INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

11

Técnico en REDES &SEGURIDAD

RECURSOS COMPARTIDOS Y DISPOSITIVOS MULTIMEDIA

En este fascículo aprenderemos a compartir recursos en Linux y Windows. Además, veremos conceptos sobre seguridad, auditoría y dispositivos multimedia.

- RECURSOS COMPARTIDOS
- SAN Y NAS
- PERMISOS Y SEGURIDAD
- AUDITORÍA
- SMART TVS, SMARTPHONES, CONSOLAS DE VIDEO Y MUCHO MÁS

USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez

Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Opciones de configuración, asignación de permisos, auditorías y administración de recursos compartidos, desde sistemas operativos Windows y GNU/Linux.

En la clase anterior, revisamos la configuración avanzada de DHCP y conocimos el mecanismo DDNS, analizamos los alcances y las características de NAT y también los protocolos UPnP. Además, vimos la tecnología QoS y los firmware alternativos. Aprendimos a realizar la instalación y configurar el firmware DD-WRT y vimos el concepto de ACL y los peligros de los backdoors por firmware.

En la presente clase, analizaremos en detalle la configuración y administración de recursos compartidos, tanto en sistemas Windows como en GNU/Linux. Aprenderemos a compartir recursos y veremos la forma de realizar networking entre dispositivos, tales como SmartTV, Smartphones y consolas de videojuegos. Revisaremos las características de las tecnologías SAN y NAS, y también profundizaremos sobre los permisos y la seguridad asociada a los recursos que se encuentran compartidos.

Para terminar, conoceremos los alcances de la auditoría, y revisaremos la regla del mínimo privilegio y la toma de posesión.

11

Conceptos sobre recursos compartidos

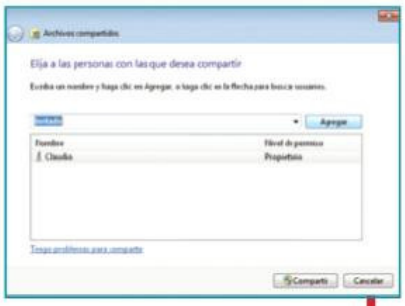
Comandos y configuraciones para un correcto control y administración sobre los recursos compartidos de la computadora.

Un recurso compartido proporciona, en una red, acceso a otros usuarios a carpetas, archivos, unidades e impresoras, entre otros servicios, de nuestra PC. A cada recurso compartido, le podremos asignar o denegar permisos para tener un control sobre los privilegios otorgados, mediante diversos métodos. El más simple de aplicar y de administrar es por medio de los permisos de recurso compartido (botón derecho y seleccionamos **Propiedades**). O bien, podemos utilizar el control de acceso de seguridad en el sistema de archivos NTFS, que nos proporcionará un control más detallado.

Primero buscamos CMD y, con el botón derecho, podemos ejecutar la consola de comandos con privilegio de administrador.

Métodos

También podríamos usar una combinación de ambos métodos. Si utilizamos ambos, pero a cada método le aplicamos distintas restricciones ya sea por error u omisión, debemos tener cuidado ya que siempre se aplicará el permiso más restrictivo.
Por ejemplo, el permiso de un recurso compartido que está definido como predeterminado es: **Todos = Lectura**.
Si solo cambiamos el permiso NTFS, se aplicará el permiso más restrictivo (el de recurso compartido, es decir **Todos = Lectura**) y parecería que nuestros cambios en los permisos no tuvieron efecto alguno.
La denegación de permisos normalmente es necesaria cuando se desea reemplazar permisos específicos que están asignados por defecto desde el sistema operativo o asignados por programas.
Nuestros archivos, con sus diferentes permisos, no solo pueden compartirse entre las distintas PCs de nuestra red, también por Internet mediante aplicaciones P2P, entre distintas sesiones de usuarios de una misma PC, o entre distintos programas que utilizan los mismos archivos.
Una recomendación al usar carpetas compartidas es trabajar con grupos, para no tener que dar permisos a cada uno de los usuarios de nuestra red.



Debemos agregar el usuario Invitado para que otras personas accedan a nuestra carpeta compartida.

Configuración

Según la configuración de la computadora, se crean distintos recursos compartidos especiales para uso administrativo y del sistema. Para ver información acerca de los recursos compartidos, podemos utilizar uno de estos comandos desde la ventana del símbolo del sistema, pero debemos hacerlo con permisos de administrador:

```
net share
net session
net file
```

- **net share** muestra información sobre los recursos compartidos en nuestra PC. Un recurso compartido especial u oculto se identifica por el símbolo de pesos ($) al final del nombre del recurso. Estos recursos no aparecen cuando se explora un equipo. Por ejemplo, \\PC-REMOTA\C$ nos permite como administradores conectarnos

al directorio raíz de una unidad.
IPC$: se utiliza en las conexiones temporales entre clientes y servidores. En especial, para la administración remota de servidores de red.
USER: usuario
CARPETA COMPARTIDA: nombre y ruta de la o las carpetas compartidas

- **net sesión** muestra información acerca de las sesiones de otros equipos de nuestra red que ingresaron a nuestra PC. Sería como una forma muy básica de realizar un honeypot (crear una carpeta compartida y, luego, ver quién accede a nuestra PC). El registro es limitado, ya que, como su nombre lo indica, solo veremos información de la actual sesión.
- **net file** es similar a **net session**, pero aquí vemos información detallada acerca de los archivos abiertos por otros usuarios en nuestra computadora.

Mapeo de unidades de red

Si accedemos con frecuencia a archivos que se encuentran en el servidor o en otra PC de la red, entonces debemos hacer un **Map Network Drive** (mapeo de unidades de red). Desde **Inicio/Equipo**, encontraremos una solapa **Conectar a unidad de red**. Asignamos una letra a la nueva unidad (por ejemplo, **Z:**) y la opción **Examinar**; ubicaremos la carpeta con los archivos compartidos en el servidor. A partir de ahora, podremos acceder la carpeta como si fuera una unidad más (unidad **Z:**).
Desde el servidor, podremos otorgar distintos permisos. Por ejemplo, para que los usuarios de un dominio tengan acceso de lectura y escritura sobre la carpeta que acabamos de convertir en unidad de red.

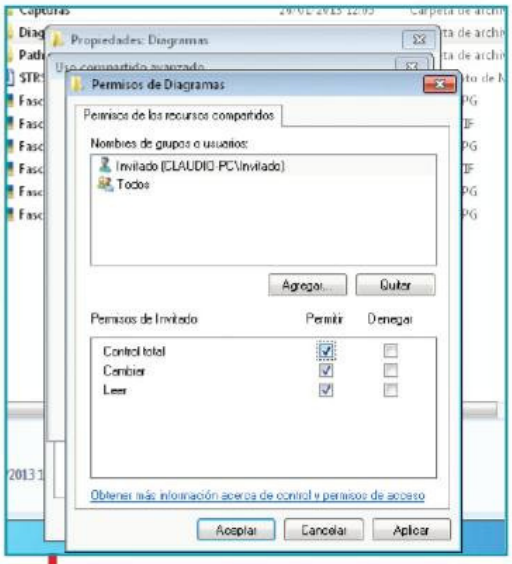
En la pestaña **Permisos** de los recursos compartidos, cambiaremos los permisos a **Control total** para el grupo **Todos**.
En la pestaña **Seguridad**, daremos permisos a los usuarios que se conectan localmente o mediante **Escritorio remoto**.

Compartir archivos sin contraseña

En ocasiones, es conveniente tener una carpeta compartida sin solicitud de contraseña. Para esto, debemos darle los privilegios necesarios al usuario **Invitado**.
Primero, debemos deshabilitar la solicitud de contraseña desde **Red/Centro de redes y recursos compartidos/Cambiar configuración de uso compartido avanzado**, marcamos la casilla **Desactivar el uso compartido con protección por contraseña**. Para trabajar sobre las propiedades de nuestra carpeta, presionamos el botón **Compartir**, agregamos al usuario **Invitado**, y le damos el nivel de **Lectura y escritura**.
También debemos compartir la carpeta con permisos para el usuario **Invitado**. Seleccionamos **Uso compartido avanzado** y, en el botón **Permisos**, agregamos nuevamente al usuario **Invitado**. Finalizamos dando permisos de **Control Total**.

Impresoras

Conectar una impresora en red es muy sencillo. Primero, debemos compartir la impresora desde la computadora local. Vamos a **Dispositivos e impresoras**; desde **Propiedades de impresora** (presionando el botón derecho del mouse sobre el icono adecuado), seleccionamos **Compartir**. También debemos habilitar la opción **Presentar trabajos de impresión en equipos cliente**.
Ahora, desde nuestra PC en red, en **Dispositivos e impresoras**, seleccionamos **Agregar una impresora**. Se iniciará un asistente de instalación; elegimos **Agregar una impresora de red, inalámbrica o Bluetooh**. Aquí debería aparecer nuestra impresora; instalamos el controlador, y el dispositivo quedará instalado. En algunas impresoras, será necesario cargar los drivers localmente y no por red. Como en cualquier recurso de red, podemos aplicar permisos a determinados usuarios, pero rara vez se utiliza esta restricción en las impresoras. ■



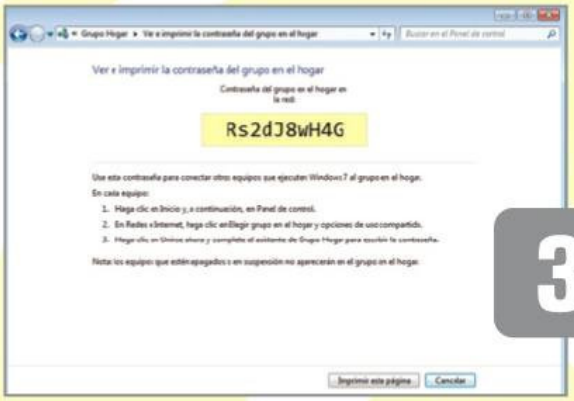
Además de configurar el uso compartido, debemos asignar permiso de control total al usuario **Invitado**.

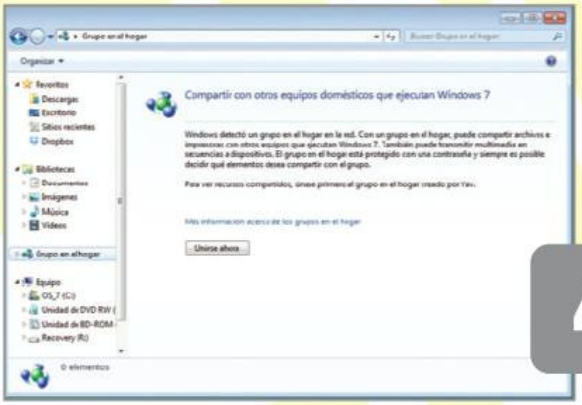
Samba

Un problema habitual en grandes redes es la necesidad de compartir archivos entre distintos sistemas operativos, por ejemplo Ubuntu, Windows, y Mac. Samba (renombrado recientemente como CIFS) es una implementación libre para archivos compartidos entre distintos sistemas. Así, es posible que PCs con Windows, GNU/Linux o Mac OS se vean como servidores o actúen como clientes en red. Ofrece múltiples posibilidades: acceso a recursos, autenticación y control de accesos, resolución de nombres, o publicación de servicios.

Cómo compartir recursos en Windows

Aquí aprenderemos a compartir archivos y recursos dentro de una red hogareña bajo un sistema Windows.



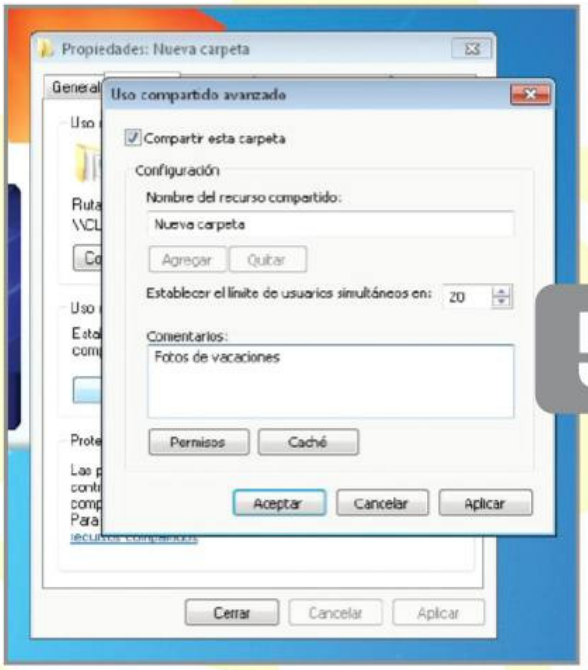


1 Antes de seleccionar carpetas o recursos para compartir, debemos activar el uso compartido de archivos, desde el **Panel de Control**. Vamos a **Centro de redes y recursos compartidos**. En el menú de la derecha, hacemos clic en **Cambiar configuración de uso compartido avanzado**.

