UNIDAD DIDÁCTICA 6

GESTIÓN DE RECURSOS EN UNA RED

MÓDULO PROFESIONAL: SISTEMAS INFORMÁTICOS

Índice

RESUMEN INTRODUCTORIO 2
INTRODUCCIÓN 2
CASO INTRODUCTORIO 3
1. PERMISOS Y DERECHOS. PERMISOS DE RED. PERMISOS LOCALES. HERENCIA. LISTAS DE CONTROL DE ACCESO 4
2. CONFIGURACIÓN DE RECURSOS COMPARTIDOS. PERMISOS DE ACCESO Y DIRECTIVAS DE SEGURIDAD 6
3. REQUISITOS DE SEGURIDAD DEL SISTEMA Y DE LOS DATOS. SEGURIDAD A NIVEL USUARIOS Y SEGURIDAD A NIVEL EQUIPOS. DERECHOS DE USUARIOS. DIRECTIVAS DE SEGURIDAD. OBJETOS DE DIRECTIVA. ÁMBITO DE LAS DIRECTIVAS. PLANTILLAS 25
3.1 Seguridad a nivel de usuarios y equipos 28
3.1.1 Uso de un cortafuegos 28
3.1.2 Uso de un antivirus 30
3.1.3 Uso de protección contra spyware 31
3.1.4 Actualización automática del sistema operativo 32
3.1.5 Instalación de la última versión del navegador 32
3.1.6 Activación de las características de seguridad del navegador 33
3.1.7 Uso de una cuenta de usuario estándar 34
4. SERVIDORES DE FICHEROS. SERVIDORES DE IMPRESIÓN. SERVIDORES DE APLICACIONES 36
4.1 Servidor de ficheros o archivos 36
4.2 Servidor de impresión 38
4.3 Servidor de aplicaciones 41
5. TÉCNICAS DE CONEXIÓN REMOTA 45
5.1 Herramientas de escritorio remoto 45
5.2 Herramientas para compartir pantalla 48
5.3 Acceso remoto por consola 49
6. UTILIDADES DE SEGURIDAD BÁSICA. HERRAMIENTAS DE CIFRADO, HERRAMIENTAS DE ANÁLISIS Y ADMINISTRACIÓN, CORTAFUEGOS Y SISTEMAS DE DETECCIÓN DE INTRUSOS 51
6.1 Utilidades de seguridad básica 51
6.1.1 Herramientas de cifrado 51
6.1.2 Herramientas de análisis y administración 53
6.1.3 Sistemas de detección de intrusos 55
7. IMPLANTACIÓN Y EXPLOTACIÓN DE DOMINIOS 59
RESUMEN FINAL 62

RESUMEN INTRODUCTORIO

A lo largo de esta unidad revisaremos las principales funciones de una red de ordenadores, centrándonos en la que sin duda es su utilidad más destacada: compartir recursos. Veremos cómo se pueden compartir desde archivos hasta aplicaciones, pasando por impresoras o el acceso a Internet.

También, presentaremos un concepto básico en los sistemas en red, el modelo cliente/servidor. Y veremos de forma práctica el modo de compartir recursos tanto en sistemas operativos libres como propietarios.

A continuación, estudiaremos distintas posibilidades de acceder de forma remota a nuestros dispositivos, y veremos las grandes ventajas que supone el poder administrar un equipo sin estar presente físicamente delante de él.

Por último, nos centraremos en los aspectos de seguridad en redes de ordenadores, algo que como veremos resulta vital en un mundo conectado como el nuestro, en el que las posibilidades de que alguien intente acceder a nuestros dispositivos con propósitos maliciosos son cada vez más elevadas.

INTRODUCCIÓN

En la unidad anterior se revisaron las técnicas y herramientas para conectar un conjunto de dispositivos formando una red. Lógicamente eso nos permitió entrever las grandes ventajas que iba a aportarnos esta interconexión de nuestros equipos una vez establecida. Pero en realidad no llegamos a ver de forma práctica de qué modo se puede sacar partido de una red de ordenadores.

A esto nos dedicaremos en la unidad actual, en la que revisaremos cómo se gestiona dicha red una vez que está creada: qué operaciones se pueden realizar sobre ella, cómo se configura el acceso a sus diferentes recursos, cómo proteger dichos recursos para garantizar su seguridad…

Todos estos son conceptos básicos para un desarrollador ya que, como se ha comentado en unidades anteriores, hoy en día prácticamente no se concibe una aplicación que no implique alguna forma de conexión y de compartición de recursos entre sus usuarios.

CASO INTRODUCTORIO

La empresa en la que trabajas ha obtenido un contrato para realizar la gestión de los sistemas informáticos de una importante cadena de supermercados. Como responsable del departamento de informática de la empresa y experto en sistemas informáticos, serás el encargado de realizar el despliegue de la aplicación a medida que se va a desarrollar para dicha cadena, y de su mantenimiento posterior. Tras una primera fase de trabajo presencial en el cliente, la idea es que todas estas tareas se desarrollen de forma remota para evitar desplazamientos continuos.

Al finalizar la unidad distinguirás las principales funciones de una red de ordenadores y sabrás cómo se configuran y gestionan, conocerás los servidores de impresión, archivos y aplicaciones, serás capaz de acceder de forma remota a un dispositivo seleccionando las herramientas adecuadas para ello, y utilizarás herramientas básicas de seguridad en red.

1. PERMISOS Y DERECHOS. PERMISOS DE RED. PERMISOS LOCALES. HERENCIA. LISTAS DE CONTROL DE ACCESO

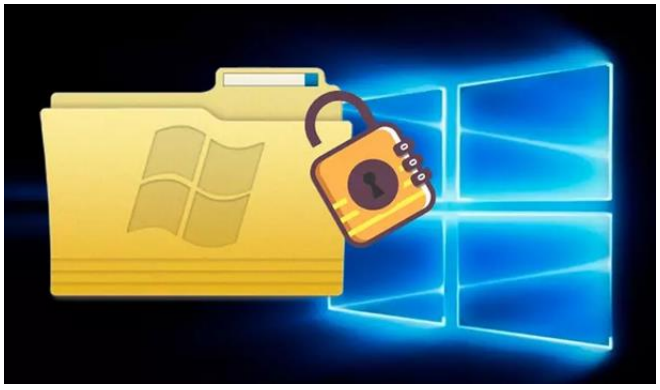
El primer paso para el desarrollo del nuevo sistema informático en el que estás trabajando, va a ser establecer la política de acceso a la red, mediante el estudio de los permisos y derechos de los usuarios, así como el nivel de acceso, los casos que se hereden y el establecimiento de mecanismos como las listas de control.

A la hora de establecer el control sobre una red de ordenadores, debemos tener en cuenta los conceptos permiso y derecho, en el sentido de que en el caso de permiso se considera sobre un recurso concreto, bien sea archivo, carpeta, etc., del propio sistema y que puede concederse o denegarse el acceso al mismo sobre un usuario concreto o grupo de usuarios. A la vez que establecer su nivel de acceso sobre el recurso como es lectura, ejecución, modificación, etc.

Podemos diferencia entre dos tipos de permisos:

- Permisos de red, relativos al acceso de un usuario a un sistema o red que le permitirá acceder a un recurso de la misma, con un nivel de manipulación que también debe ser asignado.

- Permisos locales, son los que se establecen para las carpetas (directorios) y archivos (ficheros) que contiene una red.



Permisos de carpeta.
Fuente: https://www.adslzone.net/esenciales/windows-10/cambiar-permisos-archivo-carpeta/

En el caso del otro concepto, el derecho, es el atributo que se otorga al usuario o grupo, de modo que le faculta para poder realizar distintas acciones sobre el propio sistema, no ya sólo sobre un recurso. Suelen venir los derechos determinados por defecto sobre el grupo o usuario, como ocurre en el caso de Windows.

Herencia.

Cuando se asocian permisos a determinados recursos, hay que tener en cuenta que por defecto los permisos son heredados, por ejemplo, en el caso de una carpeta o lugar de ubicación, sin contar con permisos otorgados de manera explícita sobre ese recurso en concreto.

Existe la posibilidad de incluir nuevos permisos, además de los heredados, si el usuario posee control total sobre el recurso.

Podemos distinguir dos niveles a la hora de ejercer el control sobre la herencia de permisos, pudiendo determinar, por ejemplo, los objetos y permisos que se van a heredar.

De este modo, en cada recurso, como carpeta o archivo, puede decidirse si se heredarán los permisos de la carpeta padre. O, definir de manera explícita qué recursos son los que van a heredar unos permisos determinados, incluso combinar entre heredados y asignados.

Habrá que tener en cuenta que, en el caso de creación de nuevas carpetas, por ejemplo, si se realiza como copia de una existente, la lista de permisos explícitos estará vacía, pero sí tendrá los permisos heredados de la carpeta de origen.

En el caso de Windows, es curioso que, si la acción consiste en mover una carpeta dentro del mismo volumen NFTS, el comportamiento es que la herencia queda desactivada de manera automática y sólo mantendrá los permisos explícitos. Pero si la copia tiene como destino un volumen o partición distinta, su comportamiento es idéntico al caso de una copia de carpeta, manteniendo únicamente los permisos heredados de la carpeta padre.

Lista de control de acceso.

En el caso de Windows, son atributos de protección de recursos que se utilizan en el caso de archivos NFTS, además del SID del propietario.

Podemos distinguir entre dos tipos de listas de control de acceso:

- ACL, lista de control de acceso de protección, en la que se incluyen los permisos que los usuarios tienen sobre el recurso (carpeta o archivo). Puede contar con un número de entradas indefinido, donde cada una de ellas concede o deniega un conjunto de permisos a un grupo o usuario.

Este tipo de lista de control está compuesta a su vez por otros dos tipos de lista de control de acceso discrecional (DACL), donde cada elemento es considerado una entrada de control de acceso (ACE), empleado en unir el SID de usuario o grupo con el permiso o conjunto de permisos, concedido o denegado. Y, que por tanto, existirán una DACL heredada y otra DACL explícita, en función de los permisos que contengan.

- SACL, lista de control de acceso de seguridad, donde se definen las acciones que se realizan sobre el recurso, de manera que quedan auditadas por el propio sistema, registrando el usuario, la acción y el recurso sobre el que se ha realizado.

2. CONFIGURACIÓN DE RECURSOS COMPARTIDOS. PERMISOS DE ACCESO Y DIRECTIVAS DE SEGURIDAD

En la nueva red que vais a implementar, te han encargado que configures todos los recursos compartidos que van a ser incluidos en ella, teniendo en cuenta los usuarios y grupos que pueden acceder a los recursos compartidos y deberás aplicar la política de seguridad establecida.

Lo primero que se puede preguntar un usuario cuando se plantea la posibilidad de utilización de una red, es saber cómo va a mejorar su trabajo en el ordenador al utilizar dicho entorno. La respuesta va a ser diferente según el tipo de trabajo que desempeñe. Pero, de forma general, se puede establecer que una red proporciona la facilidad de compartir recursos entre sus usuarios. Esto significa que:

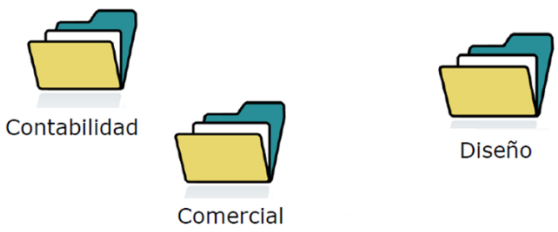
- Se pueden aprovechar las prestaciones cliente/servidor.
- Supone compartir ficheros.
- Supone compartir impresoras.
- Se puede acceder a sistemas de comunicación global (como Internet).
- Se pueden utilizar aplicaciones específicas de red.

En la configuración de recursos compartidos tendremos en cuenta los permisos de acceso y directivas de seguridad, en los distintos recursos, que detallamos a continuación:

1. Compartir ficheros.

La posibilidad de compartir ficheros es la prestación principal de las redes de ordenadores. Por ejemplo, en una red local se puede acceder a ficheros de otros usuarios sin necesidad de utilizar dispositivos de almacenamiento auxiliares, como un pendrive. Mediante la red, se puede disponer de directorios compartidos a los que tengan acceso un grupo de usuarios, y en los que se puede guardar la información que compartan dichos grupos.

Pensemos en una empresa que podría crear una carpeta para el departamento de contabilidad, otra para el departamento comercial y otra para el departamento de diseño, facilitando que los usuarios de estos departamentos tengan acceso a la información que les interesa de forma instantánea.



Carpetas compartidas mediante una red.

2. Compartir impresoras.

Las redes permiten que sus usuarios puedan acceder a impresoras de calidad y alto precio sin que suponga un desembolso prohibitivo. Por ejemplo, si tenemos una oficina en la que trabajan siete personas y sus respectivos ordenadores no están conectados mediante una red local, o bien compramos una impresora para cada usuario (en total siete), o bien cada usuario deberá grabar en un pendrive su documento a imprimir y llevarlo a donde se encuentra físicamente la impresora. Obviamente, en el primer caso los costes aumentan de forma significativa; y en el segundo la productividad del trabajador se reduce al tener que dedicar un tiempo significativo a desplazarse de un equipo a otro cada vez que desee imprimir un documento.

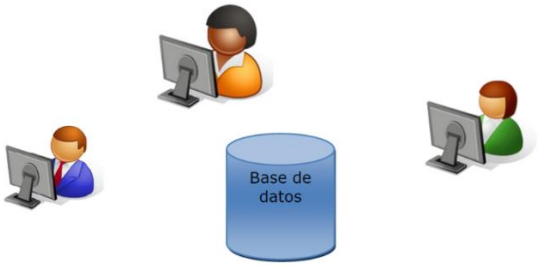
En cambio, si la empresa dispone de una red local, bastará con comprar una o dos impresoras de calidad y hacer que los usuarios puedan acceder a ellas a través de la red.

Impresora compartida en red.

3. Compartir aplicaciones.

Existe un gran número de aplicaciones que utilizan las redes de ordenadores para que el trabajo sea más provechoso. Un ejemplo claro son los programas de correo electrónico. Un programa de correo electrónico permite el intercambio de mensajes entre los usuarios. Los mensajes pueden consistir en texto, sonido, imágenes, etc. y llevar asociados cualquier tipo de ficheros binarios.

Otro ejemplo habitual en cualquier empresa serían las aplicaciones de bases de datos preparadas para el trabajo en red (la mayoría de las actuales), que permiten que varios usuarios puedan acceder de forma simultánea a los registros de la base de datos, y que las actualizaciones que realice un operador queden inmediatamente disponibles para el resto de los usuarios.



Base de datos en red.

