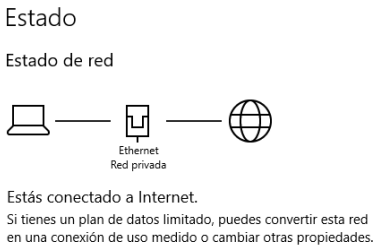
Resolución de incidencias en una red local

Caso práctico



A María en su academia le ha surgido un gran problema, el sistema se ha caído y no funciona la red. Consulta con su amiga Blanca, Técnico de Sistemas Microinformáticos y Redes, y le pregunta, esta le dice que estos casos lo normal es intentar acotar el problema hasta encontrar cual es el origen y así intentar resolverlo más rápidamente.

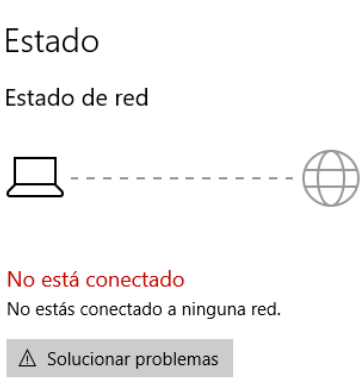
Blanca le comenta que es muy importante tener un método de trabajo bien claro puesto que los problemas que se pueden encontrar de muy diferente signo y sobre todo que lo importante es conocer los problemas más habituales y saber resolverlos.

1.- Introducción

Algo inevitable cuando empezamos a trabajar es encontrarnos con incidencias en la red, averías inesperadas y problemas que requieren destreza para solucionarlo y poner en funcionamiento de nuevo el sistema.

No es fácil encontrar la solución de estos problemas porque hoy en día los sistemas informáticos son cada vez más complejos.

El primer paso es identificar el problema, 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.



2.- Resolución de incidencias en una red local

Como hemos visto en el caso anterior es 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.

Unos pasos genéricos para llevar a cabo si encontramos un problema en una red:

1. El primer paso es tener claro cuál es el problema al que nos enfrentamos y cuales son sus síntomas. A partir de estos datos podemos describir las causas que han podido producir el problema.
2. El siguiente paso será intentar recoger toda la información posible sobre el problema concreto. Preguntar a todos los usuarios y usuarias afectados y utilizar herramientas que permitirán recoger información sobre el sistema.
3. Después de tener toda la información, necesitamos hacer un listado de los problemas que podemos encontrar en la red, desechando aquellos que no guardan relación con los hechos. Así podemos acotar los aspectos que hay que analizar a fondo.
4. Debemos establecer un plan de acción según los problemas encontrados.
5. Por último hay que pasar a la práctica, realizando todas las acciones de forma ordenada y comprobando que los síntomas desaparecen.
6. Si los síntomas no desaparecen, hay que volver a empezar desde el paso cuatro.

Autoevaluación

El primer paso a tomar en la resolución de una avería es:

- ○ Recoger información del problema
- ○ Identificar el problema
- ○ Establecer un plan de acción

Incorrecto

Exacto

Incorrecto

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto

2.1.- Estrategias

Es muy importante en el tema de la resolución de incidencias, que tener en cuenta alguna estrategia para enfrentarte a este trabajo. Una estrategia es un conjunto de acciones que hay que llevar a cabo para conseguir el 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 facilita mucho disponer de toda la información posible del estado de la red, además de estar bien preparado ante un eventual problema. Es muy recomendable disponer 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 lista 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.

Es importante plantear una estrategia organizada, siguiendo unos pasos, tener a disposición toda la información sobre cómo está diseñada la red, direcciones IP de los dispositivos, diagramas lógicos y físicos de la red.

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

2.2.- Parámetros de 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.

El principal parámetro de rendimiento de una red será la velocidad de transferencia de la red. Por tanto, si la red funciona de forma óptima tendrá una buena velocidad de transferencia.

