Apurador da Votação

Este manual apresenta as etapas de um processo de votação que são realizadas pelo 'Apurador'.

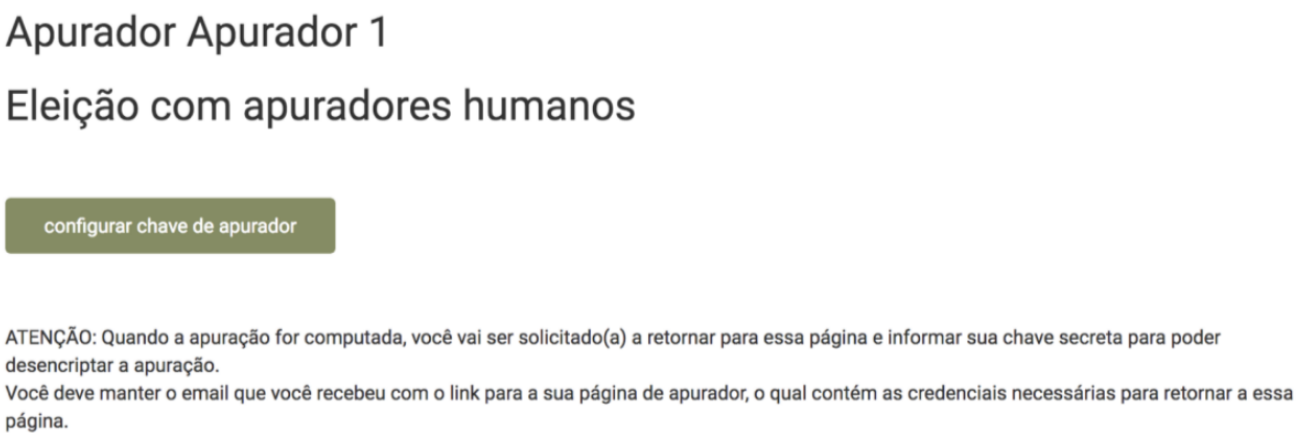
Geração da Chave de Apuração

Ao ser designada como um Apurador, a pessoa receberá um e-mail do Sistema de Votação Helios com as instruções e um link para que essa possa gerar ou carregar sua chave privada. A pessoa deve obrigatoriamente entrar no link que está no e-mail para que possa carregar suas informações de apurador.

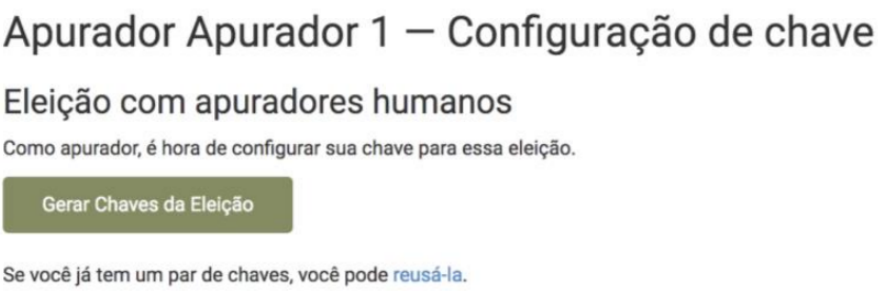
ATENÇÃO:

- O apurador deve manter esse e-mail, pois a URL contida nele deverá ser usada novamente para que se possa apurar a eleição.
- Utilize o navegador de internet Firefox para realizar este processo. Alguns navegadores não abrem a janela popup com a chave gerada.

Após clicar no link que recebeu por e-mail, clique no botão **configurar chave de apurador**.