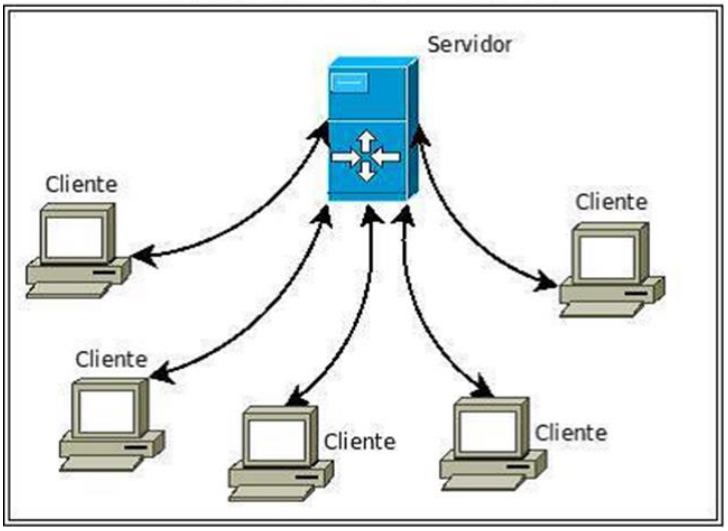
4. Compartir el acceso a internet.

Es una de las prestaciones que con el tiempo está ganando peso específico. Consiste en la posibilidad de configurar un ordenador con una conexión permanente a servicios en línea externos, de forma que los usuarios de la red local no necesiten utilizar un dispositivo propio para acceder a dichos servicios. El ejemplo más de moda es el acceso a Internet.

5. Modelo Cliente/Servidor.

Un concepto importante cuando se comparten recursos mediante una red es el de Cliente/Servidor. La idea de este modelo es dividir el trabajo en dos partes: una parte cliente (normalmente más ligera) que se realiza en el ordenador del usuario y otra parte servidor (que requiere mayor carga de trabajo) que se realiza en un ordenador destinado específicamente a ella (un servidor). De este modo se consigue:

- Aliviar la carga de trabajo del ordenador cliente.
- Reducir el tráfico de la red.



Modelo Cliente/Servidor.

Por ejemplo, si tuviésemos un ordenador que tiene instalada una base de datos de clientes compartida, pero que no emplease el modelo cliente/servidor, cuando un usuario de dicha base de datos quisiera hacer, desde otro equipo, una selección de los clientes mayores de 30 años se debería leer al equipo del usuario todos los registros de la base de datos para comprobar cuáles cumplen la condición. Esto supone un elevado tráfico en la red.

En cambio, si la base de datos estuviera implementada siguiendo el modelo cliente/servidor, una consulta como esta se enviaría al servidor, que realizaría la selección de registros y devolvería solo los campos que le interesan al usuario. Se reduce así considerablemente el tráfico en la red y el ordenador cliente se encuentra con el trabajo hecho. El sistema en sí resulta bastante más rápido, aunque a cambio requiere que los servidores tengan mejores prestaciones.

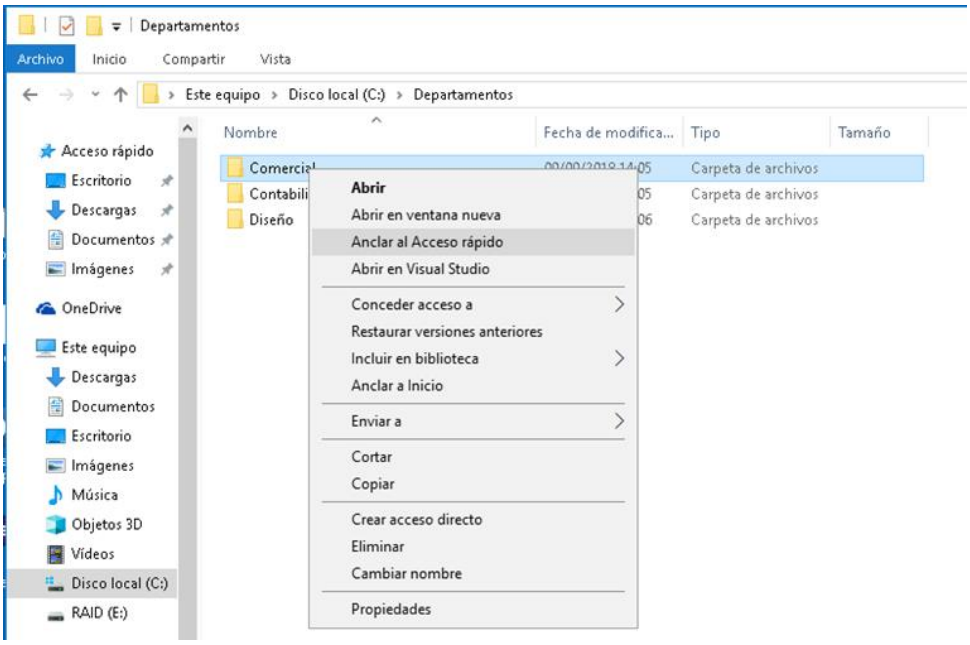
6. Compartir ficheros en sistemas operativos libres y propietarios.

A continuación, vamos a describir el modo de compartir ficheros tanto en sistemas operativos libres como propietarios.

a) En sistemas propietarios.

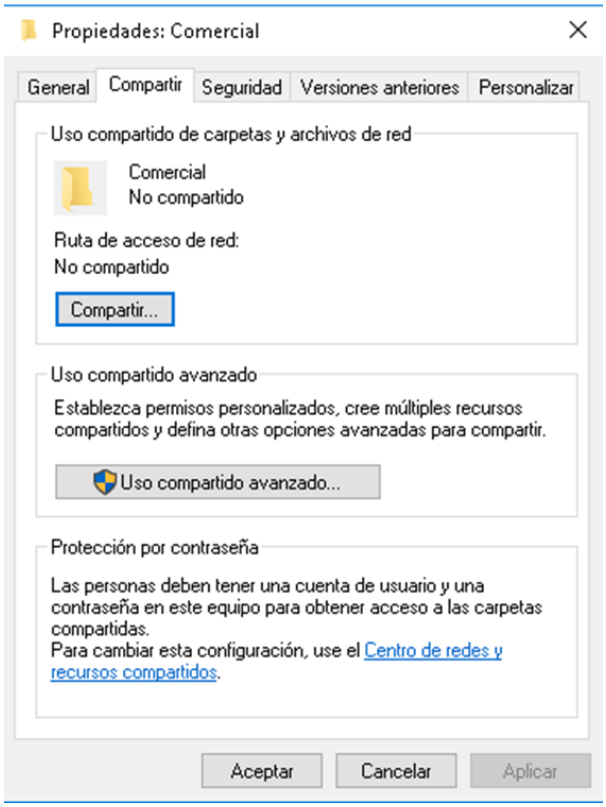
El proceso es muy parecido al empleado en la asignación de permisos locales para el acceso de los usuarios a carpetas y archivos, a la hora de compartir estos mismos recursos en red.

Para compartir un recurso (una carpeta en este caso) en Windows, debemos acceder a sus Propiedades.



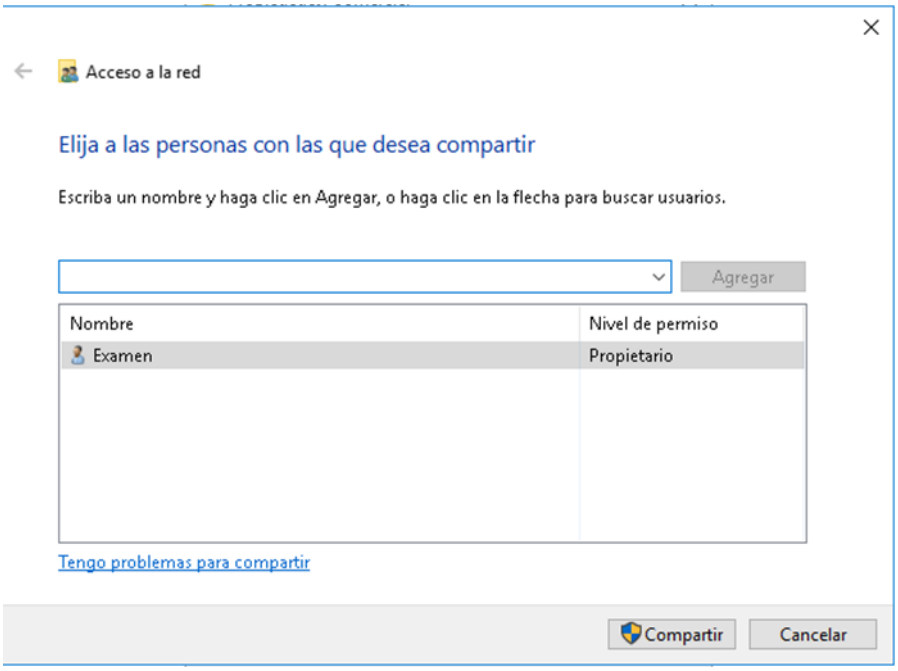
Propiedades de una carpeta.

En la ventana de Propiedades, ya conocida, se debe seleccionar en este caso la pestaña Compartir.



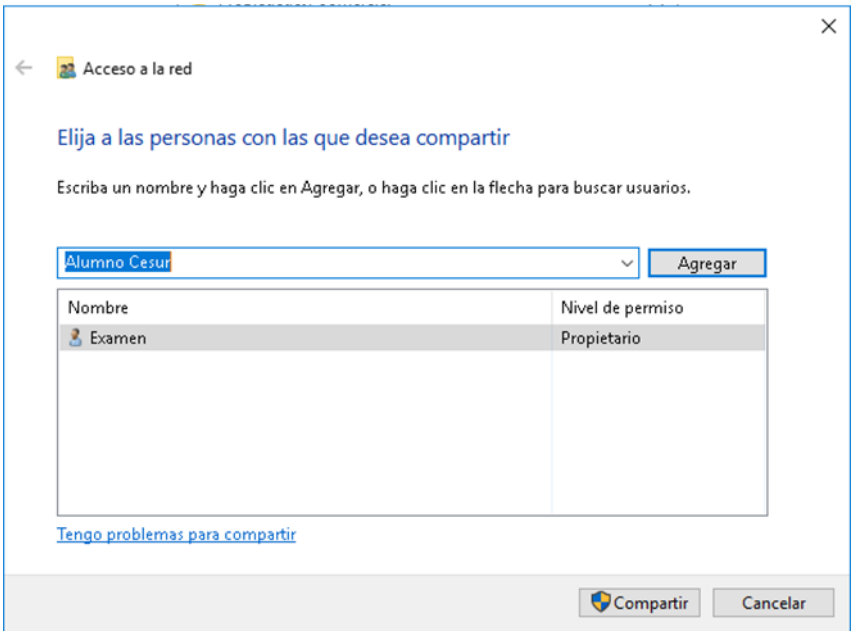
Propiedades de compartición.

Por defecto los archivos y carpetas no están compartidos, así que si queremos que nuestra carpeta lo esté se hará uso del botón Compartir.



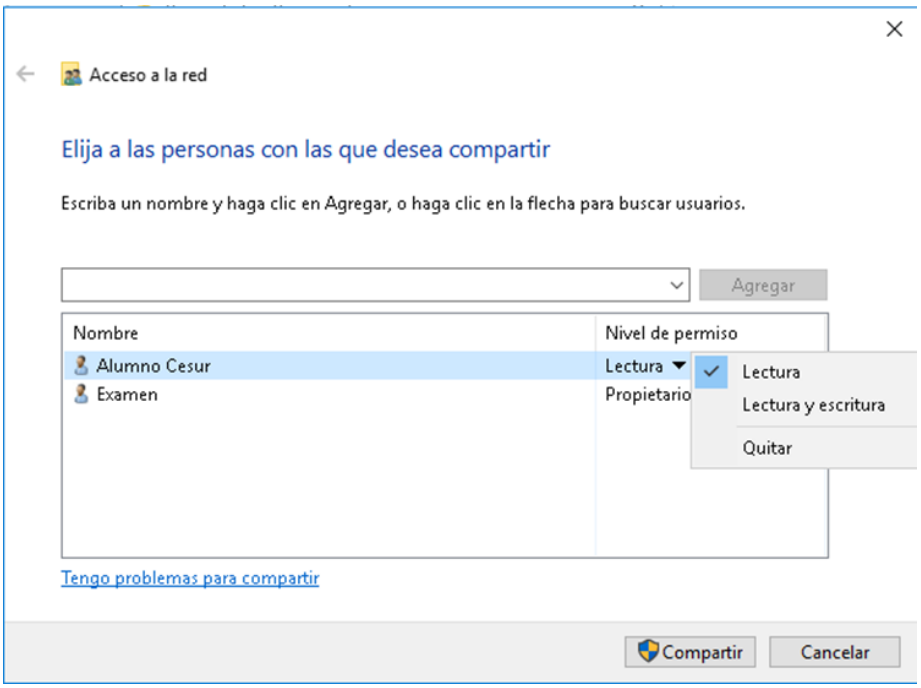
Compartir acceso a una carpeta.

Como se ve en la imagen anterior, el propietario de la carpeta, en este caso el usuario Examen, ya tiene permiso para acceder a dicha carpeta desde la red. Vamos a agregar a un nuevo usuario de los existentes en nuestro sistema, concretamente Alumno Cesur. Para ello lo seleccionamos en el desplegable y pulsamos Agregar.



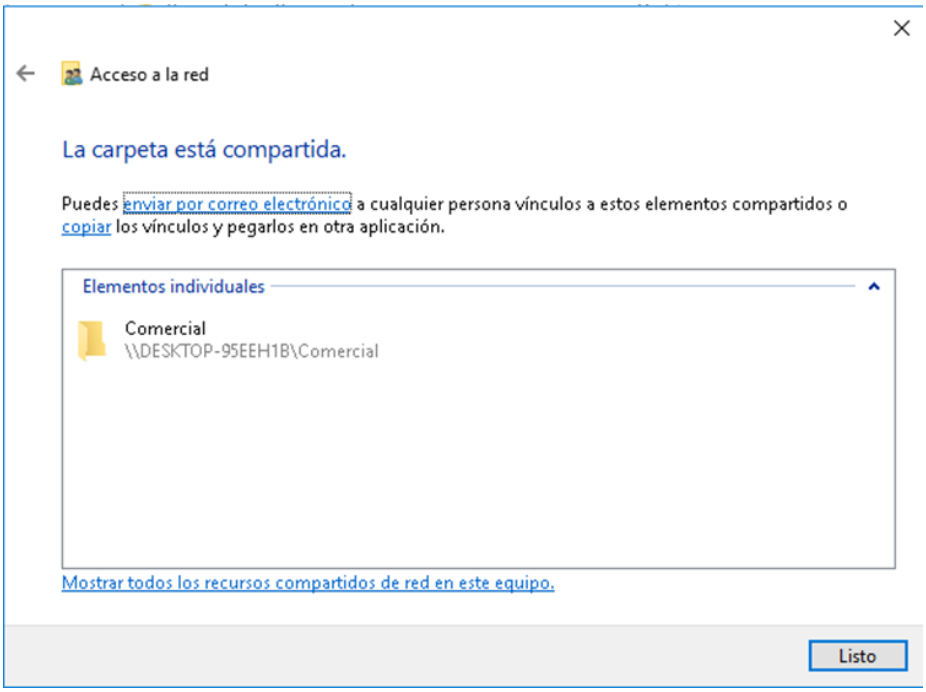
Selección del usuario para compartir.

Añadido el usuario, se pueden escoger para él los permisos que se le desean conceder cuando acceda a este recurso. Por defecto sólo se concede permiso de Lectura, pero en el desplegable se puede seleccionar también Lectura y escritura.