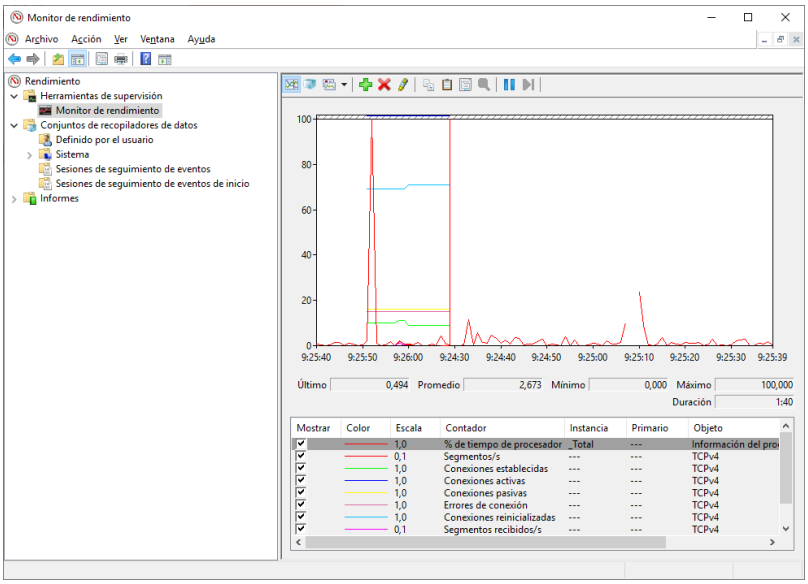
Otro parámetro de rendimiento es el número de paquetes de datos que circulan de forma correcta entre dos nodos de red. En el camino entre ambos nodos, los paquetes pueden alterarse. Si el número de paquetes que llegan a su destino sin alterarse es alto, significa que la red tiene un buen rendimiento. Actualmente la fiabilidad de la comunicación es muy alta y la pérdida de datos suele ser muy insignificante.

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 dos nodos tarden mucho en conectarse, o que uno de los nodos tarde en generar la respuesta, 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 videoconferencias.

En Windows dentro de las herramientas administrativas tenemos un monitor de rendimiento:



Autoevaluación

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

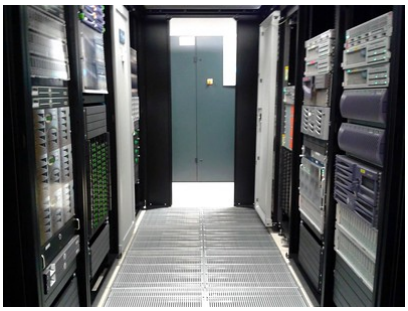
- [ ] Velocidad de transferencia y finalidad de la red
- [ ] Uso de los recursos
- [ ] Velocidad de transferencia, tiempo de respuesta y fiabilidad
- [ ] Usuarios conectados

Mostrar retroalimentación

Solución

1. Incorrecto
2. Incorrecto
3. Correcto
4. Incorrecto

2.3.- Seguridad física de los espacios



El primer paso para establecer la seguridad de los dispositivos es decidir adecuadamente dónde vamos a instalarlo. Esta decisión puede ser superflua, pero resulta vital para el mantenimiento y protección de nuestros sistemas. Los planes de seguridad física se basan en proteger el hardware de los posibles desastres naturales, de incendios, de inundaciones, sobrecargas eléctricas, robos y otra serie de amenazas.

Cada sistema informático es único. Hay centro de procesos de datos que ocupan salas enteras llenas de armarios de componentes informáticos. Otras empresas medianas disponen sólo de uno de estos módulos o armarios, y las empresas pequeñas disponen de un rack con un solo servidor. La protección física habrá que adaptarla al tipo y tamaño de la empresa, sin excesos pero sin quedarse cortos.

Las amenazas que nos podemos encontrar en un sistema informático son:

- 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%. Hay que climatizar los espacios.
- Incendios. Se pueden evitar utilizando mobiliario ignífugo, zonas lejanas a sustancias inflamables o explosivos, utilizando sistemas antincendios, detectores de humo, etc.
- Inundaciones. Podemos evitar la ubicación en las plantas bajas, impermeabilizar las paredes.
- Robos. Para evitarlos es necesario poner medidas biométricas, cámaras de seguridad, vigilantes jurados...
- Señales electromagnéticas. Evitar la ubicación en lugares próximos a radiación de señales electromagnéticas, uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.
- Apagones. Para evitar los apagones colocaremos Sistemas de Alimentación Ininterrumpida, SAI, que proporcionan corriente eléctrica durante un periodo de tiempo suficiente.
- Sobrecargas eléctricas. Los SAI deberán incorporan filtros para evitar picos de tensión, es decir, estabilizan la señal eléctrica.
- Desastres naturales. La única forma de minimizar los riesgos es permaneciendo en continuo contacto con el Instituto Geográfico Nacional y lo Agencia Estatal de Meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos en España.

2.4.- Incidencias en redes locales

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 hay un listado con las incidencias más comunes que podemos encontrar a la hora de trabajar en una red de área local.