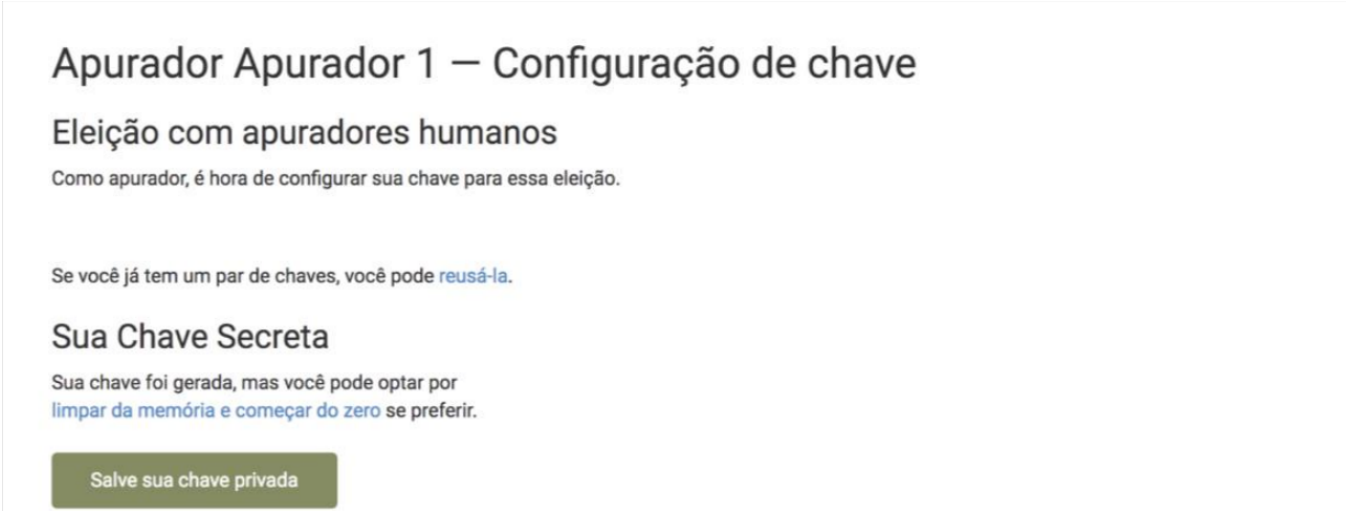


Clique no botão **Gerar Chaves da Eleição**.

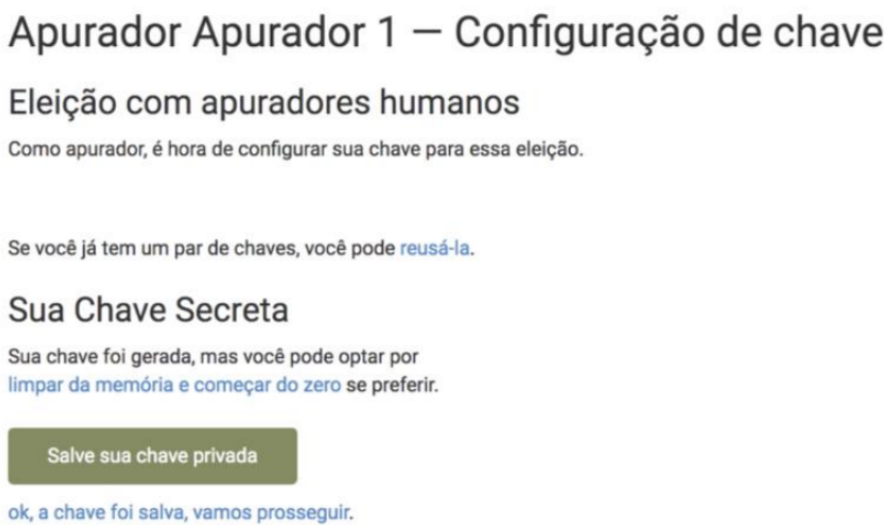


Clique no botão **Salve sua chave privada**. Será aberta uma nova aba no navegador com uma sequência numérica grande. Clique no menu **arquivo** do navegador e escolha a opção **Salvar**.