Asignación de permisos.

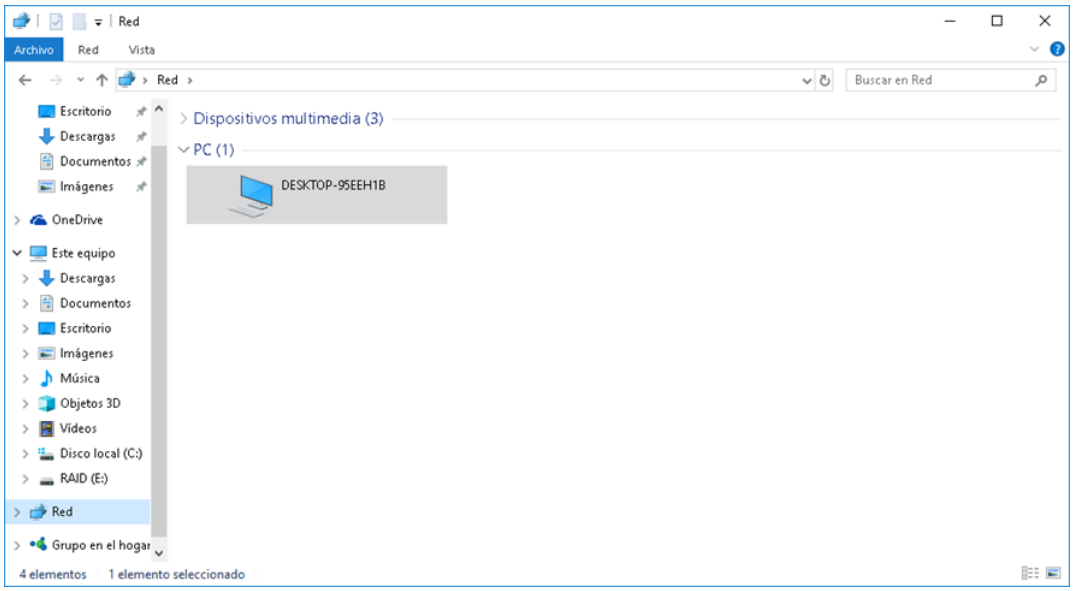
Se mantiene el permiso de Lectura y se pulsa en Compartir. Terminado el proceso se nos indicará que la carpeta ya está compartida en red, así como la dirección para acceder a ella de forma directa.



Carpeta compartida en red.

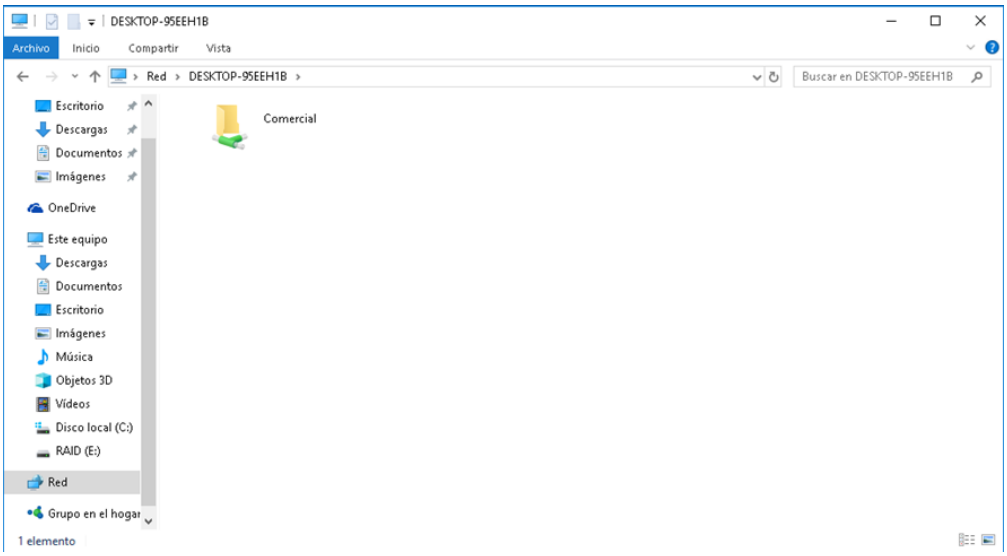
Desde este momento la carpeta Comercial puede ser accedida desde cualquier otro equipo conectado a la red. Eso sí, siempre que el acceso lo realice uno de los usuarios a los que hemos concedido permiso para ello.

Lo comprobamos accediendo desde un equipo diferente con el usuario Examen, que por ser el propietario de la carpeta tiene todos los permisos sobre ella. Para acceder mediante la red a las carpetas compartidas, utilizamos, igual que si se tratasen de directorios locales, el Explorador de Windows. Sólo que en este caso se elige la opción Red, que aparece en la parte inferior del listado de unidades del marco izquierdo. Aparece un solo equipo (que es justamente el que contiene la carpeta compartida) conectado en red con el actual.



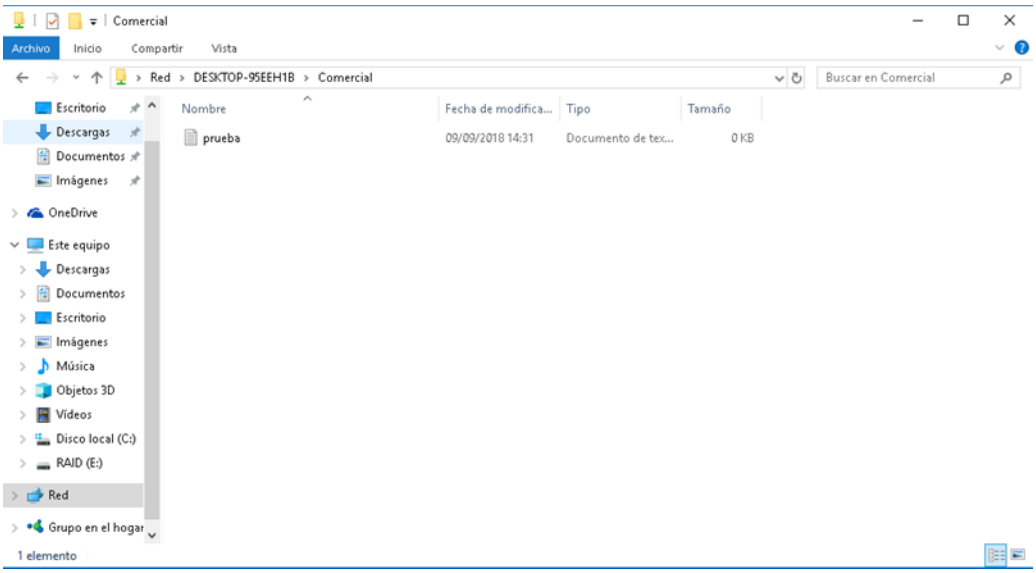
Acceso a un equipo a través de Red.

Se abre este equipo, y se visualizan sus carpetas compartidas, Comercial en este caso. Como puede apreciarse en la siguiente imagen, el icono de esta carpeta, por el hecho de estar compartida, es ligeramente diferente al de las carpetas locales. De ese modo se puede distinguir de forma visual.



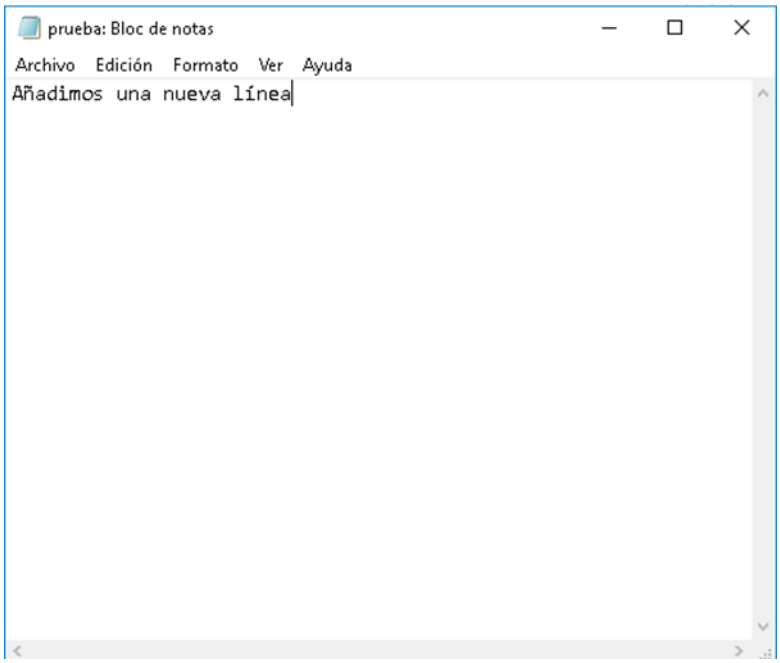
Carpeta compartida en red.

Si se abre la carpeta compartida, puede verse que se puede acceder a su contenido con normalidad, como si de una carpeta local se tratase. Hay que recordar que el usuario que está realizando todo este proceso es Examen, el propietario de la carpeta.



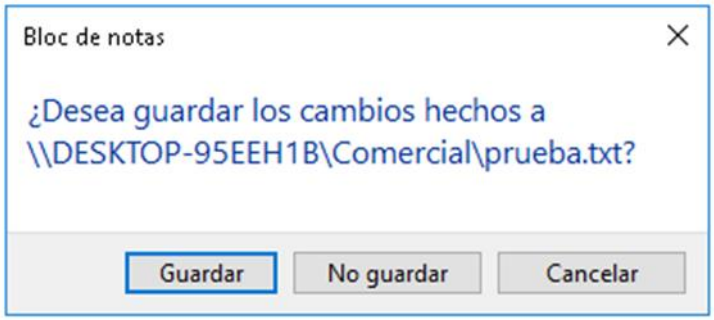
Contenido de la carpeta compartida.

Este usuario no sólo puede abrir la carpeta para ver su contenido, sino también acceder a los archivos que contiene. En este caso se trata de un documento de texto vacío. ¿Qué ocurre si se intenta escribir nuevo contenido en el documento de texto, por ejemplo añadiendo una línea?



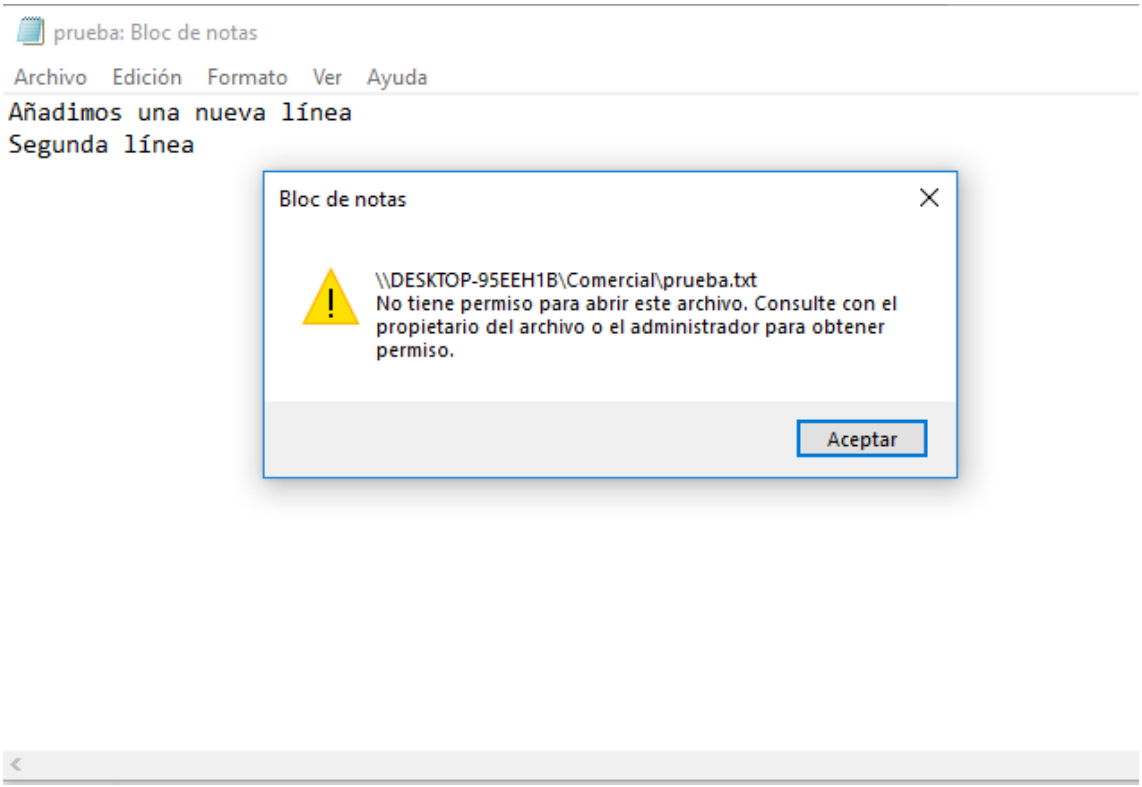
Adición de una línea al documento de texto compartido.

Ningún problema, al cerrar el archivo simplemente se nos pregunta si deseamos guardar los cambios realizados. Confirmamos y el archivo queda actualizado.



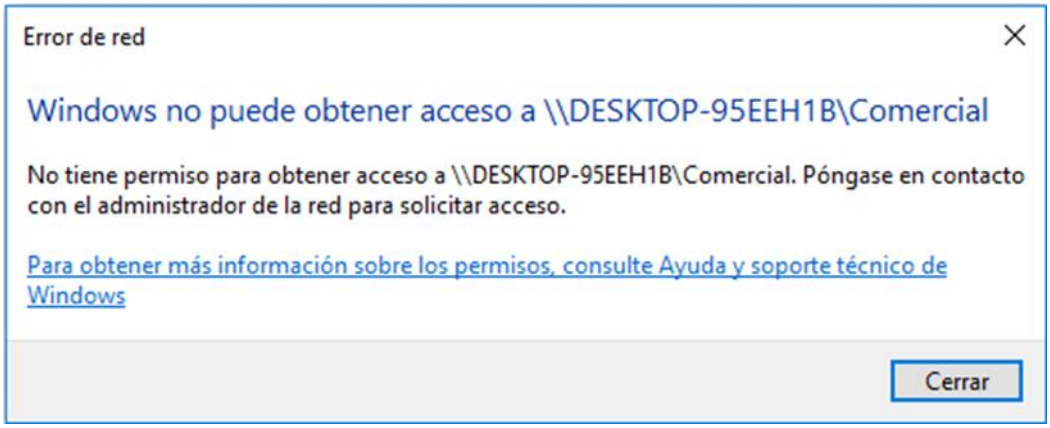
Cambios guardados en el archivo compartido.

En cambio, si se intenta realizar el mismo proceso con el usuario Alumno Cesur, al que, recordemos, se han asignado permisos sólo de Lectura, el resultado sería diferente. También se podría acceder a la carpeta compartida, igualmente mediante la opción Red del Explorador de Windows. Pero a la hora de realizar un cambio sobre el documento de texto contenido en la carpeta, por ejemplo, añadirle una nueva línea, se obtendría un error dado que este usuario no tiene permiso de Escritura.



Error en el guardado al no tener permisos de escritura.

Cualquier otro usuario que no sea uno de los autorizados a acceder a esta carpeta podría llegar a visualizarla mediante el Explorador de Windows, accediendo a su Red. Pero no podría ni siquiera leer el contenido de la carpeta.



Error obtenido al no ser un usuario con acceso a la carpeta.

b) En sistemas libres

Un ejemplo lo tenemos en el caso de Linux, concretamente con NFS (Network File System o *Sistema de archivos de red)*, es un protocolo de nivel de aplicación, si tomamos con referencia el modelo OSI. Se utiliza en sistemas de archivos distribuidos en un entorno de red local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales. Originalmente fue desarrollado en 1984 por Sun Microsystems, con el objetivo de que fuera independiente de la máquina, el sistema operativo y el protocolo de transporte. El protocolo NFS está incluido por defecto en los Sistemas Operativos UNIX y la mayoría de distribuciones Linux.

Características de NFS:

- El sistema NFS está dividido al menos en dos partes principales: un servidor y uno o más clientes. Los clientes acceden de forma remota a los datos que se encuentran almacenados en el servidor.

- Las estaciones de trabajo locales utilizan menos espacio de disco debido a que los datos se encuentran centralizados en un único lugar pero pueden ser accedidos y modificados por varios usuarios, de tal forma que no es necesario replicar la información.

- Los usuarios no necesitan disponer de un directorio “home” en cada una de las máquinas de la organización. Los directorios “home” pueden crearse en el servidor de NFS para posteriormente poder acceder a ellos desde cualquier máquina a través de la infraestructura de red.

- También se pueden compartir a través de la red dispositivos de almacenamiento como disqueteras, CD-ROM o DVD. Esto puede reducir la inversión en dichos dispositivos y mejorar el aprovechamiento del hardware existente en la organización.

Todas las operaciones sobre ficheros son síncronas. Esto significa que la operación sólo retorna cuando el servidor ha completado todo el trabajo asociado para esa operación. En caso de una solicitud de escritura, el servidor escribirá físicamente los datos en el disco, y si es necesario, actualizará la estructura de directorios, antes de devolver una respuesta al cliente. Esto garantiza la integridad de los ficheros.

ENLACE DE INTERÉS

Accede a esta web para conocer más información acerca de la instalación y configuración de un servidor NFS:

VÍDEO DE INTERÉS

Aquí podrás visualizar cómo compartir carpetas en Windows 10.

Por otro lado, es bastante habitual que en una red de ordenadores convivan dispositivos que trabajan tanto con sistemas operativos Windows como Linux. Y también en estos casos es necesario poder compartir información entre ellos. Para ello se dispone de un protocolo llamado SAMBA, que es una implementación del protocolo SMB.

SMB.

Server Message Block o SMB es un protocolo de red que, como en el caso de NFS, correspondería a la capa de aplicación en el modelo OSI. Permite compartir recursos entre nodos de una red. Es utilizado principalmente en ordenadores con sistemas operativos Windows.

SMB fue originalmente presentado por IBM, pero la versión más común hoy en día es la modificada ampliamente por Microsoft, que renombró SMB a **Common Internet File System** (CIFS) en 1998 y añadió más características, incluyendo soporte para enlaces simbólicos, enlaces duros (*hard links*), y mayores tamaños de archivo.

Hay características en la implementación de SMB de Microsoft que no son parte del protocolo SMB original.

SAMBA.

Samba es una implementación libre del protocolo SMB, creado para sistemas de tipo UNIX. De esta forma, es posible que computadoras con sistemas operativos GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows.

Samba, por tanto, configura directorios Unix y GNU/Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows estos recursos aparecen como carpetas normales de red. Los usuarios de GNU/Linux pueden montar en sus sistemas de archivos estas unidades de red como si fueran dispositivos locales, o utilizar la orden smbclient para conectarse a ellas, al estilo del cliente de la línea de órdenes ftp.

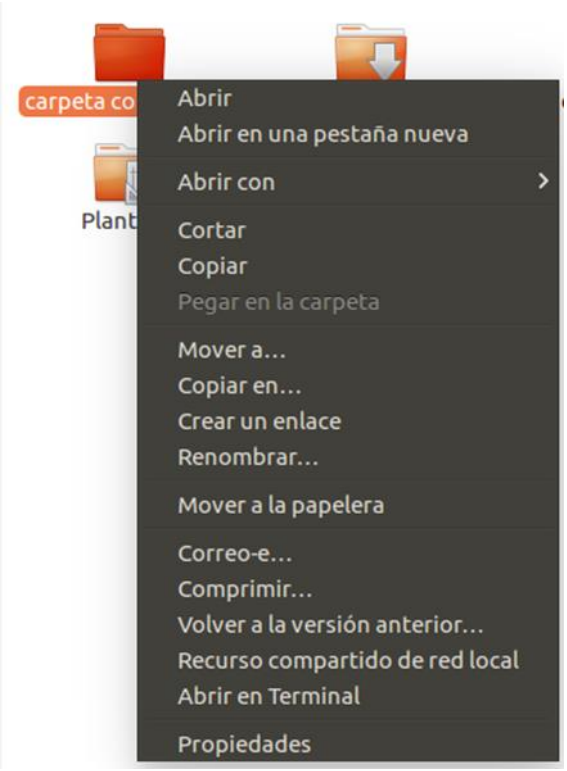
Cada directorio puede tener diferentes permisos de acceso superpuestos a las protecciones del sistema de archivos que se esté usando en GNU/Linux. Por ejemplo, las carpetas *home* pueden tener permisos de lectura y escritura para cada usuario, permitiendo que cada uno acceda a sus propios archivos; sin embargo, deberemos cambiar los permisos de los archivos localmente para dejar al resto ver nuestros archivos, ya que con dar permisos de escritura en el recurso no será suficiente.

A continuación, se va a describir de forma práctica cómo realizar esta compartición de archivos entre un sistema Ubuntu (que ha simplificado bastante el proceso de configuración de Samba) y uno Windows. Como se verá, el proceso es bastante similar al ya visto de compartición de ficheros en Windows.

En el equipo Ubuntu se dispone de una carpeta que se desea compartir.

Carpeta para compartir en Ubuntu.

Se pulsa sobre ella con el botón derecho y se elige la opción “Recurso compartido de red local”.



Conversión de la carpeta en recurso compartido.

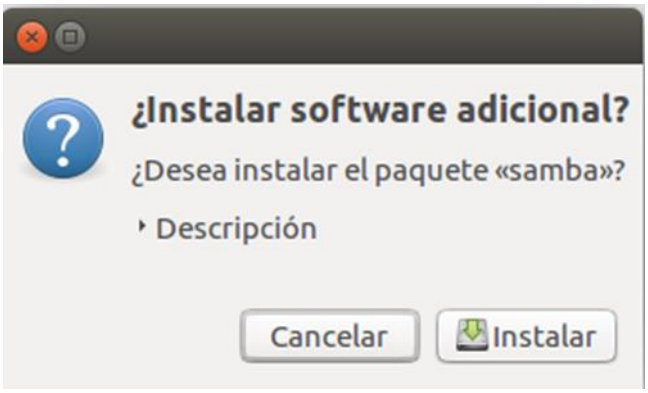
Se accede a la ventana que permite compartir la carpeta.

Compartición de la carpeta.

Al pulsar la casilla "Compartir esta carpeta", si es la primera vez que intentamos compartir un recurso en este sistema, Ubuntu nos mostrará un aviso al respecto y nos permitirá realizar la instalación de Samba en este mismo instante. Esto, como decíamos anteriormente, simplifica el proceso de forma significativa.

Aviso para proceder a la instalación de Samba.

Se elige "Instalar el servicio" y se obtiene un nuevo aviso que nos indica explícitamente que se va a proceder a instalar el paquete Samba



Aviso de instalación del paquete Samba.

Se pulsa Instalar, y una vez aplicados todos los cambios necesarios, y reiniciada la sesión, la instalación de Samba está completa y se puede utilizar el servicio de compartición de archivos.

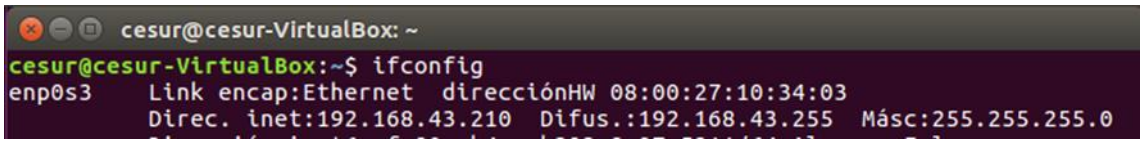
Se repiten los pasos anteriores para compartir la carpeta, y como puede verse en la siguiente imagen en este caso ya sí podemos configurar la compartición.

Configuración del acceso compartido.

Se crea la compartición, y la carpeta estará lista para ser accedida a través de la red, lo que ilustra el cambio en su icono.

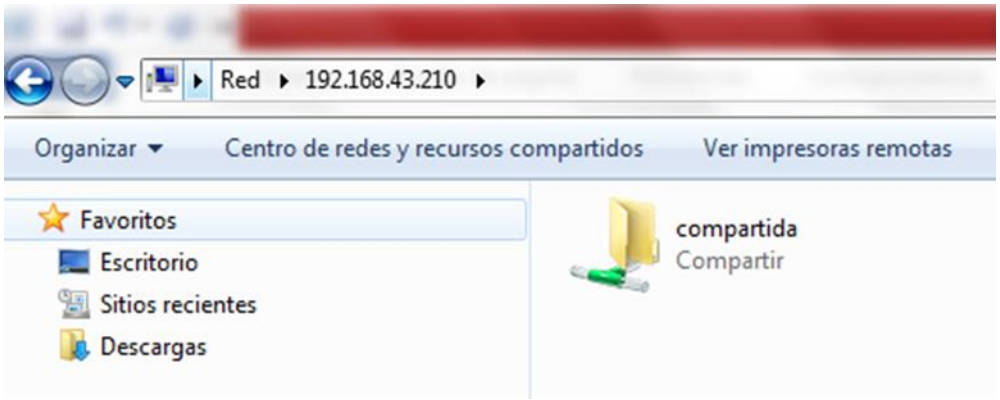
Icono para una carpeta compartida.

Para acceder a la carpeta desde Windows, vamos a emplear un método alternativo al visto en el apartado 2.1. Vamos a acceder de forma directa al equipo Ubuntu a través de su dirección IP. Recordemos que se puede consultar dicha dirección con Ifconfig.



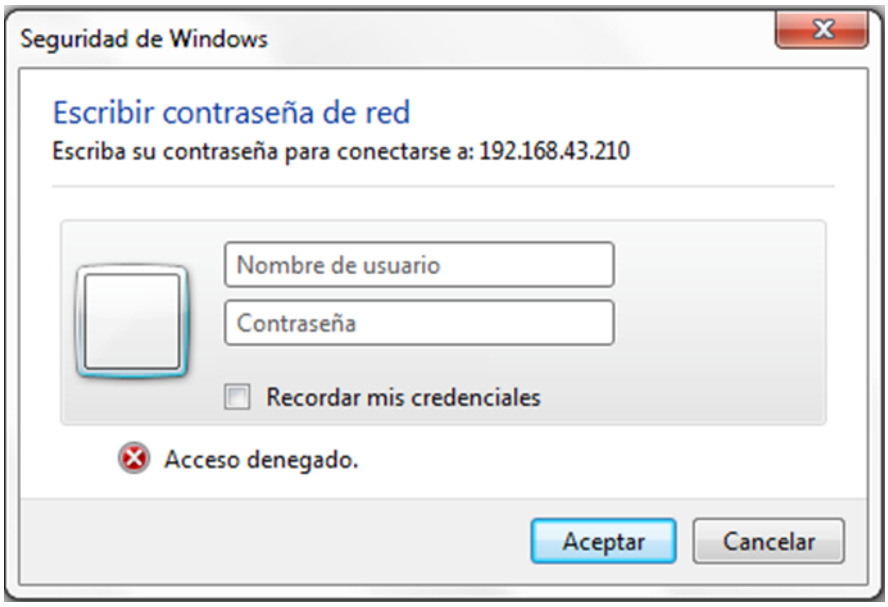
Consulta de la dirección IP del equipo Ubuntu.

Ahora, en la barra de direcciones del Explorador del equipo Windows se escribe esta dirección IP, precedida por \\, y como se aprecia en la siguiente imagen tendremos acceso a la carpeta compartida.



Acceso a la carpeta compartida en Ubuntu desde Windows.

Como es lógico, al tratar de acceder a la carpeta se nos pedirá identificación. Hay que recordar que en el sistema Windows hemos iniciado sesión con un usuario distinto al del sistema Ubuntu. Habrá que identificarse con los datos del usuario Ubuntu para poder acceder.



Autentificación del usuario.

Una vez autentificado el usuario de manera correcta, podrá acceder a la carpeta compartida de forma remota.

ENLACE DE INTERÉS

Accede a esta web para conocer cómo se instala y configura Samba:

3. REQUISITOS DE SEGURIDAD DEL SISTEMA Y DE LOS DATOS. SEGURIDAD A NIVEL USUARIOS Y SEGURIDAD A NIVEL EQUIPOS. DERECHOS DE USUARIOS. DIRECTIVAS DE SEGURIDAD. OBJETOS DE DIRECTIVA. ÁMBITO DE LAS DIRECTIVAS. PLANTILLAS

En el tema de seguridad de la red, debes tener en cuenta todos los requisitos previos para su protección, de modo que garantice la seguridad a todos los niveles, usuario y equipos. Es necesario que conozcas las directivas de seguridad a aplicar, sus ámbitos y objetivos.

La evolución de la computación y de las comunicaciones en las últimas décadas ha hecho más accesibles a los sistemas informáticos, pero a su vez ha incrementado los riesgos vinculados a la seguridad.

La **vulnerabilidad** de las comunicaciones de datos es un aspecto clave de la seguridad de los sistemas informáticos. La importancia de este aspecto es cada vez mayor debido a la proliferación de las redes de computadoras.

El nivel de criticidad y de confidencialidad de los datos administrados por los sistemas informáticos es cada vez mayor. Por ejemplo, correo personal, transferencia de fondos, control de sistemas de armas, control de tráfico aéreo, control de implantes médicos (marcapasos, etc.). Por otro lado, los sistemas deben funcionar ininterrumpidamente y sin problemas.

El sistema operativo, como administrador de los recursos del sistema, cumple una función muy importante en la instrumentación de la seguridad. Pero no engloba a todos los aspectos de la seguridad, debiendo ser complementado con medidas externas.

La simple seguridad física, local, resulta insuficiente ante la posibilidad, como hemos visto en el apartado anterior, de acceso mediante equipos remotos conectados.

ENLACE DE INTERÉS

Aquí encontrarás más información sobre la seguridad física de sistemas informáticos:

La tendencia es que los sistemas sean más asequibles y fáciles de usar, pero esa ventaja para el usuario puede implicar un aumento de la vulnerabilidad. Así que se deben identificar las amenazas potenciales, que pueden proceder de fuentes maliciosas o no.

Lógicamente, el nivel de seguridad a proporcionar depende del valor de los recursos que hay que asegurar. Los **requisitos de seguridad** de un sistema dado definen lo que significa la seguridad para ese sistema. Dichos requisitos sirven de base para determinar si el sistema implementado es o no seguro:

- Sin una serie de requisitos precisos tiene poco sentido cuestionar la seguridad de un sistema.
- Si los requisitos están débilmente establecidos no dicen mucho sobre la verdadera seguridad del sistema.

Algunos **ejemplos de formulación** de los requisitos de seguridad son los siguientes:

- **Directiva DOD 5200.28 (EE. UU.):**
  - Especifica cómo debe manipularse la información clasificada en sistemas de procesamiento de datos.

- **Manual de Referencia de Tecnología de Seguridad de la Computadora (EE. UU.):**
  - Especifica cómo evaluar la seguridad de los sistemas de computación de la Fuerza Aérea.

- **Ley de Intimidad de 1974 (EE. UU.):**
  - Requiere que las Agencias Federales aseguren la integridad y seguridad de la información acerca de los individuos, especialmente en el contexto del amplio uso de las computadoras.

NORMATIVA DE INTERÉS

Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

EJEMPLO PRÁCTICO

Esteban es programador y responsable del departamento de informática de su empresa donde necesitan tener un resumen de la normativa existente en materia de formulación de los requisitos necesarios en el tema de seguridad de redes.

¿Qué normativa debería tenerse en cuenta a la hora de la formulación de este tipo de requisitos?

Solución.

Podemos citar, en concreto, algunos ejemplos de formulación de los requisitos de seguridad:

- Directiva DOD 5200.28 (EEUU): Recoge cómo debe manipularse la información clasificada en sistemas de procesamiento de datos.
- Manual de Referencia de Tecnología de Seguridad de la Computadora (EE UU): Referida a cómo evaluar la seguridad de los sistemas de computación de la Fuerza Aérea.
- Ley de Intimidad de 1974 (EEUU): Requiere que las Agencias Federales aseguren la integridad y seguridad de la información acerca de los individuos, especialmente en el contexto del amplio uso de las computadoras.
- En nuestro país, la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

3.1 Seguridad a nivel de usuarios y equipos

Existen personas que pueden atacar nuestros equipos directamente, mediante la irrupción a través de Internet y el robo información personal; o indirectamente, mediante la creación de software malintencionado diseñado para dañar el equipo.

Afortunadamente, podemos protegernos tomando unas simples precauciones:

- **Firewall.** Un firewall puede ayudarle a proteger el equipo al impedir que los hackers o el software malintencionado obtengan acceso a él.

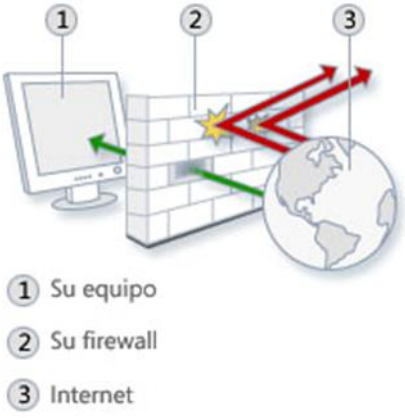
- **Protección antivirus.** Software antivirus que puede ayudarle a proteger un equipo frente a virus, gusanos y otras amenazas de seguridad.

- **Protección contra spyware y otros tipos de malware.** El software anti spyware puede ayudarle a proteger el equipo contra spyware y otro software potencialmente no deseado.

- **Windows Update.** Windows puede comprobar habitualmente las actualizaciones para el equipo e instalarlas de forma automática.

3.1.1 Uso de un cortafuegos

Un **cortafuegos o firewall** es un sistema que previene el uso y el acceso desautorizados a un ordenador. Todos los mensajes que entran o salen de nuestra red pasan a través del cortafuegos, que examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados. De este modo, un firewall puede ayudar a impedir que los hackers y el software malintencionado obtengan acceso al equipo.



Funcionamiento de un firewall.

Si se ejecuta un programa, por ejemplo, de mensajería instantánea, o un juego de red con varios jugadores, que tiene que recibir información desde Internet, el firewall nos pregunta si deseamos bloquear o desbloquear (permitir) la conexión. Si elegimos desbloquearla, se crea una excepción de modo que el firewall no se interponga cuando ese programa tenga que recibir información en el futuro.

Es importante recordar que **un cortafuegos no elimina problemas de virus del ordenador**, sino que cuando se utiliza conjuntamente con actualizaciones regulares del sistema operativo y un buen software antivirus, añadirá cierta seguridad y protección adicionales para tu ordenador o red.

Los cortafuegos pueden ser software, hardware, o una combinación de ambos:

- **Los cortafuegos hardware** proporcionan una fuerte protección contra la mayoría de las formas de ataque que vienen del mundo exterior y se pueden comprar como producto independiente o en routers de banda ancha.

- Para usuarios particulares, el cortafuegos más utilizado es un **cortafuegos software**. Un buen cortafuegos software protegerá un equipo contra intentos de controlarlo o acceder a él desde el exterior, y generalmente proporciona protección adicional contra los troyanos o gusanos de E-mail más comunes.

  La desventaja de los cortafuegos software es que protegen solamente al ordenador en el que están instalados y no protegen una red.

Hay varios tipos de técnicas cortafuegos, como son:

- **Packet filter:** mira cada paquete que entra o sale de la red y lo acepta o rechaza basándose en reglas definidas por el usuario. La filtración del paquete es bastante eficaz y transparente a los usuarios, pero es difícil de configurar. Además, es susceptible al IP spoofing.

- **Application gateway:** Aplica mecanismos de seguridad a ciertas aplicaciones, tales como servidores ftp y servidores telnet. Esto es muy eficaz, pero puede producir una disminución de las prestaciones.

- **Circuit-level gateway:** Aplica mecanismos de seguridad cuando se establece una conexión TCP o UDP. Una vez que se haya hecho la conexión, los paquetes pueden fluir entre los anfitriones sin más comprobaciones.

- **Proxy server:** Intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta con eficacia las direcciones de red verdaderas.

En la práctica, muchos cortafuegos utilizan dos o más de estas técnicas a la vez.

Un cortafuegos se considera la primera línea de defensa en la protección de la información privada. Para mayor seguridad, los datos deben ser cifrados.

3.1.2 Uso de un antivirus

Los **virus**, los gusanos y los caballos de Troya, entre otros, son programas creados por hackers que utilizan Internet para infectar equipos vulnerables. Los virus y los gusanos pueden autorreplicarse de un equipo a otro, mientras que los caballos de Troya entran en un equipo ocultándose dentro de un programa aparentemente de confianza, por ejemplo, un protector de pantalla.

Los virus, los gusanos y los caballos de Troya destructivos pueden borrar información del disco duro o deshabilitar completamente el equipo. Otros no causan ningún daño directo, pero empeoran el rendimiento y la estabilidad del equipo.

Los **programas antivirus**, son herramientas específicas que se utilizan para la detección y eliminación de diferentes tipos de malware (virus, troyanos, etc.), examinan el correo electrónico y otros archivos en busca de virus, gusanos y caballos de Troya. Si se detecta alguno, el programa antivirus lo pone en **cuarentena** (lo aísla) o lo elimina totalmente antes de que pueda dañar el equipo y sus archivos.

Cada día se identifican nuevos virus, por lo que es importante usar un programa antivirus que pueda actualizarse de manera automática. Cuando se actualiza el programa, los virus nuevos se agregan a una lista de virus que se deben comprobar, lo que ayuda a proteger el equipo de los nuevos ataques. Si la lista de virus está obsoleta, el equipo será vulnerable a las nuevas amenazas.

Para tener acceso a las actualizaciones, normalmente se requiere una cuota de suscripción anual. Hay que mantener la suscripción al día para recibir las actualizaciones de manera periódica.

ENLACE DE INTERÉS

Accede a esta web “Panda” donde encontrarás más información sobre virus con ejemplos de los virus más peligrosos y cómo actúan:

3.1.3 Uso de protección contra spyware

El **spyware** es software que puede mostrar anuncios, recopilar información sobre el usuario o cambiar la configuración del equipo, normalmente sin obtener su consentimiento, como debiera. Por ejemplo, el spyware puede instalar barras de herramientas, vínculos o favoritos no deseados en el explorador web, cambiar la página principal predeterminada o mostrar anuncios emergentes con frecuencia. Determinados tipos de spyware no muestran síntomas que se puedan detectar, sino que recopilan de forma secreta información importante como, por ejemplo, los sitios web que se visitan o el texto que se escribe. La mayor parte del spyware se instala a través del software gratuito que se descarga, pero en algunos casos una infección con spyware se puede contraer simplemente visitando un sitio web.

ENLACE DE INTERÉS

Accede a esta web para ampliar más información sobre spyware:

Para ayudar a proteger el equipo contra el spyware, se debe usar un programa anti spyware. Los sistemas Windows, por ejemplo, tienen integrado un programa anti spyware denominado Windows Defender, que está activado de forma predeterminada. Esta utilidad alerta cuando algún spyware intenta instalarse en el equipo. También puede examinar el equipo para comprobar si tiene spyware y, a continuación, quitarlo.

Cada día aparece nuevo spyware, por lo que Windows Defender debe actualizarse regularmente con el fin de detectar y protegerse contra las últimas amenazas.

3.1.4 Actualización automática del sistema operativo

Los fabricantes de sistemas operativos ofrecen periódicamente actualizaciones importantes, que pueden contribuir a proteger los equipos contra nuevos virus y otras amenazas para la seguridad. Para asegurarse de recibir estas actualizaciones lo más rápidamente posible, es recomendable activar las actualizaciones automáticas. Dichas actualizaciones se descargan en segundo plano cuando el equipo se conecta a Internet.

ENLACE DE INTERÉS

Accede a esta web para conocer más información sobre Windows Update y el modo de configurarlo:

3.1.5 Instalación de la última versión del navegador

Instalar la última versión del explorador web y mantenerlo actualizado son las dos mejores maneras de evitar problemas en línea.

En la mayoría de los casos, la última versión de un explorador contiene revisiones de seguridad y nuevas características que pueden ayudar a proteger el equipo y la privacidad en línea.

Por otro lado, muchos exploradores web ofrecen actualizaciones de seguridad periódicamente. Por lo tanto, hay que asegurarse de instalar dichas actualizaciones para el explorador siempre que estén disponibles.

En el caso de los navegadores nativos de Windows, el propio Windows Update que hemos comentado en el apartado anterior puede encargarse de realizar las actualizaciones automáticamente.

3.1.6 Activación de las características de seguridad del navegador

Muchos navegadores web poseen características de seguridad que pueden ayudarnos a explorar la Web de forma segura. Por lo tanto, es una buena idea conocer las características de seguridad que ofrece el navegador y asegurarse de que estén habilitadas.

Por ejemplo, a continuación se muestran algunas de las características de seguridad disponibles para Internet Explorer:

El filtro SmartScreen, que puede ayudar a protegerse contra ataques de suplantación de identidad (phishing) en línea, fraudes y sitios web simulados o malintencionados.

ENLACE DE INTERÉS

Aquí encontrarás más información sobre el filtro SmartScreen:

- Resaltar dominio, que permite ver más fácilmente la dirección web real de los sitios web que visitamos. Permite evitar sitios web engañosos o de suplantación de identidad (phishing) que usan direcciones web erróneas para engañarnos. El verdadero dominio que visitamos aparece resaltado en la barra de direcciones.

- Administrar complementos, que permite deshabilitar o habilitar los complementos del explorador web y eliminar los controles ActiveX no deseados.

- El filtro de scripts de sitios (XSS), que evita ataques de sitios fraudulentos y de suplantación de identidad que podrían intentar robar información personal y financiera.

- Una conexión segura (SSL) de 128 bits para usar sitios web seguros. Esto ayuda a Internet Explorer a crear una conexión cifrada con los sitios web de bancos, tiendas en línea, sitios médicos u otras organizaciones que manejan información confidencial de sus clientes.

3.1.7 Uso de una cuenta de usuario estándar

Cuando se inicia sesión en un equipo, el sistema operativo concede un nivel determinado de derechos y privilegios en función del tipo de cuenta de usuario que se tenga. Como hemos visto en unidades anteriores, existen tres tipos diferentes de cuentas de usuario: estándar, administrador e invitado.

Aunque una cuenta de administrador ofrece un control completo sobre un equipo, el uso de una cuenta estándar puede ayudar a lograr que el equipo sea más seguro. De este modo, si otras personas (o hackers) obtienen acceso al equipo con la sesión iniciada, no pueden alterar la configuración de seguridad del equipo ni cambiar otras cuentas de usuario.

ENLACE DE INTERÉS

Accede a esta web para conocer la Guía de Seguridad de las TIC, del CCN (Centro Criptográfico Nacional).

EJEMPLO PRÁCTICO

Luis es el responsable dentro del departamento de informática de su empresa, donde se está desarrollando un proyecto de implantación de una red informática en un cliente que funcionaba con equipos de forma independiente en cada una de sus delegaciones.

El cliente tiene una gran preocupación por la seguridad del sistema y la red, solicitando se adopten las medidas necesarias para prevenir los posibles ataques a través de internet y el robo de información o datos sensibles de la empresa.

¿Qué precauciones deberán implementarse para conseguir un nivel óptimo de seguridad en el sistema y la red?

Solución.

En la seguridad a nivel de usuarios y equipos pueden seguirse una serie de recomendaciones de actuación:

1. Uso de un cortafuegos.
2. Uso de un antivirus.
3. Uso de protección contra spyware.
4. Actualización automática del sistema operativo.
5. Instalación de la última versión del navegador.
6. Activación de las características de seguridad del navegador.
7. Uso de una cuenta de usuario estándar.

4. SERVIDORES DE FICHEROS. SERVIDORES DE IMPRESIÓN. SERVIDORES DE APLICACIONES

Un nuevo aspecto en la configuración del sistema de red, es el tema de servidores a utilizar. Deberás diseñar qué tipo de servidores serán necesarios en la red que estáis diseñando, así como su instalación y configuración para su uso.

En el apartado primero se presentaba la arquitectura cliente/servidor, y se indicaban las ventajas de su utilización en una red de ordenadores.

A continuación, veremos algunos ejemplos prácticos de este modelo, presentando tres de los principales tipos de servidor que se suelen encontrar en cualquier red empresarial.

4.1 Servidor de ficheros o archivos

Un **servidor de ficheros o archivos** permite almacenar y distribuir ficheros entre los clientes de una red de ordenadores. Su función principal es permitir a otros dispositivos el acceso remoto a los archivos que almacena o sobre los que tiene acceso.

Desde el punto de vista del cliente de un servidor de archivos, la localización de los archivos compartidos es transparente, es decir, en la práctica no hay diferencias perceptibles si un archivo está almacenado en un servidor de archivos remoto o en el disco de la propia máquina.

En principio, cualquier ordenador conectado a una red, dotado del software apropiado, puede funcionar como servidor de archivos. De hecho, cuando en el apartado anterior veíamos el modo de compartir carpetas tanto en sistemas Windows como Linux, en cierto modo los equipos que albergaban dichas carpetas estaban actuando como servidores de archivos, al menos de forma puntual.

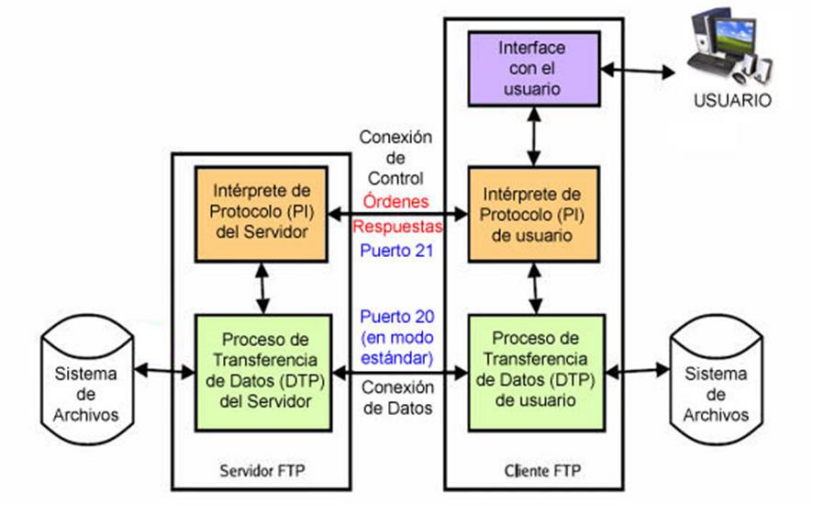
Pero el término servidor de archivos se suele reservar para aquellos equipos que realizan esta tarea de forma dedicada, no para los que comparten de manera puntual alguno de sus recursos.

Los protocolos que suelen emplearse en las transferencias de archivos son:

- FTP (multiplataforma).
- SMB/CIFS (Windows, Samba en Linux).
- NFS (Unix/Linux).

Los dos últimos ya se han tratado en apartados anteriores, así que ahora nos centraremos en el primero de ellos, **FTP.**

FTP (***F**ile **T**ransfer **P**rotocol*, "Protocolo de Transferencia de Archivos") es un protocolo de red para la transmisión de archivos entre dispositivos conectados a una red TCP/IP. Desde un equipo cliente se puede conectar a un servidor FTP para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.



Esquema de funcionamiento del protocolo FTP.

El servicio FTP pertenece a la capa de aplicación del modelo TCP/IP, y utiliza normalmente el puerto de red 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

Para solucionar este problema son de gran utilidad aplicaciones como SCP y SFTP, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.

VÍDEO DE INTERÉS

Aquí podrás visualizar cómo crear un servidor FTP en Windows 10:

4.2 Servidor de impresión

Un servidor de impresión puede ser una herramienta extremadamente útil en la oficina, ya que **nos permitirá utilizar una impresora en forma remota**, evitándonos la ardua tarea de transportar el archivo a imprimir en un pendrive o similar hasta el equipo que tiene la impresora conectada. Además, también nos ahorra la necesidad de tener instalada en dicho equipo la aplicación con que hemos desarrollado el trabajo.

Pero, ¿esto mismo no puede hacerse simplemente compartiendo la impresora? En efecto, así es, pero en ese caso en el momento mismo en que apagamos el equipo al cual se encuentra conectada dicha impresora dejamos de poder utilizarla.

En cambio, si conectamos un servidor de impresión a la red, nos aseguraremos de que la impresora **siempre se encuentre disponible**, independientemente de los dispositivos que se encuentren encendidos en ese momento.

Es justo la misma situación que comentábamos en el punto anterior, con la compartición de archivos: un equipo puede actuar de forma puntual como servidor de impresión, pero normalmente el término se reserva a los casos en que esta situación es permanente.

Un **servidor de impresión (Print Server) independiente** es un pequeño dispositivo que podemos conectar a cualquier puerto disponible en el router, y de este modo hacer accesible cualquier impresora que conectemos a él desde todos los dispositivos que sean parte de la red. Es decir, que básicamente permitirá a las computadoras en una red acceder a una misma impresora.

Servidor de impresión.

En el mercado existen varios tipos de servidores de impresión, y varían su precio de acuerdo a las posibilidades que ofrece cada uno. Desde los simples adaptadores que permiten conectar una impresora con interface paralela directamente al router, hasta servidores de impresión mediante Wi-Fi, con posibilidades de compartir dispositivos USB. Así pues, antes de decidirnos por un modelo u otro deberemos evaluar nuestras necesidades y decidir la compra en base a ello.

Servidor de impresión Wifi.

Este tipo de dispositivos son capaces de **soportar una gran variedad de protocolos de impresión** como Internet Printing Protocol, Line Printer Daemon, el protocolo de impresión en red de Microsoft, NetWare, NetBIOS, NetBEUI o JetDirect, lo que los hace particularmente flexibles, ya que podremos imprimir en ellos desde prácticamente cualquier sistema operativo.

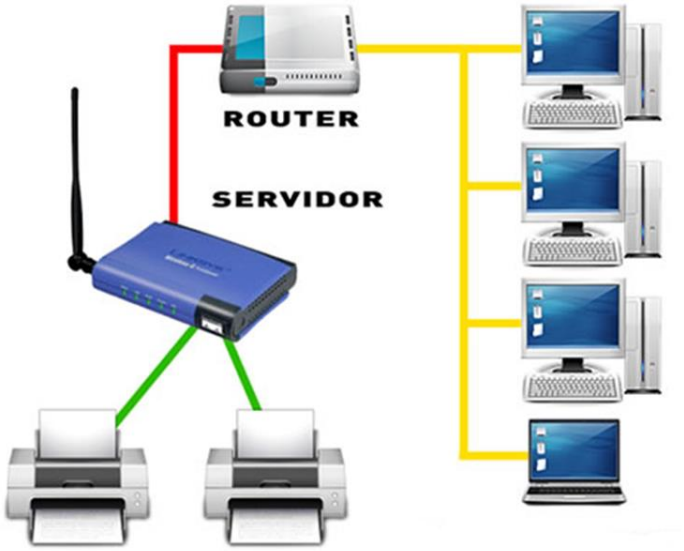
Si bien usar un servidor de impresión ofrece muchas ventajas, lo cierto es que **también poseen ciertas limitaciones,** a las cuales debemos prestarles especial atención, ya que podría estar comprometido el objetivo puntual de la compra.

Por ejemplo, algunos modelos de impresoras multifunción en el mercado no son 100% compatibles con ciertos servidores. La mayoría de las características de las impresoras de múltiples funciones (tales como fax y fotocopiadora) no son compatibles con los servidores de impresión.

Otros modelos de impresoras, como las del tipo GDI, no permiten su uso mediante servidores de impresión. Cabe destacar que GDI (Graphical Device Interface) es un sistema que utiliza recursos del equipo para poder imprimir, liberando de este modo a la impresora, lo que hace que los precios de las mismas sean mucho más económicos.

Así pues, es fundamental investigar antes de realizar la compra, y asegurarnos de que todas nuestras impresoras sean soportadas a la perfección por estos dispositivos. Y para ello, lo mejor es recurrir al sitio web del fabricante del dispositivo en cuestión.

A continuación se muestra un esquema básico de conexión utilizando un servidor de impresión:



Esquema de un servidor de impresión.

ENLACE DE INTERÉS

Accede a esta web para conocer más información que nos ofrece el INTEF sobre los servidores de impresión: sus ventajas, usos y ejemplos:

4.3 Servidor de aplicaciones

El concepto de servidor de aplicaciones está relacionado con el concepto de **sistema distribuido**. Un sistema distribuido, en oposición a un sistema monolítico, permite mejorar tres aspectos fundamentales en una aplicación: la alta disponibilidad, la escalabilidad y el mantenimiento. En un sistema monolítico un cambio en las necesidades del sistema (aumento considerable del número de visitas, aumento del número de aplicaciones, etc.) provoca un colapso y la adaptación a dicho cambio puede resultar catastrófica. Vamos a ver estas características con ejemplos.

- La **alta disponibilidad** hace referencia a que un sistema debe estar funcionando las 24 horas del día los 365 días al año. Para poder alcanzar esta característica es necesario el uso de técnicas de balanceo de carga y de recuperación ante fallos (*failover*).

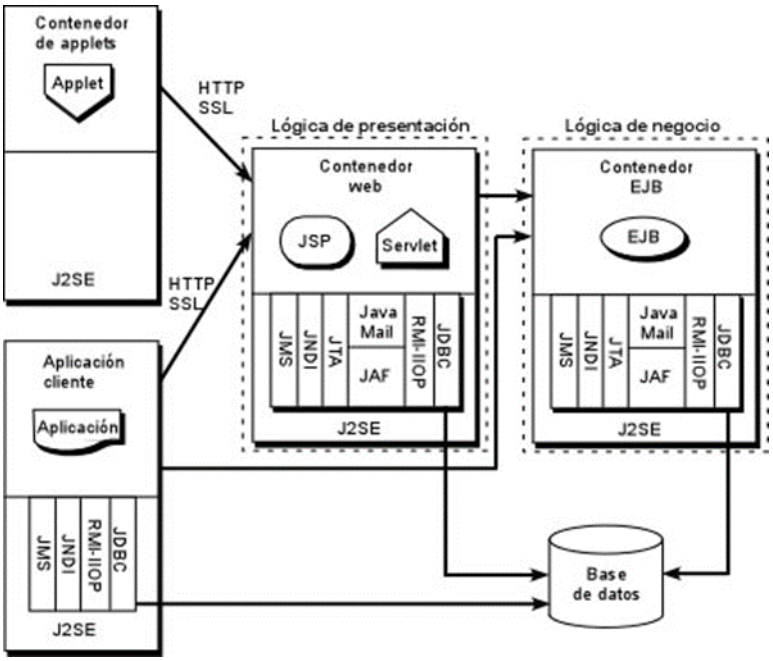
- La **escalabilidad** es la capacidad de hacer crecer un sistema cuando se incrementa la carga de trabajo (el número de peticiones).

  Cada máquina tiene una capacidad finita de recursos y por lo tanto sólo puede servir un número limitado de peticiones. Si, por ejemplo, tenemos una tienda que incrementa la demanda de servicio, debemos ser capaces de incorporar nuevas máquinas para dar servicio.

- El **mantenimiento** tiene que ver con la versatilidad a la hora de actualizar, depurar fallos y mantener un sistema. La solución al mantenimiento es la construcción de la lógica de negocio en unidades reusables y modulares.

A continuación veremos un ejemplo para ilustrar mejor los conceptos presentados: **J2EE**.

El estándar J2EE permite el desarrollo de aplicaciones de empresa de una manera sencilla y eficiente. Una aplicación desarrollada con las tecnologías J2EE permite ser desplegada en cualquier servidor de aplicaciones o servidor web que cumpla con el estándar. Un servidor de aplicaciones es una implementación de la especificación J2EE. La arquitectura J2EE es la siguiente:



Arquitectura J2EE.

Definimos a continuación algunos de los conceptos que aparecen en la figura:

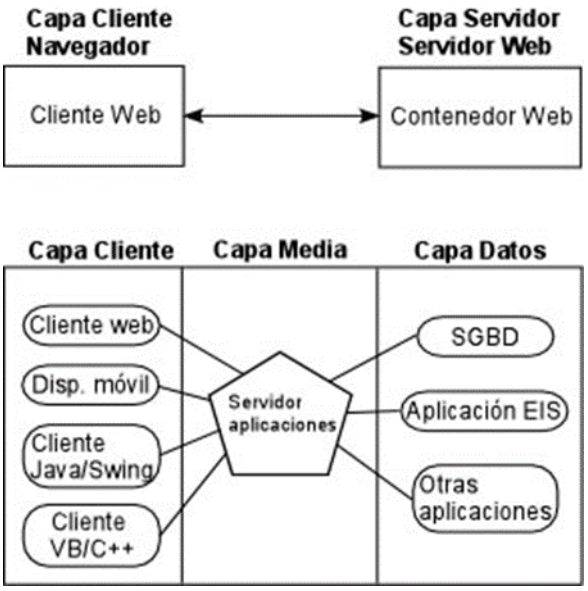
- **Cliente web (contenedor de applets):** Es usualmente un navegador e interactúa con el contenedor web haciendo uso de HTTP. Recibe páginas HTML o XML y puede ejecutar applets y código JavaScript.

- **Aplicación cliente:** Son clientes que no se ejecutan dentro de un navegador y pueden utilizar cualquier tecnología para comunicarse con el contenedor web o directamente con la base de datos.

- **Contenedor web:** Es lo que comúnmente denominamos servidor web. Es la parte *visible* del servidor de aplicaciones. Utiliza los protocolos HTTP y SSL (seguro) para comunicarse.

- **Servidor de aplicaciones:** Proporciona servicios que soportan la ejecución y disponibilidad de las aplicaciones desplegadas. Es el corazón de un gran sistema distribuido.

Frente a la tradicional estructura en dos capas de un servidor web un servidor de aplicaciones proporciona una **estructura en tres capas** que permite estructurar nuestro sistema de forma más eficiente. Un concepto que debe quedar claro desde el principio es que no todas las aplicaciones de empresa necesitan un servidor de aplicaciones para funcionar. Una pequeña aplicación que acceda a una base de datos no muy compleja y que no sea distribuida probablemente no necesitará un servidor de aplicaciones, tan solo con un servidor web (usando servlets y jsp) sea suficiente.



Arquitectura en dos capas frente a tres capas utilizando el servidor de aplicaciones.

Con base en la arquitectura J2EE existen toda una serie de implementaciones para servidores de aplicaciones, cada una con sus propias características que la pueden hacer más atractiva en el desarrollo de un determinado sistema. Algunas de las implementaciones más utilizadas son las siguientes:

- Oracle WebLogic.
- IBM WebSphere.
- JBoss Enterprise Application Platform, de Red Hat.
- Borland Enterprise Server.
- GlassFish.

Los dos primeros son los más utilizados en el mercado. La principal ventaja de WebLogic es que podemos crear un sistema con varias máquinas con distintos sistemas operativos: Linux, Unix, Windows NT, etc. El sistema funciona sin importarle en qué máquina está corriendo el servidor.

ENLACE DE INTERÉS

Aquí encontrarás más información sobre el servidor Oracle WebLogic:

EJEMPLO PRÁCTICO

En la empresa en la que trabaja Luisa, necesitan la configuración correcta de los servidores que conforman la red corporativa. Ella como experta programadora y amplia experiencia en la instalación de componentes de la red, va a realizar una propuesta de los distintos tipos de servidores que pueden emplearse en la arquitectura de la red informática de la empresa.

¿Qué tipos de servidores podemos encontrar?

Solución.

Los tres principales tipos de servidor que se suelen encontrar en cualquier red empresaria, serían:

1. **Servidor de ficheros o archivos.**
   Un servidor de ficheros o archivos permite almacenar y distribuir ficheros entre los clientes de una red de ordenadores. Su función principal es permitir a otros dispositivos el acceso remoto a los archivos que almacena o sobre los que tiene acceso.

2. **Servidor de impresión.**
   Un servidor de impresión puede ser una herramienta extremadamente útil en la oficina, ya que nos permitirá utilizar una impresora en forma remota, evitándonos la ardua tarea de transportar el archivo a imprimir en un pendrive o similar hasta el equipo que tiene la impresora conectada.

3. **Servidor de aplicaciones.**
   El concepto de servidor de aplicaciones está relacionado con el concepto de sistema distribuido. Un sistema distribuido, en oposición a un sistema monolítico, permite mejorar tres aspectos fundamentales en una aplicación: la alta disponibilidad, la escalabilidad y el mantenimiento.

5. TÉCNICAS DE CONEXIÓN REMOTA

Todo el sistema de red que se está desarrollando, necesita disponer de accesos en remoto. Serás el encargado de seleccionar qué tipos de conexiones van a ser posibles para el acceso de los usuarios en remoto, de acuerdo a las distintas técnicas que existen.

Cada vez contamos con más **herramientas de acceso remoto** a nuestros dispositivos, que nos permiten conectarnos a ellos desde otros equipos, tanto pertenecientes a la misma red, como incluso a redes externas. Con ellas se puede brindar soporte remoto a nuestros amigos y, por supuesto, también dar un servicio profesional a nuestros clientes. Dependiendo de los sistemas a los que nos vayamos a conectar tendremos que bucear entre herramientas de escritorio remoto, herramientas para acceso por consola (SSH) o bien, si buscamos algo extremadamente simple, herramientas para compartir nuestra pantalla con otro usuario remoto (y que así pueda ver lo mismo que estamos viendo nosotros).

5.1 Herramientas de escritorio remoto

Las herramientas de **escritorio remoto** son muy útiles para poder gestionar equipos sin necesidad de estar sentados delante de ellos. Si tenemos que asistir a alguien, controlar nuestro ordenador a distancia, revisar un tema del trabajo sin tener que pasar por la oficina o instalar una aplicación en un equipo sin tener que movernos de nuestro sitio, este tipo de herramientas nos vendrán extraordinariamente bien y nos harán la vida algo más sencilla.

Si se utiliza Windows, dentro de los accesorios que se instalan por defecto encontraremos la utilidad de **Escritorio Remoto** (similar al **Compartir** de **OS X**) que requiere, evidentemente, que el equipo al que nos vayamos a conectar acepte este tipo de peticiones.

Esta herramienta es interesante porque soporta la conexión a múltiples equipos remotos así como la ejecución de aplicaciones. Y también está disponible para dispositivos móviles iOS y Android.

El Escritorio remoto resulta muy útil, por ejemplo, para conectarnos a otros equipos Windows de nuestra red (incluyendo un servidor con Windows Server). Pero existen otras opciones que hacen las cosas aún más simples (y que funcionan bastante mejor a través de Internet). Por ejemplo:

- **Hangouts** de Google ofrece este tipo de opciones a través de Hangouts Remote Desktop. Google suele hacer las cosas muy fáciles a los usuarios y, en este sentido, hicieron que las conexiones por escritorio remoto se simplificasen hasta el punto de integrarlo dentro de una sesión de videoconferencia y sin más configuración que habilitar el acceso sobre la marcha.

ENLACE DE INTERÉS

Aquí encontrarás más información sobre el uso de Hangouts:

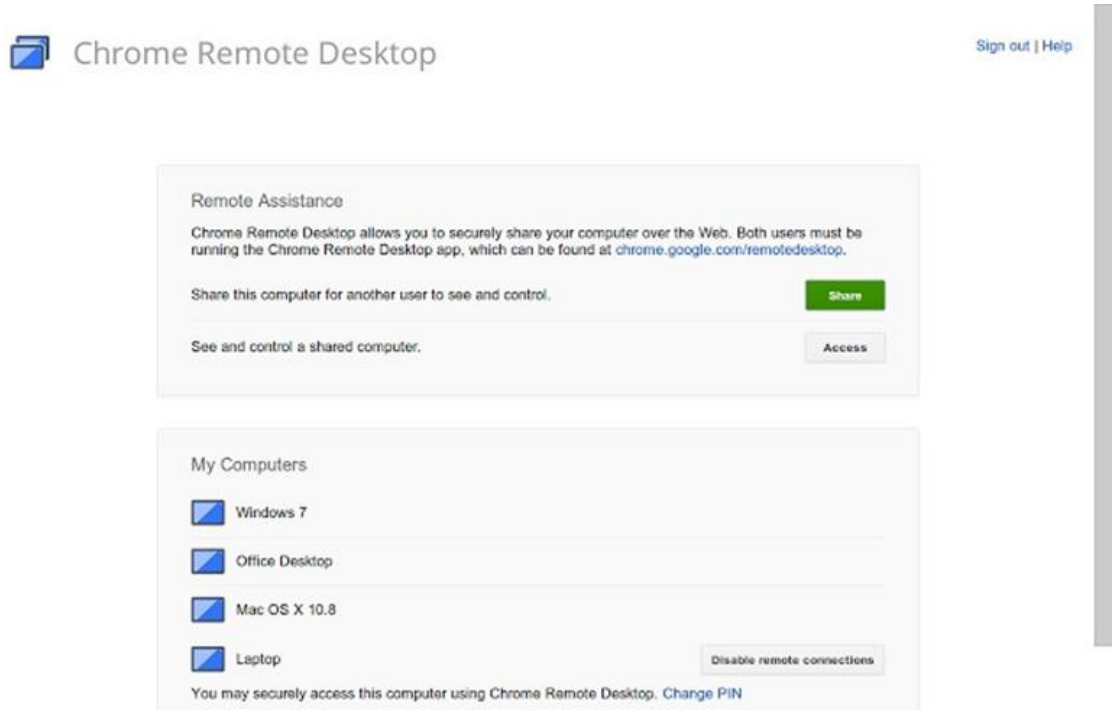
- **TeamViewer** es uno de los recursos más conocidos dentro del segmento de herramientas de acceso remoto. Se trata de una aplicación extremadamente sencilla y gratuita que nos permite la gestión remota de equipos, por ejemplo, para ofrecer soporte. Disponible en todas las plataformas (OS X, Windows, Linux y plataformas móviles), solamente tendremos que intercambiar un identificador y una contraseña para enviar archivos entre un equipo y otro o bien tomar el control. En el sector empresarial TeamViewer es bastante utilizado y, por ejemplo, ofrece opciones para personalizar el cliente y añadir el logotipo de las empresas o preconfigurarlos.

ENLACE DE INTERÉS

Aquí encontrarás más información sobre la herramienta TeamViewer y como descargarla:

- **TightVNC** y **RemoteVNC** son dos soluciones que implementan el protocolo VNC desarrollado a finales de los años 90 con el objetivo de ofrecer acceso remoto para gestionar equipos. Ambas opciones son dos implementaciones en *software* libre con las que poder realizar tareas de administración remota de equipos multiplataforma y, concretamente, en el caso de TightVNC podremos encontrar incluso clientes para ejecutarlos desde dispositivos móviles.

- **Chrome Remote Desktop** es una extensión para Google Chrome desarrollada por Google que nos permite acceder a otros equipos desde el navegador. Su instalación es extremadamente sencilla y lo único que requiere es tener Google Chrome instalado en el equipo así como esta extensión; a partir de ahí, y sin necesidad de que Google Chrome esté abierto, podremos conectarnos a nuestros equipos y visualizar el escritorio desde una pestaña de navegador. Podremos prestar servicios de soporte remoto intercambiando un "código de sesión" o configurar el acceso permanente a nuestros equipos mediante un PIN.

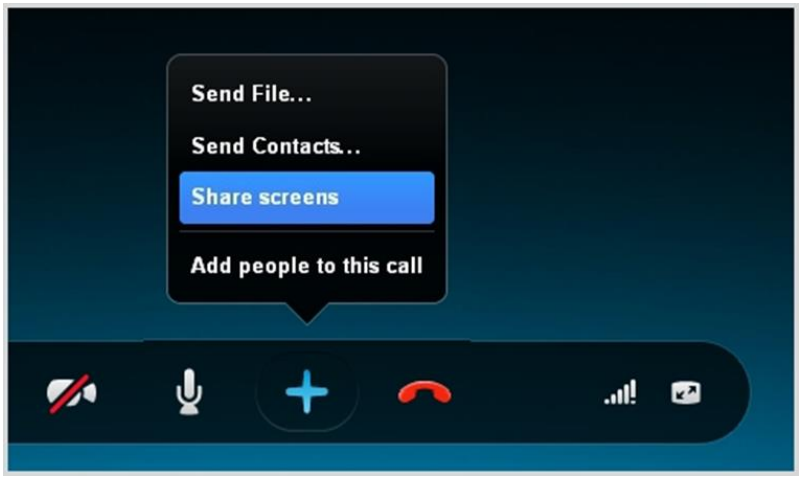


Chrome Remote Desktop.

5.2 Herramientas para compartir pantalla

Nos permiten mostrar el contenido de la pantalla de nuestro equipo a otros usuarios, pero sin que ellos tomen el control del equipo. Algunos ejemplos son:

- **Skype**, tanto en Windows como en Mac, nos permite compartir nuestra pantalla o, incluso, una ventana concreta de todas las que tenemos abiertas. Si usamos la versión gratuita de Skype, solamente podremos compartir la pantalla en una conexión con otra persona; en el caso que tengamos la versión de pago podremos usar esta opción en videollamadas de grupo.



Compartir pantalla con Skype.

- **Hangouts** de Google también incluyen esta posibilidad y, además, con menos restricciones que Skype. El servicio de mensajería multiplataforma de Google nos ofrece la posibilidad de compartir nuestro escritorio con el resto de usuarios conectados a la sesión; por tanto, podrán ver qué tenemos abierto o podrían ver una presentación en remoto. Evidentemente, no es la única opción disponible en los Hangouts porque, tal y como hemos comentado, también existe la posibilidad de conectarnos en remoto al equipo de otro usuario para controlarlo.

- **Join.me** es un servicio desarrollado por LogMeIn que también nos puede ayudar a compartir nuestra pantalla con otros usuarios. El servicio está disponible tanto en Windows como en OS X, Android e iOS y nos permite convocar reuniones con hasta 10 personas (en la versión gratuita) y compartir con ellos nuestra pantalla, archivos o chatear en directo mientras realizamos la demostración o nos muestran el problema que tenemos que diagnosticar.

ENLACE DE INTERÉS

Accede a esta web para conocer estas y otras herramientas para compartir la pantalla de nuestro ordenador:

5.3 Acceso remoto por consola

En caso de que trabajemos con servidores Linux sin entorno gráfico, la consola es nuestra mejor amiga y, evidentemente, necesitaremos algún cliente que nos permita trabajar de forma remota mediante entorno shell. Uno de los mejores recursos que uno puede instalar es **Putty**, un cliente ligero de Telnet y SSH en *software* libre.

PuTTy.

Es una herramienta que permite el acceso a equipos remotos utilizando distintos protocolos (Telnet, SSH o Rlogin), que está disponible en su página web https://www.putty.org, para descarga e instalación mediante un fichero instalable con extensión .msi.

Requiere de una sencilla configuración para establecer el acceso remoto en la que se deberán consignar una serie de datos como:

- Nombre del equipo o dirección IP a la que deseamos acceder en Host Name.
- Especificar el puerto que se va a utilizar.
- Seleccionar el tipo de acceso: SSH, Telnet, Rlogin, etc.
- Guardar los datos para sesiones futuras.

ENLACE DE INTERÉS

Aquí encontrarás más información acerca de Putty:

EJEMPLO PRÁCTICO

Sara trabaja en el departamento de informática de una empresa de servicios y ante la necesidad de trabajar desde los diferentes centros de trabajo distribuidos por toda la geografía nacional, le han solicitado que haga un estudio comparativo de las herramientas que existen en el mercado para acceso remoto a la red.

¿Qué tipos de herramientas puede proponer para los distintos tipos de conexión remota?

Solución.

De la amplia oferta que existe en el mercado de este tipo de herramientas, puede proponer las siguientes:

- Herramientas de escritorio remoto:
  - Hangouts.
  - TeamViewer
  - Chrome Remote Desktop

- Herramientas para compartir pantalla:
  - Skype
  - Hangouts
  - Join.me

Acceso remoto por consola:
  - Putty

6. UTILIDADES DE SEGURIDAD BÁSICA. HERRAMIENTAS DE CIFRADO, HERRAMIENTAS DE ANÁLISIS Y ADMINISTRACIÓN, CORTAFUEGOS Y SISTEMAS DE DETECCIÓN DE INTRUSOS

En el apartado de seguridad de red, además de una política de seguridad correcta, deberás utilizar las herramientas adecuadas para conseguir que esa seguridad sea efectiva y cumpla con el objetivo de protección de accesos y de la información. Es necesario que conozcas y analices las diferentes herramientas de este tipo que existen en el mercado y sus funcionalidades.

6.1 Utilidades de seguridad básica

Además del establecimiento de una correcta política de seguridad de acuerdo a las pautas y consejos recogidas en las directivas de seguridad, existen una serie de herramientas adicionales que nos poder servir de ayuda con la seguridad de nuestros equipos. A continuación se describen algunas de las más importantes.

6.1.1 Herramientas de cifrado

Una herramienta de cifrado es aquella que nos permite proteger nuestra información mediante un proceso que altera su contenido de legible a ilegible, con el objetivo de evitar que un tercero pueda tener acceso a ella. Una de las más populares de este tipo ha sido **TrueCrypt**, pero está descontinuada desde 2014.

Otras alternativas Open Source serían:

GnuPG.
GnuPG es una herramienta de cifrado y firmas digitales. Utiliza el estándar del IETF denominado OpenPGP y es software libre bajo la licencia GPL. GPG, como también se le conoce, es una herramienta basada en la línea de comandos que permite cifrar y firmar datos y comunicaciones. Cuenta con un sistema de llave versátil de gestión, así como módulos de acceso para todo tipo de directorios de claves públicas.

AES Crypt.

AES Crypt es un software avanzado de cifrado de archivos que utiliza el estándar *Advanced Encryption Standard* también conocido como *Rijndael*, para cifrar de forma fácil y segura los archivos. Esta herramienta se ejecuta desde la línea de comandos en Linux y se integra con la *shell* Windows. Todos los archivos y directorios cifrados con

AES Crypt son accesibles mediante una contraseña que solo debería manejar el autor, eliminando así los accesos no autorizados. También dispone de una biblioteca para los desarrolladores que utilizan Java para leer y escribir archivos con formato AES.

DiskCryptor.

DiskCryptor es un sistema completo de cifrado de disco duro para Windows, permitiendo también el cifrado de particiones individuales incluyendo la partición donde está instalado el sistema operativo. Utiliza AES-256, Twofish, Serpent o una combinación de algoritmos en cascada en el modo XTS para llevar a cabo el cifrado y está publicado bajo una licencia GPLv3.

El proyecto fue iniciado originalmente por un ex usuario de TrueCrypt conocido bajo el nombre de *ntldr,* por lo que en un principio eran compatibles, pero desde la versión 0.5 DiskCryptor se basa en su propio formato de partición desarrollado específicamente para el cifrado de particiones con datos, a diferencia del formato de TrueCrypt que fue originalmente concebido para la creación de volúmenes vacíos, medida que le otorgo estabilidad.