2.4.1.- Incidencias físicas

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 se prueba a utilizar otro puerto.
- No se puede acceder a alguna máquina: Hay que comprobar que la máquina está encendida, que no tiene fallos en la tarjeta de red o en los cables y para comprobar se puede ejecutar un comando ping a la máquina.

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

Opción correcta

Incorrecto

Incorrecto

Incorrecto

Solución

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

2.4.2.- Incidencias lógicas

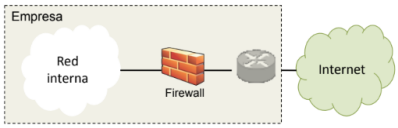
Las incidencias lógicas más comunes son:

- Error de funcionamiento de software
- Configuración errónea de dispositivos

- Incidencias provocadas por ataques a la seguridad:
  - 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), son máquinas que filtran el tráfico bloqueando los accesos no permitidos.
- 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.

Autoevaluación

¿Cuál de las siguientes incidencias están catalogadas como incidencias lógicas?

- [ ] Borrado de datos en el disco
- [ ] Virus informático
- [ ] Spam
- [ ] Mala configuración de red

Mostrar retroalimentación

Solución

1. Correcto
2. Correcto
3. Correcto
4. Correcto

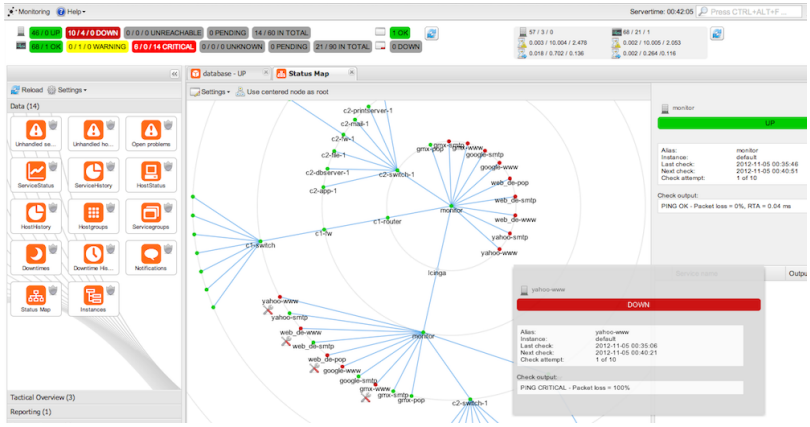
3.- Monitorización de redes cableadas e inalámbricas

La monitorización consiste en observar los cambios que se van produciendo en el sistema, el objetivo es detectar fallos en la red y asegurar el buen funcionamiento de la red-

También puede servir para mejorar el rendimiento de la red, puesto que analizan el tráfico que se genera en ésta.

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

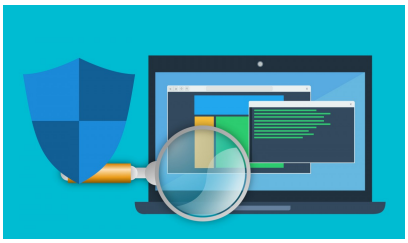
- Uso de los servicios de la red.
- Contabilidad del tráfico por la red.
- Errores y fallos ocurridos.
- Estado de los procesos que se ejecutan por la red.
- Cambios hardware.
- Cambios software.
- Cuellos de botella.
- Número de usuarios de la red.
- Número de usuarios no atendidos.
- Intentos de accesos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



Reflexiona

Existen ciertas distribuciones de Linux que nos pueden ayudar a monitorizar redes y comprobar su seguridad, puedes probar su funcionamiento, por ejemplo con Kali-linux.

3.1.- Monitores de red

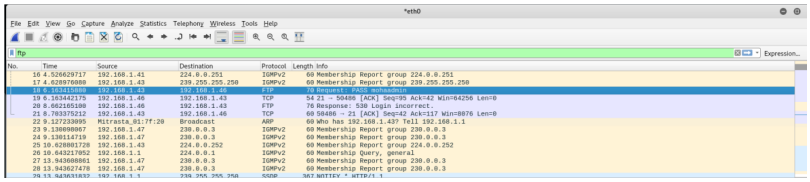


Algunos sistemas operativos de red incluyen software para la monitorización de la red. Estas herramientas capturan y analizan las secuencias de datos de la red desde y hasta el servidor, que se utilizan para diagnosticar problemas potenciales de la red.

Con el monitor de red podemos recopilar información que 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.

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.



3.2.- Monitores de rendimiento

Un monitor es un programa que permite examinar el modo en el que los programas que se están ejecutan en el 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 permite analizar el rendimiento de un equipo. Si este equipo además es el servidor de una red, se obtiene 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.

