

# Experto Universitario en Ethical Hacking

Módulo 2:

# **Administración de Servidores (Windows o Linux)**

Unidad 4:

## **Soporte, mantenimiento y solución de problemas**



## Presentación

En esta cuarta y última unidad del módulo, se aprenderán y conocerán las posibles soluciones a los errores más comunes.

Entender la importancia de un plan de contingencia, así como realizar una solución adecuada, comprendiendo el tipo de incidente.



## Objetivos

Que los participantes logren...

- Conocer sobre el mundo de los servidores informáticos, existentes en toda infraestructura informática de mediana y alta gama.
- Conocer las herramientas esenciales y las buenas prácticas necesarias para obtener el máximo nivel de seguridad en una red de servidores de arquitectura Microsoft Windows Server o Linux Server, protegiéndola de potenciales amenazas.
- Comprender los conceptos básicos referentes a la implementación, configuración, mantenimiento y soporte de servidores de infraestructura en tecnologías Windows o Linux.



## Bloques temáticos

1. Plan de contingencia
2. Soporte y mantenimiento
3. Solución de problemas
4. Final del módulo

## Plan de Contingencia

Un plan de contingencia es un conjunto de procedimientos alternativos a la operativa normal de cada empresa, ente o institución, cuya finalidad es la de permitir el funcionamiento de ésta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización.

Las causas pueden ser variadas y pasan por un problema informático, un fallo en la correcta circulación de información o la falta de provisión de servicios básicos.

**PREGUNTA PARA EL FORO:** ¿Qué ejemplo de nuestra vida cotidiana, podríamos poner como “plan de contingencia”?

Ejemplo: tengo la sube, pero me quede sin saldo y no tengo un lugar de carga cerca, por suerte tengo mi celular que puedo cargar a la misma, aparte de que me prestan un saldo.



### RESPONDER EN EL FORO DE LA UNIDAD

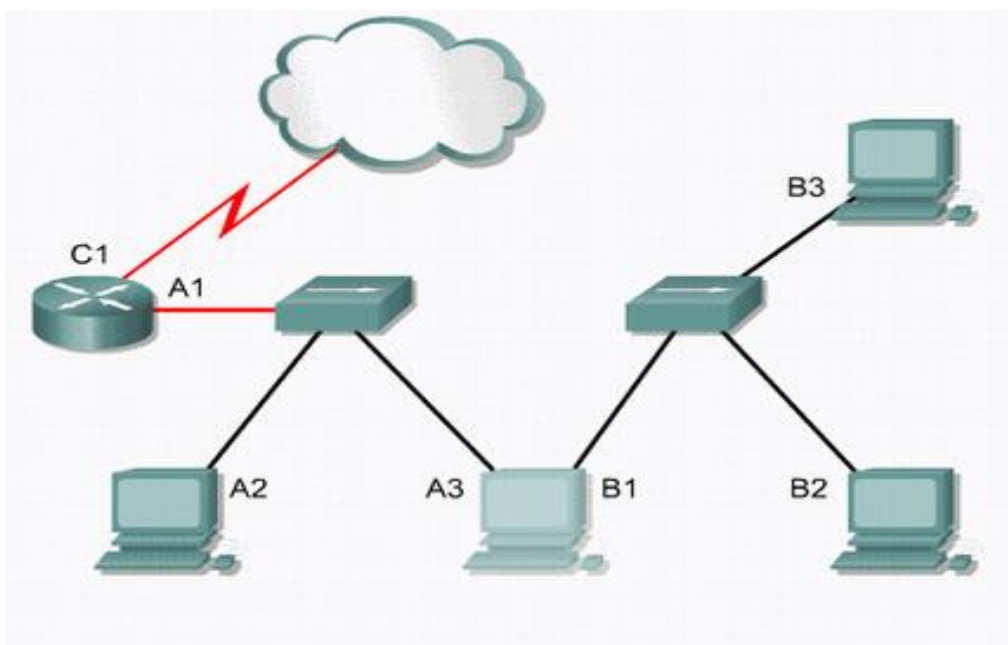
El hecho de preparar un **plan de contingencia** no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, supone un importante avance a la hora de

superar todas aquellas situaciones que pueden provocar importantes pérdidas, no solo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos largo.

### Ejercicio Número 1 Unidad 4



Observando el siguiente esquema de topología, cuantas situaciones o incidencias ¿podríamos poner como posibles problemas?



AYUDA: pensar en lo básico, conexiones, puntos que necesitan una contingencia.

**Consigna: A2 siempre tiene que llegar al equipo B3.**

**RESPONDER EN EL FORO DE LA UNIDAD**

La importancia del backup



Uno de los planes de contingencia es contar con un buen servicio de **backup**, sea datos, dispositivos o procesos.

Podemos encontrar servicios de **backup** online, lo cual de forma automática suben la información, para que en caso de un incidente, se pueda recuperar.

### Aspectos que hay que tener en cuenta

- Analizar la información que se debe guardar, tanto por su importancia para la continuidad del negocio como por requisito legal.
- Establecer una frecuencia para realizar las copias estableciendo un punto de retorno con el que la empresa pueda trabajar. ¿Puedes perder un día de datos? ¿Una semana? ¿Unas horas? ¿Cuánto te va a costar cada una de las opciones?



