

# Apurador da Votação

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

- Geração da Chave de Apuração
- Decifrar Resultado da Eleição com a Chave de Apuração

# 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**.

## Apurador Apurador 1

### Eleição com apuradores humanos

configurar chave de apurador

ATENÇÃO: Quando a apuração for computada, você vai ser solicitado(a) a retornar para essa página e informar sua chave secreta para poder descriptar a apuração.

Você deve manter o email que você recebeu com o link para a sua página de apurador, o qual contém as credenciais necessárias para retornar a essa página.

---

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

## Apurador Apurador 1 – Configuração de chave

### Eleição com apuradores humanos

Como apurador, é hora de configurar sua chave para essa eleição.

Gerar Chaves da Eleição

Se você já tem um par de chaves, você pode [reusá-la](#).

---

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.**

## Apurador Apurador 1 – Configuração de chave

### Eleição com apuradores humanos

Como apurador, é hora de configurar sua chave para essa eleição.

Se você já tem um par de chaves, você pode [reusá-la](#).

### Sua Chave Secreta

Sua chave foi gerada, mas você pode optar por [limpar da memória e começar do zero](#) se preferir.

Salve sua chave privada

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

## Apurador Apurador 1 – Configuração de chave

### Eleição com apuradores humanos

Como apurador, é hora de configurar sua chave para essa eleição.

Se você já tem um par de chaves, você pode [reusá-la](#).

### Sua Chave Secreta

Sua chave foi gerada, mas você pode optar por [limpar da memória e começar do zero](#) se preferir.

Salve sua chave privada

[ok, a chave foi salva, vamos prosseguir](#).

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

## Apurador Apurador 1 – Configuração de chave

### Eleição com apuradores humanos

Como apurador, é hora de configurar sua chave para essa eleição.

Se você já tem um par de chaves, você pode [reusá-la](#).

### Sua Chave Pública

É hora de carregar a chave pública para o servidor.

O código de identificação da sua chave pública é: **qRtH0kI1GuDyumgCNQBhwaPIHGtxsLeeLOaW/kD7CwQ**.

Você pode querer salvar isso para confirmar que a sua chave pública foi adequadamente armazenada pelo servidor.

(Sua chave pública não está sendo mostrada no momento porque você não precisa salvá-la, a impressão digital (fingerprint) é suficiente.)

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.

## Apurador Apurador 1

### Eleição com apuradores humanos

Você carregou com sucesso sua chave pública.

O código de identificação de sua chave pública é: **qRtH0kI1GuDyumgCNQBhwaPIHGtxsLeeLOaW/kD7CwQ**.

Você pode [verificar se você tem a chave privada correta](#)

**ATENÇÃO:** Quando a apuração for computada, você vai ser solicitado(a) a retornar para essa página e informar sua chave secreta para poder descriptar a apuração.

Você deve manter o email que você recebeu com o link para a sua página de apurador, o qual contém as credenciais necessárias para retornar a essa página.

# 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**.

Apurador Apurador 1

Eleição com apuradores humanos

Você carregou com sucesso sua chave pública.

O código de identificação de sua chave pública é: `qRtH0kIlGuDyumgCNQBhwaPIHGtxsLeeLOaW/kD7CwQ`.

Você pode [verificar se você tem a chave privada correta](#)

A apuração criptografada dessa eleição está pronta.

[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: ~~XXXXXXXXXXXXXXXXXXXX~~.com

Código de Identificação da Chave Pública: qRtH0kI1GuDyumgCNQBhwaPIHGtxsLeeLOaW/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 descriptação parcial.

Esse processo é executado em duas partes.

Primeiro, sua chave privada é utilizada para descriptar 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 descriptação forem computados, seu navegador precisará ficar "online" para enviá-los ao servidor. Se você preferir, você pode computar seus fatores de descriptação, 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 descriptação

[pular para o segundo passo](#)

(você precisa já ter computado os fatores de descriptação.)

---

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

## Apurador Apurador 1 – Decifrar Resultados para Eleição com apuradores humanos

Apurador: ~~XXXXXXXXXXXXXXXXXXXX~~.com

Código de Identificação da Chave Pública: qRtH0kI1GuDyumgCNQBhwaPIHGtxsLeeLOaW/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 descriptação parcial.

Esse processo é executado em duas partes.

Primeiro, sua chave privada é utilizada para descriptar 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 descriptação forem computados, seu navegador precisará ficar "online" para enviá-los ao servidor.

Se você preferir, você pode computar seus fatores de descriptação, 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":  
"1488749222496318763428242153718604080130400801774349230448173  
7382571933937568724473847106029915040150784031882206090286938  
6614644588964942152739895478892011448573526110585722365787343  
195051280426023728645704265508552014481117465798718112491147"
```

Gerar minha parte da descriptação

[pular para o segundo passo](#)

(você precisa já ter computado os fatores de descriptação.)

---

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

## Apurador Apurador 1 – Decifrar Resultados para Eleição com apuradores humanos

Apurador: ~~XXXXXXXXXXXXXXXXXXXX~~

Código de Identificação da Chave Pública: qRtH0kI1GuDyumgCNQBhwaPIHGtxsLeeLOaW/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 descriptação parcial.

Esse processo é executado em duas partes.

Primeiro, sua chave privada é utilizada para descriptar 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 descriptação forem computados, seu navegador precisará ficar "online" para enviá-los ao servidor.

Se você preferir, você pode computar seus fatores de descriptação, 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.

### SEGUNDO PASSO: carregar sua descriptação parcial

Seus fatores de descriptação parcial e provas foram gerados a seguir.

Sua chave privada foi limpa da memória.

Quando estiver pronto, você pode submeter este resultado ao servidor.

Sua descriptação parcial:

```
{ "decryption_factors":  
  [ [ "160350970035330926474225046444926217835776684501942561800064  
3753991415246400462482268069413233133834313003844714523152234  
6217182173774409126442135930873941052622276178956023145394286  
824555334698913027874884587517060298872510515407332010558960" ] ]
```

Carregar fatores de descriptação para o servidor

[restaurar e reiniciar o processo de descriptação](#)

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.

## Apurador Apurador 1 – Decifrar Resultados para Eleição com apuradores humanos

Apurador: ~~XXXXXXXXXXXXXXXXXXXX~~

Código de Identificação da Chave Pública: qRtH0kI1GuDyumgCNQBhwaPIHGtxsLeeLOaW/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 descriptação parcial.

Esse processo é executado em duas partes.

Primeiro, sua chave privada é utilizada para descriptar 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 descriptação forem computados, seu navegador precisará ficar "online" para enviá-los ao servidor.

Se você preferir, você pode computar seus fatores de descriptação, 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.

Pronto!

Voltar para eleição