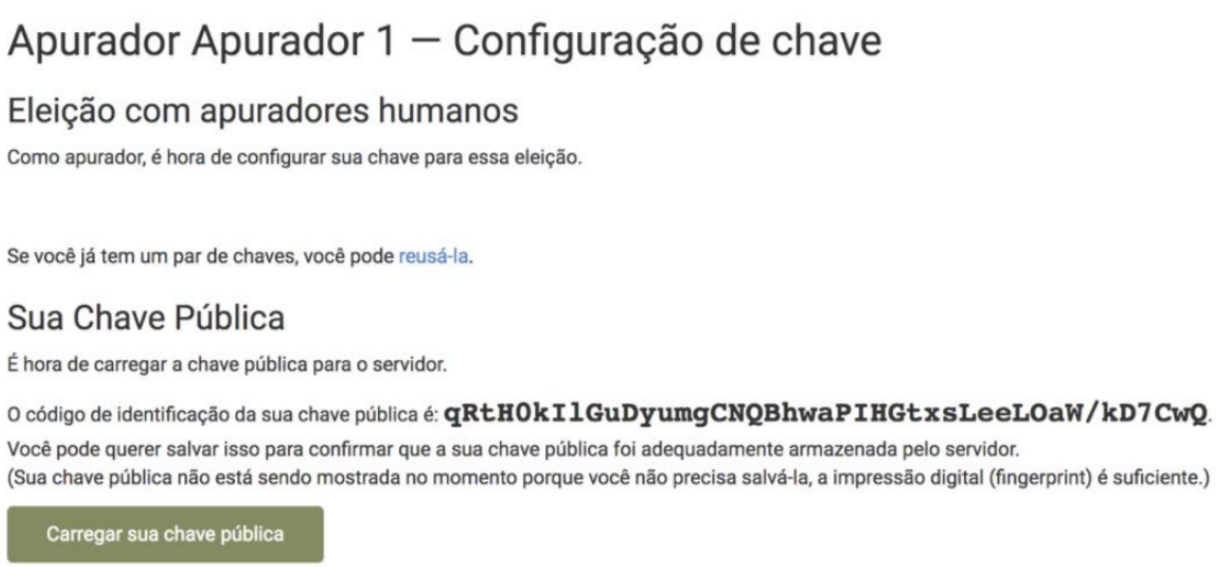
- Escolha o local e coloque o nome que desejar, mas mantenha a extensão como **.txt** (ex: `minha-chave-privada.txt`). Clique no botão salvar e feche essa janela ou aba.
- **ATENÇÃO CRÍTICA:** SALVE ESSE ARQUIVO EM UM LOCAL SEGURO. **SEM A CHAVE DE APURAÇÃO É IMPOSSÍVEL COMPUTAR O RESULTADO DE UMA VOTAÇÃO**.



Clique no link **ok, a chave foi salva, vamos prosseguir**.



Por fim, clique no botão **Carregar sua chave pública**.

