

# 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

Atualizado: 8 maio 2026 16:36:39 por Antonio Costa