

```

juan@juan-vmwarevirtualplatform:~/Desktop$ sudo mkdir -p /pki/ca
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo mkdir -p /pki/servidor

juan@juan-vmwarevirtualplatform:~/Desktop$ sudo mkdir -p /pki/clientes
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo mkdir -p /pki/miscertificados
juan@juan-vmwarevirtualplatform:~/Desktop$

```

Primero creamos las carpetas donde vamos a meter todos nuestros certificados

```

juan@juan-vmwarevirtualplatform:~/Desktop$ openssl genrsa -out ca.key 2048

```

Generamos una clave privada para la CA. Esta clave será utilizada para firmar los certificados.

```

juan@juan-vmwarevirtualplatform:~/Desktop$ openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.crt -subj "/C=ES/ST=Andalucía/L=Almería/O=MíEmpresa/OU=IT/CN=MíCA/cjho.juan@gmail.com"
req: Missing '=' after RDN type string 'cjho.juan@gmail.com' in subject name string

```

Creamos un certificado raíz de 10 años.

```

juan@juan-vmwarevirtualplatform:~/Desktop$ openssl genrsa -out servidor.key 2048

```

Genera una clave privada para el servidor

```

juan@juan-vmwarevirtualplatform:~/Desktop$ openssl req -new -key servidor.key -out servidor.crt -subj "/C=ES/ST=State/L=City/O=Organizacion/OU=IT/CN=practicapki.com"

```

Creamos un certificado para el servidor

```

juan@juan-vmwarevirtualplatform:~/Desktop$ sudo openssl x509 -req -in servidor.csr -CA /home/juan/Desktop/ca.crt -CAkey /home/juan/Desktop/ca.key -CAcreateserial -out servidor.crt -days 365 -sha256
Certificate request self-signature ok
subject=C = ES, ST = State, L = City, O = Organization, OU = IT, CN = practicapki.com

```

Firmamos el certificado por la CA

Después realizamos pruebas para comprobar que todo va bien

```

juan@juan-vmwarevirtualplatform:~/Desktop$ sudo openssl rsa -check -in /pki/ca/ca.key
RSA key ok
writing RSA key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQCiswFwblUf09Y0
iU1pv3ItZxeWo82SGIxyezrAh/WtjUFLhUYG0g8lwneff6MIBYWHNerj7Xby55V
ekSxmbd5TVD62H4Sc76iIY9TmDp+pH0RltCL/GhzjldRXJ6+tey3/or2rwsaT6Uh
5rwaBTnVdKDRXlfhPozkofb7GUqr8ia6xzC0wpCk1neH0vSiVR3lpiI0g5gsE4bV
aYFtS4KPzECUHW9w2nZ9RFR6yeNYDmPQZ8NAQbJ3IWAwwO/PbzauLYEs10+5qUPsc
7WRw01tTI9GAVkA0sn88IpgidapjKEUvFZUCZ+NHfoffzBmQNzAIbA8GupIWA0lW
E++kovULAgMBAACGgEAAYNfUNyePfQfJ7KHsqE0l5rSuIg2hLPqOf4JGUTVH77r
2+9uYCK2KYKFI5895b3U76MYsATLI522ktjb5vEM8N74dM3x/1jt11JYXE+VL3A
wAb81GIP683UCG8t6iBGy4ui3Yt0t6w6o8oui7FydVALyEcT3tutAeL9MC0yTVNy
SR9yrTBKMxPlkrnDhaIiVVg/dFqkTDIGHTysvew10xBnPP3dHeDuyCpauApBAfo
n/m7KKMhVF3lAKZadehoaUyoZxFRzZbFwRHC7rQuTbXwFUIgouk8idjcwLbX2y03
vwI/rnNFdwZrsoX1Kkn9arcg6nb+X4204+5waEkm2QKBgQDTAUCChviquvknZ3u0rS
05/nhxAJB3FF43MTu9I/SI0u4FATdYudLSZd2zXFyJ+Jixmonm8DTkq4ThHjvJvF
cjXB0vsXeV6qiZn4v1i7MpDkrlJgw8f8WqsNoEZOXm1EpMVxGj0jdDf0jJA1raU/
csFEXyzG2rVSXF8D677SHoqnzQKBgQDFZL/zmVtBeZpIdCuqnWcxrJaVbcFNzI/P
A0RfnBAXLOoxXB5wLmLfExhDl+XXSmg1Eea1M7HonSuqg5f0aDe+0Yz81SXql1w

```

Creamos la clave del clientes

```
juan@juan-vmwarevirtualplatform:/pki/clientes$ sudo openssl genrsa -out juanperez.key 2048
```

Creamos el csr del cliente

```
juan@juan-vmwarevirtualplatform:/pki/clientes$ sudo openssl req -new -key juanperez.key -out juanperez.csr -subj "/C=ES/ST=Andalucía/L=Almería/O=MiEmpresa/OU=Usuarios/CN=JuanPerez/emailAddress=juan.perez@ejemplo.com"
```

Se firma el csr con la CA

```
juan@juan-vmwarevirtualplatform:/pki/clientes$ sudo openssl x509 -req -in juanperez.csr -CA /pki/ca/ca.crt -CAkey /pki/ca/ca.key -CAcreateserial -out juanperez.crt -days 365 -sha256
Certificate request self-signature ok
subject=C = ES, ST = Andalucía, L = Almería, O = MiEmpresa, OU = Usuarios, CN = JuanPerez, emailAddress = juan.perez@ejemplo.com
```

Creamos el p12 del cliente para su uso

```
juan@juan-vmwarevirtualplatform:/pki/clientes$ sudo openssl pkcs12 -export -out juanperez.p12 -inkey juanperez.key -in juanperez.crt -certfile /pki/ca/ca.crt
Enter Export Password:
Verifying - Enter Export Password:
```

1. Instalación de Nginx y PHP

Actualizamos el sistema

```
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo apt update
```

```
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo apt upgrade
```

Instalamos nginx y php

```
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo apt install nginx
```

```
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo apt install php
```

Encendemos los servicios:

```
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo systemctl start nginx
```

```
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-12-15 16:25:25 CET; 26min ago
     Docs: man:nginx(8)
   Process: 32173 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on;
   Process: 32176 ExecStart=/usr/sbin/nginx -g daemon on; master_process on;
   Main PID: 32177 (nginx)
    Tasks: 3 (limit: 4546)
   Memory: 3.5M (peak: 4.0M)
      CPU: 48ms
   CGroup: /system.slice/nginx.service
           └─32177 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             └─32178 "nginx: worker process"
               └─32179 "nginx: worker process"

dic 15 16:25:25 juan-vmwarevirtualplatform systemd[1]: Starting nginx: A high performance web server and a reverse proxy server:/.
dic 15 16:25:25 juan-vmwarevirtualplatform systemd[1]: Started nginx: A high performance web server and a reverse proxy server:/.
lines 1-17/17 (END)
```

```

juan@juan-vmwarevirtualplatform:~/Desktop$ sudo systemctl start php8.3
juan@juan-vmwarevirtualplatform:~/Desktop$ sudo systemctl status php8.3-fpm
● php8.3-fpm.service - The PHP 8.3 FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/system/php8.3-fpm.service; enabled)
   Active: active (running) since Sun 2024-12-15 14:49:53 CET; 2h 4min
     Docs: man:php-fpm8.3(8)
  Process: 1276 ExecStartPost=/usr/lib/php/php-fpm-socket-helper in
 Main PID: 1244 (php-fpm8.3)
   Status: "Processes active: 0, idle: 2, Requests: 0, slow: 0, Tra
    Tasks: 3 (limit: 4546)
  Memory: 13.0M (peak: 14.8M)
     CPU: 522ms
    CGroup: /system.slice/php8.3-fpm.service
            └─1244 "php-fpm: master process (/etc/php/8.3/fpm/php-fp
              └─1251 "php-fpm: pool www"
                └─1252 "php-fpm: pool www"

dic 15 14:49:53 juan-vmwarevirtualplatform systemd[1]: Starting php8.3
dic 15 14:49:53 juan-vmwarevirtualplatform systemd[1]: Started php8.3
lines 1-17/17 (END)

```

Configuración de Nginx

```

juan@juan-vmwarevirtualplatform: /pki/clientes
Archivo  Acciones  Editar  Vista  Ayuda
juan@juan-vmwarevirtualplatform: /pki/clientes x
GNU nano 7.2 /etc/nginx/sites-available/practicapki
server {
    #listen 8080;
    #server_name practicapki.com;

    listen 443 ssl;
    server_name practicapki.com;

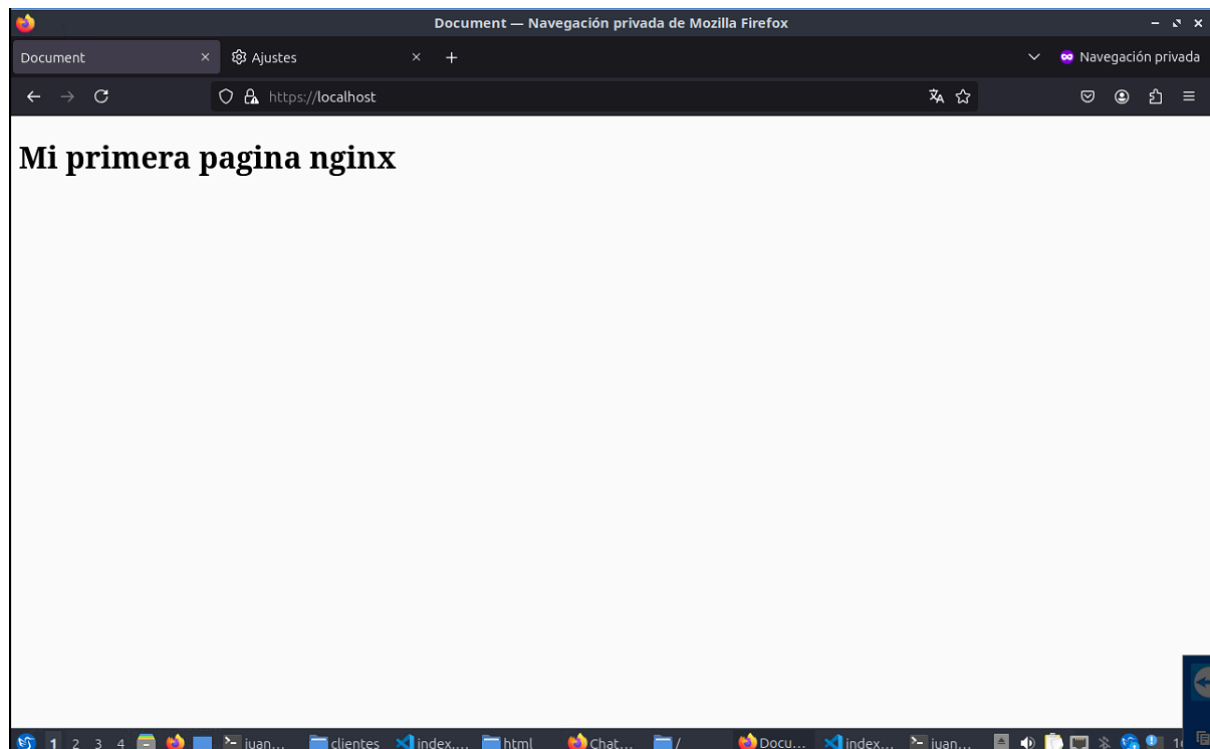
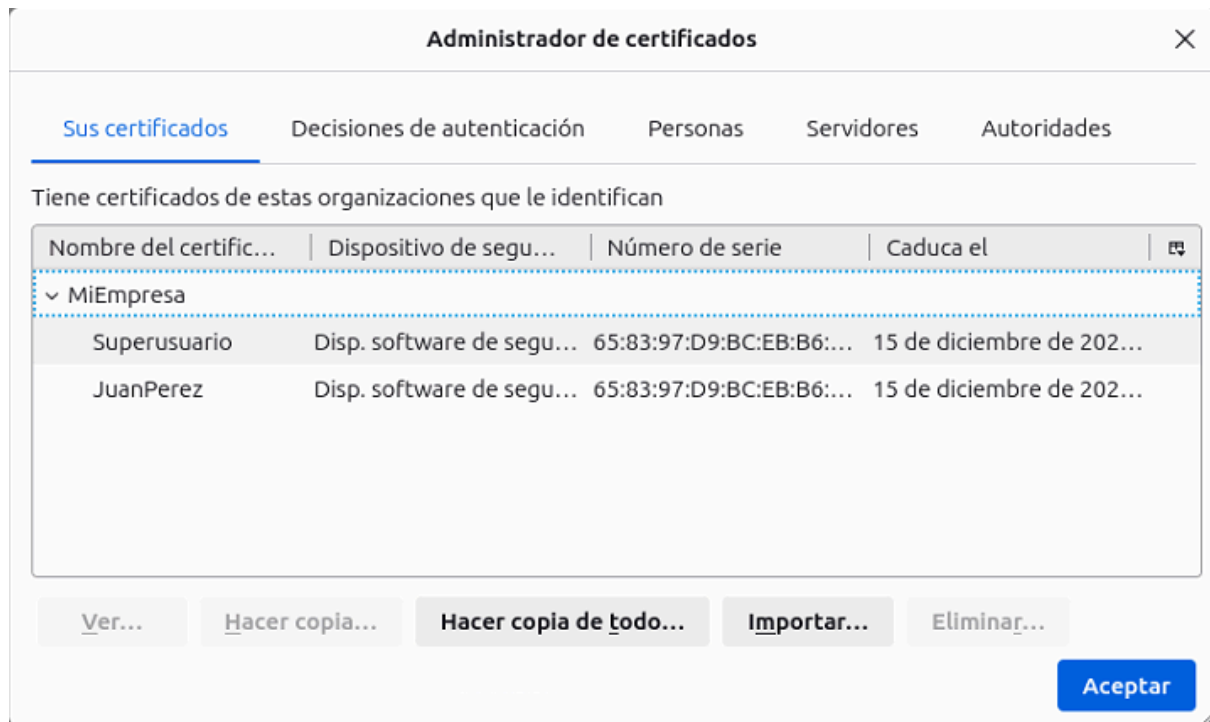
    # Certificados del servidor
    ssl_certificate /pki/servidor/servidor.crt;
    ssl_certificate_key /pki/servidor/servidor.key;

    # Cadena de certificados para confianza
    ssl_trusted_certificate /pki/ca/ca.crt;

    # Habilitar autenticación mutua (cliente debe presentar un certif
    ssl_client_certificate /pki/ca/ca.crt;
    ssl_verify_client on;
}
[ 47 líneas leídas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar      ^J Justificar

```

Creamos y modificamos el archivo para que se pueda lanzar nuestra propia pagina. Debemos añadir nuestros certificados al navegador para poder entrar en la pagina. Ya que ellos son los que tienen los permisos para ello.



Creacion de superusuario, nueva pagina, obtencion de datos del certificado por php y filtrado.

```
juan@juan-vmwarevirtualplatform:/pki/clientes$ sudo openssl genrsa -out superusuario.key 2048
```

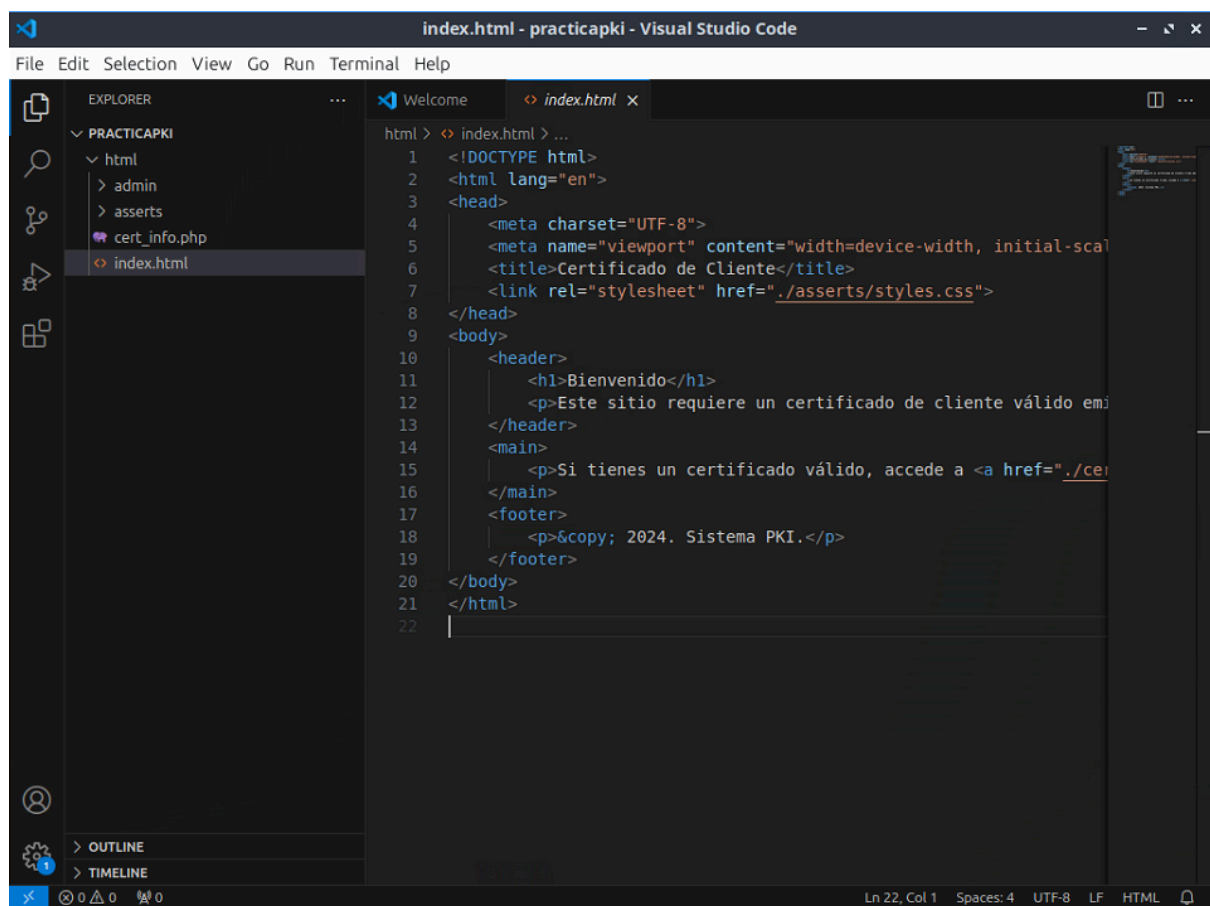
```
juan@juan-vmwarevirtualplatform:/pki/clientes$ sudo openssl req -new -key superusuario.key -out superusuario.csr -subj "/CN=Superusuario/O=MiOrganizacion"
```

```
juan@juan-vmwarevirtualplatform:/pki/clientes$ sudo openssl x509 -req -in superusuario.csr -CA /pki/ca/ca.crt -CA /pki/ca/ca.key -CAcreateserial -out superusuario.crt -days 365 -sha256
```

```
juan@juan-vmwarevirtualplatform:/pki/clientes$ openssl pkcs12 -export -out superusuario.p12 -inkey superusuario.key -in superusuario.crt -certfile /pki/ca/ca.crt
```

```
juan@juan-vmwarevirtualplatform:/pki/clientes$ sudo chown juan:juan /pki/clientes/superusuario..p12
```

Aqui hemos creado el superusuario y todos sus certificados correspondientes

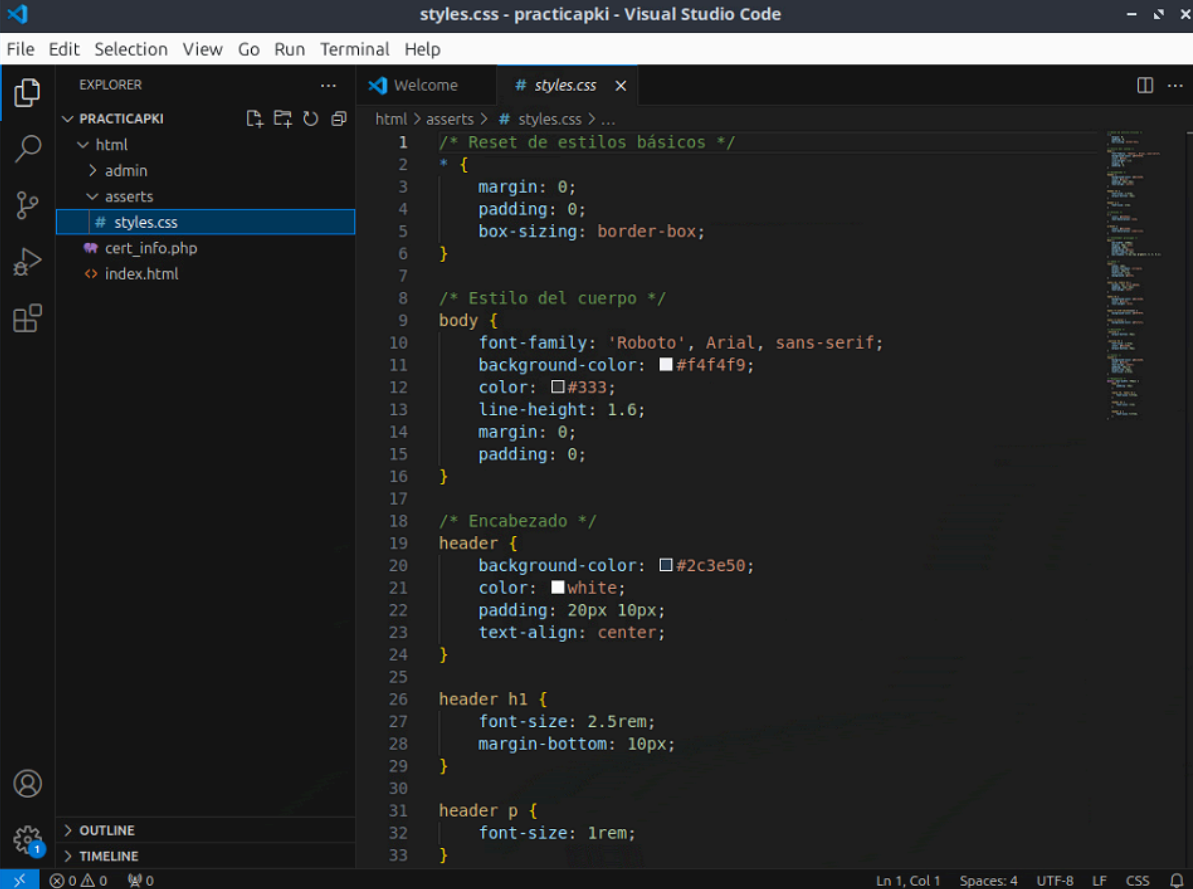


```
index.html - practicapki - Visual Studio Code
File Edit Selection View Go Run Terminal Help

EXPLORER
PRACTICAPKI
├── html
│   ├── admin
│   ├── asserts
│   ├── cert_info.php
│   └── index.html
└── ...

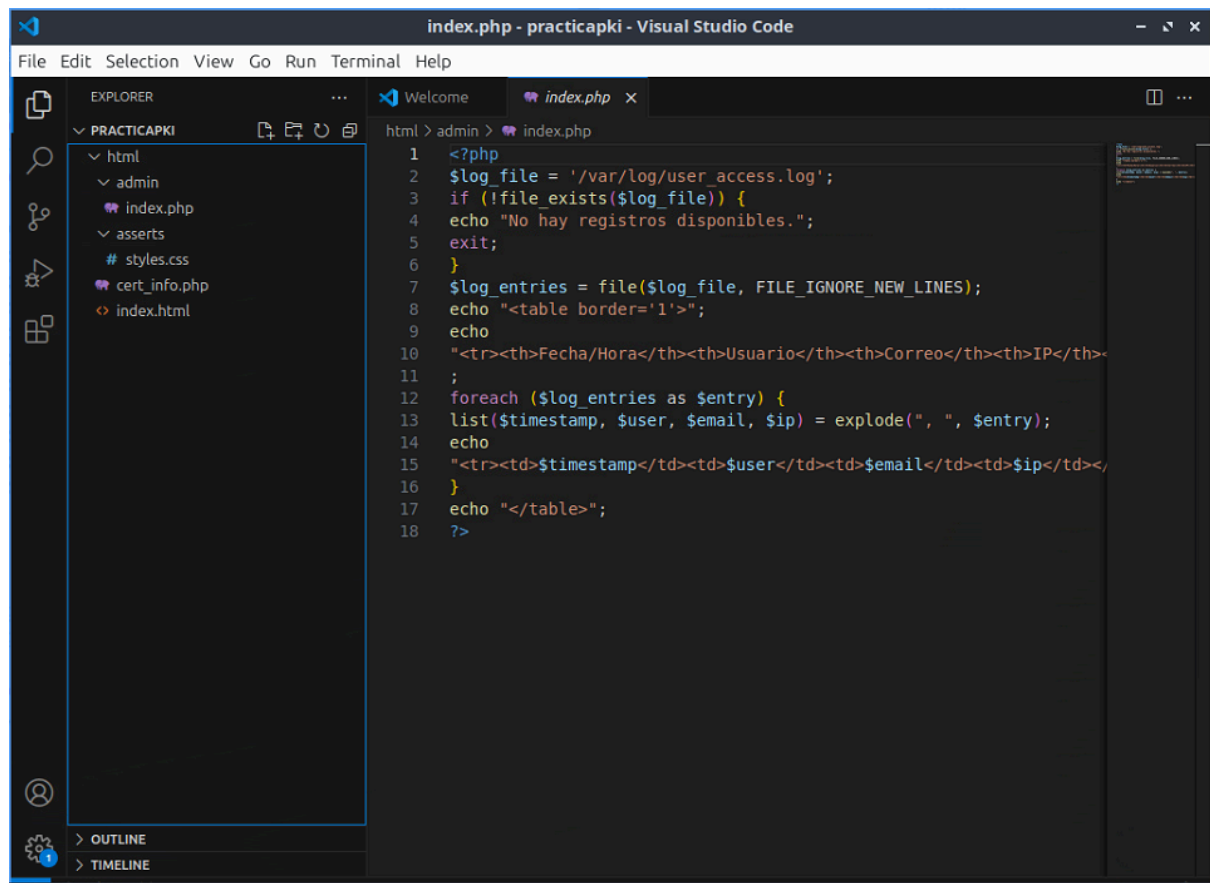
index.html
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Certificado de Cliente</title>
7   <link rel="stylesheet" href="./asserts/styles.css">
8 </head>
9 <body>
10   <header>
11     <h1>Bienvenido</h1>
12     <p>Este sitio requiere un certificado de cliente válido emi<
13   </header>
14   <main>
15     <p>Si tienes un certificado válido, accede a <a href="./cer<
16   </main>
17   <footer>
18     <p>&copy; 2024. Sistema PKI.</p>
19   </footer>
20 </body>
21 </html>
22
```

Aquí hemos añadido un nuevo index el cual esta cogido de github.



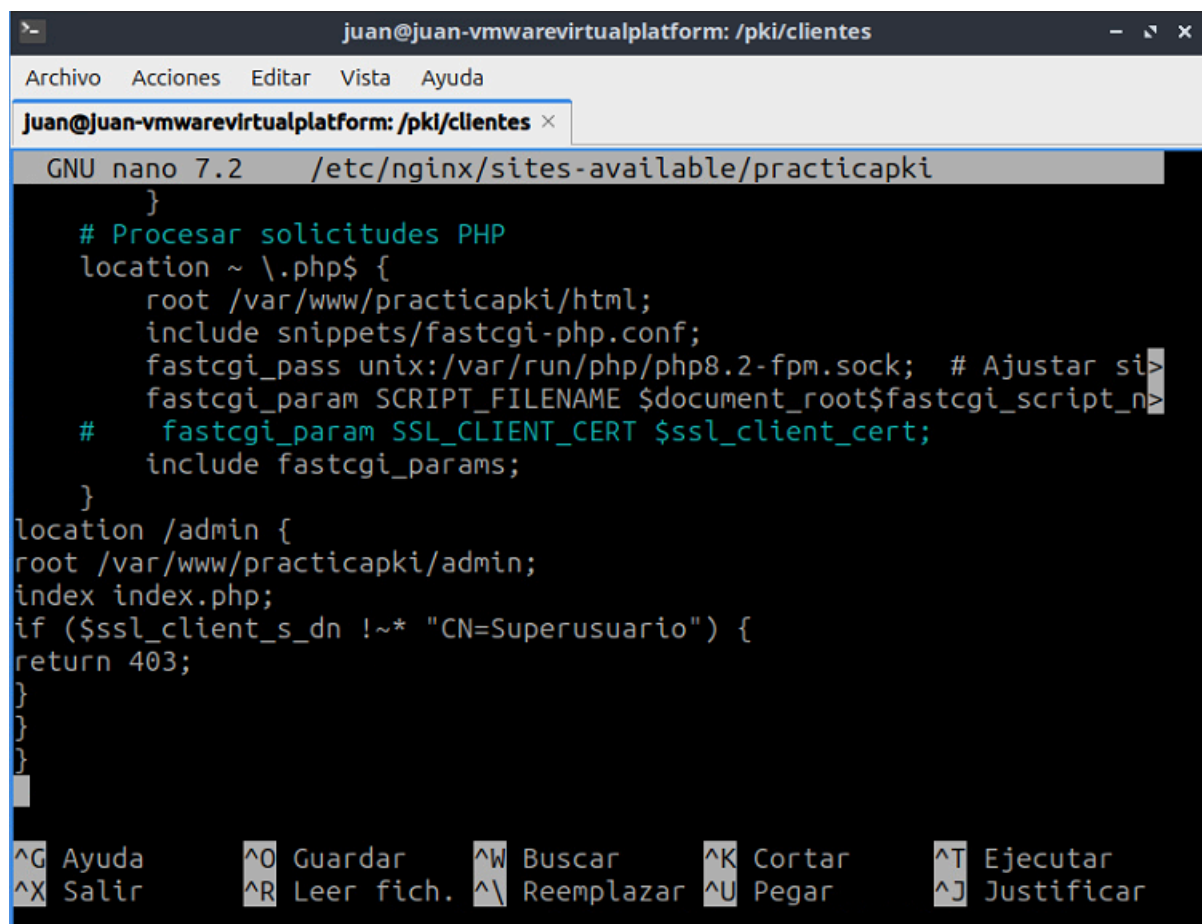
```
1  /* Reset de estilos básicos */
2  * {
3      margin: 0;
4      padding: 0;
5      box-sizing: border-box;
6  }
7
8  /* Estilo del cuerpo */
9  body {
10     font-family: 'Roboto', Arial, sans-serif;
11     background-color: #f4f4f9;
12     color: #333;
13     line-height: 1.6;
14     margin: 0;
15     padding: 0;
16 }
17
18 /* Encabezado */
19 header {
20     background-color: #2c3e50;
21     color: white;
22     padding: 20px 10px;
23     text-align: center;
24 }
25
26 header h1 {
27     font-size: 2.5rem;
28     margin-bottom: 10px;
29 }
30
31 header p {
32     font-size: 1rem;
33 }
```

con su css correspondiente.



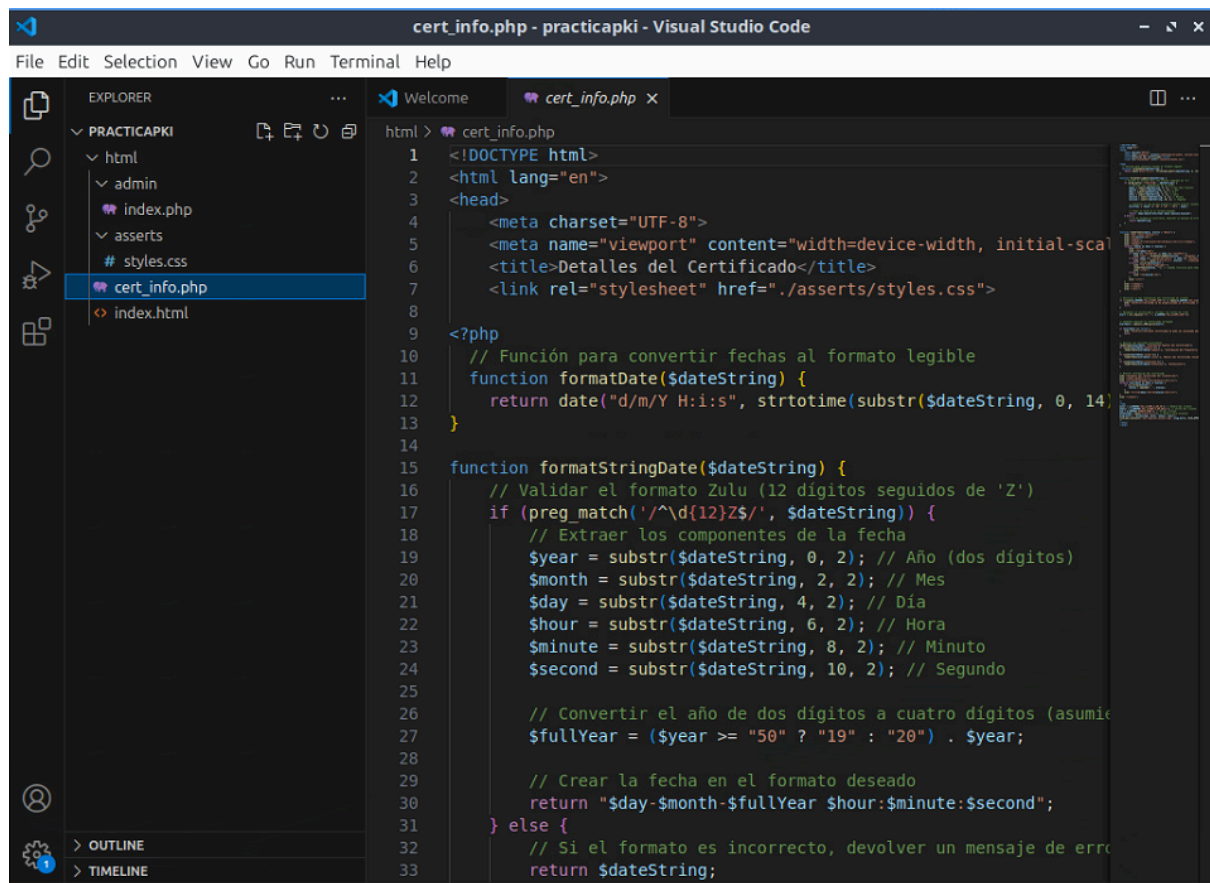
```
1 <?php
2 $log_file = '/var/log/user_access.log';
3 if (!file_exists($log_file)) {
4     echo "No hay registros disponibles.";
5     exit;
6 }
7 $log_entries = file($log_file, FILE_IGNORE_NEW_LINES);
8 echo "<table border='1'>";
9 echo
10 "<tr><th>Fecha/Hora</th><th>Usuario</th><th>Correo</th><th>IP</th><
11 ;
12 foreach ($log_entries as $entry) {
13     list($timestamp, $user, $email, $ip) = explode(" ", $entry);
14     echo
15     "<tr><td>$timestamp</td><td>$user</td><td>$email</td><td>$ip</td><
16 }
17 echo "</table>";
18 ?>
```

aquí añadimos por código php el cual es para solo permitir acceso al super usuario a la pagina.



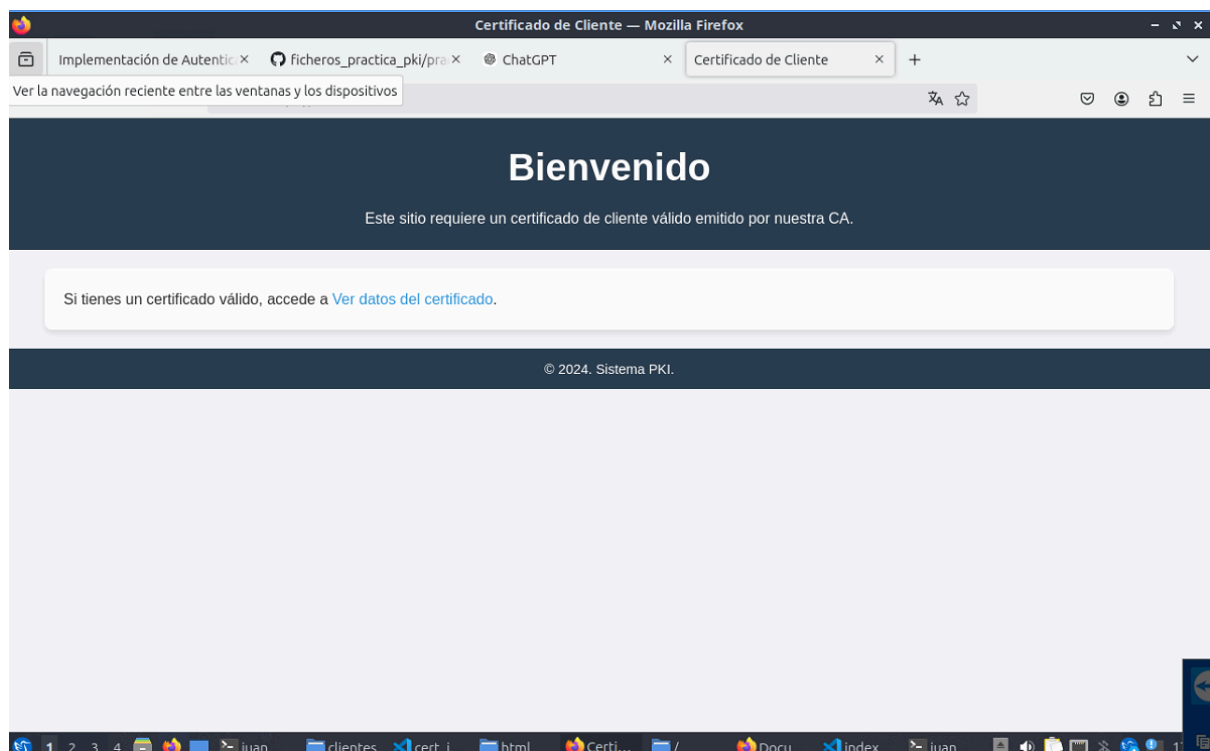
```
juan@juan-vmwarevirtualplatform: /pki/clientes
Archivo Acciones Editar Vista Ayuda
juan@juan-vmwarevirtualplatform: /pki/clientes x
GNU nano 7.2 /etc/nginx/sites-available/practicapki
}
# Procesar solicitudes PHP
location ~ /\.php$ {
    root /var/www/practicapki/html;
    include snippets/fastcgi-php.conf;
    fastcgi_pass unix:/var/run/php/php8.2-fpm.sock; # Ajustar si>
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_n>
    # fastcgi_param SSL_CLIENT_CERT $ssl_client_cert;
    include fastcgi_params;
}
location /admin {
    root /var/www/practicapki/admin;
    index index.php;
    if ($ssl_client_s_dn !~* "CN=Superusuario") {
    return 403;
    }
}
}
}
}
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar
```

se lo metemos al archivo practicapki para que lo pueda ejecutar



```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1">
6   <title>Detalles del Certificado</title>
7   <link rel="stylesheet" href="../asserts/styles.css">
8
9 <?php
10 // Función para convertir fechas al formato legible
11 function formatDate($dateString) {
12     return date("d/m/Y H:i:s", strtotime(substr($dateString, 0, 14)));
13 }
14
15 function formatStringDate($dateString) {
16     // Validar el formato Zulu (12 dígitos seguidos de 'Z')
17     if (preg_match('/^\d{12}Z$/', $dateString)) {
18         // Extraer los componentes de la fecha
19         $year = substr($dateString, 0, 2); // Año (dos dígitos)
20         $month = substr($dateString, 2, 2); // Mes
21         $day = substr($dateString, 4, 2); // Día
22         $hour = substr($dateString, 6, 2); // Hora
23         $minute = substr($dateString, 8, 2); // Minuto
24         $second = substr($dateString, 10, 2); // Segundo
25
26         // Convertir el año de dos dígitos a cuatro dígitos (asumiendo el siglo 21)
27         $fullYear = ($year >= "50" ? "19" : "20") . $year;
28
29         // Crear la fecha en el formato deseado
30         return "$day-$month-$fullYear $hour:$minute:$second";
31     } else {
32         // Si el formato es incorrecto, devolver un mensaje de error
33         return $dateString;
```

y ahora le añadimos un código el cual sirve para mostrar los datos del certificado con el que se ha entrado



y así se vería la nueva página con su enlace para mostrar los datos del certificado. Y solo hemos podido entrar con el superusuario.