Para saber más

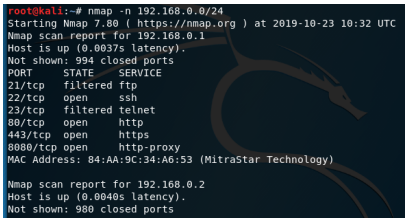
En un sistema windows puedes acceder al monitor de rendimiento dentro de las herramientas administrativas que hay en el panel de control o bien tecleando en la parte inferior "Monitor de rendimiento"

3.3.- 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. A diferencia de un monitor de red que da información sobre la carga de trabajo de la red el analizador de red supervisa la información que viaja por la red, es decir, captura la información que circula por la red.

En una red hay casos en los que es posible capturar el tráfico que circula por ella, en un hub o en una conexión wifi el tráfico es retransmitido a todos los elementos, solo es necesario poner la interfaz de red en modo promiscuo y así acceder a todo el tráfico de la red. El analizador de red más extendido es wireshark.

Por otro lado, también es posible rastrear los puertos que se encuentran en uso en la red, de forma que, sabiendo que puertos están a la escucha se sabe que servicios están en funcionamiento y, por tanto, que servicios son susceptibles de ser atacado. Por ejemplo si descubrimos que el puerto 3389 está a la escucha sabemos que un dispositivo es accesible por escritorio remoto (aunque tendremos que descubrir usuario y contraseña). Para escanear puertos es muy usado el comando nmap.



Para saber más

Sin dud el anilizador de red más utilizado es Wireshark, es gratuito y hay versiones tanto para windows como para linux.

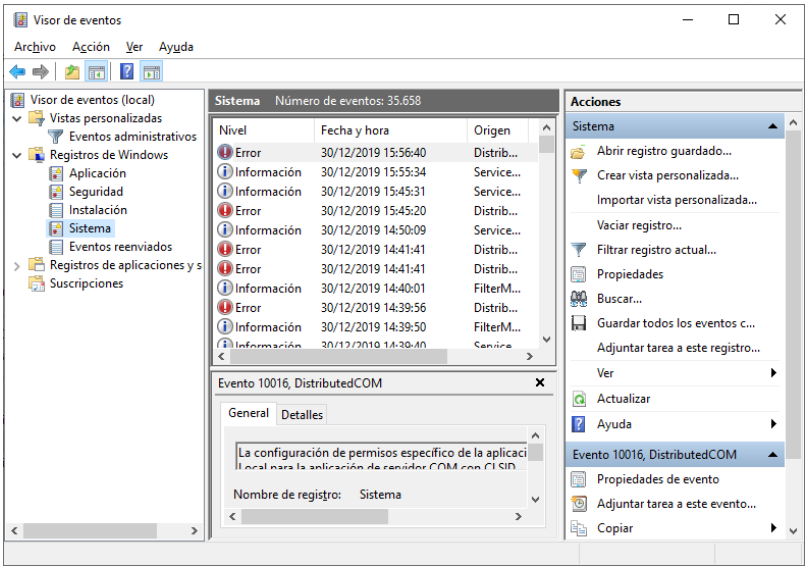
3.4.- Documentación de incidencias

Cada vez que se produce una incidencia de red es recomendable realizar un informe con el detalle de la incidencia. Este informe deberá contener entre otra la siguiente información:

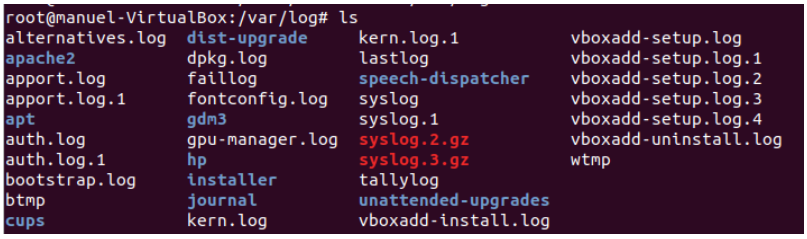
- Tipo de incidencia: fallo de seguridad, caída del sistema, etc.
- Equipos o servicios afectados
- Dia y hora
- Descripción de la incidencia
- Medidas tomadas para su resolución

Una de las fuentes que más información nos pueden dar sobre la incidencia son los logs del sistema. Un log (o diario) 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.