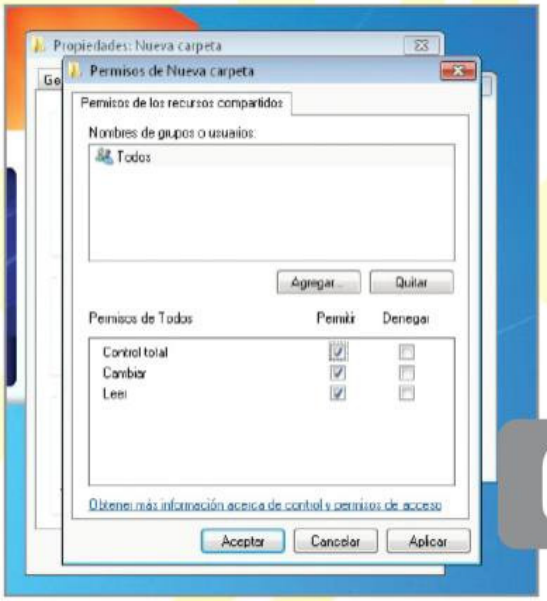
2 Luego, activamos la opción **Activar el uso compartido de archivos e impresoras**. También podremos activar el uso compartido de la carpeta pública. Esta carpeta se podrá compartir con todos los usuarios creados en el mismo equipo.

3 Para compartir rápidamente nuestros documentos, impresoras, biblioteca de música, podemos configurar **Grupo en el Hogar**, escribiendo en el menú **Inicio**, **Grupo Hogar**, esto nos llevará a su configuración. Cuando creamos el grupo, se genera una contraseña automática que más tarde podemos cambiar.

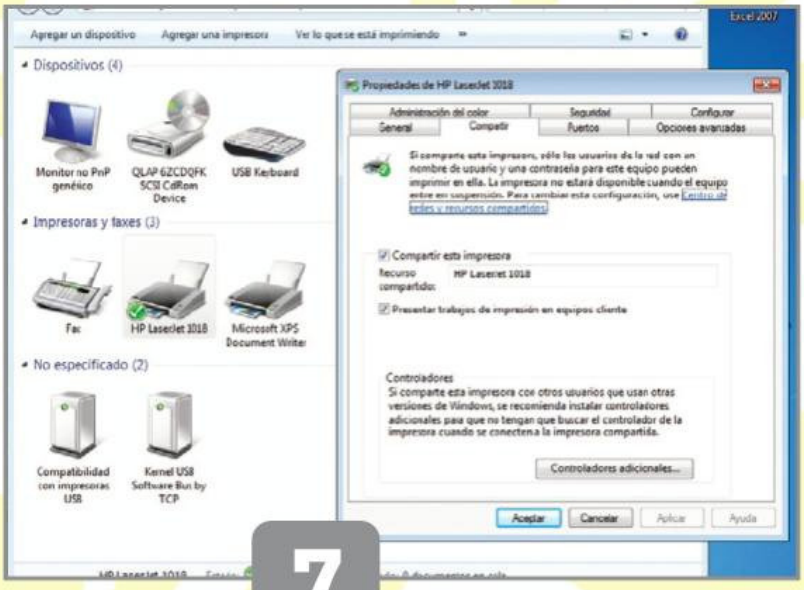
4 Cuando entramos a la configuración de **Grupo en el Hogar** desde otro equipo, nos avisará que otro equipo ya ha creado un grupo, y nos dará la opción de unirnos a él. Si hacemos clic en **Unirse ahora**, nos pedirá la contraseña del grupo creada en el equipo que creó el **Grupo**.



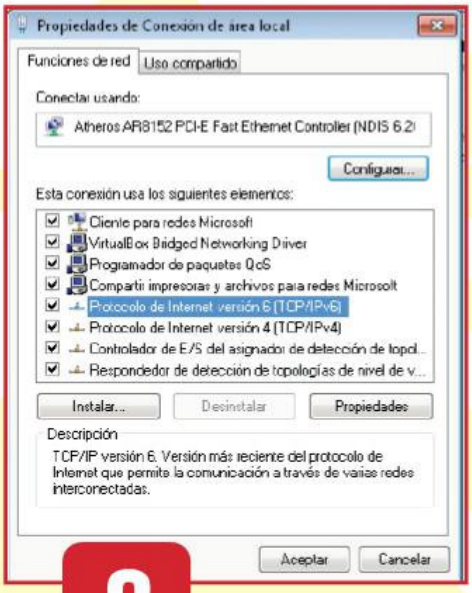
5



6



7



8

5 Para compartir una carpeta específica, hacemos clic derecho sobre la carpeta y vamos a **Propiedades**. En la pestaña **Compartir**, hacemos clic en **Uso compartido avanzado** y, en la ventana que se abre, tildaremos la opción **Compartir esta carpeta**. Aceptamos todos los cambios.

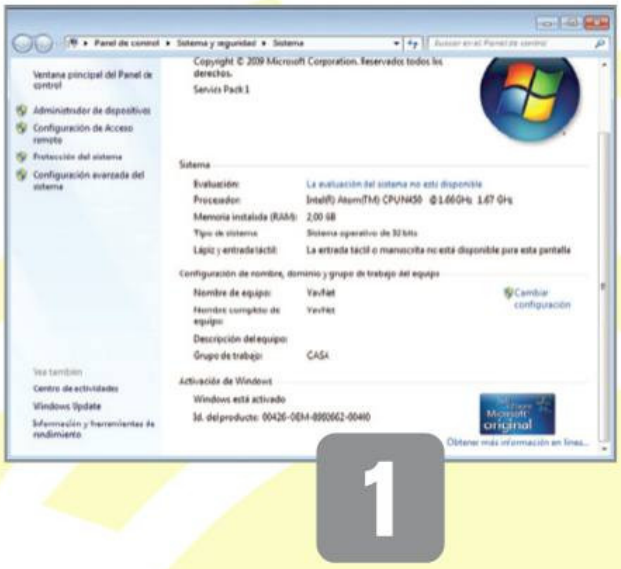
6 La carpeta que compartimos quedará disponible para los equipos del **Grupo Hogar** y, además, tendrá el atributo de **Solo lectura**. Si queremos que los demás usuarios puedan modificar los archivos, en la pestaña **Permisos** tildamos la opción **Control Total**.

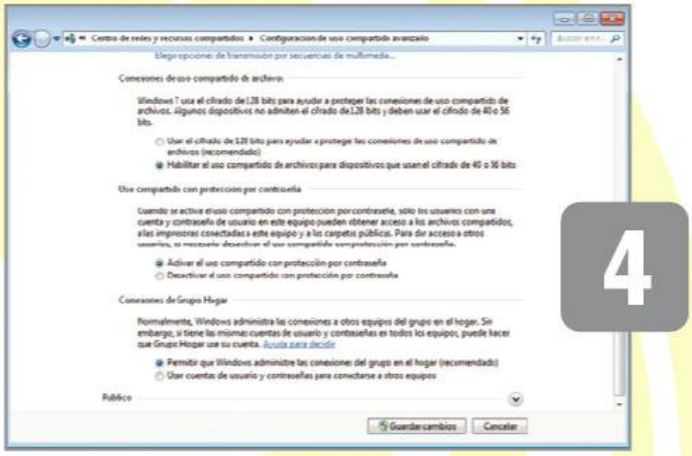
7 Para compartir una impresora vamos a **Inicio/Dispositivos e Impresoras**, hacemos clic derecho y pulsamos **Propiedades de la Impresora**. En la pestaña **Compartir**, tildamos la opción **Compartir esta impresora**, y podemos poner un nombre distintivo a la impresora compartida. En los demás equipos, se detectará en forma automática la impresora.

8 Para formar parte de un **Grupo Hogar**, todos los equipos deben tener sincronizada la hora, y, en las **Propiedades de la conexión de la red local**, debe estar habilitado el **Protocolo IPv6** (aunque no lo usemos en nuestra configuración).

Cómo compartir recursos en Linux

En estas páginas, revisaremos la forma en que podemos compartir recursos entre un sistema GNU/Linux y acceder desde Windows.



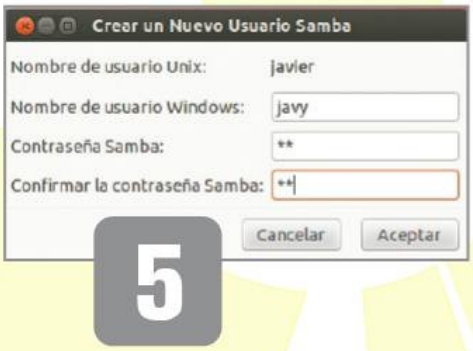


1 Para compartir recursos entre diferentes sistemas todos los equipos deben estar dentro del mismo grupo de trabajo. En Windows, haciendo clic derecho sobre **Equipo**, y luego en **Propiedades**, podemos ver un resumen de la configuración y el nombre del grupo de trabajo.

2 Desde Ubuntu, para configurar el grupo de trabajo, primero debemos instalar el paquete **Samba**. Desde el **Centro de Software Ubuntu**, escribimos en el buscador **Samba** y, luego, hacemos clic en **Instalar** en el paquete elegido. Para instalar este paquete, se nos pedirá la contraseña de usuario avanzado o **root**.

3 Después, aparecerá el icono correspondiente en la barra de iconos de la izquierda. Abrimos **Samba**, y desde **Preferencias/Configuración del Servidor**, se abrirá una nueva ventana, en la cual podemos configurar el nombre del grupo de trabajo, que deberá ser el mismo que el que tenemos en el equipo con Windows. Aceptamos los cambios.

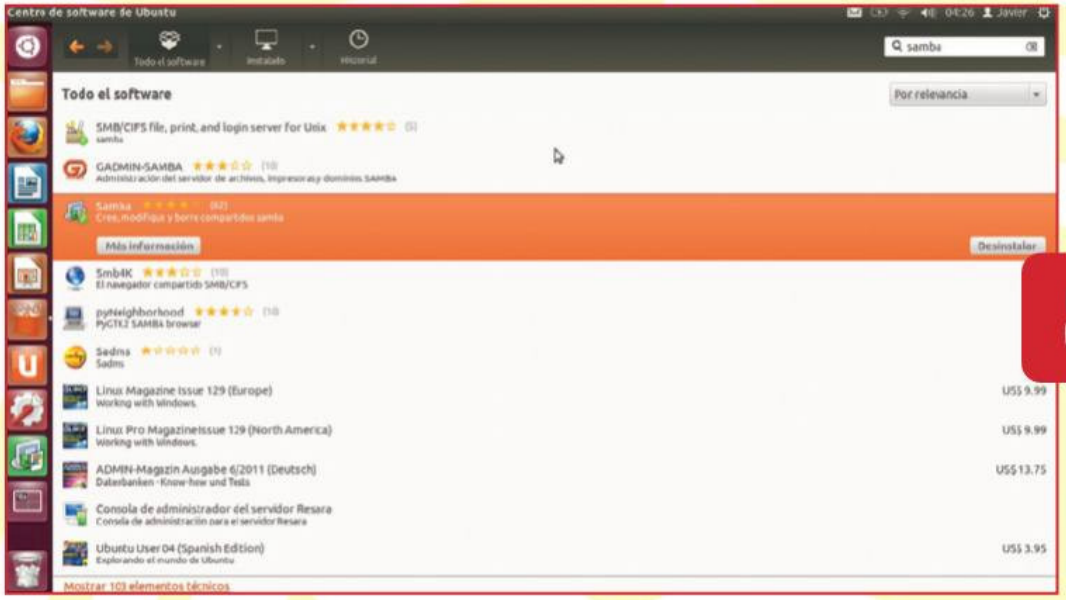
4 En Windows, desde el **Panel de Control/Centro de Redes y Recursos compartidos/Configuración de Uso compartido Avanzado**, en la sección **Uso compartido con protección de contraseña**, activamos y guardamos los cambios.



