



# Clase II

Interconexión de redes de datos (IRD101)

## Agenda

- Asignación de actividad # 1
- Detección de fallos en capas 3, 4 y 7

## Detección de fallos en capa 3

### Aplicaciones para verificación de parámetros de tarjetas de red.

Para sistemas operativos Windows se tiene la aplicación de consola **ipconfig**, la cual permite mostrar los valores de los parámetros de configuración TCP/IP presentes en el equipo.

```
C:\Windows\System32>IPCONFIG /ALL

Configuración IP de Windows

Nombre de host. . . . . : Norfi-PC
Sufixo DNS principal . . . . :
Tipo de nodo. . . . . : mixto
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no

Adaptador de Ethernet Conexión de área local:

Sufixo DNS específico para la conexión. . :
Descripción . . . . . : Realtek RTL8168D/8111D Family PCI-E Gigabit Ethernet
Dirección física. . . . . : 00-26-11-DF-6C-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::c8c9:e20d:5060:7c27231(Preferido)
Dirección IPv4. . . . . : 192.168.137.3(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . : 192.168.137.1
IAID DHCPv6 . . . . . : 620766744
DUID de cliente DHCPv6. . . . . : 00-01-00-01-12-A0-97-6C-00-26-18-DF-6C-E0
Servidores DNS. . . . . : 216.146.35.35
                          216.146.36.36
NetBIOS sobre TCP/IP. . . . . : habilitado
```

