***Laboratorio 3 SSL y SSH***

***María Cedeño 2-737-2336***

**SECCIÓN NO. 1 Instalación de OpenSSL y Creación del Certificado SSL para servidor Apache**

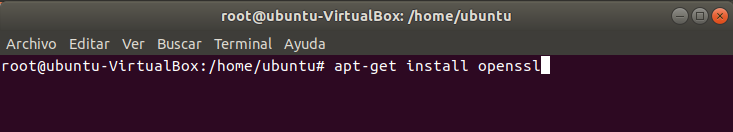


Ilustración 1 - Como primer paso se requiere instalar el paquete de openssl

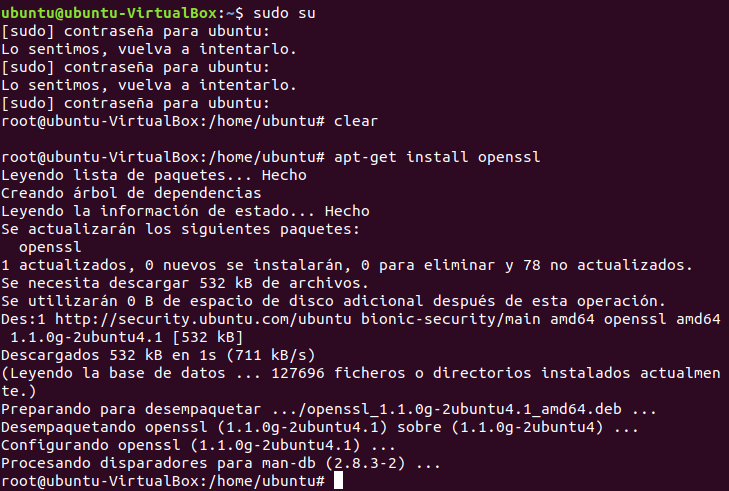


Ilustración 2 - Muestra de paquetes descargados por el openssl (ficheros)

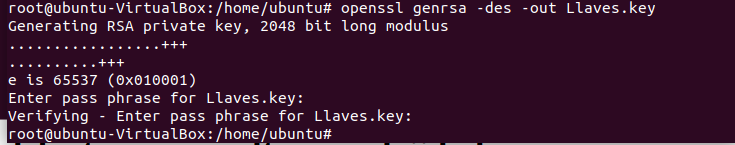


Ilustración 3 - Generación de llave de modulo RSA, Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

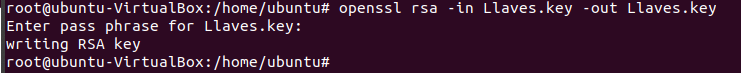


Ilustración 4 - sustituir la clave antigua del servidor RSA

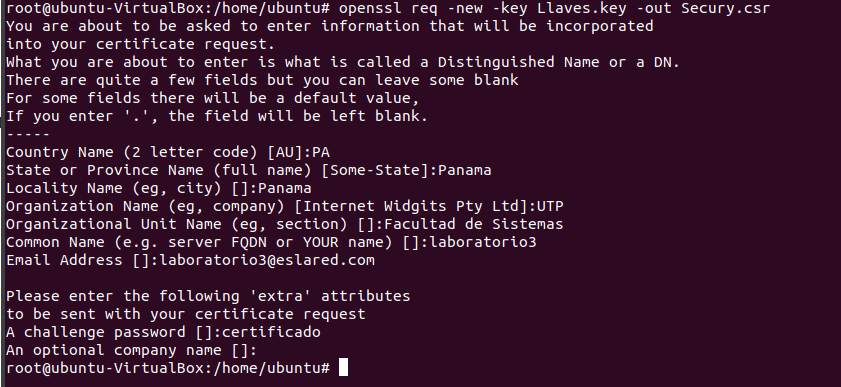


Ilustración 5 - Con esto vamos a dar un nombre al servidor Secury.csr y le asignamos la clave anteriormente, adicional se crea el certificado información que llevara el certificado como lo es, nombre, nombre de la organización, correo, etc.