5

6

7



8

5 En Ubuntu, desde **Configuración del Servidor Samba**, en **Preferencias**, hacemos clic en **Usuarios Samba**. Aparecerá el usuario, el que hayamos creado durante la instalación. Podemos usar el nombre de usuario de Windows, que debe ser el nombre que tenemos en el equipo con Windows. Aceptamos los cambios.

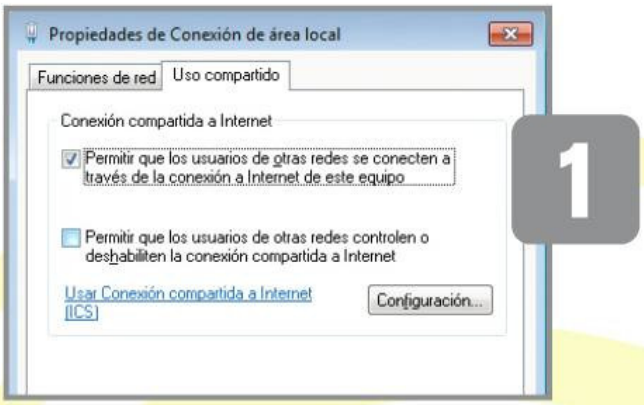
6 En Ubuntu, vamos a **Carpeta Personal** y, en **Examinar el contenido de la red**, veremos los equipos Windows. Al hacer doble clic sobre un equipo, se nos pedirá el nombre de usuario y contraseña. Este nombre es el que configuramos en Samba, y debe ser el mismo que tenemos como usuario de Windows.

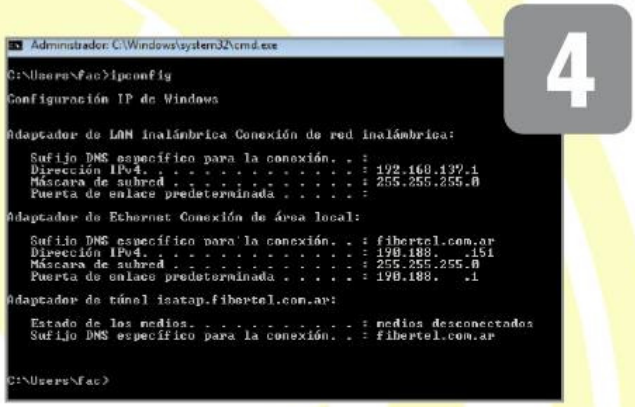
7 Para compartir una carpeta desde Ubuntu con Windows o Ubuntu, desde la **Configuración del Servidor Samba**, hacemos clic en el icono +. Seleccionamos el directorio que queremos compartir, tildamos las opciones de **Permiso de Escritura** y **Visible**. Luego aceptamos todos los cambios.

8 Para compartir recursos desde GNU/Linux, debemos instalar el paquete Samba, ya que es el que nos ofrece los servicios para compartir. En Ubuntu, desde el **Centro de Software**, buscamos **Samba** e instalamos el que nos agrade. Los usuarios avanzados pueden instalarlo y configurarlo desde la terminal utilizando comandos.

Compartir la conexión a

Aquí aprenderemos a utilizar nuestro equipo de escritorio configurándolo como enrutador de paquetes TCP/IP, formando nuestra red local con salida a Internet.





1 Conectamos nuestra WAN que proviene del módem en la placa de red Ethernet, luego nos conectamos a la red inalámbrica, con DHCP deshabilitado. Ingresamos a **Configuración del Adaptador**, y presionamos el botón derecho del mouse en **Conexión de área local/Uso Compartido**; aquí tildamos la primera opción, para compartir el recurso de red.

2 Volvemos a la solapa **Funciones de Red** y desmarcamos las opciones **Cliente para redes Microsoft**, **Compartir impresoras y archivos para redes Microsoft**, y **Protocolo de Internet versión 6 (TCP/IPv6)** en caso de que usemos IPv4. Dejamos recursos compartidos a nuestra red WAN.

3 Ahora, procedemos a verificar nuestra tarjeta de red inalámbrica; para ello, nos aseguramos de que se encuentre activa y conectada a la red inalámbrica. Verificamos que nuestro access point, brinde la red Wi-Fi con seguridad WPA2, mediante el cual vamos a conformar nuestra red LAN.

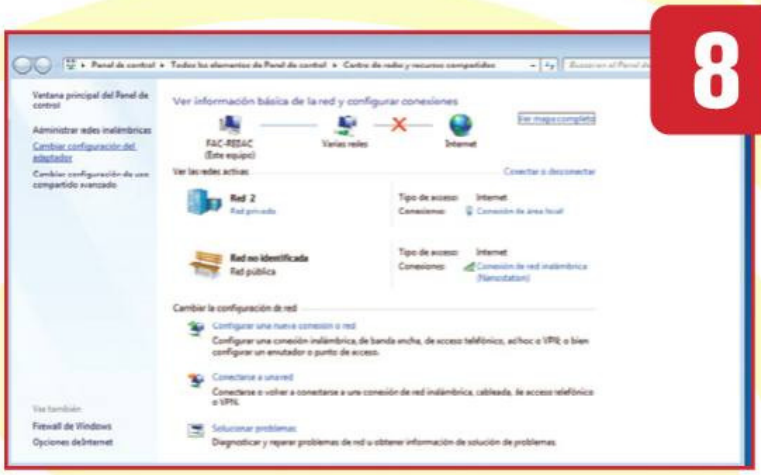
4 Vamos al **Inicio** e ingresamos **cmd**. Escribimos **ipconfig** y observamos que la red inalámbrica adoptó una IP privada de rango **192.168.137.1**, que es por defecto la que usa ICS. Luego de esto, en la Ethernet, tenemos nuestra IP pública entregada por nuestro proveedor de Internet **190.188.xxx.151**.

Internet usando ICS

5

6

7



8

5 Abrimos nuestro navegador para corroborar conectividad e ingresamos a **www.canyouseeme.org** para corroborar con qué IP pública estamos saliendo a Internet. Verificamos que es la IP pública que nos entrega nuestro proveedor de Internet.

6 Luego nos vamos a otro host de la red conectado a nuestro access point, y observamos que nuestro DHCP asigna la IP 192.168.137.184. Aquí confirmamos que Windows 7 está brindando este servicio a todos los hosts de nuestra red.

7 Realizamos este último paso de configuración para corroborar que salimos a Internet con la misma IP pública otorgada por nuestro proveedor, confirmando que Windows 7 nos esta enrutando, es decir, que cuando realizamos una petición, por ejemplo HTTP, el enrutador encapsula nuestro paquete, de manera que, al regresar con el contenido, este lo desencapsula para volver a entregarlo a nuestro host.

8 Si nos encontramos con una conectividad limitada o nula, sin acceso a Internet en todos los hosts de la red, podemos solucionarlo de la siguiente forma. Hacemos un reseteo del módem y ejecutamos los comandos `ipconfig /release` para limpiar las interfaces, luego `ipconfig /renew` para que se vuelvan a realizar las peticiones de IP y DNS del proveedor.

Networking entre dispositivos multimedia

Los gadgets nos hacen la vida más social, y aquí lograremos que interactúen para poder disfrutar de audio y video desde cualquier equipo.

La diversidad de equipos multimedia en nuestro hogar nos ha llevado a la necesidad de interconectarlos. Por ejemplo, desde nuestro Smartphone, reproducir un video familiar en el televisor; desde nuestra notebook, reproducir música en el equipo de audio, o, desde la consola de video, reproducir una película en Blu-ray sobre nuestra tablet.

DLNA

DLNA (*Digital Living Network Alliance*) es una tecnología que nos permite compartir contenido multimedia a través de nuestra red, sobre equipos que hasta ahora no tenían conexión a la red. Es necesario disponer de un servidor (*Digital Media Servers* o **DMS**) y de receptores para reproducirlo (*Digital Media Players* o **DMP**). Como servidor, no nos encasillemos en una PC o una notebook; hay discos del tipo NAS (*Network Attached Storage*) y celulares de alta gama, con esta tecnología. Para receptores, podemos usar un equipo de música hogareño certificado o un Smart TV, pero la diversidad de equipos certificados como servidor o cliente es mucha: cámaras de fotos, cámaras de video, reproductores Blu-ray, etc.

Un Apple TV es uno de los dispositivos más populares que podemos encontrar entre los usuarios de IPhone o IPad.

Con este logo, podremos identificar qué dispositivos son compatibles para interoperar con el resto de nuestra red.

La popularidad de esta norma se debe a que el DLNA es una organización sin fines de lucro con más de 250 empresas de la electrónica de consumo, móvil y PC, en las que se incluyen las principales marcas líder.

Una gran ventaja que tienen los equipos certificados con DLNA es que no necesitaremos configurarlos. Gracias al protocolo UPnP (*Plug and Play*), los dispositivos conectados a la misma red se detectan de manera automática entre sí. Solo la interfaz difiere por cada fabricante. Supongamos, por ejemplo, que vamos a casa de un amigo que tiene una TV con DLNA, y nosotros desde nuestro teléfono móvil queremos mostrarle el video de nuestras últimas vacaciones. Simplemente, tenemos que abrir la aplicación DLNA en el celular y elegir reproducir la película en su Smart TV, así de fácil.

Este sistema utiliza la tecnología de protección de datos DRM, por lo que algunos contenidos protegidos no podrán leerse.

AirPlay

Con **AirPlay**, podemos reproducir el contenido de nuestro dispositivo iOS en el televisor mediante un equipamiento llamado Apple TV que se conecta a cualquier televisor. La popularidad de los iPhone o iPad es innegable, y un pequeño dispositivo externo

como el Apple TV, compatible con cualquier televisor, ha ganado mucho terreno en los últimos años. Sus funciones son:

- **Streaming**: si las fotos o videos que estemos viendo en nuestro iPhone o iPad merecen verse a lo grande, simplemente seleccionaremos el icono de AirPlay desde la app, y todo se reproducirá en streaming sobre el televisor HD
- **Reproducción en espejo**: permite compartir el contenido de nuestra Mac, iPhone, iPad sobre la TV. Los demás verán exactamente lo mismo que nosotros en nuestra pantalla.
- **Dual Screen**: en nuestro iPhone o iPad, veremos solo una parte de la aplicación, que emplearemos como control remoto, y el resto se verá en la pantalla de la TV conectada al Apple TV.

Miracast

Miracast es un nuevo protocolo similar al DLNA, que nos permitirá transmitir audio y video mediante Wi-Fi (802.11n) entre distintos dispositivos. Podremos disfrutar de cualquier contenido multimedia en cualquier aparato de nuestro entorno que soporte esta tecnología.

La versión de Android 4.2, el sistema operativo de Google, soporta ahora Miracast, y nos permite transferir el contenido de nuestro teléfono celular o tablet a un Smart TV por WiFi. Quizás hoy no sea la tecnología más popular, pero, si en esta última versión de Android se ha implementado esta característica en forma nativa, todos los celulares y tablets Android que se fabriquen de ahora en adelante deberían poder soportarla.

Si hablamos de seguridad, Miracast soporta el cifrado WPA2-PSK, y todo lo que compartamos estará bien protegido.

El sistema dispone además de una protección de derechos de autor. Quizás a algún desprevenido le pueda alarmar esta prestación.

UPnP

UPnP MediaServer es cualquier dispositivo UPnP capaz de listar el contenido multimedia almacenado, para que el usuario pueda seleccionar el que desea renderizar y que sea transmitido en la red doméstica.

El **UPnP MediaRenderer** es el dispositivo UPnP capaz de reproducir el contenido multimedia y controlar su renderización, como el volumen o mute audio, o el brillo y contraste para video, y por supuesto, controlar la reproducción (Play, Stop, etc.).