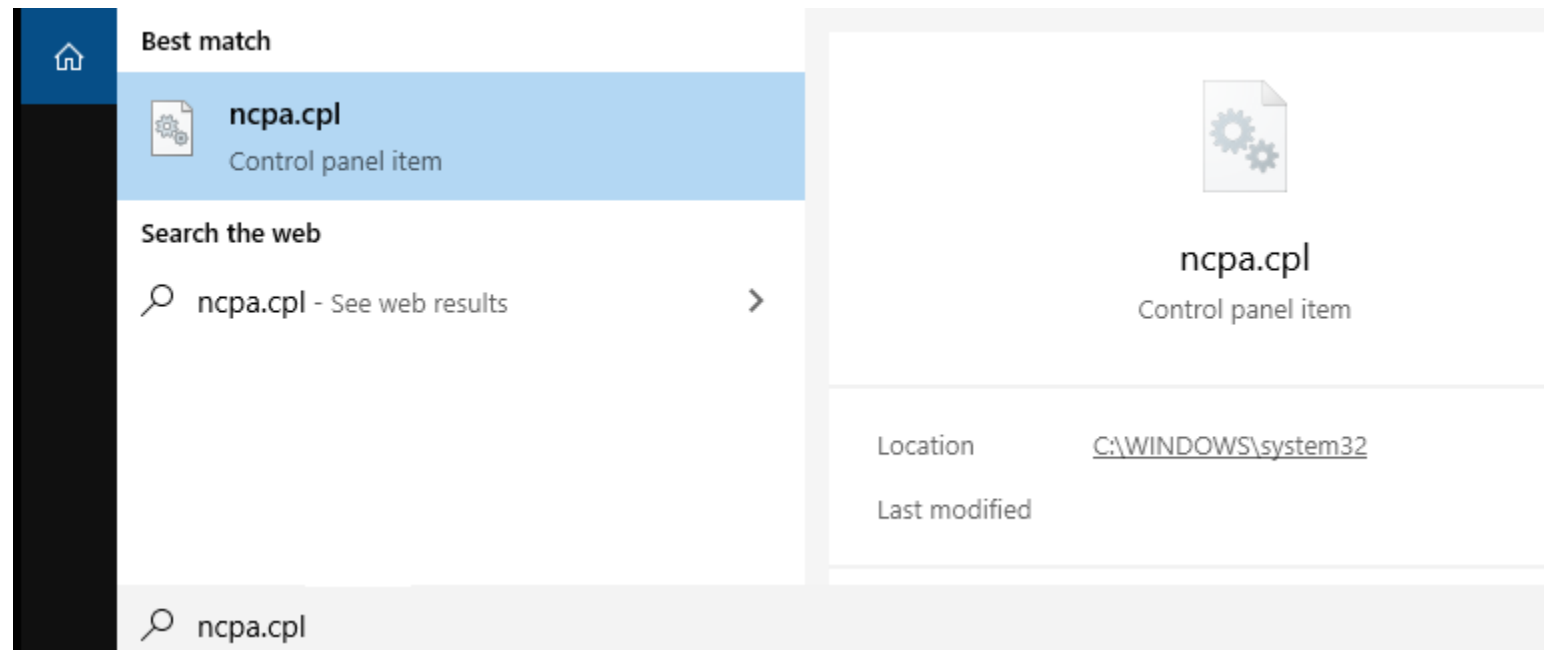
Dirección IP equipo

Dirección IP servidor local

Servidores DNS

## Detección de fallos en capa 3

Si se desea revisar/modificar las propiedades de las conexiones de red en un equipo bajo el Sistema Operativo Windows, se puede ejecutar el siguiente comando:



## Detección de fallos en capa 3

Para sistemas operativos Linux se tiene la aplicación de consola `ifconfig`, la cual permite mostrar los valores de los parámetros de configuración TCP/IP presentes en el equipo y estadísticas de tráfico.

```
himanshu@ansh:~$ ifconfig
enp3s0  Link encap:Ethernet  HWaddr 70:4d:7b:70:d2:3e
        UP BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:73925 errors:0 dropped:0 overruns:0 frame:0
        TX packets:73925 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:7911049 (7.9 MB)  TX bytes:7911049 (7.9 MB)

wlx18a6f713679b Link encap:Ethernet  HWaddr 18:a6:f7:13:67:9b
        inet addr:192.168.2.6  Bcast:192.168.2.255  Mask:255.255.255
        inet6 addr: fe80::733f:7699:a8de:78ac/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:598724 errors:0 dropped:5949 overruns:0 frame:0
        TX packets:481412 errors:0 dropped:20 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:390451501 (390.4 MB)  TX bytes:102506204 (102.5 MB)
```

# Detección de fallos en capa 3

## Ping (Packet Internet Groper)

Es una herramienta de diagnóstico (disponible en equipos Windows o Linux) que permite verificar la comunicación entre el equipo en donde es ejecutado y los destinos remotos.

Esta herramienta utiliza el protocolo ICMP (Internet Control Message Protocol)