***El siguiente comando es:***

***#openssl x509 –reg –day 365 –in Secury.csr –signkey Llaves.key –out Secury.crt***

**\* Genera un certificado autofirmado para el servidor de apache2, con 365 días de uso.**

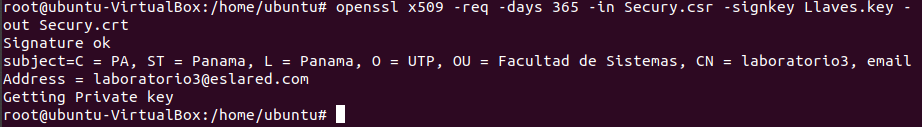


Ilustración 6 - Autogeneración de certificado para servidor apache, basado con el Secury.csr.



Ilustración 7 - Para la creación de la carpeta ssl en apache previamente se descargo el paquete del mismo.



Ilustración 8 - Se procede a mover los archivos Llaves.key y Secury.crt a la carpeta /etc/apache2/ssl

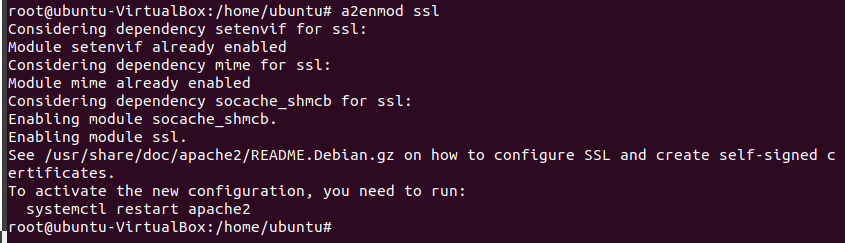


Ilustración 9 - Con estas líneas se habilita el módulo SSL de Apache.

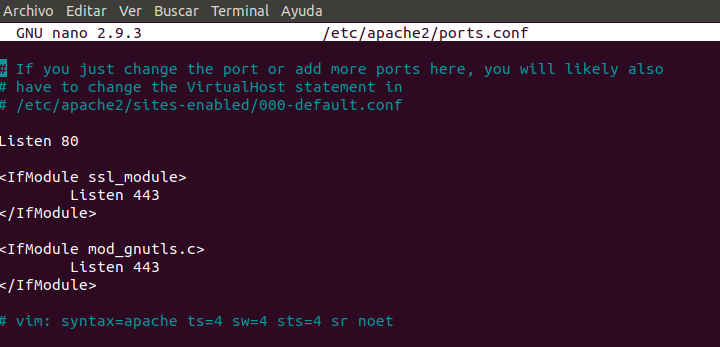


Ilustración 10 - Verificación de los puertos para apache.

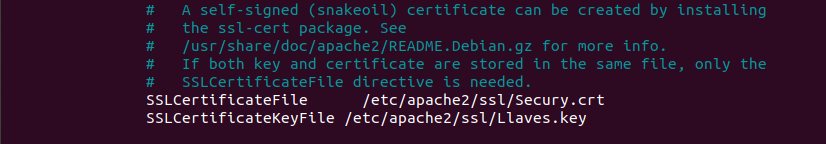


Ilustración 11 - Modificación de rutas para que selecione nuestras llaves y certificados creados.

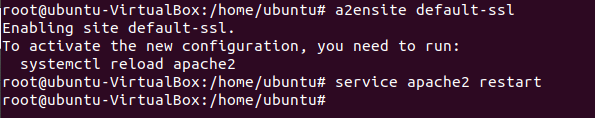


Ilustración 12 - Estas líneas habilita la configuración SSL por defecto.