Existen muchos software compatibles con los estándares UPnP AV, con licencia libre o propietaria. Pero el ya conocido XBMC (XBox Media Center) es un centro multimedia de entretenimiento bajo la licencia GNU/GPL, que corre con la ventaja de ser multiplataforma. Cualquier dispositivo que queramos conectar, ya sea una notebook, una tablet, un smartphone, o casi cualquier gadget que se nos ocurra, contará con una aplicación cliente/servidor, y si no deseamos instalarlo, nos provee de una completa interfaz web.

Entre las muchas ventajas del software, está la compatibilidad con DNLA, para una mayor interoperabilidad.

La única limitación de este software es que XBMC no reproduce ningún archivo de audio/video cifrado con DRM (*Digital Rights Management*), como música que adquirimos en la tienda iTunes.

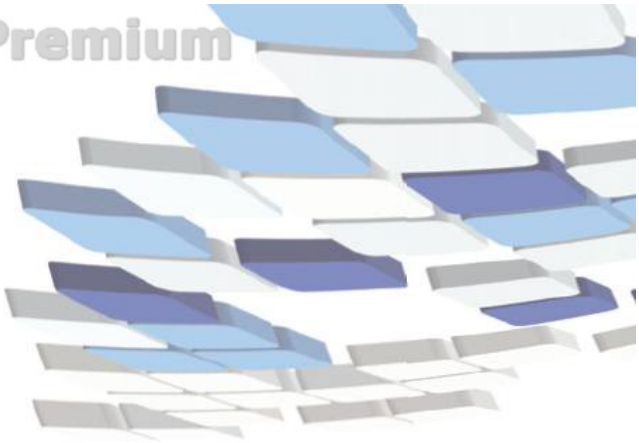
La **reproducción en espejo** nos permite compartir lo que vemos en nuestro iPhone con los demás integrantes de la casa.

Alternativas

Muchos usuarios tienen una PC conectada al televisor. Si este es nuestro caso, seguramente nos interesará instalar un Servidor Multimedia UPnP AV. Algunas alternativas son: 360 Media Server, con licencia GPL, gratuito y multiplataforma (Windows y Linux). AllShare de Samsung, es un software servidor DLNA gratuito que se puede descargar de la página de Samsung. Serviio, tiene una versión gratuita y otra paga, para Windows, Mac, Linux y hasta para discos externos NAS.■

Reproductor de Windows Media

El **Reproductor de Windows Media** es el **servidor DMS** más fácil de obtener, ya que está incluido en nuestra PC o notebook con Windows 7. La característica **Play to** o **Reproducir en**, nos brinda la posibilidad de reproducir música y videos en otros equipos con certificación DNLA, u otra PC ubicada en nuestra LAN.Con esta función, podremos cargar una lista de reproducción y elegir en qué dispositivo queremos reproducirlo por medio de **streaming**.



Tecnologías SAN y NAS

Aquí veremos la evaluación de comportamiento y redundancia de soluciones de almacenamiento, basadas en estructuras de red. Detalles para una correcta elección e implementación de storages.

Es creciente el número de empresas PyMEs, o de pequeña y mediana envergadura, que incorporan soluciones del estilo file servers, o servidores de archivos. En menor escala, se ubican soluciones encontradas por el usuario básico de una computadora, que es la carpeta compartida, donde todos los usuarios acceden, suben, modifican archivos desde este recurso. Resulta claro que este recurso deja falencias en toda su estructura, ya que cualquier usuario no deseado que ingrese a nuestra red tendrá absolutamente toda la información requerida sin mayores esfuerzos. Por otro lado, contamos con soluciones **file server**, ya con más estructuras y permisos de accesos a usuarios de la red; allí tenemos una falla corregida, que son los permisos de usuarios que se dan sin indagar con profundad los tipos de protocolos y mecanismos de autenticación. De esta manera, podemos tener una organización de jerarquías a nivel permisos divididos por grupos o áreas y usuarios. Así, es posible compartir archivos entre grupos, sin la necesidad de brindar archivos con permisos de escritura o ejecución. Como conclusión, podemos definir que permitiremos solo lo que va a poder leer, escribir y ejecutar cada usuario con su respectivo ID y contraseña privada.

Año a año, las empresas y corporaciones son más dependientes de diversas tecnologías, sobre todo con las interacciones con Sistemas, y estos, con sus respectivas Bases de Datos. Estos son los momentos en los que se disponen grandes unidades de almacenamiento para la interacción, a veces, las 24 horas del día, con una menor necesidad de eficiencia y disminuido costo operativo.

Para ello, vamos a dejar de lado los RAIDs para escalar niveles de tecnologías, con el fin de acercanos a entornos de producción reales, donde los segundos en búsquedas de registros, la seguridad de la información y la pérdida de datos tienen grandes costos e impactos.

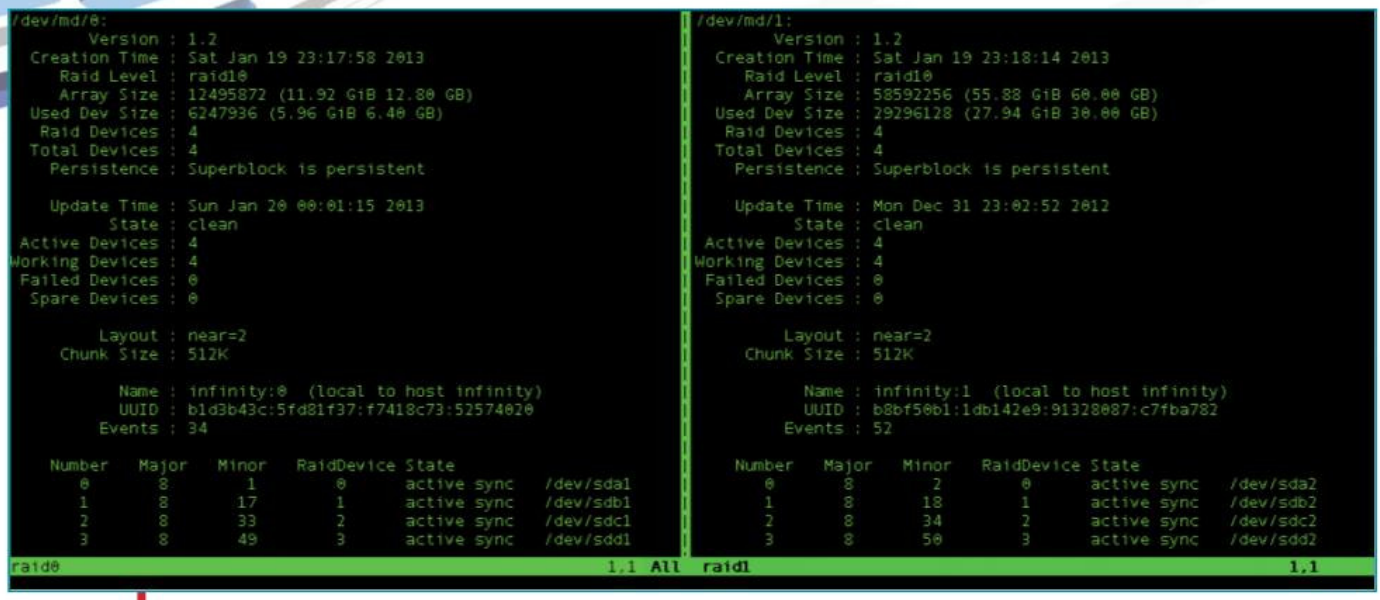
```
#       is mounted on /cdrom
#
;   preexec = /bin/mount /cdrom
;   postexec = /bin/umount /cdrom
[comex]
comment = Comercio Exterior
path = /opt/comex
valid users = @comex # todos los usuarios del grupo COMEX
write list = @comex
read only = No
browseable = Yes
[sistemas]
comment = Directorio de Sistemas
path = /opt/sistemas
valid users = @sistemas, gmoglie, #todos el grupo sistema y GMOGLIE
write list = @sistemas, gmoglie
read only = No
browseable = Yes
[ingenieria]
comment = Directorio Ingenieria
path = /opt/ingenieria
valid users = @ingenieria, fgandhi, mverta, nlombide
write list = @ingenieria
read list = fgandi, mverta, nlombide
read only = No
browseable = Yes
[programacion]
comment = Directorio de Programacion
path = /opt/programacion
valid users = @programacion, nlombide
write list = @programacion
read list = nlombide
read only = No
browseable = Yes
[rrhh]
comment = Directorio de RRHH
path = /opt/rrhh
valid users = @rrhh, fganhi
write list = @rrhh, fganhi
create mode = 777
directory mode = 777
read only = No
browseable = Yes
[serviciotecnico]
comment = Directorio Servicio Tecnico
path = /opt/serviciotecnico
valid users = @serviciotecnico, mverta
```

Archivo de configuración del servicio SAMBA en GNU/Linux, con una estructura básica de File Server, y permisos de grupos y usuarios.

SAN – Storage Area Network

Es una arquitectura basada en unificaciones de distintos protocolos y diversos dispositivos que dieron lugar a esta tecnología, en la que mediante protocolos red y almacenamiento, **SAN** brinda storage o almacenamiento a toda nuestra planta servidora, de ahí, la denominación Red de Área de Almacenamiento.

Switch Fibre Channel para la i



La imagen muestra una configuración de RAID 1+0 en MD en GNU/Linux Debian, con cuatro discos SCSI, montado en un servidor de base de datos MySQL.

La SAN puede utilizar canales fibra o Ethernet mediante **iSCSI** para proporcionar la conectividad entre los hosts y el almacenamiento, y quedar aislada de nuestra red **LAN** (*Local Area Network*). De esta forma asegura una entrega confiable a baja latencia entre dispositivos, ya que la SAN demanda un alto grado de ancho de banda, teniendo en cuenta que el acceso es a bajo nivel de bloque, es decir, trabaja o accede a ficheros de manera similar a un disco local SATA de un host.

Todos los servidores involucrados tienen acceso directo a todos los RAIDs o arreglo de discos a través de la SAN; a la vez, los escritorios o áreas de trabajo llegan a los datos mediante los servidores que les hacen el procesamiento y lógica, es decir, los storages almacenan y gestionan internamente la disponibilidad de los datos para ser compartidos a varios servidores, que hacen uso para llevar los datos de una manera eficaz, ya que se aliviana el procesamiento lógico de sistemas o bases de datos.

Una implementación SAN nos asegura una alta disponibilidad de datos, incorporando redundancia en los sistemas críticos de una empresa, ya que esta tecnología agrega protección contra fallas y capacidad de ruteo alterno en forma automática, que son claves a la hora de implementar una estructura de datos centralizados, una característica primaria de esta tecnología.

Cuando un administrador de red hace una disposición de backups para tener un respaldo de datos, realiza una tarea crítica en una red convencional, ya que se debe realizar en períodos en que la red esté en bajos niveles de consumo, pero se vuelve dificultosa cuando la red está operativa durante las 24 horas, tales son los casos de editoriales, periódicos o empresas de doble y triple jornada. Las redes SAN manejan un concepto de **serverless backup**, es decir, los datos se gestionan sin pasar por los servidores y, de allí, se mueven a las unidades de cintas o al dispositivo designado para dicha tarea; esto aumenta la

mplementación de redes SAN utilizados en topologías FABRIC.

NAS como storage de virtualización

En las soluciones en entornos de virtualización, se utilizan comúnmente storages NAS por NFS, por ejemplo, para configurar HA (alta disponibilidad) entre dos o más servidores de virtualización, como es el caso de Citrix XenServer (Free Edition). De esta manera, se comparten los discos y las máquinas virtuales que son aprovisionadas desde el NAS; esto favorece la tolerancia de fallos ya que, si sufrimos algún error de Hardware, en forma automática podemos arrancar o inicializar la misma máquina virtual en el otro servidor virtualizado que tenemos de respaldo.

Servidor NAS de categoría empresarial, con la particularidad de tener discos HOT SWAP.

disponibilidad de recursos del servidor, tales como los ciclos del procesador, acceso a memoria, y ancho de bandas para acceso a dichos recursos. Para resumir este concepto, diremos que el usuario operativo nunca percibe cuándo se está realizando un backup, ni presenta alteraciones a la hora de realizar su tarea, interactuando con el servidor en forma normal.

Para finalizar con SAN, vamos a considerar los elementos involucrados, contando con que ya tenemos una introducción a los RAIDs. Para la interconexión entre el almacenamiento y los servidores, podemos hacer uso de conectores de cobre y fibra óptica multimodo o monomodo, además de adaptadores de medio como **MIA** (*Media Interface Adapters*), convertidores de interfaz GBIC (*Gigabit Interface Converters*) y extensores de alto rendimiento que brindan mejoras con respecto a las distancias y enlaces, como GLM (*Gigabit Link Module*).

ZFS OFRECE LA POSIBILIDAD DE REALIZAR SNAPSHOTS DE LAS UNIDADES DE ARCHIVOS, YA QUE NO LIBERA LOS BLOQUES UTILIZADOS POR OTRAS VERSIONES ANTIGUAS DE ARCHIVOS.

HBAs (*Host Bus Adapters*) son adaptadores que se utilizan para conexiones de almacenamiento y servidores a la red Fibre Channel. Sus distintas versiones dependen de la topología, cables por utilizar y protocolos soportados.

Hubs Fibre Channel son utilizados para implementar conexiones Arbitrated Loop (FC_AL), que es el nombre de una topología de Fibre Channel.

Switch Fibre Channel son equipos de conmutación encargados de encaminar el tráfico entre múltiples dispositivos, incluso con otros switches, y se utilizan en las topologías Fabric.

Por último tenemos **Bridges**, usados para integrar o conectar un dispositivo SCSI a la red Fibre Channel.

NAS – Network Attached Storage

Un servidor **NAS** es una tecnología de almacenamiento dedicada a compartir su capacidad con dispositivos dentro de una red LAN mediante protocolos, como por ejemplo **NFS** (*Network File System*), **FTP** (*File Transfer Protocol*), **CIFS** (*Common Internet File System*) para los sistemas operativos Windows, ya sea administrados o accediendo por protocolos de red TCP/IP.

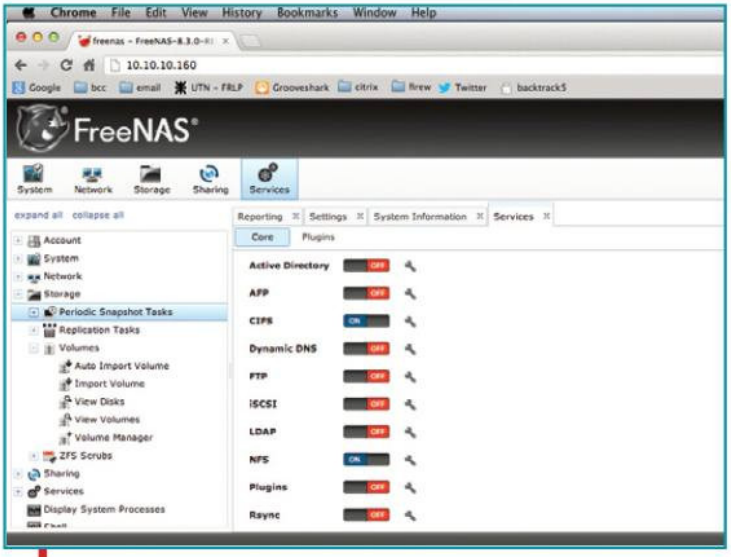
NFS es un protocolo del nivel aplicación basado en el modelo OSI; fue desarrollado por SUN para los sistemas distribuidos en un entorno de red y luego implementados en sistemas operativos UNIX y en la mayoría de distribuciones GNU/Linux.

CIFS es la modificación del protocolo SMB desarrollado por IBM, que luego utilizó Microsoft renombrando el protocolo y añadiendo algunas características, como enlaces simbólicos, más conocidos como accesos directos.

Este protocolo de comunicaciones, a diferencia de SAN, hace llamados a los datos para ser almacenados en la propia caché del cliente, para luego ser manipulados; esta es una limitación cuando se trabaja en archivos de grandes tamaños. De esta manera, se recomienda hacer uso de gran cantidad de archivos en pequeños tamaños.

Con respecto a servidores NAS, podemos encontrar gran variedad en el mercado, que van desde soluciones hogareñas a servidores de empresas más conocidas del rubro, que ya ofrecen sus soluciones con múltiples discos y placas de red, por lo general, ya con el sistema operativo y el acceso web para su configuración. Una analogía de estas soluciones a gran escala se debe al uso de grandes capacidades de almacenamiento, orientado a distintos dispositivos de red que hacen uso de esta tecnología mediante acceso de red; de esta manera, si contamos un storage con la capacidad de 2 Terabytes redundante con RAIDs 1 + 0 (*Stripe of Mirrors*), donde acceden varios servidores y usuarios de red, nos encontraríamos con un cuello de botella en la Ethernet de nuestro NAS; por eso, en muchos casos se utilizan múltiples placas de red configuradas en BOND.

El **controlador bonding** está incluido en casi todas las distribuciones de GNU/Linux y permite sumar la capacidad de varias interfaces físicas de red, creando una interfaz lógica con el objetivo de tener redundancia y balanceos de cargas entre estas, siendo transparente para el dispositivo contactado con ellas.
NAS es una tecnología robusta con pequeñas limitaciones, pero muy eficaz a la hora de resolver problemas tanto de seguridad como de rendimiento, a un bajo costo. Existen diversos tipos de implementación y configuraciones para implementaciones del tipo NAS; esto depende de nuestro servidor y la capacidad de agregar discos al sistema. Existe una tecnología JBOD que es una concatenación de discos físicos para formar uno lógico, una especie de RAID 0, pero solo necesitamos agregar disco para que el volumen lógico aumente su capacidad; si bien no es un sistema redundante del cual no recomendamos su uso, cabe mencionar que es posible aumentar la capacidad con el solo hecho de conectar un dispositivo.
Entre las ventajas, además del costo de las implementaciones, podemos mencionar que en muchos casos se utiliza NAS por medio de NFS, por ejemplo, para **storages compartidos** por varios servidores, y poder montar un sistema distribuido del tipo Clúster con placas de red dedicadas directamente a los servidores, simulando una SAN mediante topología TCP/IP. Es recomendable en este tipo de infraestructura contar con hardware apropiados, es decir, una buena configuración de **QoS** o **Calidad de Servicio**, e interfaces que soporten velocidades de 100/1000, para un correcto funcionamiento y para disminuir los riegos de caídas y cuellos de botellas.
Entre los distintos servidores que podemos mencionar, también se encuentra el montado por nosotros mismos, nuestro propio y personalizado NAS, mediante distribuciones basadas en GNU/Linux, como son **OpenFiler** y el conocido **FreeNAS**; este último es un enlatado que podemos administrar mediante una interfaz web, con la posibilidad de brindar muchos servicios (iSCSI, CIFS, NFS), también aquí podemos crear usuarios y grupos de accesos a los recursos y una particularidad como son los snapshots de los storages o programarlos periódicamente, a fin de tener un primer respaldo de datos o simplemente volver atrás algunos cambios realizados en nuestra estructura.
Estos **snapshots FreeNAS** se deben al sistema de archivos **ZFS** (*Zettabyte File System*). ZFS es un protocolo que liberó SUN para sus sistemas OpenSolaris bajo plataformas SPARC, y ahora utilizado por **FreeNAS BSD.** Entre sus grandes ventajas, podemos mencionar que ZFS con una autorreparación (**self-healing**) trabaja de manera similar a un RAID 5, es decir, hace un hash de todos los bloques lógicos, y las tomas **instantáneas** o **snapshots** mencionados antes se deben a que ZFS no libera los bloques utilizados por versiones antiguas de datos.■



Interfaz web para acceso de configuración de FreeNAS, visible con los servicios disponibles por utilizar.

En esta imagen vemos un servidor NAS de 4 TB, distribuido por la empresa Western Digital.

Sistemas híbridos SAN-NAS

Entre la variedad de tecnología y protocolos, también podemos utilizar un híbrido entre SAN y NAS. Teniendo en cuenta que ya contamos con una implementación SAN, solo nos restaría configurar un servidor NAS aprovisionado desde las unidades SAN; de esta forma, NAS puede brindar, por sus protocolos, archivos en la red o unidades compartidas, con la redundancia y tolerancia a fallos que nos ofrece la tecnología SAN.

Permisos y seguridad en recursos desde Windows

En esta oportunidad, veremos cómo configurar correctamente los permisos y la seguridad de los recursos compartidos en entornos Windows.

Cuando trabajamos dentro de una red, tenemos la posibilidad de utilizar archivos, carpetas y hasta unidades completas sin necesidad de tenerlas físicamente en nuestro equipo. ¿Qué significa esto? Significa que, haciendo uso de un recurso de Windows conocido como Uso Compartido, podemos utilizar los recursos mencionados mediante la conexión de la red a la que estemos vinculados. Por ejemplo, podríamos acceder al contenido de un DVD sin tener una unidad de ese tipo instalada en nuestro equipo. Todo dependerá de cómo configuremos el acceso compartido a los recursos disponibles en la red. Y hacia ese horizonte nos dirigimos. Entonces, veamos cómo hay que configurar los parámetros para que este recurso funcione de manera correcta.

En primer lugar, vamos a hacer una aclaración, ya que además disponemos de una alternativa de uso compartido de recursos más sencilla de poner en funcionamiento, pero también más limitada. Estamos hablando del Grupo Hogar.

Ejemplo práctico

Para volver al tema, podemos tomar un ejemplo práctico: una red de trabajo, pero en una pequeña oficina, con apenas cinco computadoras (no importa si son de escritorio, notebooks o netbooks en tanto todo esté configurado correctamente), a dos de las cuales hay conectadas una impresora en forma física.

Vamos a identificarlas: PC1 se ubica en la oficina del dueño de la PyME y tiene conectada una impresora inkjet color; PC2 se encuentra en otra habitación y funciona como servidor de impresión con una impresora láser blanco y negro conectada a ella; en otra habitación, se encuentran los oficinistas operando PC3, PC4 y PC5. A su vez, PC5 tiene un escáner conectado a uno de sus puertos. Todos los equipos de la red tienen configurado como nombre del grupo de trabajo OFICINA. Aclaramos esto, ya que todos los equipos conectados a la red deben operar bajo el mismo grupo de trabajo para que puedan verse entre ellos y, así, compartir sus recursos.

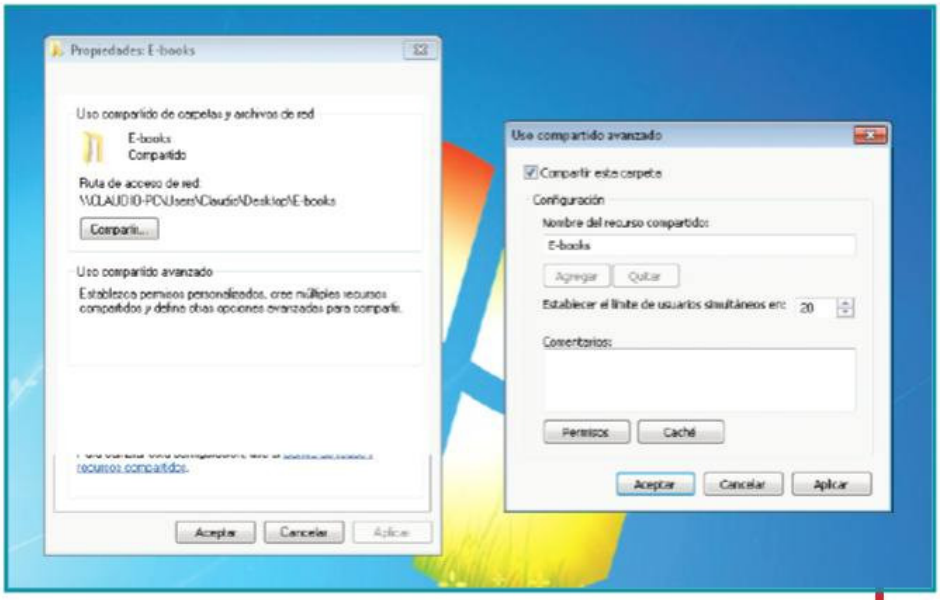
Entonces, si PC3 necesita imprimir un balance, lo hará apuntando a la impresora ubicada en PC2. Otra opción puede darse cuando PC5 necesite acceder a una planilla de Excel ubicada físicamente en la unidad D: de PC4, en cuyo caso, las acciones posibles estarán dictadas de acuerdo con los permisos configurados.