- Buscar un sistema de backup que sea incremental, es decir, que solo añada lo que ha cambiado desde el último backup. Así podrán ahorrar espacio y ancho de banda.
- Definir el tiempo que se deben mantener las copias. Algunos requerimientos legales obligan a mantener la información durante muchos años, en otros casos solo es interesante guardar la versión más reciente de los datos.
- Cada cierto tiempo realizar una prueba de restauración de las copias de seguridad. Una copia de seguridad es únicamente válida si comprobamos que se puede restaurar.
- Cifrar la información. Añadir una capa extra de seguridad a tus datos.
- Escoger una opción de **backup** en la nube, así estarán a salvo de cualquier tipo de catástrofe o robo que pueda ocurrir en las instalaciones de la empresa u organización.
- Documentar el proceso de backup y de restauración para que las personas responsables puedan actuar de la manera más ágil posible en caso de desastre y establecer alarmas por e-mail para avisar de la realización de las copias.



## Soporte y mantenimiento



Soporte y mantenimiento de servidores, muy comúnmente dicho: “administración de servidores”, es una función que se tiene cuando se necesita una administración completa y real de los mismos, obviamente sacando la tercerización (en otro momento hablaremos de esto), tener un manejo y control sobre lo que queremos, lo que ofrecemos y lo que necesitaremos en el/los servidores.

Teniendo en cuenta las necesidades para cumplir una buena administración, se arma un cronograma cuya función será el manejo de políticas que se aplicaran, relevando las debilidades que se encuentran y así poder mitigarlas o directamente anularlas.

Partes de estas necesidades son:

### **Máxima rapidez de asistencia**

Contar con técnicos que puedan atender inmediatamente las urgencias, hoy en día, utilizando mantenimiento remoto, abaratando costos.

## **Flexibilidad y Resolución de problemas**

Que se pueda poner a punto un sistema mal configurado, proceder a la actualización del sistema contra fallos de seguridad, o instalar nuevos servicios, así como también actualización de antivirus o parches de seguridad, que implicaría cortes de servicios o reinicio de los mismos.

### **Planificación**

La orientación principal de un plan de contingencia es la continuidad de las operaciones de la empresa, no sólo de sus sistemas de información.

Su elaboración la podemos dividir en cuatro etapas de 5 puntos posibles:

- 1. Evaluación**
- 2. Planificación**
- 3. Pruebas de viabilidad**
- 4. Ejecución**
- 5. Recuperación.**

La primera etapa es la unión de los 3 primeros puntos haciendo referencia a un componente preventivo.

Por último, las últimas son referidas a la ejecución del plan una vez ocurrido el siniestro/incidente:

- Copias de respaldo remoto
- Provisión de soluciones de comunicaciones e infraestructura de sistemas informáticos en caso de desastre.
- Ejecución de simulacros de ejecución del plan de contingencia al menos una vez al año, para comprobar que el plan de contingencias funciona de forma adecuada.
- Ejecución de pruebas de recuperación de datos.

**¿Sirve el mantenimiento preventivo?**



**El mantenimiento preventivo** es un tipo de mantenimiento informático que se debería realizar en todas las empresas. Con el mantenimiento preventivo se reducen al máximo los posibles problemas informáticos en la empresa a distintos niveles: infraestructura de red y comunicaciones, servidores y puestos de trabajo.

**En el mantenimiento preventivo** se realizan tareas de conservación de los equipos, software o instalaciones. En este tipo de mantenimiento informático se efectúa una revisión y mejora continua de todos los sistemas con el fin de que se garantice su buen funcionamiento.

