OFICINA DE TECNOLOGÍAS DE INFORMACIÓN DEL CONCYTEC

Software DSPACE-v6.3

Habilitar https

Historial de Versiones

Fecha	Versión	Descripción	Autor
28/09/2021	1.1	Elaboración del Documento	Vilialdo Mancisidor

Revisado y Aprobado por:

Nombre	Rol	Firma
Juan Manuel Rojas	Jefe OTI	
Mirtha Quipas	Coordinador de desarrollo	

Contenido

PROCEDIMIENTO DE CONFIGURACION Y PERSONALIZACION DE REPOSITORIO INSTITUCIONAL

1. INTRODUCCIÓN

DSPACE, que es una aplicación informática de código abierto, utilizado como estándar por CONCYTEC para la implementación de repositorios digitales en las instituciones peruanas, los cuales formaran parte de la red de repositorios del país a través de la Plataforma de código abierto ALICIA.

2. OBJETIVO

Por el presente documento, se comparten los lineamientos necesarios para realizar la configuración y personalización del Dspace.

3. ALCANCE

El procedimiento es de alcance del SINACYT.

4. PROCEDIMIENTO

Antes de iniciar los trabajos de configuración y personalización del repositorio, asegúrese de implementar un servidor con las características mínimas de hardware indicados a continuación, esto con la finalidad de que no se presenten problemas y/o conflictos durante la ejecución de los pasos.

Una vez se cuente con el hardware solicitado, se deberán de ejecutar los pasos en el orden indicado en la presente guía.

4.1. Características técnicas

Características mínimas de hardware

Memoria	3-4 GB.
CPU	Cualquiera, pc o servidor
Almacenamiento	20 GB

Software usado para la elaboración de la guía

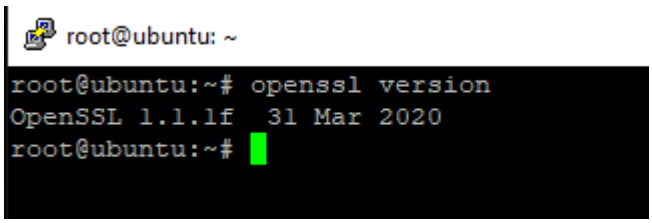
SO	Ubuntu 20.04.2 LTS
Base de datos	PostgreSQL 12.7
Java	openjdk version 1.8.0_292
Maven	Apache Maven 3.6.3
Ant	Apache Ant(TM) version 1.10.7

4.2. Pasos para configuración y personalización

Habilitar https

1. Verificar que la librería openssl está instalada. (Por defecto viene pre instalada en Ubuntu)

   Comando
   openssl versión



2. Crear una carpeta para almacenar todos los archivos de los certificados (Llave privada, csr, crt)

   Comando
   mkdir /etc/encryption

3. Crear:
   - ✓ Una llave privada (private key)
   - ✓ Una solicitud de firma de certificado (CSR: Certificate Signing Request)

   Comando
   sudo openssl req -new -newkey rsa:2048 -nodes -keyout /etc/encryption/server.key -out /etc/encryption/server.csr

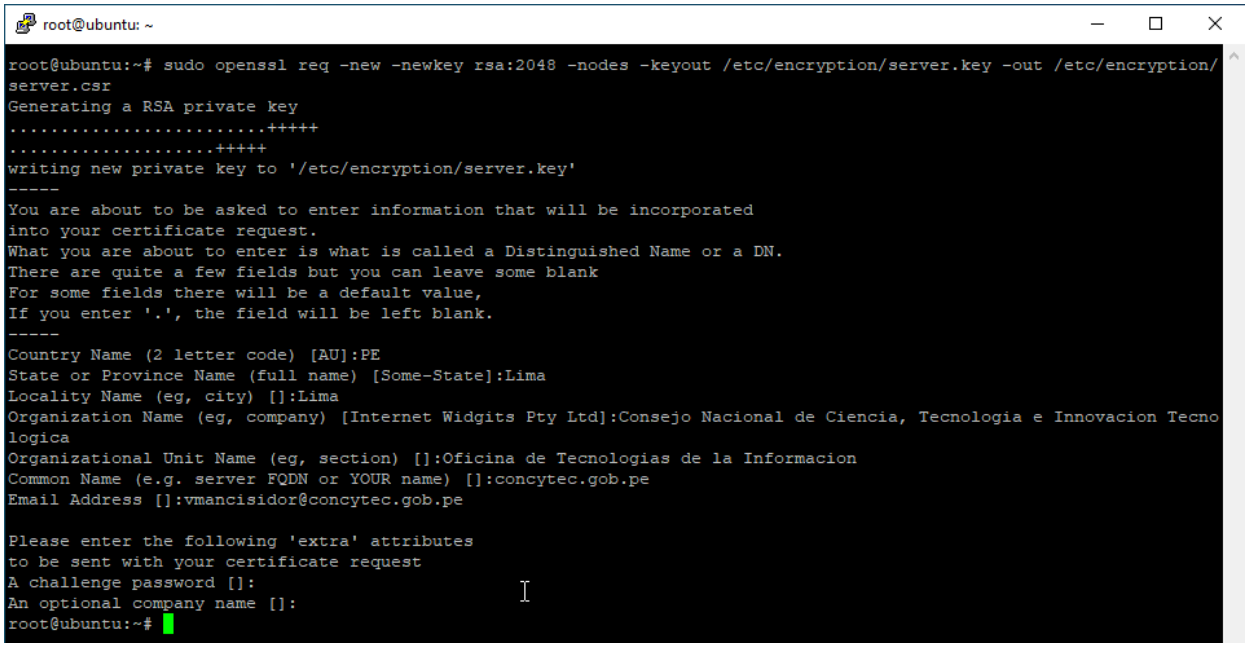
   Al ejecutar el comando anterior se nos van a realizar las siguientes preguntas:

   - ✓ Country Name (2 letter code) [AU]:PE
     Abreviación de dos letras para el país

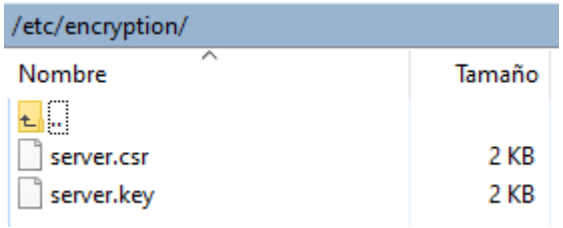
- ✓ State or Province Name (full name) [Some-State]:Lima
  Nombre completo del departamento
- ✓ Locality Name (eg, city) []:Lima
  Nombre de la ciudad
- ✓ Organization Name (eg, company) [Internet Widgits Pty Ltd]:Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica
  Nombre de la entidad
- ✓ Organizational Unit Name (eg, section) []:Oficina de Tecnologías de la Información
  Nombre de la unidad organizativa
- ✓ Common Name (e.g. server FQDN or YOUR name) []:dev-dspace.concytec.gob.pe
  Nombre del dominio o subdominio de la entidad
- ✓ Email Address []:vmancisidor@concytec.gob.pe
  Correo electrónico de contacto