Para activar el uso compartido debemos utilizar la ventana Propiedades, en la solapa denominada Compartir.

El Grupo Hogar

Desde la salida al mercado de Windows 7, se incorporó una opción conocida como Grupo Hogar. Los equipos conectados a él, comparten de manera transparente bibliotecas tales como las de **Música**, **Imágenes**, **Videos** y **Documentos**. También es factible agregar bibliotecas personalizadas. Además de las bibliotecas, podemos acceder a las impresoras que están conectadas a cualquiera de los equipos que integran la red y se hayan conectado al **Grupo Hogar**. Cabe destacar que, para que el Grupo Hogar funcione correctamente, debe estar configurado dentro de una red identificada como **Doméstica** y solo se podrán unir equipos que configuren la conexión de dicha manera.

Al momento de compartir archivos e impresoras, tenemos dos alternativas: el uso compartido simple y el avanzado. El método simple, nos permite compartir archivos y carpetas creadas por cualquier usuario en tres simples pasos. Primero, abrimos el menú contextual de la carpeta o archivo por compartir con un clic derecho del mouse y accedemos a sus **Propiedades**; luego, en la solapa **Compartir** pulsamos el botón homónimo y, finalmente, en la pantalla emergente, seleccionamos con quién vamos a compartir el recurso del desplegable y lo agregamos; luego, seleccionamos el permiso que se le otorgará al usuario y pulsamos el botón **Compartir**. Hecho esto, la carpeta o archivo en cuestión debería estar disponible como recurso de red para el usuario que acabamos de indicar.



Al hacer clic en el botón **Uso compartido avanzado...**, tendremos acceso a una mayor personalización de las opciones.

Uso compartido avanzado

En cambio, el **Uso compartido avanzado** nos permite llegar más allá, pues nos dará la posibilidad de compartir la unidad principal (el disco **C:** o raíz del sistema operativo) y carpetas del sistema. De todos modos, es altamente recomendable compartir los recursos de manera individual ya que, al compartir toda la unidad **C:** o las carpetas de sistema, corremos el riesgo de que algún usuario elimine un archivo crítico (involuntariamente) tornando al sistema operativo, como mínimo, inestable.

En cuanto al **Uso compartido avanzado**, tendremos algunas opciones adicionales que podremos manipular para alcanzar los objetivos deseados. Veamos cómo podemos configurarlas.

Repetimos el procedimiento anterior, ingresando a las **Propiedades** de la carpeta que queremos compartir, pero esta vez haremos clic en el botón **Uso compartido avanzado...**. Activamos la casilla **Compartir esta carpeta** y le asignamos un nombre al recurso. Luego, podemos indicar la cantidad de usuarios que podrán utilizarlo simultáneamente, y debajo podemos ingresar algún comentario que nos permita identificar en forma específica el contenido del recurso compartido.

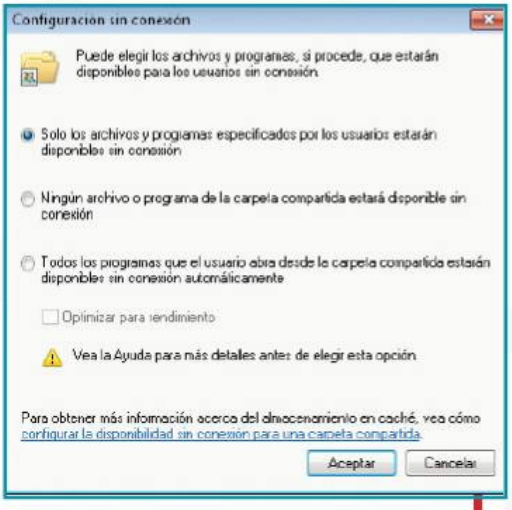
Hacemos clic en el botón **Permisos**; en la ventana que se presenta, podemos agregar o quitar usuarios de la lista y asignar permisos individuales. **Control total** le otorga al usuario la capacidad tanto de utilizar el recurso como de modificar o eliminar su contenido; la opción **Cambiar** nos permitirá modificar el contenido mas no eliminarlo; por último, la opción **Leer** solo nos permitirá visualizar el contenido, pero sin realizarle ninguna modificación ni eliminarlo.

Caché

Si hacemos clic en el botón denominado **Caché**, accedemos a las opciones que nos permiten indicar la disponibilidad de contenido sin conexión. Este contenido, según se especifique, podrá estar disponible aun cuando el equipo que creó el recurso no se encuentre conectado a la red. Veamos entonces qué podemos configurar.

La primera opción de la pantalla es la que se activa por defecto al compartir una carpeta. Con esta opción, son los mismos usuarios quienes controlan a qué parte del recurso compartido desean tener acceso sin conexión. En la segunda opción, se indica que no habrá ninguna parte del recurso compartido disponible sin conexión, por lo que, cuando el equipo servidor del recurso está desconectado, el recurso en sí queda inaccesible.

Finalmente, la tercera opción genera de manera automática la disponibilidad sin conexión de cualquier archivo del recurso compartido que un usuario utilice. Además, si tildamos la casilla de **Optimizar para rendimiento**, se hará lo propio con cualquier archivo **EXE** o **DLL** que el usuario cliente utilice, y lo almacenará en su caché local.■



En algunos casos, configuraremos la caché de trabajo sin conexión para asegurar el acceso a los archivos.

Permisos y seguridad en recursos desde Linux

En estas páginas, analizaremos la administración de grupos y usuarios, y sus respectivos permisos desde un sistema Linux.

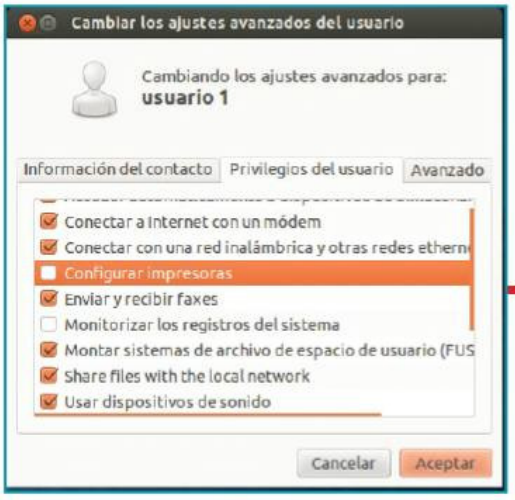
En las distribuciones basadas en GNU/Linux, al momento de crear usuarios y establecer sus permisos, podemos también establecer permisos directamente en carpetas o archivos específicos, con lo que es posible aumentar el nivel de seguridad, sobre todo si el equipo es compartido por varios usuarios. En todas las siguientes modificaciones que realicemos, se nos pedirá la contraseña del usuario root.

Administración de usuarios

Es posible agregar o modificar usuarios, desde **Configuración del sistema**, en el apartado de **Sistema/Cuentas de Usuario**. Para una cuenta de usuario nueva, hacemos clic en el símbolo +, y luego se nos pedirán datos muy básicos, como tipo de cuenta (**Estándar** o **Administrador**), nombre completo y nombre de usuario. Si queremos editar más detalles, debemos hacerlo a través de la terminal.

Para agregar usuarios y modificar varios detalles desde el modo gráfico, instalaremos el paquete **gnome-system-tools** desde el **Centro de Software de Ubuntu**. Aparecerá en la barra de la izquierda, un icono nuevo con la leyenda de **Usuarios y Grupos**. Si no aparece, desde **Inicio** escribimos **Usuarios**, y lo veremos.

Con esta herramienta, al crear un usuario, podemos definir todas sus configuraciones, dónde se guardarán sus archivos, información de contacto.



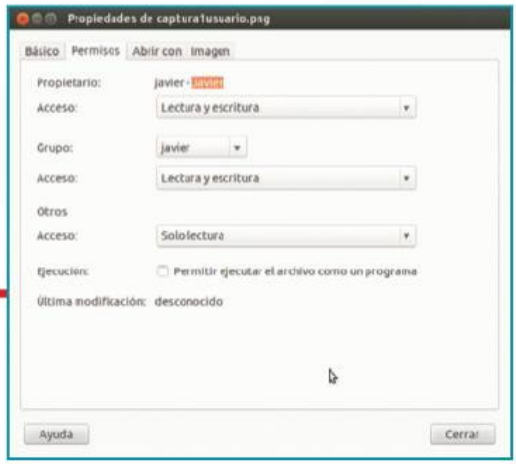
Al usuario1, que estamos creando, le hemos quitado los privilegios de Configurar impresoras y Monitorizar los registros del Sistema.

Una de las características más importantes de este paquete es que nos permite configurar los privilegios del usuario, así por defecto podemos limitar las actividades que puede realizar el usuario. Si queremos eliminar un usuario, lo seleccionamos y hacemos clic en **Eliminar**. Se nos preguntará si queremos mantener o eliminar los archivos del usuario. Si no queremos eliminar al usuario, pero sí bloquearlo, lo podemos hacer desde **Ajustes avanzados**, donde tildamos la opción **Desactivar cuenta**.

Para crear usuarios desde el Terminal, utilizamos los comandos **sudo adduser nombredeusuario**. Se nos pedirá la contraseña de root, y luego todos los datos del usuario que estamos creando: contraseña, confirmación de contraseña, nombre completo de usuario y datos de contacto. También se creará por defecto el grupo con el mismo nombre que utilizamos para el usuario, quien será parte de ese grupo por defecto. Si queremos que el usuario sea parte de un grupo específico, escribimos **sudo adduser nombredeusuario nombredegrupo** (el grupo debe estar creado previamente).

Permisos globales

Se debe tener cuidado de no dar permisos globales a las aplicaciones, ya que cualquier usuario inexperto, al tener permisos de ejecución, podrá provocar daños en la configuración del sistema o borrar datos que no deseamos perder. Para una mayor seguridad, es recomendable dejar los permisos de ejecución de programas por defecto y, si algún usuario requiere un permiso en particular, evaluar la situación.



De la misma forma que creamos un usuario, creamos un grupo y elegimos a los usuarios que formarán parte de ese grupo.

Para modificar un usuario, utilizamos el comando **usermod**, seguido de un parámetro que indica qué deseamos modificar, por ejemplo, si queremos cambiar el nombre de usuario de Iván a Ricardo, escribimos **sudo usermod -l ricardo juan**, donde -l es de login. Para eliminar un usuario, escribimos **sudo userdel usuario**, con eso solo eliminaríamos al usuario; para borrar todos los archivos pertenecientes a él, escribimos **sudo userdel –r usuario**.

Gestión de grupos

Un grupo es un conjunto de usuarios a los cuales, para facilitar su administración, en vez de otorgar permisos a cada uno de ellos, se otorgan los permisos al grupo. Estos permisos pueden ser para utilizar hardware instalado, realizar modificaciones o poder compartir carpetas. Para establecer un directorio que sea un grupo específico, utilizamos el comando **chgrp** con la siguiente sintaxis: **chgrp nombredegrupo directorio**, si habíamos creado el directorio **tecnicos** en **/home/técnicos**, para que ese directorio sea del grupo **tecnicos**, en la terminal escribiremos **chgrp técnicos / home/tecnicos**. Luego, al directorio le daremos permisos totales de grupo, para que los archivos que se guarden ahí puedan ser leídos o modificados por cualquier miembro del grupo.