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
-t          Ping the specified host until stopped.
            To see statistics and continue - type Control-Break;
            To stop - type Control-C.
-a          Resolve addresses to hostnames
-n count    Number of echo requests to send.
-l size     Send buffer size.
```

## Detección de fallos en capa 3

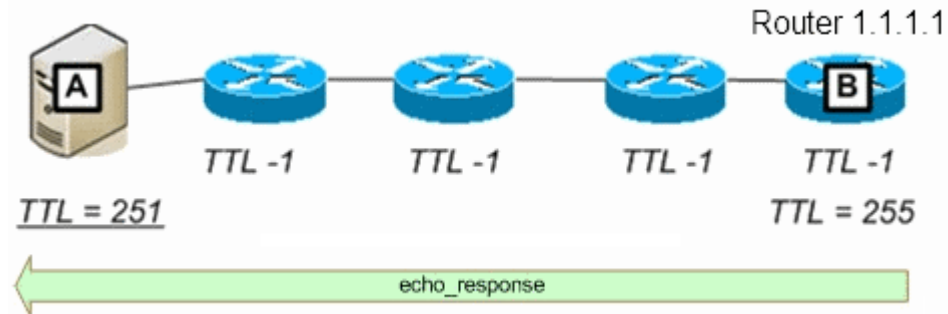
El paquete TTL (**Time To Live**) brinda una métrica del número de routers existentes entre el origen y destino.

TTL es utilizado para prevenir loops en las comunicaciones de la siguiente forma: el valor inicial del paquete TTL es 255 y es decrementado por uno cada vez que se encuentra un router.

Cuando este valor llega a 0, el paquete es descartado por el router.

Por defecto, un equipo Windows decrementará el valor del paquete TTL por 128 y un equipo Linux por 192.

## Ejemplos:

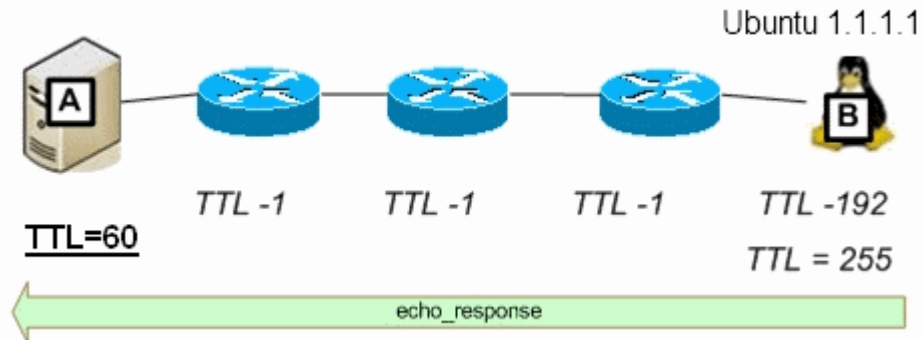


Pinging B [1.1.1.1] with 32 bytes of data:

Reply from 1.1.1.1: bytes=32 time=18 ms **TTL=251**  
 Reply from 1.1.1.1: bytes=32 time=21 ms **TTL=251**  
 Reply from 1.1.1.1: bytes=32 time=20 ms **TTL=251**  
 Reply from 1.1.1.1: bytes=32 time=33 ms **TTL=251**

Ping statistics for 1.1.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
 Approximate round trip times in milli-seconds:  
 Minimum = 18ms, Maximum = 33ms, Average = 23ms

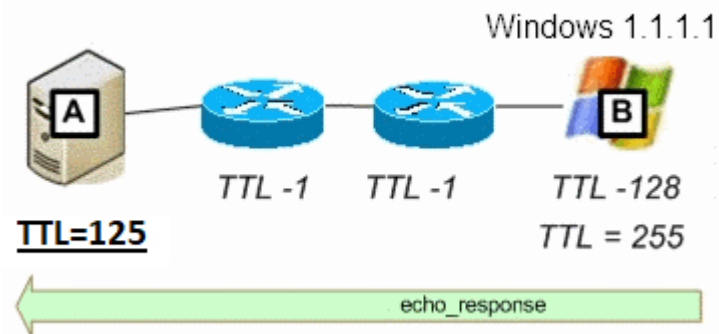


Pinging B [1.1.1.1] with 32 bytes of data:

Reply from 1.1.1.1: bytes=32 time=18 ms **TTL=60**  
 Reply from 1.1.1.1: bytes=32 time=21 ms **TTL=60**  
 Reply from 1.1.1.1: bytes=32 time=20 ms **TTL=60**  
 Reply from 1.1.1.1: bytes=32 time=33 ms **TTL=60**

Ping statistics for 1.1.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
 Approximate round trip times in milli-seconds:  
 Minimum = 18ms, Maximum = 33ms, Average = 23ms



Pinging B [1.1.1.1] with 32 bytes of data:

Reply from 1.1.1.1: bytes=32 time=18 ms **TTL=125**  
 Reply from 1.1.1.1: bytes=32 time=21 ms **TTL=125**  
 Reply from 1.1.1.1: bytes=32 time=20 ms **TTL=125**  
 Reply from 1.1.1.1: bytes=32 time=33 ms **TTL=125**

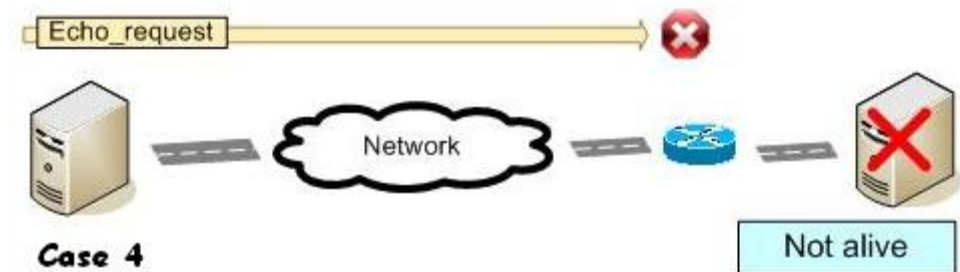
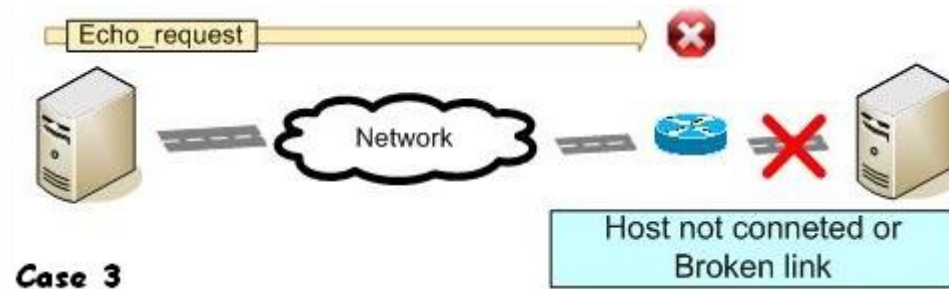
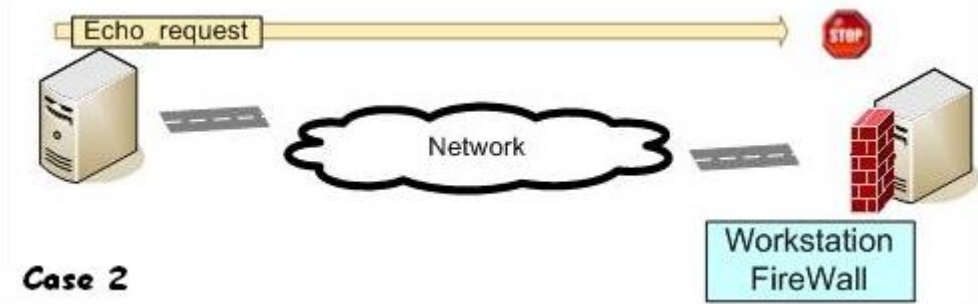
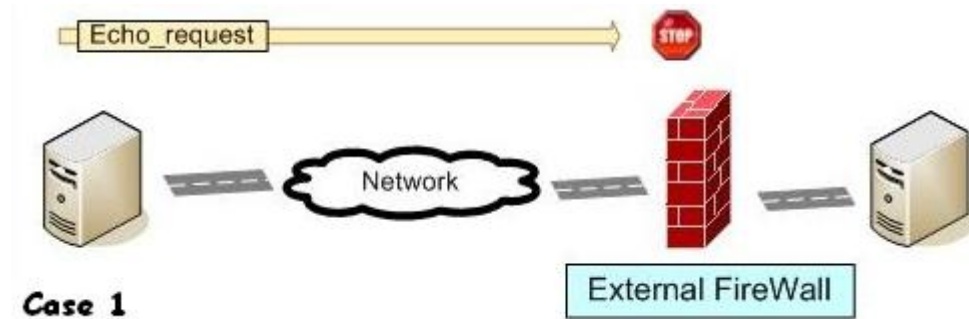
Ping statistics for 1.1.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
 Approximate round trip times in milli-seconds:  
 Minimum = 18ms, Maximum = 33ms, Average = 23ms



## Detección de fallos en capa 3

Escenarios de fallos más comunes en respuesta prueba de ping.



## Detección de fallos en capa 3

### tracert (Windows) / traceroute (Linux)

Es una herramienta de diagnóstico permite determinar la ruta a un destino mediante el envío de paquetes ICMP.

Dado que los routers deben disminuir el TTL del paquete como mínimo una unidad antes de reenviar el paquete, cuando el TTL de un paquete alcanza el valor cero (0), el router devuelve al equipo de origen un mensaje ICMP de "Tiempo agotado".

TRACERT es útil a la hora de solucionar problemas en las redes grandes, donde se pueden tomar varias rutas para llegar a un destino o donde existen muchos componentes intermedios (routers o firewalls).

## Detección de fallos en capa 3

La opción -d con el comando tracert le indica a TRACERT que no efectúe una búsqueda de DNS en todas las direcciones IP, de manera que TRACERT devuelve la dirección IP de la interfaz del lado cercano de los routers.

```
C:\>tracert 11.1.0.1
```

El resultado del comando:

```
Tracing route to 11.1.0.1 over a maximum of 30 hops
```

```
-----  
 1          2 ms          3 ms          2 ms          157.54.48.1  
 2         75 ms         83 ms         88 ms         11.1.0.67  
 3         73 ms         79 ms         93 ms         11.1.0.1
```

```
Trace complete.
```

## Detección de fallos en capa 3

Es posible utilizar TRACERT para averiguar en qué lugar de la red se detuvo un paquete.

Para la salida anterior el Default Gateway ha determinado que no existe una ruta válida para el router de destino, probablemente haya un problema de configuración en el router o no exista la red a la cual pertenece la IP de destino.

```
C:\>tracert 22.110.0.1
```

El resultado del comando:

```
Tracing route to 22.110.0.1 over a maximum of 30 hops
```

```
-----  
1  157.54.48.1  reports: Destination net unreachable.
```

```
Trace complete.
```

## Detección de fallos en capa 3

### Nslookup

Es una aplicación que se utiliza para consulta, obtener información, probar y solucionar problemas de los servidores DNS.

```
C:\>nslookup www.udb.edu.sv
Server:  ns.intelcom.com.gt
Address:  216.230.147.90
```

```
Non-authoritative answer:
Name:     www.udb.edu.sv
Address:  186.190.247.40
```

## Detección de fallos en capa 3

Si es requerido realizar pruebas desde un servidor DNS diferente al configurado en los valores de la tarjeta de red, se puede utilizar el comando **nslookup** de la siguiente forma:

```
C:\>nslookup
Default Server:  ns.intelcom.com.gt
Address:  216.230.147.90

> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

> mh.gob.sv
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    mh.gob.sv
Addresses:  190.57.24.24
           190.5.131.13
```

# Detección de fallos en capa 4

## Telnet

Es un protocolo de red que permite contar con control remoto de un servidor de destino tal como si estuviéramos ejecutando comandos directamente desde la consola de línea de comandos del servidor.

Utiliza el puerto TCP 23, es considerado un protocolo no seguro debido a que los datos que se transmiten se envían mediante texto plano.

La forma de ejecutarlo es la siguiente:

**telnet direccion\_ip\_o\_hostname\_de\_destino**

## Detección de fallos en capa 4

No viene habilitado por defecto en los equipos con sistema operativo Windows.



### Programs and Features

Uninstall a program | Turn Windows features on or off  
Run programs made for previous versions of Windows | Ho

Hardware and Sound

- Programs

User Accounts and Family Safety

Appearance and Personalization

Clock, Language, and Region

Ease of Access



### Default Programs

Change default settings for media or devices | Make a file type always open in a specific program  
Set your default programs





## Detección de fallos en capa 4

Es posible utilizar el comando telnet para efectos de troubleshooting, ya que nos permite conocer si un puerto esta escuchando o esta abierto en un destino, la forma de utilizarlo es la siguiente:

**telnet direccion\_ip\_o\_hostname\_de\_destino**

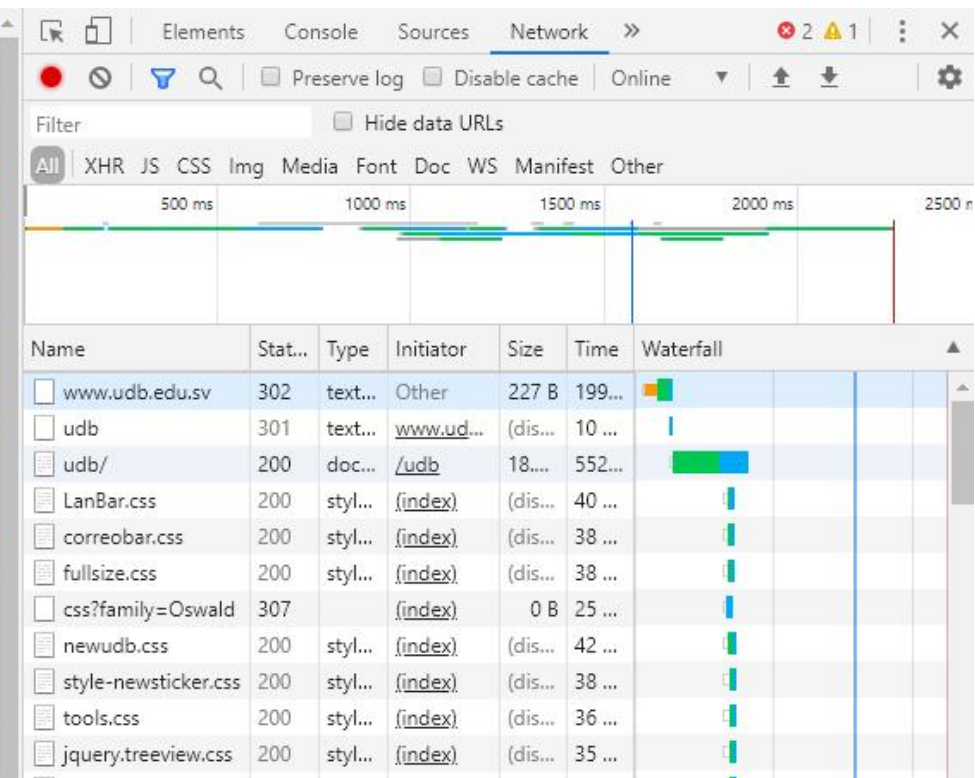
```
C:\>telnet 10.26.243.142 3389
```

# Detección de fallos en capa 7

## Google Chrome Developer Tools.

Es un conjunto de herramientas que poseen los navegadores modernos como Google Chrome que permiten verificar ciertas características que impactan el rendimiento de las aplicaciones web como lo son: inspección de HTML, CSS y JavaScript, enfocándose en los objetos que han sido cargados el tiempo que han demorado, etc.

# Detección de fallos en capa 7

The screenshot shows the Chrome DevTools Network tab. The top bar indicates 2 errors and 1 warning. The filter is set to 'All'. The table below lists the network requests:

Name	Stat...	Type	Initiator	Size	Time	Waterfall
www.udb.edu.sv	302	text...	Other	227 B	199...	
udb	301	text...	www.ud...	(dis...	10 ...	
udb/	200	doc...	/udb	18...	552...	
LanBar.css	200	styl...	(index)	(dis...	40 ...	
correobar.css	200	styl...	(index)	(dis...	38 ...	
fullsize.css	200	styl...	(index)	(dis...	38 ...	
css?family=Oswald	307		(index)	0 B	25 ...	
newudb.css	200	styl...	(index)	(dis...	42 ...	
style-newsticker.css	200	styl...	(index)	(dis...	38 ...	
tools.css	200	styl...	(index)	(dis...	36 ...	
jquery.treeview.css	200	styl...	(index)	(dis...	35 ...	

# Detección de fallos en capa 7

## Revisión de parámetros SSL

Existen herramientas online que permiten realizar diagnósticos rápidos de problemas con certificados SSL que pueden ocasionar errores en los contenidos que consultan los usuarios de aplicaciones web.

A continuación un ejemplo de las herramientas disponibles en la web:

<https://www.sslshopper.com/ssl-checker.html>

## Detección de fallos en capa 7

← → ↻ ⚠ Not secure | expired.badssl.com ☆



### Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_DATE\_INVALID

☐ Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced

Back to safety

<https://expired.badssl.com/>



## EDUCACIÓN SUPERIOR CON ESTILO SALESIANO



Certificación del Técnico  
en Mantenimiento Aeronáutico  
2016-2021



Agencia Centroamericana de Acreditación de  
Programas de Arquitectura y de Ingeniería



INTERNATIONAL SOCIETY FOR  
PROSTHETICS AND ORTHOTICS  
Acreditación Internacional en la  
carrera de Técnico en Ortesis y Prótesis  
Presencial 2016-2021  
A distancia 2019-2020



Comisión de Acreditación  
Calidad de la Educación Superior  
UNIVERSIDAD DON BOSCO  
ACREDITADA  
2017 - 2022

