TEMA 7

INDICE

Administración de redes. (Windows III).

Caso práctico

***Juan**, empleado de la empresa BK Programación, está trabajando con su Windows 7 recién instalado, y mientras espera a que se actualice automáticamente desde Internet, está reflexionando sobre lo fácil que ha sido hacer la instalación y sobre todo que el equipo esta conectado a una red y él no ha tenido que configurar prácticamente nada. Sin embargo, han debido de establecerse una serie de configuraciones internas que a él le gustaría conocer por si necesita manejarlas en un futuro.*

1.- Administración de redes en Windows 7.

Caso práctico

***Juan** se plantea cómo se ha configurado el ordenador de forma automática, y que apenas ha tenido que intervenir en la configuración de la red. Está pensando que debería conocer más sobre la configuración de redes en Windows, ya que puede serle útil en algún momento y además, en algunos casos, puede necesitar no sólo quedarse con la configuración por defecto, si no ir más allá. Por eso va a repasar la administración de la red dentro del sistema operativo.*

Administrar una red consiste en aplicar una serie de técnicas que la mantengan siempre operativa, de forma óptima y segura, para gestionar el uso eficiente de sus recursos y garantizar la calidad de los servicios que ofrece.

Con Windows 7 es posible administrar nuestro equipo para mantenerlo operativo dentro de las redes en las que podamos integrarlo, aprovechando por un lado los recursos que ofrezcan y de otro aportándoles nuestros propios recursos. Windows 7 ofrece la posibilidad de definir y fijar varias configuraciones en función de las diferentes redes a las que tengamos acceso, para después conectarnos a una u otra con sólo seleccionar su configuración. Y si tenemos varios adaptadores de red podemos usarlos para conectar a distintas redes a la vez, y después, incluso podemos hacer puente entre ellas.

Iremos viendo el hardware y el software que se necesita para realizar, en cada caso, cada uno de los tipos de conexiones posibles, en función del tipo de red a la que los dispositivos de comunicación, permitan conectar. Además de ver como conectarnos, veremos qué se necesita para compartir y utilizar recursos compartidos.

Existen diversas opciones para implementar redes, de modo que hay que utilizar un hardware, en concreto un determinado tipo de adaptador de red, acorde con la tecnología empleada por la red a la que haya que conectar.

Haciendo un repaso de las tecnologías de red más comunes y del tipo de hardware que utilizan, nos encontramos con los siguientes tipos de redes: Inalámbrica, Ethernet, y Powerline.

- ✓ Las redes inalámbricas Wi-Fi utilizan ondas de radio para la comunicación entre los equipos. Su velocidad de transmisión depende del estándar que utilizan y de las condiciones ambientales en que se desarrolla la comunicación. El más común, IEEE 802.11g, puede transmitir datos a una velocidad máxima de 54 Mbps y el más reciente, el IEEE 802.11n puede llegar a transmitir datos a velocidades de 600 Mbps. Se necesita un adaptador de red inalámbrico para el equipo, que bien ya puede tener integrado, o que puede conectarse mediante USB.
- ✓ Las redes inalámbricas WWAN, también llamadas tecnología de red de área extensa inalámbrica, usan la banda ancha móvil para proporcionar conexión móvil a Internet, dependiendo su velocidad del caudal contratado al operador móvil. Normalmente, el operador proporciona el adaptador adecuado con un módulo SIM (Modulo de Identificación de Suscriptor) incorporado, que se conecta al equipo mediante USB. Hoy día puede llegar a velocidades de 1,8 Mbps y en un futuro próximo de 3 a 6 Mbps.

- ✓ Las redes Ethernet usan cables de tipo Ethernet para el envío de información entre equipos. En función de las características del hardware de red que interviene en la comunicación, (adaptadores de red, cables de red, concentradores, conmutadores, enrutadores, etc.) los datos se van a transmitir a velocidades de 10, 100 o 1.000 Mbps. Se necesita un adaptador, que suele estar instalado en el interior del equipo, con conexión del tipo RJ45 al que se conecta el cable de red.
- ✓ Las redes Powerline son un caso especial de redes Ethernet, que usan la instalación de cableado eléctrico doméstico para enviar la información de un equipo a otro, pero que necesita un adaptador especial para que los datos pasen del cable Ethernet que sale del ordenador, al cable eléctrico y al llegar a su destino, otro adaptador que pase los datos del cable eléctrico al cableEthernet del otro ordenador. Tiene la ventaja de no necesitar concentradores ni conmutadores para conectar más de dos equipos en la red Powerline. Pueden transferir datos a 500 Mbps.

Aunque el hardware pueda ser distinto, todas estas tecnologías de red tienen en común el hecho de que utilizan el mismo protocolo de comunicación, el TCP/IP.

Con Windows 7 la dirección IP que necesita cada adaptador de red para comunicarse a través del protocolo TCP/IP puede asignarse de forma manual, o dinámica por medio de DHCP, y se utiliza tanto IPv4 como IPv6.

A la hora de elegir una tecnología de red, debe tenerse en cuenta dónde y cómo van a estar ubicados los equipos y la velocidad de transferencia deseada de la red.

En la Web de Microsoft puedes ver los requisitos hardware necesarios para la instalación de las distintas tecnologías de red.
http://windows.microsoft.com/es-ES/windows7/What-you-need-to-set-up-a-home-network

Con Windows 7 podemos integrar nuestro equipo en distintas redes, pero:

- ○ Debemos instalar el software de red adicional necesario para ello.
- ○ Sólo si son redes cableadas de tipo Ethernet.
- ○ Es necesario utilizar el protocolo de comunicaciones DHPC/IP para comunicarse con otros equipos.
- ◉ **Todas la respuestas anteriores son incorrectas.**

1.1.- Instalar y configurar componentes de red.

En la configuración para la conexión de los equipos en red intervienen elementos hardware, los dispositivos de comunicación y elementos software; los drivers para el hardware de comunicación, y los programas que manejan y gestionan los protocolos de las comunicaciones, y los transvases de información.

Es evidente que cada tipo de red necesita de un hardware específico adaptado a las características particulares del sistema de comunicación empleado. Por ello a la hora de conectar un nuevo equipo, a una red existente, hay que asegurarse de emplear hardware que mantenga la compatibilidad.
Una vez instalado el adaptador de red adecuado hay que configurarlo adecuadamente para la conexión, lo que incluye tanto la instalación de sus drivers, como la configuración de los protocolos y valores de red necesarios.

Es habitual que en los ordenadores actuales haya integrada una tarjeta de red de tipo Ethernet con conector RJ45 y si se trata de equipos portátiles, no les va a faltar un adaptador de red de tipo Wi-Fi. Estos dispositivos habrán sido detectados durante la instalación del sistema operativo Windows 7 y normalmente, sus controladores configurados adecuadamente sin problemas.

También existe la posibilidad de agregar, posteriormente a la instalación del sistema operativo, tarjetas PCI internas que pueden ser adaptadores de red Ethernet tanto alámbricos como inalámbricos, o adaptadores de red inalámbricos externos de tipo USB.

Pero aunque Windows 7 los detecte, instale sus drivers y les asocie protocolos y servicios de red, quizás sea necesario configurarle a cada adaptador los parámetros particulares de red, (dirección IP, máscara de red, etc.) que permitan integrarlo en la red deseada, si no hay en dicha red un servidor que lo haga automáticamente, o si el adaptador de red no ha sido configurado para ello.

Finalmente se puede verificar si nuestro equipo ya está conectado a la red y funciona correctamente observando el gráfico del esquema de red desde el Centro de redes y recursos compartidos, como veremos a continuación.

En adelante veremos como configurar distintos tipos de conexiones administradas por Windows 7.
Si la red no existe aun, primero habrá de instalarse el hardware necesario (router, switch, punto de acceso, cableado, …) para crear una infraestructura adecuada que permita mantener la comunicación. Después se empieza configurando la red en un equipo, y posteriormente se pueden ir añadiendo nuevos equipos.

En la Web de Microsoft puedes ver cómo se asigna una dirección IP a una tarjeta, aunque se hable de Vista, el proceso es idéntico en Windows 7.
http://windows.microsoft.com/es-ES/windows-vista/Change-TCP-IP-settings

Se puede obtener más información sobre las redes, buscando el término "red" en Ayuda y soporte técnico, opción que se despliega desde el botón de Inicio.

¿Cual de las siguientes respuestas completaría la frase correctamente?
Los equipos administrados por Windows 7 que vayan a conectarse en red……

- ○ Deben configurarse como switch de red con sus controladores y protocolos correspondientes.
- ◉ **Necesitan de una infraestructura de red adecuada que permita mantener la comunicación.**
- ○ Necesitan tener instalado y configurado para la conexión, al menos un adaptador de red inalámbrico y otro por cable.
- ○ Necesitan protocolos distintos e independientes para redes inalámbricas y para redes Ethernet.

1.2.- Centro de redes y recursos compartidos. Mapa de red y redes activas.

El Centro de redes y recursos compartidos es un entorno proporcionado por Windows 7 en el que se centraliza todo lo relacionado con las redes. Se trata de una ventana desde la que se puede obtener información básica sobre el estado de la red, ya que muestra las conexiones actuales del equipo; si está conectado o no, el tipo de conexión establecido, los niveles de acceso permitidos a otros equipos y a otros dispositivos de la red, etc.

Toda esta información puede llegar a ser muy útil a la hora de configurar nuevas conexiones de red o cuando haya que repararlas, si surgen problemas de conexión, tareas también centralizadas desde esta ventana, a la que se llega haciendo clic en **Inicio**, **Panel de control**, **Redes e Internet**, y por fin en **Centro de redes y recursos compartidos**, o desde el enlace que aparece al abrir el icono de red del área de notificación. En ella podemos diferenciar varias zonas de actuación:

Se puede ver en la zona superior un gráfico, a modo de esquema, con la representación visual de la red. Contiene una línea representando al medio de comunicación que une los tres iconos, que a su vez representan al equipo, a la red y a Internet. Podemos hacer clic sobre ellos y nos aparecerán respectivamente: la ventana Equipo, la ventana con los dispositivos y las carpetas que comparte el equipo en la red, y la ventana del navegador.

Si surgen problemas en la red, como errores de configuración o corte en la conexión, aparece un pequeño icono sobre la línea de comunicación para dar una pista de lo que ocurre, y al que se le puede hacer clic para que se ponga en marcha el asistente de diagnósticos de red de Windows e intente solucionarlos.

A la derecha del esquema aparece el enlace **Ver mapa completo** desde dónde ver, si es que los hay, más equipos y dispositivos conectados a la red y encontrar información más detallada acerca de la red. Igualmente se muestra un gráfico de los equipos y dispositivos de la red unidos por líneas a modo de esquema de la forma en que están conectados. También se señalan las áreas que puedan tener problemas, para intentar darles solución.

Más abajo separadas por una raya se pueden ver las redes activas, normalmente hay una, pero si se dispone de más adaptadores se puede estar conectado a más de una red. Al final de la raya hay un enlace para **Conectar o desconectar**, que en este caso, al ser pulsado, abre el icono de red del área de notificación para que podamos desconectarnos de la red actual y en su caso, conectarnos a una red distinta.

Cada red activa, esta representada por un icono, por su nombre de red y pertenece a un tipo de red. El icono y el nombre podemos cambiarlo a nuestro gusto en la ventana que se abre al pulsar sobre el icono. El tipo de red es en sí un enlace que abre la ventana **Establecer ubicación de red**, donde poder cambiar su tipo a una de las tres posibles preestablecidas: red domestica, de trabajo y pública, en función de lo cual, Windows 7 ajusta sus niveles de seguridad.

Si aquí no aparece un icono de red es porque no hay ninguna conexión de red activa, hecho que puede verificarse sobre el esquema de red de más arriba.

A la derecha del icono de red correspondiente a la conexión activa se muestra la siguiente información:

El tipo de acceso, si se pertenece o no al grupo hogar (enlace para cambiar configuraciones de grupo en el hogar) y la conexión de red utilizada, (enlace para llegar a la ventana Estado de la conexión). Ventana desde la que podremos ver Detalles de la conexión y actuar sobre sus Propiedades.

La siguiente es la zona que ocupa la parte inferior de la pantalla, contiene varios enlaces; útiles para Configurar una nueva conexión en red, para Conectarse a una red, para Elegir grupo en el hogar, y opciones de uso compartido y para Solucionar problemas de red.

La zona de la banda izquierda de la ventana del Centro de redes y recursos compartidos contiene una serie de enlaces esenciales para la configuración de las redes. Desde ella, además de volver a la ventana del panel de control, podemos:

- ✓ **Administrar redes inalámbricas.**
- ✓ **Cambiar configuración del adaptador.**
- ✓ **Cambiar configuración de uso compartido avanzado.**
- ✓ Y también: **Administrar el Firewall** de Windows 7, **El grupo en el hogar** y las **Opciones de Internet**.

Algunos de estos enlaces nos llevan a sitios que ya se han visto y comentado. Otros serán objeto de próximo estudio.

Señala la respuesta que no corresponde a la siguiente pregunta: ¿Qué es centro de redes y recursos compartidos?

- ○ Es el entorno proporcionado por Windows 7 en el que se centraliza todo lo relacionado con las redes.
- ◉ **El dispositivo al que hay que conectar el equipo para que pertenezca a una red.**
- ○ La ventana desde donde ver un gráfico, a modo de esquema, con la representación visual de la red.
- ○ La ventana desde donde configurar nuevas conexiones de red, o elegir grupo en el hogar, o solucionar problemas de red, entre otras operaciones relativas a la red.

1.3.- Grupo Hogar y área local.

Grupo Hogar es una característica de Windows 7 que facilita el uso compartido de archivos e impresoras en una red doméstica, pero teniendo en cuenta que para poder formar parte de un Grupo en el hogar todos los equipos de la red deben ejecutar Windows 7. Es una forma sencilla de compartir, y de tener acceso a los archivos y a los dispositivos compartidos de otros equipos del la red doméstica, a los que puedo llegar a través de mi explorador de archivos, y utilizarlos como si estuvieran en mi propio equipo.

Crear un grupo en el hogar, o unirse a uno que ya existe, es tan fácil como ejecutar un asistente, y durante su proceso de configuración decidir a base de clic, las carpetas, las bibliotecas y las impresoras que se quieren compartir, y las que se quieren mantener privadas. Posteriormente, y siempre que interese, cada usuario puede variar lo que comparte con igual facilidad.

Los recursos compartidos en un grupo hogar se protegen mediante una contraseña que el asistente genera durante su creación y cada vez que un equipo se incorpora al grupo debe utilizarse esa contraseña. La contraseña inicial que se genera para Grupo Hogar puede ser sustituida cuando se quiera, pero teniendo en cuenta que como todos los equipos miembros están protegidos por la misma contraseña, si se cambia hay que cambiársela a todos.

Un Grupo Hogar puede crearse y administrar su configuración desde el Centro de redes y recursos compartidos, desde donde se pueden vincular o separar fácilmente equipos con Windows 7 de una red domestica, para así poder compartir, o dejar de compartir; imágenes, música, videos, documentos y dispositivos.

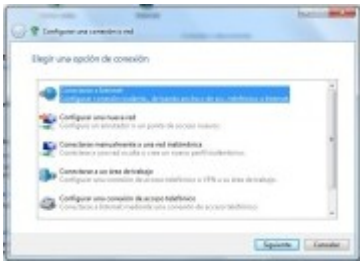
Página de Microsoft en el que se hace una breve presentación de lo que es un Grupo en el hogar.
http://windows.microsoft.com/es-ES/windows7/products/features/homegroup
En las distintas pestañas de esta Web de Microsoft puedes ir viendo que es un Grupo Hogar de principio a fin.

http://windows.microsoft.com/es-ES/windows7/help/homegroup-from-start-to-finish
Otra Web de Microsoft que contiene vínculos relacionados con Grupo Hogar para obtener más información.
http://windows.microsoft.com/es-ES/windows7/HomeGroup-recommended-links
Vídeo de Microsoft que explica como Compartir archivos con Grupo Hogar
http://windows.microsoft.com/es-ES/windows7/help/videos/sharing-files-with-homegroup

¿Cuáles de las siguientes afirmaciones respecto al asistente de creación de un grupo en el Hogar son correctas?

- [x] **El asistente te permite elegir los recursos que compartes.**
- [ ] El asistente te permite elegir con que usuarios de dominio compartes los recursos.
- [x] **El asistente te solicita una clave cuando quieres unirte a un grupo en el hogar que ya existe.**
- [ ] El asistente le crea a cada miembro del grupo en el hogar su clave particular cuando se une al grupo para compartir recursos.

1.4.- Configuración de una nueva conexión de red.



Como hemos visto anteriormente, **Configuración de una nueva conexión de red** es una de las opciones incluidas en el **Centro de redes y recursos compartidos** que cuando se activa, abre la ventana **Configurar una conexión o red** en la que se puede elegir de una lista, una de las siguientes posibles opciones de conexión. Cada una de ellas iniciará un asistente que nos guiará por un camino u otro en función del tipo de red escogida, e irá solicitándonos los datos que necesite mientras va creando la conexión correspondiente:

Conectarse a Internet. Para configurar conexión inalámbrica de banda ancha o de acceso telefónico a Internet.

Configurar una nueva red. Para configurar un enrutador o un punto de acceso nuevos.

Conectarse manualmente a una red inalámbrica. Para conectarse a una red oculta o para crear un nuevo perfil inalámbrico.

Conectarse a un área de trabajo. Para configurar una conexión de acceso telefónico o VPN a su área de trabajo.

Configurar una conexión de acceso telefónico. Para conectarse a Internet mediante una conexión de acceso telefónico.

Configurar una red ad hoc inalámbrica (de equipo a equipo). Para configurar una red temporal para compartir archivos o una conexión a Internet.

Iremos viendo este tipo de conexiones en los próximos apartados del tema.

Página de Microsoft que explica las diferentes formas de organizar equipos en las redes con Windows 7.
http://windows.microsoft.com/es-ES/windows7/What-is-the-difference-between-a-domain-a-workgroup-and-a-homegroup

¿Cuál de las siguientes opciones no pertenece a Configurar una conexión o red?

- Conectarse a Internet.
- Conectarse a un área de trabajo.
- **Conectarse a un grupo en el hogar.**
- Configurar una red ad hoc inalámbrica.

1.5.- Configuración de una red inalámbrica.

Las principales ventajas que ofrece una red inalámbrica son, por un lado la posibilidad de movilidad física de los equipos que se conectan a ella dentro de su radio de cobertura, y por otro la facilidad de configuración y de uso que han llegado a conseguir.

A continuación vemos los pasos necesarios para configurar y para utilizar una red inalámbrica, pero antes de nada, comentar que es esencial el uso de un router o punto de acceso inalámbrico al que se puedan conectar los adaptadores inalámbricos de los distintos equipos que formarán la red inalámbrica. La situación del router debe elegirse cuidadosamente para que su señal llegue con buena calidad y con el mínimo de interferencias a todos los puntos de nuestro entorno de conexión. Sin embargo también hay que valorar el hecho de que su señal, puede traspasar nuestros límites y puede ser accedida y utilizada por terceras personas con buenas o malas intenciones. Por ello debemos poner espacial cuidado en extremar los detalles relativos a su seguridad.

El primer paso de la configuración será configurar el router o punto de acceso inalámbrico con los valores que se ajusten a nuestras necesidades o preferencias. Así podemos:

- ✓ Cambiar el nombre y contraseña genéricos que el fabricante asigna de forma predeterminada al usuario con el que se configura el dispositivo, protegiéndolo así de accesos indeseados.
- ✓ Personalizar el nombre de la red, asignándole un nuevo nombre de SSID, que es el identificador que aparece en la lista de redes disponibles. Con el cambio se evitan confusiones de identificación con otros modelos que puedan estar funcionando alrededor con el mismo SSID predeterminado asignado de fábrica.
- ✓ Establecer una clave de seguridad de red, para impedir que se conecten usuarios no autorizados y para activar el cifrado de cualquier información que se envíe a través de ella. Existen varios métodos de cifrado de red inalámbrica muy comunes, y con distintos grados de seguridad: WEP, WPA, WPA2, ...

Si aún no esta configurado, puede ser necesario ejecutar el **Asistente para configurar un enrutador o punto de acceso inalámbrico** que se encuentra en el panel izquierdo de la ventana de Centro de redes y de recursos compartidos. Asistente que nos guiará durante el proceso de agregar otros equipos y dispositivos a la red.

Página de Microsoft con explicaciones acerca de la configuración de los routers inalámbricos en Windows 7.
http://windows.microsoft.com/es-ES/windows7/set-up-a-wireless-router

El siguiente paso en la configuración, es ir agregando equipos a la red inalámbrica, que es tan fácil como hacer clic en el icono de la red del área de notificación para abrir **Conectarse a una red,** seleccionar el nombre de nuestra red de entre la lista de redes que aparecen y entonces hacer clic en **Conectar**.

Cuando se solicite, hay que escribir la clave de seguridad definida anteriormente para la red. También se puede utilizar una unidad flash USB que contenga la clave de seguridad, si es que la grabamos anteriormente.