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. En Windows podemos acceder a Panel de control - Herramientas administrativas -Visor de eventos:



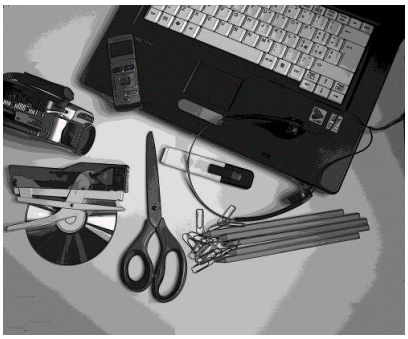
En Linux estos ficheros están en la carpeta /var/log:



A partir de estos logs se puede tener una idea de si el problema es del sistema, software o de seguridad, encauzándonos para buscar la solución.

4.- Herramientas de diagnóstico

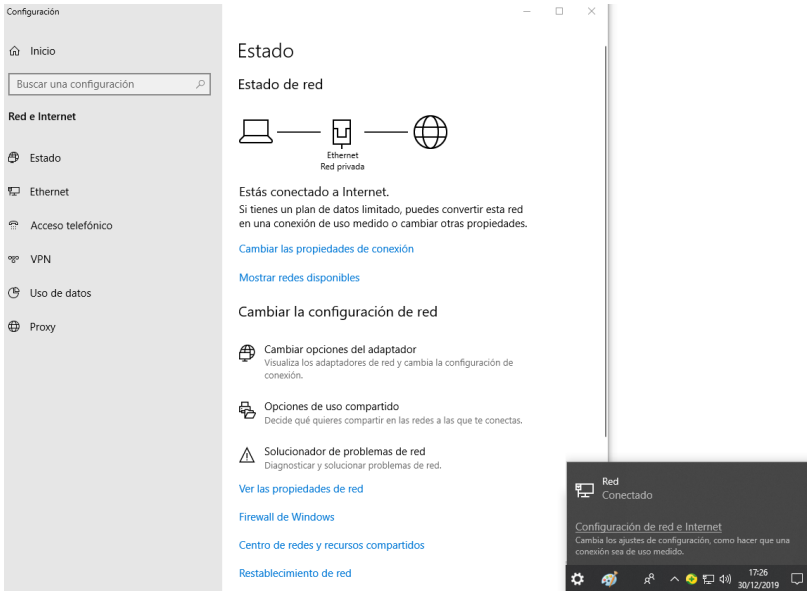
Es interesante conocer las posibles averías, sus efectos y la manera de repararlos, conociendo las herramientas existentes para ello.



En este apartado vamos a ver 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.

4.1.- Herramientas de red en Windows

En Windows la herramienta de red básica es “Configuración de red e internet” accesible desde la parte inferior derecha.



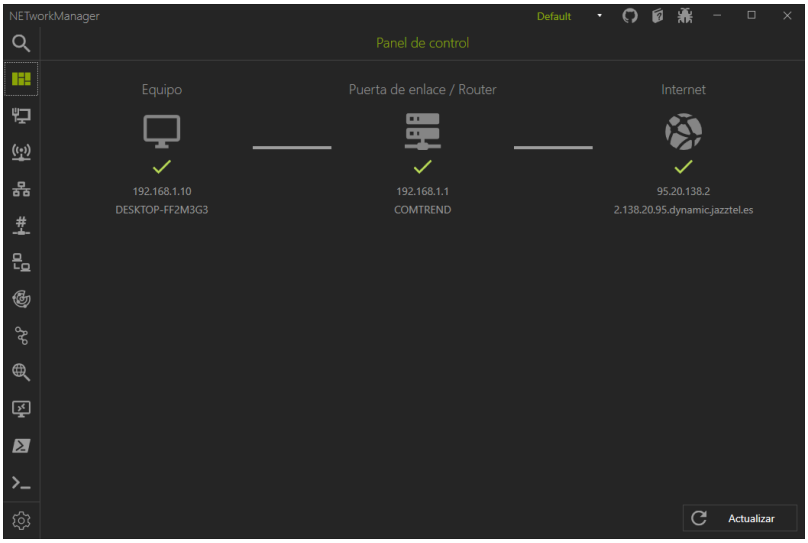
Desde el menú lateral izquierdo podemos: Estado: Nos indica la situación de la conexión

- Ethernet - Wifi - Acceso telefónico: nos informan sobre cada conexión concreta de las que dispongamos
- VPN: Permite crear una conexión privada virtual con otro dispositivo (es una conexión directa que utiliza la red pública -internet- para conectar redes privadas)
- Uso de datos: Informa del consumo de datos en nuestro equipo.
- Proxy: Permite configurar un proxy (servicio que hace de intermediario entre nuestro equipo e internet memorizando las consultas web que hacen los usuarios para poder reutilizarlas cuando otros usuarios realizan esas mismas consultas)