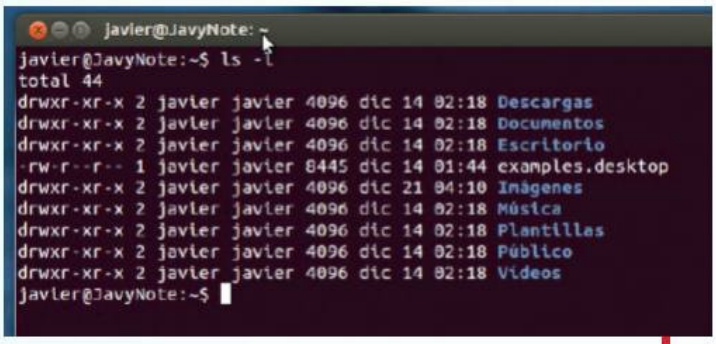
Permisos

Las carpetas y archivos tienen permisos para poder ser leídos, modificados o ejecutados (correr una aplicación). Cuando un usuario crea un archivo, automáticamente el archivo tiene permisos de lectura y escritura para su propietario
Los permisos para una carpeta o archivo se pueden otorgar indistintamente a tres grupos: el propietario, el grupo y los demás que no pertenecen al grupo. El propietario es el usuario que creó el archivo. Tengamos en cuenta que el grupo podrá tener o no algunos permisos sobre los archivos creados por otros usuarios. También, podemos dar permisos al resto de los usuarios que no formaban parte del grupo anterior.

Los permisos se dividen en tres partes: lectura, escritura y ejecución, que serán identificadas por sus siglas en inglés **r** de **read**, **w** de **write** y **x** de **execute**. Como vimos, estos permisos pueden otorgarse a tres grupos, por lo tanto, un archivo puede tener permisos totales para un grupo, y de solo lectura para el resto de los usuarios.
Para ver los permisos que tiene un archivo, ejecutamos el comando **ls –l nombredearchivo**. Se nos mostrará en columnas, y la primera dirá algo similar a **drwxr-xr-x**. Los permisos se dan en orden y por grupo, tendremos las letras **rwx**: la primera **r** indica el permiso de lectura para el propietario, la segunda **r** indica el mismo permiso pero para el grupo, y la tercera **r** indica el permiso para el resto de los usuarios. Con el guion (-), se simboliza un permiso vacío; en el ejemplo anterior, únicamente el propietario tiene permiso de modificación (**w**).
Para cambiar los permisos de un archivo, hacemos clic sobre sus **Propiedades** y, en la pestaña de permisos, los podemos modificar. Para modificarlos desde la terminal, utilizaremos el comando **chmod**, con símbolos de **+** y **–** para agregar o quitar permisos respectivamente.

SI INICIAMOS SESIÓN COMO ROOT, DEBEMOS TENER MUCHO CUIDADO SOBRE QUÉ PERMISOS O COMANDOS ESTAMOS EJECUTANDO.

Suponiendo que tenemos el archivo **horarios.txt**, del cual somos propietarios y no queremos que nadie lo pueda modificar, al escribir desde la terminal el comando **chmod +r-w horarios.txt** habremos establecido para todos los usuarios los permisos de lectura y denegamos el de modificación. Para modificar los permisos según su categoría, utilizaremos letras que identifican al propietario (**u**), grupo (**g**) y al resto de los usuarios (**o**). Tomando el ejemplo anterior, daremos control total a nuestro archivo propio: **chmod u+r+w+x horarios.txt**, solo el de lectura para el grupo **chmod g+r-w-x horarios.txt**, y denegamos todos los permisos para el resto del grupo **chmod o-r-w-x horarios.txt**.■



Desde la terminal, cuando ejecutamos el comando ls –l, veremos que se listarán todos los archivos, detallando sus respectivos permisos

Auditoría

Descubriremos y aplicaremos seguridad sobre los sistemas informáticos por medio de políticas de auditoría en un sistema Windows Server.

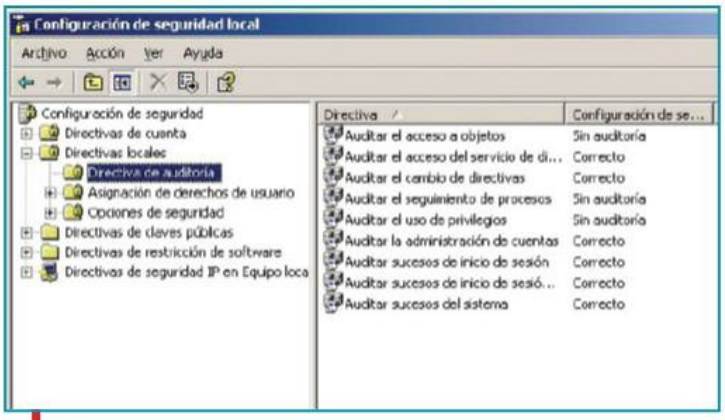
La auditoría corresponde a la acción conjunta del análisis y la apreciación de los procesos de comunicación, veracidad/fiabilidad de la información y designación de pautas de cumplimiento sobre el buen tratamiento de la información, en lo que a informática respecta. Además, es una parte fundamental de administración de seguridad, ya que gracias a ella podemos:

- Mejorar los procesos de autenticación en los sistemas.
- Detectar riesgos y evidencias de vulnerabilidad debido a uso incorrecto (intencional o no) de los sistemas.

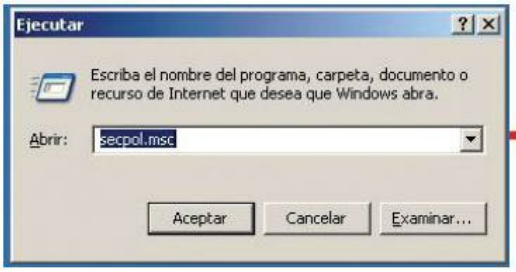
La auditoría nos permite reducir la posibilidad de pérdida de datos dentro de la organización y reconocer los hechos de defraudación realizado por personas no autorizadas.

Políticas locales

Para auditar los equipos o los servidores, deberemos abrir las políticas locales de nuestro sistema. Accederemos a ellas por medio de Inicio/Ejecutar, ingresamos secpol.msc y aceptamos. Otra forma es desde Inicio/Todos los programas/Herramientas administrativas; finalizamos abriendo el icono correspondiente a Políticas de Seguridad Local o Local Security Policy.



Dentro de las configuraciones de seguridad, elegimos Políticas locales y, luego, Directiva de auditoría, para configurar las distintas políticas.



Para habilitar los tipos de auditoría dentro de un sistema Windows, tendremos que acceder a la consola de políticas de seguridad local.

Una vez abierta la ventana de directivas de seguridad local, estamos en condiciones de aplicar una auditoría a nuestro servidor o al equipo. Navegaremos por el panel de la izquierda, ampliaremos la rama Políticas Locales y, por último, la subcategoría Directiva de auditoría. En el panel de la derecha, obtendremos una lista con una serie de políticas listas para habilitar o deshabilitar.
A partir de este momento, tendremos que identificar los tipos de políticas que se ajustan mejor a los requerimientos de la organización o los nuestros (si es una PC hogareña).
Es preciso aclarar que la auditoría se aplica a:

- Usuarios: estas políticas se refieren a los inicios de sesión y cierres (logout), modificación de permisos, creación o eliminación de cuentas de usuarios.
- Objetos: hacen referencia a los recursos compartidos de una red, carpetas, archivos, entradas de registro.
- Sistema: vinculado con los sucesos que inciden sobre el sistema reinicio, apagado o evento inesperado que afecte la seguridad del sistema.

Además, las políticas tienen cuatro estados de los intentos o hechos: Correctos, Incorrectos, Ambos o Ninguno. En cualquiera de los tres primeros resultados mencionados, la política se encuentra activa, y, cuando ningún resultado es auditado, la política se encuentra sin efecto Sin auditoría.

Configuración

La configuración de auditoría es muy importante en entornos empresariales, por eso estas configuraciones de políticas se

pueden aplicar tanto a nivel local como a nivel global.

Si queremos aplicar algún tipo de auditoría a nivel global, tendremos que contar con un controlador de dominio en el cual podamos aplicar la configuración necesaria para poder desplegarla a nivel global por todas las PC que conforman la organización.

Básicamente, lo que necesitamos para poder implementar una auditoría a nivel de dominio es estar conectados al controlador de dominio, en forma local o remota, abrir el **GroupPolicy Management**, ubicarnos sobre el nombre de nuestro dominio, hacer clic derecho y, de las lista de opciones, elegir la que dice **Crear una GPO en este dominio...**. En la nueva ventana que aparece, introduciremos un nombre a nuestra política, y aceptamos.

La nueva política aparece debajo del nombre de nuestro dominio. Tenemos que tener en cuenta que, en forma predeterminada, existe una política por defecto del dominio; esta se genera al momento de crear dicho dominio.

LA VERIFICACIÓN Y EL ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD ES PARTE DE NUESTRO EXTENSO TRABAJO DE AUDITAR.

Para modificar nuestra política recién creada, nos posicionamos sobre ella y hacemos clic derecho, seleccionamos la opción **Editar**. Se abrirá una ventana (**GroupPolicy Management Editor**) en la cual tendremos que dirigirnos al panel de la izquierda y desplegaremos el árbol de la siguiente forma: **Políticas/Configuración de Windows/Configuración de seguridad/Políticas locales/Directiva de auditoría**. Notaremos que tendremos la misma vista de consola (**Políticas de Seguridad Local**) que teníamos cuando configuramos la auditoría para implementarla en forma local (solo a una PC). Pero recordemos, en esta ocasión, que lo modificado aquí quedará guardado en la política de forma definitiva o hasta que necesitemos modificarla.

Gracias al EventViewer, vamos a poder verificar los resultados de la auditoría en nuestros equipos y servidores.

Una vez configurados los elementos por auditar, cerramos la ventana, y esta política ya puede ser implementada por todo el dominio o destinada para la unidad organizativa (**Grupo de trabajo**) que se nos indique por requerimiento.

Último paso

Como último paso, lo que nos resta es verificar que la auditoría esté procesando en forma correcta las políticas y almacenando los resultados. Esto nos permite verificar cómo se encuentra nuestro sistema y si hemos tenido algunos intentos de incorrecta manipulación de archivos, o intentos de ingresar incorrectos y correctos, según lo que hayamos establecido en las políticas de auditoría.

Si queremos inspeccionar esta información, deberemos hacerlo por medio del **Visor de Sucesos** (**EventViewer**). Es importante aclarar que la forma de ver los resultados es válida para las políticas aplicadas a nivel local (solo una PC) o a nivel global (**GroupPolicy Management**).

Nos dirigimos a **Inicio**, luego **Ejecutar** y escribimos **EVENTVWR.MSC**; hacemos clic en **Aceptar** o presionamos **ENTER**.

La forma alternativa para que accedamos es ir a **Inicio/Todos los programas/Herramientas administrativas/EVENT VIEWER** o **Visor de sucesos**.

Se abrirá una ventana nueva, esta es la consola de eventos de Windows; nos posicionamos sobre el panel de la izquierda, desplegamos la opción **Windows Logs** y, de las categorías que están contenidas dentro de él, seleccionamos, por ejemplo, **Security**; veremos en el panel de la derecha los intentos de inicio de sesión. Esta información se puede filtrar para una rápida y mejor observación de los eventos, porque es demasiado extensa. ■

Controlador de dominio

Si lo que deseamos es una implementación a nivel global, es decir, que todas las PC de la red, o gran parte de ellas, tengan aplicadas políticas de auditoría, tendremos que configurar un servidor como controlador de dominio. Sus funciones serán centralizar las cuentas de los usuarios y agrupar usuarios en unidades organizativas (grupos de trabajo); otras configuraciones pueden ser: establecer un fondo de escritorio igual para todos, una configuración específica para **Internet Explorer**, o denegar el acceso a ciertas funciones y aplicaciones de la PC (estaciones de trabajo).

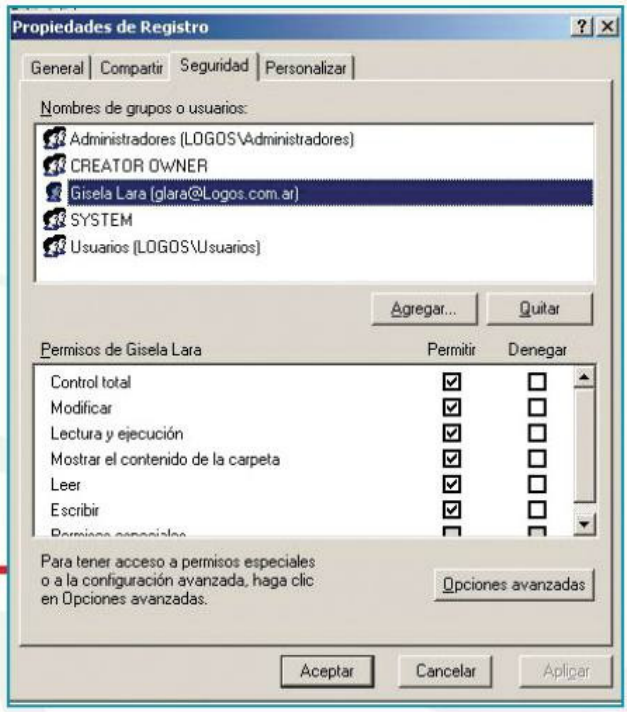
Usar la regla del mínimo privilegio

En estas páginas, veremos cómo podemos asignar los permisos adecuados para proteger la información de nuestra red y la integridad de los sistemas.