Preguntas adicionales:

- ✓ A challenge password []:
  Dejar en blanco y presionar enter
- ✓ An optional company name []:
  Dejar en blanco y presionar enter



4. Verificar la creación de la llave privada y de la solicitud de firma de certificado (CSR)



Comando

nano /etc/encryption/server.csr

root@ubuntu: ~

```
  GNU nano 4.8                                  /etc/encryption/server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDNTCCAh0CAQAwge8xCzAJBgNVBAYTAlBFMQ0wCwYDVQQIDARMaWlhMQ0wCwYD
VQQHDARMaWlhMUkwRwYDVQQKDEBDb25zZWpvIE5hY2lvbmFsIGRlIENpZW5jaWEs
IFRlY25vbG9naWEgZSBJbm5vdmFjaW9uIFRlY25vbG9naWNhMTEwLwYDVQQLDChP
ZmljaW5hIGRlIFRlY25vbG9naWFzIGRlIGxhIEluZm9ybWFjaW9uMRgwFgYDVQQD
DA9jb25jeXRlYy5nb2IucGUxKjAoBgkqhkiG9w0BCQEWG3ZtYW5jaXNpZG9yQGNv
bmN5dGVjLmdvYi5wZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKtD
Ti8mWl4P5pZDOO0LbQwcj4Eb4ic+p0ieKdc3pZmolBAsKou+lO5IqbJgqbHDW343
+Payt3bB3mfWnsgqaB04DYjhNcQVZ3iAuTgJChzuz/F+PKRRray6WaTplTVqX29Z
DtNyfbYlwwLXU+VfUNIC9MEUGCs9BY9XpozoO39bRLkXivUL9+0RbBP/dMElirIc
6Zl2mbrdmLF8bebr6+BCUU+Vlr8fl/l5J+O65JyvfohLpuKyMlr0Nj7q+5z2UBc4
qnK7ytUtLlGYukch4J7juPDxnwG89V0QKh3JiNH7EsH5rw6P5Q9/pI+OFBd4HRqh
RwQpg/ZZxFZh8Ga+0hcCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQA45sImIb7z
br/P36Gl0SIiuAHXnA0vs6f4rSMax6jNC8aTPp/OSCGet3ZqakcohVkJjI8SQVOX
fWHPj3WHXplfQpCqj2J0Cv9yxAhmDP0Wlf42TMuj2v4Pz7DGEYmdXGJjxRHFpauA
DiXsrMavuLhc0ElMiScFbCn+wWC9jBIZDJJY3dWyhA/+0CzVtVzGNFRRN3+/oTn0
WPvDnmeyHm7/vofW7OmZ0g56eZnlwXlNQ5DRFlOuRjKGAwU5IHygv+2UpNzkZwCy
9AjCHi+nYaJQLnAH44L8YlyT4DMX0WGHTwduXlpAQC1km7fFuo034FuBnWX2s+Qe
jzuBV22QdR2A
-----END CERTIFICATE REQUEST-----
```

Comando

nano /etc/encryption/server.key

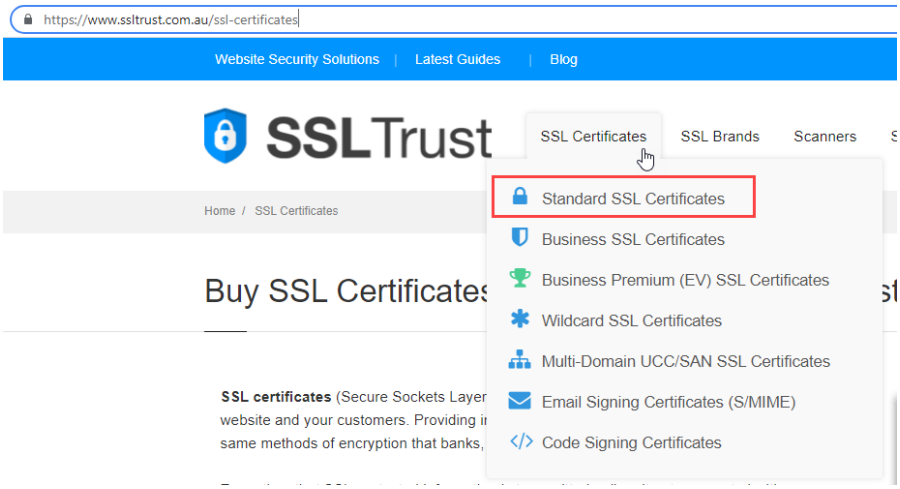
root@ubuntu: ~

```
  GNU nano 4.8                                  /etc/encryption/server.key
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQCrQ04vJlpeD+aW
QzjtC20MHI+BG+InPqdIninXN6WZqNQQLCqLvpTuSKmyYKmxwlt+N/j2srd2wd5n
lp7IKmgdOA2I4TXEFWd4gLk4CQoc7s/xfjykUa2sulmkz5U1al9vWQ7Tcn22JcMC
llPlXlDSAvTBFBgrPQWPV6aM6Dt/W0S5F4rlC/ftEWwT/3TBNYqyHOmZdpm63Zix
fG3m6+vgQlFPlZa/H5f5eSfjuuScr36IS6bisjJa9DY+6vuc9lAXOKpyu8rVLS5R
mLpHIeCe47jw8Z8BvPVdECodyYjR+xLB+a8Oj+UPf6SPjhQXeB0aoUcEKYP2WcRW
YfBmvtIXAgMBAAECggEAcpuy6Yif9sxrQekwYilASledjQfs2thpuAXn+BdMIblC
VKRJwITEQ4Wq0i0vwj76rkekuuq0LavlOtX8IfWHAO6u2AfmJBcyzAhQarhZ5SzH
SVNyH4BtWebG8KzdrAZIYUpWypeWmttAWllg0mFrw26o/cCFwAGxA9DjKu6KSlnf
sGuv/SzaQIRDYllwHRcvpXDKmGCwINByVUOW8AY/Ls8XpA76kbQu6dtkoGaD03cC
z3JOXlL0uKk6hsEaW3UorxYmfj3uzDeTkurDYl+5ptq9u4XgUChBhhSxOsU9zewk
ziFm6Y8z7EwFwPal/LaHk75QE3ydlapVe5BljBgd8QKBgQDeN+E3IAmGNOcDJMQI
AetQ8JVIZmpCC23h7n2kpPLVa6cbyCqTEgBfDPnm+JtlZSIqTrVRw5eVQwvWwllO
yFoZNCF92F0Ho7NZHjDXuumcsUWHpWgwzootoIzwLruftkxpmWB4iRYBCFvjzPo7
ws167/muhBbMlIlelNP0ypwwHwKBgQDFTGI/6SGSPepIlNJOen9SZxGjJGaxXsZ2
/hRReExde0zFzJWsqGgwYkKFYjSpsBiXFjycV77sYzOQ6uo2X7fdOhsd5B6/BlBW
dLFAF9gFsGhCemTZmPo7U9nn/Tlk3dIHmKWyyewClRx3yLjA7u2DjJXRGTZs2MZQ
NnXCDWa/CQKBgQCMr037S2IcQFPczqL4+tYS2Sl5t7Uf+QJpHkcXPIKskUorsY8a
qzPm+V0hWFV7fjqiFFCA4laOXfMZlXUuBnPcLv/hH2DOXFpIWm/LtH7//88oMJUF
CU2700BHMx7/3zcDR+ImjYuLvdIHJ5dozEywv0sQrHmOliZmWlGSUc+OOwKBgQCN
b417LV/wm0wJTg5ZTflaECMXpa+sdTmm8cuU/70Wwp4tqdSeWneeP8JaJiWEg4WN
QdafaVOn2BGOUKkn44RGJjJsQi08WYVcBPlP7gfhRC3pgh4r0zuHLjwmz2PGiDHZ
WjdmrNPwof4vbIftXxqLVEvOAtn+O4Qm2nOeccb3KQKBgQC6ke/xH4Se9LlhqnGt
2lmQt+6IDv6iYWBzBuAslbSvf7rolUQZ0WdhZBZWIiM25aIWKsU93AxytWDmlYga
AGQ8lLWhcl4PtV8+w2w2+9/lPbSoLCmZ2tQKHXQjHe2EBbMdVJGUY6+RRZAJB+a9
gWSYrZMiJHHTlsOi8l5tOrezsA==
-----END PRIVATE KEY-----
```