Vídeo-tutorial que explica cómo configurar una red inalámbrica en Windows 7.
http://www.youtube.com/watch?feature=player_embedded&v=mNDs7ijK7Fs

Para configurar una conexión inalámbrica Wi-Fi, es necesario:

- ○ Un adaptador de red inalámbrico de tipo WWAN.
- ○ Usar el nombre o SSID del punto de acceso como clave de seguridad.
- ○ Estar fuera del radio de interferencias del punto de acceso.
- ◉ **Tener configurado el adaptador de red con los parámetros adecuados del protocolo TCP/IP.**

Se configuran por medio de un servidor DHCP, o manualmente.

1.6.- Configuración de una red de equipo a equipo (ad-hoc).

Una red ad hoc está formada únicamente por 2 equipos, que se unen exclusiva y directamente por medio de sus adaptadores inalámbricos, sin necesidad de conectarse a través de un enrutador. Este tipo de redes, que solo pueden ser inalámbricas, se suelen utilizar de modo temporal para jugar en red, para compartir ficheros, o compartir la conexión a Internet entre dos equipos que deben estar relativamente próximos entre sí.

Para configurar una red de equipo a equipo (**ad hoc**) hay que ir a Centro de redes y recursos compartidos, seleccionar Configurar una nueva conexión o red y hacer clic en Configurar una red ad hoc inalámbrica (de equipo a equipo), después hacer clic en Siguiente y, a continuación, seguir los pasos del asistente.

Puede activar el uso compartido con protección con contraseñas para exigir a otros usuarios que tengan una cuenta de usuario en el equipo para tener acceso a los elementos compartidos. Para ello hay que ir a Centro de redes y recursos compartidos y en su panel izquierdo, hacer clic en Cambiar configuración de uso compartido avanzado.

Después hay que expandir el perfil de red actual haciendo clic en las comillas angulares e ir a Activar el uso compartido con protección por contraseña, si esta desactivado, y por último Guardar cambios. Para hacer este cambio es posible que el sistema solicite una contraseña de administrador.

Una red **ad hoc** puede convertirse en permanente si así se decide durante su proceso de creación, en caso contrario, se eliminará automáticamente cuando deje de haber conexión, ya sea porque uno de los dos usuarios se desconecte de la red, o porque la conexión se corte por alejamiento o interferencias.

Vídeo que muestran cómo hacer una red ad hoc con Windows 7
http://www.youtube.com/watch?feature=player_embedded&v=0eVH1lOFISA
Explicación para crear y configurar una red ad hoc.
http://www.comusoft.com/crear-y-configurar-una-red-ad-hoc-en-windows-7

El tipo de redes **ad hoc** sólo pueden crearse mediante conexiones inalámbricas, sin embargo también existe la posibilidad de conectar dos equipos directamente, con un cable cruzado de tipo Ethernet, que es como un cable normal pero con algunos de sus contactos en distinta posición. Para ello es necesario que ambos equipos dispongan de adaptador de red Ethernet.

Pagina de Microsoft que explica como conectar dos equipos directamente con un cable Ethernet cruzado.
http://windows.microsoft.com/es-ES/windows7/Connect-two-computers-using-a-crossover-cable

Una configuración de red ad hoc es la unión temporal de dos ordenadores para compartir sus recursos a través de:

- ○ Sus dos adaptadores Ethernet mediante cable directo.
- ◉ **Sus dos adaptadores Wi-Fi en conexión directa.**
- ○ Sus dos adaptadores powerline en conexión directa.
- ○ Sus dos adaptadores Wi-Fi conectados ambos con un punto de acceso intermedio.

1.7.- Configuración de una conexión con banda ancha.

Para configurar una conexión a Internet de banda ancha es imprescindible disponer de una cuenta con un proveedor de servicios de Internet (ISP) y el dispositivo de red (enrutador o cable módem) que nos suele facilitar el proveedor, convenientemente preconfigurado para que conectemos con él, de modo que sólo necesitamos enchufarle nuestro adaptador de red para tener conexión inmediata.

Se puede comprobar que la conexión a Internet funciona correctamente, si se pueden ir abriendo páginas con el navegador de Internet normalmente y no aparecen mensajes de error.

Si el proveedor de servicios de Internet no configuró el dispositivo de red, o se quiere usar uno que no haya sido facilitado por él, será necesario configurarlo con los parámetros adecuados para la conexión, que en ese caso nos tiene que facilitar nuestro proveedor. Sólo hay que buscar un poco en la red para encontrar páginas de ayuda, que proporcionan tutoriales con los pasos necesarios para configurar la mayoría de los routers y para los distintos proveedores.

Pagina de Microsoft que explica como realizar una conexión de banda ancha (ADSL o de cable).
http://windows.microsoft.com/es-ES/windows7/Set-up-a-broadband-DSL-or-cable-connection

Existe otra forma novedosa de conectarse a Internet que es usando la Banda Ancha Móvil. Es un servicio ofrecido por los proveedores de telefonía móvil que permite la conexión a Internet en cualquier lugar en el que se disponga de cobertura móvil. Dependiendo del operador y del tipo de conexión (GPRS, 3G, HSDPA) se puede trabajar con velocidades de casi 2 Mbps o superiores.

La conexión a Internet se realiza por medio de un módem de tipo USB, normalmente subvencionado y bloqueado por la operadora a la que se contrata el servicio. También se puede aprovechar la capacidad que tienen para actuar como módem algunos de los teléfonos móviles actuales. Y estos pueden conectarse al ordenador por USB o Bluetooth.

Página de Microsoft que explica como usar la banda ancha móvil para conectarse a Internet.
http://windows.microsoft.com/es-ES/windows7/Use-mobile-broadband-to-connect-to-the-Internet

Señala las respuestas correctas: La conexión de banda ancha necesita:

- [x] **Un dispositivo de conexión como un router o un cable módem correctamente configurado para conectar con el proveedor de Internet.**
- [x] **Los datos de conexión proporcionados por el proveedor.**
- [x] **Una cuenta con un proveedor de Internet, por ADSL o por cable.**
- [ ] Todas las respuestas anteriores son falsas.

1.8.- Configuración de una conexión de acceso telefónico.

Este tipo de conexión, que emplea la línea telefónica se ha quedado obsoleta y esta desfasada debido a sus bajas tasas de transferencia que se estancaron en un máximo de 56 Kbps. Aun así Windows7 la mantiene para poder realizar conexiones punto a punto entre dos equipos, o para utilizarla en lugares dónde no se disponga de una mejor alternativa, y para conexiones a través de líneas RDSI.

Se necesita conectar al ordenador un módem analógico por puerto serie o USB, y este a su vez a la línea telefónica. También es necesario tener conectado un módem al otro lado de la línea telefónica con el que establecer la comunicación.

Página de Microsoft donde explica la forma de conectarse a Internet a través de la conexión de acceso telefónico.
http://windows.microsoft.com/es-ES/windows7/Advanced-dial-up-settings

1.9.- Comandos básicos para resolución de problemas de red.

Windows 7 posee gran cantidad de solucionadores de problemas, incluso para aquellos problemas relacionados con la red, pero a veces, es necesario conocer las utilidades o comandos IP, para analizar y para obtener información que ayude a la hora de configurar y mantener una red TCP/IP.

A continuación vemos una lista de utilidades o comandos básicos del protocolo TCP/IP, que deben ejecutarse desde el símbolo del sistema en una ventana de comandos:

`arp`: Resolución de direcciones IP en direcciones MAC. Muestra las tablas de traducción de direcciones IP a direcciones físicas utilizadas por el protocolo de resolución de dirección (ARP).

`hostname`: Muestra el nombre del equipo en el que se ejecuta.

`ipconfig`: Muestra o actualiza la configuración de red TCP/IP. Se utiliza para conocer la configuración de direcciones IP de la red local. Muestra entre otras cosas: la dirección IP activa, la máscara de red, y la puerta de enlace predeterminada de las interfaces de red conocidas en el equipo local.

`nbtstat`: Actualización del caché del archivo Lmhosts. Muestra estadísticas del protocolo y las conexiones TCP/IP actuales utilizando NBT.

`netstat`: Muestra el estado de la pila TCP/IP en el equipo local. Se utiliza para mostrar el estado actual de las conexiones y verificar si los puertos que utilizan están abiertos o cerrados.

`nslookup`: Comprueba registros, alias y servicios de hosts de dominio, haciendo consultas a servidores DNS.

`ping`: Comprueba y diagnostica la existencia de conexión entre nuestro equipo y una dirección IP remota.

`route`: Muestra o modifica la tabla de enrutamiento.

`tracert`: Muestra todas las direcciones IP intermedias por las que pasa un paquete entre el equipo local y la dirección IP especificada. Este comando es útil si el comando ping no da respuesta, para establecer cual es el grado de debilidad de la conexión.

Cada uno de los enlaces de esta relación te lleva a la página correspondiente en la se trata específicamente de cada uno de los comandos básicos de TCP/IP. En el último se puede ver la relación completa de utilidades TCP/IP: conectividad, de diagnóstico y de servidor, empleadas por Microsoft.

Comando	Descripción	Sintaxis
arp	Muestra y modifica entradas en la caché de Protocolo de resolución de direcciones (ARP), que contiene una o varias tablas utilizadas para almacenar direcciones IP y sus direcciones físicas Ethernet o Token Ring resueltas. Existe una tabla independiente para cada adaptador de red Ethernet o Token Ring instalados en el equipo. Si no se utilizan parámetros, el comando **arp** muestra Ayuda.	**arp**[**-a** [direcciónDeInternet] [**-N**direcciónDeInterfaz]] [**-g** [direcciónDeInternet] [**-N**direcciónDeInterfaz]] [**-d**direcciónDeInternet [direcciónDeInterfaz]] [**-s**direcciónDeInternet direcciónEthernet [direcciónDeInterfaz]]
hostname.	Muestra la parte correspondiente al nombre de host del nombre completo del equipo.	hostname
ipconfig.	Muestra los valores actuales de la configuración de la red TCP/IP y actualiza la configuración de DHCP (Protocolo de configuración dinámica de host) y DNS (Sistema de nombres de dominio). Si se utiliza sin parámetros, **ipconfig** muestra las direcciones IPv6 o la dirección IPv4, la máscara de subred y la puerta de enlace predeterminada de todos los adaptadores.	**ipconfig** [**/all**] [**/renew**[*adaptador*]] [**/release** [*adaptador*]] [**/flushdns**] [**/displaydns**] [**/registerdns**] [**/showclassid***adaptador*] [**/setclassid***adaptador*[*idDeClase*]]
nbtstat.	Muestra estadísticas del protocolo NetBIOS sobre TCP/IP (NetBT), las tablas de nombres NetBIOS para el equipo local y el remoto, y la caché de nombres NetBIOS. **Nbtstat** permite actualizar la caché de nombres NetBIOS y los nombres registrados con el servicio WINS. Cuando se usa sin parámetros, **nbtstat**muestra ayuda.	**nbtstat**[**-a***nombreRemoto*] [**-A***direcciónIP*] [**-c**] [**-n**] [**-r**] [**-R**] [**-RR**] [**-s**] [**-S**] [*intervalo*]
nslookup.	Muestra información que puede usar para diagnosticar la infraestructura de DNS (Sistema de nombres de dominio). Para utilizar esta herramienta, debería familiarizarse con el funcionamiento de DNS. El comando Nslookup sólo está disponible si se ha instalado el protocolo TCP/IP.	**nslookup** [-subComando...] [{equipoBuscado | -servidor}]
ping.	Comprueba la conectividad de nivel IP en otro equipo TCP/IP al enviar mensajes de solicitud de eco de ICMP (Protocolo de mensajes de control Internet). Se muestra la recepción de los mensajes de solicitud de eco correspondientes, junto con sus tiempos de ida y vuelta. Ping es el principal comando de TCP/IP que se utiliza para solucionar problemas de conectividad, accesibilidad y resolución de nombres. Cuando se usa sin parámetros, **ping** muestra ayuda.	**ping**[**-t**] [**-a**] [**-n**recuento] [**-l** tamaño] [**-f**] [**-i**TTL] [**-v**TOS] [**-r**recuento] [**-s**recuento] [{**-j**listaHost | **-k** listaHost}] [**-w**tiempoDeEspera] [**-R**] [**-S**direcciónDeOrigen] [**-4**] [**-6**] nombreDeDestino
route.	Muestra y modifica las entradas de la tabla de rutas IP local. Si se utiliza sin parámetros, **route** muestra su Ayuda.	**route** [**-f**] [**-p**] [commando [destino] [**mask** máscaraDeSubred]

		`[puertaDeEnlace] [metric métrica]] [if intefaz]]`
tracert.	Determina la ruta tomada hacia un destino mediante el envío de mensajes ICMPv6 o de petición de eco del Protocolo de mensajes de control de Internet (ICMP) al destino con valores de campo de tiempo de vida (TTL, Time to Live) que crecen de forma gradual. La ruta mostrada es la lista de interfaces de enrutador casi al lado de los enrutadores en la ruta entre el host de origen y un destino. La interfaz casi al lado es la interfaz del enrutador que se encuentra más cercano al host emisor en la ruta. Cuando se utiliza sin parámetros, el comando **tracert** muestra Ayuda.	`tracert [-d] [-hnúmeroMáximoDeSaltos] [-jlistaHost] [-wtiempoDeEspera] [-R] [-SdirecciónDeOrigen] [-4] [-6] nombreDeDestino`
Relación de comando y utilidades TCP/IP.		http://technet.microsoft.com/es-es/library/cc781020(WS.10).aspx

Página de Microsoft con un tutorial diseñado para ayudar a identificar y resolver problemas de conexión de red en Windows.
http://windows.microsoft.com/es-ES/windows/help/network-connection-problems-in-windows?T1=tab03

¿En cuál de las siguientes líneas aparecen comandos que no están relacionados con el protocolo TCP/IP?

- [x] **IPCONFIG, PING, FIND.**
- [ ] NETSTAT, NDTSTAT.
- [ ] TRACERT, ROUTE, NSLOOKUP.
- [x] **HOSTNAME, SSIDNAME, ARP.**

1.10.- Conexiones remotas: Telnet, SSH, VNC, VPN.

Conexión a Escritorio Remoto es una utilidad de los sistemas operativos Windows con la que desde un equipo en local, que ejecute Windows, se puede acceder, mediante una conexión de red, a otro equipo, el remoto, que también ejecute Windows, con el propósito de manejarlo a distancia, ya que desde el primero se puede acceder a las aplicaciones y a los datos almacenados en el segundo prácticamente como si estuvieras sentado frente a él. Esto, siempre que el ordenador local tenga los permisos adecuados para poder conectarse al remoto, que previamente debe haber habilitando la Conexión a Escritorio Remoto para permitir el acceso.

Así por ejemplo, desde un equipo en casa se puede conectar al equipo del trabajo, y se pueden usar todos sus programas, archivos y recursos de red como si se estuviese sentado frente al equipo en la oficina. Se puede ejecutar, como si estuviera instalado en el ordenador de casa, el procesador de texto que está instalado en el equipo remoto.

Una forma rápida de iniciar la Conexión a Escritorio remoto, es tecleando mstsc en el cuadro de búsqueda del menú de Inicio. Aunque también se puede ejecutar mediante el acceso directo **Conexión a Escritorio remoto**, al que se llega haciendo clic en el botón Inicio, después en Todos los programas o Programas y por último en Accesorios.

En los siguientes enlaces se puede consultar la forma de utilizar las conexiones remotas:

http://windows.microsoft.com/es-ES/windows7/Connect-to-another-computer-using-Remote-Desktop-Connection
http://windows.microsoft.com/es-ES/windows-vista/Connect-to-another-computer-using-Remote-Desktop-Web-Connection

Otras formas de conexión directa entre dos equipos pueden hacerse a través de `Telnet`, `SSH`, `VPN`, o `VNC`:

Telnet es el nombre de un protocolo de TCP/IP y a la vez, el nombre de un programa que permite acceder en modo Terminal (en modo texto, sin gráficos), mediante una red, a un equipo remoto a través de dicho protocolo, para manejarlo como si se estuviera frente a él. Para ello es necesario que en el equipo al que se acceda tenga instalado un programa especial, el servidor de Telnet, que reciba y gestione las conexiones. Ha dejado de utilizarse por no considerarse un protocolo seguro, ya que en las conexiones se envían los datos en texto plano, es decir sin codificar, y pueden ser espiadas con facilidad, así que hoy día se suele utilizar su variante segura: SSH. (Secure SHell, en ingles o intérprete de órdenes segura en español).

SSH tiene la misma funcionalidad que **telnet**, e igualmente es el nombre de un protocolo y de un programa, pero se le han añadido: el cifrado de las conexiones para evitar que los datos sean interceptados, la autentificación mediante llave pública, para asegurarse, por si acaso, que el equipo remoto es realmente quién dice ser. Además puede emplear mecanismos de autenticación más seguros para los usuarios que se conectan.

VNC (*Visual Network Control*) es una herramienta que permite controlar equipos conectados a una red de forma remota como si estuviéramos delante de ellos. Para ello es necesario instalar un programa llamado servidor VNC en cada uno de los equipos que se quieren controlar, y un programa llamado cliente o visualizador VNC en la máquina desde la que se va a llevar el control. En cuanto se establece la comunicación, el equipo cliente puede utilizar el equipo servidor, sin limitación alguna, salvo la impuesta por el ancho de banda de la red, ya que puede ver en su pantalla, el escritorio del equipo remoto, y acceder a todos sus programas mediante el teclado y ratón propios para manejarlo a distancia.

Por su parte, las **VPN** o redes privadas virtuales también son conexiones punto a punto a través de una red privada o pública, como Internet, que utilizan protocolos especiales llamados de túnel basados en TCP/IP, para realizar llamadas virtuales a un puerto virtual en un servidor VPN.

Para emular un vínculo punto a punto, los datos se encapsulan, o se ajustan, con un encabezado. El encabezado proporciona la información de enrutamiento que permite a los datos recorrer la red compartida o pública hasta alcanzar su extremo. Para emular un vínculo privado, los datos enviados se cifran por motivos de confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar sin las claves de cifrado. El vínculo en el que los datos privados están encapsulados y cifrados se denomina conexión VPN.

Páginas para investigar cuestiones acerca de otras formas de conexión directa entre dos equipos.
http://windows.microsoft.com/es-ES/windows7/Telnet-frequently-asked-questions
http://www.aemilius.net/soporte/manuales/acceso-ssh-ssl-secure-shell-telnet-PuTTY.html
http://es.wikipedia.org/wiki/VNC
http://es.wikipedia.org/wiki/Red_privada_virtual

Señala la respuesta que sea completamente correcta. Las conexiones remotas se pueden hacer mediante:

- Telnet, SSIP, VNC.
- **Telnet, VPN, VNC.**
- SSH, VCN, VNP.
- Telnet, TSEMS, VNC.

2.- Administración de recursos compartidos en red.

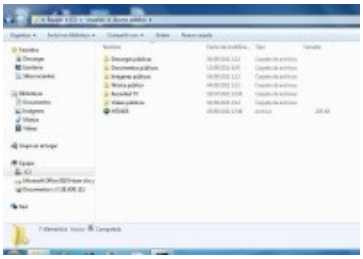
Caso práctico

Un tema que le preocupa a Juan es cómo compartir a través de la red los recursos de equipos conectados.

Porque poner todo a disposición de todos, que sería lo más fácil, puede suponer problemas de seguridad en la red y una mala gestión de los recursos. Así que será necesario, establecer una política de gestión de permisos en torno a los recursos compartidos.

En cuanto a la configuración que Windows hace en el equipo para acceder a la red, se pregunta:

- ¿Cuánta libertad tienen los otros usuarios en otros equipos de la red para llegar a mi ordenador y tomar lo que necesiten?
- ¿Qué se ha quedado a la vista de los demás para que puedan utilizarlo?
- ¿Qué puedo yo utilizar de los equipos de los demás?



Cuando hablamos de recursos compartidos en red estamos tratando de carpetas, de ficheros y de dispositivos que se hayan en un equipo, pero que de alguna manera, se ponen a disposición de todos aquellos que se conectan a él a través de una red, o sólo a disposición de algunos de ellos dependiendo de la forma de compartirlos. Y todo ello haciéndose extensivo a cada uno de los equipos que forman parte de dicha red.

Para hacer que un recurso sea compartido hay que ponerlo accesible a través la red, y una vez que esta compartido, los usuarios, con los permisos adecuados, podrán acceder a su contenido ya sean aplicaciones o datos, o utilizarlo remotamente si se trata de un dispositivo, tal como una impresora.

En un entorno de red es preciso definir permisos de acceso y privilegios de uso sobre los recursos que se comparten, para mantener cierto nivel de seguridad y asegurar que lo compartido sólo pueda ser utilizado por quien tenga derecho, y bajo las condiciones de uso fijadas sobre el recurso, mientras que se bloquea el acceso a usuarios no autorizados.

En Windows 7 la seguridad de acceso a carpetas y ficheros compartidos se determina por:

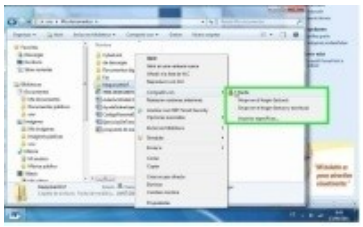
- Los sistemas de asignación de **Permisos de acceso,** propios de los sistemas de ficheros NTFS, con los que se puede controlar de forma individual o por grupos, quienes y en qué condiciones, pueden acceder a carpetas y ficheros.
- La configuración de los **Permisos de recursos compartidos** del equipo, que establecen la forma en que se comparten los recursos y que permiten el acceso en modo Sólo lectura, o en modo Lectura/Escritura.

Cuando se pertenece a una red, con Windows 7, es posible compartir archivos e impresoras con otros miembros de la red. Pero para compartir es preciso tener activada la **Detección de redes** necesaria para encontrar otros equipos y dispositivos en la red y para que ellos te localicen a ti. Y también es preciso tener activado el **uso compartido de archivos e impresoras**.

Respecto a Windows 7: ¿Cuales de las siguientes afirmaciones son ciertas?

- [ ] Cualquier fichero o recurso que se comparta puede ser utilizado sin limitación por cualquier usuario de cualquier red.
- [ ] Si se activa el uso compartido de archivos e impresoras no es necesario tener en cuenta los permisos de los ficheros.
- [x] **Los permisos de recursos compartidos se complementan con los permisos de los ficheros para mantener la seguridad del acceso a los recursos de la red.**
- [x] **Para compartir en red es necesario tener activada la detección de redes.**

2.1.- Controles de acceso a los recursos: ficheros, carpetas y dispositivos.



En Windows 7 no solo se decide quién puede ver un recurso, sino también qué pueden hacer con él los que tengan acceso.

Windows 7 utiliza dos modelos distintos para compartir recursos: el estándar y el de carpeta pública.

El modelo Estándar permite compartir los recursos del equipo; carpetas y ficheros, desde su propia ubicación y controlar quién y con qué nivel se puede acceder a ellos. No hay necesidad de moverlos de su sitio para compartirlos. Para compartir según este modelo estándar se tiene la opción de **Compartir con,** que esta accesible al abrir cualquier carpeta con el explorador de Windows o desde el menú contextual propio de cada fichero o de cada carpeta. (o de cada impresora).

El menú Compartir con proporciona opciones para compartir un recurso de forma rápida y sencilla, opciones que no son siempre las mismas, porque dependen del recurso en sí y del tipo de red a la que se este conectado. Esto último es debido a que Windows 7 aplica al equipo una configuración diferente en función de que esté como miembro de un grupo domestico, de un grupo de trabajo o de un dominio.

En un grupo en el hogar los usuarios tienen la opción de compartir con cualquiera del mismo grupo.

En un grupo de trabajo o dominio, los usuarios tienen la opción de compartir con usuarios específicos.

En cualquier caso, también se tiene la opción **Nadie** para no compartir.
Las opciones más comunes del menú **Compartir con** son:

- ✓ **Nadie.** Para hacer que el elemento sea privado, y nadie tenga acceso a él.
- ✓ **Grupo en el hogar (lectura).** El elemento se pone disponible en modo lectura para los miembros del grupo hogar pero no lo podrán modificar ni borrar.
- ✓ **Grupo en el hogar (lectura y escritura).** Hace que el elemento esté disponible con permisos de lectura y escritura para los miembros del grupo en el hogar, así que pueden leerlo, modificarlo o eliminarlo.
- ✓ **Usuarios específicos.** Para abrir el asistente de Uso compartido de archivos con el cual poder elegir usuarios específicos con los que compartir el recurso. Si hay que cambiar el permiso de sólo lectura que se asigna de forma predeterminada hay que pulsar sobre el usuario o grupo y seleccionar un nuevo permiso.
- ✓ **Configuración de uso compartido avanzado.** Es una opción alternativa de este menú que se muestra cuando el elemento no esta accesible directamente para compartir. Es el caso de ciertos ficheros y carpetas: como la carpeta que corresponda a una unidad completa, y especialmente si corresponde a la carpeta raíz del sistema, o el caso de las carpetas de los usuarios o de las carpetas del propio sistema operativo. Se podrá utilizar esta opción cuando sea absolutamente imprescindible compartir alguna de estas ubicaciones, pero como norma general no se recomienda compartir toda la unidad ni las carpetas del sistema de Windows.

El modelo de Carpeta Pública que permite compartir el contenido de ciertas carpetas predeterminadas como públicas. Cuando se quiere compartir algo, se copia o mueve a una de las carpetas públicas de Windows 7, como por ejemplo a Música pública, Imágenes públicas o Videos públicos, dejándolo disponible para otros usuarios del equipo y de la red con los mismos permisos que tiene la propia carpeta, ya que al copiarse se ajustan sus permisos a los de su carpeta contenedora. La carpeta pública puede verse como un contenedor al que todo usuario puede llegar y lo que se ponga en ella puede ser utilizado libremente, o en todo caso en función de los permisos de

acceso con que esté configurada. Se pueden localizar estas carpetas formando parte de las bibliotecas de cada usuario.

El uso compartido de las carpetas de Acceso público está activado de forma predeterminada para un grupo en el hogar y desactivado para su uso en otras redes. Mientras está activado, cualquier usuario que esté en su equipo o red puede tener acceso a las carpetas públicas, pero cuando está desactivado, solo podrán tener acceso los usuarios que tengan cuenta de usuario y con contraseña en el equipo.

Se puede comprobar que es lo que se está compartiendo desde el panel de detalles del Explorador de Windows 7. Sólo hay que hacer clic sobre un archivo o sobre una carpeta para que en el panel de detalles que aparece en la parte inferior de la ventana se vea si está compartido, o no, y con quién. También se ve lo que otros me aportan.

Para utilizar impresoras o unidades de disco como recursos de una red, hay que definirlos uno por uno como recurso compartido, proporcionarles un nombre para que sean reconocidos en la red y asignarles un nivel de acceso. Esto se hace fácilmente a partir de la opción **compartir como** del menú contextual que se muestra al pulsar el dispositivo con el botón derecho.

Página de Microsoft que explica las distintas formas de compartir archivos utilizando Windows 7.
http://windows.microsoft.com/es-ES/windows7/Share-files-with-someone

¿Qué modelos utiliza Windows 7 para compartir los recursos?

- [x] **Modelo estándar.**
- [ ] Modelo de recurso público.
- [x] **Modelo de carpeta pública.**
- [ ] Modelo de asignación directa recurso-usuario.

2.2.- Configuración de permisos.

Windows 7 gestiona de forma independiente las conexiones de los distintos tipos de red porque permite que se puedan configurar perfiles particulares e independientes, para cada tipo de conexión.

De esta forma se pueden aplicar características distintas a cada perfil, para que tengan comportamientos adecuados y ajustados a las necesidades de cada conexión. Y así diferenciar las conexiones públicas de las conexiones privadas.

Se puede configurar un perfil de red ajustado a una red en el hogar o para el trabajo, compartiendo recursos entre sus miembros, con conexiones, o una red pública según nuestras necesidades. Para hacerlo, hemos de ir a **Centro de redes y recursos compartidos** y seleccionar la opción **Cambiar configuración de uso compartido avanzado** del panel izquierdo. Para ajustar las características de configuración de cada perfil de red podemos cambiar el estado de las siguientes opciones:

La primera es: Detección de redes.
Es imprescindible tener esta opción activada en un equipo para hacerlo visible en la red y para ver al resto de equipos que la forman. Esta opción se activa por defecto cuando conectamos a una red Privada, y se desactiva al conectar a una red Pública.

La segunda es: Compartir archivos e impresoras.

Esta opción debe activarse si queramos que los otros equipos de la red puedan acceder a los recursos que hemos compartido. Si esta desactivada, aunque los otros equipos puedan vernos, no podremos compartir nada con ellos.

La tercera es: Uso compartido de la carpeta pública.

Cuando esta opción está activada, cualquier usuario que tenga acceso al equipo tiene acceso a las carpetas públicas. Pero cuando está desactivada se les niega el acceso a dichas carpetas. La carpeta de Acceso público puede estar activada y permitir el acceso a los usuarios de la red con independencia de que el **Uso compartido de archivos e impresoras** este desactivado.

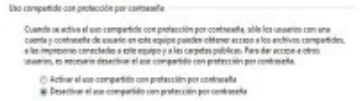
La cuarta es: Transmisión por secuencias de multimedia.

Esta opción permite poner a disposición de los usuarios de la red los contenidos multimedia que hayan sido compartidos. Al pulsar **Elegir opciones de transmisión por secuencias de multimedia**… se activa el servicio o puede modificase si ya esta activado. Se puede decidir qué equipos pueden acceder a la transmisión y personalizar en función de la clasificación del fichero. Estas transmisiones puede ralentizar la velocidad de la red.

La quinta es: Conexiones de uso compartido de archivos.

Con esta opción se puede seleccionar el tipo de cifrado a utilizar en las conexiones de uso compartido de archivos.

La sexta es: Uso compartido con protección por contraseña.



Si esta activado el uso compartido con protección por contraseña, sólo los usuarios que tengan cuenta con contraseña en el equipo podrán acceder a las carpetas compartidas y a los recursos del equipo, ya sean usuarios locales o de red. Así que para compartir con un usuario de otro equipo será necesario que tenga una cuenta en nuestro equipo, o tendremos que desactivar la opción para que cualquier usuario de la red pueda acceder a nuestras carpetas y recursos disponibles.

La séptima es: Conexiones de grupo hogar.

Esta opción sólo está disponible para el perfil de red de casa o trabajo. Activaremos la primera opción cuando queramos que Windows se encargue de gestionar el acceso mediante contraseña entre equipos de una red en el hogar que tenga usuarios comunes en distintos equipos. Si activamos la segunda opción, se solicitará identificación cada vez que se acceda de un equipo a otro.

Si en cualquier momento tiene problemas para compartir, puede usar el **Solucionador de problemas de carpetas compartidas** para buscar e intentar corregir automáticamente algunos de los problemas más comunes.

¿Cuáles de las siguientes opciones pertenecen a: Cambiar configuración de uso compartido avanzado?

- ☐ Transmisión por secuencias de multiplataforma.
- ☑ **Uso compartido con protección por contraseña.**

- ☐ Detección del uso compartido en redes públicas.
- ☑ **Conexiones de grupo hogar.**

3.- Servicios en red.

Caso práctico

__María__ se dispone a montar una plataforma web para unos clientes de BK Programación. Sabe que a __Carlos__ le interesa el tema de los servicios de Internet, por lo que le incorpora al proyecto para trabajar conjuntamente y que aprenda sobre ello. Durante las primeras reuniones para coordinar las tareas a __Carlos__ le surgen ciertas dudas:
—¿En qué consiste la arquitectura cliente-servidor?
—Si hay varios servicios funcionando o recursos a compartir en un equipo, ¿cómo podemos hacerlos accesibles a otros ordenadores?
—¿La información de cada servicio viaja por canales independientes? ¿Qué tipos de servidores existen? ¿Qué diferencia hay entre un servidor de aplicaciones y un servidor web? ¿Y entre un servidor de ficheros y un servidor FTP?
__María__ decide explicarle detenidamente cada una de sus preguntas. __Carlos__ escucha con atención y toma nota de los conceptos clave.

Los servicios en red son importantes en toda infraestructura de red, ya que gracias a ellos los diferentes ordenadores puedes comunicarse, y el sistema informático es más potente.

Dentro de los servicios de red verás cómo gestionarlos y qué puertos están relacionados con los mismos. Posteriormente estudiaras la configuración y gestión básica de algunos servidores importantes, tales como los servidores de archivos, de impresión y de aplicaciones. Para finalmente mostrarte cómo controlar estos servicios.

3.1.- Gestión de servicios y puertos.

En la anterior unidad ya introdujimos los servicios y cómo se accedía a ellos. Los servicios son procesos, programas en ejecución, que suelen ejecutarse de forma transparente al usuario. Muchos se activan ante determinados eventos o condiciones del sistema, por ejemplo, de forma automática al inicio del sistema operativo, tras una petición del usuario, en función del rendimiento del equipo, del tráfico de la red, etc. En este apartado nos centraremos en los servicios de red.

Existen muchos servicios relacionados con el funcionamiento de la red y sus aplicaciones, tales como, servicios de control remoto, cortafuegos, antivirus, servidores web, de FTP, P2P… Además, todos los sistemas conectados en una red (y estos entre sí, en Internet) tienen una dirección IP que los identifica, ya sean crdenadores cliente o servidores.

Aparte, cada sistema operativo posee unos **puertos lógicos**. Esto significa que, al contrario que los puertos físicos (USB, Firewire, DVI, HDMI, etc.) sólo existen virtualmente para el ordenador. Los sistemas operativos cuentan con más de 65.000 **puertos virtuales** disponibles para abrir conexiones, y se las ceden a los programas para que vuelquen sus datos en la red. Los programas los solicitan y el sistema operativo los gestiona para poder utilizarlos y establecer una **conexión lógica**. Esto permite que puedan comunicarse con otro ordenador "punto a punto". Finalmente, toda comunicación entre dos dispositivos en Internet se traduce en un flujo de datos entre dos puertos virtuales abiertos por alguna aplicación.

Teniendo en cuenta lo anterior, tenemos que una **comunicación en Internet**, se establece entre una parte **cliente** y una **servidora**.

Los programas que **comienzan la comunicación** en un puerto se llaman **clientes** y los programas que están siempre usando un puerto **esperando que los clientes se conecten** a él, se llaman**servidores**. Por ejemplo, una página web, está siempre esperando que un cliente (el navegador) se conecte para mostrarle su contenido. El servidor web suele utilizar permanentemente el puerto 80 para esperar conexiones entrantes y los navegadores suelen usar (solo mientras lo necesitan) un puerto cualquiera de los 65.000 para establecer el flujo de comunicación. El hecho de que se utilice el puerto

80 para ofrecer páginas web es una convención histórica, pero en realidad podría utilizarse cualquier otro. Para enviar y recibir correo, por ejemplo, se utiliza el 25.

Ya hemos comentado que existen miles de puertos (codificados con 16 bits, es decir, se cuenta con 65536 posibles puertos). Es por ello que la **IANA** (Internet Assigned Numbers Authority, Agencia de Asignación de Números de Internet) desarrolló una aplicación estándar para ayudar con las configuraciones de red.

- ✓ Los puertos del **0 al 1023** son los **puertos conocidos** o reservados. En términos generales, están reservados para procesos del sistema (daemons) o programas ejecutados por usuarios privilegiados. Sin embargo, un administrador de red puede conectar servicios con puertos de su elección.
- ✓ Los puertos del **1024 al 49151** son los **puertos registrados**.
- ✓ Los puertos del **49152 al 65535** son los **puertos dinámicos y/o privados**.

A continuación, se indican algunos de los puertos conocidos más utilizados:

Puertos conocidos asociados a servicios o aplicaciones	
Puerto	**Servicio o aplicación**
21 (control), 20 (datos)	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
119	NNTP

Por lo tanto, un servidor (un equipo conectado que ofrece servicios como FTP, Telnet, etc.) cuenta con números de puertos fijos a los cuales el administrador de red conecta los servicios. Los puertos del servidor generalmente se encuentran entre 0 y 1023 (rango de valores relacionado con servicios conocidos).
Del lado del cliente, el sistema operativo elige el puerto entre aquéllos que están disponibles de forma aleatoria. Por lo que, los puertos del cliente nunca incluirán los puertos que se encuentran entre 0 y 1023, ya que este rango de valores representa a los *puertos conocidos*.

Conoce más puertos asignados a otros conocidos servicios de red.
http://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_puerto

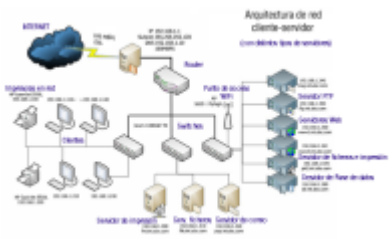
¿A qué puerto está asociado el servicio de IMAP?

- ○ 119
- ○ 110
- ◉ **143**
- ○ 210

¿Qué puerto tiene asociado el servicio de DNS?

- ◉ **53**
- ○ 110
- ○ 43
- ○ 119

3.2.- Configuración y gestión básica de servidores.



La **arquitectura cliente-servidor** es un modelo de aplicación distribuida en el que las tareas se repart en entre los proveedores de recursos o servicios, conocidos como servidores, y los solicitantes de estos, que son los clientes. Un cliente realiza peticiones a otro programa, el servidor, que atiende dichas peticiones dando respuesta. Esta idea también se puede aplicar a programas que se ejecutan sobre un solo equipo, aunque es más ventajosa en un sistema operativo multiusuario en red.

La capacidad de procesamiento se encuentra repartida entre los clientes y los servidores. Sin embargo, la organización de los recursos o servicios y el establecimiento de responsabilidades tienen, habitualmente, una administración centralizada en el equipo servidor, lo que facilita y clarifica el diseño y funcionamiento de la arquitectura.

La separación entre cliente y servidor es una separación de tipo lógico, donde el servidor no se ejecuta necesariamente sobre una sola máquina, ni es necesariamente un sólo programa. Existen distintos tipos específicos de servidores, entre los que se incluyen los servidores web, los servidores de archivos, los servidores FTP, de impresión, correo, etc. Mientras que sus propósitos varían de unos servicios a otros, la arquitectura básica seguirá siendo la misma.

Si aplicamos la idea de la arquitectura cliente-servidor al campo de las redes, nos encontramos que una red cliente-servidor es aquella red de comunicaciones en la que todos los clientes están conectados a un servidor. En el servidor se centralizan los diversos recursos y aplicaciones existentes; además, el servidor se encarga de tenerlos disponibles para los clientes, cada vez que estos los solicitan.

3.2.1.- Servidores de ficheros y FTP.

Las redes de ordenadores se idearon para el intercambio de información y la compartición de ficheros. En ocasiones necesitamos mover archivos con cierto volumen de tamaño y no resulta operativo hacerlo mediante correo electrónico. Para estos casos, se puede emplear un servicio de Internet dedicado a la transferencia de ficheros entre equipos a través de la red.

Tenemos dos opciones, a través de un servidor de archivos, o mediante el uso de un servidor FTP.

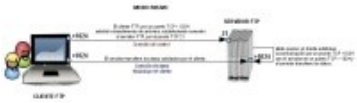
Un **servidor de archivos** o ficheros nos permite compartir recursos, habitualmente, dentro de una misma red local. Se establecen una serie de recursos compartidos, usuarios autorizados, y unos permisos para cada usuario o grupo sobre los recursos compartidos. Recuerda que ya vimos en el apartado “Administración de recursos compartidos en red” cómo compartir información en Windows7.

Por otro lado, un **servidor FTP** utiliza el Protocolo de Transferencia de Ficheros (FTP). El servicio FTP permite conectarse a un equipo (el servidor FTP) y transferir ficheros desde éste hacia el equipo del cliente (cliente FTP) y en sentido inverso. El protocolo FTP establece una doble conexión TCP entre el cliente y el servidor:

- ✓ **Conexión de control:** suele emplearse el puerto **21** del servidor y sirve para indicarle a éste las operaciones que se quieren llevar a cabo.
- ✓ **Conexión de datos:** se usa normalmente el puerto **20** del servidor y es la que se sirve para la transferencia de ficheros hacia o desde el servidor. Existen dos modos de funcionamiento para este tipo de conexión:

- **Modo activo:** Es el utilizado por defecto. El cliente establece una conexión a través del puerto **20** para la transferencia de datos.

- **Modo pasivo:** Existe la posibilidad de que cliente y servidor negocien otro puerto distinto del **20** para la transferencia de datos. Este proceso de negociación se realiza por medio del puerto de control **21**. El servidor responderá al cliente con el número puerto, superior al **1024**, a través del cual atenderá la conexión de datos.



Para utilizar este servicio necesitas un cliente FTP (una serie de comandos o programa para establecer la conexión con el servidor FTP), que es el que establece la conexión con el programa servidor FTP situado en un equipo remoto. Cuando un cliente se conecta a un servidor FTP lo hará utilizando un usuario registrado, también existirá la posibilidad de conexión de usuarios anónimos, esto viene determinado por el tipo de autenticación del servidor FTP. Los permisos sobre los archivos del sitio FTP, lugar donde se almacenan los archivos del servidor FTP, podrán ser de lectura (los usuarios podrán descargarse archivos) y/o de escritura (los usuarios podrán subir archivos). Estos parámetros (el tipo de autenticación y los permisos) se establecerán durante la configuración del sitio FTP en el equipo servidor.

Las aplicaciones del servicio FTP son infinitas, desde universidades, empresas de diversa índole, alojamiento y gestión de los recursos de un sitio web, pasando por fabricantes de hardware que cuelgan sus controladores y manuales, hasta usuarios domésticos que montan sus propios servidores FTP para acceder desde cualquier lugar a sus archivos. Seguidamente, veremos en el recurso siguiente cómo crear un sitio web y configurarlo en Windows 7.

Instalación y configuración de un servidor FTP en Windows 7.

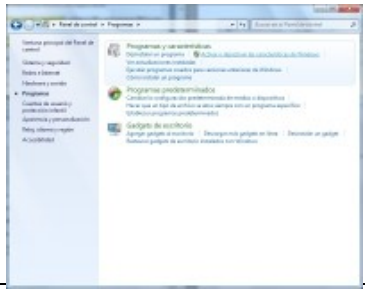
Los **servidores FTP se utilizan** para descargar y subir archivos a servidores remotos o locales y parar compartir archivos de una forma rápida y segura.

En este tutorial vamos a instalar y configurar el servidor FTP que viene con Windows 7. Crearemos un sitio FTP con nombre 'damsi' que exija autenticación a los usuarios y donde estos tengan permisos para bajar y subir archivos. Además, veremos cómo se conecta un cliente al servicio FTP.

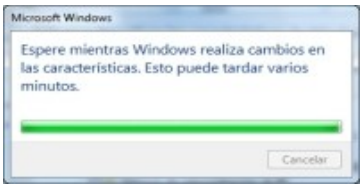
Con IIS 7 (Internet Information Server, servidor web de Microsoft) se pueden usar dos servidores FTP: FTP 7.0 y FTP 7.5, éste último es el que se incluye con Windows 7.

Instalar el servidor FTP de Windows no implica tener instalado el servidor web, pero si necesitamos tener instalado el Administrador de IIS para poder realizar las labores de configuración del sitio FTP.

Comenzaremos en el Panel de control de Windows, donde iremos a la opción `'Programas'` y desde ahí a `Activar/desactivar funcionalidades de Windows`.

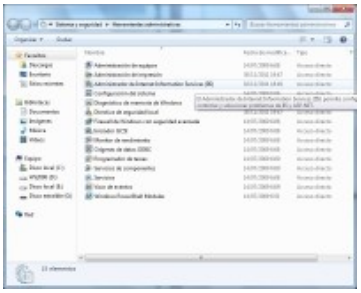


Marcamos las opciones de "`Consola de administración de IIS`" y de "`Servicio FTP`".



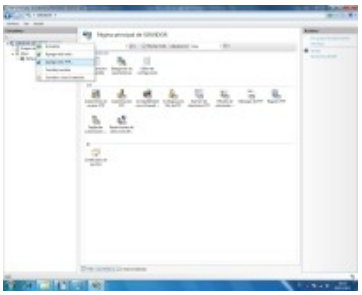
El sistema Windows aplicará los cambios en la configuración.

CONFIGURACIÓN DEL SERVICIO FTP



Para configurar el servicio FTP regresamos de nuevo al `Panel de control - Sistema y seguridad - Herramientas Administrativas` y hacemos clic sobre "`Administrador de Internet Information Server (IIS)`".

Desde esta herramienta crearemos nuestro sitio FTP. Para ello, seguiremos los siguientes pasos:



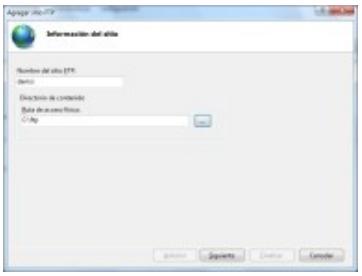
1. Nos situamos sobre el nombre del equipo, en nuestro caso SERVIDOR y haciendo clic con el botón derecho del ratón del menú contextual seleccionamos "`Agregar sitio FTP`".

Antes de comenzar a completar la **configuración del sitio FTP** definiremos los **campos** que nos aparecerán:

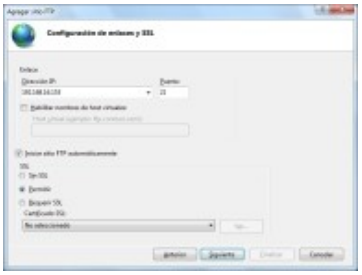
- ✓ **Ventana "Información del sitio"**:
  - ➔ **Nombre del sitio FTP**: introduciremos el nombre que tendrá el sitio FTP, puesto que podemos varios sitios, lo identificará unívocamente, por ejemplo "**damsi**".
  - ➔ **Ruta de acceso física**: introduciremos la unidad y carpeta del equipo con Microsoft Windows 7 donde alojaremos los ficheros del sitio FTP, en nuestro caso "`C:/ftp`".
- ✓ **A continuación, en la ventana "Configuración de enlaces y SSL":**
  - ➔ **Enlace - Dirección IP**: en este campo podremos indicar qué dirección IP se le asignará a este sitio FTP, ya que el equipo puede tener varias direcciones IP (varias interfaces de red). Por defecto quedará seleccionado "`Todas las no asignadas`". Si tenemos varios sitios FTP y queremos que sean accesibles desde fuera del equipo, podremos indicar qué dirección IP se le asignará a cada sitio FTP.
  - ➔ **Habilitar nombres de host virtuales**: si queremos tener varios sitios FTP en un equipo con una sola dirección IP y queremos que sean accesibles desde fuera del equipo (LAN o Internet) podremos marcar esta opción de "`Habilitar nombres de host virtuales`" e indicar el nombre del sitio ftp que queramos establecer, por ejemplo: `ftp.ajpdsoft.com`. Si queremos que este sitio FTP esté disponible en Internet, introduciremos en "`Host virtual`" el nombre de dominio del sitio igual que lo escribirían los usuarios en un explorador, por ejemplo, `ftp.damsi.com`. En el caso de este tutorial este campo lo dejaremos sin rellenar.
  - ➔ **Iniciar sitio FTP automáticamente**: marcaremos esta opción para que el servicio del sitio FTP se inicie automáticamente al arrancar el equipo.
  - ➔ **Sin SSL**: seleccionando esta opción de `Secure Sockets Layer` (Protocolo de Capa de Conexión Segura) desactivaremos este protocolo.
  - ➔ **Permitir**: con esta opción tendremos la posibilidad de conexión SSL o sin SSL.

➔ **Requerir SSL**: marcando esta opción sólo podremos conectarnos mediante SSL.

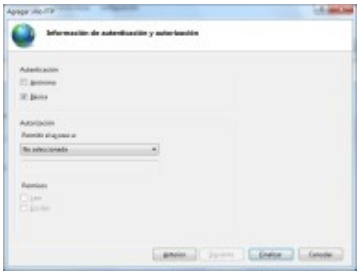
2. Una vez vistos los parámetros en detalle iniciamos la configuración del sitio FTP. La primera ventana nos pide nombre del sitio, '**damsi**', y el directorio físico a compartir donde estarán los archivos a descargar o donde se subirán. Esta carpeta debe tener los permisos necesarios para esta tarea. En nuestro caso hemos creado la carpeta en `C:\ftp`.



3. La siguiente ventana es la de Configuración de enlaces y SSL. Pide la dirección IP de la máquina que tiene el servicio (`192.168.16.153`) y puerto (por defecto el **21**). Podremos indicar la existencia de sitios FTP virtuales y especificar si se usa SSL o no (para cifrado de comunicaciones). Recomendamos la opción de "`Permitir SSL`". En este caso dejaremos las opciones como aparecen en la pantalla siguiente:

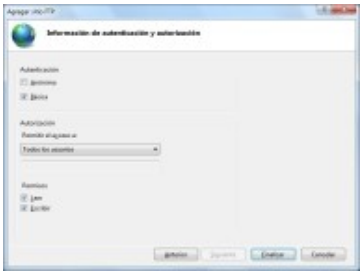


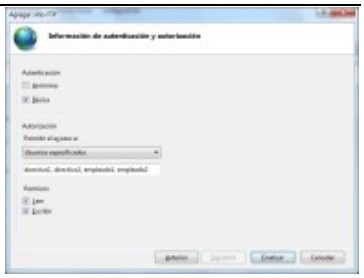
4. En la siguiente ventana sobre "`Información de autenticación y autorización`" especificamos el tipo de Autenticación y autorización que queremos. Veamos en qué opciones tenemos:
   a. **Autenticación anónima**: es un método de autenticación integrado que permite a los usuarios el acceso a cualquier contenido público proporcionando un nombre de usuario anónimo y una contraseña. De forma predeterminada, la autenticación anónima está deshabilitada. Esta autenticación se usará sólo cuando se desee que todos los clientes que visiten el sitio FTP puedan ver su contenido.
   b. **Autenticación básica**: es un método de autenticación integrado que requiere que los usuarios proporcionen un nombre de usuario de Windows y una contraseña válidos para obtener acceso al contenido. La cuenta de usuario puede ser local en el servidor FTP o una cuenta de dominio. La autenticación básica transmite contraseñas no cifradas por la red. Sólo se debe utilizar la autenticación básica cuando se tenga la certeza de que la conexión entre el cliente y el servidor está protegida con SSL.
   c. **Autorización**: podremos indicar los usuarios del equipo Windows que tendrán permisos de acceso a la carpeta del sitio FTP:
      i. En "`Permitir el acceso a`" podremos indicar:
         1. **Todos los usuarios**: todos los usuarios del equipo tendrán los permisos indicados (lectura y/o escritura).
         2. **Usuarios anónimos**: cualquier usuario tendrá los permisos indicados.
         3. **Roles o grupos de usuarios especificados**: los grupos indicados tendrán los permisos de lectura y/o escritura.
         4. **Usuarios especificados**: los usuarios indicados tendrán los permisos de lectura y/o escritura.



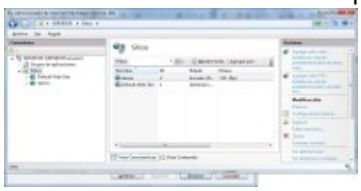
      ii. En "`Permisos`" indicaremos si queremos que los usuarios o grupos indicados puedan leer o escribir en la carpeta del sitio FTP.

5. Una vez vistas las opciones, seleccionamos `Autenticación Básica` y en `Autorización`, en el campo "`Permitir el acceso a`" indicaremos a los usuarios, grupos de usuarios que permitimos el acceso al sitio FTP. En este caso, seleccionamos `Todos` y les damos permisos de `Leer y Escribir`.



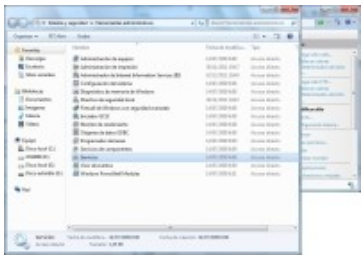


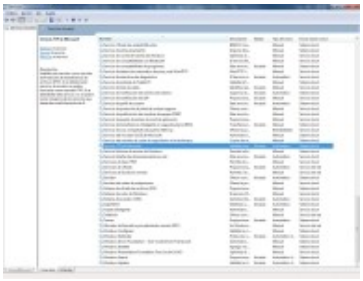
6. Depende de la situación, puede interesarnos restringir los permisos o el acceso a ciertos usuarios o grupos de usuarios, tal y como se muestra en la captura siguiente:



Con esto finalizamos la creación del sitio FTP que aparecerá en la parte central del Administrador de IIS:

Podemos comprobar que el servicio de FTP está activo en `Panel de control - Sistema y seguridad - Herramientas administrativas - Servicios`, localizamos el servicio FTP y vemos si se encuentra iniciado.

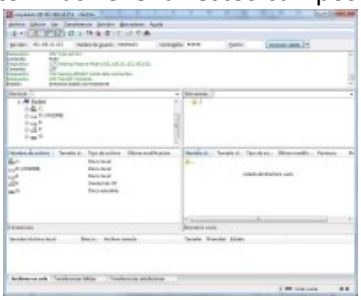




CONEXIÓN DE CLIENTES AL SERVICIO FTP

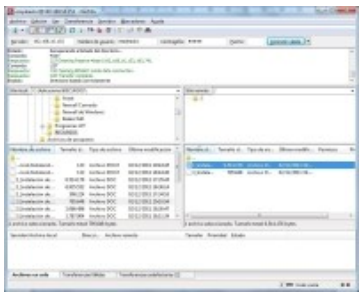
Para el cliente FTP utilizaremos una popular herramienta, **Filezilla Client**, es gratuita y podemos descargarla en:
http://filezilla-project.org/download.php

Una vez instalado Filezilla Client lo ejecutamos para iniciar una conexión con nuestro sitio FTP. En los campos "`Servidor`" indicaremos la dirección IP o nombre DNS del servidor FTP, en "`Nombre de usuario`" uno de los usuarios con acceso al sitio FTP, su contraseña y el puerto lo dejamos sin rellenar a no ser que hayamos especificado uno distinto al que viene por defecto. Tras rellenar estos campos pulsamos el botón "`Conexión rápida`" para iniciar la conexión.

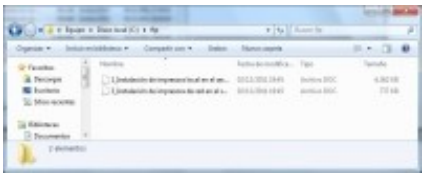


Comprobaremos en el recuadro de la parte inferior los mensajes que indican si la conexión se ha establecido correctamente. En caso de que no sea así, podemos fijarnos en el mensaje de error para averiguar dónde está el problema.

En el recuadro de "`Sitio remoto`" (parte central a la derecha) vemos los archivos compartidos del sitio FTP (en esta pantalla anterior está vacío). Por lo que el usuario "**empleado1**" se dispone a subir dos archivos. Los archivos se localizan a través del recuadro central izquierdo donde aparecen las unidades del equipo local del cliente.



El usuario simplemente seleccionará y arrastrará los archivos de su ubicación local a la remota en el servidor FTP para su transferencia. En este ejemplo ha seleccionado dos archivos `.doc`.



Una vez subidos al sitio FTP, en el equipo servidor FTP comprobamos que dentro de la ruta `C:\ftp` se encuentran los archivos que acaba de subir el usuario.

¿Qué tipo de autenticación permite el servidor FTP configurado bajo Windows 7?

- Básica y Avanzada.
- **Básica y Anónima.**
- Anónima y Avanzada.
- Ninguna de las anteriores.

3.2.2.- Servidores de impresión.

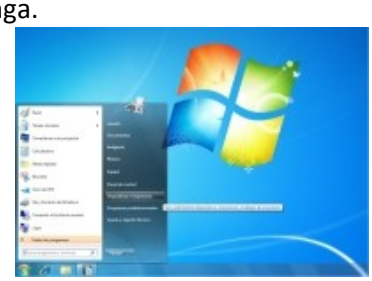
Los servicios de impresión nos permiten la impresión de trabajos en impresoras compartidas o conectadas en red.

Cuando hablamos de impresoras, distinguiremos entre el dispositivo de impresión físico (el hardware), que proporciona la impresión, y la impresora lógica, que es el modo en que esa impresora es reconocida por el sistema operativo que estemos utilizando, de modo tal que podríamos tener varias impresoras lógicas sobre una misma impresora física. Cuando se inicia un trabajo de impresión, éste se coloca en la cola de la impresora lógica antes de enviarlo a la impresora real. Esto puede sernos útil para, por ejemplo, establecer colas de impresión con diferentes prioridades por grupos de usuarios.

Explicaremos dos formas distintas de compartir impresoras en Windows 7 para que puedan ser utilizadas por los equipos clientes de una red:

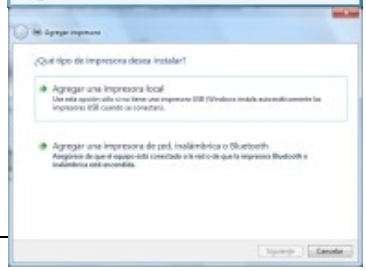
Conectar e instalar localmente una impresora en un equipo servidor con Windows 7 y compartirla.

Vamos a ver como agregar una impresora que esté conectada físicamente a nuestro equipo servidor con Windows 7, de modo que una vez instalada los clientes de nuestra red puedan hacer uso de ella para imprimir. Para ello, nos ayudaremos de una impresora de marca y modelo concreta, pero los pasos serán similares para cualquier otra impresora de la que se disponga.

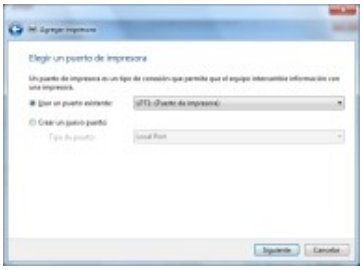


En primer lugar, conectaremos físicamente la impresora al puerto **LPT1** (o al **USB**) del equipo que actuará como servidor (el que más tarde compartirá la impresora), y encenderemos dicho periférico. Después en Windows 7 pulsaremos sobre el botón "`Inicio`" y posteriormente seleccionamos la opción "`Dispositivos e impresoras`".

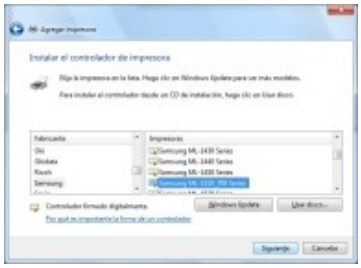
Se nos abrirá la ventana siguiente y haremos clic en "`Agregar una impresora`".



En la pantalla que aparece seleccionamos la opción "`Agregar una impresora local`" y continuaremos el proceso.

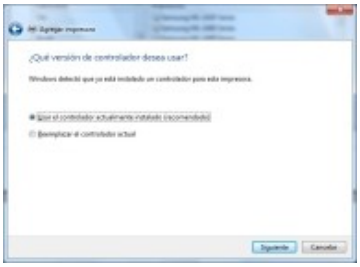


Indicaremos el puerto de conexión de la impresora. Windows 7 permite la instalación automática de las impresoras USB cuando se conectan al equipo. En este caso, nuestra impresora está conecta en el puerto LPT1.



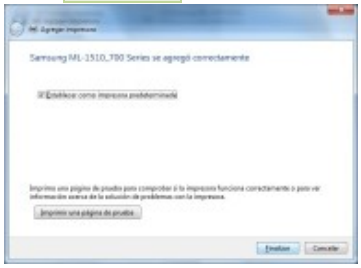
Indicaremos la marca y modelo de la misma.

En el caso de que no nos aparezca el modelo concreto de la impresora pulsaremos la opción "`Usar disco`" para indicarle la ruta exacta de los controladores o si nos los hemos descargado de la página del fabricante procederemos a la instalación con el ejecutable que se suministre.

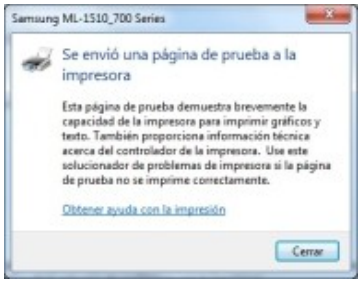


Si los controladores ya están instalados nos aparecerá la ventana siguiente (dejamos la opción por defecto):

Tras instalar los correspondientes controladores, pasa a ser mostrada la siguiente ventana en la cual indicaremos en el campo "`Nombre de la impresora`", la cadena de texto con la que identificaremos a nuestra impresora, en este caso "**Samsung ML-1510**", tras lo cual pulsamos sobre el botón "`Siguiente`".



Nos preguntará si deseamos establecer la impresora como predeterminada (escogeremos la opción que nos interese) e imprimiremos una página de prueba.



Después de comprobar que la página de prueba se imprimió correctamente cerramos la ventana y nos dirigimos a "`Dispositivos e impresoras`" donde deberá aparecer la nueva impresora.

Partimos de la base que la impresora se ha instalado correctamente. De esta forma, clicamos sobre la impresora y nos dirigimos a Propiedades de la misma para conocer las opciones que nos suministra y poder compartirla con otros equipos de la red.

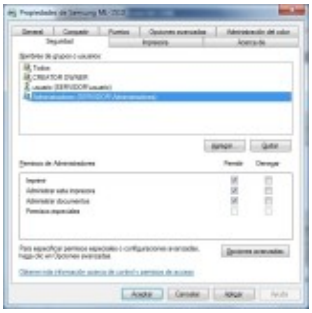
Para ello, en la pestaña "`Compartir`" activaremos la casilla "`Compartir esta impresora`" e indicaremos el nombre de la impresora compartida para que sea localizada fácilmente por los otros equipos.

Si queremos instalar controladores adicionales para el acceso a la misma de ordenadores clientes con sistema operativo distinto a Windows 7, se lo

indicaremos también en esta pantalla, mediante el botón "Controladores adicionales".

Veamos el contenido de las otras pestañas. Nos dirigimos a "Puertos" donde aparece el puerto de conexión de la impresora (en nuestro caso, en el **LPT1**, puerto paralelo).

En la pestaña "Opciones avanzadas" podemos configurar, por ejemplo, cuestiones tales como los horarios permitidos de impresión para dicha impresora, la prioridad de la misma y otras opciones de impresión.



En la pestaña "Seguridad" pueden ser establecidos los permisos de impresión y administración sobre la impresora de los distintos usuarios y grupos del sistema; aquí podremos especificar a qué usuarios y/o grupos deseamos dar acceso a la impresora en cuestión, y en qué condiciones.

Una vez llegados a este punto ya tenemos nuestra impresora local instalada en el equipo y compartida para que sea accesible desde otros ordenadores.

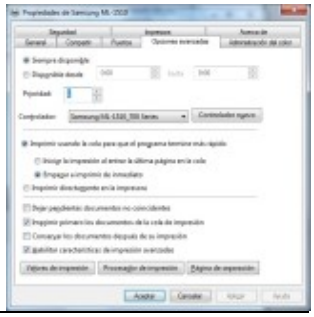
ASIGNAR PRIORIDADES EN LA COLA DE IMPRESIÓN.