La **regla del mínimo privilegio** se refiere al concepto de que cada usuario, cuando inicia sesión en una PC, tiene que poseer un mínimo conjunto de privilegios para acceder al sistema. Estos privilegios o permisos nos brindan un acceso restrictivo. Es decir, el usuario solo se limita a realizar la tarea que le fue asignada y, en caso de daños, mal uso del sistema o por un software malintencionado, no afecte la integridad del equipo.

Este estándar de configuración se encuentra conceptualizado en un documento de sistemas informáticos y fue creado por el departamento de defensa de los Estados Unidos. Se aplica en función de asegurar los equipos por medio de un restricto uso de las cuentas administrativas sobre las PCs. Estas características de protección podemos implementarlas tanto en entornos hogareños como empresariales con servidores productivos; este último es el de mayor relevancia.

Las cuentas administrativas solo tenemos que usarlas con el único fin de realizar tareas que requieran permisos elevados sobre el sistema. Cuando iniciamos sesión con una cuenta que tenga privilegios administrativos, todos los programas o servicios que se ejecuten con ella también tendrán permisos administrativos, motivo por el cual el sistema queda expuesto a la ejecución de software que contenga código malintencionado (virus, troyanos, spyware, entre otros).



Cuando compartimos un recurso, podemos aplicar distintos permisos que permiten o deniegan acciones.

Seguridad

A nivel de seguridad, es muy efectivo ya que, desde una perspectiva defensiva, nuestros sistemas se encuentran menos vulnerables. Pero, en la práctica, el panorama que se nos presenta es muy distinto, debido a que existen aplicaciones que nos exigen tener ciertos privilegios o permisos en el sistema operativo. Esto es así, porque necesitan, por ejemplo, tener acceso a la raíz del disco duro y grabar ahí un pequeño archivo para su control de procesos internos, y, si el usuario que ejecuta esta aplicación no tiene los permisos necesarios, la aplicación y el sistema entran en conflicto ya que la aplicación se vuelve inestable.

Permisos

Dentro de los sistemas operativos Windows, esto se aplica gracias a los distintos grupos de usuarios que se pueden administrar en el sistema. Existe un orden de jerarquías con distintos permisos.

Administradores locales: para tener control total sobre el equipo.

Usuarios avanzados: este grupo tiene permisos administrativos limitados para acceder al sistema y compartir archivos por la red.

Usuarios: estos no pueden instalar software en el sistema, y todo lo que quieran modificar solo es posible que lo hagan en su carpeta de usuario.

Invitados: tienen más restricciones que el grupo usuarios.

Existen otros grupos que varían según el sistema operativo instalado, pero cada grupo de usuario, dependiendo de su función, tiene más o menos restricciones. Como mencionamos, esto se puede aplicar en nuestra PC hogareña, pero resulta

primordial en los entornos corporativos. Por eso, si queremos implementar estos permisos en nuestra red empresarial, necesitamos un servidor, por ejemplo Windows Server, y tener configurado el rol de Active Directory Domain Services.

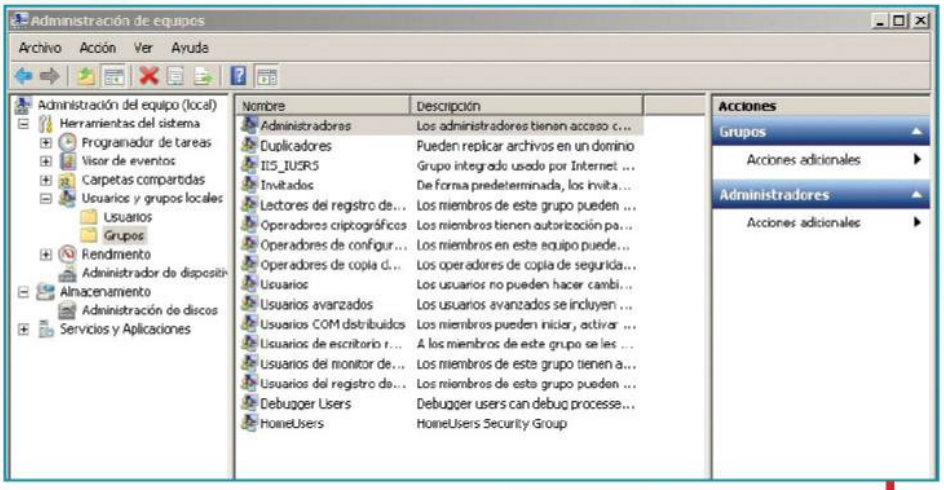
Una vez configurado, podremos empezar a crear nuestros usuarios y unidades organizativas (UO). Las unidades organizativas son contenedores de objetos en los cuales vamos a alojar usuarios, grupos y equipos. Por lo general, las UO se suelen crear con el nombre del departamento que corresponda dentro de la organización o según su rango de jerarquía; por ejemplo, podemos crear una UO llamada Finanzas y, dentro de ella, otras UO llamadas: Jefes, Supervisores y Agentes.

Este nos permite crear, a su vez, grupos de trabajo para que los vinculemos con cada uno de los usuarios que correspondan.

Una vez creadas las UO con los usuarios y los grupos, podemos compartir recursos en la red, como por ejemplo, impresoras y carpetas. Procederemos a compartir las impresoras y carpetas que nosotros deseemos, teniendo en cuenta que podemos aplicar permisos para permitir o negar su uso a determinados usuarios y grupos.

Los usuarios pueden tener acceso a una carpeta de red, pero podemos restringir la creación, borrado y modificación de archivos existentes o nuevos; incluso, es posible denegarles que vean alguna carpeta específica.

Estos permisos se aplican a los usuarios que inician sesión en alguna PC con sus credenciales de red. Una vez corroborados los datos suministrados por el usuario (usuario de red y password), Active Directory verifica a qué OU pertenece, dentro de qué grupo se encuentra si pertenece a alguno y qué permisos tiene el usuario para aplicarlos en la PC. Cargados los permisos, el usuario ve el escritorio de Windows y ya puede utilizar la PC con total normalidad, solo con los privilegios configurados con anterioridad.



> Los distintos grupos que existen en cada sistema pueden variar, e incluso existen programas que crean sus propios grupos.

Consideraciones finales

A nivel empresarial, siempre tendremos requerimientos en los que nos pedirán el acceso de un usuario o grupo de usuarios a cierto recurso, pero que se lo neguemos a otros. Estos niveles de seguridad son los que tenemos que aplicar en nuestros servidores de archivos para mantener la seguridad de la información y su integridad. Esto se debe a que, en los recursos compartidos, vamos a tener información sensible de los distintos departamentos de la organización, la cual tiene que estar protegida de usuarios no autorizados, impidiendo su mala manipulación.

Puede suceder que alguna persona dentro de la compañía escale a una jerarquía mayor y tenga que acceder, a partir de ese momento, a los archivos del nuevo puesto alcanzado; nosotros tendremos que otorgarle los nuevos permisos. Lo que realizaremos es verificar en que UO se encuentra el usuario en cuestión, quitar los permisos del grupo que deja y agregar los nuevos permisos de grupo del cual pasa a formar parte. ■

Toma de posesión

Aquí aprenderemos a tomar el control sobre una carpeta o archivo generado por otro usuario, saltando las restricciones de seguridad implantadas en forma original.

Si somos los propietarios de un archivo o de una carpeta, siempre podremos cambiar los permisos que los protegen. Para obtener acceso a un archivo o a una carpeta sobre los que no tenemos derechos, debemos tomar posesión de ellos y reemplazar los permisos de seguridad creados originalmente. Como es de imaginar, esta tarea solo la puede hacer un Administrador, y por esto, debemos verificar si nuestro usuario tiene privilegios de administrador. Si no lo somos, no vamos a poder tomar posesión total del archivo.

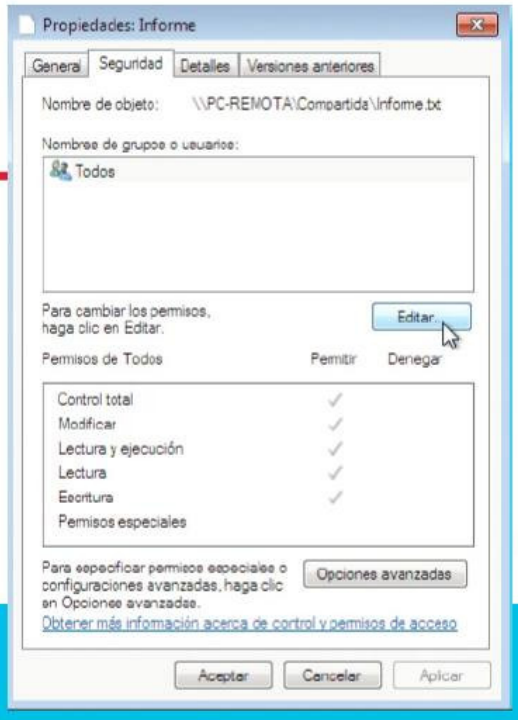
Ejemplo

Como ejemplo, imaginemos a un usuario que comparte un informe con todos los usuarios de la red. Nosotros, al hacer toma de posesión, podremos administrar con quiénes se compartirá el archivo, y sus privilegios (**Control total**, **Modificar** o solo **Leer**). Primero accedemos desde nuestra PC al archivo en la carpeta compartida del usuario. Allí, vamos a **Propiedades del archivo** (botón derecho del mouse) y, en la solapa **Seguridad**, veremos que se comparte con el usuario **Todos**, y sus privilegios.
Con el botón **Editar**, accederemos a los permisos del archivo y, desde la solapa **Usuarios**, por supuesto agregaremos a nuestro propio usuario (grupo **Administradores**). Luego, podremos quitar al usuario compartido **Todos**, agregaremos los usuarios que creamos convenientes (no olvidemos al usuario original), y los privilegios relacionados, como por ejemplo, modificar el informe, pero no eliminarlo.

Limitaciones

Debemos tener en cuenta que existen algunas limitaciones, como el sistema de cifrado de archivos (EFS), que es la protección de mayor nivel que proporciona Windows. Este sistema permite almacenar información en un formato cifrado que solo se puede acceder si conocemos la contraseña. No podremos tener acceso a un archivo cifrado sin la clave, incluso si disponemos de los permisos necesarios para la toma de posesión.
Take Ownership Shell Extension es una extensión gratuita que nos facilita mucho la tarea. Desde el menú contextual y con solo un clic, ya tenemos el archivo a nuestra disposición.■

Desde la solapa **Seguridad**, podremos ver los privilegios del archivo y modificarlos luego de la toma de posesión.



Conexión al directorio raíz

Desde el explorador, la opción **\\PC-REMOTA\C$** nos permitirá como administradores conectarnos al directorio raíz de una unidad y buscar un archivo que no se encuentre compartido. Aun teniendo los privilegios de administrador, a veces debemos preparar previamente la PC modificando el registro. Sobre la cadena **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**, creamos un valor **DWORD** igual a **1**, y, luego de restablecer la PC, deberíamos de poder acceder al directorio raíz de la PC remota.

PRÓXIMA ENTREGA

12 SEGURIDAD FÍSICA DE LA RED

En el próximo fascículo analizaremos la importancia de la seguridad en una red, conoceremos aplicaciones útiles y recomendaremos prácticas seguras para los usuarios.

Técnico en REDES &SEGURIDAD

▶ PROFESORES EN LÍNEA
profesor@redusers.com
▶ SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00011
9 789871 857784

CONTENIDO DE LA OBRA