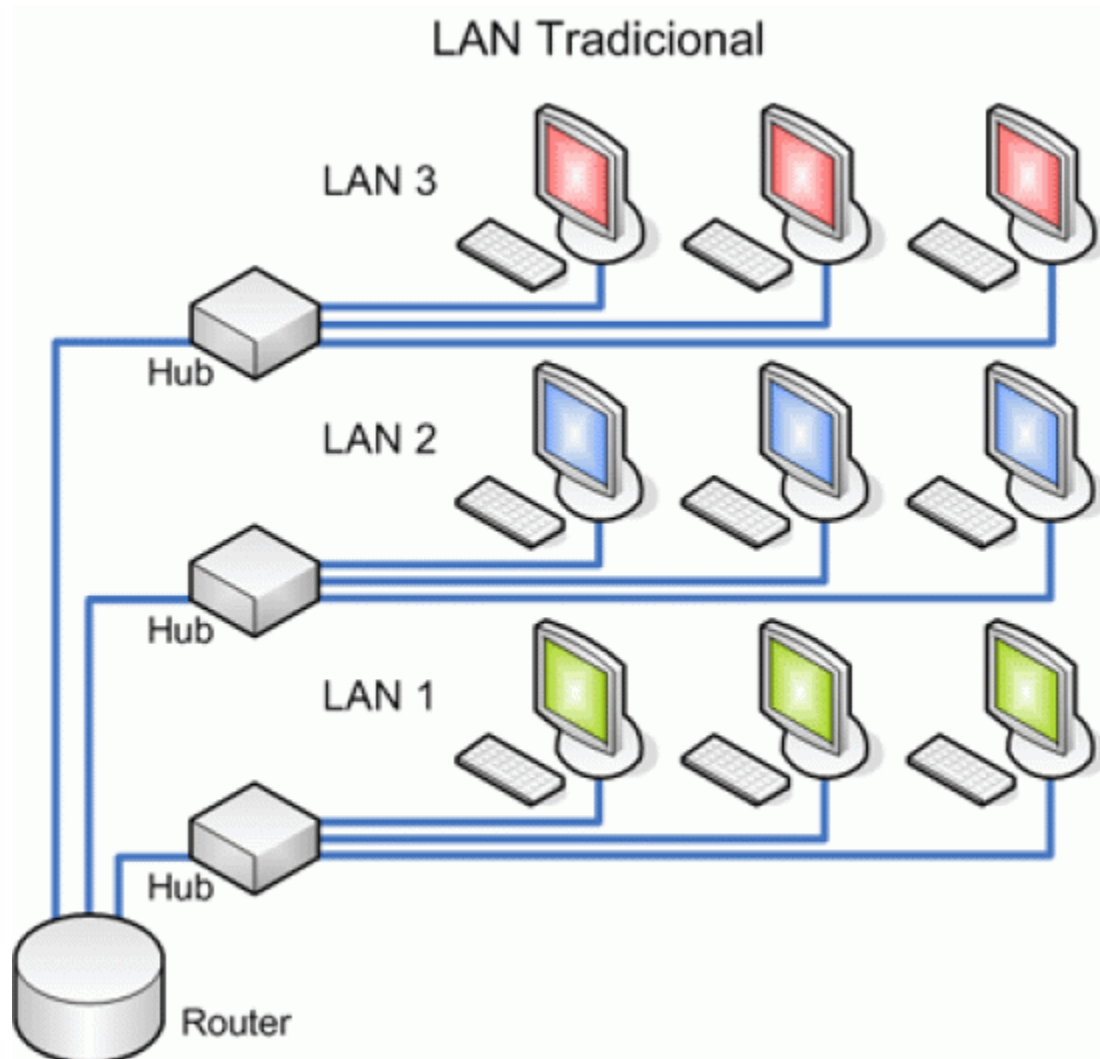
La principal diferencia que existe entre el **mantenimiento preventivo** y el **mantenimiento correctivo** es que el mantenimiento preventivo se realiza en equipos o software que tienen unas buenas condiciones de funcionamiento y el mantenimiento correctivo cuando ya ha surgido un fallo y necesita una reparación.

Se puede realizar en diferentes niveles, como son a nivel de infraestructura y red, servidores y puestos de trabajo. Independientemente del nivel, este mantenimiento siempre tiene el mismo objetivo prevenir futuras averías.

### **Infraestructura de red y comunicaciones**

En la infraestructura de red y comunicaciones de cualquier empresa se debe realizar un mantenimiento preventivo periódicamente para que no aparezcan averías en el futuro.

En cualquier tipo de empresa existen diferentes elementos que pertenecen a la infraestructura de red y comunicaciones como son el **cableado**, **armarios de comunicaciones** y servicios de red (**switches**, **routers**, **puntos de acceso**, **Firewall**, etc.).



Son todos los elementos hardware y software que intervienen en la transmisión de datos dentro de la empresa.

Switch, routers, cortafuegos, proxys, tarjetas de red, puntos de acceso, vpn's, radioenlaces, configuración de todos ellos.

A nivel de hardware hay que tener en cuenta los siguientes factores para realizar un buen mantenimiento preventivo informático:

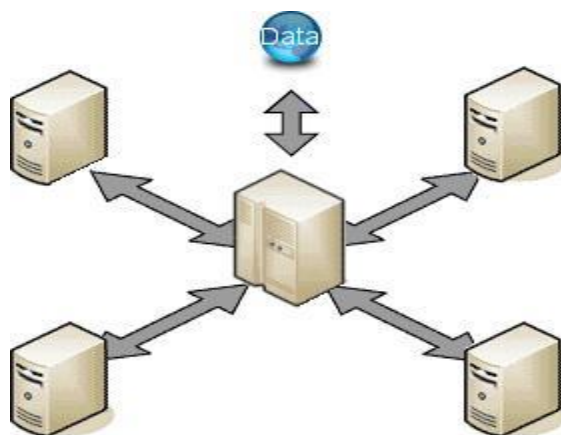
- Revisión de cableado de punto de conexión
- Comprobación del estado de la electrónica de red y switch
- Revisión de router y punto de acceso
- Posibilidad de ampliación, escalabilidad
- Limpieza física de la instalación y estado de la refrigeración
- Actualización y/o ampliaciones mejoras del sistema

A nivel de software tener en cuenta los siguientes factores para realizar un buen mantenimiento preventivo informático:

- Software de monitorización del estado de red (LAN y WIFI). Puntos críticos, servidores y puestos de trabajo
- Actualización firmware de los servicios de red
- Control de usuarios, de la red y limitación de entrada y salida de red

### Servidores

Los servidores de una empresa son muy importantes para el funcionamiento de la misma hoy en día, por lo que se debe tener en cuenta que se tiene que realizar un mantenimiento preventivo informático para que tengan un buen rendimiento.



Son los equipos de la organización y se encargan de proveer a la misma los servicios necesarios para la gestión, normalmente centralizada, de los procesos que se desarrollan en ella.

Algunos ejemplos de servidores dentro de una empresa son: correo electrónico, software de gestión centralizado, centralización y seguridad de archivos, bases de datos, páginas web...



Los servidores podríamos decir que son equipos informáticos de alto rendimiento y capacidad que contienen todos los datos de la empresa y el distinto software de gestión de la misma, siendo el equipo informático más importante de la empresa.

Los factores a nivel de hardware que hay que tener en cuenta a la hora de realizar un mantenimiento preventivo en una empresa en los servidores son:

- Garantizar que los componentes de los servidores estén a pleno rendimiento
- Predicción y comprobación de fallos de discos
- Comprobación del sistema de memoria
- Limpieza física y estado de refrigeración
- Actualización y/o ampliaciones mejoras del sistema

En cuanto al software los factores que hay que tener en cuenta en el mantenimiento preventivo de software de servidores son los siguientes:

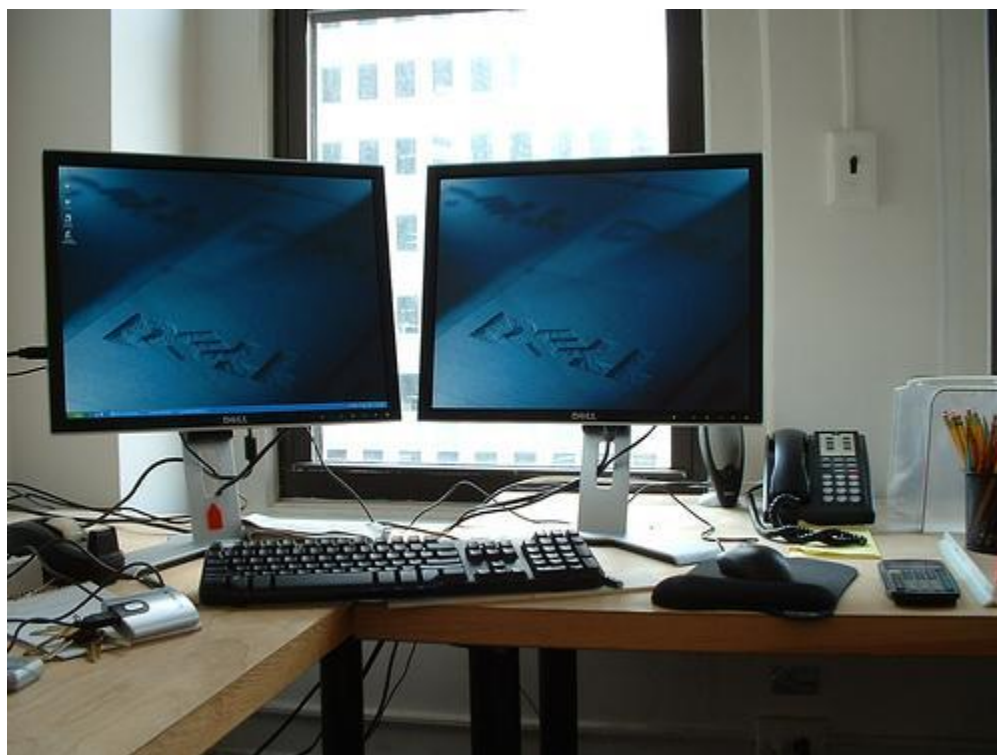
- Comprobación y actualización del sistema operativo
- Comprobación de aplicaciones propias de la base de datos y aplicaciones de clientes y servidor
- Mantenimiento, gestión y administración del servidor de correo
- Mantenimiento, gestión y administración de usuarios
- Gestión, administración y comprobación de copias de seguridad

### **Puesto de trabajo**

En el puesto de trabajo es donde se desarrolla la mayor parte de la actividad de la empresa, los usuarios trabajan toda la jornada laboral en los mismos, del funcionamiento de estos depende la productividad de la empresa.

También se debe realizar un mantenimiento preventivo informático, con el fin de que el puesto del trabajador funcione correctamente.

Son muchos los factores que pueden influir para que ocurra una avería, con ello se perdería ese puesto de trabajo durante un tiempo y el trabajador no podría desarrollar su jornada laboral con normalidad.



Al igual que en infraestructura de redes y comunicaciones y servidores en el puesto de trabajo se divide el mantenimiento preventivo en dos niveles, hardware y software.

Tener en cuenta en el hardware de un puesto de trabajo:

- Actualización y/o ampliaciones mejoras del equipo
- Limpieza física y revisión del sistema de refrigeración
- Comprobación de disco duros, memoria y componentes

Tener en cuenta en el software de un puesto de trabajo:

- Mantenimiento del sistema operativo
- Aplicaciones básicas de gestión del puesto de trabajo
- Aplicaciones de ofimática, correo, clientes y de la propia empresa



## Solución de problemas

Hoy en día, nos encontramos con inconvenientes que pueden ser críticos a la hora de estar aplicados en un servidor de producción, o leves cuando necesitamos instalar un nuevo servicio que no interrumpiría las funciones principales del servidor.

La función de un administrador de servidores, que esté a cargo del cuidado de los mismos, tiene que contemplar varios escenarios que se le pueden presentar, así poder solucionarlos en el menor tiempo posible.

El manejo de varios sistemas operativos, el conocimiento de hardware de servidores, el entendimiento de las políticas de acción en la empresa, son algunos de los ingredientes que harán de esta decisión algo positivo o no...

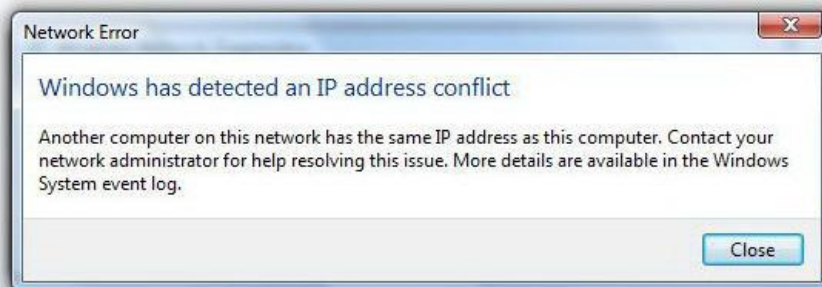
Ejemplo de lo que podemos encontrar:

### Problemas en entrega de IP por intermedio de un servidor DHCP

**Causa:** Un cliente solicita una dirección **IP** específica o intenta ampliar un permiso para su dirección IP actual. El servidor **DHCP** no puede encontrar la tabla de red **DHCP** para esa dirección.

**Solución:** Es posible que la tabla de red **DHCP** se haya eliminado por error. Se puede recrear la tabla de red agregando la red de nuevo mediante **DHCP** Manager o comandos de sistema

Obsérvese: “es posible”, un problema que puede ser muy deducible, no significa una confirmación del mismo, podría tranquilamente ser otro error, por ejemplo, duplicación de **IP**.



Ejemplo de lo que podemos encontrar:

## Problemas de acceso al servidor DNS

**Causa:** se obtiene acceso al servidor DNS mediante pruebas de red básicas, pero no responde a las consultas de DNS de los clientes.

**Solución:** si el cliente DNS puede hacer ping al equipo servidor de DNS, comprobar que el servidor DNS se haya iniciado y pueda escuchar y responder a las solicitudes de los clientes.

**Intente usar el comando “nslookup” para comprobar si el servidor**

**Puede responder a los clientes DNS.**

Obsérvese: “Intente”, una solución no siempre depende de nosotros.



Uf. Tenemos problemas para encontrar ese sitio.

No podemos conectar al servidor en [www.wpseguro.es](http://www.wpseguro.es).

**Si esa dirección es correcta, aquí hay otras tres cosas que puede probar:**

- Vuelva a intentarlo más tarde.
- Compruebe su conexión de red.
- Si está conectado a través de un cortafuegos, compruebe que Firefox tiene permiso para acceder a la web.

[Reintentar](#)

## Problemas de envío de mensajes a través del servidor de correo

**Causa:** los mensajes de Correo Electrónico (e-mails) no llegan a destino.

Son muchas las causas por las cuales no llegan a destino:

- El mensaje no salió del servidor de email de origen

- El mensaje se encuentra retrasado en algún servidor intermedio o aún está en la cola (queue) del servidor saliente

En este caso, obsérvese que las causas pueden ser varias, por lo que la solución también podría ampliarse en varios escenarios diferentes,

Solución: debería enviarse un email desde la cuenta que supuestamente presenta errores a otra cuenta distinta independiente del servidor de la cuenta remitente.

Por ejemplo enviar un email a otra cuenta de Hotmail, Yahoo, Gmail, etc., y a continuación verificar si le llega o no.

Si llega, obviamente el problema de que no salió sería descartado.



**Mail Delivery Subsystem** <mailer-daemon@googlemail.com>  
para mí ▾

🌐 inglés ▾ > español ▾ [Traducir mensaje](#)



### El mensaje no se ha podido enviar

Vas a enviar este mensaje desde otra dirección o alias con la función Enviar mensaje como. La configuración de tu cuenta de Enviar mensaje como no es correcta o se ha quedado obsoleta. Revisa la configuración e intenta enviarlo otra vez.

[MÁS INFORMACIÓN](#)

Esta es la respuesta del servidor remoto:

535 5.7.8 Error: authentication failed: authentication failure

## Ejercicio Número 2 Unidad 4



**Realizar una búsqueda en Internet y verificar cuántos posibles ataques distintos a correos electrónicos se pueden encontrar**

**En caso de conocer alguno, subir un ejemplo explicando en modo resumen, una captura, una descripción.**

### TIPS



**PHISHING:** uno de los más conocidos y utilizados, se aprovechan de los desconocimientos de los usuarios, donde el atacante logra incentivando o forzando a que la víctima realice un click en un proceso, lo cual puede llevar a obtener datos de importancia.

Comandos de red de importancia

En esta unidad, solicita al instructor un documento para su lectura y comprensión, donde a través del mismo, podrán ponerse al tanto de los comandos de Windows, más utilizados en todo lo relacionado con troubleshooting de redes e investigación de datos de los entornos de red.

**Te invitamos a que lo leas y que des tu opinión sobre el uso de los mismos respondiendo estas preguntas:**

**1- ¿Cuál piensan que es el objetivo principal de estos comandos?**

**2- ¿Si tuvieran la oportunidad de crear un nuevo comando de red, que te gustaría que haga?**

### Consejos para la administración segura

**No borrar, mover:** Es común borrar datos por error que más tarde requerimos durante el proceso de mantención de un servidor, no borrar, mover; crear un directorio temporal en /tmp/prueba y mover allí los datos que deseen borrar pero borrar el directorio al finalizar todo. Este simple consejo puede ahorrar trabajo extra causado por los típicos errores que uno comete.

## ¿Quieres mover los elementos a la papelera?

Los elementos movidos a la Papelera desaparecerán de



Tu biblioteca de Google Fotos



Todos los dispositivos sincronizados



Contenido como álbumes

**Guarda los comandos que has utilizado en un fichero de log:** llamado «work bash log» en similitud al conocido changelog. Resulta una muy buena práctica; trata simplemente de

documentar no sólo el proceso sino que los comandos en terminal que utilizan para realizar los procesos de administración, existen varias buenas razones para hacer esto, sin embargo, quizá la más importante sea que con el tiempo se aprenda a utilizar comandos cada vez más potentes, reducidos y sin causar daños colaterales.

Se puede incluso utilizar un comando que se llama "script" para automatizar la creación en un fichero de los comandos que ejecutar en terminal (como lo haría bash\_history pero sin necesidad de cerrar sesión).

```
root@myserver:~# tailf /var/log/apache2/access.log
::1 - - [13/Mar/2013:14:08:11 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:10:07 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:12:26 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:24:04 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:34:54 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:35:14 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:46:05 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:47:02 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:50:05 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
::1 - - [13/Mar/2013:14:51:08 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Debian) (internal dummy connection)"
```

**Ser paranoico es tu obligación, no una elección, pero hay un límite:** sea el tipo de servidor que sea excepto cuando no sea uno en tu red local casera, siempre y ante todo debes esperar que alguien atacara tu servidor, esta es casi una regla de oro en lo que respecta a administración de servidores.



Si dejas un servidor con la posibilidad de acceder por ssh como usuario root estás perdido; si dejas un servidor sin un firewall adecuado estás perdido; si dejas un servidor apache sin módulos



de seguridad estas perdido, y así hay mil ejemplo de prácticas comunes en temas de seguridad que no se necesita ser hacker para utilizar.

**Controla el acceso físico a la máquina:** Esto tiene mucho que ver con el punto anterior, pero hay que recalcar, ambos (acceso físico y por software) son importantes, no se saca nada teniendo un servidor totalmente protegido a nivel de software con firewall espectaculares si el acceso físico a la máquina es cosa de niños.



Hay que tomar el control de servidores en forma física (con autorización claro) en minutos, tener acceso físico a un servidor es incluso peor que no utilizar contraseña para acceder vía ssh por ejemplo.

### A tener en cuenta

A veces uno por ser muy paranoico, ante el menor evento de incidencia, podría ejecutar una tarea o proceso que pueda llegar a complicar o aumentar el riesgo en que se encontraba, por eso hay que tener mente despejada y abierta ante de tomar decisiones.

Se expondrá a continuación, lo que debemos tener en cuenta, basándonos cuando uno piensa que tiene un malware en la máquina o dispositivo, y piensa en borrar todo lo que no conoce, la idea es saber lo que **NO HAY QUE HACER con los procesos activos**.

**PROCESOS IMPORTANTES = NO BORRAR - TOCAR o MODIFICAR !!!!**

**System** maneja el Kernel, que es aquel software que constituye una parte fundamental del Sistema Operativo.

Por ejemplo, **System** hospeda los drivers que aseguran que el software pueda comunicarse con el hardware.

Administrador de tareas

Archivo Opciones Vista

Procesos	Rendimiento	Historial de aplicaciones	Inicio	Usuarios	Detalles	Servicios
Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
svchost.exe	6516	En ejecución	SYSTEM	00	372 K	No permitida
svchost.exe	9612	En ejecución	Laboratori...	00	532 K	Deshabilitada
svchost.exe	4264	En ejecución	SYSTEM	00	564 K	No permitida
svchost.exe	7472	En ejecución	SYSTEM	00	284 K	No permitida
svchost.exe	7892	En ejecución	SYSTEM	00	384 K	No permitida
svchost.exe	3092	En ejecución	LOCAL SE...	00	932 K	No permitida
svchost.exe	8364	En ejecución	LOCAL SE...	00	216 K	No permitida
svchost.exe	8416	En ejecución	LOCAL SE...	00	352 K	No permitida
System	4	En ejecución	SYSTEM	00	20 K	
SystemSettings.exe	7828	Suspendido	Laboratori...	00	0 K	Deshabilitada

Si cierra System, se perderá el acceso al disco duro o a sus dispositivos USB.








**Su dispositivo se quedará bloqueado** y tendrá que hacer un cierre forzoso.

**Winlogon** está asociado al famoso **Ctrl + Alt + Supr.**

También activa el protector de pantalla o **bloquea tu PC después de un tiempo de inactividad.**








Cierra winlogon.exe y tu PC tan solo mostrará **una ominosa pantalla negra.** Tendrá que forzar un reinicio.



 VBoxSVC.exe	11580	En ejecución	Laboratori...	00	1.760 K	Deshabilitada
 Video.UI.exe	11132	Suspendido	Laboratori...	00	0 K	Deshabilitada
 VirtualBox.exe	1752	En ejecución	Laboratori...	00	1.432 K	Deshabilitada
 WindowsInternal.Co...	8092	En ejecución	Laboratori...	00	2.496 K	Deshabilitada
 wininit.exe	616	En ejecución	SYSTEM	00	4 K	No permitida
 winlogon.exe	688	En ejecución	SYSTEM	00	932 K	No permitida
 YourPhone.exe	8568	Suspendido	Laboratori...	00	0 K	Deshabilitada

**Wininit**, carga herramientas y servicios básicos nada más se enciende el ordenador.

Es como un “despertador” para múltiples procesos igual de importantes como lsass.exe o lsm.exe.