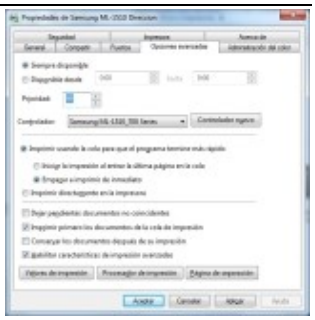
Comentamos en la unidad que existe una diferencia entre la impresora física (el dispositivo hardware que realmente imprime los trabajos) y la impresora lógica. Pues en este punto vamos a ver la utilidad de esta distinción. En ocasiones puede interesarnos tener en consideración la prioridad de los trabajos a la hora de imprimir en una impresora. Por ejemplo, imaginemos una impresora compartida en la que pueden imprimir varios grupos de usuarios de una empresa. Si un directivo necesita imprimir de forma urgente un documento y la impresora tiene en su cola de impresión múltiples documentos de otros departamentos (Ventas, Administración, …) tendría que esperar a que terminasen los trabajos de impresión previos. Por este motivo, podemos plantearnos la posibilidad de asignar prioridades en la cola de impresión de nuestros servidores de impresión. A continuación, vamos a ver cómo podemos llevar a cabo este proceso.

Para indicar la prioridad de impresión de un grupo de usuarios sobre otro (por ejemplo Dirección sobre Ventas), debemos seguir los siguientes pasos:

1. Hacer clic en "Agregar una impresora" para agregar una segunda impresora lógica para la misma impresora física.
2. Hemos creado una segunda impresora lógica llamada "Samsung ML-1510 Dirección" para asignar una mayor prioridad al grupo de usuarios de Dirección.
3. Una vez añadida hacer clic sobre ella con el botón derecho del ratón, seleccionar la opción "Propiedades de la impresora" y después hacer clic en la ficha "Opciones Avanzadas".
4. En el apartado "Prioridad", establecer una prioridad mayor que la que estableció en la primera impresora lógica, ya que el valor "1" es la prioridad mínima y "99" es la prioridad máxima.

   Pestaña de Opciones avanzadas de la primera impresora lógica (para el grupo de usuarios de menor prioridad) con la prioridad a **1**:

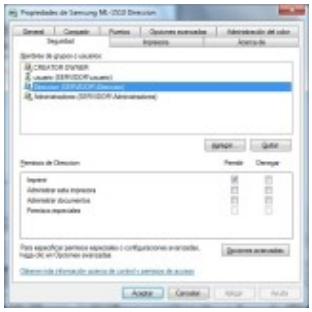




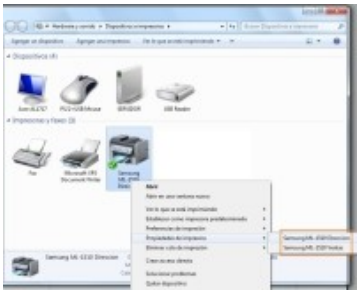
Pestaña de `Opciones avanzadas` de la segunda impresora lógica (para el grupo de usuarios de mayor prioridad) con la prioridad a **99**:

5. Finalmente debemos indicar el grupo de usuarios que utilice la primera impresora lógica y al grupo que utilice la segunda impresora lógica (con mayor prioridad), estableciendo los permisos deseados para los distintos grupos.

Pestaña `Seguridad` para la **primera impresora lógica** destinada a los usuarios con menor prioridad de impresión.



Pestaña `Seguridad` para la **segunda impresora lógica** (“**Samsung ML-1510 Dirección**”) destinada a los usuarios del grupo Dirección, con mayor prioridad de impresión.

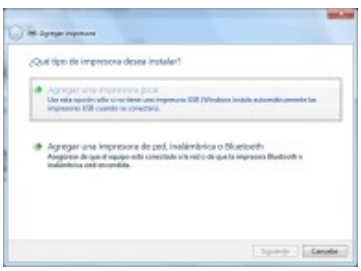


En la sección de “`Dispositivos e impresoras`” vemos las dos impresoras lógicas (**Samsung ML-1510 Ventas** y **Samsung ML-1510 Dirección**) creadas sobre la impresora física.

Instalar en el equipo servidor con Windows 7 una impresora con interfaz de red.

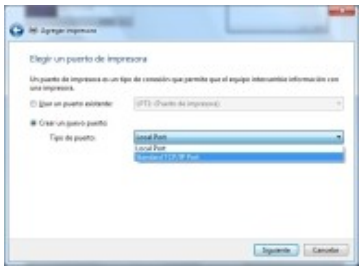
A continuación vamos a ver cómo definir en nuestro servidor con Windows 7, impresoras que dispongan de tarjeta de red. Estas impresoras harán uso del protocolo TCP/IP para conectarse a la red teniendo su propia dirección IP y configuración de red similar a la de otros equipos de la misma.

Para ello desde nuestro equipo Windows 7, accederemos a la opción de "`Agregar una impresora`" dentro del apartado "`Dispositivos e impresoras`" de la opción "Inicio”.



En la siguiente pantalla, al contrario de lo que podríamos suponer, para conectar una impresora con tarjeta de red debemos seleccionar la opción "`Agregar una impresora local`" y continuamos.

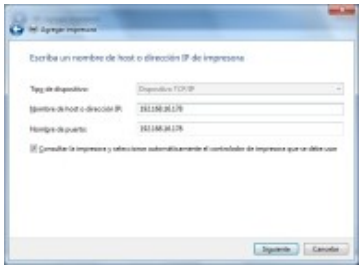
En la siguiente pantalla activamos la opción "`Crear un nuevo puerto`", y posteriormente en el desplegable "`Tipo`", especificamos la opción "`Standard TCP/IP Port`", puesto que lo que vamos a hacer es definir un puerto TCP/IP en nuestro equipo Windows 7 para poder establecer una conexión TCP/IP con la impresora; finalmente pulsamos sobre el botón "`Siguiente`".



En el menú de configuración de la impresora física o a través de alguna herramienta suministrada por el fabricante configuraremos los datos de red para la impresora. En nuestro caso son:

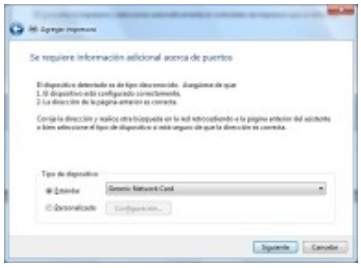
Dirección IP: 192.168.16.178 (dirección estática)
Máscara de red: 255.255.255.0
Gateway o puerta de enlace: 192.168.16.1

Una vez introducidos estos datos en la impresora. Continuamos con el asistente de Windows 7 para impresoras. En la siguiente pantalla pondremos la dirección IP de nuestra impresora en la entrada "`Nombre de host o dirección IP`" (en este caso "`192.168.16.178`"), pues el apartado "`Nombre de puerto`" lo rellena el sistema de forma automática (aunque podemos cambiar su valor si así lo deseamos); a continuación pulsaremos sobre el botón "`Siguiente`".

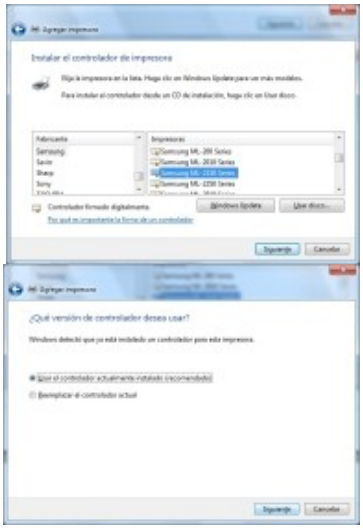


Se intentará detectar la impresora en red.

Si el sistema no puede encontrar el dispositivo en la red, es decir, la IP de la impresora no está accesible en este momento en la red, debemos analizar el motivo que provoca dicha inaccesibilidad; en cualquier caso podemos seguir con la instalación de la impresora en el servidor y analizar el posible problema existente posteriormente; para continuar el proceso de instalación, cuando se nos pregunta por el tipo de dispositivo en la siguiente ventana, seleccionamos la opción "`Estándar`", y de la lista desplegable seleccionamos la opción "`Generic Network Card`", para pulsar posteriormente sobre el botón "`Siguiente`".

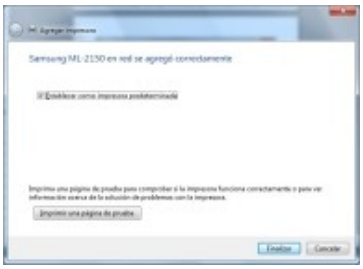


Tras esto, indicaremos la marca y modelo de la impresora (en nuestro caso es una **Samsung ML-2150**). En el caso de que no nos aparezca el modelo concreto de la impresora pulsaremos la opción "`Usar disco`" para indicarle la ruta exacta de los controladores o si nos los hemos descargado de la página del fabricante procederemos a la instalación con el ejecutable que se suministre.

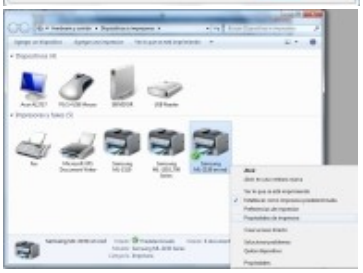


Si los controladores ya están instalados nos aparecerá la ventana siguiente (dejamos la opción por defecto):

El siguiente paso consiste en indicar el nombre que queremos que tenga la impresora en el "`Panel de impresoras`" de nuestro Windows 7, decidimos si queremos que sea la impresora predeterminada. Dejaremos las opciones por defecto o modificamos según interese y pulsaremos el botón "`Siguiente`".


Finalizamos el asistente de instalación y nos dirigimos a "`Dispositivos e impresoras`" para ver las `Propiedades` de la impresora.



Vamos a la pestaña "`Puertos`" y comprobamos el puerto de la impresora y la compartimos desde la pestaña "`Compartir`".

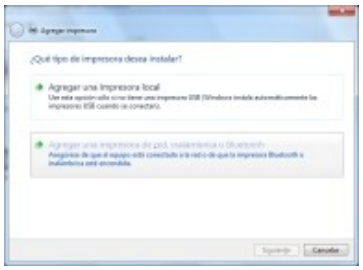
Finalmente, veremos **cómo instalar una impresora en red en los equipos cliente**.

Instalación de una impresora compartida o en red en los equipos cliente.

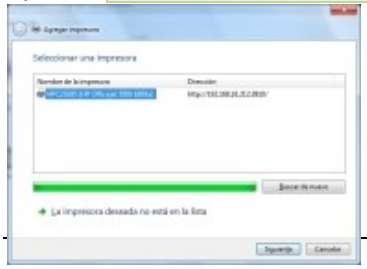
En este apartado veremos cómo conectar a un equipo cliente con una impresora instalada y compartida por nuestro equipo servidor Windows 7 y también configuraremos la conexión a una impresora con interfaz de red.

El proceso de instalación en el equipo cliente lo realizaremos con independencia de si la impresora está conectada físicamente al equipo servidor o se conecta directamente a la red. En el primer caso será necesario que el equipo al que está conectada la impresora esté encendido para que ésta pueda imprimir los trabajos de impresión de los equipos cliente. En el segundo caso, una impresora con su interfaz de red, la impresora no depende de ningún equipo, es autónoma, con lo que nos brinda una mayor flexibilidad a la hora de imprimir.

Para que cualquier equipo cliente pueda conectarse a la impresora instalada y compartida en nuestro Windows 7, lo primero que debemos hacer es desde el equipo cliente Windows, abrir el menú de "`Impresoras y faxes`" (para Equipos con Windows XP) o "`Dispositivos e impresoras`" (para Windows 7) y pulsar sobre el enlace "`Agregar una impresora`".

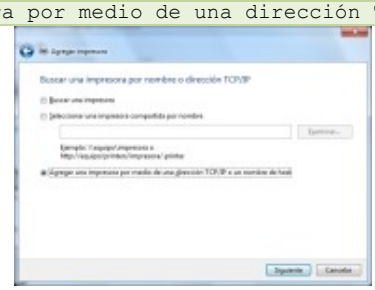


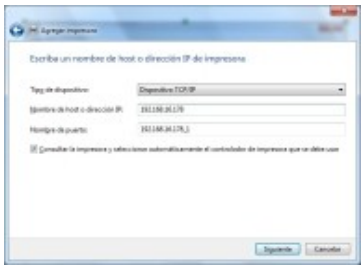
En la siguiente ventana mostrada por el asistente, activaremos la opción "`Agregar una impresora de red`".

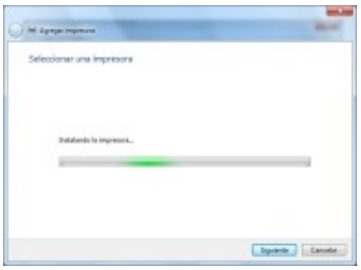


Intentará buscar automáticamente las impresoras en red, mostrándonos las que encuentre.

Si la impresora a instalar no está en la lista podemos "`Buscar de nuevo`" o buscarla de forma manual (si es una impresora compartida indicaremos el nombre del equipo que la comparte y el nombre de la impresora en la opción "`Seleccionar una impresora compartida por nombre`", si la impresora está conectada directamente a la red indicaremos su dirección IP por medio de la opción "`Agregar una impresora por medio de una dirección TCP/IP`"):







Una vez localizada hacemos doble clic para instalarla en el equipo cliente.

En la sección de "`Dispositivos e impresoras`" deberá aparecernos la impresora en cuestión:

3.2.3.- Servidores de aplicaciones y web.

Cuando hablamos de **servidor de aplicaciones** nos estamos refiriendo a u n equipo servidor, dentro de una red, que proporciona servicios de aplicación a los equipos cliente. Un servidor de aplicaciones, con frecuencia, gestiona la mayor parte o totalidad de las funciones de la lógica de negocio y de acceso a los datos de la aplicación. Las aplicaciones cliente pueden usar esta lógica tal y como lo harían al llamar a un método de un objeto (en el paradigma orientado a objetos) o a una función (en programación estructurada).

Estas aplicaciones cliente pueden incluir interfaces gráficas de usuario ejecutándose en un ordenador, un servidor web, o incluso otros servidores de aplicación. La información que viaja entre un servidor de aplicaciones y sus clientes no está restringida al formato simplemente HTML. En lugar de eso, la información es lógica de programa. Ya que la lógica toma forma de datos y llamadas a métodos con distinta funcionalidad.

Además, un servidor de aplicaciones administra sus propios recursos. Esta acción de mantenimiento incluye la seguridad, procesamiento de transacciones, la puesta a disposición de recursos y otros servicios. Las ventajas más importantes del sistema de servidores de aplicación son la centralización y la disminución de la complejidad en el desarrollo de aplicaciones.

Un servidor web se encarga de alojar y proporcionar las páginas web solicitadas por los clientes desde sus navegadores. Un servidor Web maneja el protocolo HTTP. Cuando el servidor Web recibe una petición HTTP, este responde con una respuesta HTTP, como por ejemplo, enviándonos de respuesta una página HTML. Para procesar una petición, un servidor Web puede responder con una página HTML estática, una imagen, enviando una redirección, o delegando la generación dinámica de la respuesta a algún otro programa, como por ejemplo algún script CGI, JSP (JavaServer Pages),

Servlets, ASP (ActiveServer Pages) o alguna otra tecnología del lado del servidor. Cualquiera que sea su propósito, este tipo de programas del lado del servidor generan una respuesta, a menudo en HTML, para que pueda ser vista en un navegador Web.

Como veremos en este apartado, instalar un servidor web no resulta una tarea complicada. Windows suministra de serie la posibilidad de instalar el servidor web IIS, sin embargo, existen otras opciones. Una buena alternativa al servidor web IIS de Microsoft, es el servidor web Apache. Apache es actualmente el servidor web más implantado entre los distintos servidores que ofertan servicios web en Internet. Además, Apache es compatible tanto para plataformas Linux como Windows. Una de las principales razones del éxito del servidor web Apache es que se trata de una aplicación libre y puede descargarse de forma gratuita.

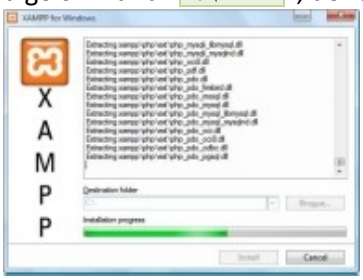
En este apartado vamos a ver la instalación y configuración básicas de la aplicación XAMPP. XAMPP es realmente un paquete que aglutina varios programas: el servidor web Apache, un intérprete del lenguaje de script PHP, el gestor de bases de datos MySQL, etc. Nos decantamos por esta opción por simplicidad y por la utilidad de tener instalados todos esos servicios en un único proceso de instalación. Para ver todo el proceso descarga el siguiente recurso.

Instalación del servidor web apache con XAMPP en Windows 7.

El primer paso es descargar XAMPP, nos dirigirnos a:
http://sourceforge.net/projects/xampp/files/latest/download

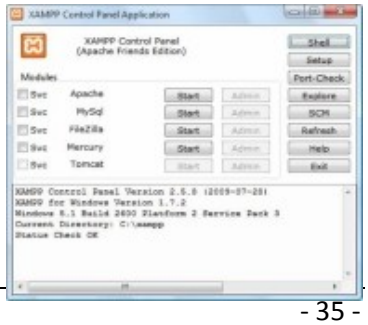
Accedemos al enlace XAMPP Windows y buscamos la última versión para descargar.

Una vez descargado el archivo de instalación lo ejecutamos y comenzaremos el proceso. La instalación es sencilla, indicaremos el directorio donde se instalará XAMPP. Por defecto se instala en "`C:\`" creando una carpeta '`XAMPP`' donde se alojarán todos los archivos de la aplicación. Podemos cambiar dicha dirección pero tenemos que tener en cuenta que no puede estar albergado en una carpeta cuyo nombre contenga espacios, como por ejemplo, en la carpeta "`C:\Archivos de Programa`", ya que podría daros conflictos con Apache. En principio dejaremos la ruta por defecto o si tenemos una partición vacía o con suficiente espacio para albergar XAMPP lo pondremos en la raíz de dicha partición, quedándonos algo similar a "`X:\XAMPP`", donde X es la unidad destino.

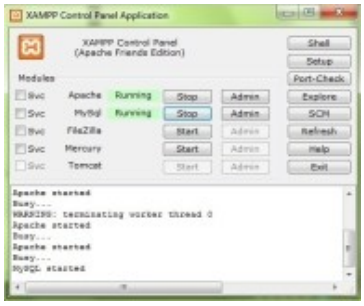


Tras esto comienza la extracción y copiado de los archivos a la ruta de destino.

Una vez terminada la instalación podemos abrir el panel de control de XAMPP desde donde tenemos la opción de arrancar los servicios del servidor web Apache y del gestor de bases de datos MySQL. Para ello pulsaremos los botones Start o Iniciar para ambos servicios. En el

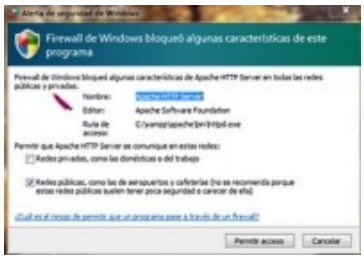


recuadro inferior se nos informará si los servicios se han activado correctamente (Apache / MySQL started, iniciado).

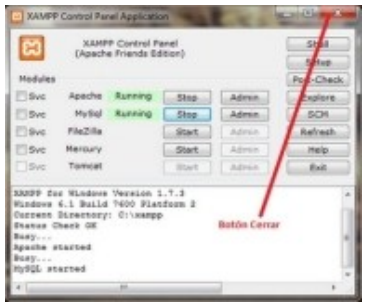


Al lado de los servicios aparecerá un texto sobre fondo verde con la palabra "`Running`" (activo).

Si tienes el Firewall de Windows activado te saldrán éstas dos ventanas cuando inicializas los servicios de Apache y MySQL. Debes permitir el acceso, ya que en caso contrario no podrás trabajar con el XAMPP, en especial cuando trabajas con scripts o códigos que se comuniquen con un servicio web específico.

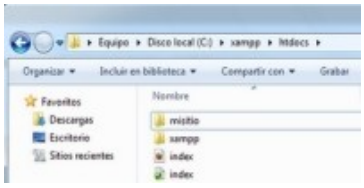


Una vez los servicios estén activos podemos cerrar el panel de control de XAMPP. Si en algún momento necesitamos acceder al mismo, lo tendremos en la barra de Tareas junto al reloj del sistema, haciendo doble clic sobre su icono se abrirá de nuevo.



Para terminar comprobaremos que el servidor web funciona adecuadamente. Abrimos una ventana del navegador y tecleamos **`http://localhost`** y se debe abrir el servidor web local. Se verá una página similar a la siguiente:

Ahora nos preguntamos, ¿dónde se alojan las páginas y recursos, -imágenes, archivos multimedia, scripts, ..- que suministra el servidor web mediante una URL desde el navegador? En el caso de Apache en un directorio llamado '**htdocs**'. Como la ruta de XAMPP vimos que, en nuestro caso, era `C:\xampp`, el directorio público del servidor web Apache será **`C:\xampp\htdocs`**. Dentro de htdocs podemos crear subcarpetas para organizar los recursos de uno o varios sitios web.



Ahora podemos crear una página html o nuestro primer script en php para ver que todo funciona correctamente.

A continuación, creamos una subcarpeta '`misitio`' dentro de `C:\xampp\htdocs`. Después creamos un nuevo fichero (con un editor de texto plano, por ejemplo, el Bloc de notas de Windows), lo llamamos `index.php` y lo guardamos en la carpeta (`C:\xampp\htdocs\misitio`).