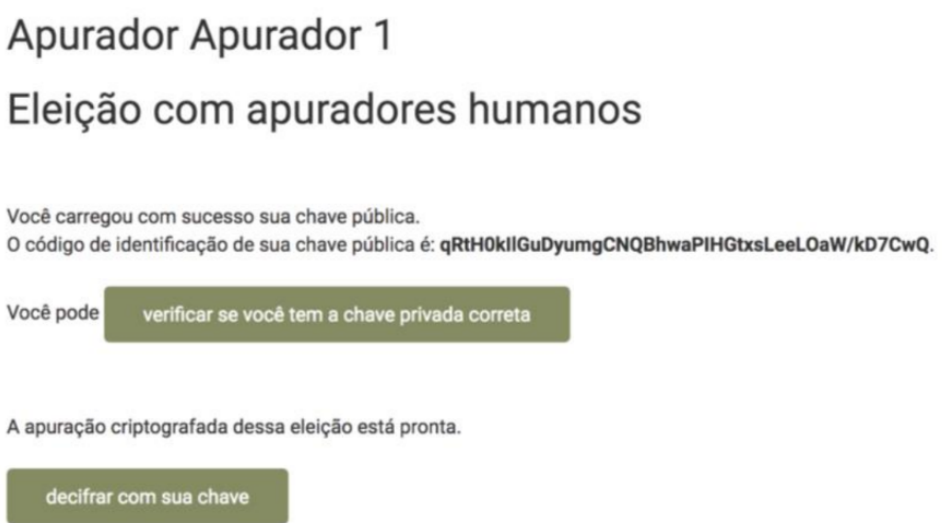


Parabéns, você carregou a chave com sucesso! Se desejar, você pode fazer um teste a fim de verificar se possui a chave privada correta, basta clicar no botão **verificar se você tem a chave privada correta**. Esse passo é opcional.

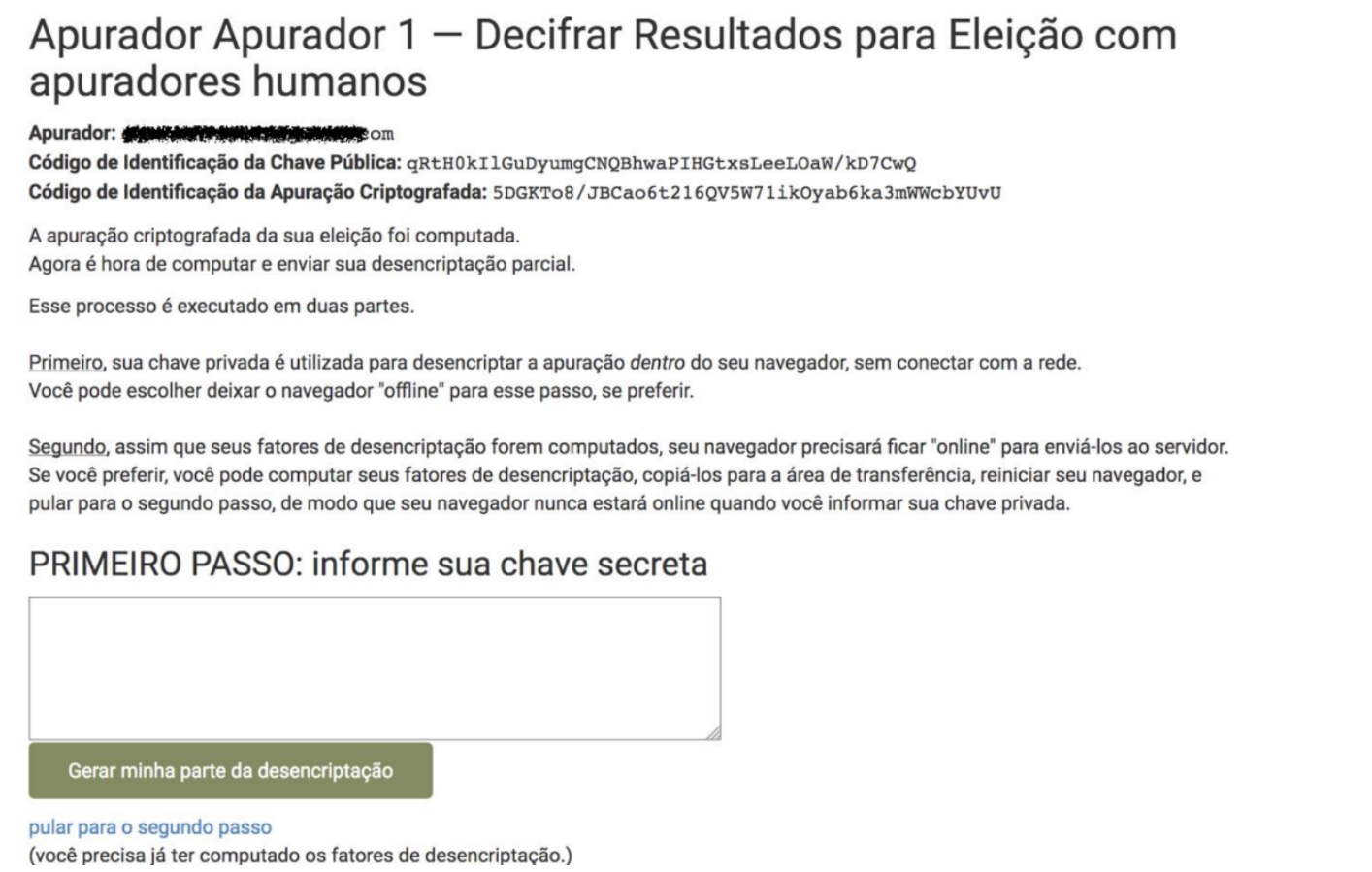
Decifrar Resultado da Eleição com a Chave de Apuração