 WindowsInternal.Co...	8092	En ejecución	Laboratori...	00	2.480 K	Deshabilitada
 wininit.exe	616	En ejecución	SYSTEM	00	4 K	No permitida
 winlogon.exe	688	En ejecución	SYSTEM	00	940 K	No permitida
 CompPkgSrv.exe	7036	En ejecución	Laboratori...	00	104 K	Deshabilitada
 csrss.exe	540	En ejecución	SYSTEM	00	528 K	No permitida
 csrss.exe	624	En ejecución	SYSTEM	00	596 K	No permitida
 ctfmon.exe	5844	En ejecución	Laboratori...	00	6.136 K	Deshabilitada

Las dos tareas más importantes de **csrss.exe** son cerrar Windows y lanzar el proceso conhost.exe que, a su vez, **lanza los Comandos de Windows. (Pantalla azul peligro).**

### Windows Session Manager (smss.exe)

smss.exe es el “despertador” del ya mencionado winlogon. **Si smss.exe no arranca, winlogon no arrancará** y tal vez se produzca una paradoja temporal. Además, smss.exe “vigila” que ciertos procesos críticos marchen bien y prepara el arranque de algunos drives en el inicio. Cierre smss.exe prematuramente y se colgará el PC.

### Windows Shell Experience Host

He aquí un proceso que debutó en Windows 10. Es el proceso encargado de darle un toque moderno a elementos clásicos como **el calendario o el reloj**. También se encarga del color y de los efectos de transparencia del Menú de Inicio y de la Barra de Tareas.

### **Windows Explorer (explorer.exe)**

**explorer.exe** lleva muchos elementos de la interfaz gráfica. Si cierra este proceso, se cerrará cualquier ventana del Explorador de Archivos y **no podrás usar el Menú de Inicio o la Barra de Tareas**.

No obstante, reiniciar este proceso sí que puede ser útil.

Si nota que el Menú de Inicio o la Barra de Tareas hacen un funcionamiento inadecuado (su rendimiento es lento, se bloquea a ratos), **reiniciar explorer.exe** y posiblemente se solventará los problemas.

Es un proceso más rápido que reiniciar todo el ordenador.

### **Ejercicio Final Módulo 2**



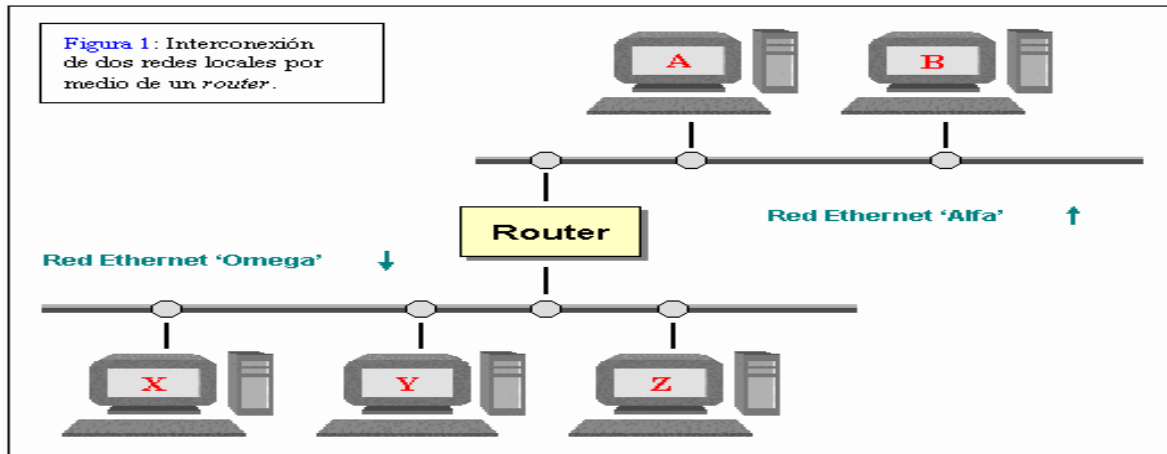
A continuación se mostrarán distintas topologías las cuales tendrán que definir qué problemas pueden encontrarse y cuales serian sus soluciones de acuerdo a lo enseñado o deducción por experiencia

El tiempo de entrega, será el especificado por el instructor, para que sean corregidos lo más pronto posible, lo entregado fuera de fecha no tiene fecha de corrección, por lo que es recomendable subirlo a tiempo.

