**Diseño de un sistema de gestión de productos e inventario para cafetería**

Brayan Alberto Silva Cabra

Javier Mauricio Rodríguez Dueñas

Grupo G

Universidad del Norte

Barranquilla

Programa Misión Mintic 2022

21 de diciembre de 2020

1. **Integración de la aplicación con Amazon Web Services y Certificados SSL**

**1.1 Nombre del Proyecto**

Desarrollo de un sistema de gestión de productos e inventario para cafetería

**1.2 Credenciales de Acceso para acceder a las funciones de la aplicación**

Para acceder a cada una de las funcionalidades del sistema se tiene que garantizar que es un usuario registrado ya sea como Administrador o como Cliente. De esta manera, si se proveen las siguientes credenciales se garantiza un correcto inicio de sesión a la aplicación a través de la IP pública [**https://54.242.231.31/**](https://54.242.231.31/) **:**

|  |  |
| --- | --- |
| **Administradores**  **Id de Usuario:** elpepe  **Clave:** Uruguay11  **Id de Usuario:**memito  **Clave:** Venezuela987 | **Usuarios**  **Id de Usuario:** elJoe  **Clave:** Bolivia345  **Id de Usuario:** LaPaquis  **Clave:** Chile567 |

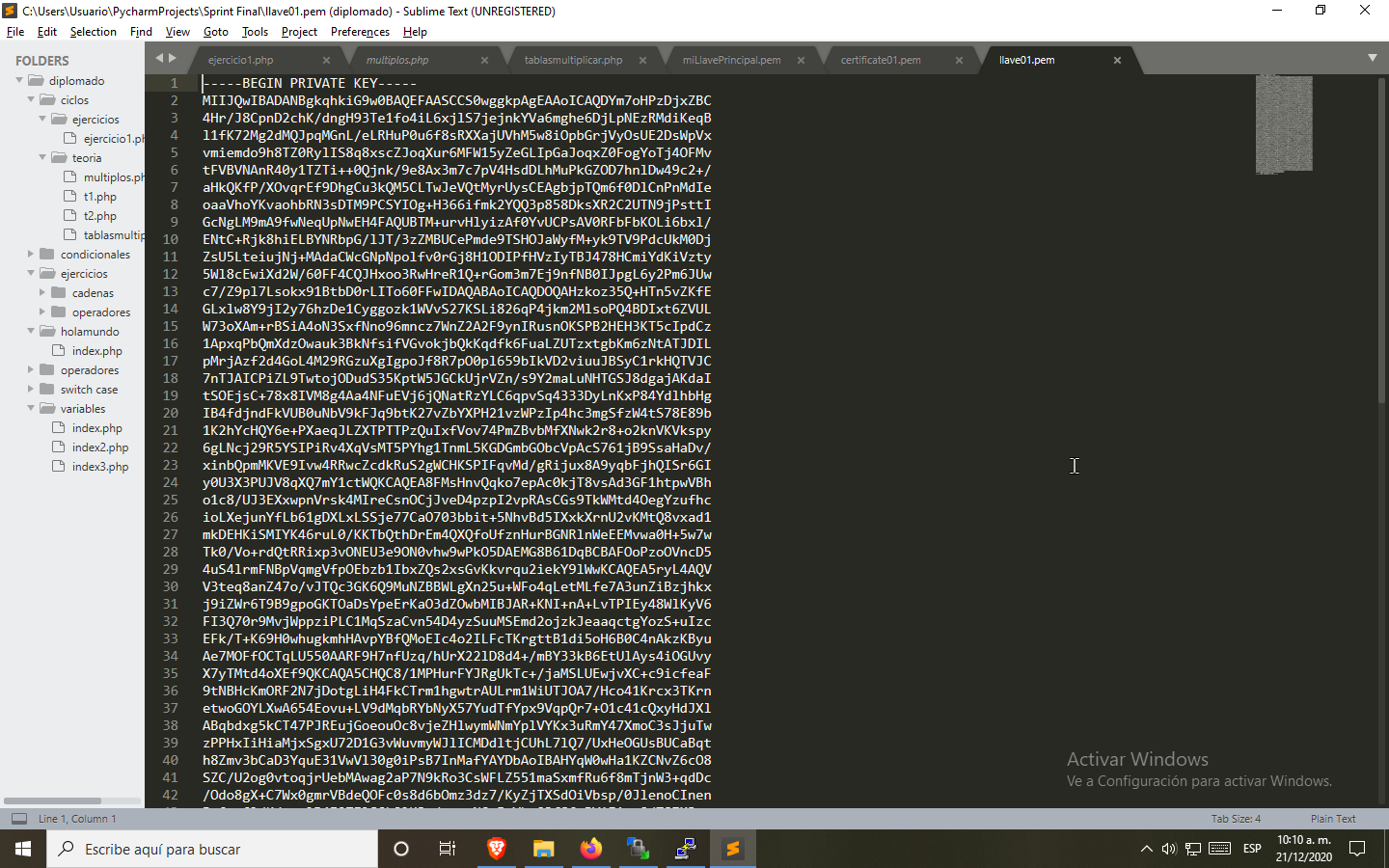
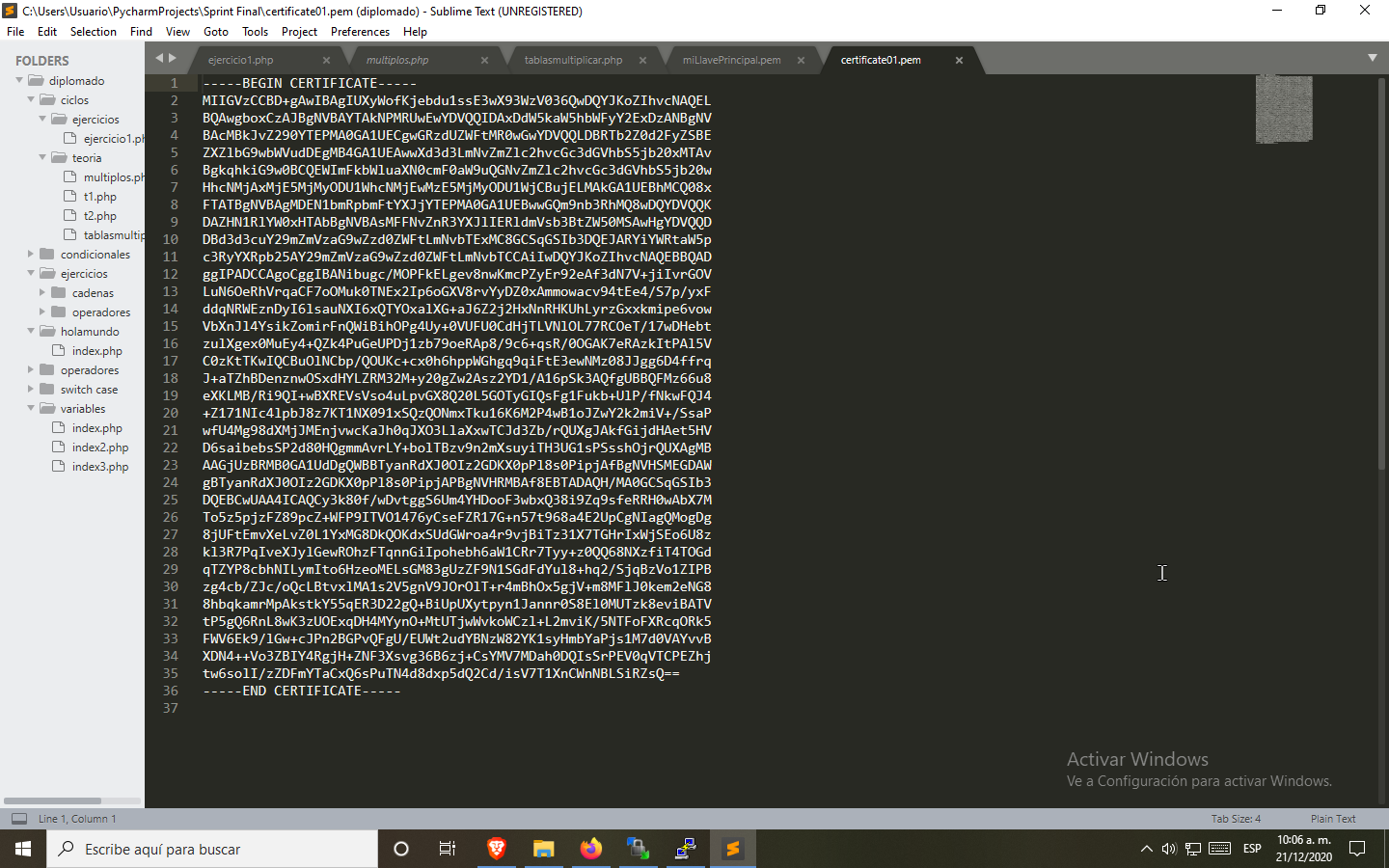
Estas credenciales deben ser ingresadas en la página de inicio tal como se muestra acá:



**Figura 1 -** Login del sistema

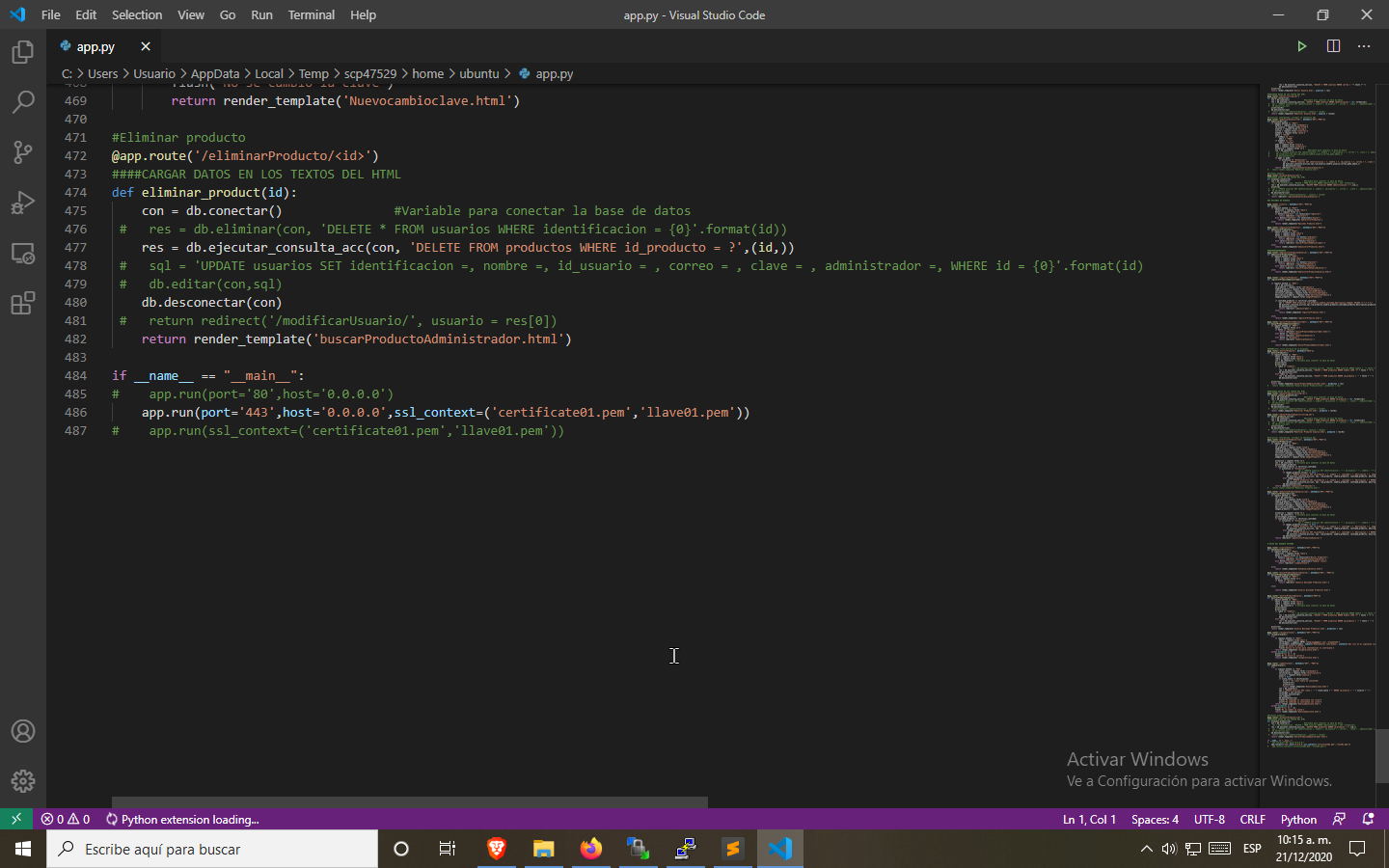
**1.3 Protocolo HTTPS y Certificado SSL**

