Resolución de incidencias en una red local.

Caso práctico

Julia, la técnica superior en Administración de Sistemas Informáticos en red que está realizando la instalación de redes de área local en la academia de Antonio, se encuentra conversando por teléfono con su prima Laura, que es una directiva de unas oficinas de un banco.

- Tenemos un poco de lío hoy en la oficina. Resulta que se ha caído el sistema y no podemos trabajar. - Laura, pero ¿desde cuando estáis con ese problema? - Pues llevamos unos días que la red a veces nos fallaba y ahora lo están intentando solucionar. ¿De que crees que puede ser, Julia? - Para poder hacer un diagnóstico de un problema en una red hay que hacer una serie de pasos para tratar de entender el problema y así buscar una solución. No es una tarea sencilla, aunque sí muy importante. - Ojalá que el problema esté resuelto en poco tiempo, tenemos tanto trabajo… - Si necesitáis ayuda, me llamas, que puedo ir a echar una mano.

Como se desprende de esta conversación, una vez que ya tenemos una red en marcha, la principal tarea que hay después es la del mantenimiento y resolución de posibles incidencias en la red. El problema que tiene esta tarea es que es compleja y difícil puesto que los problemas con los que te puedes encontrar en una red son muchos y muy variados.

Cuando te incorpores al mundo laboral y trabajes como técnico o técnica de Sistemas Microinformáticos y Redes, te darás cuenta de que la tarea más difícil que te vas a encontrar será una avería o mal funcionamiento de una red. Además, es probable que sea necesario que esta avería se resuelva con rapidez porque esto puede suponer pérdidas económicas o desconfianza de los clientes.

Las **tareas de administración de redes y de localización de averías** son muy complejas, puesto que las redes de hoy en día tienen gran cantidad de servicios y muchos usuarios y usuarias dependen de ellas. Una avería puede aparecer de muchas maneras, desde una avería que afecta a un solo puesto, por ejemplo, que no se puede conectar a la red o que afecte a todos los puestos, como por ejemplo, la caída de un servidor.

Después de identificada la causa por la cual la red está averiada, es necesario atajar la situación a través de una serie de acciones para intentar solucionarlo. Es más eficiente que estas acciones estén bien definidas y estructuradas que ponerse a probar cosas sin sentido.

Te propongo ahora que veas la siguiente **presentación**, donde se hace un recorrido por los distintos apartados de los que consta el tema, para que tengas una idea global de lo que vas a aprender en esta última unidad.

Resumen de la unidad

RESOLUCIÓN DE INCIDENCIAS EN UNA RED LOCAL

1.- INTRODUCCIÓN

- Importante seguir unos pasos en la resolución de incidencias.
- Planificar y preparar una estrategia de actuación.
- Tener información disponible a mano.
- Comprobar y descartar problemas en función del error.

Parámetros de rendimiento

- Velocidad de transferencia.
- Tiempo de respuesta.
- Paquetes de datos que circulan correctamente.
- También depende la finalidad de la red.

Resumen de la unidad

Condiciones físicas y ambientales

- Condiciones físicas:
  - Tamaño de los armarios.
  - Ubicación de los armarios.
- Condiciones ambientales:
  - Temperatura y humedad.
  - Ruidos.
  - Inundaciones, iluminación e incendios.

Incidencias en redes locales

Tipos de incidencias:

- Incidencias físicas
  - Fallos en tarjetas de red, cableado, dispositivo de interconexión…
- Incidencias lógicas
  - Ataques a la seguridad, software espía, correo spam, etc.

Resumen de la unidad

2.- MONITORIZACIÓN

- Herramientas disponibles:
  - Comprobadores de red.
  - Monitores de red: se incluyen en los propios sistemas operativos.
  - Analizadores de red: rastrean todo el tráfico de la red.

Protocolo SNMP y logs del sistema

- SNMP: Protocolo utilizado en la capa de aplicación del modelo OSI.
- Recoge información de la red a través de unos agentes.
- Logs del sistema: Recogen información sobre lo sucedido en el sistema en un intervalo determinado.

Resumen de la unidad

3.- HERRAMIENTAS DE DIAGNÓSTICO

- En Windows:
  - Centro de Redes y recursos compartidos.
  - Una serie de comandos.
- En Linux:
  - Monitor del sistema.
  - También dispone de unos comandos muy parecidos a Windows.

Problemas de acceso a redes

- Tipos de problemas a los que nos podemos enfrentar:
  - Problemas de conexión de un equipo a la red.
  - Problemas de conexión en una red cableada.
  - Problemas de conexión en una red inalámbrica.

Resumen de la unidad

4.- PREVENCIÓN DE RIESGOS PROFESIONALES

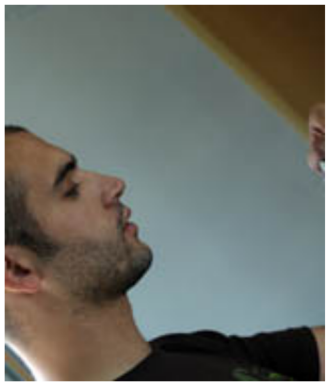
- Riesgos a los que nos enfrentamos.
- Medidas de prevención:
  - Ergonomía en el trabajo.
  - Riesgo eléctrico.
  - Riesgo de caídas.

Normativa de prevención

- Distintas leyes de prevención a nivel:
  - Europa.
  - España.
  - Comunidades.
- También existe normativa de protección ambiental.

Introducción.

Caso práctico



Julia se encuentra ahora comentando con Samuel, el técnico auxiliar de Sistemas Microinformáticos y Redes sobre la conversación que acababa de mantener con su prima Laura.

- Tienen un gran problema en la oficina de mi prima Laura, se les ha caído el sistema… - En casos como esos, lo mejor es intentar acotar el problema hasta encontrar cual es el origen y así intentar resolverlo más rápidamente, aunque eso no siempre es fácil, ¿verdad Julia? - Sí, es muy importante tener un método de trabajo bien claro puesto que los problemas que puedes encontrar en una red son muchos y muy variados. También es importante conocer los errores más comunes que te puedes encontrar. - El tema de las incidencias en una red es tan amplio…

Como acabas de leer en la conversación que mantenían Julia y Samuel, es más muy importante utilizar un método bien definido para actuar frente a un problema que ponerse a probar todo lo que sabes sin ningún sentido. Esto es debido a la complejidad en la resolución de los problemas en una red. Un método estructurado en una serie de pasos será mucho más eficiente, aprovecharás mejor el tiempo y evitarás que los problemas puedan complicarse más de lo que ya están.

Te puede resultar útil, para ir empezando a familiarizarte con este tema, tomar estos pasos genéricos que habrías de llevar a cabo si te encuentras con algún problema en una red:

1. El primer paso es tener claro **cuál es el problema** al que te estás enfrentando y cuales son sus síntomas. A partir de estos datos puedes describir las causas que han podido producir el problema.
2. El siguiente paso será intentar **recoger toda la información** posible sobre el problema concreto. Preguntarás a todos los usuarios y usuarias afectados y podrás utilizar herramientas que te permitirán recoger información sobre el sistema.
3. Después de tener toda la información, necesitas hacer un **listado de los problemas** que puedes encontrarte en la red, desechando aquellos que no guardan relación con los hechos. Así te podrás concentrar en aquello que tiene realmente importancia.

4. Tienes que establecer un **plan de acción** según los problemas que has establecido.
5. En este paso es donde tendrás que pasar del papel a la práctica, realizando todas las acciones de forma ordenada y comprobando que los síntomas desaparecen.
6. **Si los síntomas no desaparecen**, tendrás que volver a empezar desde el paso cuatro.

Debes conocer

El siguiente enlace propuesto es un enlace a una página Web donde se explica de manera clara cuales son lo pasos en la resolución de incidencias. El contenido de la página es extenso y muchos de los apartados se trabajarán a lo largo de esta unidad, pero es interesante que tengas una visión global y aprecies la importancia que tiene el ser riguroso con los pasos para la resolución de problemas en redes.

Solución de problemas en una red.

Estrategias.

Es muy importante en el tema de la resolución de incidencias, que tengas en cuenta alguna estrategia para enfrentarte a este trabajo. Una estrategia es un conjunto de acciones que tendrás que llevar a cabo para conseguir tu objetivo. El objetivo principal es que una red de área local funcione y si aparece algún problema, que éste sea resuelto en un breve espacio de tiempo.

Para realizar esta tarea te facilitará mucho el disponer de toda la información posible del estado de la red, además de estar bien preparado ante un eventual problema. Es muy recomendable que dispongas de las siguientes informaciones:

- Tener un **mapa de red actualizado**, con la topología, las direcciones de los equipos y dispositivos de interconexión.
- Mantener una **lista de las direcciones y puertos** que son accesibles desde el exterior.
- Guardar **información de los servidores** de red, si es que hay alguno instalado.
- Mantener una l**ista bien documentada de los diferentes problemas** que hayan ido surgiendo en la red, es decir, que indiquen que problemas han surgido y como se han solucionado.

Una de las cosas más importantes y que debes tener en cuenta a la hora de enfrentarte a un problema en la red es el hecho de hacer las cosas de forma organizada, siguiendo unos pasos. Es muy importante que siempre tengas a tu disposición toda la información sobre como está diseñada la red, las direcciones IP que ha de tener cada máquina. Es muy recomendable que tengas a mano los diagramas lógicos y físicos de la red. Así, en un primer vistazo, podrás comprobar si el error es de configuración del equipo o, por el contrario, se trata de algún componente que no funciona adecuadamente.

Autoevaluación

¿Cuál de las siguientes opciones no es necesario tener en cuenta a la hora de arreglar una incidencia en la red?

- ○ No necesitas saber las direcciones que usan los equipos.
- ○ Guardar información sobre los servidores.
- ○ Documentar los errores producidos.
- ○ El sistema operativo con el que trabaja el equipo.

No es correcta porque si es necesario saber la configuración de cada equipo.

Incorrecta, porque es necesario conocer sus características.

No es la respuesta correcta porque esto siempre ayuda en el futuro.

Muy bien. Nos es indiferente el sistema operativo utilizado para resolver problemas en la red.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

Parámetros de rendimiento.

Antes de explicar los parámetros de rendimiento en una red de área local, te será útil tener una idea de que significa la palabra rendimiento. El rendimiento es la proporción entre el resultado obtenido y los medios utilizados para conseguir ese resultado. Se trata de indicar si la red nos da los servicios esperados en función de cómo son las tecnologías invertidas en su construcción.

Es importante que sepas que uno de los parámetros de rendimiento de una red será la **velocidad de transferencia** de la red. Te será fácil de calcular y así saber si la red está funcionando de forma óptima.

Otro parámetro de rendimiento que debes conocer será el número de **paquetes de datos que circulan de forma correcta** entre dos nodos de red. En el camino entre ambos nodos, los paquetes pueden alterarse. Si el número de paquetes que llegan a su destino sin alterarse es alto, significa que la red tiene un buen rendimiento.

Otra medida del rendimiento es el **tiempo de respuesta**. Este factor también es determinante. La velocidad de transferencia entre dos nodos puede ser alta pero puede suceder que tengas una red en la que dos nodos tardan mucho en conectarse, con lo que el rendimiento de la red ha bajado. Este parámetro de rendimiento será fundamental en algunos tipos de redes, por ejemplo, en un juego online en el que las reacciones de los jugadores se demoran varios segundos en llegar a su destino.

El rendimiento de una red depende de más factores, como por ejemplo, la tecnología utilizada para la red, el diseño de la red, el sistema operativo de red, los adaptadores de red, etc…

Además, el rendimiento adecuado de red en concreto puede ser distinto según la finalidad para la que se ha diseñado dicha red. No es lo mismo el rendimiento exigido a una red cuyo objetivo es compartir una impresora, que el rendimiento exigido a una red donde se comparten datos en tiempo real, como en un juego online.

Te propongo ahora que sigas las siguientes indicaciones sobre distintos modos de averiguar los parámetros de rendimiento en una red.

- Controlar el ancho de banda de la red: Administrador de tareas de Windows (Control+Alt+Supr y haz clic en la ficha funciones de red)
- Monitor de rendimiento: Inicio -> Panel de control ->Herramientas administrativas -> Monitor de rendimiento. Si no están presente las Herramientas administrativas (Windows 7 y Windows XP) tenemos que realizar los siguientes pasos: Menú inicio -> Personalizar -> Herramientas Administrativas -> Mostrar en el menú todos los programas y en menú inicio.

Ambas herramientas se utilizan para obtener información sobre los distintos parámetros de rendimiento que hemos comentado en este apartado.

Autoevaluación

¿Cuál de los siguientes factores es determinante en el rendimiento de una red?

- Velocidad de transferencia y finalidad de la red.
- Uso de los recursos.
- Velocidad de transferencia, tiempo de respuesta y paquetes de datos que circulan de forma correcta.
- Número de usuarios en la red.

No es correcta porque hay una que no es determinante.

Incorrecta, porque es no un factor básico.

Muy bien. Has captado la idea.

No es la respuesta correcta porque no influye en el rendimiento.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Condiciones físicas de una red.

Has de tener siempre presente que para que una red de área local funcione correctamente y alcance los parámetros de rendimiento esperado para esa red en concreto, es muy importante tener en cuenta una serie de factores a la hora de hacer una correcta instalación de la red. Una red que no esté bien instalada respetando una serie de condiciones, es más probable que con el tiempo nos de más problemas.

Dentro de la de instalación de una red empezarás viendo aquellas condiciones que tienen que ver con la **instalación física** de la red.

La primera de ellas se trata de decidir donde se **ubican los armarios de cableado**. Los armarios de cableado recogen los cables y dispositivos de interconexión central de una red, por lo que su ubicación es importante. Tendrás que tener en cuenta para llevar a cabo la decisión de donde instalarlo qué necesidades de suministro necesita, como la toma de corriente, toma de tierra y climatización. Ha de estar situada lo más cerca posible del sitio donde estará la red, pero impidiendo el acceso no autorizado, cumpliendo todo el tiempo con las normas de seguridad.

Respecto a las normas de seguridad de los armarios de cableado se tendrán en cuenta para decisiones como la ubicación, materiales para paredes, suelos y techos, temperatura, humedad, iluminación, toma de corriente, acceso a la sala y al equipo y soporte y acceso a los cables.

Otro aspecto importante que tendrás que valorar será el **tamaño del armario de cableado**. En función del tamaño de la red y de su crecimiento previsto en el futuro, se elige el tamaño del armario de cableado. Ha de ser lo suficientemente grande como para tener los dispositivos de interconexión y el cableado, contemplando las ampliaciones futuras. A veces es suficiente con un armario pequeño en la misma sala donde tenemos la red de área local cerrado con llave, y otras veces estará en un armario de gran tamaño en otra sala distinta de donde se encuentra la red.

Condiciones ambientales de una red.

Las condiciones ambientales de una red son muy importantes como te puedes imaginar, ya que de ellas depende el buen funcionamiento de éstas. Las condiciones ambientales se han de tener en cuenta sobre todo para prevenir posibles accidentes fuera de nuestro control. Si alguno de estos accidentes sucediera, deberás tener la red preparada para que sea afectada de un modo mínimo. Como te puedes imaginar, este tipo de accidentes serán, por ejemplo, inundaciones o incendios. Aunque ahora las tienes aquí señaladas:

- **Temperatura y humedad**: La temperatura del armario de cableado debe mantenerse entre 18º y 24º centígrados y una humedad relativa entre el 30% y el 55%.

- **Ruidos e interferencias electromagnéticas**: Son aquellas que están causadas por lámparas fluorescentes, líneas de alta tensión, motores, microondas, teléfonos móviles, etc. Estas interferencias pueden causar errores en la transmisión, por eso, es importante elegir la ubicación de la red donde estas interferencias sean mínimas.
- **Inundaciones**: Hay que proteger a los armarios de posibles inundaciones, evitando instalarlos cerca de algún lugar con amenaza de inundación, como tuberías.
- **Iluminación**: Los armarios deben estar bien iluminados, con luz situada en el techo, colores claros en las paredes y hacer uso de la luz de emergencia.
- **Incendios**: Los armarios deben estar protegidos de incendios. Esto implica que haya extintores, detectores de humo, pintura ignífuga y demás medidas de seguridad contra incendios.

Se puede concluir que es de gran importancia el como se realice la instalación de una red, teniendo en cuenta las condiciones físicas y ambientales, para que esto repercuta en un mejor rendimiento de la red.

Autoevaluación

¿Cuál de las siguientes opciones hay que tener en cuenta como condición ambiental en el diseño de una red?

- ○ Número de administradores de la red.
- ○ Temperatura de los armarios.

- Cercanía entre un equipo y la impresora.
- Sistemas operativos utilizados.

No es correcta porque no es importante.

Muy bien. Esto no se tiene en cuenta como condición ambiental.

Incorrecta, no es una condición ambiental.

No es la respuesta correcta porque no es una condición ambiental.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Incidencias en redes locales.

Como te puedes imaginar, en función de los problemas que te encuentres en una red de área local, la forma de actuar será distinta en cada caso. Es por eso importante que conozcas cuales son las incidencias más comunes con las que te puedes encontrar para poder luego buscar una posible solución del modo más eficiente.

Las incidencias en una red local se pueden dividir en dos apartados:

- **Incidencias físicas**: Son aquellas que tienen que ver con algún dispositivo físico que tengamos instalado en la red, como la tarjeta de red o el cableado utilizado.

- **Incidencias lógicas**: Son aquellas que tiene que ver con el mal funcionamiento de algún programa, como por ejemplo, que una impresora no imprima o que un ordenador tenga un virus.

En los dos siguientes apartados verás un listado con las incidencias más comunes con las que te vas a encontrar a la hora de trabajar en una red de área local.

Para saber más

En el siguiente enlace encontrarás una plantilla tipo de las que son necesarias rellenar por los usuarios y usuarias de una red cuando se encuentran con una incidencia en la red. Es interesante que veas con detalle como se recogen todos los posibles síntomas, que son los que te acercarán a encontrar una solución de forma más rápida y eficiente.

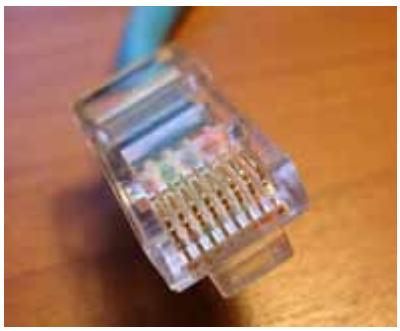
Parte de incidencias.

Incidencias físicas.

Como acabas de ver en el apartado anterior, una incidencia física es aquel problema que puede surgir en la red por el mal funcionamiento de algún componente físico en la red. Verás en el siguiente listado los problemas más comunes:

- **Fallos en las tarjetas de red**: La primera comprobación que has de hacer es comprobar si sus LED están parpadeando. Si están en verde es que funciona bien y si está en amarillo es que tienen algún problema. Aunque esto dependerá del fabricante. En caso de que no funcionara bien hay que:
  - Comprobar que el cable de red está bien conectado a la tarjeta.
  - Verificar que el dispositivo de interconexión está conectado a la toma de corriente.
  - Asegurarse de que el conector está bien conectado al dispositivo de interconexión.
  - Revisar que la tarjeta de red está bien instalada.

- **Fallos de los cables**: Que los cables estén en buen estado. Si estos fallan hay que:
  - Revisar el estado de los conectores de los dos extremos del cable.
  - Analizar la conexión entre los cables y las tarjetas de red.
  - controlar la conexión entre los cables y los dispositivos de interconexión.
  - Comprobar que los cables no superan la longitud máxima para su categoría.
  - Examinar el estado del cable en sí.



- **Fallos de los dispositivos de interconexión**: Un fallo en uno de estos dispositivos puede dejar sin conexión a uno o a varios nodos de la red, en función de cuál sea el fallo. Si estos fallan hay que:
  - Comprobar que el dispositivo de interconexión está conectado a la red.
  - Comprobar que el dispositivo de interconexión no está recalentado.
  - Si el problema solo afecta a un equipo de la red, puede deberse a un fallo en el puerto al que está conectado. En ese caso el led de dicho puerto estará apagado y probarás a utilizar otro puerto.

- **No se puede acceder a alguna máquina**: En este caso tendrías que comprobar que la máquina está encendida, que no tiene fallos en la tarjeta de red o en los cables y por último ejecutar un comando ping a la máquina.

Debes conocer

En el siguiente enlace tienes un artículo sobre como se resuelven los problemas de cableado físico que te puedes encontrar en una red. Se explica como se localizan y como se reparan.

Localizar y resolver problemas en los cables de red.

Autoevaluación

¿Cuál de los siguientes fallos es una incidencia física?

- Cable de red mal conectado.
- Virus informático.
- Gestor de arranque defectuoso.
- Correo electrónico no deseado.

Muy bien. Has captado la idea...

No es correcta porque eso es un fallo lógico.

Incorrecta, porque eso no es un fallo físico.

No es la respuesta correcta porque no es un fallo físico.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

Incidencias lógicas.

Al igual que en el apartado anterior, verás ahora un listado de las incidencias lógicas más comunes que puedes encontrarte cuando realices un trabajo de mantenimiento de una red de área local. Las incidencias lógicas se refieren a posibles fallos de un programa o a una configuración errónea de alguno de ellos.

- **Incidencias provocadas por ataques a la seguridad**: Pueden ser ataques de muy distintas formas, pero has de tener en cuenta que los efectos que producen son los siguientes:
  - Destrucción de la información almacenada en el disco duro.
  - Destrucción o inutilización del sistema operativo.
  - Borrado de la BIOS.
  - Destrucción del disco duro, inutilizándolo.
  - Apertura de una puerta trasera que permita el acceso no autorizado a nuestro ordenador.
  - Impedir la ejecución de determinados programas.
  - Recopilación de información de nuestro ordenador y envío de dicha información a otro (spyware o software espía).
  - Consumo de recursos de nuestro ordenador.
  - Envío de tráfico inútil para saturar la red.
  - Mensajes en la pantalla de vez en cuando.
  - Envío de spam a nuestra cuenta de correo electrónico.
  - Lectura no autorizada de nuestro correo electrónico.
  - Colapso de servidores.

Este tipo de incidencias se pueden resolver, pero has de saber que también son evitables si tomamos ciertas medidas de prevención en nuestro equipo. Entre ellas destacan:

- Uso de antivirus actualizados.
- Uso de cortafuegos (firewall).
- Acceso a los equipos protegidos por usuario y una buena contraseña.
- Uso de técnica de cifrado de los datos que guardamos en nuestros equipos y los que viajan por la red.
- Activación de las funciones de seguridad de los navegadores Web.
- Uso de protocolos de seguridad en caso de redes inalámbricas.

Con estas medidas, es posible que la mayor parte de los problemas arriba citados los tengas bajo control. Además, existe software disponible para escanear el estado de nuestro equipo y hacer limpiezas exhaustivas.

Para saber más

Existen muchos programas gratuitos en Internet muy potentes que te facilitaran la tarea de chequear el estado de un equipo o limpiarlo en caso

de que algo no funcione bien. Como ejemplo, te dejo aquí el enlace de la página oficial del programa Ad-Aware. Se trata de un programa antiespía, capaz de detectar spyware, adware, troyanos y demás complementos. En la última versión también incluye antivirus.

Programa Ad-Aware.

Además de todos los enlaces que has ido visitando, se proponen como visita no obligatoria los siguientes enlaces a páginas Web. Aunque están escritas en inglés, se entienden bastante bien puesto que se trata de ampliaciones de temas ya vistos anteriormente.

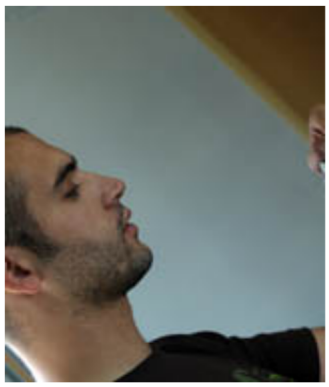
Resolución de problemas en Linux.

Cómo resolver problemas en redes.

Resolución de problemas en redes TCP/IP.

Monitorización de redes cableadas e inalámbricas.

Caso práctico



Samuel se encuentra ultimando la instalación de la red en la academia de Antonio. Éste aparece por allí y, como es bastante curioso, comienza a preguntarle acerca del futuro uso y rendimiento de la red.

- Hola Samuel, ya veo que casi habéis acabado vuestro trabajo. - Así es, Antonio, solo queda realizar alguna comprobación del uso de la red. - Ah! Eso sí que me interesa, ¿Cómo sabes si la red está funcionando con normalidad? - Bueno, eso se consigue si haces uso de alguna herramienta de monitorización de la red. Te indica en el momento como es el tráfico en la red y si existe algún problema te facilita encontrar donde está su origen. - Eso es muy interesante, no sabía que se pudiera obtener ese tipo de información. - Sí, es bastante sencillo utilizando herramientas de monitorización de redes. - ¿Y también se puede hacer con la red inalámbrica? - Por supuesto que sí, Antonio. Se puede comprobar sin importar que tipo de red estés utilizando.

Tal y como le explica Samuel a Antonio, tu también debes saber que el objetivo de la monitorización es asegurar que la red funciona correctamente. También puede servir para mejorar el rendimiento de la red, puesto que analizan el tráfico que se genera en ésta. Al realizar esta tarea puedes tener una idea exacta de lo que está haciendo la red, qué usuario lo está haciendo, si hay fallos en la red y por que se han producido.

Todo aquello que sucede en la red, se puede monitorizar, aunque no toda la información recogida te será útil. Con lo cual, debes plantearte cuales son los datos que necesitas conocer:

- Uso de los servicios de la red.
- Contabilidad del tráfico por la red.
- Errores y fallos ocurridos.
- Estado de los procesos que se ejecutan por la red.
- Cambios hardware.
- Cambios software.
- Cuellos de botella.
- Número de usuarios de la red.
- Número de usuarios no atendidos.

- Intentos de accesos no autorizados al sistema.

Reflexiona

Existen ciertas distribuciones de Linux que nos pueden ayudar a monitorizar redes y comprobar su seguridad, tanto para redes cableadas como para redes inalámbricas. Te animo a que las pruebes en alguna red para ver su funcionamiento.

- **Backtrack** -> Distribución Linux en forma de Live CD diseñada para la auditoria de seguridad informática en general y de las redes inalámbrica en particular.
- **Wifiway** -> Distribución Linux en forma de Live CD diseñada para la auditoria de seguridad de las redes inalámbrica, bluetooth y de radio frecuencia.
- **Wifislax** -> Distribución Linux en forma de Live CD diseñada para la auditoria de seguridad informática en general y de las redes inalámbrica en particular.

Monitores de red.

Debes saber que algunos sistemas operativos de red incluyen software para la monitorización de la red. Estas herramientas capturan y analizan las secuencias de datos de la red desde y hasta el servidor, que se utilizan para diagnosticar problemas potenciales de la red.

Con el monitor de red puedes recopilar información que le ayudará a mantener la red a pleno rendimiento, gracias a funciones que permiten desde identificar patrones a evitar o solucionar problemas. El Monitor de red proporciona información acerca del tráfico de la red que fluye hacia y desde el adaptador de red del equipo donde está instalado. Al capturar información y analizarla puede evitar, diagnosticar y solucionar muchos tipos de problemas relativos a la red.

Te convendrá saber que dentro de las herramientas de monitorización de red se pueden distinguir tres tipos diferentes:

- **Comprobadores de red**: se utilizan para comprobar la continuidad en un cable u otros parámetros más avanzados.
- **Monitores de red**: muestran un mapa de la actividad de la red en un intervalo de tiempo determinado, ya que capturan los mensajes que circulan por ella. No decodifican el contenido de los mensajes, sino que se limitan a contar los que circulan, su tamaño, los que han llegado con error y el número de ellos que se envían y reciben por estación. Estos datos pueden ser útiles para crear perfiles de tráfico en la red, localizar congestiones, detectar intrusos, planificar una expansión de la red y distribuir el tráfico más eficientemente.
- **Analizadores de red**: son dispositivos muy parecidos a los monitores de red pero que son capaces de comprender y mostrar la información que lleva cada mensaje. Los analizadores de red son capaces de comprender diferentes tipos de mensajes de distintas arquitecturas y protocolos. Se identifica la capa de la arquitectura que está involucrada en cada comunicación y si existe algún problema en ella. Se pueden seleccionar los tipos de mensajes a capturar, generar mensajes para enviarlos a la red y ofrecer soluciones a los problemas de la red.

En los sucesivos apartados de este tema ampliarás conocimientos sobre los monitores de red y los analizadores de red, utilizando ejemplos de ellos en los dos tipos de sistemas, tanto en Windows como en Linux.

Para saber más

Te recomiendo que visites el siguiente enlace sobre monitorización de redes. Es bastante completo y se proponen distintas herramientas de monitorización para usar.

Análisis y Monitoreo de redes.

Monitores de rendimiento.

Ya sabes que un **monitor** es un programa que te permitirá examinar el modo en el que los programas que se están ejecutando en tu equipo afectan al rendimiento general de éste. Esta recopilación de datos puede ser en tiempo real o mediante la recopilación de información para su posterior análisis.

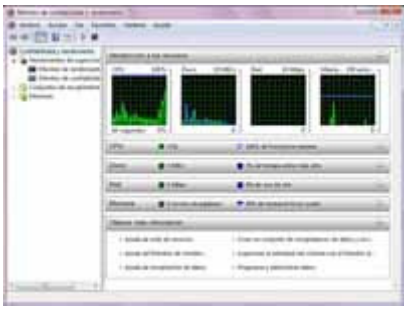
La mayoría de los sistemas operativos incluyen esta herramienta que te permitirá analizar el rendimiento de un equipo. Si este equipo además es el servidor de una red, pues obtendrás información valiosa sobre el rendimiento general de toda la red. Los monitores de rendimiento suelen ofrecer la siguiente información:

- Obtener y almacenar datos de rendimiento.
- Enviar alertas al administrador de la red.
- Iniciar otro programa que devuelva al sistema a unos rangos aceptables.

El Monitor de rendimiento de Windows es un complemento de Microsoft Management Console (MMC) que proporciona herramientas para analizar el rendimiento del sistema. Desde una sola consola puede supervisar el rendimiento de las aplicaciones y del hardware en tiempo real, personalizar qué datos desea recopilar en los registros, definir umbrales para alertas y acciones automáticas, generar informes y ver datos de rendimientos pasados en una gran variedad de formas.

Para iniciar el Monitor de rendimiento de Windows:

Haga clic en **Inicio**, haga clic en el cuadro **Iniciar búsqueda**, escriba **perfmon** y presione Entrar.
O bien pulsas Ctrol+Alt+Supr y das la opción Iniciar Administrador de Tareas. En la pestaña de rendimiento pulsas el botón Monitor de recursos.



En un sistema operativo de Linux, por ejemplo con Ubuntu, encontrarás un Monitor de Rendimiento en el menú **Sistema, Administración, Monitor del Sistema.**

Autoevaluación

¿Qué dato no se recoge en el Monitor del Sistema de Ubuntu?

- ○ Uso actual de la CPU.
- ○ Uso actual de la memoria.
- ○ Bytes enviados y recibidos por la red.
- ○ Uso actual de la tarjeta de red.

No es correcta porque ese dato se recoge.

Incorrecta, porque ese dato se recoge.

No es la respuesta correcta porque ese dato se recoge.

Muy bien. Ese dato no tiene nada que ver.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

Análisis del tráfico en la red.

Otro tipo de aplicaciones que te conviene conocer son los analizadores del tráfico en la red, o analizadores de red. En uno de los apartados anteriores viste cual era la diferencia entre este tipo de programas y un monitor de red. Un monitor de red nos daba información sobre la carga de trabajo de la red pero no analizaba el uso ni el significado de la información que viaja por ella. En cambio, un analizador de red supervisa la información que viaja por la red, es decir, captura la información que circula por la red.

En una red no conmutada, los datos que circulan por la red se envían a todos los equipos de la red. En uso normal, los equipos ignoran los paquetes que se les envían. Así, utilizando la interfaz de red en un modo específico, modo promiscuo, es posible supervisar todo el tráfico que pasa a través de una tarjeta de red.

Un **analizador de red, o rastreador de puertos** es una herramienta que permite supervisar el tráfico de una red. En general lo utilizarás para diagnosticar problemas en las redes y obtener información del tráfico que circula en la red.

El problema que tienen estas herramientas es obvio. Si alguien malintencionado accede a la red puede usar un rastreador para recopilar información. Este riesgo es mayor en redes inalámbricas, ya que es difícil limitar las ondas de radio.

Como ejemplo de un analizador de red te propongo el Wireshark. Es un analizador de red gratuito y válido tanto para plataforma Linux como Windows. Antes a este programa se le conocía como Ethereal.

Para saber más

Uno de los analizadores de red más utilizados es el Wireshark. Ya hemos comentado que es gratuito y válido para ambas plataformas. En el primer enlace tienes la página oficial desde donde te le puedes descargar. Y en el segundo enlace tienes un manual para instalar el programa en Linux y una explicación del entorno de trabajo. Esta explicación te será válida también para Windows. Y en el tercer enlace tienes una explicación un poco más en detalle de la información que aporta el programa.

Programa Wireshark.

Instalación en Linux de Wireshark.

Manejo del programa Wireshark.

Existen herramientas para el estudio de una red inalámbrica que permite comprobar la fortaleza y seguridad de una red empresarial, de un centro educativo o de una red doméstica.

Programa Aircrack-ng.

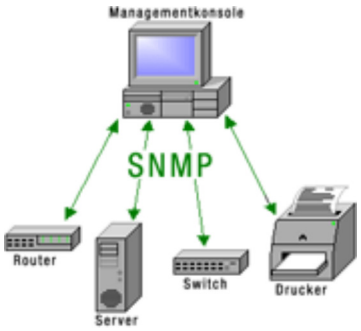
Programa ERW.

Programa NetStumbler.

Programa Kismer.

Programa Airsnort.

Protocolo de administración de redes (SNMP).



Es bastante probable que recuerdes que protocolo **SNMP** (siglas de Simple Network Management Protocol), es un protocolo que se utiliza en la capa de Aplicación del modelo OSI y en la misma capa en el modelo TCP/IP. En un entorno SNMP, hay unos programas denominados agentes que se ejecutan en cada dispositivo de la red administrada (en los hubs, switches, servidores, tarjetas de red, routers…). Los agentes monitorizan el tráfico de la red para recopilar datos estadísticos que guardan en sus bases de información de gestión. Esa información se guarda en una base de datos denominada **MIB**, (siglas de Management Information Base).

Además de estos agentes, en un entorno que utiliza este protocolo hay un gestor que sondea de forma periódica, pidiéndole la información contenida en su MIB. El gestor procesa esta información y puede actuar en consecuencia activando alarmas, provocando la ejecución de programas, etc…

Ejemplo de programas que trabajan utilizando este protocolo podrían ser OpenView de HP, SysUpTime para Windows. Y para Linux se puede utilizar SysUpTime, válido para ambas plataformas.

En el siguiente enlace te propongo que te descargues precisamente este programa, el SysUpTime, basado en el protocolo SNMP. Este programa es un gestor de redes que puede controlar el tráfico, estado y carga de todos los dispositivos de una red. Puede descubrir la topología de una red, monitorizar cargas y tráfico por bloques, gestiona bases de datos MIB, etc.

Para saber más

En el siguiente enlace tienes la dirección para poder descargarte el programa.

Programa SysUpTime.

En el siguiente enlace encontrarás un artículo bastante completo sobre el protocolo SNMP.

Protocolo SNMP.

Autoevaluación

Señala la afirmación que es correcta.

- SNMP es un protocolo que trabaja en la capa de red del modelo OSI.
- SNMP es un protocolo que recopila información solo de los routers de una red.
- La información recogida por SNMP se guarda en una base de datos llamada MIB.
- No existen programas para trabajar con el protocolo SNMP, es obligatorio trabajar sobre él directamente.

No es correcta porque trabaja en la capa de aplicación.

Incorrecta, porque recoge información de todos los dispositivos de la red.

Muy bien. Has captado la idea...

No es la respuesta correcta porque se nombran varios ejemplos de programas que se basan en este protocolo.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Documentación del sistema y logs del sistema.

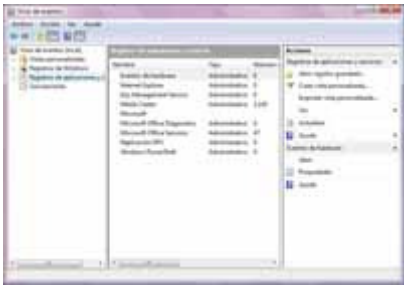
Debes familiarizarte con el concepto de **log (o diario) del sistema**. Un log del sistema es un fichero en el que se registra lo que sucede en un determinado sistema durante un intervalo de tiempo específico. Los ficheros de log pueden ser generados por el sistema operativo o por otras aplicaciones que graban eventos mientras ocurren y los guardan para analizarlos posteriormente.

Te convendría entender que un fichero de log puede **almacenar datos de monitorización de la red**: tráfico de paquetes, colisiones, fallos, etc. Estos datos podrán ser analizados por el administrador de la red para comprobar si todo funciona correctamente, detectar problemas potenciales, monitorizar diferentes aspectos de la red o conocer aspectos como los niveles de uso o intentos de intrusión.

Te puede suceder en un momento determinado que un sistema operativo basado en Windows falle. Los errores del sistema son recogidos y guardados en unos logs. Si tienes la necesidad de verlos puedes hacerlo siguiendo estos pasos:

Inicio->Panel de control->Herramientas administrativas->Visor de eventos.

Aquí ves que tienes distintas categorías según los logs que quieras consultar.



Estos logs te darán una idea de si el problema es del sistema, software o de seguridad, encauzándonos para buscar la solución.

Como te podrás imaginar, dentro del entorno Linux también se guardan distintos logs. Éstos se guardan en archivos ubicados en el directorio /var/log, aunque muchos programas manejan sus propios logs y los guardan en /var/log/ . Además, es posible especificar múltiples destinos para un mismo mensaje. Algunos de los log más importantes son:

- **/var/log/messages**: aquí encontraremos los logs que llegan con prioridad info (información), notice (notificación) o warn (aviso).
- **var/log/kern.log**: aquí se almacenan los logs del kernel, generados por klogd.
- **/var/log/auth.log**: en este log se registran los login en el sistema, las veces que hacemos su, etc. Los intentos fallidos se registran en líneas con información del tipo invalid password o authentication failure.
- **/var/log/dmesg**: en este archivo se almacena la información que genera el kernel durante el arranque del sistema.

En el entorno gráfico hay varias aplicaciones para monitorizar logs, pero la mejor es

KSystemLog (paquete ksystemlog).

Autoevaluación

Señala cuál de las siguientes afirmaciones es correcta.

- Un log es un fichero que se genera exclusivamente cuando hay algún problema en la red.
- Los logs del sistema te permiten saber de que tipo es un problema determinado.
- Los logs del sistema solo se utilizan en sistemas Windows.
- En Linux no existe el modo de monitorizar los logs en un entorno gráfico.

No es correcta porque se pueden generar por otros motivos.

Muy bien. Has captado la idea.

Incorrecta, porque has visto que se utilizan en ambas plataformas.

No es la respuesta correcta porque existen varias opciones para ello.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Herramientas de diagnóstico.

Caso práctico

Julia, que como recuerdas es técnica en Administración de Sistemas Informáticos en Red, ha llamado otra vez a su prima Laura, la directiva de unas oficinas de un banco.

- ¿Ya habéis arreglado la avería del otro día en la oficina, Laura? - Sí, menos mal que nos enviaste a Samuel para que nos ayudara. Nuestro técnico no sabía por donde empezar y Samuel le ha servido de gran ayuda. - Ya le digo yo muchas veces a los técnicos lo importante que es buscar las averías en la red con un orden y un método, utilizando herramientas adecuadas en función del tipo de fallo que este dando. - Pues ya te digo, Samuel nos lo reparó rápidamente.

Ya has podido comprobar lo importante que resulta utilizar una serie de pautas y un orden a la hora de buscar una solución a un problema de redes. Es interesante conocer las posibles averías, sus efectos y la manera de repararlos, conociendo cuantas herramientas tengas a tu disposición.

En este apartado conocerás algunas herramientas muy importantes a la hora de resolver incidencias en una red, tanto en sistemas basados en Windows como en sistemas basados en Linux.

Herramientas de red en windows. Comandos net y netstat.

Cuando te encuentres trabajando con redes con sistema Windows, has de saber que dispones de una serie de herramientas que te permitirán realizar un diagnóstico del funcionamiento de la arquitectura de red. Una de ellas será la ventana de **Propiedades de Red**.

La ventana de Propiedades de red es muy útil para comprobar la configuración de red del equipo en general y así ayudarte a encontrar posibles conflictos en asignación de direcciones IP.

Para que puedas acceder a la ventana de propiedades tienes que ir al panel de control, Centro de redes y recursos compartidos. En esa ventana podrás visualizar el estado de la conexión, así como activar o desactivar distintas opciones para compartir recursos.

Es necesario que conozcas, además del Centro de redes y recursos compartidos, una serie de comandos básicos de monitorización y configuración de redes. Todos los comandos que a continuación se detallan sirven para detectar el funcionamiento de una red de área local e Internet con respecto a la información que se transmite. Todos estos comandos se ejecutan desde la consola de comandos. (Recuerda, se accede a la consola de comandos desde **Inicio, Ejecutar**, escribimos **cmd** y damos **enter**).

- **NET**: Este comando permite realizar un diagnóstico de funcionamiento de la red Microsoft en varios aspectos. También se utiliza para el acceso a recursos compartidos.
  - Net **Send**: Envía un mensaje a través del servicio mensajero.
  - Net **Start**: Inicia un servicio de Windows.
  - Net **Stop**: Detiene un servicio de Windows.
  - Net **Share**: Indica que recursos comparte la maquina.
  - Net **View**: Indica a que máquinas se tiene acceso mediante la red.
  - Net **Sessions**: Indica quienes han entrado en nuestros recursos compartidos.
  - Net **Time * /SET**: Sincroniza la hora con una maquina de la red.
  - Net **User**: Crea o elimina usuarios.
  - Net **Localgroup**: Crea o elimina grupos.

- **Netstat**: Muestra todas las conexiones activas en el equipo.
  - Netstat **-a**: nos muestra todas las conexiones y puertos.
  - Netstat **-e**: muestras las estadísticas Ethernet.
  - Netstat **–n**: muestra direcciones y puertos en forma de número.

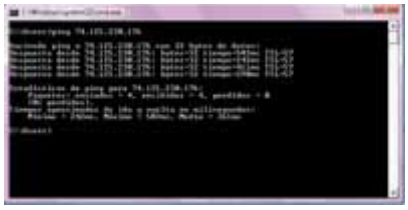
- Netstat **-o**: muestra que programa esta asociado a la conexión activa.
- Netstat **-p (protocolo)**: permite especificar que protocolo se desea ver. TCP/UDP.
- Netstat **-s**: muestra estadísticas clasificas por protocolo.

Comandos de red en windows.

En este apartado puedes seguir estudiando parte de los comandos que puedes utilizar en Windows para la resolución de incidencias en una red de área local.

- **Ipconfig**: Proporciona información sobre TCP/IP, adaptadores, etc.
  - Ipconfig /**all**: ofrece información detallada sobre todas las t. de red y conexiones activas.
  - Ipconfig /**renew**: renueva petición a un servidor DHCP.
  - Ipconfig /**release**: libera la Ip asignada por DHCP.
  - Ipconfig /**registerdns**: registra todos los nombres DNS.
  - Ipconfig /**flushdns**: borrar todas las entradas DNS.

- **Ping**: Informa del estado de un host. Es necesario permitir paquetes ICMP para su funcionamiento.
  - Ping **-t**: se hace ping hasta que pulsemos Ctrl+C para detener los envíos.
  - Ping **-a**: devuelve el nombre del host.
  - Ping **-l**: establece el tamaño del buffer. Por defecto el valor es 32.
  - Ping **-f**: impide que se fragmenten los paquetes.
  - Ping **-n (valor)**: realiza la prueba de ping durante un determinado número de ocasiones.
  - Ping **-i TTL**: permite cambiar el valor del TTL y sería sustituido por el nuevo valor.
  - Ping **-r (nº de saltos)**: indica los host por los que pasa nuestro ping.(máximo 9)
  - Ping **-v TOS**: se utiliza en redes avanzadas para conocer la calidad del servicio.



- **Tracert**: Indica la ruta por la que pasa nuestra petición hasta llegar al host destino.
  - Tracert **-d**: no resuelve los nombres del dominio.
  - Tracert **-h (valor)**: establece un nº máximo de saltos.

- **Route**: muestra y modifica la información sobre las rutas IP del equipo.
  - Route **PRINT**: muestra la tabla completa de rutas
  - Route **ADD** (red_destino) MASK (mascara_destino) (puerta de enlace) [METRICmetrica] [IF interfaz]: Añade una ruta. Con el modificador -p (route add -p ...) hace la ruta persistente, de manera que se mantendrá aunque se reinicie el equipo.
  - Route **DEL** (red_destino) MASK (mascara_Destino) [puerta de enlace]: Elimina la ruta especificada. Admite caracteres comodines.
  - Route **CHANGE** (red_destino) MASK (mascara_destino) (IP_salida/siguientesalto) [METRIC metrica] [IF interfaz]: Modifica la metrica, o la puerta de enlace en una ruta existente

  NOTA: parámetros entre paréntesis ( ) son obligatorios y entre corchetes [ ] son

opcionales.

Autoevaluación

¿Qué comando utilizarías para comprobar si hay comunicación entre dos máquinas?

- Ping.
- Ipconfig.
- Netstat.
- Route.

Muy bien. Es correcto.

No es correcta porque su utilidad es otra.

Incorrecta, porque su utilidad es otra.

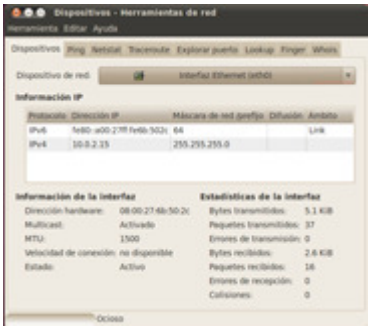
No es la respuesta correcta porque sirve para otra cosa.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

Herramientas de red en linux.

Al igual que en Windows, es interesante que sepas que en Linux también podemos utilizar una serie de herramientas que te servirán para resolver incidencias en una red de área local. Dentro del menú **Administración** existen dos herramientas que son **Herramientas de Red** y **Monitor del Sistema**, con las que podrás monitorizar el uso de tu red.



Aparte de estas herramientas gráficas, y al igual que sucede con Windows, también dispones de comandos a ejecutar en un Terminal de Linux para estas tareas que ahora te ocupan. Para abrir un Terminal en Ubuntu, por ejemplo, vas al menú Aplicaciones, Accesorios, Terminal. Los comandos que puedes utilizar son:

- **Ifconfig**: lo podrás utilizar para consultar la configuración de red del adaptador, aunque también te permite su modificación. Se puede utilizar este comando para comprobar si no hay ningún otro equipo que tiene asignada la misma dirección IP o para consultar si está activo el adaptador. (Equivalente de ipconfig en Windows).
- **Ip**: lo puedes utilizar para consultar la configuración de los parámetros TCP/IP y de encaminamiento del equipo y también para modificarlos a bajo nivel.
- **Route**: podrás consultar o establecer los parámetros de encaminamiento del equipo a bajo nivel
- **Ping**: al igual que en Windows, se utiliza para comprobar si el equipo puede enviar mensajes a la red o alcanzar a otros equipos.
- **Netstat**: se utiliza para consultar los puertos abiertos o los puertos que están a la escucha en el equipo. Este comando se utiliza prácticamente igual que en Windows.

Para saber más

En el siguiente enlace a esta página Web encontrarás un excelente y completo artículo de los distintos comandos que se han comentado en este apartado y en el anterior, tanto para plataforma Windows como para Linux. Es interesante que lo visites puesto que también hay ejemplos de uso de los comandos.

Detectar problemas en una red LAN.

Autoevaluación

¿Qué comando utilizarás en Linux para averiguar la configuración de tu adaptador de red?

- Ping.
- Ifconfig.
- Ipconfig.
- Route.

No es correcta porque su uso es otro.

Muy bien. Has captado la idea...

Incorrecta, porque ésta se utiliza en Windows.

No es la respuesta correcta porque su utilidad es otra.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Problemas de conexión a la red de un equipo.

Cuando vayas a realizar el mantenimiento de una red de área local, uno de los problemas que más frecuentemente suelen darse es que un equipo tenga problemas de conexión a la red. El usuario se encontrará con mensajes del estilo “no puedo acceder a Internet”, “no puedo entrar en una carpeta compartida” o “no puedo acceder al servidor”.

Los **pasos que deberías seguir** para resolver este tipo de problemas son los siguientes:

1. Consultar la configuración del equipo comprobando que los parámetros correspondientes a TCP/IP y a la red son correctos. Si no es así, establecer los valores correctos.
2. Si el equipo consigue su configuración de red a través de un servidor DHCP, comprobar que esta asignación se realiza de forma correcta.
3. Realiza un ping a la puerta de enlace. Si el ping se realiza sin problemas, se puede descartar un error en la configuración del equipo. Es una forma rápida de comprobar si el problema de conexión está en ese equipo en concreto, o el error se produce fuera de la red.

Si has ejecutado el **Ping a la puerta de enlace** y el resultado ha sido que no se puede conectar, debes comprobar las siguientes opciones:

1. Comprobar si la tarjeta de red está correctamente instalada.
2. Si estás en una red cableada, comprobar si el cable está en perfectas condiciones.
3. Si es una red inalámbrica, comprobar si se recibe señal suficiente.

En caso de que el equipo tenga acceso a la red, debes comprobar si los servidores DNS funcionan correctamente.

Si todo esto funciona correctamente y aún así no se puede acceder a un sitio web concreto, el problema puede ser que el sitio no funciona correctamente o existe algún problema de congestión.

Debes conocer

Los siguientes documentos que se proponen serán de lectura obligatoria. En ellos encontraras ejemplos prácticos sobre localización y resolución de problemas en redes. Se especifica para los problemas tipo que puedes

encontrar, cuál es el mejor camino para encontrar la solución.

Localización de problemas (0.23 MB)

Soluciona problemas en red. (1.80 MB)

Solución de problemas en redes IP. (20.0 KB)

Problemas de conexión en una red cableada.

Otro tipo de problemas con los que es bastante probable que en algún momento te encuentres, serán aquellos derivados de la conectividad de los dispositivos de interconexión central. Este tipo de errores son importantes porque pueden llegar a afectar a un número alto de usuarios. Estos fallos pueden ser debidos a problemas físicos de los dispositivos o el cable.

Has de saber, como norma general, que un cable tiene conexión cuando ha sido enchufado a dos dispositivos activos en sus extremos. En ese momento, se activan los indicadores luminosos de los puertos (en verde o naranja), lo que te indica si hay comunicación por ese enlace.

Si te encuentras con problemas de comunicación entre dos dispositivos, hay que comprobar si el cable es la causa. Para comprobarlo es necesario que sigas estos pasos, siempre en los dos extremos del cable:

1. **Comprueba el enlace luminoso del estado del dispositivo**. Si no están activas las luces, el problema puede estar en cualquiera de los dos extremos o en dispositivos intermedios, como enchufes o adaptadores de distintos cables.

2. Verifica que los **conectores están bien montados** y se ajustan correctamente a los puertos. Si se han manipulado hace poco, pude ser que se hayan soltado.
3. Realiza una inspección de **los pines del conector** y del puerto, para comprobar si se han deteriorado.
4. Comprueba que el **puerto en cuestión no ha sido desactivado** desde su configuración.
5. Aunque las luces de los dispositivos estén activos, no asegura que el **cable esté en buen estado**. Haz la prueba de utilizar otro cable de red.

Estas son en principio las situaciones más comunes que puedes encontrar en una red de área local cableada.

Para saber más

En el siguiente enlace a una página de Internet, encontrarás una guía rápida de resolución de problemas que te puedes encontrar cuando vayas a reparar los equipos de una red.

Guía rápida de resolución de problemas.

Autoevaluación

Busca cuál de las siguientes opciones no es posible si las luces de una tarjeta de red no funcionan.

- ○ Que el cable esté mal conectado a la tarjeta de red.
- ○ Que el cable esté roto en algún punto entre la tarjeta de red y el dispositivo de interconexión central.
- ○ Está mal configurado algún dispositivo hardware del equipo.
- ○ Los pines del conector y del puerto se pueden haber deteriorado.

No es correcta porque es una opción posible.

Incorrecta, porque es una opción válida.

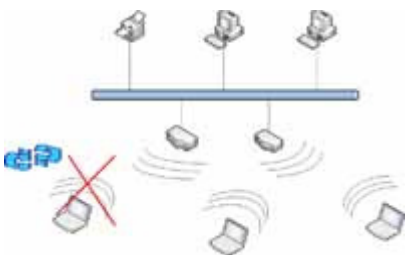
Muy bien. Has captado la idea, esto no implica que no funcionen las luces de la tarjeta de red.

No es la respuesta correcta porque es una opción probable.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Problemas de conexión en una red inalámbrica.



Te darás cuenta, a medida que se incremente tu experiencia en estos temas, que es mucho más sencillo encontrar la causa de un fallo de conexión en una red cableada que diagnosticarlo en una red inalámbrica. Te puedes encontrar con una red inalámbrica que lleve funcionando mucho tiempo sin ningún problema, y de repente deja de funcionar sin motivo aparente. Hay una serie de cosas puedes hacer como primer paso para solucionarlo.

Antes de que pienses en la solución más complicada, debes pararte en las cosas más sencillas. A veces son las que más éxito tienen.

Lo primero que tienes que hacer es abrir desde el Panel de Control, **Centro de Redes y Recursos Compartidos**. En la parte de la derecha le das a **Administrar conexiones de red**. Y encima del icono de red inalámbrica, botón derecho, Diagnosticar. Haz que la conexión se desactive y luego se vuelve a activar. Después de reiniciar el ordenador, esto suele funcionar.

Si la conexión a la red inalámbrica es a través de un conector USB, puedes comprobar si se ha perdido. Desconecta todo y vuélvelo a conectar. Tendrás que desenchufar el cable USB del ordenador.

Te puedes encontrar en el caso en el que una nueva red inalámbrica ha sido instalada, y crear interferencias con la red que tú ya utilizabas. La señal de la nueva red puede tomar control sobre la señal de tu propia red. En este caso, tienes que ir al **Centro de Redes y Recursos Compartidos**, y dar la opción de **Administrar redes inalámbricas**. Ahí verás las redes a las que tienes acceso y a cuál estás conectado o conectada. Tienes que conectarte a aquella que quieras y eliminar las que no correspondan, para no volverte a conectar a ellas.

Si descubre que la conexión funciona cuando pones el ordenador cerca del origen de la señal de Internet, y deja de funcionar cuando te mueves, lo más probable es que el problema sean las interferencias. En este caso, busca los últimos cambios realizados en la zona donde antes te conectabas. Por ejemplo, teléfonos inalámbricos que pueden emitir señales que se solapan con las de la red Wifi.

Otras veces los fallos pueden ser causados por haber tocado la configuración del equipo. Si no encuentras la causa, lo mejor es que vuelvas a la configuración inicial. Por este motivo es tan importante tener anotados todos los detalles de configuración de la red. Nunca sabes en que momento los vas a necesitar.

Si aún así no has encontrado el origen del problema, todavía tienes alguna cosa más para comprobar. Los pasos que debes dar para seguir buscando lo que pasa con la red inalámbrica serán:

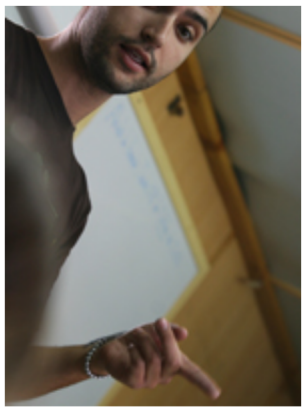
1. Comprueba si la **potencia de la señal recibida** en el equipo es suficiente. Para ello puedes utilizar las herramientas de monitorización que se instalan con el adaptador

inalámbrico. Si la potencia recibida no es la suficiente, será necesario instalar un punto de acceso más cercano.

2. Has de fijarte en el **indicador luminoso de estado del adaptador de red**. Si no está encendido, significa que no existe conexión con el punto de acceso.
3. Si la red está en el exterior, es posible que las condiciones meteorológicas influyan a la señal emitida por el punto de acceso, no llegando con suficiente potencia para que el adaptador se pueda conectar.
4. Y por último, y no menos importante, comprueba si los **parámetros de acceso** a la red inalámbrica son correctos, como el SSID o la clave de cifrado.

Prevención de riesgos profesionales.

Caso práctico



Samuel está en la academia de Antonio, terminando de instalar un punto de acceso en uno de los pasillos. En ese momento ha llegado Julia. Ella se ha fijado en que Samuel está realizando la instalación con prácticamente ninguna medida de seguridad, puesto que en vez de utilizar una escalera para desempeñar su trabajo, está utilizando una silla encima de una mesa.

- Samuel, eso que estás haciendo no está bien. En cualquier momento la silla se podría resbalar y tendrías un accidente. - Ya lo sé, es que me he dejado la escalera en el coche, y por no ir a por ella… - Pues esto no puede ser. Las medidas de seguridad en el trabajo son muy importantes conocerlas y utilizarlas, para no tener ningún accidente laboral. Así que es mejor que bajes de ahí y te vayas a por la escalera. - Sí, tienes razón. No me sentía precisamente muy seguro aquí arriba. - Debemos evitar los accidentes en la medida de lo posible. Una mala caída puede tener consecuencias nefastas…

Esta situación en la que se encontraba Samuel es más habitual de lo que nos parece. La base de nuestra seguridad en el trabajo pasa por conocer que tipo de incidentes se pueden tener en nuestro trabajo para así evitarlos. La empresa debe poner a tu disposición las medidas de seguridad y equipos de protección necesarios para el desempeño de tu trabajo. Pero de tu parte has de poner el interés de utilizarlo y trabajar de acuerdo a ciertas normas de prevención.

Riesgos.

En primer lugar tienes que saber que un **riesgo** es la posibilidad de que se produzca un daño en las personas que realizan una determinada tarea. La **seguridad en el trabajo** es el conjunto de actividades y medidas adoptadas o previstas para evitar los riesgos que producen accidentes. Al aplicar determinadas medidas de seguridad, se consigue que exista un estado de seguridad más alto, aunque es improbable llegar a un estado de seguridad completa.

Se considera **factor de riesgo** de un determinado tipo de daño aquella condición del trabajo, que, cuando está presente, incrementa la probabilidad de aparición de ese daño.

Los riesgos laborales a los que puede estar expuesto un trabajador en su centro de trabajo dependen de las condiciones en las que preste sus servicios. Una **condición de trabajo** es cualquier característica del mismo que pueda tener una influencia significativa en la generación de riesgos para la seguridad y la salud del trabajador o trabajadora. En esta definición están incluidas:

- Las características generales de los locales, instalaciones, equipos, productos y demás útiles existentes en el lugar de trabajo.
- La naturaleza de los agentes físicos, químicos y biológicos presentes en el ambiente de trabajo.
- Los procedimientos para la utilización de los agentes citados que influyan en la generación de riesgos.
- Todas las características del trabajo, incluidas las relativas a su organización y ordenación que influyan en la magnitud de riesgos a los que esté expuesto el trabajador o la trabajadora.

Reflexiona

Ya conoces a Antonio, el dueño de la academia que ha contratado a una empresa para que realice la instalación de una red en sus aulas, y a Samuel, el Técnico de Sistemas Microinformáticos y Redes que ayuda en la instalación de las canaletas y el cableado en las aulas.

Antes de su contratación la empresa ha informado a Samuel sobre los riesgos específicos de su trabajo, como el riesgo a caídas, heridas o golpes si no manipula bien las herramientas de trabajo. Como medidas de prevención deberá evitar el mal uso de dichas herramientas y se le ha facilitado información sobre como se debe hacer.

¿Cuál es el riesgo laboral de Samuel, el daño derivado del trabajo y la medida preventiva a adoptar?

Mostrar retroalimentación

El riesgo laboral: mala utilización de las herramientas de trabajo. **El daño laboral**: caídas, golpes o heridas. **Medida preventiva**: formación sobre el uso de las distintas herramientas.

Medidas de prevención.

Es útil que conozcas que las **medidas de prevención** tienen como principal objetivo eliminar los riesgos o, en su defecto, proteger a los trabajadores y trabajadoras para minimizar las consecuencias cuando se produce un accidente. Las medidas de seguridad que se pueden tomar son de distintos tipos:

- **Medidas preventivas**: para evitar que se produzca un accidente.
- **Medidas protectoras**: para minimizar las consecuencias en caso de accidente.
- **Medidas reparadoras**: para reparar los daños que ha producido un accidente.

Además de esta clasificación que acabas de ver, las medidas de seguridad que se aplican en cualquier empresa son de dos tipos:

- **Generales**: son aquellas que se aplican de forma genérica independientemente de los riesgos que puedan existir. Estas medidas que se aplican son:
  - **Previas a los accidentes:**
    - Inspecciones de seguridad.
    - Análisis del trabajo.
    - Diseño de los equipos y las instalaciones.
    - Selección y evaluación del personal.
    - Sistemas de seguridad.
    - Señalizaciones.
    - Formación del personal.
  - **Posteriores a los accidentes:**
    - Investigación de los accidentes.
    - Registro y notificación de los accidentes.
- **Específicas**: son aquellas que intentan eliminar determinados riesgos concretos. Las medidas de seguridad incluyen:
  - Riesgo eléctrico.
  - Riesgo de incendio.

Las normas de prevención de riesgos laborales obligan a los empresarios y empresarias y a los propios trabajadores y trabajadoras a la aplicación de las normas. Así es que tú, como futuro empleado o empleada en una empresa, tendrás la obligación de conocer los riesgos a los que te enfrentas en tu puesto de trabajo y a tomar las debidas medidas de prevención para evitar accidentes en tu lugar de trabajo.

Autoevaluación

Señala cuál de las siguientes medidas de seguridad es posterior al accidente.

- Inspecciones de seguridad.
- Señalizaciones.
- Formación del personal.
- Registro y notificación de los accidentes.

No es correcta porque ésta actividad se realiza antes del accidente.

Incorrecta, porque también ha de realizarse antes del accidente.

No es la respuesta correcta porque se realiza antes del accidente.

Muy bien. Has captado la idea.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

Trabajo con ordenadores.

Como ya sabes, toda persona que trabaja en el sector de la informática y las comunicaciones requieren utilizar ordenadores con pantallas de visualización, teclados y ratones. Es importante que conozcas cuales son las molestias que pueden ocasionar el mal uso de estos dispositivos y que recomendaciones existen al respecto.

Es muy probable que ya hayas sufrido alguno de los siguientes problemas cuando has trabajado de manera continuada delante de la pantalla de un ordenador: dolor de cabeza, molestias en los ojos, dolores cervicales, etc… Para evitar estos problemas se recomienda seguir una serie de pautas. También son muy importantes las recomendaciones de uso de la silla de trabajo.

En la siguiente figura se ilustra la postura correcta de una persona sentada trabajando con un ordenador.

En un puesto de trabajo informático aspectos como la **pantalla y la postura del usuario o usuaria** relacionada con el espacio útil son relevantes. Aspectos que te conviene tener en cuenta sobre la pantalla son los siguientes:

- La pantalla debe estar situado de forma que reciba la menor cantidad de luz posible, **evitando así reflejos**.
- El tamaño de la **pantalla debe ser del tamaño suficiente** para no tener que forzar la vista. Los modelos recomendables deben tener un tamaño entre 17 y 19 pulgadas.
- Utilizar **resoluciones adecuadas** con frecuencia de refresco igual o superior a 70Hz.
- Evitar los reflejos modificando la iluminación ambiental o utilizando los dispositivos antirreflejos.
- Trabajar a una **distancia de la pantalla** de más de 40 cm. Y a una **altura que permita** su visualización desde la línea visual horizontal hasta un ángulo máximo de 60º. La pantalla debe estar a la altura o por debajo de los ojos del usuario o usuaria.

Además de esto, es muy importante que la **postura** responda a unos parámetros o medidas que no te fuercen las articulaciones. Es importante que tengas en cuenta los siguientes apartados:

- La silla es un componente clave. Debe **tener ruedas** que faciliten los cambios de postura.
- Debe tener un **tejido transpirable** y su respaldo no debe ser muy rígido, situándose la zona de apoyo a la altura de las vértebras lumbares.

- **Altura ajustable.**
- **Respaldo** con prominencia para adaptarse a la zona lumbar.
- **Profundidad de asiento** regulable, con borde redondeado.
- **Levantarse de la silla con cierta frecuencia.**

Por último, aquí tienes una serie de **consejos a seguir**, sobre todo si pasas muchas horas sentado delante del ordenador:

- Utilizar el **ratón** alternativamente con la mano **derecha y con la izquierda**.
- El **teclado** debe estar a la **altura de los codos**.
- Realizar **estiramientos** y ejercicios de **respiración**.

Trabajo con riesgo eléctrico o con riesgo de caídas.

En el trabajo que vas a desempeñar como Técnico o Técnica de Sistemas Microinformáticos y Redes en el futuro existe **riesgo eléctrico** puesto que trabajas con equipos y dispositivos conectados a la red eléctrica. Es por ello importante que entiendas lo siguiente: los trabajos que se realizan sin tensión tienen menos riesgos para los trabajadores y trabajadoras.

Como es bastante probable que más de una vez tengas que desmontar un equipo o hacer comprobaciones en algún dispositivo, siempre que sea posible es mejor que trabajes con los equipos desconectados de la red eléctrica, aunque tengas que realizar de operaciones adicionales para desconectar la corriente antes de realizar el trabajo y volver a conectarla una vez finalizado.

En otras ocasiones, te encontrarás en situaciones a la hora de realizar instalaciones de equipos de comunicaciones y redes en los que tendrás que instalar sistemas de emisión y recepción en paredes, torres o estructuras a alturas considerables. Los riesgos más importantes en estas condiciones son las caídas, tanto en la zona de trabajo como durante la elevación o descenso, por lo que es necesario utilizar **equipos de protección individual** en estos casos. Estos equipos pueden ser:

- **Cinturón de sujeción**: se utiliza cuando el operario no está realizando desplazamientos desde el punto donde está realizando su trabajo.
- **Cinturón de suspensión**: se utiliza cuando el operario u operaria está suspendido en la zona de trabajo.
- **Cinturón anticaídas**: cuando el riesgo de caída es muy alto por la inestabilidad del lugar u otros factores.
- **Escaleras**: se utiliza en paredes y fachadas, recomendando no subir más de una persona, acceder a ella siempre de cara, sujetarlas perfectamente en la parte superior y evitar el cierre accidental de las escaleras plegables.

Normativa de prevención.

Como puedes entender, existe una preocupación por reducir los accidentes de trabajo y las enfermedades profesionales. Esta preocupación es compartida por los trabajadores y trabajadoras, sus familias, las empresas, el Estado, y en general, el conjunto de la sociedad.

En el artículo 40.2 de la Constitución Española encomienda a los poderes públicos velar por la seguridad e higiene en el trabajo. Esto obliga a desarrollar una **política de protección** de la salud de los trabajadores y trabajadoras mediante la prevención de riesgos derivados de su trabajo.

Es interesante que sepas que a nivel europeo también existen una serie de **Directivas** que definen disposiciones mínimas que sirvan de marco común a toda la Unión Europea. En una de estas Directivas, la Directiva 89/391/CEE hace referencia a la aplicación de medidas para promover la mejora de la seguridad y de la saludo de los trabajadores y trabajadoras. Indica que el empresario u empresaria deberá aplicar las siguientes **medidas**:

- Evitará los riesgos.
- Evaluará los riesgos que no se pueden evitar.
- Combatirá los riesgos en su origen.
- Adaptará el trabajo a la persona.
- Tendrá en cuenta la evolución de la técnica.
- Antepondrá la protección colectiva a la individual.
- Planificará la prevención.
- Dará las debidas instrucciones a los trabajadores y trabajadoras.

Debes saber que existe una Ley de Prevención de Riesgos Laborales (LPRL), que es la Ley 31/1995 que aplica la Directiva Europea al Decreto Español. Esta ley establece los conceptos básicos en esta materia que nos dice las obligaciones de los empresarios y empresarias y pretende el desarrollo de una cultura preventiva.

La **LPRL** establece una serie de conceptos básicos:

- **Prevención**: Conjunto de actividades o medidas adoptadas o previstas entre todas las fases de actividad de la empresa con el fin de evitar o disminuir los riesgos derivados del trabajo.
- **Riesgo laboral**: Es la posibilidad de que un trabajador o trabajadora. sufra un determinado daño derivado del trabajo. Para calificar un riesgo desde el punto de vista de su gravedad, se valorarán conjuntamente la probabilidad de que se produzca el daño y la severidad del mismo.
- **Daños derivados del trabajo**: Son las enfermedades, patologías o lesiones sufridas con motivo u ocasión del trabajo.
- **Riesgo laboral grave e inminente**: Aquel riesgo con posibilidad inmediata de realización con consecuencias graves para la salud.
- **Equipos potencialmente peligrosos**: Los que en ausencia de medidas preventivas ocasionen riesgo para la salud.
- **Equipo de trabajo**: Cualquier dispositivo utilizado en el trabajo.

- **Condición de trabajo**: Características del trabajo que puedan ocasionar riesgos para la salud.

Autoevaluación

¿Cómo se denomina a una característica del trabajo que puede ocasionar riesgos para la salud?

- ○ Condición de trabajo.
- ○ Riesgo laboral grave.
- ○ Riesgo laboral.
- ○ Daños derivados del trabajo.

Muy bien. Has captado la idea.

No es correcta.

Incorrecta.

No es la respuesta correcta.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

Normativa de protección ambiental.

Te resultará interesante saber que todo el fundamento jurídico de las políticas de medio ambiente de la Unión Europea se recoge en los artículos 174 a 176 del **Tratado de Amsterdam**. En estos artículos se establece una política medioambiental basada en los siguientes principios:

- Prevención, evitando la contaminación.
- Quien contamina, paga.
- Integración.
- Corrección de la fuente que perjudica el medio ambiente.

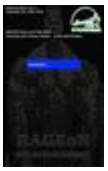
Aunque la Unión Europea trabaja en la protección del medio ambiente, reconoce que muchos problemas ambientales deben resolverse en el ámbito de estos estados. Es por ello que cada país tiene una normativa de protección ambiental diferente. **En España existen las siguientes reglamentaciones:**

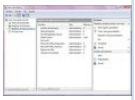
- Ley 10/1998, de 21 de Abril, de **residuos**.
- Real Decreto 952/1997, de 20 de Junio, por el que se modifica el reglamento para la ejecución de la Ley 20/1986, de 14 de Mayo, básica de **residuos tóxicos y peligrosos**, aprobado mediante Real Decreto 833/1998, de 20 de Julio.
- Real Decreto Legislativo 1/2008, de 11 de Enero, por el que se aprueba el texto refundido de la Ley de Evaluación de **Impacto Ambiental** de proyectos.
- Ley 34/2007, de 15 de Noviembre, de **calidad del aire** y protección de la atmósfera.

Las respectivas **Comunidades Autónomas** también tienen sus propias reglamentaciones por las competencias atribuidas en materia de protección ambiental. Además, las empresas pueden adherirse voluntariamente a la norma ISO 14001:2004, que establece una serie de auditorías para asegurar la adecuación y eficacia a las condiciones de protección ambiental que define el mercado actual.

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del rec
	Autoría: jmaldona. Licencia: CC BY-NC 2.0 Procedencia: http://www.flickr.com/photos/jmaldona/45435969/		Autoría: Esparta. Licencia: CC BY 2.0 Procedencia: http://w /photos/esparta/3347 /o/in/photostream/
	Autoría: Paolos Paolos. Licencia: Dominio Público. Procedencia: http://commons.wikimedia.org/wiki/File:Arrows-orphanize.png		Autoría: Magicknight Licencia: Dominio pú Procedencia: http://commons.wikin /wiki/File:High-speed
	Autoría: Lgate74. Licencia: CC 3.0 Procedencia: http://commons.wikimedia.org/wiki/File:Dcentre_racks.jpg		Autoría: Bushido92w Licencia: CC 2.5. Procedencia: http://commons.wikin /wiki/File:18C.svg
	Autoría: Bushido92wiki. Licencia: CC 2.5. Procedencia: http://commons.wikimedia.org/wiki/File:24C.svg		Autoría: Dmitry G. Licencia: CC 3.0. Procedencia: http://commons.wikin /wiki/File:Cable_sala
	Autoría: Drouet. Licencia: CC 3.0 Procedencia: http://commons.wikimedia.org/wiki/File:Virus_rezon.gif		Autoría: Justin. Licencia: CC 2.0 Procedencia: http://commons.wikin /wiki/File:CAT5e- RJ45.jpg?uselang=es
	Autoría: Faction. Licencia: CC 3.0 Procedencia: http://commons.wikimedia.org/wiki/File:Ragebios.gif		Autoría: Nuria Celis N Licencia: Uso educat comercial. Procedencia: Pantall Wireshark.
	Autoría: Nuria Celis Nieto. Licencia: Copyright (cita). Procedencia: Pantallazo de Windows Vista.		Autoría: Nuria Celis N Licencia: Uso educat comercial. Procedencia: Pantall Ubuntu.

	Autoría: Ktdreyer. Licencia: Dominio público. Procedencia: http://es.wikipedia.org /wiki/Archivo:Wsicon.svg		Autoría: Stefan Mülle Licencia: CC 3.0. Procedencia: http://commons.wikin /wiki/File:SNMP-Managementkonsole
	Autoría: Nuria Celis Nieto. Licencia: Copyright (cita). Procedencia: Pantallazo del Visor de Eventos de Windows Vista.		Autoría: Nuria Celis N Licencia: Copyright (Procedencia: Pantall de Redes de Windo
	Autoría: Nuria Celis Nieto. Licencia: Copyright (cita). Procedencia: Pantallazo de la ventana del sistema de Windows Vista.		Autoría: Nuria Celis N Licencia: Uso educat comercial. Procedencia: Pantall Ubuntu.
	Autoría: Nuria Celis Nieto. Licencia: Uso educativo, no comercial. Procedencia: Pantallazo de Ubuntu.		Autoría: Nuria Celis N Licencia: Uso educat comercial. Procedencia: Pantall Firefox.
	Autoría: Junta de Andalucía. Licencia: Dominio Público. Procedencia: http://www.juntadeandalucia.es/empleo /recursos/material_didactico/especialidades /materialdidactico_administrador_servidores /mod2_6.html		Autoría: Axel Springe Licencia: CC. Procedencia: Revista Hoy.
	Autoría: Colin Vosper. Licencia: CC 2.0 Procedencia: http://commons.wikimedia.org /wiki/File:Rock_fall_at_Oddicombe_-_geograph.org.uk_-_1724234.jpg		Autoría: Pavel Sevela Licencia: CC 3.0 Procedencia: Montaj http://commons.wikin /wiki/File:Window_cle Palác,_Brno.jpg
	Autoría: Sodipodi. Licencia: CC 2.5 Procedencia: http://es.wikipedia.org /wiki/Archivo:High_voltage_warning.svg		Autoría: Incosv. Licencia: Dominio Pú Procedencia: http://commons.wikin /wiki/File:Inco_Ladde
	Autoría: Creado por varios usuarios en Wikimedia. Licencia: Dominio Público. Procedencia: http://commons.wikimedia.org /wiki/File:Flag_of_Europe.svg#Licensing		Autoría: T3rminatr. Licencia: Dominio Pú Procedencia: http://commons.wikin /wiki/File:Aerosolcan_

Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.

Antes de cualquier uso leer detenidamente el siguente Aviso legal

Historial de actualizaciones

Versión: 01.00.01	Fecha de actualización: 13/05/21
Actualización de materiales y correcciones menores.	
Versión: 01.00.00	**Fecha de actualización: 25/10/14**
Versión inicial de los materiales.	