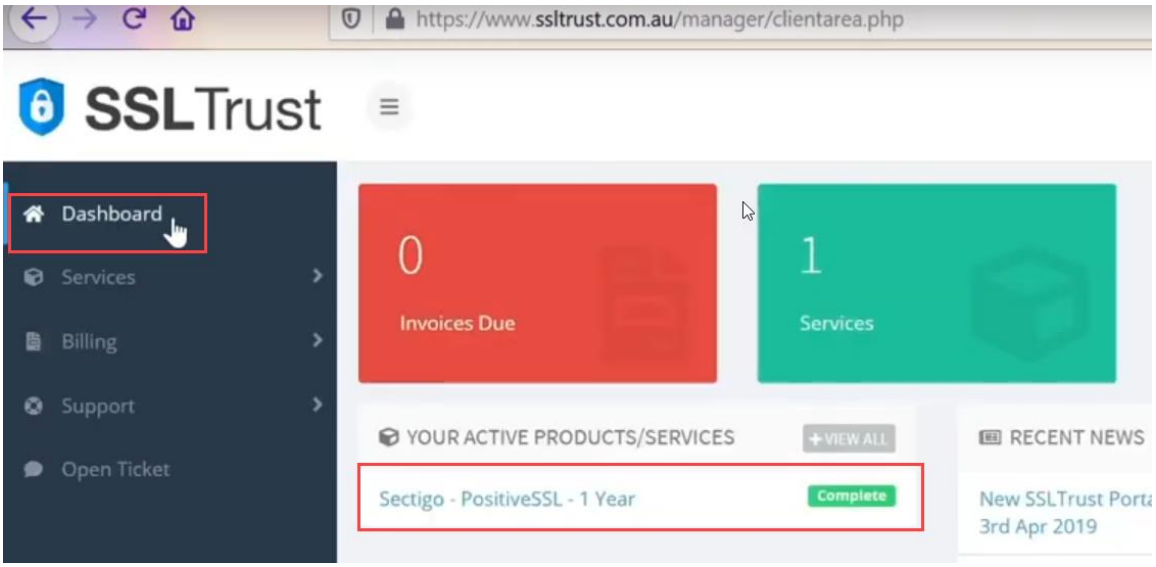
5. Comprar un certificado SSL. Por ejemplo, puede revisar la página del siguiente proveedor de Certificados:

   https://www.ssltrust.com.au/ssl-certificates

Existen varios tipos de certificados, para este ejemplo vamos a usar el Certificado Estándar



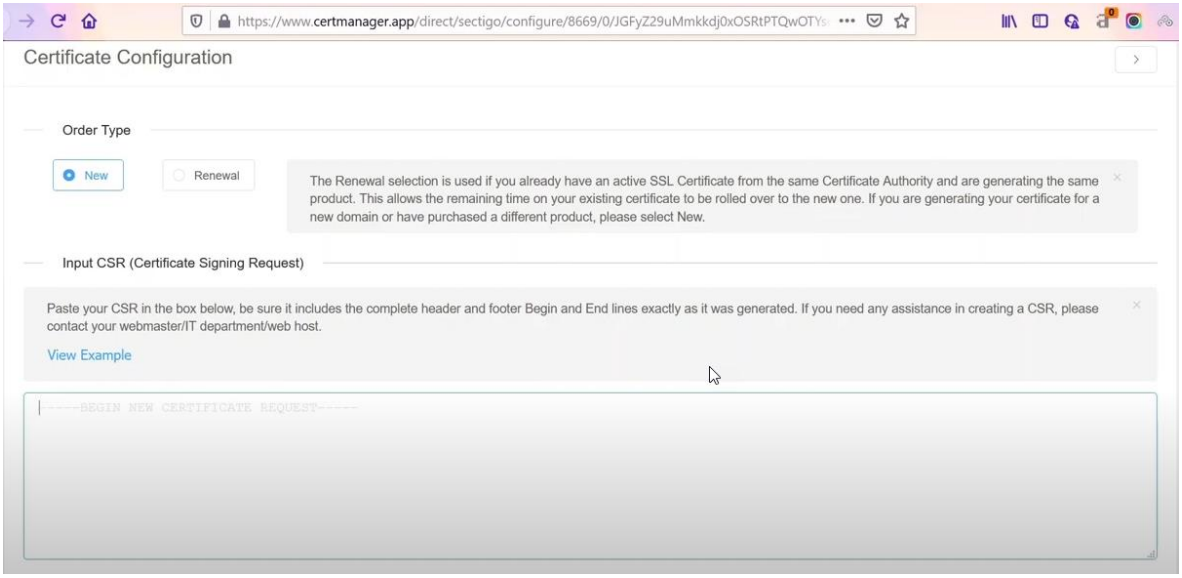
Una vez haya realizado el pago del certificado, el proveedor que eligió le habilitara un acceso a su página web para que realice la configuración del certificado.

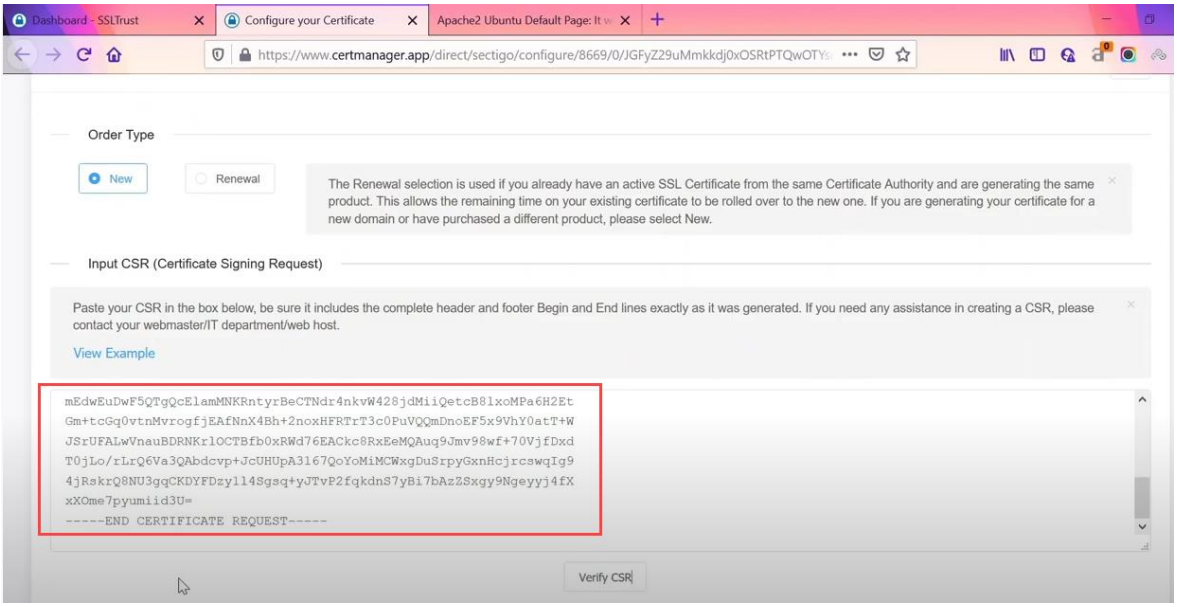


6. En el panel de control que su proveedor de certificados le habilitó, tendrá que realizar las siguientes actividades para que su certificado este habilitado.

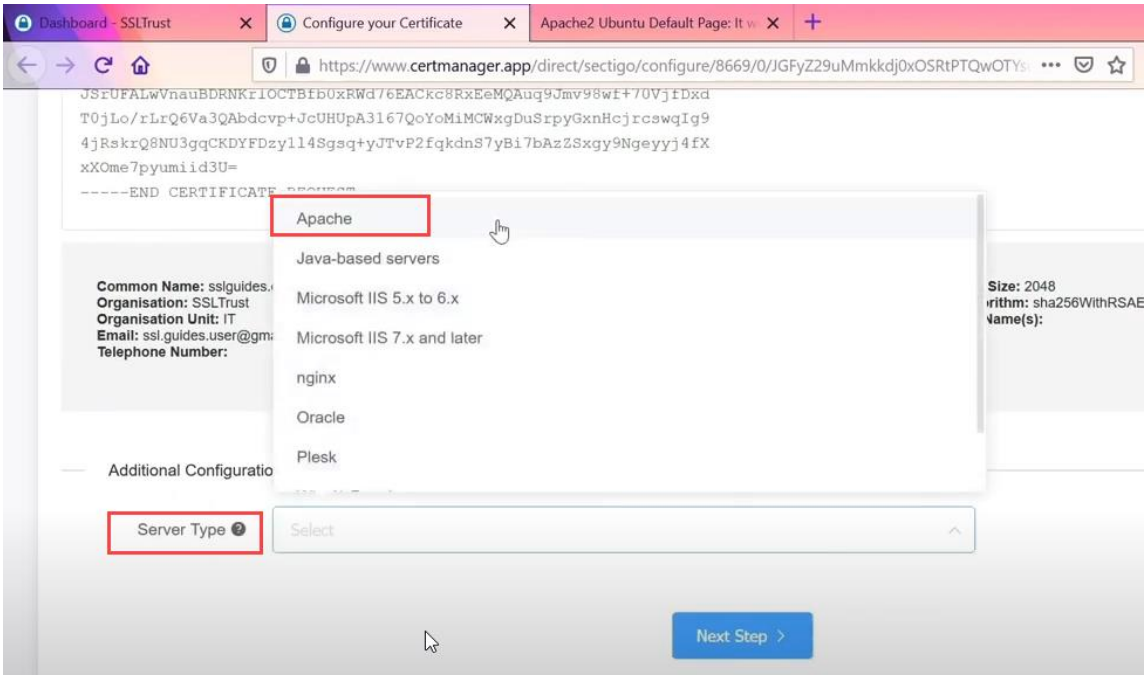
   ✓ **Registrar la configuración del certificado.**

   Esto se realiza registrando el contenido del archivo **server.csr** creado en el punto 3.

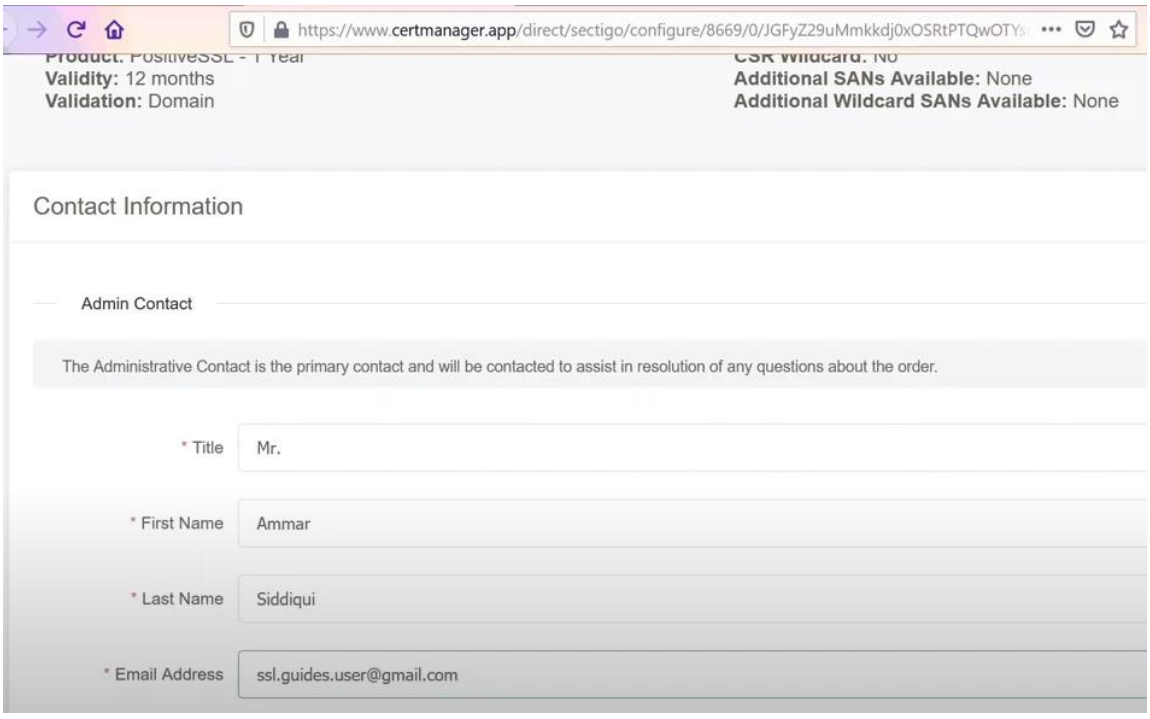




Se selecciona el tipo de servidor en donde será usado el certificado, en este caso será Apache.

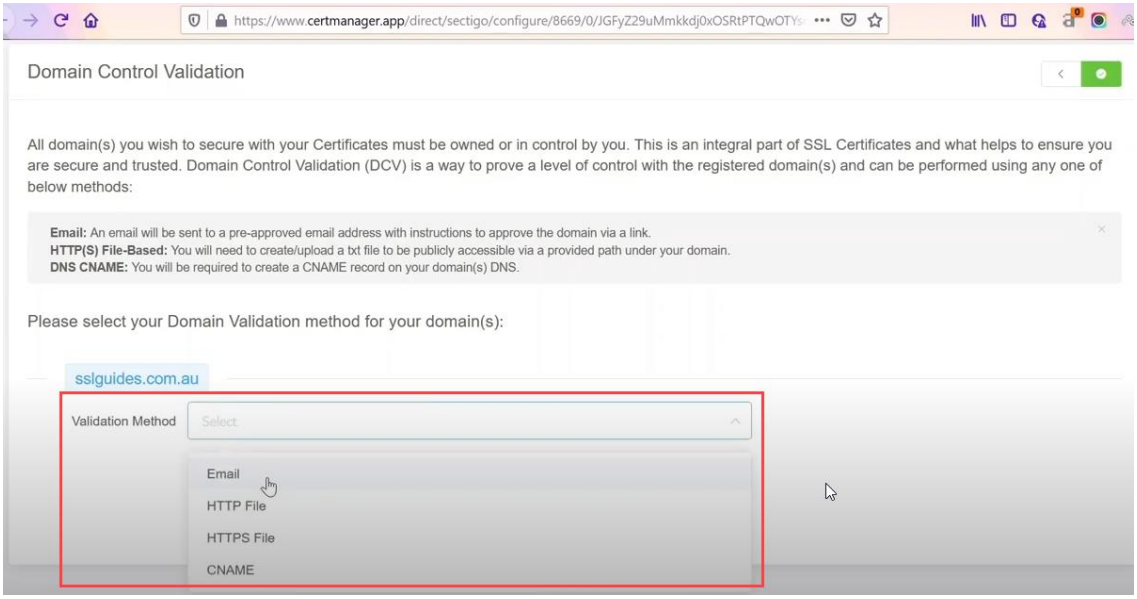


Por último, se registran los datos del administrador del certificado.

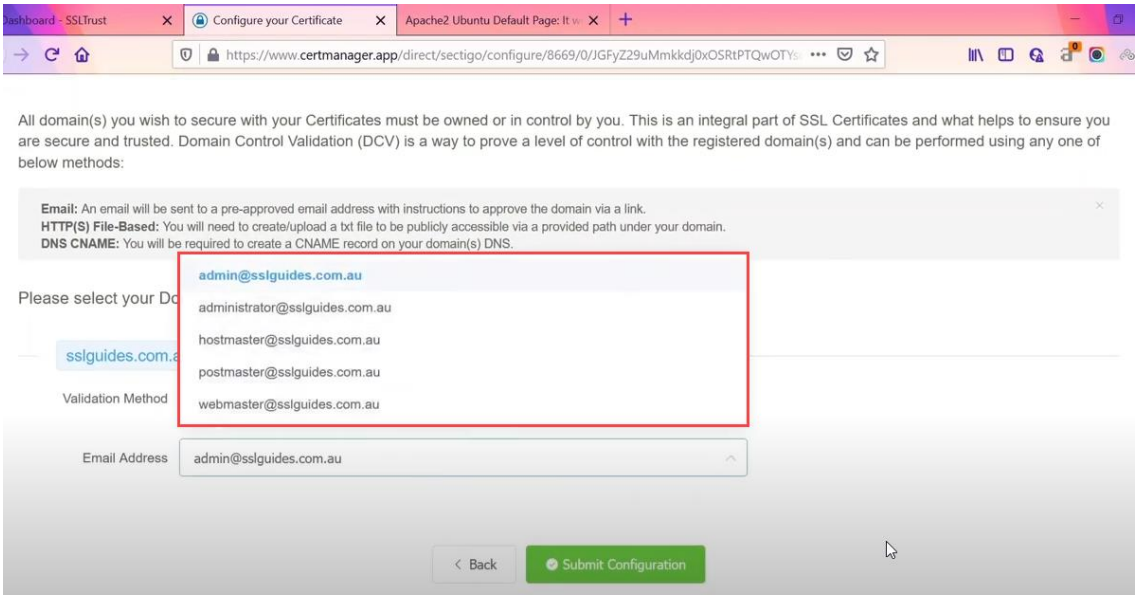


- ✓ **Validar que usted es el dueño o administrador del dominio que se quiere asociar al certificado**

Existen 4 métodos para realizar la validación, el más sencillo es Email

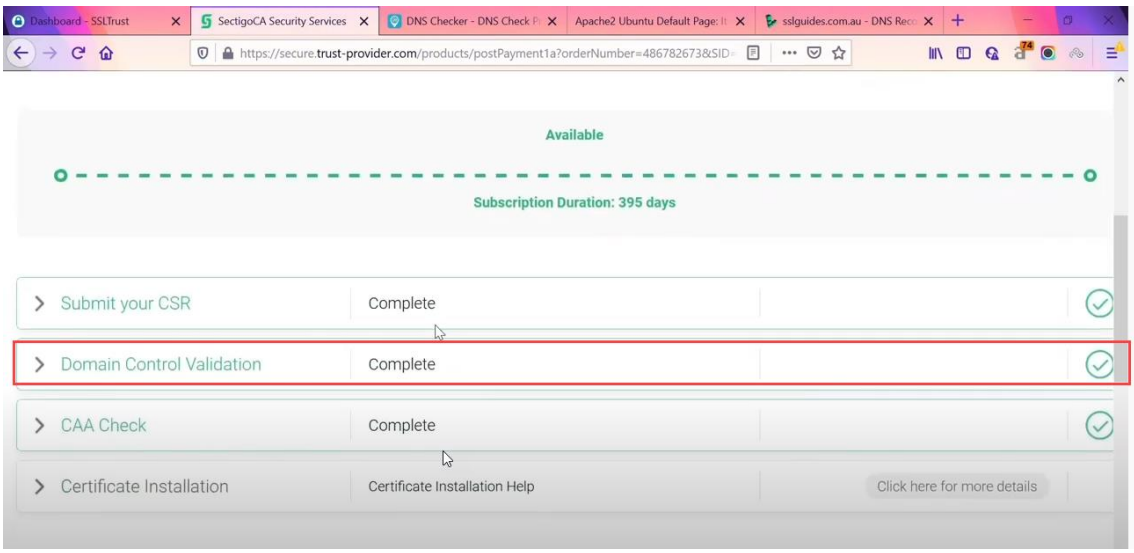


Se debe seleccionar del listado el correo del administrador de su dominio. Por ejemplo: admin@concytec.gob.pe

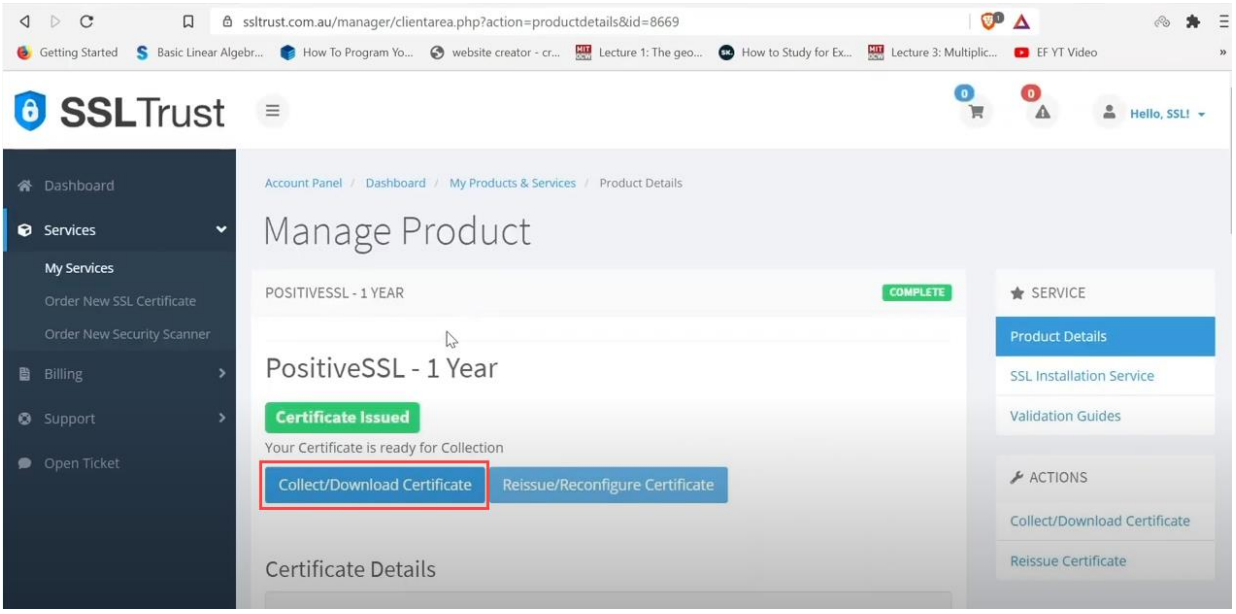


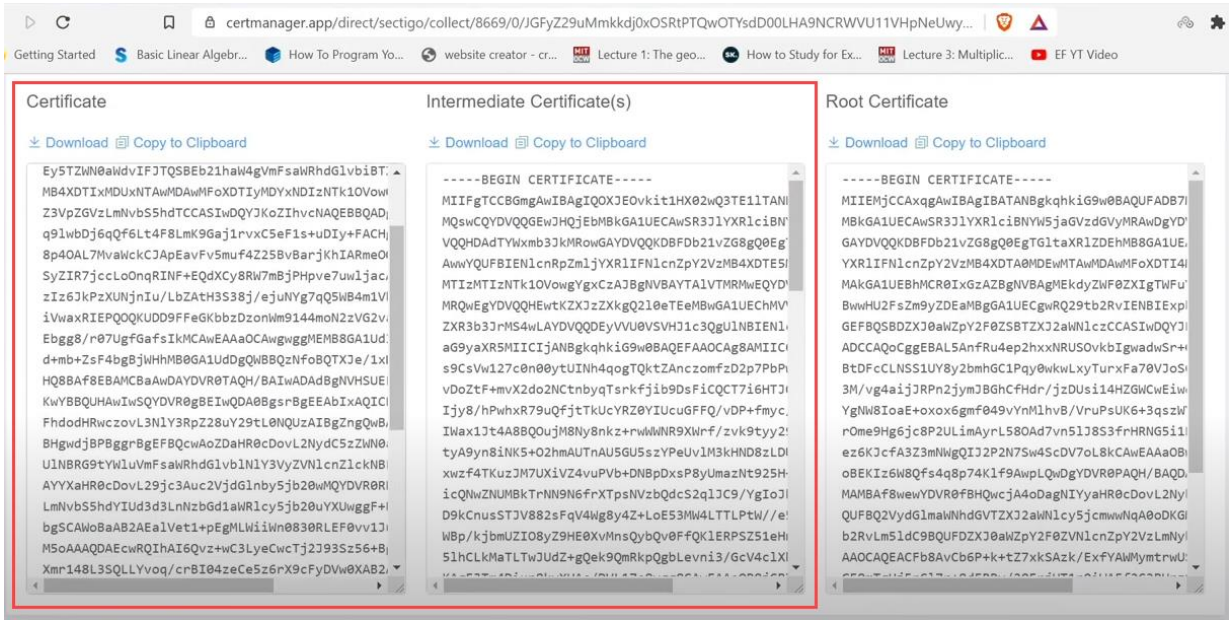
Después de confirmar que usara el método de validación por email, la cuenta de correo de su administrador de dominio recibirá un enlace enviado por la Autoridad emisora de certificados. Mediante este enlace usted podrá probar que es el dueño o administrador del dominio para el cual se le desea generar un certificado.

Una vez realizada la validación de la propiedad del dominio, esta no se reflejará inmediatamente como concluida en el panel de administración del certificado, pudiendo tomar unos minutos en actualizarse el estado.



7. Una vez el certificado este habilitado debido a las 2 actividades realizadas en el paso anterior, se procederá a descargar los certificados desde el panel de control.





8. Ir a la carpeta que se creó para contener los certificados y crear los certificados emitidos por nuestro proveedor.

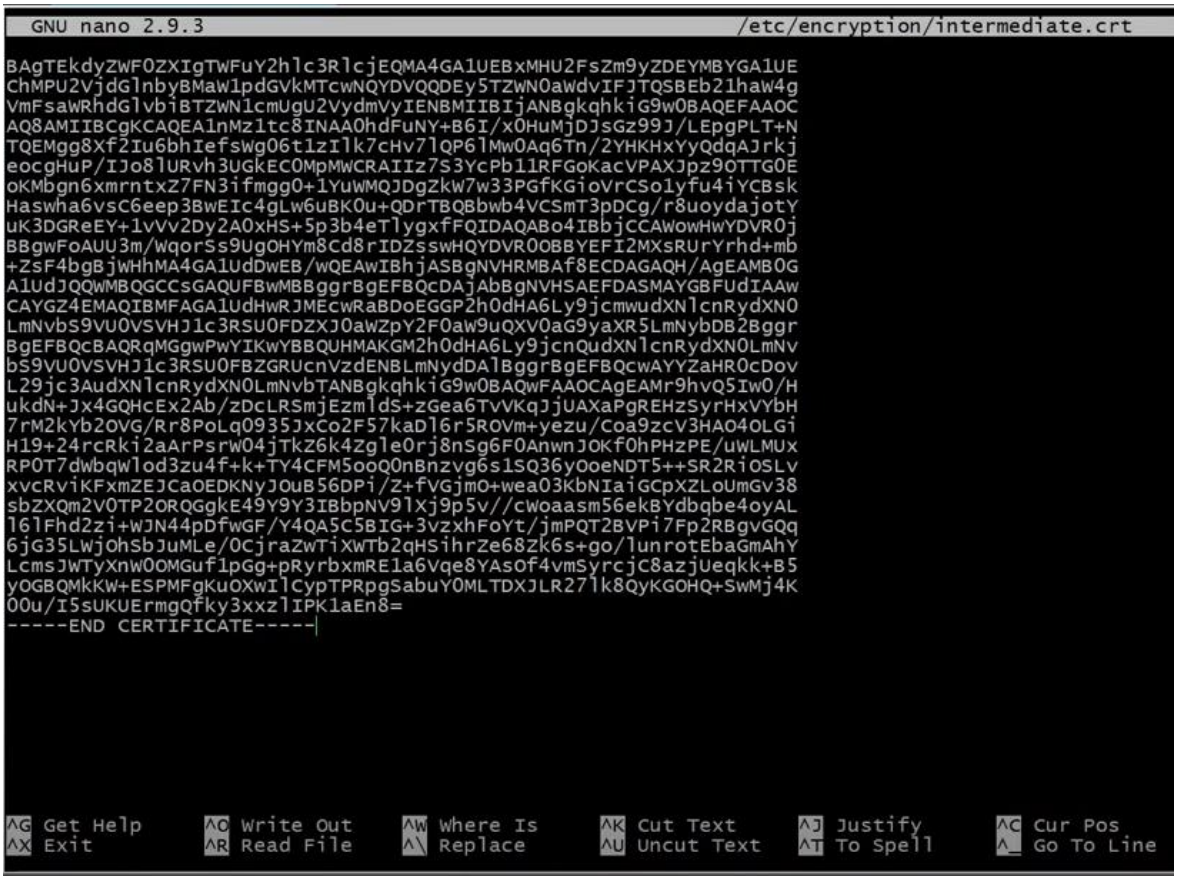
Comandos

cd /etc/encryption

nano /etc/encryption/certificate.crt

[Copiar y pegar el contenido del certificado obtenido en el punto anterior (Columna Certificate)]

nano /etc/encryption/intermediate.crt
[Copiar y pegar el contenido del certificado intermedio obtenido en el punto anterior (Columna Intermediate Certificate)]



9. Configurar los parámetros SSL para el Apache, mediante las siguientes directivas:

Directivas

SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
Disable preloading HSTS for now. You can use the commented out header line that includes
the "preload" directive if you understand the implications.
Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
Requires Apache >= 2.4
SSLCompression off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
Requires Apache >= 2.4.11
SSLSessionTickets Off

Comandos

sudo nano /etc/apache2/conf-available/ssl-params.conf

[Copiar y pegar las directivas]

```
 GNU nano 2.9.3                                  /etc/apache2/conf-available/ssl-params.conf

SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
# Disable preloading HSTS for now.  You can use the commented out header line that includes
# the "preload" directive if you understand the implications.
# Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
# Requires Apache >= 2.4
SSLCompression off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
# Requires Apache >= 2.4.11
SSLSessionTickets Off
```

10. Habilitar SSL en Apache2

Comando
a2enmod ssl

```
root@ubuntu: ~
root@ubuntu:~# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@ubuntu:~# systemctl restart apache2
root@ubuntu:~#
```

11. Habilitar los headers y los parámetros para el SSL en Apache2

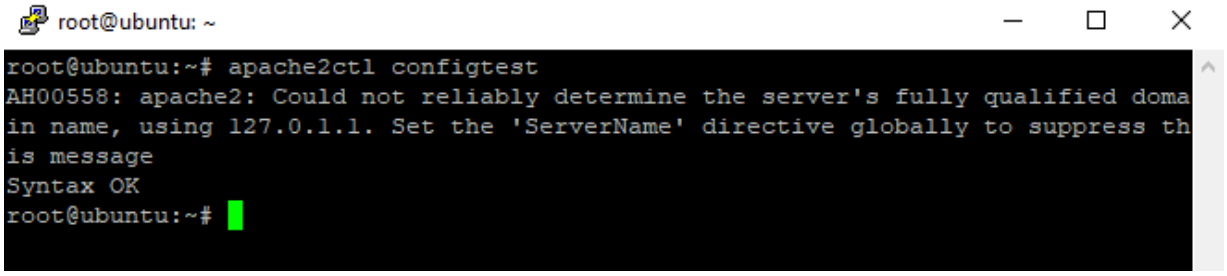
Comando
a2enmod headers
a2enconf ssl-params

```
root@ubuntu: ~
root@ubuntu:~# a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@ubuntu:~# a2enconf ssl-params
Enabling conf ssl-params.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@ubuntu:~#
```

12. Probar la configuración del Apache2

Comando
apache2ctl configtest

Si se muestra el mensaje "Syntax Ok", la configuración es correcta. Omitir el mensaje de error sobre ServerName Global Directive.



13. Editar el archivo:

/etc/apache2/sites-available/[nombre del subdominio]

Por ejemplo:
/etc/apache2/sites-available/dev-dspace.concytec.gob.pe.conf

Nota: Revisar el manual técnico “009 Cambiar el puerto 8080 al 80” en el cual se describen los pasos para asociar un subdominio al Dspace usando Apache2.

Realizar los siguientes cambios:

- ✓ Crear otro VirtualHost para el puerto 443, para esto copiar y pegar el VirtualHost del puerto 80.

- ✓ En el VirtualHost del puerto 443, agregar las líneas:

  SSLEngine on
  SSLCertificateFile [Ruta del certificado]
  SSLCertificateKeyFile [Ruta de la llave privada]
  SSLCertificateChainFile [Rtua del certificado intermedio]

  Ejemplo:
  SSLEngine on
  SSLCertificateFile /etc/encryption/certificate.crt
  SSLCertificateKeyFile /etc/encryption/server.key
  SSLCertificateChainFile /etc/encryption/intermediate.crt

- ✓ Modificar el log para que se genere un log independiente para el puerto 443

  Ejemplo:
  ErrorLog ${APACHE_LOG_DIR}/dev-dspace-ssl.error.log

CustomLog ${APACHE_LOG_DIR}/dev-dspace-ssl.access.log combined

✓ En el VirtualHost del puerto 80, comentar las líneas:

#ProxyPass / ajp://localhost:8009/
#ProxyPassReverse / ajp://localhost:8009/

Y agregar la linea:
Redirect permanent / https://[tu-dominio]/

Ejemplo:
Redirect permanent / https://dev-dspace.concytec.gob.pe/

Antes

dev-dspace.concytec.gob.pe.conf | new 162 | new 163 | new 161 | new 166 | new 16

```
1  <VirtualHost *:80>
2      ServerName dev-dspace.concytec.gob.pe
3
4      ServerAdmin webmaster@localhost
5      #DocumentRoot /var/www/html
6
7      ProxyPass / ajp://localhost:8009/
8      ProxyPassReverse / ajp://localhost:8009/
9
10     ErrorLog ${APACHE_LOG_DIR}/dev-dspace.error.log
11     CustomLog ${APACHE_LOG_DIR}/dev-dspace.access.log combined
12
13 </VirtualHost>
14
```

Después

dev-dspace.concytec.gob.pe.conf

```
<VirtualHost *:80>
    ServerName dev-dspace.concytec.gob.pe

    ServerAdmin webmaster@localhost
    #DocumentRoot /var/www/html

    #ProxyPass / ajp://localhost:8009/
    #ProxyPassReverse / ajp://localhost:8009/
    Redirect permanent / https://dev-dspace.concytec.gob.pe/

    ErrorLog ${APACHE_LOG_DIR}/dev-dspace.error.log
    CustomLog ${APACHE_LOG_DIR}/dev-dspace.access.log combined

</VirtualHost>

<VirtualHost *:443>
    ServerName dev-dspace.concytec.gob.pe

    ServerAdmin webmaster@localhost
    #DocumentRoot /var/www/html

    ProxyPass / ajp://localhost:8009/
    ProxyPassReverse / ajp://localhost:8009/

    SSLEngine on
    SSLCertificateFile /etc/encryption/certificate.crt
    SSLCertificateKeyFile /etc/encryption/server.key
    SSLCertificateChainFile /etc/encryption/intermediate.crt

    ErrorLog ${APACHE_LOG_DIR}/dev-dspace-ssl.error.log
    CustomLog ${APACHE_LOG_DIR}/dev-dspace-ssl.access.log combined

</VirtualHost>
```

Así debe quedar

<VirtualHost *:80>
ServerName dev-dspace.concytec.gob.pe

ServerAdmin webmaster@localhost
#DocumentRoot /var/www/html

#ProxyPass / ajp://localhost:8009/
#ProxyPassReverse / ajp://localhost:8009/
Redirect permanent / https://dev-dspace.concytec.gob.pe/

ErrorLog ${APACHE_LOG_DIR}/dev-dspace.error.log
CustomLog ${APACHE_LOG_DIR}/dev-dspace.access.log combined

</VirtualHost>

<VirtualHost *:443>

ServerName dev-dspace.concytec.gob.pe

ServerAdmin webmaster@localhost
#DocumentRoot /var/www/html

ProxyPass / ajp://localhost:8009/
ProxyPassReverse / ajp://localhost:8009/

SSLEngine on
SSLCertificateFile /etc/encryption/certificate.crt
SSLCertificateKeyFile /etc/encryption/server.key
SSLCertificateChainFile /etc/encryption/intermediate.crt

ErrorLog ${APACHE_LOG_DIR}/dev-dspace-ssl.error.log
CustomLog ${APACHE_LOG_DIR}/dev-dspace-ssl.access.log combined

</VirtualHost>

14. Reiniciar Apache2

    systemctl restart apache2

15. Si el Apache2 no inicia, realizar lo siguiente:

    ✓ Revisar el log:

    Comando
    tail /var/log/apache2/error.log

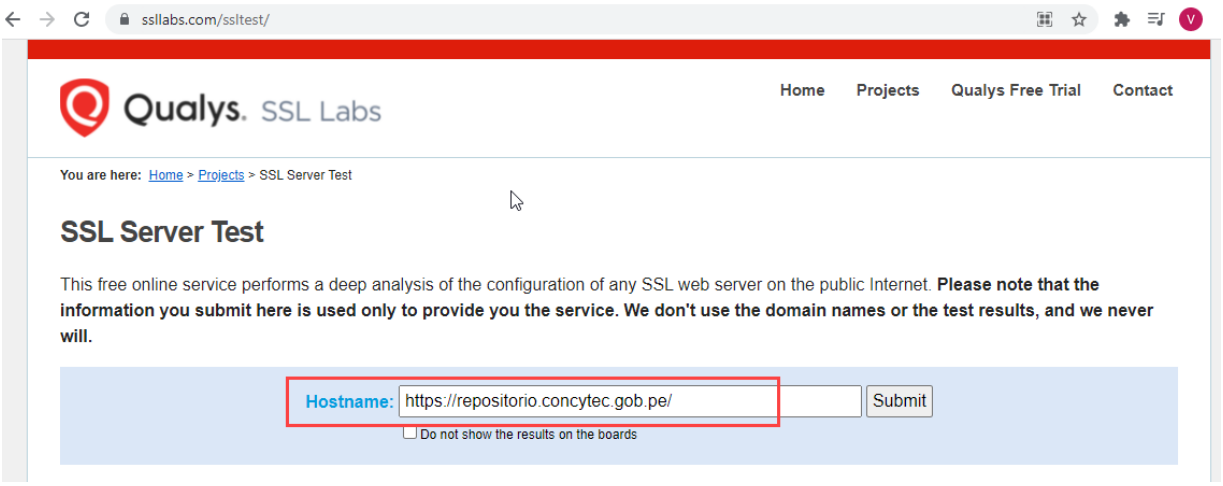
    ✓ Si se muestra un mensaje genérico como:

    AH00016: Configuration Failed

    Instalar y ejecutar el siguiente comando para obtener el detalle de inicialización del Apache2

    Comandos
    sudo apt-get update
    sudo apt-get install strace
    sudo strace -f apache2ctl start

16. Verificar el estado de la configuración del servicio SSL.
    Ir a la página:
    https://www.ssllabs.com/ssltest/



17. Referencias

https://www.youtube.com/watch?v=zgUshTJa4sc
https://www.ssltrust.com.au/help/setup-guides/apache-ubuntu-ssl-install-guide