Ahora editamos el fichero index.php con el siguiente código:

```
<?php
echo "La información de mi servidor:<p />";
phpinfo();
?>
```

Lo guardamos en la carpeta '`misitio`', tras eso, vamos a nuestro navegador web y tecleamos "`http://localhost/misitio`" y nos debe de aparecer el script que acabamos de crear. Ya tendríamos funcionando nuestro servidor web Apache.

¿Cuál es la carpeta pública del servidor web Apache?

- ○ Htdos.
- ◉ **Htdocs.**
- ○ Inetpub.
- ○ Htpub.

3.3.- Monitorización de red.

En ocasiones, podemos notar que la velocidad de nuestra red decrece notablemente y nos preguntamos cuál puede ser el motivo: ¿hay algún usuario ajeno a la red que está aprovechándose de nuestro ancho de banda? ¿Podemos estar siendo víctimas de otro tipo de ataque? ¿**sniffing** (*Olfateando - programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos*)? ¿**spoofing IP** (*Suplantación de identidad - uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación*)? ¿**DoS** (*Denial ofService, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos*)?

La solución es incrementar el control sobre la red controlando su rendimiento y funcionamiento para detectar comportamientos anómalos o sospechosos. Para lo cual, nos ayudaremos de herramientas de análisis de red. Estas herramientas realizan un estudio detallado y pormenorizado del tráfico que circula por la red.

La monitorización se considera, también, una tarea de mantenimiento preventivo, tanto a nivel de seguridad como de dimensionamiento de red. Si una red no está bien dimensionada, su tamaño no es adecuado. Dada esta situación puede ocurrir que el ancho de banda sea insuficiente o por el contrario esté sobredimensionado, pueden darse cuellos de botella en el acceso a servidores, etc.

A continuación, referenciamos algunas de las herramientas de monitorización de redes más conocidas:

Herramientas de monitorización de redes	
Herramientas de monitorización de red	**Características**
Spiceworks	Es una potente utilidad gratuita para administradores de redes. Cuenta con numerosas herramientas útiles y una configuración sencilla. Tiene una interfaz de navegador y muestra de forma gráfica toda la información de la red. El exhaustivo monitoreo de Spiceworks comienza con un escaneo general en busca de dispositivos conectados a la red, programas instalados y otros elementos.
Wireshark	Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones. Tiene una interfaz gráfica, y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo. Wireshark incluye un completo lenguaje para filtrar lo que

	queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Wireshark es software libre y se ejecuta sobre la mayoría de sistemas operativos Unix, Linux, Mac OS X y Microsoft Windows.
Nmap	Es un programa de código abierto que sirve para efectuar rastreo de puertos. Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

Estas **herramientas de monitorización** nos darán **información sobre**:

- ✓ Número de equipos conectados y sus direcciones IP.
- ✓ Tipo de tráfico predominante.
- ✓ Qué puertos están abiertos.
- ✓ Qué conexiones establecidas hay.
- ✓ Algunos programas nos permiten la realización de inventarios de los equipos de la red (puntos de red, segmentos, cableado, switches, routers, PC, etc.)

Algunos de los **datos** o **eventos** a los que debemos **prestar especial atención** cuando **monitoricemos redes** son:

- ✓ Número de usuarios conectados.
- ✓ Tiempos de respuesta de los sistemas.
- ✓ Cuellos de botella (posible mal dimensionamiento de la red o indicio de un ataque, por ejemplo, de denegación de servicio).
- ✓ Registros de servicios.
- ✓ Registro de intentos fallidos de conexiones.
- ✓ Comportamientos anómalos de posibles usuarios malintencionados.
- ✓ Controlar el inventario de red (comprobar si hay equipos que han sufrido cambios).
- ✓ Y otros que pudieran interesarnos.

Página donde conocerás con detalle las posibilidades del comando netstat, muy útil para identificar las conexiones activas, puertos que están a la escucha en un equipo, etc.
http://norfipc.com/redes/netstat-conocer-ver-conexiones-activas.html

Una herramienta de monitorización de red nos permite …

- ○ Dimensionar la red.
- ○ Conocer qué puertos están abiertos.
- ○ Hacer inventario de los equipos de una red.
- ◉ **Todas son ciertas.**

4.- Gestión de la Seguridad de las conexiones.

Caso práctico

__María__ le comenta a __Carlos__ que tan importante es saber montar un servicio en red cómo monitorizarlo y protegerlo, para mantener su rendimiento y seguridad. Por ello, le comenta que existen diversas herramientas, más o menos especializadas, según el entorno de uso, para conseguir un nivel aceptable de seguridad en la red y en los equipos que forman parte de ella. __María__ se refiere a los programas de antivirus, cortafuegos y el aseguramiento de las comunicaciones inalámbricas, tan comunes actualmente, cuya protección es, en ocasiones, descuidada y puede suponer una grave brecha de seguridad por la que lleguen numerosos ataques.

Al conectarnos en red enviamos y recibimos información. Esta información viaja por la red de forma que el destinatario pueda recibirla y enviar una respuesta si fuera necesario. Cuando un conjunto de ordenadores se encuentran conectados en la misma red existe la posibilidad de compartir información y servicios. El esquema que suele utilizarse para ello es la arquitectura cliente/servidor. Cada ordenador o equipo tiene un rol, servidor o cliente. Si un equipo actúa como servidor, entonces, puede suministrar acceso a determinada información (servidores de ficheros) o uno o varios servicios (servidor de aplicaciones, de correo, web, …). Los equipos clientes solicitan los recursos o acceso a los servicios siguiendo una serie de pasos o protocolos, a través de un puerto determinado. La gestión de la información compartida y de los servicios en red no siempre es sencilla, ya que debe ser protegida para garantizar que sólo los usuarios legítimos tengan acceso a los recursos o aplicaciones en red.

El activo más valioso de una organización son sus datos, al fin y al cabo, la información que utilizan las aplicaciones. Por ello, debemos ser conscientes de la importancia de protegerla mediante sistemas de seguridad. Estos sistemas de seguridad aparecen por la aparición de **amenazas** sobre la información y los sistemas que la gestionan.

Veamos qué entendemos por amenaza. Una **amenaza** es “una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso ilegítimo).”

En una red donde millones de ordenadores intercambian ingentes cantidades de información diariamente, podemos distinguir tres **características básicas deseables en toda comunicación**:

- ✓ **Confidencial**. Referido al contenido de la información enviada/recibida, y también al origen y destino de la misma.
- ✓ **Íntegra**. Los datos no han sido modificados en el trayecto del emisor al destinatario, no hay suplantación de un usuario por otro y no pueden ser repudiados. Todo ello debe poder comprobarse en el momento de su recepción.
- ✓ **Disponible**. El emisor y el destinatario han de poder intercambiar información cuando sea necesario.

Entre las **amenazas** o ataques pueden distinguirse de manera general cuatro grupos distintos:

- ✓ **Interrupción**. El acceso a un recurso/comunicación se v e interrumpido, de manera física (destrucción de la red) o lógica (saturación de servidores con pérdida de la disponibilidad de los servicios que suministran, cambio de localización de los servicios/recursos de información, etc.).
- ✓ **Interceptación**. Alguien no autorizado consigue tener acceso al recurso/comunicación (pinchar la línea de red, captura ilícita de paquetes de información de la red, etc.).
- ✓ **Modificación**. Obtención no sólo de acceso no autorizado al recurso/comunicación, sino también de la capacidad de modificarlo (modificación de los datos enviados/recibidos entre dos ordenadores, etc.).
- ✓ **Fabricación**. Además de conseguir acceso al recurso/comunicación, se tiene la posibilidad de generar e insertar información adicional falsa.

Según la amenaza podemos clasificar los **ataques** en dos categorías. Estos pueden ser **de tipo pasivo y activo**. En los ataques de tipo pasivo el atacante no altera la comunicación, tan sólo tiene acceso a ella (por ejemplo, curiosear la información que viaja por la red, a qué horas, frecuencia y entre qué equipos). Los ataques de tipo activo son mucho más graves, ya que el atacante modifica la información transmitida o incluso genera una falsa, permitiendo incluso la suplantación de un usuario legítimo. El éxito de los ataques puede suponer, que en caso de usar algún sistema de seguridad, éste ha sido violado, y se ha descubierto su clave de acceso y el método utilizado para cifrar y descifrar las comunicaciones.

La aparición y rápida expansión de Internet ha supuesto no sólo la proliferación de servicios útiles para millones de usuarios alrededor del mundo, sino también, un número cada vez mayor de ataques que aprovechan las debilidades de los protocolos de red y los sistemas de información. Esto nos lleva a pensar en el concepto de **seguridad**. La seguridad (o sistema de seguridad) de los sistemas de información es el conjunto de funciones, servicios y mecanismos que permitan garantizar las siguientes **dimensiones**:

- ✓ **Autenticación**. Es el proceso de verificación de la identidad digital del emisor en una petición para conectarse a un sistema. El emisor que busca autenticarse puede ser una persona, un equipo o una aplicación. En una web de confianza, "autenticación" es un modo de garantizar que los usuarios son quienes dicen ser, y la comprobación de que tienen autorización para las funciones que solicitan sobre el sistema.
- ✓ **Confidencialidad**. Se define como la "condición que asegura que la información no pueda estar disponible, o ser descubierta, por personas, entidades o procesos no autorizados".
- ✓ **Integridad**. Se define como la "condición de seguridad que garantiza que la información es modificada, incluyendo su creación y destrucción, sólo por los usuarios autorizados".
- ✓ **Disponibilidad**. Se define como el "grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un Sistema de Información en un periodo de tiempo considerado aceptable". Se asocia a menudo a la fiabilidad técnica (tasa de fallos) de los servicios del sistema de información.

- ✓ **Trazabilidad**. Se puede definir como la creación, incorporación y conservación de información sobre el movimiento y uso de documentos, servicios, o actividades de un sistema informático. Para ello debe registrarse cualquier actividad, o utilización de los servicios y/o de la información.

El **sistema de seguridad** requerido por un sistema de información o una organización variará dependiendo de una serie de **factores**, entre los que pueden destacarse los siguientes:

- ✓ Si existe dispersión geográfica de los usuarios.
- ✓ Topología de la red de comunicaciones.
- ✓ Instalaciones donde residen los equipos físicos.
- ✓ Hardware que soporta el sistema de información.
- ✓ Configuración del equipo lógico básico.
- ✓ Tipo y estructura de las bases de datos.
- ✓ Forma de almacenamiento de los datos.
- ✓ Número y complejidad de los procesos a realizar.

En este punto nos centraremos en conocer los tipos de ataques más habituales, a nivel lógico, y cómo prevenirlos con los recursos que tenemos a nuestro alcance para conseguir un adecuado nivel de seguridad, no sólo en el ámbito doméstico sino también en el empresarial.

Las dimensiones de seguridad de la información son:

- ○ Trazabilidad, Autenticidad, Confidencialidad, Autenticación e Integridad.
- ◉ **Trazabilidad, Confidencialidad, Autenticación, Integridad y Disponibilidad.**
- ○ Cifrado, Confidencialidad, Disponibilidad, Autenticación e Integridad.
- ○ Autenticidad, Cifrado, Accesibilidad, Autenticación e Integridad.

4.1.- Principales ataques y protección ante los mismos.

Como vimos con anteriormente, se pueden señalar cuatro **categorías** habituales de formas de **ataques o amenazas lógicas**:

- ✓ **Interceptación** (escucha o monitorización).
- ✓ **Denegación del servicio** (Interrupción).
- ✓ **Modificación** (manipulación o alteración).
- ✓ **Suplantación** (impostura o fabricación).

Los **ataques o amenazas lógicas más comunes** para cada una de las categorías son los siguientes:

Los ataques o amenazas más habituales por categorías				
	Interceptación	**Denegación del servicio**	**Modificación**	**Suplantación**
Descripción	Cuando una tercera parte, no autorizada, accede al contenido de la información con el objetivo de apropiarse de la misma o con otros objetivos futuros lícitos o no. Se observa a la víctima para obtener información, establecer vulnerabilidades y posibles formas de acceso futuras.	Consiste en saturar los recursos del equipo hasta que éste sea incapaz de seguir prestando sus servicios, mediante consumo de recursos, alteración de configuraciones o alteración de componentes de red. También una tercera parte puede impedir que una comunicación se establezca.	Cuando una tercera parte no autorizada accede al contenido de la información y la modifica de forma que los datos que llegan al receptor de la misma difieren de los originales.	Se busca suplantar al usuario o sistema original utilizando distintas técnicas y así tener acceso a la información. Generalmente se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y contraseña mediante distintos mecanismos.
Dimensiones de seguridad afectadas	Son ataques contra la confidencialidad pero el resultado puede ser utilizado en el futuro en otro tipo de ataques.	Disponibilidad del sistema y la autenticación (caso de suplantación).	Afecta principalmente a la integridad y disponibilidad.	Son ataques contra la autenticación y confidencialidad, principalmente.
Ejemplos de ataques	• Sniffing. • Scanning. • Ataques con señuelos	• Connection flood. • Jamming o flooding con IP Spoofing.	• El Tampering o data diddling. • Ataques	• IP splicing-hijacking. • Browser hijacking. • Man In The

	(decoy). • Keyloggers. • Snooping-downloading.	• Ping de la muerte. • eMail bombing. • Smurf o broadcast storm. • Supernuke o winnuke. • Hoaxes (bulos).	contra agujeros de seguridad del software/sistema operativos. • Software malintencionado (virus, troyanos, gusanos, …).	Middle. • IP spoofing. • Spoofing-looping. • Web spoofing. • DNS spoofing (pharming). • Mail Spoofing. • Ingeniería social.

¿Qué efectos produce el ping de la muerte? ¿Qué se busca con el pharming? ¿Qué supone ser víctima de un hoax? ¿Y qué es una botnet? Para poder responder a estas cuestiones te animamos a que leas el siguiente recurso y conozcas con más detalle en qué consisten los ejemplos de ataques mencionados en la tabla anterior.

Ataques o amenazas lógicas contra los sistemas de información clasificados por categorías.

Hemos visto que los ataques o amenazas lógicas pueden clasificarse, según sus efectos e intenciones del atacante en estas cuatro categorías:

- ✓ **Interceptación** (escucha o monitorización).
- ✓ **Denegación del servicio** (interrupción).
- ✓ **Modificación** (manipulación o alteración).
- ✓ **Suplantación** (impostura o fabricación).

Conozcámoslas más a fondo:

1. **Interceptación (escucha o monitorización).**
   Cuando una tercera parte, no autorizada, accede al contenido de la información con el objetivo de apropiarse de la misma o con otros objetivos futuros lícitos o no.

   Consiste en observar a la víctima con el objetivo de obtener información, establecer vulnerabilidades y posibles formas de acceso futuras.

   Son ataques contra la confidencialidad principalmente, aunque el resultado se utilice en el futuro para otro tipo de ataques.

   Algunos conceptos relacionados con la interceptación son los siguientes:
   - ✓ **Espionaje**: espiar en busca de contraseñas, normalmente pegadas con post it al monitor. Un tipo especial es el **trashing**: buscar en la basura contraseñas (tanto en la física como en los buffers de información). O el **Shoulder Surfing** (*mirar por encima del hombro*) para ver cómo se teclea la contraseña.
   - ✓ **Decoy**: falsas interfaces que simulan a la real y permiten almacenar las contraseñas introducidas.
   - ✓ **Scanning**: escaneo de puertos abiertos para ser usados posteriormente.

- ✓ **Sniffer**: escucha en modo promiscuo de todos los paquetes que circulan por la red.

Algunos ataques concretos son:

- ✓ **Ataques con señuelos (decoy).**
  - ➔ Programas diseñados con la misma interfaz que otro original y que solicitan usuario y contraseña.
- ✓ **Keyloggers.**
  - ➔ Otra técnica es utilizar los keyloggers, que son programas que guardan todas las acciones de un usuario (las teclas pulsadas, los clicks del ratón, las ventanas activadas, los sitios visitados en Internet, los correos enviados) y luego se analiza el archivo generado para conocer su usuario y contraseña, u otro tipo de información.
- ✓ **TCP connect scanning.**
  - ➔ Esta es la forma básica del escaneo de puertos TCP.
  - ➔ Se envía el paquete **SYN**.
  - ➔ Si el puerto está escuchando, devolverá una respuesta de éxito (paquete **SYN-ACK**); cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.
  - ➔ Su principal desventaja es que este método es fácilmente detectable por el Administrador del sistema.
  - ➔ Una variante es el **TCP SYN Scanning.** Consiste en que el cliente (atacante) envía, después del **SYN-ACK** del servidor, un paquete **RST** (reset) para terminar la conexión y registrar el puerto abierto.
- ✓ **Fragmentation scanning.**
  - ➔ Es una modificación de las anteriores en la que en lugar de enviar paquetes completos de sondeo, estos se dividen en un par de fragmentos IP, partiéndose así la cabecera IP en distintos paquetes.
  - ➔ Esto lo hace más difícil de detectar y filtrar por los mecanismos de protección de la máquina amenazada (cortafuegos).
- ✓ **Eavesdropping - packet sniffing.**
  - ➔ Se realiza con Packet Sniffers, que son programas que controlan los paquetes que circulan por la red.
  - ➔ Los sniffers pueden ser colocados tanto en estaciones de trabajo conectadas a la red, como en un equipo Router o en un Gateway de Internet, y puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías a las instalaciones.
  - ➔ Cada máquina conectada a la red verifica la dirección destino de los paquetes TCP. Un sniffer consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por tanto todos los paquetes enviados a la red llegan a esta placa. Obteniéndose acceso a toda la información que circula por la red.
- ✓ **Snooping-downloading.**
  - ➔ Significa obtener la información sin modificarla, como el sniffing. Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante accede a los documentos, mensajes de correo electrónico y otra información, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propio ordenador, para luego hacer un análisis exhaustivo de la misma.
  - ➔ El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

2. **Denegación de servicio (interrupción).**
   En general consisten en saturar los recursos del equipo hasta que éste sea incapaz de seguir prestando sus servicios, mediante consumo de recursos, alteración de configuraciones o

alteración de componentes de red. También cuando una tercera parte impide que una comunicación se establezca, evitando que los datos del emisor lleguen al receptor.

Son amenazas que atentan contra la disponibilidad del sistema y la autenticación (caso de suplantación).

Algunos conceptos generales relacionados con la interrupción son los siguientes:

DoS (denial of service): También se conoce como jamming o flooding. Consiste en el consumo de recursos limitados, escasos o no renovables: ancho de banda, memoria, espacio en disco, tiempo de CPU, acceso a otras máquinas, número máximo de conexiones, etc. Ejemplos: **ICMP**, **UDP**, envío de gran número de mensajes, ficheros enormes, etc.

DDoS (Distributed Denial of Service): Involucra varias máquinas. Los bots o botnet, que es la red de máquinas a disposición de un atacante, y la máquina zombi que es una máquina atacada a la que se introduce un malware que nos hace dominarla. Es un ataque bajo control de una máquina maestra. Permite consumir fácilmente recursos de una víctima, como el ancho de banda, al utilizar una red de zombies. Ejemplo: ataque de fuerza bruta mediante el uso de muchos zombis que van a solicitar un servicio a una victima.

Las amenazas más habituales relacionadas con este tipo de ataques son las siguientes:

- ✓ **Connection flood** (inundación de conexiones).
  - ➔ Empresas que brindan servicios de Internet tienen un límite máximo en el número de conexiones simultáneas.
  - ➔ Un atacante establece muchas conexiones y no realiza ninguna petición sobre ellas, de esta forma monopolizará la capacidad del servidor.
  - ➔ Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones para mantener fuera de servicio al servidor.
- ✓ **Jamming o flooding con IP Spoofing.**
  - ➔ El atacante satura el sistema con mensajes para establecer una conexión.
  - ➔ En vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando “IP Spoofing" (Suplantación de IP).
  - ➔ El sistema responde al mensaje, pero al no recibir respuesta acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.
- ✓ **Ping de la muerte.**
  - ➔ Una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado forzado del equipo.
  - ➔ Se basan en manipular el tamaño de paquete que se envía en el comando ping, de manera que se produce el desbordamiento de memoria de la máquina atacada. Normalmente todas las máquinas tienen resuelta esta vulnerabilidad.
- ✓ **eMail bombing.**
  - ➔ Otra acción común es la de enviar millares de correos sin sentido a todos los usuarios posibles, de forma continua, buscando la saturación de los distintos servidores de correo de destino.
- ✓ **Smurf o broadcast storm.**
  - ➔ Recolectar una serie de direcciones de Broadcast, para, a continuación, mandar una petición ICMP (*Internet Control Message Protocol*), que es un subprotocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que unrouter o host no puede ser localizado. Pues bien, lo que se hace

es simular un ping (**ICMP**), y se envía a cada una de ellas en serie, falsificando la dirección IP origen, donde se pondrá la dirección IP de la víctima.
- ➔ Así cientos o miles de hosts mandarán una respuesta a la dirección IP de la víctima.

✓ **Supernuke o winnuke.**
- ➔ Un ataque característico (y quizás el más común) de los equipos con Windows es el Nuke, que hace que los equipos que escuchan por el puerto **UDP 137** a **139** (utilizados por los protocolos Netbios de Wins), queden fuera de servicio (o disminuyan su rendimientos) al enviarle paquetes UDP manipulados.
- ➔ Generalmente se envían fragmentos de paquetes, que la máquina víctima detecta como inválidos pasando a un estado inestable.