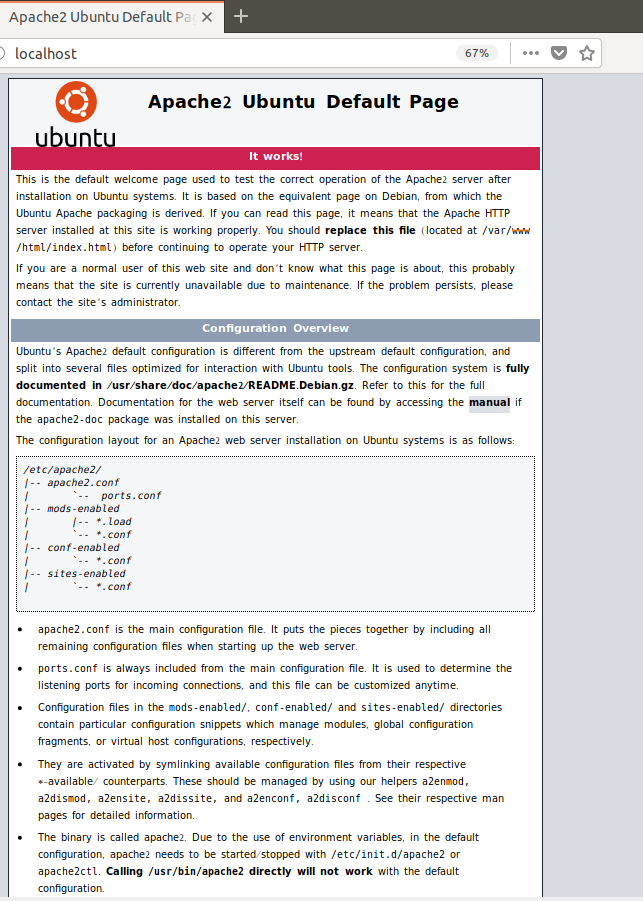


Ilustración 13 - Vista previa en nuestro explorador firefox del apache instalado con nuestras configuraciones básicas de SSL.

**SECCIÓN NO. 2 Crear Autoridad de Certificación (CA)**

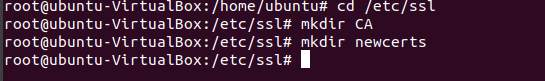


Ilustración 14 - Creación de nuevos carpetas o directorios llamados CA y newcerts

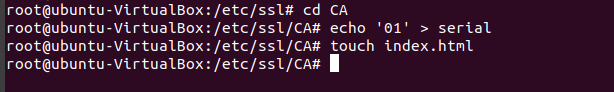


Ilustración 15 - Creacion de archivo serial y creación de archivo index.txt que sera utilizado como base de datos más adelante.

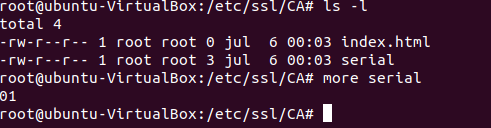


Ilustración 16 - Comando ls -l nos permite visualizar las carpetas y archvos creados con sus respectivos detalles de fechas y permisos.

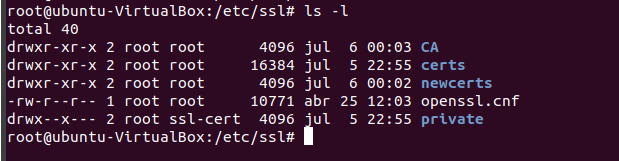




Ilustración 17 - Antes de llegar a este punto se respaldo el archivo openssl.cnf, y editamos un nuevo fichero openssl.cnf pero solamente en la sección de CA.

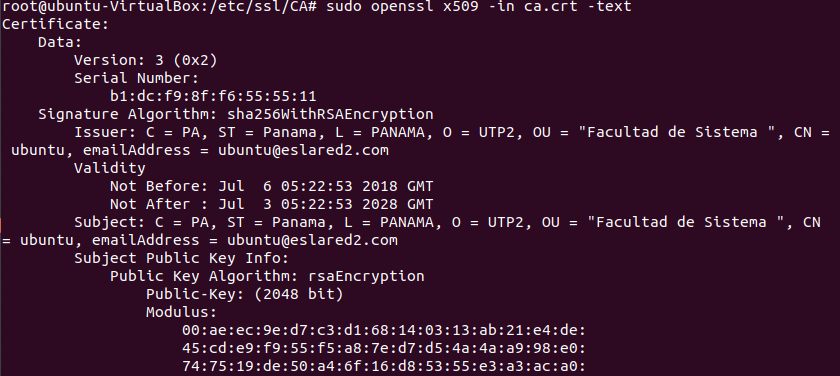


Ilustración 18 - Comprobando el contenido del certificado y la clave privada de nuestra Autoridad Certificadora privada.

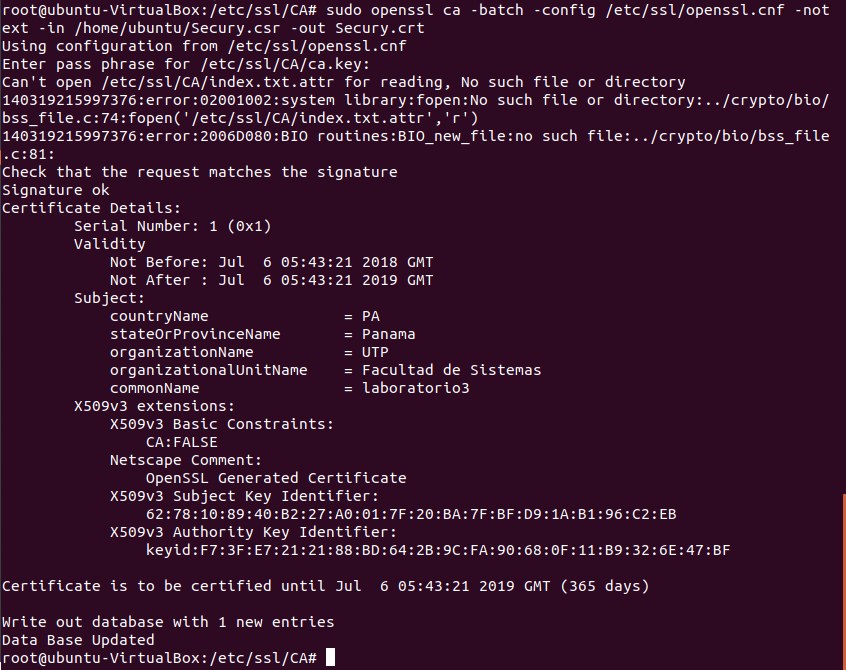


Ilustración 19 - Al servidor Web creado, le procedemos a firmar con la CA “privada”

´

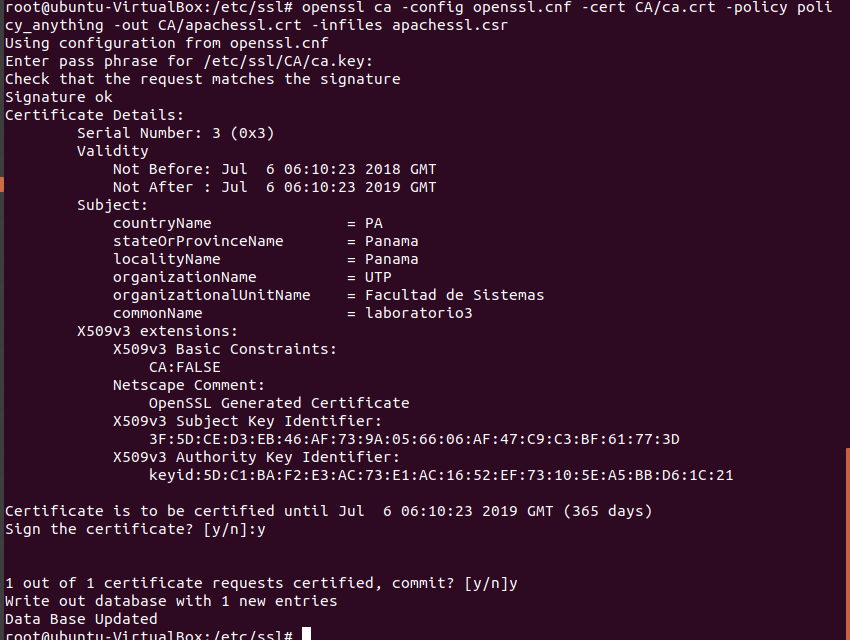


Ilustración 20 - Firma del pedido de certificado para generar el certificado para el servidor.



Ilustración 21 - Creación de un archivo pkcs12 para instalar en navegadores.



Ilustración 22 - Configuraciones previas para importar certificado creado.

