

# Prescrição Digital:

Certificado Digital para ativação do  
HTTPs no e-SUS PEC 5.2

## Linux



MINISTÉRIO DA  
SAÚDE

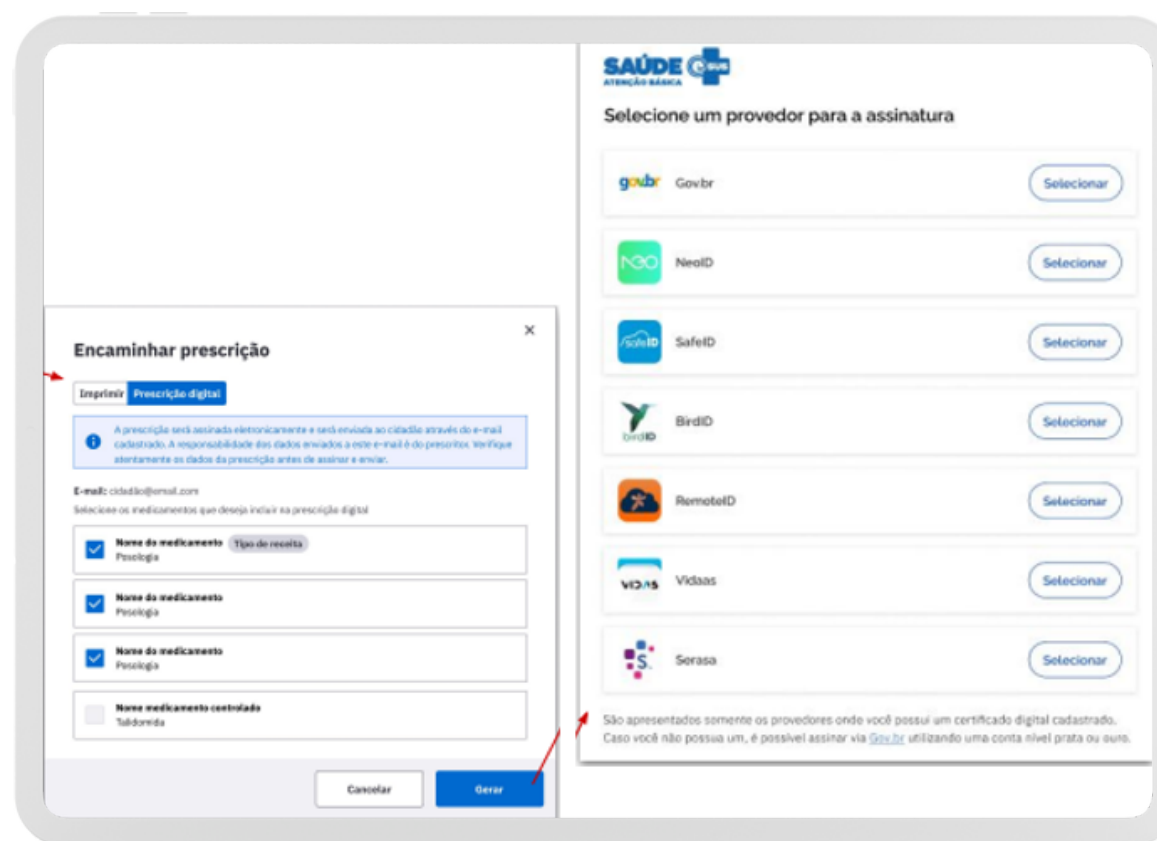




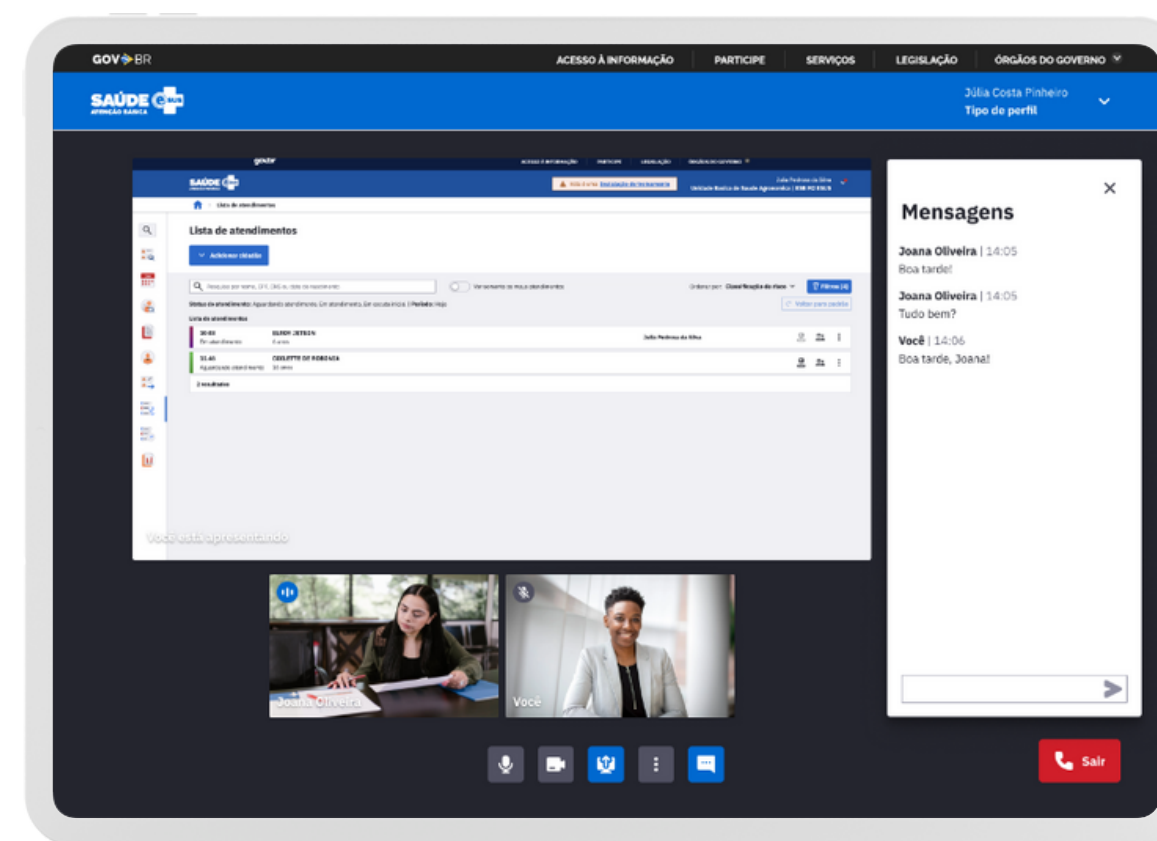