Desde la zona central podemos:

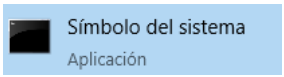
- Cambiar opciones del adaptador: permite configurar entre otros los parámetros IP (dirección, puerta de enlace, DNS), activar/desactivar la conexión, etc.
- Opciones de uso compartido: Configura uno de los servicios más usados en redes Windows las carpetas y recursos compartidos (impresoras, etc).
- Solucionador de problemas de red: Asistente para solucionar problemas de conexión
- Ver propiedades de red: Información sobre la red, es muy utilizada para comprobar la configuración de la red y encontrar posibles problemas de funcionamiento.
- Firewall de Windows: Administrar los accesos permitidos y prohibidos a nuestro equipo
- Centro de redes y recursos compartidos: Acceso a la configuración general de la red.
- Restablecimiento de red: Reiniciar la configuración de la red.

Además de las herramientas incorporadas en el sistema Windows podemos encontrar herramientas de otros fabricantes como NetworkManager herramienta gratuita que ofrece una gran cantidad de utilidades, tiene incluso una versión portable que no es necesario instalar.



4.2.- Comandos de red en Windows

Además de las herramientas gráficas anteriores ofrecidas por el sistema hay una serie de comandos que permiten monitorización y configuración de redes. Estos comandos se ejecutan desde la consola del sistema (Podemos acceder directamente buscando cmd).



Para obtener una información detallada de los comandos podemos escribir el comando seguido de /help o /?

En la ayuda mostrada los parámetros entre entre corchetes [ ] son opcionales.

Algunos de los comandos más importantes son:

- ipconfig sirve para informar de la configuración de red:

ipconfig /all: ofrece información detallada sobre todas las conexiones.

ipconfig /renew: Renueva la IP automática.

ipconfig /release: Libera la IP automática.

ipconfig /flushdns: Borra todas las entradas DNS. Esto es debido a que nuestro equipo memoriza las consultas DNS realizadas recientemente para evitar tener que consultar constantemente las mismas IP de dominios.

- ping comprueba la comunicación con otros equipos (estos equipos deben permitir las respuestas a ping, por seguridad es frecuente que estén desactivadas).
- tracert muestra la ruta hacia un equipo remoto detallando los routers que se atraviesan. Un comando más detallado y similar a este es pathping
- getmac obtiene la mac de la conexión de red. También podemos obtenerla ipconfig /all
- nslookup se emplea para probar el funcionamiento del DNS
- net este un comando amplio que permite realizar un diagnóstico de funcionamiento de la red en varios aspectos. También se utiliza para el acceso a recursos compartidos.

net start Inicia un servicio o muestra la lista de servicios iniciados

net stop detiene un servicio de Windows.

net share muestra los recursos compartidos

net user crea o elimina usuarios.

- netstat muestra las conexiones activas en el equipo, con el parámetro -a muestra todas las conexiones y puertos.
- route muestra y modifica la tabla de enrutamiento del dispositivo. Con la opción print muestra la tabla de enrutamiento. Con la opciones add, del y change añade borra y cambia.
- netsh es un símbolo del sistema especial para red, permite modificar, administrar y diagnosticar la configuración de una red, con más detalle y potencia que los anteriores

