Instalação do certificado SSL

- Consultar no DNS qual a máquina responsável por redirecionar o serviço (VM própria ou *proxy*).

Na máquina do serviço a ter o certificado instalado:

- Acessar a pasta */etc/nginx* e conferir no diretório *conf.d* os arquivos de configuração *serviço.conf* e onde estão localizados os certificados (geralmente `/etc/ssl/icpedu`);
- Acessar o diretório dos certificados e mover os agora expirados para uma pasta de "*antigos*":

```
sudo mv serviço.ifsertao* antigos/
```

- Criar arquivos *CSR, KEY, CRT* para cada nome de domínio (ex.: ifsertao-pe e ifsertaope):
  - CSR e KEY:
    - utilizar script `./gerar_csr.sh` para criar a requisição (.csr) e a chave (.key);
  - CRT:
    - emitir certificado no site da Global Sign e criar arquivo `serviço.crt` contendo o conteúdo do certificado.

NGINX:

- Criar arquivo serviço.pem concatenando três arquivos (para cada nome de domínio):
  - serviço.crt
  - root (gs_root.pem)
  - intermediate.pem

```
cat serviço.crt intermediate.pem gs_root.pem > serviço.pemcaso retorne "Permissão negada":
sudo bash -c "cat serviço.crt intermediate.pem gs_root.pem > serviço.pem"
```

- Testar arquivos de configuração em uso pelo NGINX:

```
nginx -t
```

- Reiniciar serviço do NGINX e verificar status:

```
systemctl restart nginx
```

```
systemctl status nginx
```

APACHE

- O apache utiliza de forma separadadois arquivos criados no processo (a chave .key e o certificado .crt).
- Testar arquivos de configuração em uso pelo Apache:

```
apachectl configtest
```

- Reiniciar serviço do Apache e verificar status:

```
systemctl restart httpd (apache)
```

```
systemctl status httpd (apache)
```

- Acessar página do serviço pelo navegador e verificar a validade do certificado.

Revision #5
Created Thu, Mar 9, 2023 8:30 PM by Júlio Luiz
Updated Fri, Oct 27, 2023 11:21 AM by Júlio Luiz