EncFS.

EncFS es un sistema de archivos cifrado basado en FUSE, el sistema de archivos en el espacio de usuario. Cifra los archivos utilizando un directorio arbitrario como almacenamiento de los mismos, quedando esto transparente al usuario. De esta manera son dos los directorios involucrados en el montaje de un sistema de archivos EncFS: el directorio de origen y el punto de montaje. Los archivos son cifrados mediante una clave del volumen que se almacena cifrada en el directorio de origen y es necesaria una contraseña para descifrarla. EncFS es un software de código abierto, licenciado bajo la GPL.

Axcrypt.

Axcrypt es un software de cifrado de archivos de código abierto que hace uso del algoritmo AES-128 y SHA-1 para estos fines. Se integra perfectamente con Windows para comprimir, cifrar, descifrar, almacenar, enviar y trabajar con archivos individuales. Protege con contraseña cualquier número de archivos a través de una fuerte encriptación y viene listo para usar ya que no requiere configuración.

6.1.2 Herramientas de análisis y administración

Cuando hablamos de administración de redes, un aspecto a destacar es la utilización de herramientas de análisis que permitan la monitorización del tráfico de red que se transmite entre los equipos que la integran.

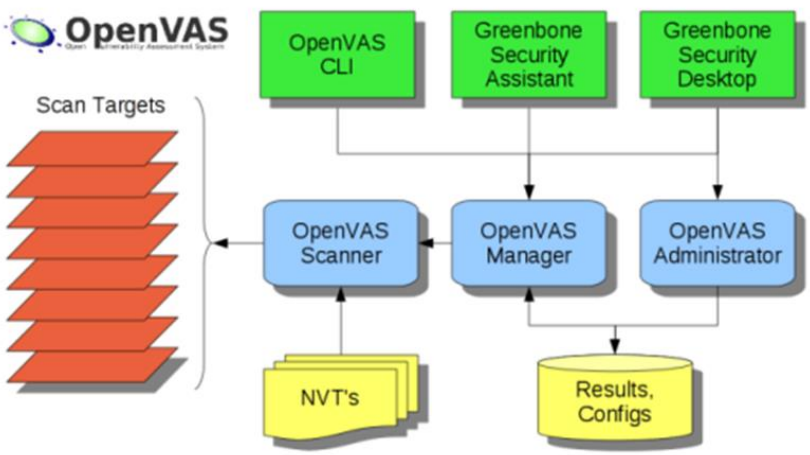
Mediante la información obtenida podremos realizar un gran número de acciones para detectar si existe algún tipo de tráfico de red no deseado, o el buen funcionamiento en la transmisión de paquetes, por ejemplo.

Existen un gran número y tipos de herramientas de este tipo, tanto propietarias o de pago, como de código abierto y gratuitas, entre las que destacamos OpenVas y Nmap.

OpenVAS (*Open Vulnerability Assessment System*, inicialmente denominado *GNessUs)*, es una suite de software que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos.

OpenVAS es una herramienta principal de OSSIM, todos los productos que la componen son software libre y la mayoría de ellos son distribuidos bajo licencia GPL. Entre sus características principales están:

- Escaneo concurrente de múltiples nodos.
- Soporte SSL.
- Soporte para WMI.
- Escaneo automático temporizado.
- Reportes en múltiples formatos (XML, HTML, LaTeX, entre otros).
- Servidor web integrado.
- Multiplataforma.



Herramienta de análisis OpenVAS.

ENLACE DE INTERÉS

Accede a esta web para conocer más información sobre muchas de las opciones que proporciona OpenVAS:

NMAP.

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

```
notwist@notwist:~$ nmap localhost

Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-02 15:50 CEST
Interesting ports on localhost (127.0.0.1):
Not shown: 1691 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
3306/tcp open  mysql

Nmap finished: 1 IP address (1 host up) scanned in 0.213 seconds
notwist@notwist:~$
```

Ejemplo de ejecución de Nmap.

Ha llegado a ser una de las herramientas imprescindibles para todo administrador de sistemas, y es usado para pruebas de penetración y tareas de seguridad informática en general.

Como muchas herramientas usadas en el campo de la seguridad informática, es también una herramienta muy utilizada para hacking.

Los administradores de sistema pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crackers pueden usarlo para descubrir objetivos potenciales.

Nmap permite hacer el inventario y el mantenimiento del inventario de computadores de una red. Se puede usar para auditar la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte.

Entre sus características principales están:

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como *fingerprinting*).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

ENLACE DE INTERÉS

Conoce la guía de referencia de Nmap:

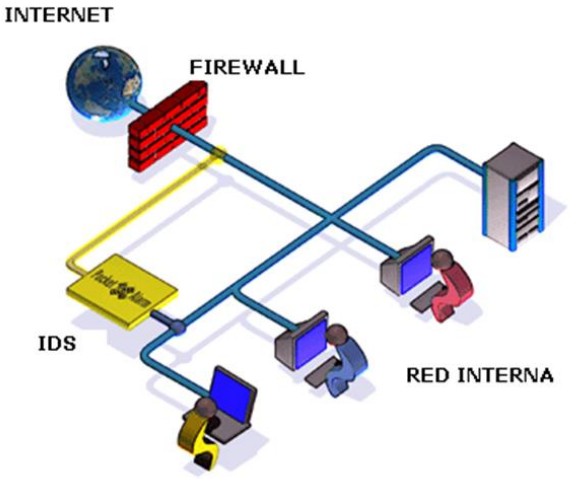
6.1.3 Sistemas de detección de intrusos

El término **IDS** (*Sistema de detección de intrusiones*) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos familias importantes de IDS:

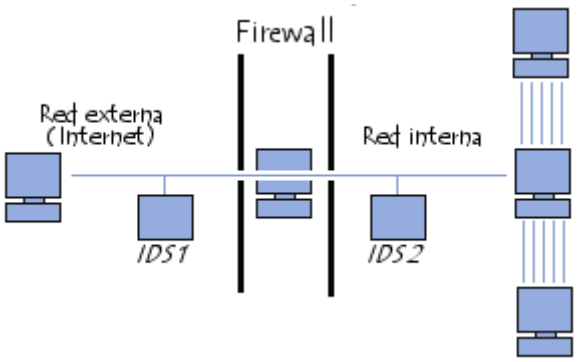
- El grupo **N-IDS** (*Sistema de detección de intrusiones de red*), que garantiza la seguridad dentro de la red.

- El grupo **H-IDS** (*Sistema de detección de intrusiones en el host*), que garantiza la seguridad en el host.



Esquema de red con IDS.

Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.



Colocación de varios IDS dentro de una red.

El H-IDS se encuentra en un host particular. Por lo tanto, su software cubre una amplia gama de sistemas operativos como Windows, Solaris, Linux, HP-UX, Aix, etc.

El H-IDS actúa como un daemon o servicio estándar en el sistema de un host. Tradicionalmente, el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer).

ENLACE DE INTERÉS

Accede a esta web para conocer más información sobre la implantación de un sistema de detección de intrusos en la Universidad de Valencia:

Los principales métodos utilizados por N-IDS para informar y bloquear intrusiones son:

- **Reconfiguración de dispositivos externos (firewalls o ACL en routers)**: Comando enviado por el N-IDS a un dispositivo externo (como un filtro de paquetes o un firewall) para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).

- **Envío de una trampa SNMP a un hipervisor externo**: Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa como HP Open View Tivoli, Cabletron, Spectrum, etc.

- **Envío de un correo electrónico a uno o más usuarios**: Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.

- **Registro del ataque**: Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.

- **Almacenamiento de paquetes sospechosos**: Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.

- **Apertura de una aplicación**: Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora).

- **Envío de un "*ResetKill*"**: Se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válido para técnicas de intrusión que utilizan el protocolo de transporte TCP).

- **Notificación visual de una alerta**: Se muestra una alerta en una o más de las consolas de administración.

EJEMPLO PRÁCTICO

Eva es programadora y experta en seguridad de redes informáticas dentro del departamento de informática de su empresa, donde se están planteando la instalación y configuración de un IDS (Sistema de detección de intrusiones), mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

En ellos encontramos dos tipos de IDS:

- El grupo N-IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red.
- El grupo H-IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host

Estando interesados en concreto, en los principales métodos utilizados por N-IDS para informar y bloquear intrusiones.
¿Cuáles serían esos métodos?

Solución.

Los principales métodos utilizados por N-IDS para informar y bloquear intrusiones son:

- Reconfiguración de dispositivos externos (firewalls o ACL en routers).
- Envío de una trampa SNMP a un hipervisor externo.
- Envío de un correo electrónico a uno o más usuarios.
- Registro del ataque.
- Almacenamiento de paquetes sospechosos.
- Apertura de una aplicación.
- Envío de un "ResetKill".
- Notificación visual de una alerta.

7. IMPLANTACIÓN Y EXPLOTACIÓN DE DOMINIOS

Desde la empresa que ha solicitado el desarrollo del nuevo sistema informático están planteando la posibilidad de cambiar el nombre de dominio, para ello deberás recopilar la información existente en nuestro país sobre la implantación y explotación de dominios, las condiciones de registros y opciones que ofrece el registro de dominios de alto nivel, tipo ".es"

Las redes conectadas a través de internet, son de carácter global y permiten la comunicación a través de direcciones IP numéricas únicas. El DNS (Sistema de Nombres de Dominio) funciona como una de las capas de la infraestructura IP, donde el nombre de dominio facilita el acceso a la navegación a los usuarios, además de proporcionar el nombre del proveedor del contenido y del alojamiento, existiendo una base de datos de dominios registrados.

A nivel europeo existe el CENTR (Council of European National Top-Level Domain Registries) cuyo miembros son registros de ccTLD encargados de la administración de dominios de alto nivel de cada país, proporcionando la estructura técnica para el DNS, organizando el registro de nombres de dominio y manteniendo de forma proactiva la base de datos de registro de los nombre de dominio.

ENLACE DE INTERÉS

Accede a esta web para conocer más información sobre la normativa aplicable a los dominios ".es".

La infraestructura de IP e internet, nos lleva a la necesidad de simplificar su contenido, difícil de recordar para los humanos, estableciendo nombres de dominio que son más fáciles de manejar con lo que conocemos como DNS para poder hacer referencia a las largas y tediosas direcciones IP.

El DNS posee una estructura jerárquica, que tiene una serie de dominios de nivel superior (TLD) bajo una única raíz. La extensión de un nombre de dominio, como por ejemplo, ".es", indica el TLD en el que se ha registrado el nombre. De este modo el funcionamiento del DNS es posible gracias a su estructura jerárquica, y la búsqueda de los nombres de dominio, gracias a su forma iterativa.

El registro de un nombre de dominio es el responsable de la administración de uno o más TLD, además de tener que respetar las normas técnicas y los requisitos propios del DNS, de acuerdo a las políticas establecidas por cada TLD, responsables de sus propias reglas.

Un dominio nos lleva a un sitio web donde encontraremos un contenido que deberá estar alojado en algún lugar para poder acceder a él, de modo que existirán tanto unos proveedores de contenido, propio o no, y un proveedor de alojamiento, caso de que se aloje en servidores externos conectados a internet e identificados por su dirección IP única.

El tercer proveedor, es el que suministra los servicios de internet (ISP), dando acceso a la red y la infraestructura ISP, permitiendo a los usuarios su acceso a internet, que en ocasiones también incluyen puntos de intercambio de red (IXP), operadores de red de corta o larga distancia y redes de distribución de contenidos.

El nombre de dominio funciona como una etiqueta sobre la dirección IP, y puede contener información de utilidad para el usuario, como puede ser el nombre de la empresa. Características propias del dominio son:

- El titular de un nombre del dominio no es necesariamente el único proveedor de contenidos.

- El titular de un nombre de dominio tiene derechos al uso de un nombre específico, que obtendrá mediante el registro del nombre en el TLD, siendo responsable de su uso.

- El registrador de nombre de dominio, debe verificar la disponibilidad del nombre de dominio y administrar su registro.

- El registro administra la única base de datos autorizada de nombres de dominio registrados bajo su TLD y publica esta información en el DNS.

Existen unos marcos legales que definen los tipos de contenido que deben recoger los dominios, esta legislación varía de unos países a otros, pero sí los registros de dominios de primer nivel territoriales o ccTLD (country code Top Level Domains) son los encargados en cada uno de ellos, de establecer los requisitos para el registro de nombres de dominio y los deberes a cumplir, así como una serie de directrices para el correcto contenido de los dominios, entre las que destacan:

- Educación y sensibilización a nivel comunitario, a través de las comunidades locales de internet con distintas iniciativas, como advertencias sobre contenidos no adecuados y cómo actuar en caso de detectarlos.
- Colaboración con la administración y autoridades para una coordinación de acciones.
- Uso de los registros para identificación de los proveedores y titulares de los dominios, y respuestas a través del filtrado de entradas, verificaciones automáticas, comprobación de datos de registro, etc.

ENLACE DE INTERÉS

Aquí encontrarás más información acerca de DNSSEC:

VÍDEO DE INTERÉS

Aquí podrás visualizar como Alberto López explica que es el DNS (Sistema de Nombres de Dominio):

RESUMEN FINAL

En esta unidad didáctica hemos tratado el tema de gestión de recursos de una red, comenzando con la administración de los permisos y derechos de los usuarios, y sus características y posibilidades de ser heredados, así como su administración mediante las listas de control de acceso, conociendo sus dos tipos: De protección (ACL) y de seguridad (SACL).

El punto fuerte de la gestión de recursos de red, es el uso compartido de recursos, donde hemos ido viendo los diferentes aspectos de su configuración, permisos y directivas de seguridad, en compartir ficheros, impresoras, aplicaciones, acceso a internet, desde el modelo cliente/servidor. Continuando con los casos de compartir ficheros en los distintos sistemas, libres y propietarios.

Volviendo sobre la seguridad del sistema y datos, hemos hecho un recorrido por las recomendaciones básicas como instalación de cortafuegos, antivirus, actualización de software, etc. Y las distintas directivas y ámbitos de las mismas.

Conocer los tipos de servidores existentes: Ficheros, impresión y aplicaciones, es el siguiente punto que hemos tratado por la importancia que tiene su instalación, estructura y configuración correcta, para trabajar de forma remota, con las distintas técnicas o herramientas que existen según el tipo, como de escritorio remoto (Hangouts o TeamViewer), para compartir pantalla (Skype) o de acceso remoto por consola (Putty).

En la seguridad básica, hemos abordado los diferentes tipos de herramientas como son las de cifrado (TrueCrypt o GnuPG), de análisis y administración (OpenVAS o Nmap) y de detección de intrusos con métodos utilizados por N-IDS como son reconfiguración de dispositivos externos, registro del ataque o envío de una trampa SNMP a un hipervisor externo, entre otros.

Para finalizar, hemos visto la implantación y explotación de dominios web, con la intervención del CENTR (Council of European National Top-Level Domain Registries) y los miembros encargados de los registros en cada país (ccTLD), con su estructura y existencia del DNS (Sistema de Nombres de Dominio).