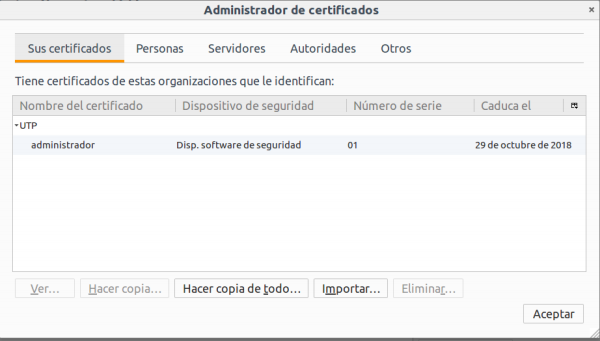


Ilustración 23 - Importación del certificado creado.

***SECCIÓN NO. 3 Utilización de las Listas de Revocación de Certificados (CRL)***

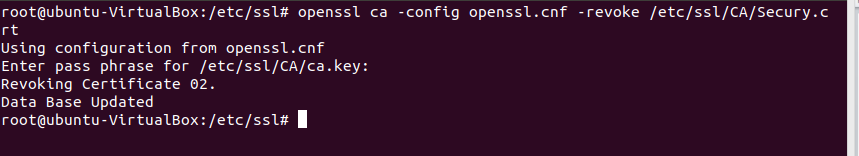


Ilustración 24 - Revocar certificado válido para que deje de funcionar.

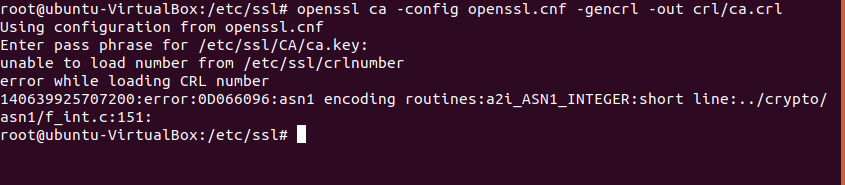


Ilustración 25 - Generar un nueva CRL (Certificate Revokation List)

***SECCIÓN NO. 4 Generación de certificados X.509***

**Esta sección no se pudo realizar ya que la terminal enviaba un error de que el certificado x509 no era un directorio válido al igual se investigó que es un certificado x509 y para que se usa, el cual encontré:**

El formato de certificados X.509 es un estándar del ITU-T (International Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (International Standards Organization / International Electrotechnical Commission) que se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios. Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996.

Los elementos del formato de un certificado X.509 v3 son:

* **Versión**. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
* **Número de serie del certificado**. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
* **Identificador del algoritmo de firmado**. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
* **Nombre del emisor**. Este campo identifica la CA que ha firmado y emitido el certificado.
* **Periodo de validez**. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
* **Nombre del sujeto**. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
* **Información de clave pública del sujeto**. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
* **Identificador único del emisor**. Este es un campo opcional que permite reutilizar nombres de emisor.
* **Identificador único del sujeto**. Este es un campo opcional que permite reutilizar nombres de sujeto.
* **Extensiones**.

Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:

1. **Tipo de extensión**. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.
2. **Valor de la extensión**. Este subcampo contiene el valor actual del campo.
3. **Indicador de importancia**. Es un flag que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

***SECCIÓN NO. 5 Cifrado Asimétrico***

**Al igual que la sección 4, esta parte no se pudo realizar ya que algunos comando no eran reconocidos por la terminal como lo era: openssl --ciphers y otros como openssl dgst -sha1 fichero.**

***Que es Cifrado Asimétrico?***

**R:** A diferencia de la criptografía simétrica, la asimétrica hace uso de dos claves, una pública y una privada, y es por ello que también se la llama, junto con los mecanismos de cifrado y autenticación asimétricos, Infraestructura de clave pública, o PKI por sus siglas en inglés.

Se basa en un par de claves en el cual solo existe una clave pública para una privada, y viceversa, de modo que no sería posible encontrar otra clave publica que se relacione con la privada, ni tampoco otra privada que se relacione con la pública del par. Además de esta condición, otra condición para la generación de claves, es que la clave privada nunca puede ser obtenida a partir de la clave pública, y esto es necesario para cualquier algoritmo asimétrico, ya que éstos métodos requieren el intercambio, por un medio hostil como Internet, de las claves públicas de los nodos de cifrado.

En cifrado asimétrico cada nodo dispone de las dos claves de cifrado, y pueden intercambiar libremente sus claves públicas, y así un nodo podrá cifrarle a otro utilizando la clave publica del destinatario, mientras que el destinatario podrá descifrar el contenido mediante su clave privada secreta. Es por esta razón que la clave privada debe ser protegida de cualquier extraño, puesto que quien la tenga podrá descifrar todo contenido, archivos o tráfico, destinado a su poseedor, y además, podrá autenticarse por su propietario original en cualquier servicio que utilice PKI y en el que haya estado registrado.

En este caso la ventaja es que las claves publicas pueden ser intercambiadas sin mediar ningún resguardo, y pueden intercambiarse directamente, o por medio de certificados digitales x509.

***Investigue:***

1. ¿En qué consiste el formato pem utilizados en la clave y el certificado de la Autoridad

Certificadora?

***R:*** Este es un formato contenedor que puede incluir sólo el público certificado (como con Apache se instala, y archivos de certificados de CA /etc/ssl/certs), o puede incluir toda una cadena de certificados, incluyendo la clave pública, la clave privada, y de los certificados de root. El nombre de Privacidad de Correo electrónico Mejorada, un error de método para correo electrónico seguro, pero el formato de envase que se utiliza vidas, y es un base64 traducción de la x509 ASN.1 teclas.

2. ¿Cuál es el funcionamiento de las líneas de comando introducidas al shell en el paso 7 de la sección 3?

***R:*** La sección 3 solo tiene dos líneas de comando no hay paso 7.

3. ¿Es posible utilizar un certificado digital generado por una AC implementada en Linux para proveer soporte SSL (utilizando certificados digitales) a un Servidor Web basado en Windows, como por ejemplo IIS? Explique

***R:*** Se puede ya que son configuraciones para los navegadores, con contraseñas y accesos.

4. Presentar el procedimiento a seguir para instalar un certificado digital en un servidor Web Microsoft IIS 6.0.

***R:***

Para instalar el certificado:

* Abra el Administrador de servicios Internet y expanda el nombre del servidor para que pueda ver los sitios Web.
* Haga clic derecho en el sitio Web para el que creó la solicitud de certificado y haga clic en Propiedades.
* Haga clic en la ficha Seguridad de directorios. En Comunicaciones seguras, haga clic en Certificado de servidor. Esto inicia al Asistente para la instalación de certificados. Haga clic en siguiente para continuar.
* Seleccione procesar la petición pendiente e instalar el certificado y haga clic en siguiente.
* Escriba la ubicación del certificado que ha descargado en la sección "Emisión y descarga un certificado" y haga clic en siguiente. El asistente mostrará el resumen del certificado. Compruebe que la información es correcta y haga clic en siguiente para continuar.
* Haga clic en Finalizar para completar el proceso.

5. Investigar 3 razones para indicar que un certificado ya no es válido.

***R:*** Las razones son:

* Fecha de caducidad
* Sitios con firmas erroneas
* Bloqueados por firewall

6. Investigue 5 sitios Web de Internet en donde se pueden encontrar Listas de Revocación de Certificados (CRL)

***R:***

En el siguiente link se pueden obtener la lista de certificados revocados.

* https://certificacion.cgcom.es/infoacomc/crl

Las listas de revocación de certificados incluyen los números de serie de todos los certificados que han sido revocados. Estas listas se actualizan cada 24 horas y pueden ser consultadas a través de las siguientes URL:

* http://crl3.cgcom.es/crl/eccgcom.crl
* http://crl4.cgcom.es/crl/eccgcom.crl

***ULTIMA PARTE***

1. Con la información y los conocimientos que ha adquirido trate de llenar la tabla siguiente. Marque aquellas casillas que puedan obtenerse con las funciones que se mencionan en cada caso. Tome como ejemplo la primera fila.