**Certificado digital é uma ferramenta que confere autenticidade e garante que o provedor de um serviço é de fato, quem realmente diz ser!**

**PEC 5.2** | **Https**

Prescrição Digital

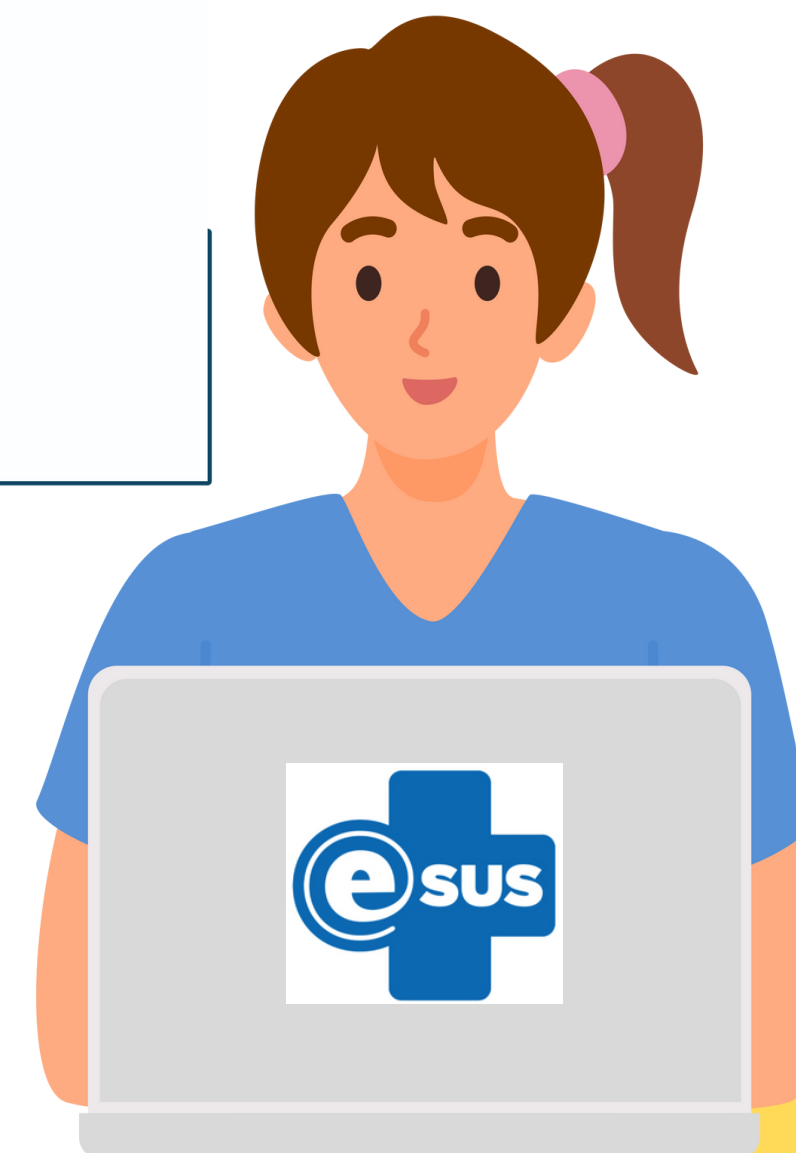
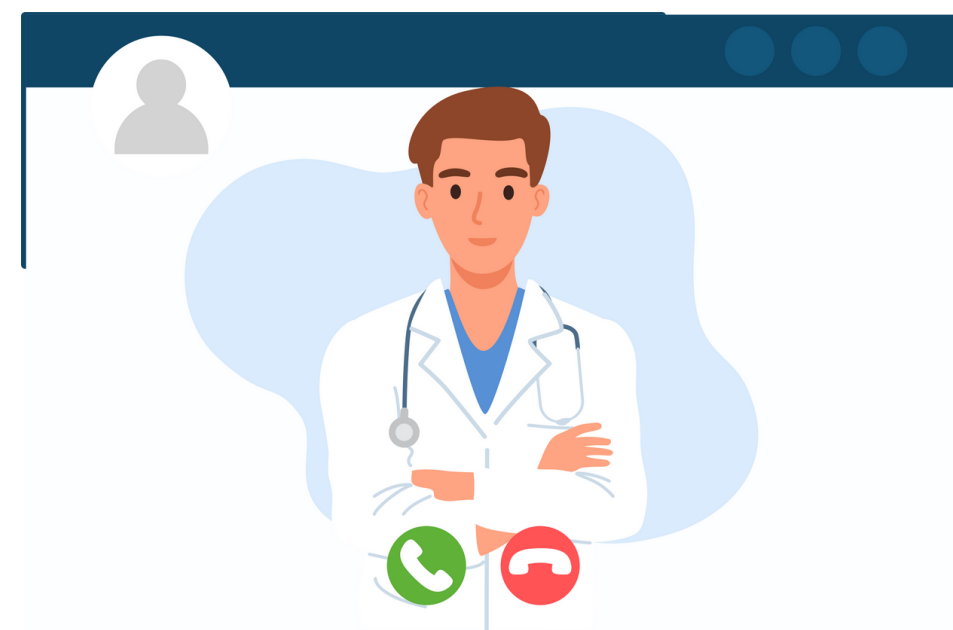


Vídeochamada



# HTTPS:

Viabiliza uma **conexão criptografada**, permitindo que os participantes envolvidos na comunicação tenham os seus dados protegidos, assegurando-se maior **confidencialidade** e **sigilo** das informações !!!



# Let's Encrypt:

Para geração do certificado digital, utilizaremos a **Let's Encrypt** que é uma autoridade certificadora **gratuita**, automatizada e aberta que se tornou possível graças à organizações sem fins lucrativos na Internet.

 **Atenção!!!**

Let's Encrypt não emite certificados para endereços IP simples, apenas **nomes de domínio**.

**Exemplo:** [sisaps.saude.gov.br](https://sisaps.saude.gov.br)



# Etapas:

É importante destacar que as etapas descritas abaixo para geração do certificado através do Let's Encrypt, são apenas **sugestões**, podendo o Município utilizar a certificadora que desejar para geração do certificado.

## Serão duas etapas:

1

Geração do Certificado Digital  
via Certbot da Let's Encrypt



2

Configuração e  
Parametrização do PEC 5.2





Descrição passo a passo da geração do certificado e parametrização do PEC:



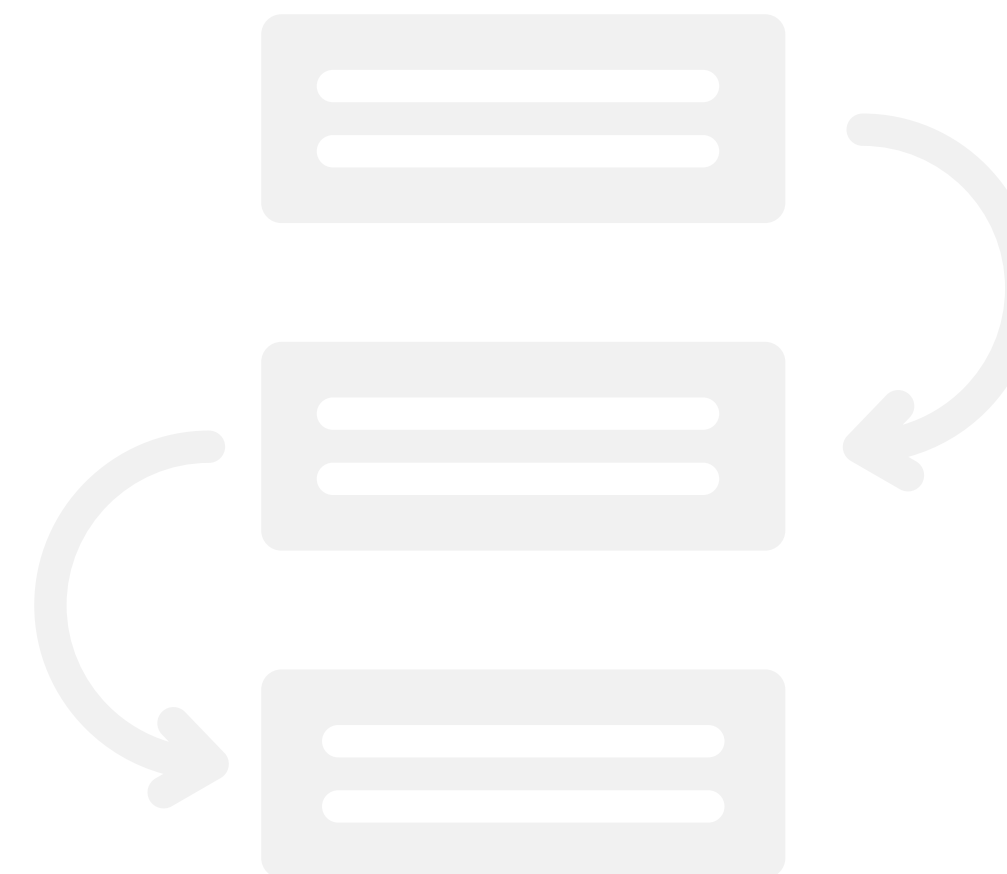
### Gerar Certificado Digital

- 1 Alteração da porta no PEC
- 2 Reiniciar o serviço
- 3 Instalar Core do **snspd**
- 4 Instalar e configurar o **certbot**
- 5 Geração do certificado digital
- 6 Importar certificado e criar a keystore



### Parametrização PEC 5.2

- 1 Parametrização do PEC





## Algumas premissas:

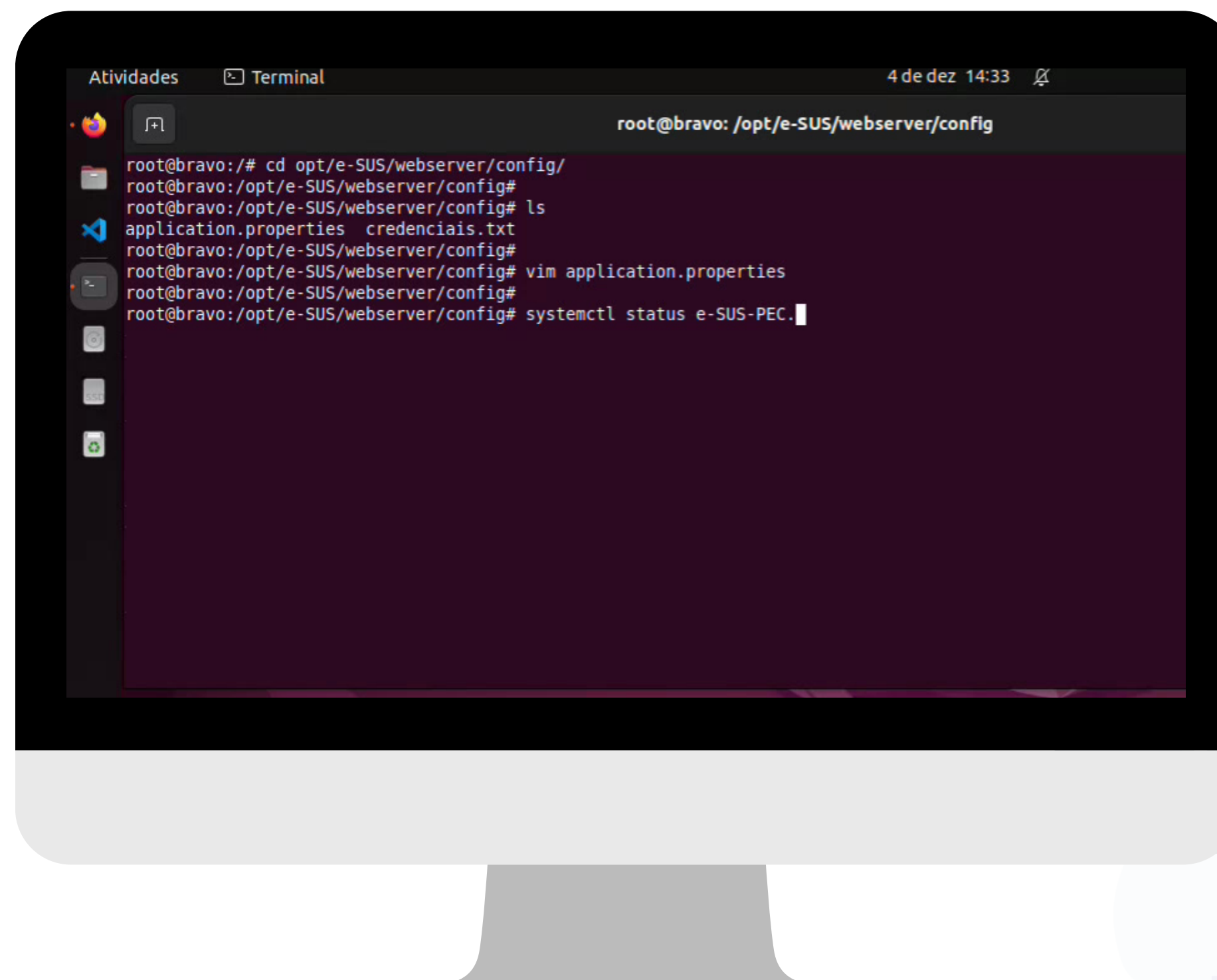
- 1** Necessário ter um DOMÍNIO (DNS) próprio;  
Ex.: [www.municipio.esus.gov.br](http://www.municipio.esus.gov.br)
- 2** Como este tutorial é para Sistemas Operacionais (SO) GNU/Linux, exige-se uma distribuição linux para execução dos procedimentos;  
Ex.: Debian, Ubuntu, CentOS, etc
- 3** Liberação das portas: 80 e 443.





## Geração do Certificado Digital via Certbot da Let's Encrypt:

- 1 Alterar a porta do PEC:
  - a. Caminho: `/opt/e-SUS/webserver/config/application.properties`
  - b. Inserir a linha: **`server.port=80`**
- 2 Reiniciar o serviço do PEC: `systemctl restart e-SUS-PEC.service`



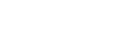
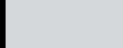
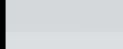
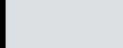
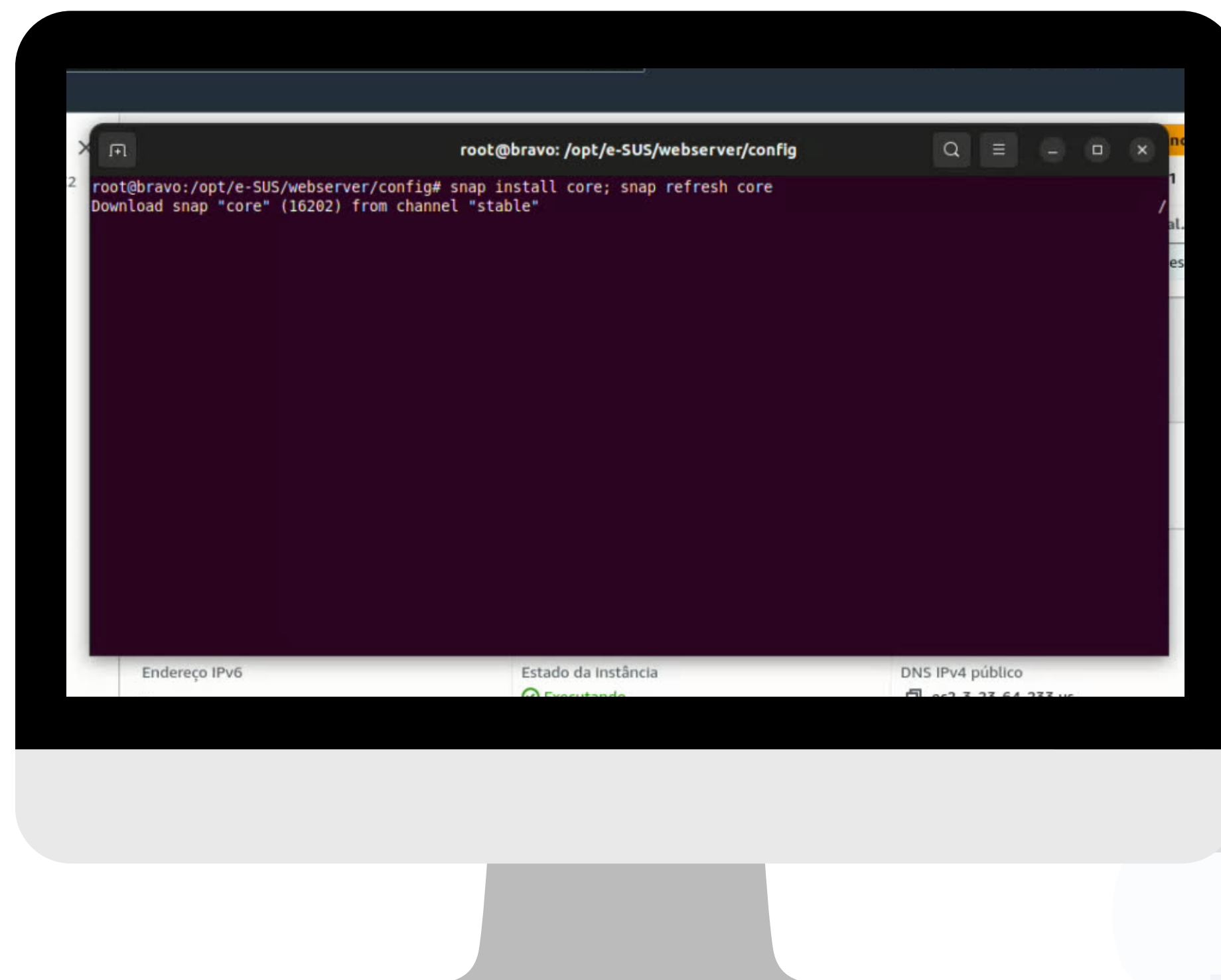




## Geração do Certificado Digital via Certbot da Let's Encrypt:

- 3 Com o **snapt** instalado, execute:

```
sudo snap install core; sudo snap refresh core
```

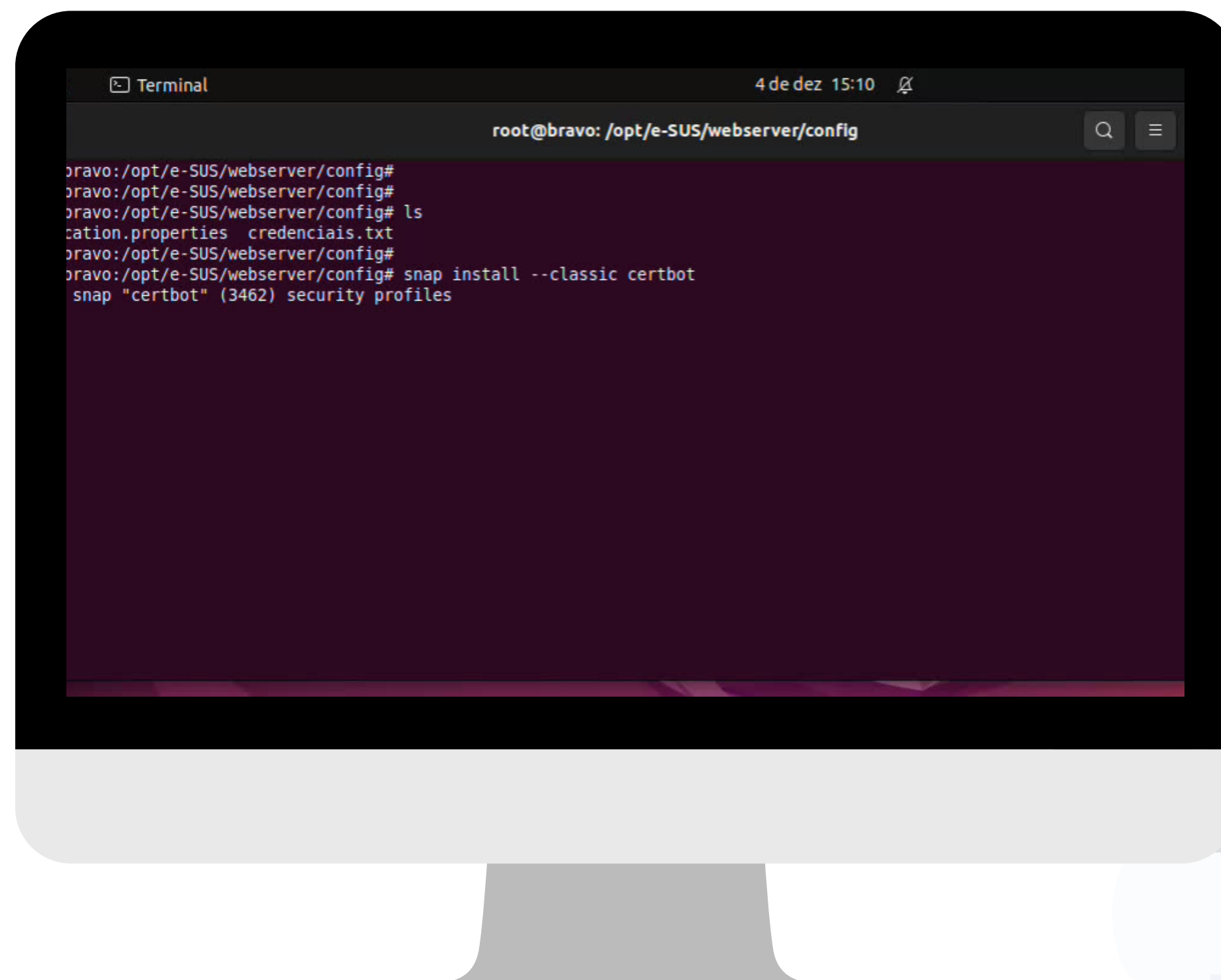




## Geração do Certificado Digital via Certbot da Let's Encrypt:

### 4 Instalar e configurar o **certbot**:

- a. `sudo snap install --classic certbot`
- b. `sudo ln -s /snap/bin/certbot /usr/bin/certbot`





Geração do Certificado Digital via Certbot da Let's Encrypt:

**5** Após a instalação do **certbot**: `certbot certonly --webroot`

Informe: **e-mail**, **DNS** e o endereço **webroot** da aplicação

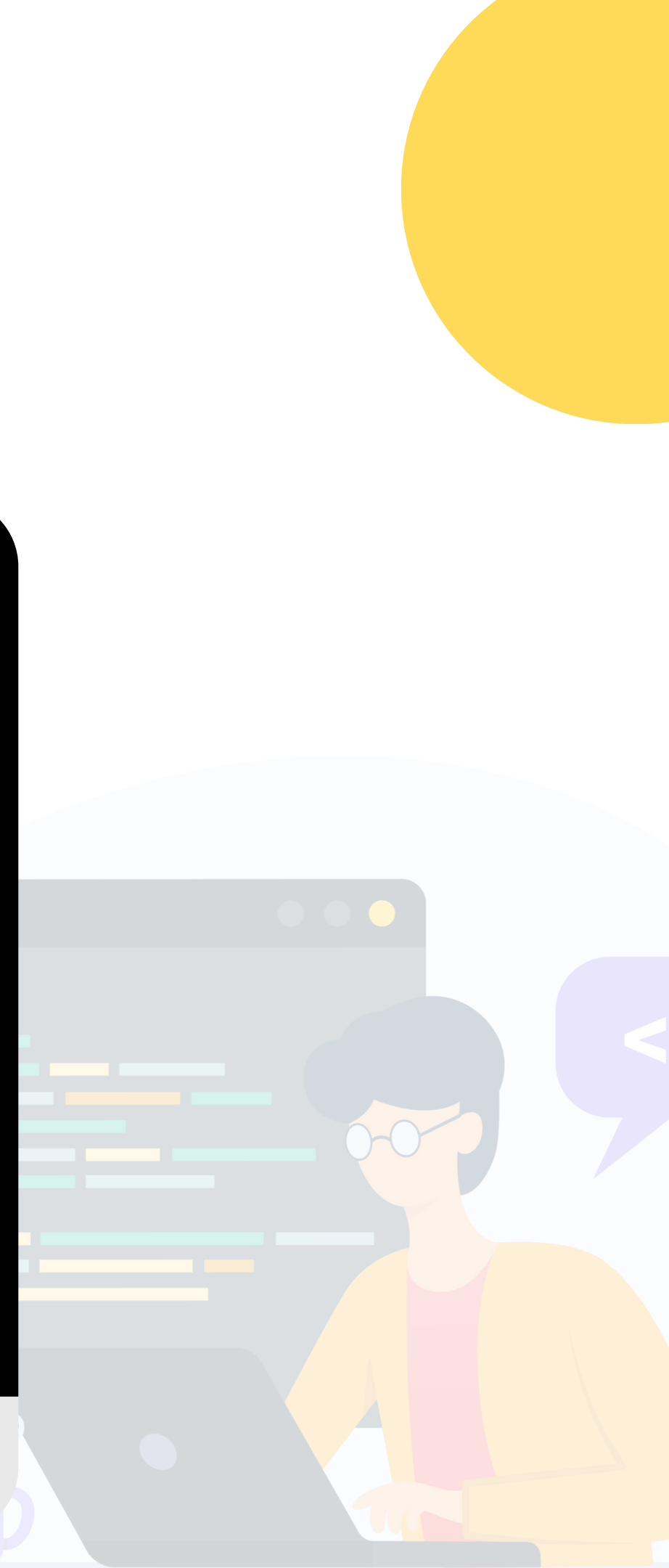
Por padrão, os certificados são armazenados no seguinte caminho:

**Exemplo:** `/etc/letsencrypt/live/municipio.esus.gov.br/`

```
aws Serviços Search [Alt+S]
EC2
root@bravo:/opt/e-SUS/webserver/config# ln -s /snap/bin/certbot /usr/bin/certbot
root@bravo:/opt/e-SUS/webserver/config#
root@bravo:/opt/e-SUS/webserver/config#
root@bravo:/opt/e-SUS/webserver/config#
root@bravo:/opt/e-SUS/webserver/config# certbot certonly --webroot
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): treinamento-esuspec.ddns.net
Requesting a certificate for treinamento-esuspec.ddns.net
Input the webroot for treinamento-esuspec.ddns.net: (Enter 'c' to cancel): /var/www/html

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/treinamento-esuspec.ddns.net/fullchain.pem
Key is saved at: /etc/letsencrypt/live/treinamento-esuspec.ddns.net/privkey.pem
This certificate expires on 2024-02-28.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

-----
If you like Certbot, please consider supporting our work by:
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
* Donating to EFF: https://eff.org/donate-le
-----
root@bravo:/opt/e-SUS/webserver/config#
```





Geração do Certificado Digital via Certbot da Let's Encrypt:

**6** Importar o certificado e criar a keystore:

```
keytool -import -alias esusaps -file /etc/letsencrypt/live/esus/municipio.esus.gov.br/  
fullchain.pem -keystore esusaps.p12 -storepass esus
```

Armazene o certificado **.p12** no diretório **/opt/e-SUS/webserver/config/**

```
root@bravo: /etc/letsencrypt/live/treinamento-esusaps.ddns.net

#7: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
]

#8: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: treinamento-esusaps.ddns.net
]

#9: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: 2F BB DC F2 5C 61 C3 EC   F8 A6 F2 4F 3E 68 46 0C   /...a.....0>hF.
    0010: 3F F3 E2 96                ?...
  ]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
root@bravo:/etc/letsencrypt/live/treinamento-esusaps.ddns.net#
root@bravo:/etc/letsencrypt/live/treinamento-esusaps.ddns.net# ls
README cert.pem chain.pem esusaps.p12 fullchain.pem privkey.pem
root@bravo:/etc/letsencrypt/live/treinamento-esusaps.ddns.net#
```

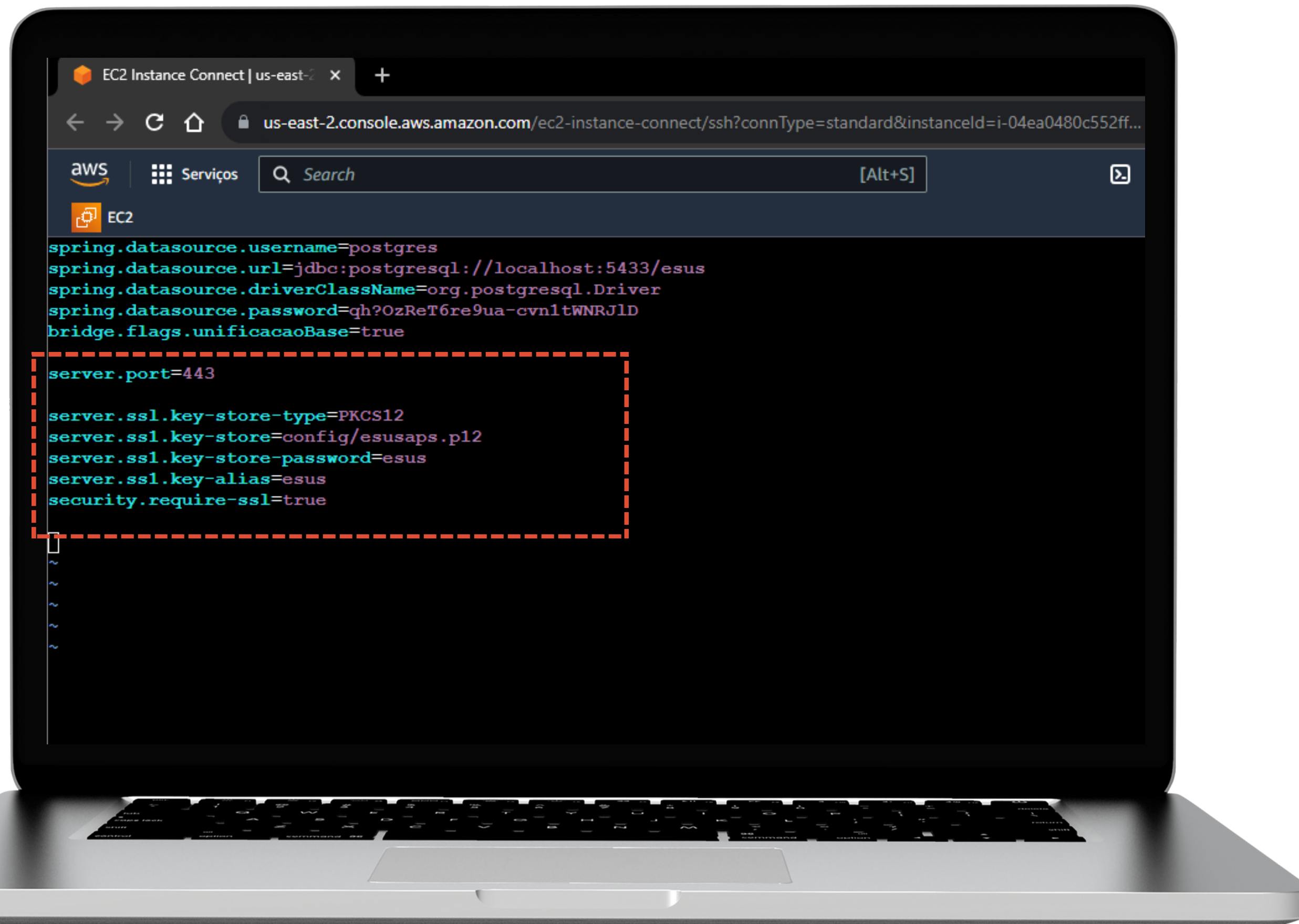






## Configuração e Parametrização do PEC 5.2:

`/opt/e-SUS/webserver/config/application.properties`





## Lista de comandos executados:

- 1 Alteração de porta no PEC:**
  - a. Caminho: `/opt/e-SUS/webserver/config/application.properties`
  - b. Inserir a linha: `server.port=80`
- 2** Reiniciar o serviço do PEC: `systemctl restart e-SUS-PEC.service`
- 3** Com o **snapd** instalado, execute: `sudo snap install core; sudo snap refresh core`
- 4** Instalar e configurar o **certbot**:
  - a. `sudo snap install --classic certbot`
  - b. `sudo ln -s /snap/bin/certbot /usr/bin/certbot`
- 5** Após a instalação, execute-o: `certbot certonly --webroot`
- 6** Importar certificado e criar a keystore:  
**Exemplo:**  
`keytool -import -alias esusaps -file /etc/letsencrypt/live/esus/sisaps.saude.gov.br/fullchain.pem -keystore esusaps.p12 -storepass esus`



# Lembre-se:



Portal APS:



Manual PEC:



Suporte:

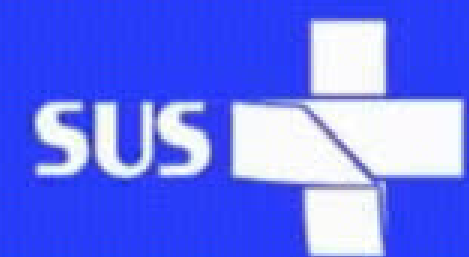


SUBSCRIBE



Share





MINISTÉRIO DA  
SAÚDE