Para garantizar la seguridad de la conexión del usuario con la aplicación se generó un certificado SSL (certificate01.pem) con su respectiva llave privada (llave01.pem) tal como se muestra a continuación:

****

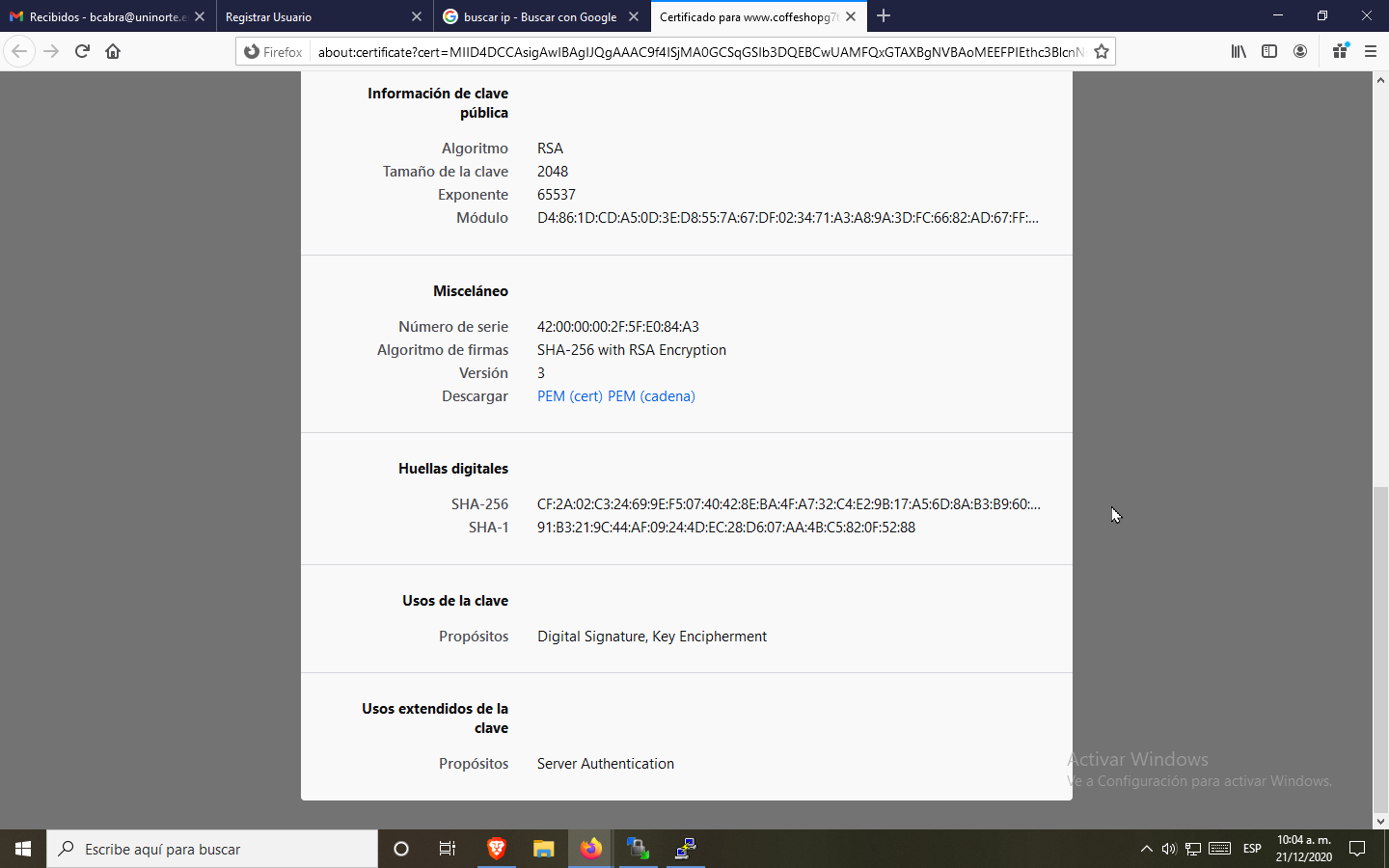
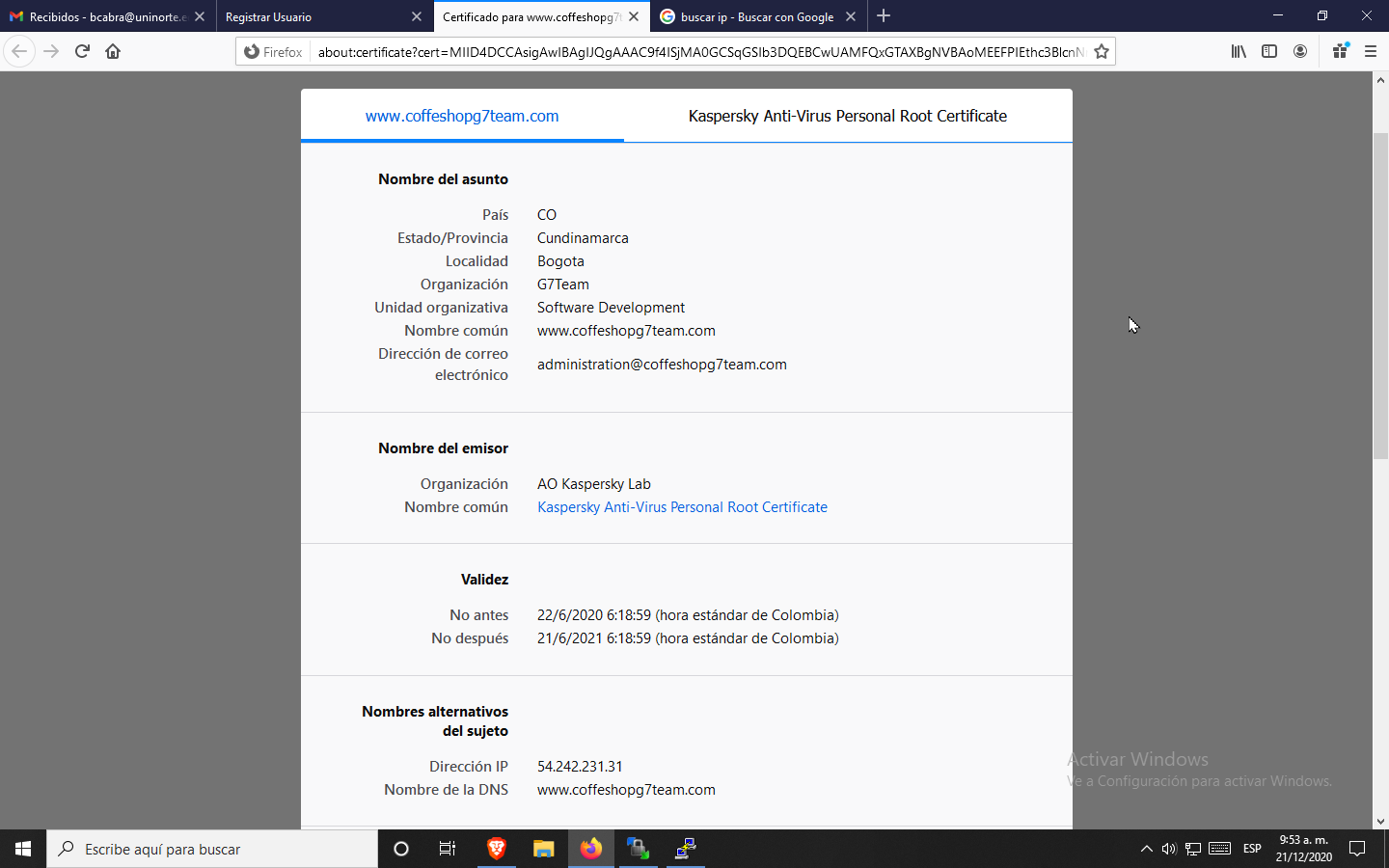
**Figura 2-** Certificado SSL  **Figura 3 -** Llave privada

Posteriormente dichos archivos fueron integrados a la aplicación principal “app.py” , asisgnando el puerto 443, con sus respectivos certificado y llave:



**Figura 4-** Integración de certificados de seguridad en la aplicación

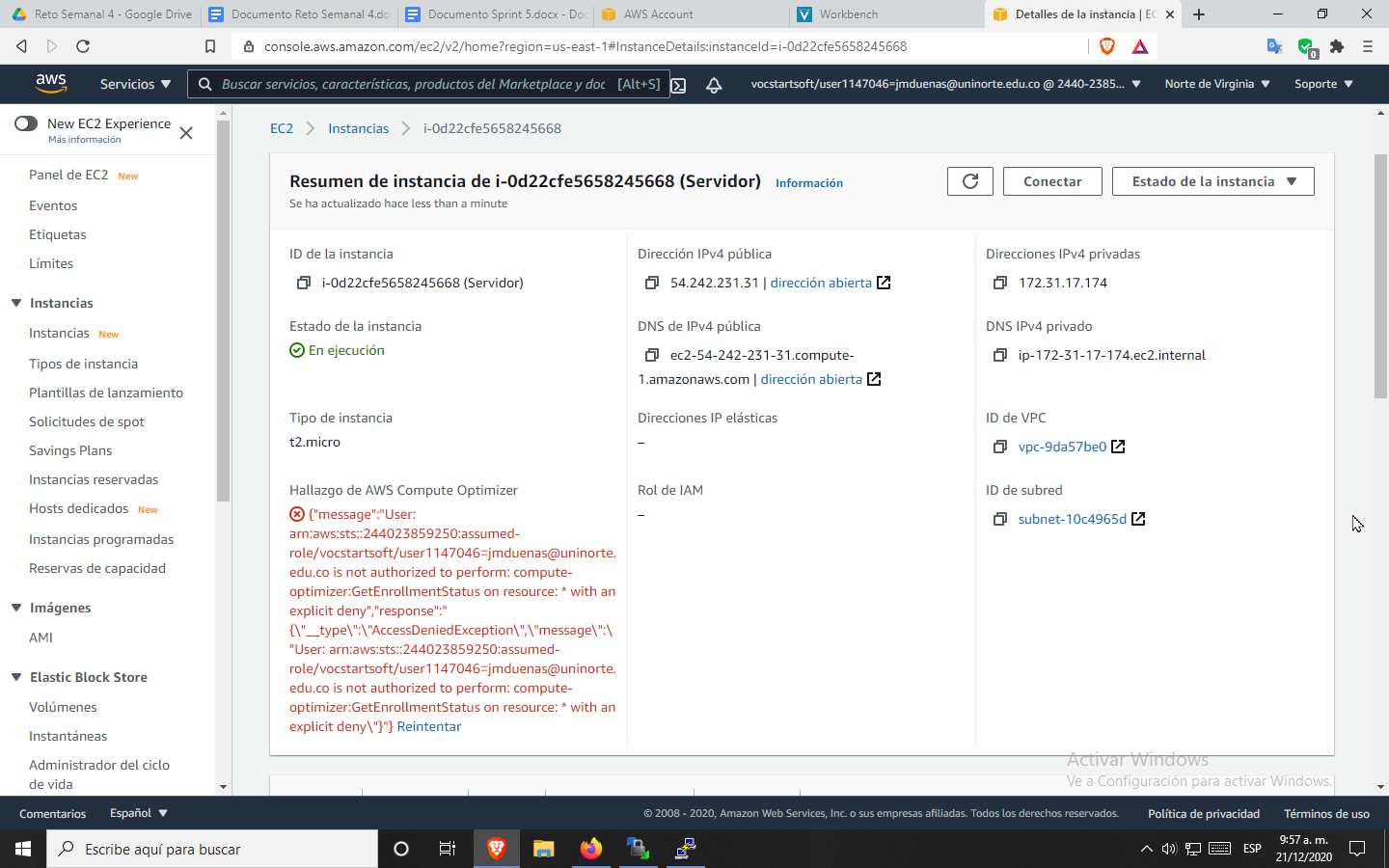
De esta manera, al ingresar a la dirección IPv4 IP Pública**:** [**https://54.242.231.31/**](https://54.242.231.31/) se puede ver el certificado generado por el navegador:

****

**Figura 3 -** Certificado de conexión segura del navegador

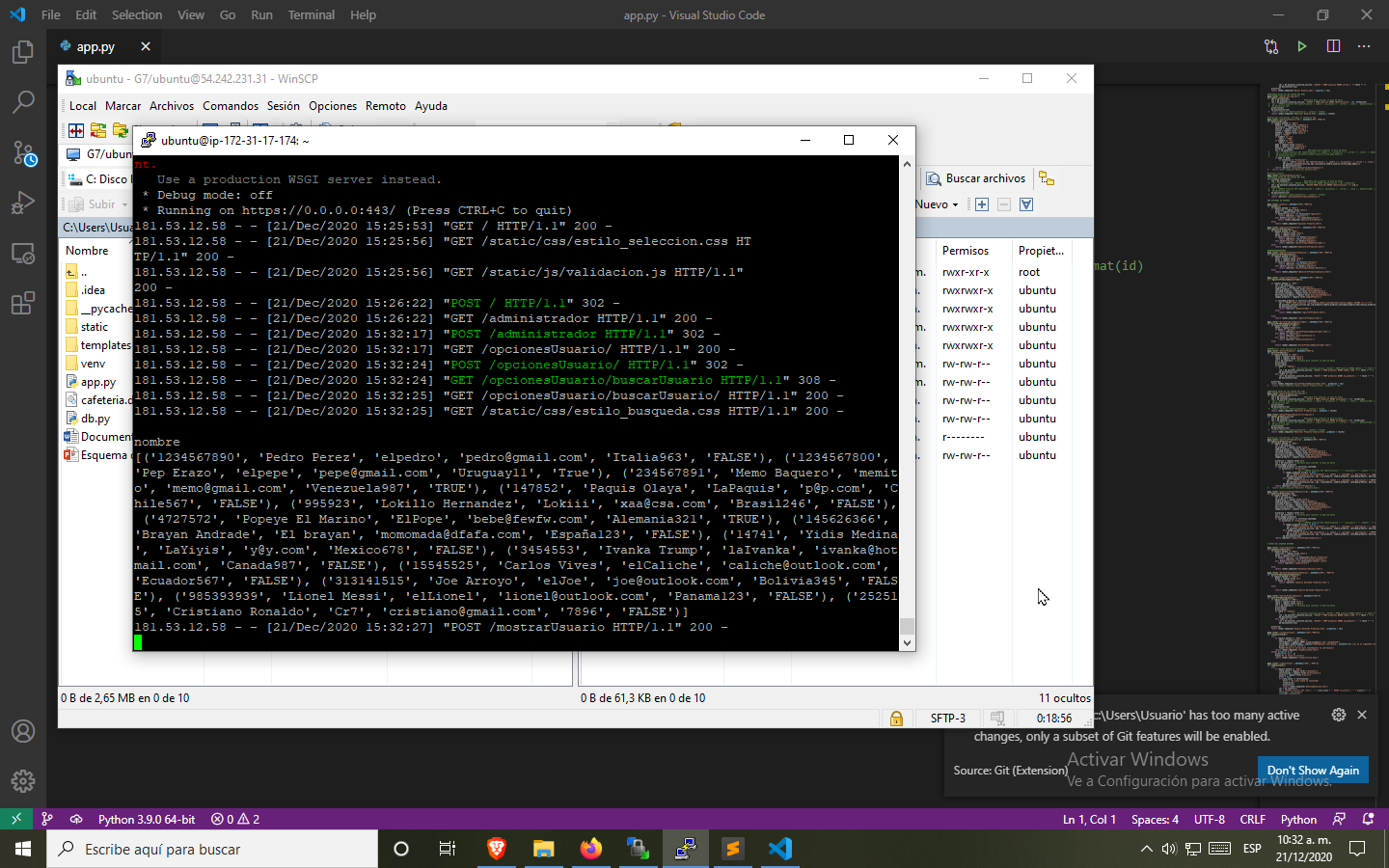
**1.4 IP Pública y Resumen de la Instancia en el Servidor**

La aplicación está disponible en la dirección IPv4 pública [**https://54.242.231.31/**](https://54.242.231.31/)**,** teniendo en cuenta que al conectarse por primera vez aparecerá un mensaje de sitio web no seguro, se debe seleccionar la opción de continuar de todos modos, y a continuación se pueden ver algunas características generales de la instancia en Amazon Web Services:

****

**Figura 4 -** Resumen de la instancia en Amazon Web Services

De esta manera, cualquier persona a través de la IP especificada puede acceder a los servicios de nuestra aplicación siempre y cuando se encuentre registrada o tenga la autorización del administrador; igualmente nosotros podemos hacer seguimiento a cada una de las peticiones realizadas y verlas por consola tal como se muestra a continuación:



**Figura 4 -** Seguimiento de peticiones HTTPS a través de consola

Para subir los archivos HTML y demás componentes de nuestra aplicación, se utilizó una herramienta llamada WinSPC, para conexión remota mediante protocolo SSH a través del puerto 22, de manera que gracias a su interfaz visual, se subieron los archivos de forma fácil al servidor AWS, cuyo equipo quedó configurado con sistema operativo Ubuntu.

Para la conexión desde el WinSPC al equipo configurado en el servidor AWS, se procedió a crear una llave pública Openssh con extensión pem, la cual tuvo que convertirse luego a extesión ppk, ya que los comandos de funcionamiento para configuración del servidor se hacen a través de una consola de comandos con Putty.