Quando uma eleição possui apuradores humanos, é necessário que estes forneçam suas chaves no momento de apuração para que o resultado seja computado. Para isto, abra o e-mail que recebeu quando foi designado como apurador e clique no endereço link contido neste.

Clique no **botão decifrar com sua chave**.



Abra o arquivo onde você salvou sua chave criptográfica (usando por exemplo o aplicativo bloco de notas), copie toda a sequência de caracteres e cole na área de texto em branco da figura abaixo.



Apurador Apurador 1 — Decifrar Resultados para Eleição com apuradores humanos

Apurador: [redacted]om
Código de Identificação da Chave Pública: qRtH0kIlGuDyumgCNQBhwaPIHGtxsLeeLOaW/kD7CwQ
Código de Identificação da Apuração Criptografada: 5DGKTo8/JBCao6t216QV5W71ikOyab6ka3mWWcbYUvU

A apuração criptografada da sua eleição foi computada.
Agora é hora de computar e enviar sua desencriptação parcial.

Esse processo é executado em duas partes.

Primeiro, sua chave privada é utilizada para desencriptar a apuração *dentro* do seu navegador, sem conectar com a rede.
Você pode escolher deixar o navegador "offline" para esse passo, se preferir.

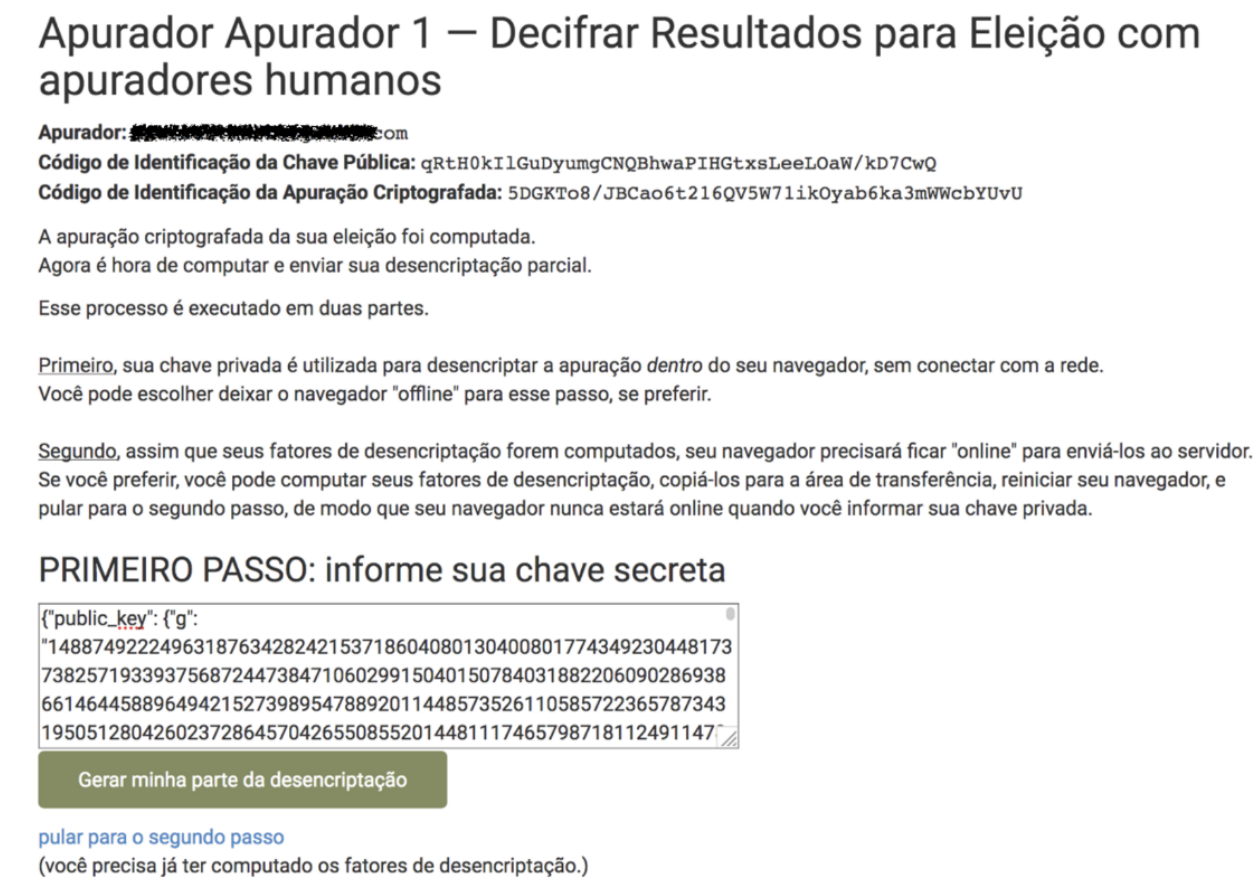
Segundo, assim que seus fatores de desencriptação forem computados, seu navegador precisará ficar "online" para enviá-los ao servidor.
Se você preferir, você pode computar seus fatores de desencriptação, copiá-los para a área de transferência, reiniciar seu navegador, e pular para o segundo passo, de modo que seu navegador nunca estará online quando você informar sua chave privada.

PRIMEIRO PASSO: informe sua chave secreta

Gerar minha parte da desencriptação

pular para o segundo passo
(você precisa já ter computado os fatores de desencriptação.)

Clique no botão **Gerar minha parte da desencriptação**.



Apurador Apurador 1 — Decifrar Resultados para Eleição com apuradores humanos

Apurador: [redacted]com
Código de Identificação da Chave Pública: qRtH0kIlGuDyumgCNQBhwaPIHGtxsLeeLOaW/kD7CwQ
Código de Identificação da Apuração Criptografada: 5DGKTo8/JBCao6t216QV5W71ikOyab6ka3mWWcbYUvU

A apuração criptografada da sua eleição foi computada.
Agora é hora de computar e enviar sua desencriptação parcial.

Esse processo é executado em duas partes.

Primeiro, sua chave privada é utilizada para desencriptar a apuração *dentro* do seu navegador, sem conectar com a rede.
Você pode escolher deixar o navegador "offline" para esse passo, se preferir.

Segundo, assim que seus fatores de desencriptação forem computados, seu navegador precisará ficar "online" para enviá-los ao servidor.
Se você preferir, você pode computar seus fatores de desencriptação, copiá-los para a área de transferência, reiniciar seu navegador, e pular para o segundo passo, de modo que seu navegador nunca estará online quando você informar sua chave privada.

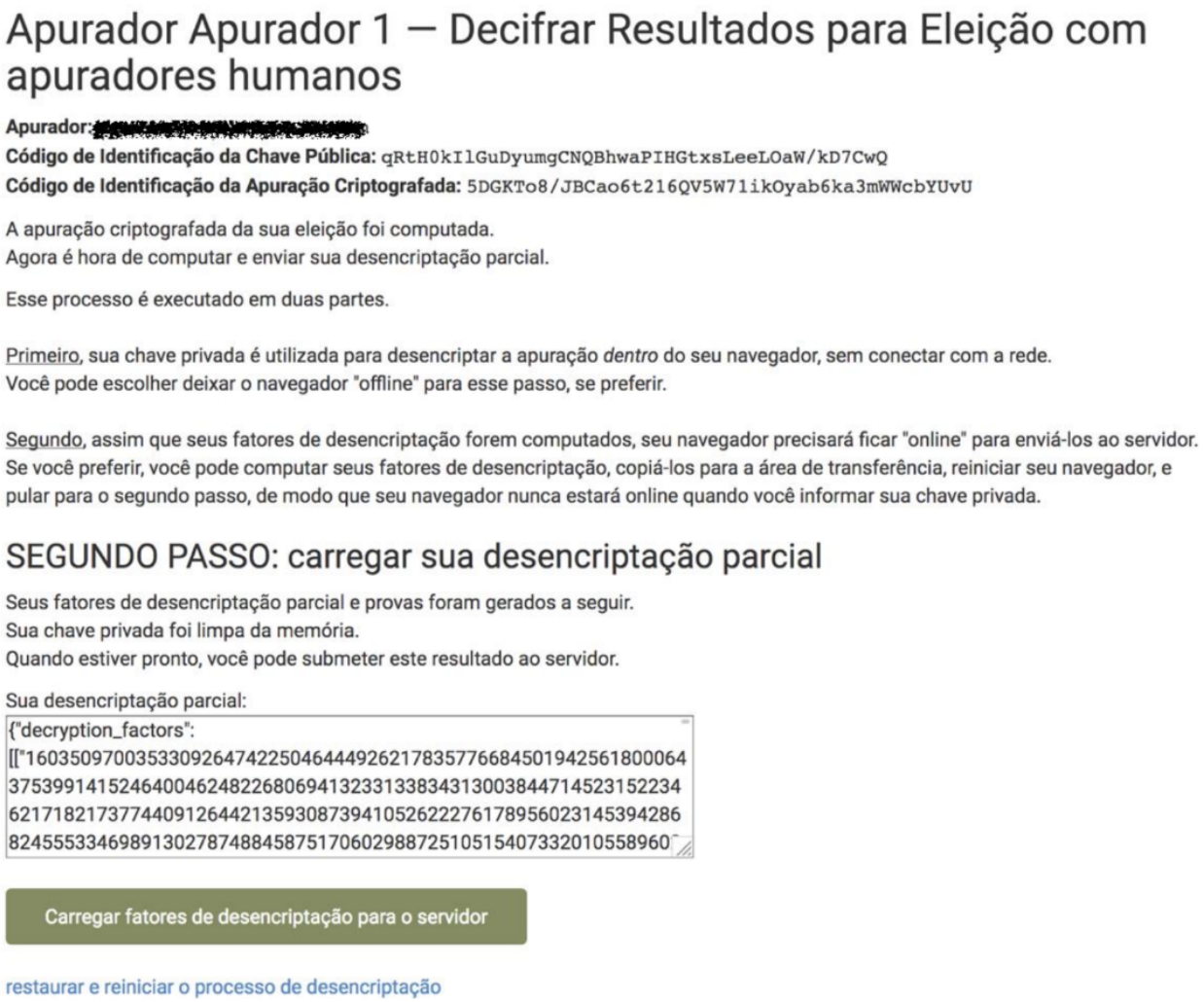
PRIMEIRO PASSO: informe sua chave secreta

{"public_key": {"g":
"14887492224963187634282421537186040801304008017743492304481737382571933937568724473847106029915040150784031882206090286938661464458896494215273989547889201144857352611058572236578734319505128042602372864570426550855201448111746579871811249114 7

Gerar minha parte da desencriptação

pular para o segundo passo
(você precisa já ter computado os fatores de desencriptação.)

Clique no botão **Carregar fatores de desencriptação para o servidor**.



Pronto, você concluiu a sua parte da apuração desta eleição. Cabe agora ao administrador da eleição realizar o procedimento para computar e publicar o resultado da eleição.