La verdad es que ya no hay excusas para tener sitios mediante HTTPS sin certificados reales.

La variante más usada actualmente para solicitar certificados SSL libres es LetsEncrypt (adelante LE) (http://letsencrypt.org)

En su sitio web se puede encontrar información bastante detallada por lo que nos vamos a limitara dar algunas recetas.

Instalación: LA variante recomendada es: https://certbot.eff.org/

Cuando se instala desde paqueteria para Ubuntu o Debian el mecanismo para la renovación queda configurada en el cron de forma automática.

Después de instalado el programa se se pueden pedir los certifiacos. Esto lleva un proceso de validacion pues la entidad emisora debe estar segura de que el certificado será instalado en la máquina que responde realmente al nombre de dominio dado.

Para evitar interrupciones en el servicio LE soporta integración con los servidores web más comunes: Apache y NGINX.

Si usted no desea usar ninguno de estos servidores y solo necesita tener el certificado puede usar el servidor integrado en el cliente certbot mediante la opción certonly

Para certificados tipo wildcard se puede usar este comando:

```
certbot certonly --server https://acme-v02.api.letsencrypt.org/directory --
manual --preferred-challenges dns -d *.uclv.edu.cu
```

La primera vez se muestra un comentario como este:

```
Please deploy a DNS TXT record under the name
_acme-challenge.uclv.edu.cu with the following value:

xxxxxxxx

Before continuing, verify the record is deployed.
```

Para el caso particular de la UCLV buscar en la Wiki Interna los pasos aseguir.