafe 

Não sou um robô



[Voltar](#)

[Próximo](#)

6º PASSO

PREENCHIMENTO DO CÓDIGO DE EMISSÃO



Após ter selecionado o dispositivo de armazenamento, você digitará o “*Código de Emissão*”, que contém 6 caracteres.

Se você realizou a validação de *forma presencial*, o código foi entregue a você, pelo Agente de Registro, em um *documento impresso*.

No atendimento efetuado por *videoconferência*, o código foi mostrado em tela no final do procedimento. Você foi orientado pelo Agente de Registro a tirar um print da tela ou anotá-lo em um papel.

Digite o código de emissão, marque a opção “*Não sou um robô*” e clique em “*Próximo*”.


Insira seu código de emissão.

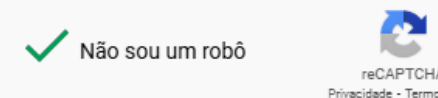
Dados da Solicitação

Tipo:	Certificado do tipo PF A3 – Videoconferência
Emitido por:	AC SyngularID Multipla
Nome:	Cliente SP Certificado Digital
CPF:	123.456.789-10
Protocolo:	2BQ-8AM2-RWV

Insira seu código aqui

F 9 7 6 E A

* Dispositivo Token/Smartcard:
ACS CCID USB Reader 0 - G&D Sm@rtCafe 



[Voltar](#)

[Próximo](#)

7º PASSO

CRIAÇÃO DAS CHAVES CRIPTOGRÁFICAS



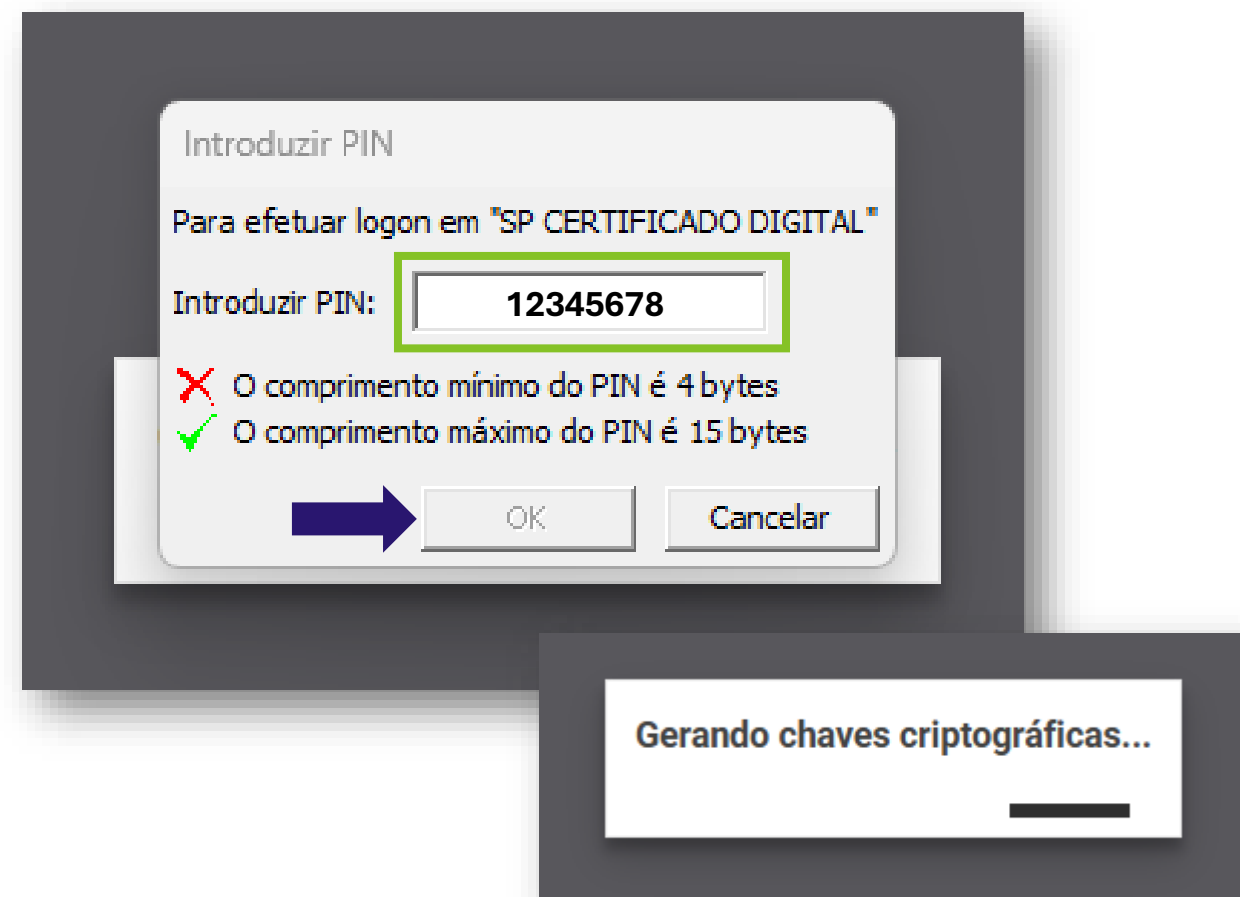
Um Pop-up será aberto para que você insira a "Senha PIN" .

A Senha PIN foi inserida em seu Smartcard antes de ser entregue a você.

Digite "12345678" e clique no botão "OK" .

Nesse momento, o sistema irá gerar as Chaves Criptográficas.

**Não deixe de alterar suas senhas ao final de todo o processo na Etapa 3!*



8º PASSO

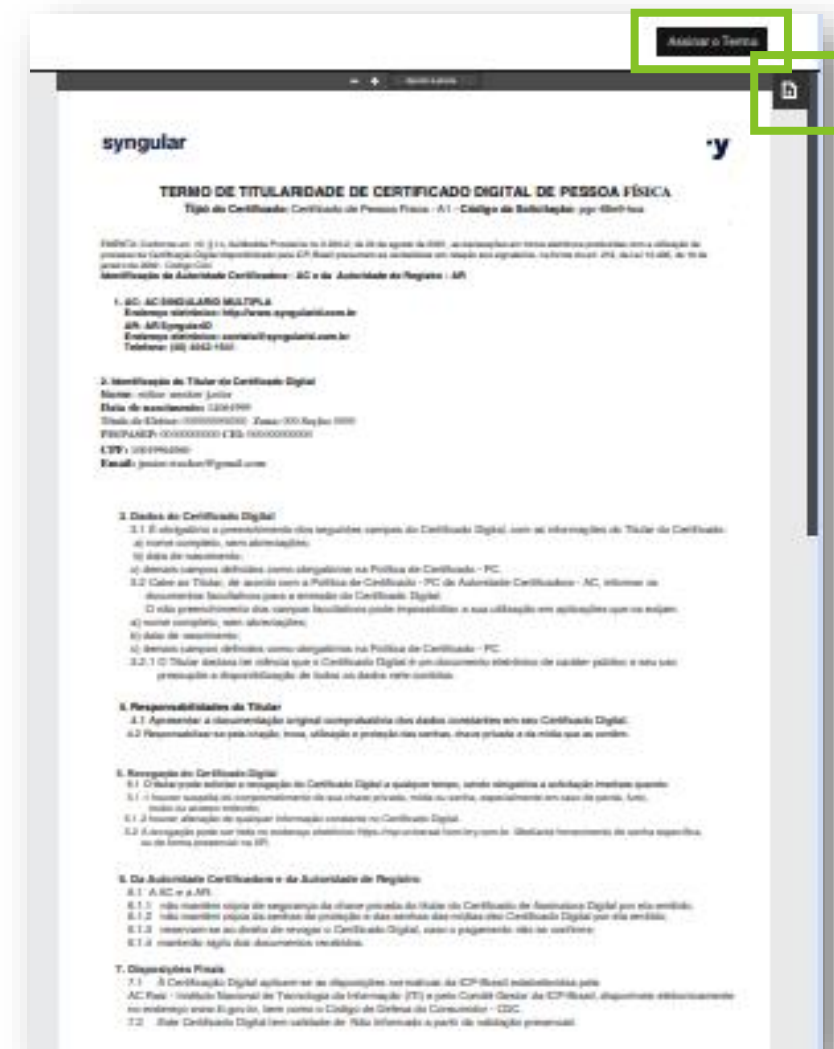
ASSINATURA DO TERMO DE TITULARIDADE



Aqui, você lerá e assinará o *Termo de Titularidade e Responsabilidade de Certificado Digital*.

Clique em *“Assinar o Termo”*, no canto superior direito e insira *Senha PIN* novamente, quando solicitada.

Você pode optar também por efetuar o download do Termo.



9º PASSO

CONFIRMAÇÃO DO DISPOSITIVO



Confirme se o dispositivo de instalação é o correto e garanta que ele fique conectado até o final do processo.

Clique no botão *"Emitir Certificado"* .

Insira a *Senha PIN*.

**E agora, o mais importante pra finalizar:
confirme o dispositivo de instalação do seu
certificado.**

Dispositivo Token/Smartcard
ACS CCID USB Reader 0 - G&D Sm@rtCafe Expert 7.0 FIPS

Atenção

- 1 Não retire o dispositivo Token/Smartcard do equipamento durante o processo de emissão do seu certificado.
- 2 Quando solicitado digite a senha do seu dispositivo Token/Smartcard para prosseguir com a emissão.

[Voltar](#)

Emitir certificado

10º PASSO

CONCLUSÃO DA 2ª ETAPA



Parabéns!

Você realizou a instalação do seu Certificado Digital no dispositivo escolhido, mas ainda não acabou!

Por questões de segurança você precisa alterar a *Senha PIN* e a *Senha PUK*.



Parabéns, SP CERTIFICADO!
Seu certificado foi emitido com sucesso.

Armazene seu token em um local seguro. Em caso de dúvidas, consulte o manual de instalação.

[Voltar à Tela Inicial](#)



ETAPA 3

Alterando as Senhas PIN e PUK.

Para garantir total segurança é fundamental que as **Senhas** do seu **Certificado Digital** sejam alteradas e guardadas em local seguro.

1º PASSO

ACESSANDO O SAFESIGN



Abra o Gerenciador do seu Certificado, *SAFESIGN* que foi instalado em seu equipamento no momento que você baixou as extensões, no início do processo.

Você identificará o seu certificado e em seguida clicará no quadro verde, no canto direito em *"Gerenciar PIN/PUK"* .



2º PASSO

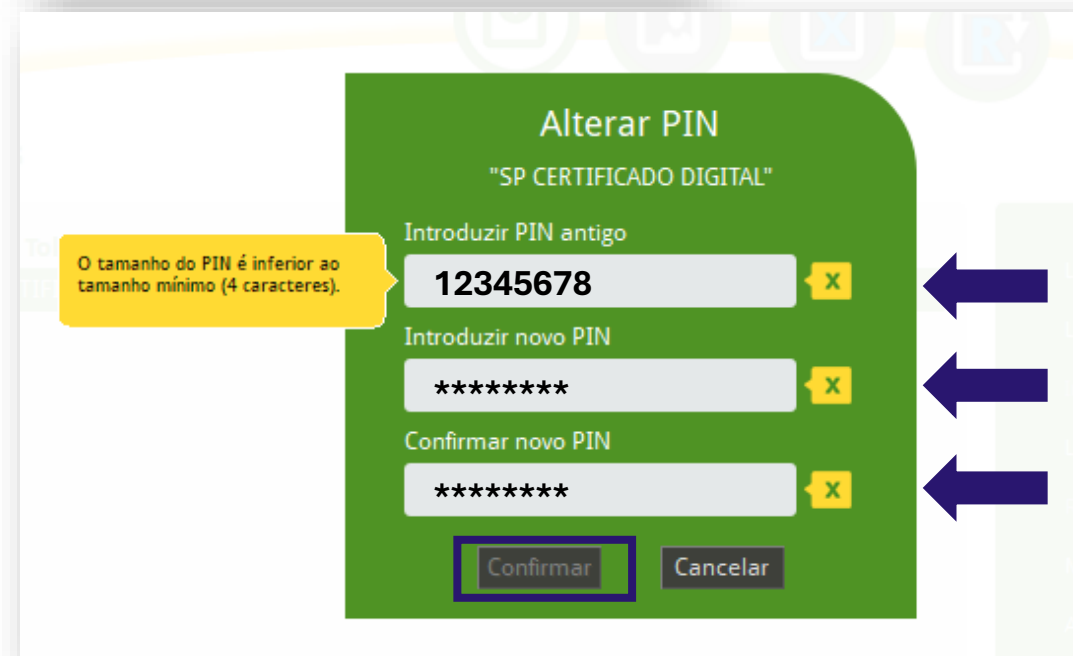
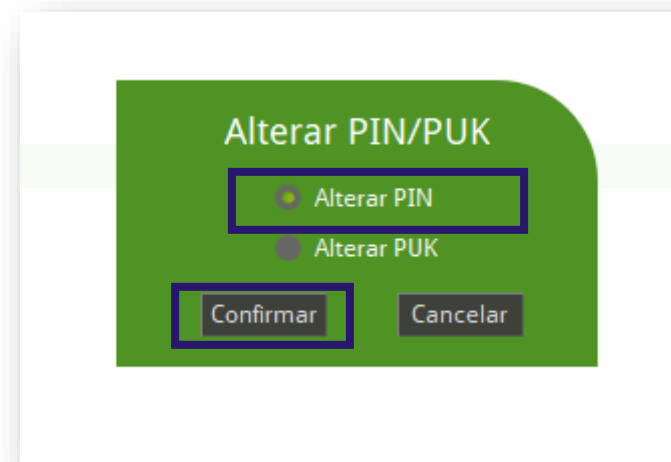
ALTERANDO A SENHA *PIN*



Selecione "*Alterar PIN*" e clique no botão "*Confirmar*".

No primeiro campo digite o *PIN* antigo "*12345678*" e em seguida, crie um *Novo PIN* com no mínimo 4 caracteres confirmando a sequência criada no terceiro campo.

Clique em "*Confirmar*".



3º PASSO

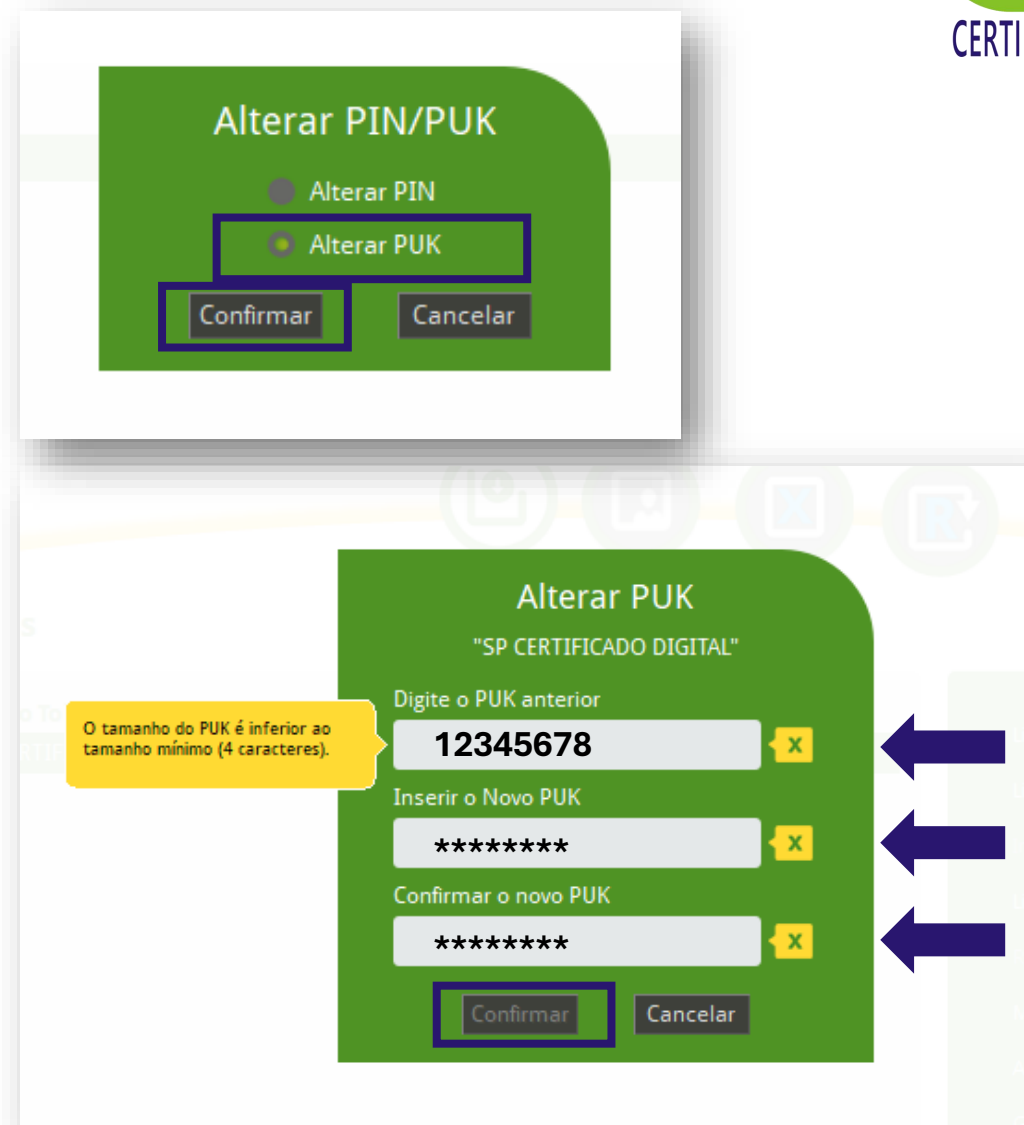
ALTERANDO A SENHA *PUK*



Agora, selecione "*Alterar PUK*" e clique no botão "*Confirmar*".

No primeiro campo digite o *PUK* antigo "*12345678*" e em seguida, crie um *Novo PUK* com no mínimo 4 caracteres confirmando a sequência criada no terceiro campo.

Clique em "*Confirmar*".



The image shows two screenshots of the SP CERTIFICADO DIGITAL interface. The top screenshot is titled "Alterar PIN/PUK" and has two radio buttons: "Alterar PIN" (unselected) and "Alterar PUK" (selected). Below the radio buttons are two buttons: "Confirmar" and "Cancelar". The bottom screenshot is titled "Alterar PUK" and has the subtitle "SP CERTIFICADO DIGITAL". It contains three input fields: "Digite o PUK anterior" with the value "12345678", "Inserir o Novo PUK" with "*****", and "Confirmar o novo PUK" with "*****". A yellow callout box points to the first field with the text "O tamanho do PUK é inferior ao tamanho mínimo (4 caracteres)". At the bottom are "Confirmar" and "Cancelar" buttons. Three blue arrows on the right point to the input fields.

AGORA SIM, TUDO PRONTO!

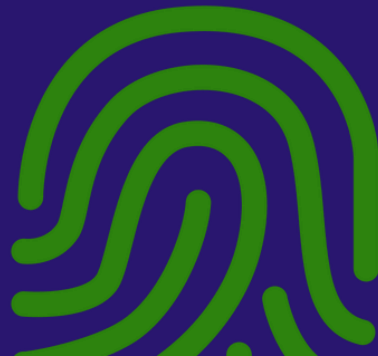
Mas atenção às orientações abaixo:

Anote e guarde suas senhas em local seguro.

As senhas **PIN** e **PUK** são **personais, intransferíveis e de responsabilidade do titular** ou do responsável pelo certificado digital.

Não existem cópias ou meios para recuperá-las, por isso, caso o dispositivo criptográfico seja bloqueado devido à perda ou ao uso incorreto das senhas, **o dispositivo será bloqueado** e o certificado perdido.

Dessa forma, caberá ao titular realizar uma nova aquisição, pois o uso incorreto das senhas não está previsto na política de garantia da **SP CERTIFICADO DIGITAL**.





AINDA POSSUI DÚVIDAS?
Entre em contato com
nosso time.



(11) 4862-4088

**AGRADECEMOS A
PREFERÊNCIA**