✓ **Bulos (hoaxes).**
- ➔ Transmitir por correo la falsa existencia de un virus, esto ocasiona que se reenvíe a otros usuarios, lo que puede colapsar servidores de correo o ser usados por spammers.

3. **Modificación (manipulación).**

Cuando una tercera parte no autorizada accede al contenido de la información y la modifica de forma que los datos que llegan al receptor de la misma difieren de los originales.
Se trata de una amenaza, principalmente, contra la integridad y disponibilidad.
Conceptos relacionados con ataques de modificación de la información son los siguientes:

✓ **El Tampering o data diddling.**
- ➔ Modificación desautorizada de los datos o el software instalado en el sistema víctima incluyendo borrado de archivos.
- ➔ Son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador, con la capacidad de ejecutar cualquier comando.

✓ **Ataques contra vulnerabilidades de diseño.**
- ➔ Muchos sistemas están expuestos a “agujeros” de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje.
- ➔ Estas vulnerabilidades ocurren por varias razones y miles de “puertas invisibles” son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, exploradores de Internet, correo electrónico y toda clase de servicios informáticos disponibles.

✓ **Los Malware.**
- ➔ Término inglés “Malicious Software” o badware. Se refiere a todo software diseñado para realizar acciones maliciosas o distintas al proceso habitual de información.
- ➔ Una clasificación habitual es.
  - → **Virus**: término genérico que comprende virus, troyanos, gusanos y bombas lógicas.
  - → **Código móvil malicioso**: código escrito para hacer daño pero que no encaja exactamente en las clasificaciones anteriores: Applets, Active X, SQL Inject y programas en Javascript o VisualBasic script.

Normalmente se utiliza el término genérico virus para referirnos a cualquier código malicioso, sin embargo interesa diferenciar cada término en función de cómo accede a un sistema (infecta), tipo de acciones que realiza y cómo se propaga. En este sentido, se diferencian en los siguientes apartados: virus, gusanos, troyanos y bombas lógicas:

✓ **Virus.**
- ➔ Bajo este término se englobarían todas aquellas amenazas que no entran dentro de otras categorías como código móvil malicioso, troyano, gusano o bomba lógica.
- ➔ Suelen tener dos características: propagación y destrucción, aunque esta segunda no es imprescindible.

- Algunos virus eliminan archivos, otros sólo muestran mensajes molestos, bromas, bloqueo de accesos, robo de datos, corrompen el sistema, dañan el equipo, etc.
- Clasificación según el modo de infección:
  - **Infección de archivos**: infectan archivos ejecutables con extensión .exe, .com, .bat. Se les llama por eso virus parásitos Se extienden a otros archivos. El sistema operativo verá el virus como parte del programa que se está ejecutando y le asignará los mismos privilegios. Esto le permitirá infectar otros archivos, cargarse en memoria o realizar cualquier otra fechoría.
  - **Infección sector de arranque**: fueron los primeros en aparecer, infectan el sector de arranque de discos duros y otros dispositivos de almacenamiento. Quedan residentes en memoria.
  - **Multipartitos**: infectan el sector de arranque y el sistema de archivos.
  - **Macros**: aprovecha las capacidades de automatización mediante macros de los programas de ofimática como Word, Excel, ... para infectar sus archivos. Se propagan junto al documento por lo que se extienden rápidamente.

✓ **Gusanos (Worms).**

- Se caracterizan en que se propagan de sistema en sistema de manera masiva. Crean copias exactas de ellos mismos. Su principal misión es reproducirse y extenderse al mayor número de ordenadores posibles.
- Internet y el correo electrónico han supuesto el verdadero auge de este tipo de código malicioso, que pueden infectar miles de ordenadores en cuestión de horas. Su mecanismo de distribución suele ser en la mayoría de los casos muy simple. Camuflados en un mensaje aparentemente inocente, llegan a nuestro correo electrónico. Una vez ejecutado leen nuestra lista de contactos (libreta de direcciones) y se reenvían de forma automática a todas las direcciones que contengan.
- También pueden utilizar otro archivo para propagarse, como un documento Word, enviando copias de sí mismo por correo; o explotar agujeros de seguridad en los sistemas para saltar de máquina en máquina. Estos son más devastadores, pues no dependen de que un usuario abra, o no, un mensaje del correo.
- Ejemplos: Core Red, Blaster.

✓ **Troyanos.**

- Un caballo de Troya es un programa que en su ejecución realiza tareas no previstas de antemano. El usuario ejecuta lo que cree un programa normal, permitiendo al troyano realizar tareas ocultas y, a menudo, malignas.
- Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti-troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el caballo que los griegos regalaron a los troyanos.
- Este malware puede tener muchos fines: destrucción de archivos, registrar la actividad del usuario o instalar una puerta trasera para el control remoto del equipo de la víctima.
- Uno de los caballos de Troya más sofisticados en la actualidad es el RAT (Remote Access Trojan) que permiten un control absoluto de las máquinas asaltadas. Debido al uso cada vez más generalizado de Internet con ADSL donde las máquinas están continuamente conectadas, este troyano cada vez está más extendido. Uno de los usos es tomar el control de varias máquinas

de la red a través de un RAT para, por ejemplo, atacar a otra máquina de la red.

- ✓ **Bombas Lógicas.**
  - ➔ Código malicioso que permanece dormido o latente hasta que se produce el evento programado para despertarlos, por ejemplo en una fecha determinada o una combinación de teclas.
  - ➔ El código no suele replicarse.
  - ➔ Un ejemplo es el de un empleado que se le va a despedir y que prepara una bomba lógica para actuar cuando ya no esté en la compañía.
  - ➔ Son muy difíciles de detectar por los antivirus.

4. **Suplantación (impostura o fabricación).**

La suplantación es similar a una interceptación pero con el objetivo de sustituir a una parte.

Se busca suplantar al usuario/sistema original utilizando distintas técnicas y así tener acceso a la información. Generalmente se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y contraseña mediante distintos mecanismos.

También ocurre cuando una tercera parte no autorizada introduce mensajes propios en una comunicación para hacer creer al receptor que proceden del emisor utilizando técnicas de suplantación (spoofing).

Son ataques contra la autenticación y confidencialidad, principalmente.

Algunos conceptos generales relacionados con este tipo de ataques son los siguientes:

- ✓ **Spoofing o falsificación.**
  - ➔ El intruso oculta su identidad real haciéndose pasar por otro usuario, equipo o aplicación.
  - ➔ Para ello se realiza, tanto la modificación de paquetes existentes en la red, como la creación de nuevos, cuyo objeto sea falsear la identidad de algún componente de la transmisión de un mensaje o del sistema en su conjunto.
  - ➔ En sentido genérico, el spoofing o *falsificación* se puede hacer: de dirección IP, sitios Web, DNS, correo, etc.
- ✓ **Hijacking.**
  - ➔ Significa "*Secuestro*" en inglés y en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñamiento o robo de algo (generalmente información) por parte de un atacante, es por tanto un concepto muy abierto y que puede aplicarse a varios ámbitos, de esta manera podemos encontramos con el adueñamiento o secuestro de conexiones de red, sesiones de terminal, servicios, navegadores, etc.

Algunos ataques concretos son los siguientes:

- ✓ **IP splicing-hijacking.**
  - ➔ Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la victima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.
  - ➔ El atacante que ha visto, mediante un Sniffer, los paquetes que circularon por la red, calcula el número de secuencia siguiente para continuar con la comunicación.
- ✓ **Browser hijacking.**
  - ➔ Secuestro del navegador. Se llama así el efecto de apropiación que realizan algunos programas sobre el navegador web lanzando popups, modificando la página de inicio, modificando la página de búsqueda predeterminada, etc.

- ✓ **Man In The Middle.**
  - ➔ El intruso usa una aplicación para simular el comportamiento del cliente o del servidor, o bien intercepta los paquetes de información que circulan por la red, pudiendo visionarlos y modificarlos a su antojo.
  - ➔ Como consecuencia el servidor o cliente creen estar comunicándose con el equipo legítimo, cuando en realidad se trata del equipo del atacante, que aparece a todos los efectos como el destino auténtico.
- ✓ **IP spoofing.**
  - ➔ El atacante genera paquetes de Internet con una dirección IP de red falsa en el origen, pero que es aceptada por el destinatario del paquete.
  - ➔ Paquetes manipulados con la dirección de un tercero, de forma que la víctima "**ve**" un ataque proveniente de ese tercero, y no la dirección real del atacante.
  - ➔ Desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza, basada en el nombre o la dirección IP del equipo suplantado.
- ✓ **Spoofing-looping.**
  - ➔ Una forma común de "Spoofing" es conseguir el nombre y contraseña de un usuario para, una vez se ha entrado al sistema, tomar acciones en nombre de él.
  - ➔ El intruso usualmente utiliza este primer sistema para obtener información y acceder a un segundo sistema y luego utiliza este para entrar en un tercero y así sucesivamente. Este proceso llamado "Looping", tiene la finalidad de ocultar la identificación y ubicación del atacante.
  - ➔ De esta manera se oculta la verdadera procedencia de un atacante, llegando incluso a provocar graves incidentes si la organización atacada cree que proviene de otra organización.
- ✓ **Web spoofing.**
  - ➔ El atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante permitiéndole controlar todas las acciones de la víctima, desde sus datos hasta las contraseñas, número de tarjeta de crédito, etc. No confundir con phising.
- ✓ **DNS spoofing (pharming).**
  - ➔ Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP", ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto, o por su confianza hacia servidores poco fiables. Las entradas falseadas de un servidor DNS son susceptibles de infectar (envenenar) el caché DNS de otro servidor diferente (DNS Poisoning).
- ✓ **Mail Spoofing.**
  - ➔ Suplantación en el correo electrónico de la dirección de correo de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de correos hoax (bulos) como suplemento perfecto para el uso de phising y para SPAM.
- ✓ **Ingeniería social.**
  - ➔ Manipulación de las personas para conseguir que digan o hagan algo que beneficie al atacante (sirven para conseguir contraseñas y acceso a redes).
  - ➔ Ejemplos:
    - → **Aplicación adicional a los virus**. Por ejemplo darle un nombre que incite a la víctima a ejecutar el archivo que viaja en el correo (virus I love you) o como si se tratara de un falso parche antivirus.
    - → **Phishing**: a través del correo se envían enlaces a páginas web que se hacen pasar por bancos o tiendas virtuales, con el objeto de capturar la cotraseña o el número de cuenta de la víctima.

→ **Timos** (*scams*): timos varios que prometen dinero, usualmente vía correo electrónico.

¿Qué es DoS?

- Consiste en el consumo de recursos de un equipo para provocar la caída de uno o varios servicios.
- También se conoce como jamming o flooding.
- Puede llevarse a cabo a través del envío de gran número de mensajes, ficheros enormes, etc.
- **Todas son ciertas.**

La suplantación de una dirección IP se conoce como:

- Flooding IP
- Phishing
- **Spoofing IP**
- IP splicing-hijacking

4.2.- Configuración de antivirus.

Como vimos en la anterior unidad los antivirus se encargan de detectar, bloquear y eliminar virus y otros programas malintencionados. Para ello monitorizan las aplicaciones que se ejecutan y la entrada y salida de archivos en el ordenador para evitar que alguno de ellos pueda llevar a cabo una acción malintencionada.

Actualmente, los antivirus consumen una cantidad moderada de recursos con lo que no afectan tanto al rendimiento del equipo. Además, nos permiten programar análisis periódicos según nuestras necesidades y pueden observar patrones de comportamiento potencialmente peligrosos en procesos, y detectar así nuevo software malintencionado no recogido en la lista de definiciones de virus. La base de datos de virus contiene todo el software malintencionado que es capaz de reconocer el antivirus. En ella el antivirus tiene el código de cada virus conocido, incluidas sus actualizaciones y cuando revisa los archivos lo que hace es comparar esos códigos. La base de datos de virus se actualiza periódicamente con nuevas amenazas detectadas. La predicción de amenazas no reconocidas se realiza mediante técnicas heurísticas.

En este apartado vamos a ver qué opciones tiene y cómo configurar un programa antivirus concreto. Hoy en día, contamos con una amplia oferta para elegir entre antivirus comerciales y gratuitos de gran calidad. En nuestro caso, tomamos como alternativa un antivirus gratuito, Avast! Free Antivirus, debido a su accesibilidad, amplio uso y eficacia. Seguiremos los siguientes pasos:

- ✓ **Descarga e instalación.**
- ✓ **Navegar por las opciones del menú.**
- ✓ **Protección con sandbox o caja de arena.**
- ✓ **Uso de la heurística.**
- ✓ **Mejorar el rendimiento.**
- ✓ **Planificar análisis periódicos.**

Descarga e instalación.

Para comenzar accedemos a la web de Avast para descargar el antivirus:
http://www.avast.com/

Haremos clic en el enlace correspondiente para descargar Avast! Free Antivirus. Avast! Además de su antivirus gratuito ofrece otros productos comerciales que incluyen opciones adicionales (protección contra el spam, cortafuegos, compras y banca online más seguras, etc.).

Terminada la descarga, haremos doble clic sobre el fichero de instalación, setup_av_free.exe, para iniciar la instalación. El proceso de instalación es sencillo y lo primero que realiza es un punto de restauración, para que en caso de algún problema, se pueda volver al estado anterior a la instalación del antivirus.

Navegar por las opciones del menú

Ya hemos finalizado la instalación y vamos a conocer la interfaz del programa. Ésta es bastante intuitiva y clara, está organizada por bloques situados a la izquierda de la pantalla principal. Estos bloques son:

- ✓ General.
- ✓ Analizar el equipo.
- ✓ Escudos en tiempo real.
- ✓ Protección adicional.
- ✓ Mantenimiento.

En el bloque General podemos ver el estado actual del equipo y a continuación, nos permitirá activar el modo silencioso o de juego. La opción que viene por defecto es el modo silencioso que supone que el antivirus no nos molestará con ningún tipo de alerta. Esto puede ser útil en situaciones puntuales, pero lo recomendable es que no se active este modo de manera permanente si queremos preservar la seguridad del equipo.

Este antivirus proporciona protección para el sistema de archivos, el correo electrónico, servicio de mensajería instantánea, la web, las conexiones P2P, además de tener un escudo de scripts de red y para el comportamiento de las aplicaciones.

Tipos de análisis, configuración y programación de los mismos

El antiviruas Avast! nos da la posibilidad de realizar distintos tipos de análisis, todos ellos configurables:

- ✓ **Análisis rápidos**: Analiza la unidad del sistema, rootkits, programas de inicio automático, se pueden incluir programas potencialmente peligrosos (PDD). Podemos modificar las opciones por defecto para este tipo de análisis y adaptarlo a nuestras necesidades.
- ✓ **Análisis completo del sistema**: Realiza un análisis exhaustivo del sistema, es más lento que el anterior. Incluye el análisis de todos los discos duros, rootkits, programas de inicio automático y módulos cargados en memoria. La prioridad del análisis y sensibilidad heurística (ampliaremos este concepto posteriormente) son mayores que en el análisis rápido.
- ✓ **Análisis de unidades extraíbles**.
- ✓ **Análisis de carpeta seleccionada**.
- ✓ **Crear análisis personalizado**: Permite seleccionar los elementos que se quieren analizar (todos los discos duros, la unidad del sistema, la memoria, rootkits, programas de inicio automático, …)

y escoger otras opciones de análisis (sensibilidad heurística, archivos que deben descomprimirse para analizarlos, posibles exclusiones, activar la generación de informes, la programación de tareas, etc.).

- ✓ **Análisis durante el arranque**.

Estos tipos de análisis se pueden adaptar a las necesidades del usuario en aspectos tales como el nivel de sensibilidad heurística, las extensiones de archivos que debe descomprimir para analizar, posibles exclusiones, activación de la generación de informes, la programación de tareas, etc.

Un punto importante es la **programación de tareas de análisis**, con ello evaluaremos el estado de seguridad de nuestro equipo y podremos despreocuparnos de tener que hacerlo manualmente cada cierto tiempo. En Avast! Programamos el análisis desde la opción: Más detalles - Opciones – Programar. En la pantalla de Programar podemos fijar la periodicidad del análisis (una vez, diaria, semanal, mensual), la hora de comienzo, el día de inicio, etc.

Protección con autosandbox.

Avast! nos da la posibilidad de ejecutar cualquier aplicación sospechosa en un entorno seguro de pruebas o sandbox (caja de arena). Cualquier operación que hagamos con un programa o archivo dentro del sandbox no afectará al sistema con lo que podremos estar seguros de probarlo. Para acceder a la opción de configuración de este entorno seguro de ejecución nos dirigiremos a la opción `Protección adicional – Autosandbox – Opciones`.

Por defecto esta característica está activada en modo '`Preguntar`', con lo que consultará previamente al usuario si quiere transferir la ejecución de una aplicación sospechosa al entorno seguro de pruebas. Para una mayor seguridad, puede ser útil activar el modo '`Auto`' y evitar continuas preguntas. Así se aplicará a todos los programas que se ejecuten, por lo que es aconsejable excluir deSandbox las aplicaciones que utilicemos con frecuencia y sobre las que tengamos confianza para no ralentizar el uso de las mismas. Esto puede hacerse desde el botón '`Examinar`' del apartado de '`Archivos que serán excluidos del Sandbox automático`'.

Uso de la heurística.

Las técnicas heurísticas se utilizan para poder detectar amenazas no registradas en la lista de virus conocidos por el antivirus. Consiste en una comparación de patrones de código sospechosos y ciertos comportamientos con los programas o archivos del equipo. El empleo de estas técnicas consume bastantes recursos por lo que el rendimiento del equipo puede verse afectado, por esta razón el antivirus permite ajustar el nivel de sensibilidad de la heurística. Podemos adaptar la heurística en la opción principal `Escudos en tiempo real – Escudo del sistema de archivos – Opciones avanzadas`. Una vez ahí, clicamos sobre el enlace, `Sensibilidad de la heurística` y podremos también activar el `examen de los archivos completos`, y la `búsqueda de programas potencialmente peligrosos`.

Mejora del uso de los recursos.

Los desarrolladores de antivirus han realizado un esfuerzo considerable para conseguir que los programas antivirus consuman la menor cantidad de recursos posible. Avast! nos permite configurar ciertas opciones que nos ayudarán a mejorar

el rendimiento del antivirus. Para acceder a ellas accedemos a `Escudos en tiempo real - Escudo del sistema de archivos - Opciones avanzas - Avanzado`. Desde aquí podemos decirle al antivirus que no analice las bibliotecas de enlace dinámico (DLLs – *Dynamic Link Libraries*) comprobadas. Otra posibilidad es utilizar la memoria caché transitoria en la que se guardan los archivos ya analizados durante la actual sesión de trabajo para evitar que vuelvan a ser comprobados hasta que el equipo se reinicie, o la base de datos de virus sea actualiza. Por último, si se activa la caché persistente, conseguiremos almacenar los identificadores de los archivo "seguros" vigentes siempre para que sean analizados sólo una vez, incluso si reiniciamos o se actualiza la base de datos de virus.

Mantenimiento

Desde la opción principal de Mantenimiento podemos actualizar la base de datos de virus y el programa, de forma automática – *el programa detecta por sí sólo las actualizaciones, se las descarga y avisa al usuario* – o pueden hacerse manualmente. Además, otro módulo útil es el baúl de virus, consistente en una ruta a la que se mueven los archivos detectados como peligrosos o infectados (*archivos en cuarentena*). Si durante el análisis se encuentra alguno de estos archivos puede darse la opción al usuario de desinfectar, eliminar, ignorar o mover al baúl.

¿Para qué sirve el sandbox o caja de arena en un programa antivirus?

- ○ Se trata de una técnica para reconocimiento de nuevas amenazas.
- ◉ **Es un entorno de ejecución seguro para aplicaciones sospechosas o desconocidas.**
- ○ Se emplea para planificar tareas de análisis.
- ○ Ninguna es cierta.

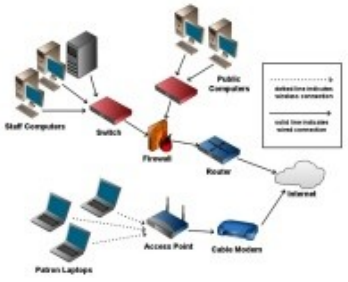
4.3.- Configuración de cortafuegos.

Los cortafuegos o firewalls se encargan de controlar, permitiendo o denegando, las conexiones entrantes y salientes de un ordenador. Las conexiones ocurren de forma general cuando nos encontramos conectados a Internet o una red local. Un cortafuegos puede implementarse bajo una aplicación software, pero también puede ser un dispositivo hardware, o una combinación de ambos.

Los cortafuegos establecen una barrera entre el ordenador y la red a la que está conectado, bloqueando el tráfico, discriminando entre aplicaciones permitidas y las que no lo están. Ofrece diferentes niveles de seguridad en función del uso y conocimientos del usuario.

Entre las funciones de un cortafuegos están:

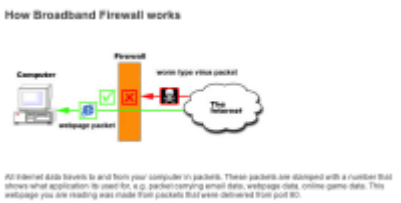
- ✓ Evitan ataques bloqueando accesos y conexiones no autorizadas, impidiendo que se produzcan.
- ✓ Complementa las defensas antivirus, antispyware, etc.
- ✓ Bloquean el tráfico basándose en un esquema de aplicaciones fiables - no fiables (permiten configurar reglas de filtrado de conexiones, de paquetes de información, ...).
- ✓ Ofrecen varios niveles de seguridad, preconfigurados, para satisfacer las distintas necesidades de seguridad del usuario.



- ✓ Proporcionan información sobre los intentos de ataque.

Los cortafuegos protegen de:

- ✓ Los accesos no permitidos a través de la red.
- ✓ Los intentos automatizados de acceso a su equipo que producen saturación de los recursos, impidiendo el buen funcionamiento del mismo.
- ✓ Permiten controlar las conexiones salientes de la máquina evitando que el software malicioso que haya conseguido instalarse en un ordenador pueda establecer conexiones hacia el exterior. También es una forma de detectar cualquier actividad sospechosa en el ordenador.



Recordemos que los equipos conectados en una red se identifican a través de una dirección IP. Además, los sistemas operativos cuentan con un número de puertos virtuales disponibles para abrir conexiones y se las ceden a los programas para que los utilicen. Los programas solicitan los puertos y el sistema operativo los asigna estableciéndose una conexión lógica entre dos equipos conectados en red. La comunicación entre equipos se convierte en un flujo de datos entre dos puertos virtuales abiertos por un programa.

El cortafuegos se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores. Es como un semáforo que, en función de la dirección IP y el puerto (entre otras opciones), dejará establecer la conexión o no siguiendo unas reglas establecidas.

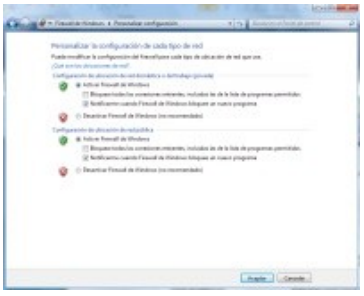
Ya sabemos que Windows cuenta con un cortafuegos de serie, el **Firewall de Windows**, en este apartado vamos a conocer su funcionamiento en detalle, y además, aprenderemos ciertos parámetros que nos permitirán sacarle un mayor rendimiento al cortafuegos. Todos los pasos expuestos a continuación se deben realizar con una cuenta con privilegios de Administrador.

Acceso al Firewall de Windows.

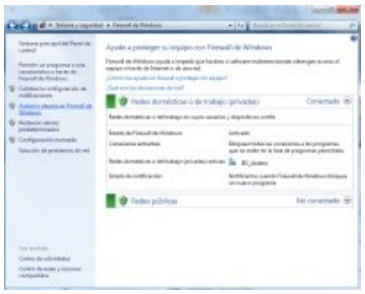
Podemos acceder al programa desde Inicio siguiendo la ruta: `Panel de control - Sistema de Seguridad - Firewall de Windows`.
Debemos saber que Windows establece dos grandes grupos de redes: privadas y públicas. Dentro de las redes privadas se incluyen, a su vez, los tipos: Dominio (para grandes organizaciones, cuya gestión recae en el administrador de red), Trabajo (para Pymes y grupos departamentales) y Doméstica.

Opciones básicas.

En la pantalla principal del Firewall de Windows la primera opción que nos da es la de activar o desactivar el programa. Además existen otras opciones de configuración adicionales que dependen del tipo de red utilizada. Si queremos modificarlas pulsaremos sobre Activar o desactivar el Firewall de Windows. Una opción que es muy recomendable activar es Notificarme cuando el Firewall deWindows bloquee un nuevo programa. Con ella indicaremos al cortafuegos que nos notifique mediante una alerta los accesos o programas potencialmente peligrosos. Estas alertas pueden aparecer cuando un programa de nuestro equipo intenta conectarse a Internet, a través del mensaje de alerta podemos decidir si permitimos o bloqueamos la conexión, dándonos un mayor control sobre la seguridad de nuestro equipo.



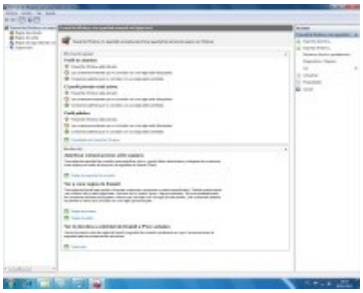
Programas con acceso a Internet.



Para permitir el acceso de ciertos programas a Internet debemos modificar la configuración del cortafuegos, ya que por defecto los bloqueará. Desde la pantalla principal del cortafuegos pulsaremos en la parte izquierda sobre la opción Permitir un programa o una característica a través de Firewall de Windows. Surgirá una nueva ventana donde podremos habilitar o deshabilitar la comunicación en red de los programas y servicios que te interesen de entre los que aparecen en la lista. Esta lista se crea a partir de los programas instalados en el equipo que han sido detectados por Windows y que en alguna ocasión ha solicitado conexión. Para cada programa o servicio aparecerán varias casillas de selección que indican el tipo de red que permite gestionar el cortafuegos. Si no marcamos ninguna casilla, el cortafuegos bloqueará siempre las peticiones de salida. En el caso de activar alguna, si la comunicación se realiza desde ese tipo de red seleccionada, la conexión tendrá acceso al exterior. Realizaremos las modificaciones según las necesidades del usuario o del sistema.

Reglas de conexión.

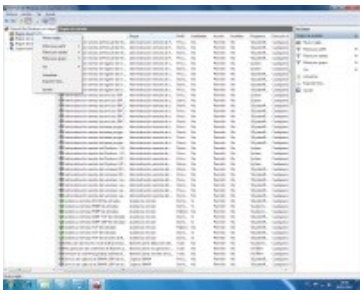
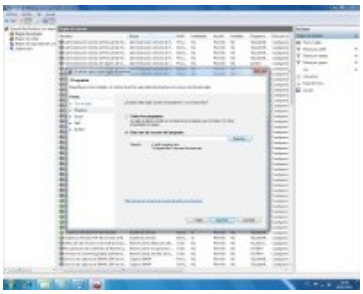
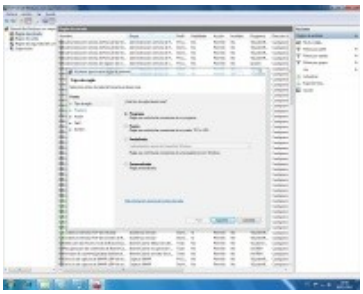
Con las reglas de conexión se consigue una configuración más detallada y a medida del cortafuegos. Podemos crear reglas, especificando ciertos parámetros, que facilitarán o bloquearán que determinados programas, puertos o dispositivos accedan a Internet o conecten desde ésta con el equipo. Distinguimos dos tipos de reglas, reglas de entrada (sirven para establecer qué accesos externos pueden acceder al equipo) y reglas de salida (se utiliza para determinar qué aplicaciones en ejecución pueden salir a Internet).



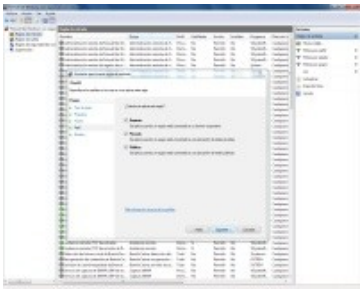
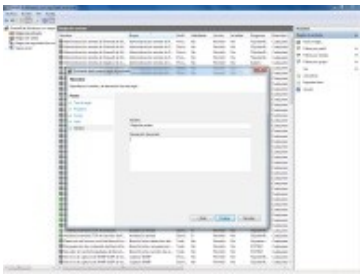
Para definir las reglas nos dirigimos a la pantalla principal y pulsamos sobre **Configuración avanzada**. Verás las dos opciones de Reglas de entrada y Reglas de salida. Se definirán tantas reglas como sea necesario. Un lema muy conocido en seguridad nos dice “todo lo que no está explícitamente permitido, estará prohibido”. Teniendo en cuenta esto, la idea es partir de una situación en la que todo está bloqueado y por medio de la creación de las reglas de entrada y salida estrictamente necesarias, consigamos que los programas ‘permitidos’ del equipo funcionen adecuadamente y tengamos un nivel aceptable de protección.

En nuestro equipo utilizamos multitud de programas que necesitan conexión en red, algunos de ellos pueden ser clientes FTP, programas de descarga, juegos on-line, … que pueden no funcionar si los puertos para esos servicios están bloqueados por el Firewall. Para solucionar esto comprobaremos que los puertos del router no están cerrados en el Firewall de Windows. Para ello, definiremos reglas que permitan la salida a las aplicaciones que nos interese que accedan a Internet.

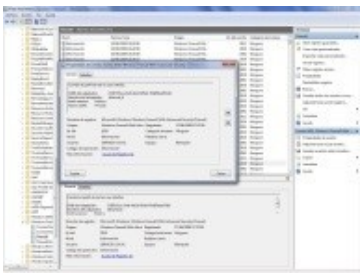
Supongamos que queremos utilizar un juego on-line que necesita que el puerto **300** del cortafuegos esté abierto. Para lo cual necesitaremos crear una regla de salida. Desde la pantalla de Configuración avanzada del Firewall de Windows seleccionamos, Reglas de salida en la parte izquierda y pulsamos sobre `Nueva regla`. En la ventana que se nos abre tenemos cuatro opciones: Programa, Puerto, Predefinida y Personalizada. Queremos asociar la regla a una aplicación, así que pulsamos en Programa y, después, hacemos clic en Siguiente. En la opción ‘Esta ruta de acceso del programa’ localizamos en el disco duro el archivo ejecutable de la aplicación y pulsamos Abrir.

La siguiente ventana nos presenta dos alternativas: Permitir la conexión (para permitir que el programa pueda acceder a Internet siempre) y Permitir la conexión si es segura (sólo permite el acceso si la red utilizada está protegida por contraseña). La más recomendable de las dos opciones es la última. Además, encontramos la posibilidad de elegir a qué equipos de la red se les aplicará la regla y cuales estarán excluidos. Tras esto, escogeremos los tipos de red a los que afecta la regla y finalizaremos la configuración de ésta. A partir de este momento el Firewall de Windows tendrá en cuenta la nueva configuración.

Control de eventos.



El Firewall de Windows proporciona información de todas las incidencias detectadas, del estado de las conexiones y de a qué servicios se ha conectado el equipo. Esta información puede ser consultada a través del Visor de Eventos. El Visor de Eventos genera un informe de cada incidencia. Para acceder a esta herramienta escribimos '`Visor de Eventos`' en el cuadro de búsqueda del menú de `Inicio`. Una vez abierto el Visor de Eventos, en la parte izquierda de la pantalla, localiza el apartado `Registro de aplicaciones y servicios` y, seguidamente, seguimos la ruta `Microsoft - Windows - WindowsFirewall With Advanced Security` y, finalmente, selecciona `Firewall` para ver todos los eventos y buscar los que te interesen.

¿Un cortafuegos es?

- ○ Una herramienta software para filtrar el tráfico que entra y sale de una red.
- ○ Una herramienta hardware para bloquear accesos no autorizados en una red.
- ○ Permite configurar reglas de entrada y salida.
- ◉ **Todas son verdaderas.**

4.4.- Configuración de seguridad en redes inalámbricas.

Nuestra situación de partida para explicar los puntos críticos en la configuración de seguridad en una red WiFi será una red de equipos conectados mediante un punto de acceso o router WiFi. Seguidamente, veremos los modos de conexión inalámbrica que existen y las características de seguridad de un router inalámbrico.

Redes en modo infraestructura y en modo Ad hoc.

Ya vimos que para montar una red inalámbrica tenemos dos opciones, funcionar en m infraestruodoctura y en modo Ad hoc. La primera opción es la más extendida y requiere de un punto de acceso que actuará como base inalámbrica a la que se conectarán los equipos de la red vía WiFi y se encargará de centralizar las comunicaciones en la red. Actualmente los Proveedores de Servicios de Internet (PSI), suministran con frecuencia a sus clientes routers WiFi. Estos dispositivos aúnan las funciones de router ADSL y las de punto de acceso inalámbrico con antenas internas o externas.

El modo Ad Hoc por el contrario, permite conectar dos equipos de manera directa, sin necesidad de punto de acceso intermedio o router WiFi. Estas redes se conocen como Ad hoc y, aún no siendo tan utilizadas como las anteriores, nos permiten enlazar nuestros equipos portátiles entre sí. Por ejemplo, conectar dos portátiles entre sí para intercambiar datos sin necesidad de punto de acceso, también podemos conectarnos directamente a una impresora con interfaz WiFi, o enlazar nuestro portátil a la Tablet o PDA para navegar por Internet sin cables, etc. El modo Ad hoc no es muy utilizado pero Windows nos permite configurar este tipo de redes desde su Centro de redes y recursos compartidos.

Contraseña del router.

Los routers WiFi que los PSI proporcionan tienen una contraseña por defecto para acceder a la página de gestión y configuración. Es muy recomendable cambiar dicha contraseña. Las contraseñas que vienen de fábrica pueden encontrarse por Internet con cierta facilidad. Por lo que si un atacante accede a nuestro router con la contraseña original podría realizar cambios en la configuración de nuestra red y, en el peor de los casos, cambiarnos la clave de acceso. En caso de que esto último ocurra, la solución será reiniciar el router (estos dispositivos tienen un botón que habrá que mantener pulsado durante unos segundos), para restablecer la configuración de fábrica del router (y con ella la contraseña de acceso original) y cambiar de inmediato dicha contraseña.

Los routers suelen tener una interfaz de administración vía web a través de la cual podremos cambiar su configuración y contraseña de acceso. La opción del menú donde cambiaremos la clave de acceso variará según el fabricante y modelo del router. Por ejemplo, en la siguiente imagen, para un router Comtrend modelo CT-5361, la opción está en `Management - Access Control - Passwords`. Tomaremos este modelo de enrutador inalámbrico como referencia en los siguientes apartados.

No confundas la contraseña de acceso a la configuración del punto de acceso o router WiFi con la clave de red, son conceptos distintos y por lo tanto, es muy recomendable que sean diferentes.

Clave de red y activación del cifrado seguro.

Es de vital importancia "asegurar" las comunicaciones vía WiFi, evitando que la red inalámbrica esté abierta, (accesible a todos), y además cifrar los paquetes de datos. Esto se consigue aplicando estándares de seguridad, tales como **WEP** (Wired Equivalent Privacy) y **WPA** (WiFi Protected Access). Con la activación del cifrado evitaremos numerosos ataques: dificultaremos el sniffing, la consecución ilícita de la clave de acceso a la red, la suplantación de equipos 'permitidos' y, en definitiva, el aprovechamiento fraudulento del ancho de banda de la red.

El protocolo de seguridad más antiguo en redes inalámbricas es WEP. Permite utilizar claves de 64 a 128 bits. Este tipo de cifrado es bastante inseguro, ya que actualmente existen multitud de utilidades

que rompen fácilmente la seguridad de redes con WEP. WEP codifica los datos mediante una clave de cifrado antes de enviar la información. Cuanto más longitud tenga la clave, más fuerte será el cifrado. Pero, si la clave de seguridad es estática o no cambia, es posible que un intruso persistente consiga romper la seguridad de la red WiFi. Por lo tanto, se recomienda cambiar la clave WEP frecuentemente.

Debido a la inseguridad del protocolo WEP, nos decantaremos por el estándar WPA. Este protocolo de seguridad y su variante WPA2 proporcionan una protección más fiable y robusta que su antecesor, WEP. Sin embargo, no todos los dispositivos soportan WPA, sobre todo los que son algo más antiguos, los actuales sí lo implementan. WPA emplea el cifrado de clave dinámico, lo que significa que la clave cambia constantemente. WPA aporta uno de los más altos niveles de seguridad inalámbrica para redes WiFi, es el método recomendado si el dispositivo es compatible con este tipo de cifrado. **WPA** se sirve del protocolo de integridad de claves temporales (**TKIP**) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. WPA2 es la segunda generación de WPA y está actualmente disponible en los puntos de acceso más modernos del mercado. Es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y **WPA2** es que la segunda necesita el Estándar avanzado de cifrado (**AES**) para el cifrado de los datos, mientras que WPA original emplea TKIP. Tendremos que pensar una contraseña para WPA o WPA2 que sea difícil de romper, lo aconsejable son combinaciones de caracteres alfanuméricos sin sentido, símbolos especiales y uso de mayúsculas y minúsculas. Un buen ejemplo de contraseña robusta sería:

```
p@SDw96-Ah#jQ1502@sSnG3792peEu041
```

Dentro de la configuración del punto de acceso o router WiFi localizamos la opción sobre las claves de red en '**Wireless – Security**' (la ruta dependerá de cada dispositivo, en el dispositivo Comtrend CT-5361 es la anterior). Desde ese punto activaremos el **modo de autenticación** (Open Shared, WPA, WPA2, …) y la contraseña.

Ocultar el SSID.

Dentro de Windows 7 en la opción `Ver redes inalámbricas disponibles` aparecen todas las redes a nuestro alcance lo que vemos son los SSID (Service Set Identifier) de cada red, es decir, sus nombres. Pueden existir redes no visibles. El router WiFi nos permite deshabilitar la señal WiFi de la antena, con esto evitaremos que la señal sea utilizada por terceras personas externas a nuestro hogar u organización, pero también estaremos deshabilitando la posibilidad de tener red inalámbrica para nuestros equipos (activar el parámetro 'Enable Wireless' del menú de configuración del router WiFi). Otra opción, es la de ocultar el identificador de la red (SSID). Esto se lleva a cabo ocultando el punto de acceso, de esta manera, sólo podrán acceder a la red los equipos que conozcan el SSID. Así, conseguimos que el nombre de

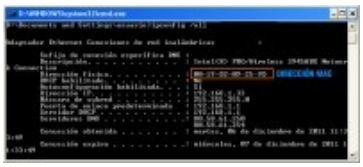
nuestra red WiFi no aparezca en el listado de redes inalámbricas disponibles (activar el parámetro 'Hide Access Point' del menú de configuración del router WiFi).

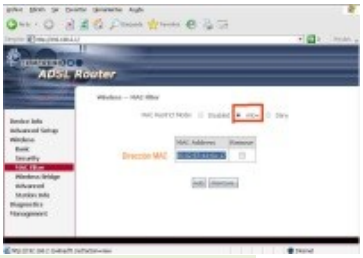
El hecho de ocultar el SSID no es muy seguro, ya que un usuario con ciertos conocimientos podría utilizar ciertas herramientas para descubrir y capturar paquetes de información de la red oculta y conseguir así su identificador.

Filtrado MAC.

A través de la configuración del router WiFi o punto de acceso podremos activar el Filtrado por direcciones MAC. Todas las interfaces de red cuentan con un número identificador único de 48 bits conocido como dirección MAC. Este número está expresado con 12 dígitos hexadecimales (cada dígito hexadecimal se representa con 4 bits).

Los puntos de acceso o routers WiFi ofrecen la posibilidad de permitir o bloquear el acceso de los equipos que quieren conectarse a la red inalámbrica según su dirección MAC. Esto se conoce como filtrado de direcciones MAC. Consiste en completar, en la configuración del punto de acceso o router WiFi, una tabla en la que aparecerán las direcciones MAC de los equipos permitidos o bloqueados en nuestra red, según nos interese. Para ello, debemos averiguar la dirección MAC de las interfaces de red ejecutando por ejemplo, ipconfig /all.





En el router Comtrend CT5361 esta opción se encuentra en `Wireless - MAC Filter`. Puede parecer un sistema bastante seguro pero tiene sus debilidades. Primero, los paquetes que se envían a los equipos con direcciones MAC permitidas viajan sin cifrar con lo que las comunicaciones son más rápidas pero también más inseguras (más fácil de interceptar e interpretar mediante un sniffer). En segundo lugar, existe la posibilidad de averiguar una dirección MAC 'permitida' y de que un atacante pueda utilizarla con su equipo haciéndose pasar por un equipo 'fiable' de la red. Este ataque se conoce como suplantación de MAC. En resumen, el filtrado puede sernos útil pero lo recomendable es emplearlo para bloquear el acceso a la red de equipos concretos, combinándolo con el cifrado de las comunicaciones mediante WPA.

Filtrado por IP y puerto.

Los puntos de acceso y routers WiFi cuentan, con frecuencia, con características de cortafuegos, permitiéndonos filtrar el tráfico por puertos y direcciones IP (IP/Port filter) . Con esta alternativa podemos identificar el origen de los paquetes de datos que atraviesan el router o punto de acceso y conseguir bloquear aquellos que pueden resultar sospechosos o peligrosos. El dispositivo que filtra los paquetes consulta una tabla con los puertos y direcciones IP, de equipos potencialmente peligrosos para saber qué hacer en cada caso. Nos puede interesar bloquear sólo los paquetes que provengan sólo de uno o varios puertos, y no de todos los puertos relacionados con una IP. Para ello, debemos conocer los puertos en los que operan los servicios o aplicaciones que queremos bloquear/permitir.

En redes inalámbricas, WPA es el acrónimo de ...

- (●) **WiFi Protected Access.**
- ( ) Wireless Protected Access.
- ( ) Wired Protected Authentication.

- WiFi Privacy Access.

TKIP, el protocolo de integridad de claves temporales se utiliza en:

- WPA2.
- WEP.
- **WPA.**
- Ninguna de las anteriores.