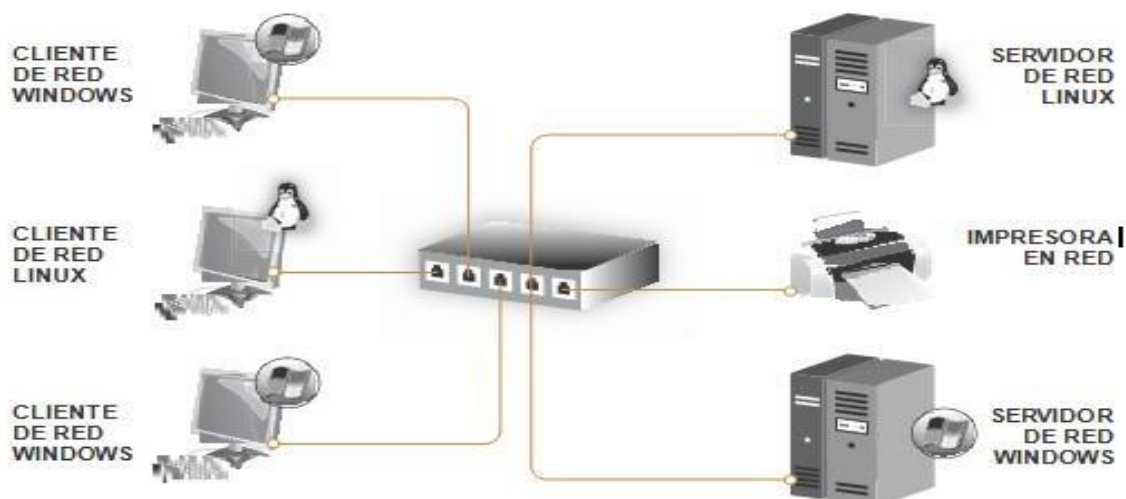
Pueden seleccionar cualquiera de los tres o todos, y presentarlos en el foro correspondiente al final del módulo.

Del gráfico expuesto, deducir y exponer 3 problemas en esta topología, y que aplicarían para mitigar o solucionar los mismos

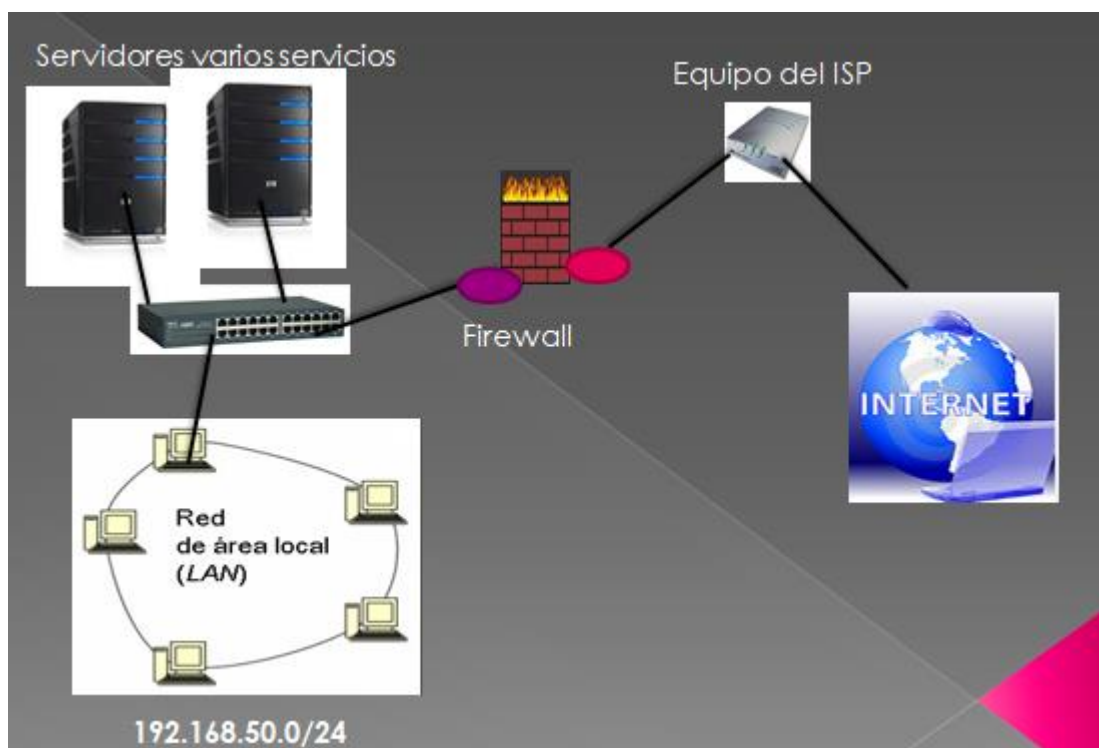
Ejemplo: si el direccionamiento IP es igual en ambos lados, la solución sería al haber un router en el medio, cambiar el direccionamiento de ambas redes



2- Usted pertenece al área de soporte y se encuentra con este escenario, explicar los pasos a seguir que piensa que son necesarios para que la red funcione adecuadamente, esto significa que cambiaría o agregaría en cuanto a lo enseñado.



3- De acuerdo a lo que vemos, que podríamos agregar para mejorar esta red, puede ser aspectos físicos como nuevo hardware o lógicos como servicios de Vlan.



## **IMPORTANTE**

**Para evitar confusiones, el trabajo será interpretado por el instructor de acuerdo a lo que USTEDES expliquen qué entendieron, por favor, no enviar mails al instructor, preguntando qué se quiere decir en el dibujo.**

**Se solicita en los ejercicios, lo que ustedes consideren soluciones, cambios, etc.**

**Dudas o consultas, por mail al instructor**

**Por favor, no preguntar nada del ejercicio final en el foro, la misma será borrada**

**En caso de querer realizar los dos ejercicios, avisar luego de subirlos al instructor.**

## **Cómo presentar los ejercicios de la unidad**

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido\_UnidadX.doc (donde apellido será el de cada uno y la “X” el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy **IMPORTANTE** que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

### **Los ejercicios de esta unidad no llevan calificación**

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.



## Bibliografía utilizada y sugerida

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learn the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU