## Universidade Federal Rural de Pernambuco Sistemas de Informação Segurança e Auditoria de Sistemas Lhaíslla Eduarda Cavalcanti Rodrigues da Silva RECIFE-PE

2023

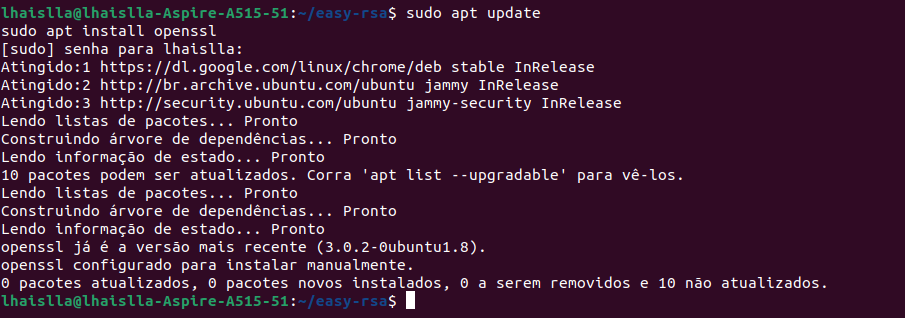
**Certificado**

Uma autoridade certificadora (CA) é responsável pela emissão de certificados digitais para verificação de identidades na internet. Neste arquivo contam os comandos necessários para criar uma certificação publica e privada no ubuntu 22.04.

**Instalação:**

**Usando o Openssl para configurar o certificado:**

Utilizando a ferramenta openssl para criar uma chave privada e um certificado.



openssl req -x509 -sha256 -days 356 -nodes -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt

x-509: Formato padrão para certificados de chave pública

sha256: Hash que será utilizado no certificado

days: quantidade de dias que o certificado será valido

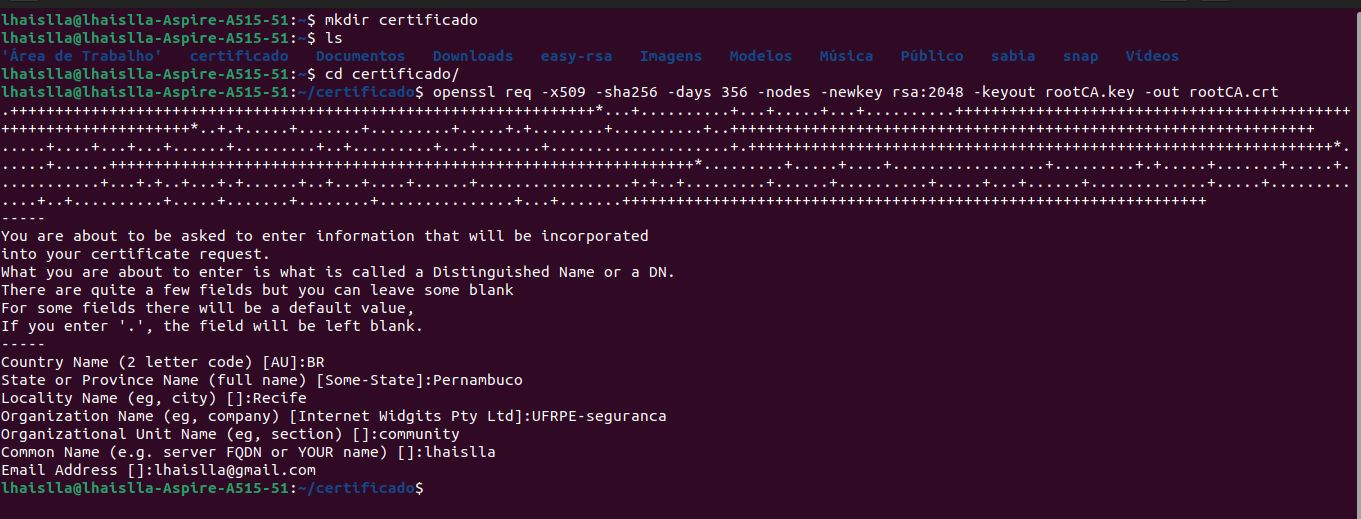
-nodes: comando para não decriptar o certificado criado

-newkey rsa:2048 o tamanho com 2048 bits

-keyout é a chave que será gerada:

A chave vai se chamar rootCA.key

-out rootCA.crt a definição do certificado da CA  
  
preencher os campos de informação



**Listagem de certificados criados:**

ls -la

Entre os arquivos gerados os que identificam as chaves são:

* rootCA.crt é o arquivo de certificado público da CA. Usuários, servidores e clientes usarão esse certificado para verificar se fazem parte da mesma rede de confiança. Todo usuário e servidor que usa sua CA precisará ter uma cópia desse arquivo. Todas as partes confiarão no certificado público para garantir que alguém não esteja personificando um sistema e realizando um [ataque Man-in-the-middle](https://en.wikipedia.org/wiki/Man-in-the-middle_attack) .
* rootCA.key é a chave privada que a CA usa para assinar certificados para servidores e clientes. Se um invasor obtiver acesso à sua CA e, por sua vez, ao seu ca.keyarquivo, você precisará destruir sua CA. É por isso que seu ca.keyarquivo deve estar apenas em sua máquina CA e que, idealmente, sua máquina CA deve ser mantida off-line quando não estiver assinando solicitações de certificado como uma medida extra de segurança.



**Criar a chave privada(private-key):**

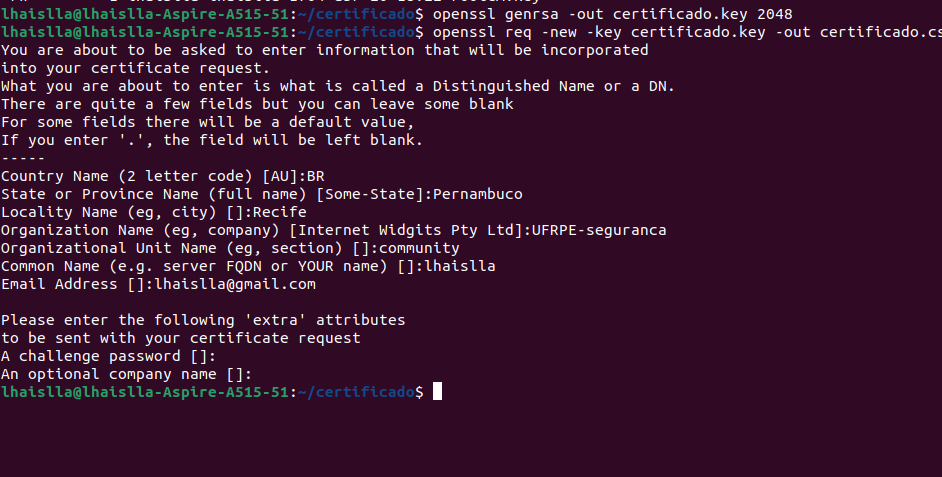
openssl genrsa -out certificado.key 2048



**Criação da solicitação de assinatura de certificado (CSR)/Pedir para C.A Assinar o certificado:**

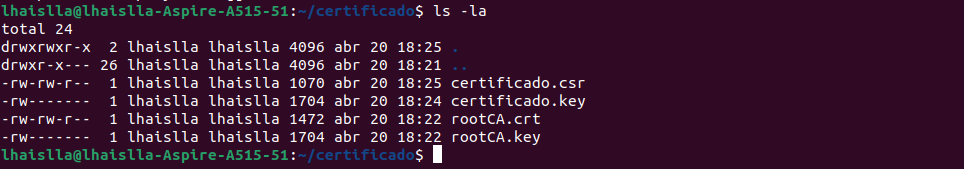
Geração de uma chave privada e solicitação de certificado.[Solicitação de Assinatura de Certificado](https://en.wikipedia.org/wiki/Certificate_signing_request) (CSR) consiste em três partes: uma chave pública, informações de identificação sobre o sistema solicitante e uma assinatura da própria solicitação, que é criada usando a chave privada da parte solicitante. A chave privada será mantida em segredo e será usada para criptografar informações que qualquer pessoa com o certificado público assinado poderá descriptografar.

openssl req -new -key certificado.key -out certificado.csr



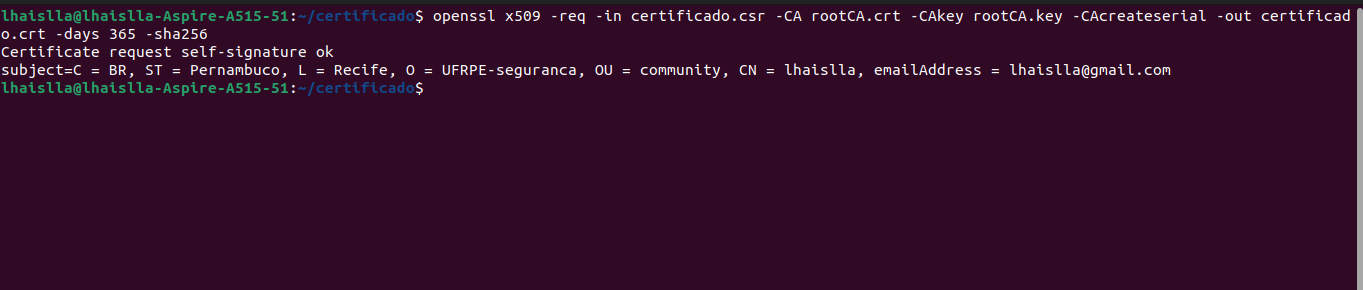
Verificando a criação de solicitação do certificado:

ls -la



**Criação do certificado assinado pela CA:**

openssl x509 -req -in certificado.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out certificado.crt -days 365 -sha256

Esse certificado é para utilizar em ambientes internos. Pode ser utilizado em ambientes externos, mas irá precisar o certificado e chave da CA, para validar a informação.

**Referência:** <https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-a-certificate-authority-on-ubuntu-22-04>

<https://youtu.be/HZ2OKVu5O0s>