Autoevaluación

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

- ○ ping
- ○ ipconfig
- ○ netstat

Correcto

No. Con este comando solo obtenemos información del propio equipo

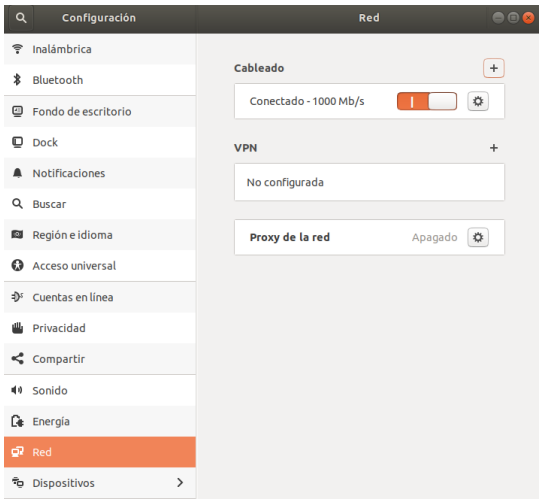
Incorrecto

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

4.3.- Herramientas de red en Linux

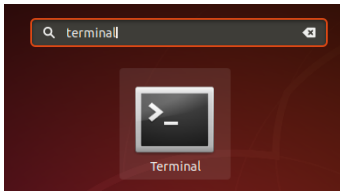
El funcionamiento de las herramientas y configuraciones de red en Linux es similar al que hemos visto en Windows, hay una herramienta básica incluida para la configuración de red, es equivalente a la “Configuración de red e internet”, desde esta opción establecemos la configuración básica de red (automática – estática, IPv4 IPv6 etc), también podemos crear VPNs ó establecer la configuración de un proxy (si salimos a través de un equipo proxy hacia internet), basta con buscar la aplicación “Configuración”:



En Linux también podemos utilizar una serie de herramientas para resolver incidencias en una red de área local como son el Monitor del Sistema u otras herramientas de terceros instalables con las que se puede administrar la red.

4.4.- Comandos de red en Linux

En las últimas versiones de Linux (Ubuntu 18.04 LTS) ha cambiado un poco el trabajo con comandos desde la consola y hay un comando principal “ip”. Para acceder a la consola buscamos la palabra “terminal”:



Al igual que en Windows podemos obtener información detallada indicando el comando seguido de help (por ejemplo, ip help), y si deseamos más información de una opción tecleamos comando opción help (por ejemplo, ip address help nos informa de las posibilidades de la opción address del comando ip)

Algunas de las opciones más usadas del comando ip son:

- ip address muestra y cambia la configuración de red. Se puede indicar en forma abreviada ip a
- ip link Activa desactiva la interface de red, le cambia el nombre, la pone en modo promiscuo, etc.
- ip route muestra y manipula la tabla de enrutamiento del equipo
- ip neigh muestra y manipula la tabla ARP

Además del comando ip tenemos:

- ping comprueba la comunicación con otros equipos
- ss muestra información acerca de las conexiones existentes, puertos en escucha o abiertos.
- dig para realizar consultas DNS

Reflexiona

¿Con qué comando comprobarías que tienes conexión a internet?

Mostrar retroalimentación

Una opción es hacer ping a algún servidor de internet, por ejemplo, ping www.google.es

Otra opción puede ser el comando dig (siempre que nuestro servidor DNS sea externo a nuestra red) porque si consultamos por ejemplo información de un dominio necesitará salir al exterior: dig google.es

4.5.- Problemas de conexión a la red de un equipo

Es habitual encontrarnos con problemas como que un usuario que no tenga acceso a internet o al servidor de la empresa.

En general podemos realizar una serie de comprobaciones básicas que suelen solucionar bastantes de estos problemas:

- Lo primero será comprobar la conexión del cable o WIFI, desde el propio equipo nos avisa solo tenemos que observar los iconos en pantalla, también podemos comprobar el cable físico:
  - Red cableada 
  - Red inalámbrica 
- Si es aspecto es que la conexión físicamente es correcta ó los parámetros WIFI son correctos, lo siguiente es consultar la configuración del equipo y comprobar los parámetros básicos IP, máscara, puerta de enlace y DNS con las herramientas y comandos aprendidos anteriormente   :
- Si la conexión es automática, comprobar que esta asignación se realiza de forma correcta (NO deber tener una IP del tipo 169.254.X.X, esto es síntoma de que el servidor DHCP no funciona o no conectamos con él)
- Si es estática repasar los parámetros para comprobar que no hay errores:
  - Hacer un ping a la puerta de enlace (si no funciona el problema lo tenemos dentro de nuestra red: cableado, switchs, señal WIFI deficiente, etc.)
  - Si funciona, hacer un ping a una IP externa (por ejemplo 8.8.8.8, si no funciona el problema está posiblemente nuestro router al exterior, es recomendable probar más de una IP)
  - Si funciona, hacer un ping a un dominio (por ejemplo google.es, si no funciona es posible que sea el servicio DNS el que este mal)

Pero aparte de las averías típicas, que suelen ser las más frecuentes y que se ven rápidamente con los pasos anteriores, a veces nos encontramos con averías difíciles de solucionar como un mal funcionamiento del hardware de red o un parámetro mal configurado en el router (hay que tener en cuenta que estos dispositivos tienen muchos parámetros configurables).

5.- Prevención de riesgos profesionales

Caso práctico

Blanca está en la academia de María acabando de instalar un punto de acceso, cuando María se acerca ve que está realizando la instalación sin prácticamente ninguna medida de seguridad. María le advierte, en cualquier momento puede pasar algo, caerte por estar subido en una silla, que te de una descarga eléctrica no has desconectado la luz y estás manipulando el enchufe.

María le recuerda que las medidas de seguridad en el trabajo son muy importantes.

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

5.1.- Riesgos

En primer lugar hay 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 trabajo 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

En el caso de la instalación comentado anteriormente, lo correcto es que antes de su contratación la empresa haya informado al trabajador sobre los riesgos específicos de su trabajo, como el riesgo a caídas, heridas o golpes si no manipula bien las herramientas de trabajo.

Por su parte el trabajador como medidas de prevención deberá evitar el mal uso de dichas herramientas y se le habrá facilitado información sobre cómo se debe hacer.

5.2.- 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

Incorrecto, se realiza antes del accidente

Incorrecto, se realiza antes del accidente

Incorrecto, se realiza antes del accidente

Efectivamente

Solución

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

5.3.- Trabajo con ordenadores

Toda persona que trabaja en el sector de la informática y las comunicaciones necesita utilizar ordenadores con pantallas de visualización, teclados y ratones. Es importante que conocer 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 conviene tener en cuenta sobre la pantalla son los siguientes:

- La pantalla debe estar situada 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 al menos 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.

5.4.- Trabajo con riesgo eléctrico o con riesgo de caídas

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

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

En otras ocasiones a la hora de realizar instalaciones de equipos de comunicaciones y redes habrá 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.

6.- Normativa de prevención

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 salud 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.

Siguiendo el mandato de la Constitución Española y también el deber de transponer la Directiva Europea 89/391/CEE aparece la Ley 31/1995 de Prevención de Riesgos Laborales (LPRL), modificada y actualizada por la Ley 54/2003, de 12 de diciembre, de reforma del marco normativo de la prevención de riesgos laborales. 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

Opción correcta

Incorrecto

Incorrecto

Incorrecto

Solución

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

7.- Normativa de protección ambiental

Resulta 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 11/2014, de 3 de julio, por la que se modifica la ley 26/2007, de 23 de octubre, de Responsabilidad Medioambiental.
- Real Decreto 1015/2013, de 20 de diciembre, por el que se modifican los anexos I, II y V de la Ley 42/2007, de 13 de diciembre, del Patrimonio Natural y de la Biodiversidad.
- Ley 21/2013, de 9 de diciembre, de evaluación ambiental.
- Ley 11/2012, de 19 de diciembre, de medidas urgentes en materia de medio ambiente.
- Real Decreto-ley 17/2012, de 4 de mayo, de medidas urgentes en materia de medio ambiente.
- Ley 26/2007, de 23 de octubre, de Responsabilidad Medioambiental.

Para saber más

Desde la web del Ministerio para la Transición ecológica podemos obtener más información:

https://www.miteco.gob.es/es/calidad-y-evaluacion-ambiental/legislacion/

Anexo. Licencia de Recursos

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurso (2)
	Autoría: Sodipodi Licencia: CC 2.5 Procedencia: http://es.wikipedia.org/wiki/Archivo:High_voltage_warning.svg		Autoría: Creado por varios usuarios en Wikimedia Licencia: Dominio público Procedencia: http://commons.wikimedia.org/wiki/File:Flag_of_Europe.s
	Autoría: khaase Licencia: Pixabay License Procedencia: https://pixabay.com/es/vectors/sin-conexi%C3%B3n-desconectado-wifi-red-525700/		Autoría: Desconocido Licencia: Libre uso comercial Procedencia: https://www.pxfuel.com/es/free-photo-xijxp
	Autoría: Antonio Cañas Vargas Licencia: CC BY 2.0 Procedencia: https://www.flickr.com/photos/acanasvargas/10962355176		Autoría: Desconocido Licencia: Creative Commons CC0 Procedencia:https://pxhere.com/es/photo/1565521
	Autoría: graziola Licencia: CC BY 2.0 Procedencia: https://www.needpix.com/photo/download/5807/office-tools-computer-free-pictures-free-photos-free-images-royalty-free-free-illustrations		Autoría: Desconocido Licencia: Creative Commons CC0 Procedencia:https://in3.umg.edu.gt/images/3.png
	Autoría: Desconocido Licencia: CC BY 2.0 Procedencia: https://economipedia.com/ranking/ranking-de-inflacion-por-paises-2018.html		Autoría: Desconocido Licencia: Creative Commons CC0 Procedencia:https://psicologiaymente.com/miscelanea/ti termometros
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY