U.D.2. Gestión manual y automatizada de usuarios
Objetivos
• Gestionar los usuarios e grupos de un sistema operativo. • Conocer os diferentes perfiles de usuario. • Establecer procesos automatizados de gestión de cuentas e grupos de usuario.
Contenidos conceptuales
• Cuentas de grupo e usuario. • Tipos de perfiles de usuario: perfiles móviles. • Gestión de grupos: tipos e ámbitos. • Usuarios e grupos predeterminados. • Cuentas de usuarios: patrones. • Cuentas do sistema.

1 Cuentas de grupo e usuario en Windows Profesional y Server.

Podemos considerar al **usuario** como el objeto que puede utilizar, gestionar o administrar al sistema operativo.

Un **grupo de usuarios** es una política utilizada generalmente por un sistema operativo para referirse a más de un usuario en su configuración y privilegios.

Plantearemos el estudio de la gestión de los usuarios y grupos en Windows y Linux sin tener en cuenta la instalación del Directorio Activo. En la última unidad del curso en cambio, si llevaremos a cabo la gestión de usuarios y grupos bajo un Dominio. U

1.1 Usuarios y grupos en Windows XP/Vista/7

Antes de nada comentar que hay versiones de Windows (por ejemplo Windows Vista Starter, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7 Starter) que no soportan la gestión de usuarios. Haremos referencia a versiones tipo Profesional.

Una **cuenta de usuario define** las **tareas** que se pueden realizar en un equipo informático en función de los **privilegios** que posee el mismo.

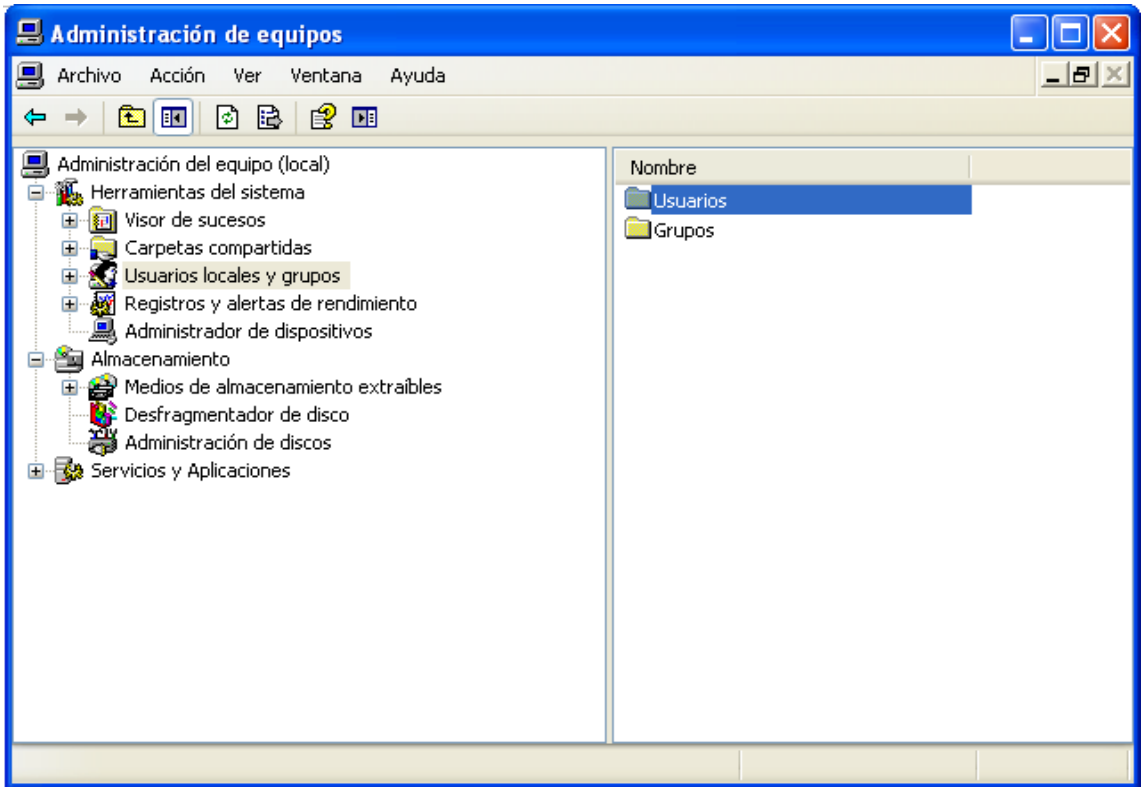
Cada cuenta de usuario de Windows XP consta de:

- Nombre de usuario que debe ser **único**
- Grupo de Trabajo. *Mi PC → Botón derecho Propiedades → Nombre equipo y grupo*
- Contraseña. *Panel de control → Cuentas de usuario*

Una cuenta de usuario permite:

- Personalizar tu escritorio
- Personalizar el navegador (Favoritos..)
- Permitir/denegar acceso a información propia en la carpeta **Mis documentos** y **poner contraseñas** para archivos privados

Si ejecutamos **compmgmt.msc** nos aparece la siguiente ventana donde podremos configurar los usuarios de un sistema Windows XP.



Los tipos de cuenta, también llamados **perfiles,** de usuarios de XP son los siguientes:

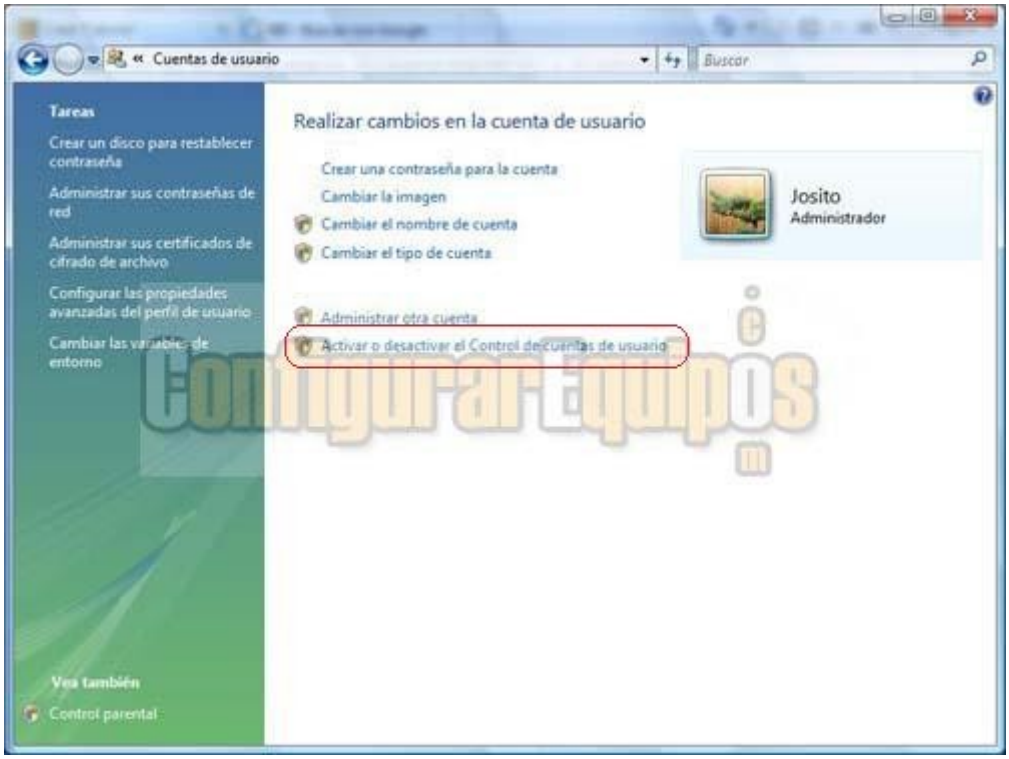
- **Administradores**. Tienen acceso completo y sin restricciones al equipo.
- **Usuarios avanzados**. Tienen derechos administrativos más limitados, por ejemplo, para compartir archivos, instalar impresoras locales y cambiar la hora del sistema. Los usuarios avanzados también tienen amplios permisos para tener acceso a archivos en las carpetas de sistema de Windows.
- **Usuarios**. Tienen derechos de usuario limitados y se les impide realizar cambios intencionales o accidentales que puedan afectar a todo el sistema. Las cuentas de usuario que son miembros *sólo* de este grupo se denominan *cuentas de usuario limitadas*.
- **Invitados**. Tienen menos derechos que los usuarios limitados. Prácticamente solo pueden acceder al equipo y hacer consultas, navegar por Internet...

Los derechos se otorgan a las cuentas de usuario a través de la pertenencia a uno o más de estos grupos. Por ejemplo, la cuenta de Administrador integrada tiene derechos administrativos porque es miembro del grupo Administradores. Pertenecer a este grupo otorga a la cuenta de Administrador derechos elevados, como el derecho a apagar un

sistema desde un equipo remoto.

Es importante recordar que se recomienda utilizar el equipo con una cuenta de usuario avanzada y **no** como administrador, dejando esta para cuestiones puramente administrativas del sistema.

Uno de los cambios cualitativos que supuso el salto de XP a Vista/7 fue el discutido sistema de **Control de Cuentas de Usuario (UAC).** Discutido porque después de años criticando la falta de seguridad de Windows cuando se implementa el UAC, el usuario medio criticó duramente las molestias que ocasionaban los continuos mensajes de advertencia cada vez que se ejecutaba una aplicación desconocida para el sistema que accedía a ficheros “sensibles” como el registro. De todas formas dicho UAC se puede desactivar y simplemente con tener un antivirus, firewall y Windows Defender se puede obtener un sistema de seguridad medianamente aceptable.



En Windows Vista hay dos tipos de usuarios: **usuarios estándar** y **administradores**.

Pues bien, cada tipo de usuario tiene una serie de privilegios y de niveles de uso y acceso, pero a nivel de acceso a recursos y ejecución de aplicaciones, en el contexto de seguridad TODOS son considerados como **usuarios estándar**.

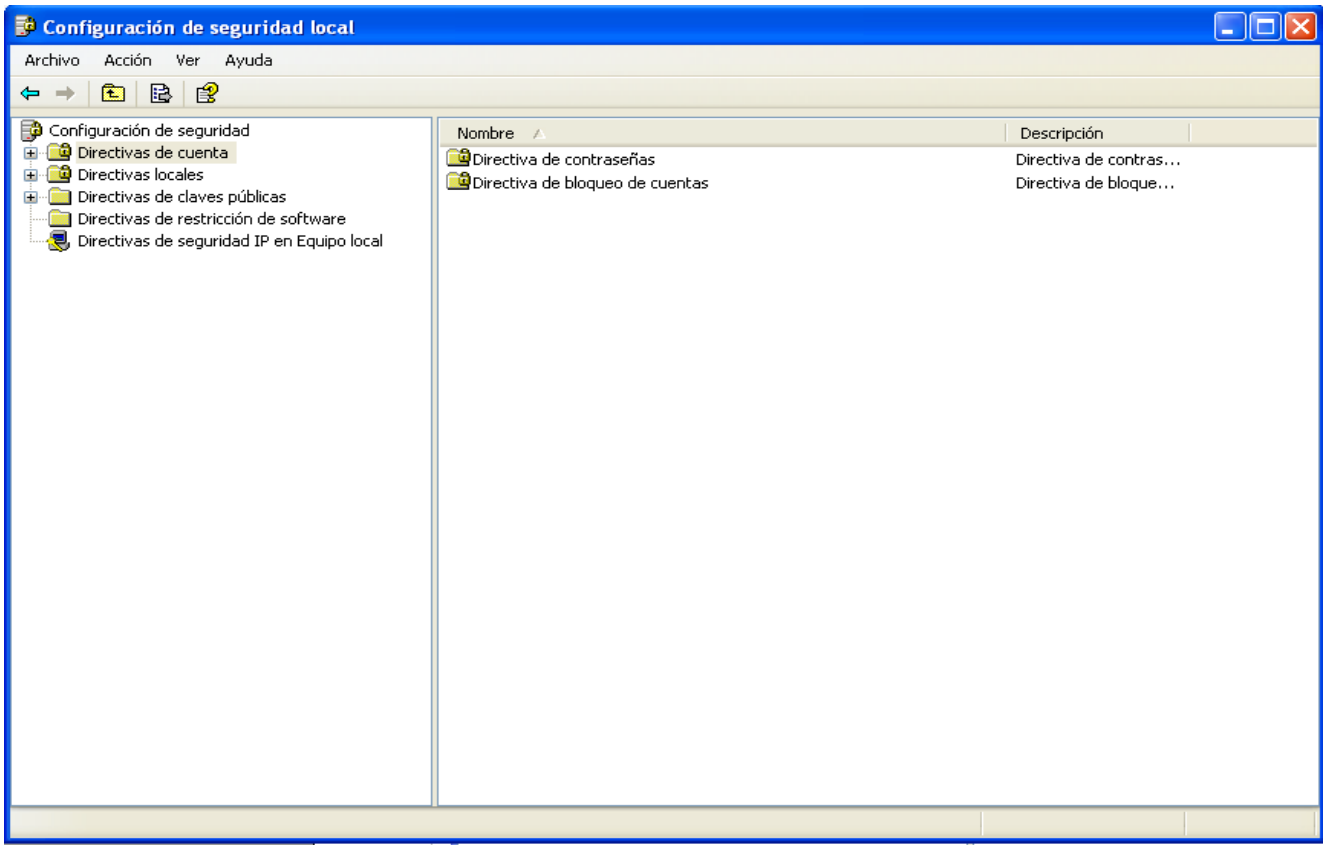
Cuando un usuario inicia una sesión, el sistema crea un control de acceso para dicho usuario. Este control de acceso contiene información acerca del nivel de acceso que tiene el usuario en cuestión, incluyendo **identificadores de seguridad específicos (SID)** y **privilegios de Windows.** Cuando un administrador inicia una sesión, Windows crea dos controles de acceso independientes para el usuario, un control de acceso de usuario estándar y un control de acceso de administrador. El control de acceso de usuario estándar tiene la misma información específica de usuario que el control de acceso de

administrador pero se han quitado los privilegios administrativos y los SID. El control de acceso de usuario estándar se utiliza para iniciar aplicaciones que no realizan tareas administrativas.

Cuando el administrador tiene que ejecutar aplicaciones que realizan tareas administrativas, Windows pide que cambie su nivel de seguridad de usuario estándar a administrador. Este sistema se denomina ***Modo de aprobación de administrador***. En este modo, las aplicaciones cuya ejecución implique cualquier tipo de modificación en el sistema (por mínima que esta sea, incluso cuando se trate solo de consultas) o bien se trate de una aplicación que no tenga los permisos de administrador, siempre van a pedir confirmación para ejecutarse, o lo que es lo mismo, que **pasemos de un nivel de seguridad al superior.**

Cuando se está iniciando una aplicación que requiere nivel de seguridad de administrador, aparece una ventana de Control de cuentas de usuario de manera predeterminada. Si el usuario es un administrador, en la ventana se le da la opción de permitir que se inicie la aplicación o de evitar que se inicie. Si el usuario es un usuario estándar, en esta ventana se puede especificar el nombre de usuario y la contraseña de una cuenta que sea del grupo de Administradores local.

Si ejecutamos **secpol.msc** nos aparece la imagen siguiente que se corresponde con las directivas de seguridad local.



En primer lugar nos aparece las directivas de cuenta. Las directivas de cuentas se definen en los equipos, aunque afectan a la forma en que las cuentas de usuario pueden

interactuar con el equipo o el dominio. Las directivas de cuentas contienen tres subconjuntos:

- **Directivas de cuenta:** Se utiliza para las cuentas de usuario del dominio o las locales. Determina la configuración de las contraseñas, como la obligatoriedad y su ciclo de vida.
- **Directiva de bloqueo de cuentas:** Se utiliza en las cuentas de usuario del dominio o las locales. Determina las circunstancias y el período que una cuenta va a estar bloqueada en el sistema.
- **Directiva Kerberos**: Se utiliza cuentas de usuario de dominio. Determina la configuración relacionada con Kerberos, como la obligatoriedad y el ciclo de vida de los vales. **Las directivas Kerberos no existen en la directiva de equipo local.**

Practica 1. Crea cuatro usuarios **Adan, Eva, Ping, Pong.** Todos como usuarios limitados. Para ello deberás entrar en **Administración de Equipos.** Puedes hacerlo de tres formas distintas:

1. Inicio/Panel de control/Rendimiento y mantenimiento/Herramientas administrativas/ Administración de equipos
2. Inicio/Ejecutar/**compmgmt.msc**
3. Botón derecho sobre Mi PC/Administrar.

A continuación aplicar las directivas de cuenta y operaciones siguientes:

- longitud máxima de la contraseña 5
- combinación de números y letras
- ciclo de vida de 30 días.
- eliminar la cuenta creada en la instalación
- ver la cuenta oculta de administrador (a veces tras la instalación está oculta)

Existes una seria de comandos que nos permiten realizar operaciones con usuarios en Windows XP (Vista/7 son similares con lo que solo nos centraremos en XP). Inicia la consola y ejecútalas:

- **gpresult:** Muestra información sobre las políticas de grupo aplicadas a un usuario.
- **control userpasswords:** Permite modificar las claves y los permisos de los diferentes usuarios, así como requerir la pulsación de control+alt+suprimir para poder iniciar sesión, haciendo el inicio de sesión más seguro.
- **net accounts**: Muestra/modifica la cuenta del usuario.
  Parámetros:
  /minpwlen X -> longitud mínima de password (en caracteres)
  /uniquepw:X ->No se puede utilizar la misma password durante X cambios de clave
  /Domain: X -> realiza los cambios en el dominio.
  /Sync -> Actualizar también los BDC (solo con /domain)
- **net send** x y: Enviar el mensaje Y a X (usuario u ordenador)
  Si nombre es *: Envía a todos los miembros del grupo/dominio
- **net user**, puede utilizar los siguientes parámetros (solo los principales):
  nombreDeUsuario: Es el nombre de la cuenta de usuario que desea agregar, eliminar, modificar o ver. El nombre de la cuenta de usuario puede tener hasta 20 caracteres.

* :Genera un mensaje que pide la contraseña. La contraseña no se muestra al escribirla en la solicitud de contraseña.
contraseña: Asigna o cambia una contraseña para la cuenta del usuario. Una contraseña debe satisfacer la longitud mínima establecida con la opción **/minpwlen** del comando **net accounts**. Puede contener hasta 14 caracteres.
/add: Agrega una cuenta de usuario a la base de datos de cuentas de usuario.
/delete: Quita una cuenta de usuario de la base de datos de cuentas de usuario.

/active:{yes | no}: Activa o desactiva la cuenta. Si la cuenta no está activa, el usuario no puede obtener acceso al servidor. El valor predeterminado es yes (sí).
/comment:"texto": Establece un comentario de la cuenta de usuario (48 caracteres, como máximo). Asegúrese de colocar las comillas alrededor del texto que utilice.
/expires:{date | never}: Hace que la cuenta caduque si se establece una fecha. La opción **never** establece que la cuenta no tiene límite. La fecha de caducidad está en el formato mm/dd/aa o dd/mm/aa, según el código de país.
/fullname:"*nombre*": Es el nombre completo de un usuario entre “” (en lugar de un nombre de usuario).
/homedir:*nombreDeRuta:* Establece la ruta de acceso del directorio principal del usuario.
/passwordchg:{yes | no}: Especifica si los usuarios pueden cambiar su propia contraseña. El valor predeterminado es yes (sí).
/passwordreq:{yes | no} Especifica si una cuenta de usuario debe tener una contraseña. El valor predeterminado es yes (sí).
/profilepath[:rutaDeAcceso] Establece una ruta de acceso para el perfil de inicio de sesión del usuario.
/scriptpath:*nombreDeRuta* Es la ubicación del script de inicio de sesión del usuario.
/times:{times | all} Son las horas de inicio de sesión. La opción **times** se expresa como día[-día][,día[-día]],hora[-hora][,hora[-hora]], y se limita a incrementos de una hora. Los días se pueden deletrear o abreviarse. Las horas pueden estar en notación de 12 o de 24 horas. En la notación de 12 horas, use am, pm, a.m. o p.m. La opción **all** especifica que un usuario siempre puede iniciar sesión, y un valor en blanco especifica que un usuario nunca puede iniciar sesión. Separe las entradas de día y hora con una coma, y separe varias entradas de día y hora con un punto y coma.
/usercomment:"texto" Permite que un administrador agregue o cambie el comentario para el usuario de la cuenta.
net help user | more Muestra la Ayuda pantalla por pantalla.

- **net localgroup:** Este comando agrega, muestra o modifica grupos locales.

En XP/Vista/7 además de los **grupos de usuarios** vistos podemos crear nuestros propios grupos. Una forma sería modificar los existentes, por ejemplo, en **usuarios limitados** podemos ir a las **directivas locales y modificar alguna** de sus características. Otra forma sería **crear un grupo nuevo** (una vez insisto Windows Home Basic, Windos Starter y Home Premium en las diferentes versiones del sistema no puede realizar la creación ni de grupos ni de usuarios). Para ello seguimos los siguientes pasos:

Práctica resuelta.

- Abrir Microsoft Management Console, ya visto en apartados anteriores
- En el panel izquierdo, haga clic en Usuarios y grupos locales. Si no ve Usuarios y grupos locales, probablemente se deba a que no se ha agregado ese complemento a Microsoft Management Console. Para instalarlo, siga estos pasos:
- En Microsoft Management Console, haga clic en el menú Archivo y luego haga clic en Agregar o quitar complemento.
- Haga clic en Usuarios y grupos locales y, después, haga clic en Agregar.
- Haga clic en Equipo local y, después, en Finalizar.
- Haga clic en Aceptar.
- Haga doble clic en la carpeta Grupos.
- Haga clic en Acción y, a continuación, haga clic en Grupo nuevo.
- Escriba un nombre de grupo y una descripción, por ejemplo, **Genesis**
- Haga clic en Agregar y escriba el nombre de la cuenta de usuario, por ejemplo **Eva.**
- Haga clic en Comprobar nombres y, a continuación, haga clic en Aceptar.
- Haga clic en Crear

Practica 2. Busca ayuda en Internet para modificar la configuración del grupo **Genesis** para que cuando haga login **Eva** no pueda ejecutar el Messenger ni modificar el fondo de escritorio.

Perfiles de usuario locales en XP

Cuando damos de alta un usuario en un ordenador con XP el propio sistema genera una configuración personal y específica sobre todo del escritorio, panel de control y utilización de aplicaciones para cada usuario. La carpeta ***Documents and Settings (Usuarios en W7)*** contiene varias subcapetas entre ellas la del Administrador y la de los usuarios que hayas creado. Cada carpeta tien todas las opciones de inicio de sesión personalizado para cada usuario (Escritorio, fondo, panel de control, ..) de forma que si modifica algo no le afectará a otro usuario.

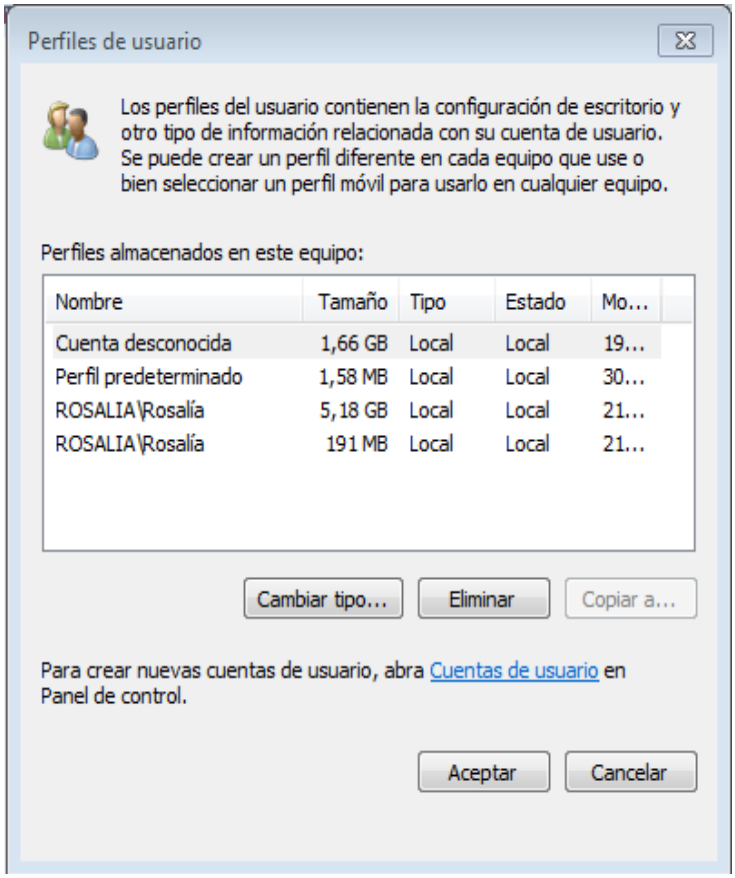
Un usuario no podrá eliminar las carpetas de otro usuario, solo el **administrador o un usuario con suficientes privilegios.**

Oculta, existe una carpeta llamada ***Default User*** que almacena el **perfil por defecto de cada usuario nuevo creado.** Si es eliminada generará problemas a nuevos usuarios creados.

Otra carpeta de interés es ***All Users*** que contiene la información de programas, escritorio y panel de control común para todos los usuarios del sistema, incluido el administrador.

Para ver los **perfiles de usuario** vamos *Inicio → panel de control → Sistema → Opciones Avanzadas → Perfiles de usuario* y saldrá una pantalla como la siguiente:

En W7 la ruta es igual pero en vez de *Opciones Avanzadas es Configuración Avanzada.*



Si hubiese un dominio aparecerían también las cuentas del mismo bajo el aspecto similar a este ***Midominio/Usuariodominio***

Si por el contrario el aspecto es ***NombreMaquinaLocal/Usuario*** nos referiremos a un usuario local.

Si seleccionamos con el botón secundario del ratón **Propiedades** del usuario o doble clic sobre su icono nos aparecerá la pantalla donde nos permitirá modificar algunas de la configuraciones:

- En la ficha **perfil** nos presenta tres opciones:
  - **ruta de acceso al perfil** donde están definidas las opciones de configuración del entorno de usuario.
  - **script de inicio o archivo de comandos de inicio de sesión** que define la ruta de un archivo que contiene secuencias de comandos a ejecutar cuando el usuario inicia la sesión.
  - **ruta de acceso local:** especifica el directorio que utiliza el usuario para almacenar sus archivos personales. Se puede **mapear** si se desea una ruta a una unidad de red.

Con respecto a la **eliminación de usuarios** comentar que se realiza como con otro cualquier otro objeto del sistema. Simplemente señalar que los perfiles de usuario que se

generaron en la **alta** en la carpeta *Document and Settins o Usuarios* si es W7 **no se borran.** Para ello deberemos ir a esa carpeta como **Administrador** y eliminarlos manualmente.

Practica 3. Establece un fichero .**bat** que cuando los usuarios **Adán y Eva** inicien su sesión se muestre en un fichero **aviso.html** (visionado con un navegador) el mensaje siguiente: "**NO COMED DE LA FRUTA PROHIBIDA".** Puedes consultar en Internet lo que desees.

Grupos locales

Cuando comentamos los tipos de grupos de usuarios que presenta XP y W7 nos refriemos a dos tipos: **administradores, usuarios y usuarios avanzados.** En realidad hay más pero relacionados con aspectos de los dominios.

- **Duplicadores:** pueden duplicar archivos en un dominio.
- **Operadores de red:** tienen algunos privilegios administrativos para administrar la configuración de las características de la red.
- **Operadores de copia:** pueden sobrescribir restricciones de seguridad en lo que respecta copias seguridad.
- **Usuarios escritorio remota:** se les concede el derecho de iniciar sesión remotamente.
- **HelpsServiceGroup:** grupo para ayuda y soporte técnico.

Solo el **administrador** puede dar alta de grupos locales. La forma es la misma que Acción → *Grupo nuevo.* De la misma forma se pueden dar de baja y modificar.

1.2 Usuarios y grupos en Windows Server

Estudiaremos los usuarios y grupos de Server sin considerar el Directorio Activo. En la unidad 5 retomaremos estos conceptos dentro del mismo.

A grandes rasgos podemos hablar de usuarios:

– **Usuarios globales:** se crean en equipos Windows Server que **sean controladores de dominio** y pueden usarse para conectarse a los dominios en que se crean y en otros en los que se confía.

– **Usuarios locales:** además de en los XP y 7 Profesionales se pueden crear usuarios locales en los Windows Server que **no sean controladores de dominio,** por tanto estas cuentas no pueden usarse para conectarse a ningún dominio, **solamente al equipo local.**

Una de las ventajas de los usuarios globales englobados en un dominio es que podemos realizar distintas operaciones al mismo tiempo con varias cuentas de usuario.

De la misma forma podemos hablar de:

– **Grupos locales:** al igual que antes solo se pueden englobar en versiones Profesional en versiones **Server que NO sean controladores de dominio.**

– **Grupos locales de ámbito de dominio:** solo pueden crearse en equipos con **Server y que sea controlador de dominio.**

– **Grupos de ámbito global:** son los que pertenecen a un **Server controlador de dominio.** Además puede tener miembros a grupos globales y cuentas solo del dominio en el que se definió.

– **Grupos de ámbito universal:** además de lo anterior pueden tener miembros de cualquier dominio de Windows Server.

Los **grupos predeterminados** en Windows Server 2003 son:

- **Administradores**

Los miembros de este grupo tienen control total del servidor y pueden asignar derechos de usuario y permisos de control de acceso a los usuarios según se necesite. La cuenta Administrador es miembro de este grupo de forma predeterminada. Cuando el servidor se une a un dominio, se agrega automáticamente al grupo el grupo Admins. de dominio.

- **Operadores de copia de seguridad**

Los miembros de este grupo pueden realizar copias de seguridad y restaurar archivos del servidor, independientemente de los permisos que protejan dichos archivos. Es así porque el derecho a realizar una copia de seguridad tiene preferencia sobre todos los permisos de archivo. No pueden cambiar la configuración de seguridad.

- **Administradores de DHCP (se instala con el servicio Servidor DHCP)**

Los miembros de este grupo tienen acceso como administradores al servicio Servidor de Protocolo DHCPt. El grupo proporciona una forma de conceder acceso administrativo limitado solamente al servidor DHCP, sin proporcionar acceso completo al equipo servidor pero no pueden realizar otras tareas administrativas en el servidor.

- **Usuarios de DHCP (se instala con el servicio Servidor DHCP)**

Los miembros de este grupo tienen acceso de sólo lectura al servicio Servidor DHCP. De este modo, los miembros pueden ver la información y las propiedades almacenadas en un servidor DHCP especificado. Esta información resulta útil para que el personal del departamento de soporte técnico realice informes de estado de DHCP.

- **Invitados**

Los miembros de este grupo disponen de un perfil temporal que se crea al iniciar la sesión y que se elimina cuando el miembro la cierra. La cuenta Invitado (deshabilitada de forma predeterminada) también es miembro del grupo de forma predeterminada.

- **HelpServicesGroup**

Este grupo permite que los administradores establezcan permisos comunes para todas las aplicaciones de soporte técnico. De forma predeterminada, el único miembro del grupo es la cuenta que **se asocia a las aplicaciones de soporte técnico de Microsoft,** como Asistencia remota. No se debe agregar usuarios a este grupo.

- **Operadores de configuración de red**

Los miembros de este grupo pueden modificar la configuración TCP/IP y renovar y liberar las direcciones TCP/IP.

- **Usuarios del monitor de sistema**

Los miembros de este grupo pueden supervisar los contadores de rendimiento del servidor, tanto de forma local como de forma remota.

- **Usuarios del registro de rendimiento**

Los miembros de este grupo pueden administrar los contadores de rendimiento, registros y alertas del servidor, tanto de forma local como de forma remota.

- **Usuarios avanzados**

Los miembros del grupo Usuarios avanzados pueden crear cuentas de usuario y modificar y eliminar las cuentas que crean.

- **Opers. de impresión**

Los miembros de este grupo pueden administrar las impresoras y las colas de impresión.

- **Usuarios de escritorio remoto**

Los miembros de este grupo pueden iniciar sesión en un servidor de forma remota. Permitir inicio de sesión a través de Servicios de Terminal Server.

- **Replicador**

El grupo Replicador admite funciones de replicación. El único miembro del grupo Replicador debe ser una cuenta de usuario de dominio que se utilice para iniciar los servicios Replicador de un controlador de dominio. No agregue a este grupo las cuentas de usuario de los usuarios reales.

- **Usuario de Terminal Server**

Este grupo contiene todos los usuarios que iniciaron sesión en el equipo que utiliza Servicios de Terminal Server actualmente. Cualquier programa que un usuario puede ejecutar en Windows NT 4.0 lo ejecutará un usuario miembro del grupo Usuario de Terminal Server.

- **Usuarios**

Los miembros del grupo Usuarios pueden realizar las tareas más habituales, como ejecutar aplicaciones, utilizar impresoras locales y de red, y bloquear la estación de trabajo. No pueden compartir directorios ni crear impresoras locales. Los grupos Usuarios de dominio, Usuarios autenticados e Interactivo son miembros de este grupo de forma predeterminada. Por tanto, todas las cuentas de usuario que se crean en el dominio son miembros de este grupo.

- **Usuarios de WINS (se instala con el servicio WINS)**

Los miembros de este grupo tienen acceso de sólo lectura al Servicio de nombres Internet de Windows (WINS). De este modo, los miembros pueden ver la información y las propiedades almacenadas en un servidor WINS especificado.

1.3. Perfiles de usuario

Los perfiles de usuario permiten especificar aspectos del escritorio, barra de tareas, contenido del menú inicio... incluyendo aplicaciones y programas.

Cada usuarios tiene asociado un perfil que se guarda en el equipo local, **pefil local.** Cuando hablamos de un servidor Windows **2003/2008** pueden tener perfiles que se mantiene **independientemente de la estación de trabajo o equipo cliente** en el cual se conecten. Estos perfiles se denominan **perfiles de red.**

Hay dos tipos de perfiles de red:

- **perfiles móviles:** son asignados por el administrador al usuario pero pueden ser modificados por éste y los cambios permanecen tras finalizar la conexión.
- **perfil obligatorio:** similar al anterior pero obliga al usuario a utilizar el perfil asignado por el administrador. Lo puede modificar pero los cambios finalizan al finalizar la sesión.

Todos los perfiles se guardan por defecto en **\Document and Settings (Usurios en W7)*nombre_de_usuario.*** Además de las carpetas del administrador y del usuario tenemos otras dos (o al menos una de las siguientes):

- **All Users:** incluye aspectos comunes de los perfiles de todos los usuarios del equipo.
- **Default user:** corresponde a todo usuario que se conecta por primera vez o no tenga un perfil específico.

  En cada uno de los perfiles puede haber las siguientes carpetas: **datos de programa, cookies, entorno de red, escritorio,, favoritos, menu inicio, mis documentos, impresoras, menú inicio, sendto, mis imágenes y plantillas.** Algunas de ellas están ocultas

Practica 4 .- En la carpeta de uno de los usuarios creados haz clic en ***herramientas*** → ***opciones de carpeta*** → ***mostrar archivos y carpetas ocultos.*** Se mostrarán la mayoría de las carpetas anteriores.

Los **perfiles móviles** modificados por el usuario se guardan en un archivo **ntuser.dat** que se encuentra en un subdirectorio en la carpeta **Document and Settings.** Existe un archivo **ntuser.dat.log** que guarda los cambios anteriores.

Los **perfiles obligatorios** se guardan en un archivo llamado **ntuser.man** dentro de un subdirectorio de la carpeta **Document and Settings.**

Tanto un perfil como el otro cuando el usuario se conecta se copian en la categoría del **Registro** HKEY_CURRENT_USER

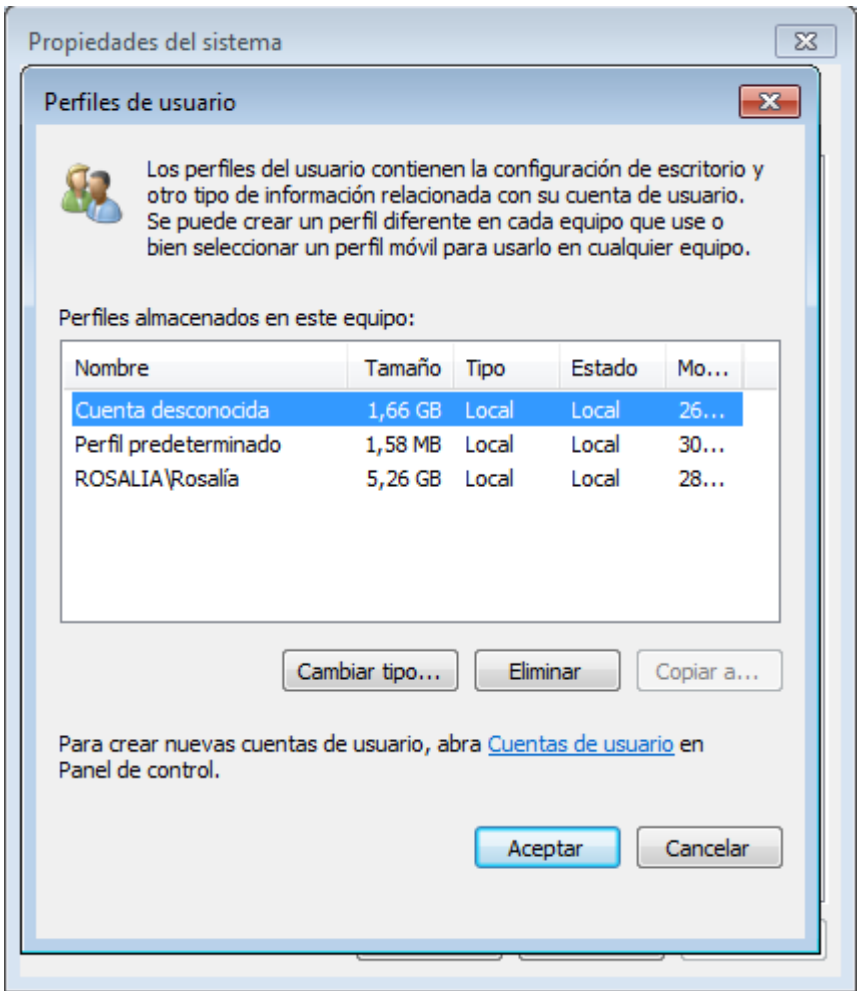
Práctica 5. Copiar un perfil de usuario **Eva (cambiar papel tapiz) en el de Adán.**

Para copiar un perfil de usuario existente a la cuenta de otro usuario, seguir estos pasos:

1. Haga clic en **Inicio**, haga clic con el botón secundario del *mouse*(ratón) en **Mi PC** y, después, haga clic en **Propiedades** en el menú contextual que aparece.
2. Haga clic en la ficha **Avanzadas** y, en **Perfiles de usuario**, haga clic en **Configuración**.
3. En la lista **Perfiles almacenados en este equipo** haga clic en el perfil que desea

copiar.

4. Haga clic en **Copiar a**.



5. En el cuadro de diálogo **Copiar a**, realice una de las siguientes acciones:
   - En el cuadro **Copiar perfil en**, escriba la ruta de acceso UNC (Convención de nomenclatura universal) a la carpeta del perfil del usuario de destino. Por ejemplo, escriba lo siguiente:
     \\nombreServidor\recursoCompartido\directorioPerfilDelUsuario
     O bien
   - O bien Haga clic en **Examinar** y, a continuación, vaya a la carpeta de perfiles de usuario en la que desea copiar el perfil. Haga clic en **Aceptar**.
6. En **Está permitido usar**, haga clic en **Cambiar**. Escriba el nombre del usuario al que se permitirá utilizar este perfil y, a continuación, haga clic en **Aceptar**. En el cuadro de diálogo **Copiar a**, haga clic en **Aceptar**. Si recibe el mensaje "Confirmar copia", haga clic en **Sí**.
7. Haga clic dos veces en **Aceptar**.

Estos conceptos se repasarán y desarrollarán, sobre todo con prácticas, cuando en la UD 5 estudiemos el Active Directory

2 Cuentas de grupo e usuario en GNU/LINU.

Linux es un **sistema multiusuario**, por lo tanto, la tarea de añadir, modificar, eliminar y en general administrar usuarios se convierte en algo no solo rutinario, sino importante, además de ser **un elemento de seguridad** que mal administrado o tomado a la ligera, puede convertirse en un enorme hoyo de seguridad.

2.1. Tipos de usuarios

Los usuarios en Unix/Linux se identifican por un número único de usuario, **User ID, UID**. Y pertenecen a un grupo principal de usuario, identificado también por un número único de grupo, **Group ID, GID**. El usuario puede pertenecer a más grupos además del principal.

Usuario root

- También llamado superusuario o administrador.
- Su UID (User ID) es 0 (cero).
- Es la única cuenta de usuario con privilegios sobre todo el sistema.
- Acceso total a todos los archivos y directorios con independencia de propietarios y permisos.
- Controla la administración de cuentas de usuarios.
- Ejecuta tareas de mantenimiento del sistema.
- Puede detener el sistema.
- Instala software en el sistema.
- Puede modificar o reconfigurar el kernel, controladores, etc.

Usuarios especiales

- Ejemplos: **bin, daemon, adm, lp, sync, shutdown, mail, operator, squid, apache, etc.** Se les llama también **cuentas del sistema.**
- No tiene todos los privilegios del usuario root, pero dependiendo de la cuenta asumen distintos privilegios de root.
- Lo anterior para proteger al sistema de posibles formas de vulnerar la seguridad.
- No tienen contraseñas pues son cuentas que no están diseñadas para iniciar sesiones con ellas.
- También se les conoce como cuentas de **"no inicio de sesión" (nologin)**.
- Se crean (generalmente) automáticamente al momento de la instalación de Linux o de la aplicación.
- Generalmente se les asigna un UID entre 1 y 100 (definifo en /etc/login.defs)

Usuarios normales

- Se usan para usuarios individuales.
- **Cada usuario dispone de un directorio de trabajo, ubicado generalmente en /home**.
- Cada usuario **puede personalizar** su entorno de trabajo.
- Tienen **solo privilegios completos** en su directorio de trabajo o HOME.
- Por seguridad, **es siempre mejor trabajar como un usuario normal** en vez del usuario root, y cuando se requiera hacer uso de comandos solo de root, utilizar el comando su o sud.
- En las distros actuales de Linux se les asigna generalmente un UID superior a 500.

La administracion de grupos en linux permite a **root** la posibilidad de integrar a un **conjunto de usuarios con ciertos provilegios y limitaciones dentro de un grupo,** donde podrán existir uno a mas usuarios.
El sistema operativo hace uso de tres importantes ficheros durante el proceso de alta de algún usuario en el sistema por parte del administrador (root), estos ficheros son:

- **/etc/passwd**
- **/etc/shadow**
- **/etc/group**
- **/etc/login.defs**

Son editados por el sistema tras haber creado los usuarios por el administrador(root).

/etc/passwd

En este fichero se encuentran almacenados los datos sobre los comandos y directorios de cada usuario dado de alta en el sistema. Tiene la siguiente estructura

pepito:x:501:500:Sergio González:/home/sergio:/bin/bash

Usuario.-Nombre de la cuenta con la que el usuario se logeara para acceder al sistema

Password.-Contraseña de la cuenta del usuario que usara para logearse en el sistema

UID.-Identificador del Usuario

GID.-Identificador que indica a cual grupo pertenece el usuario

Informacion Adicional.-Informacion detallada del usuario

Home del Usuario.- Directorio de trabajo del usuario

Shell.- Bash particular con la que el usuario trabajara

/etc/group

En este fichero se encuentran almacenados los datos sobre los grupos creados en el sistema asi como los usuarios que pertenecen a cada grupo. Tiene la siguiente estructura:

ventas:x:502:pepito,juanito,maria

Grupo.-Nombre del grupo

Password.- Contraseña del grupo

GID.-Identificador que indica a cual grupo pertenece el usuario

Miembros.- Usuarios pertenecientes al grupo

/etc/shadow

En este fichero se encuentran almacenados los datos sobre las contraseñas encriptadas de cada usuario del sistema. Tiene la siguiente estructura:

pepito:rfgf886DG778sDFFDRRu78asd:10568:0:-1:9:-1:-1::

Usuario.-Nombre de la cuenta con la que el usuario se logeara para acceder al sistema

Password Cifrado.- Contraseña del usuario cifrada

Parámetros del Password.-Informacion particular sobre el alta y caducidad de la cuenta.

Anteriormente (en sistemas Unix) las contraseñas cifradas se almacenaban en el mismo **/etc/passwd**. El problema es que 'passwd' es un archivo que puede ser leído por cualquier usuario, aunque solo modificado por root. Un ordenador potente con un buen programa de descifrado de contraseñas y paciencia es posible "crackear" contraseñas débiles (por eso la conveniencia de cambiar periódicamente la contraseña de root y de otras cuentas). El archivo 'shadow', resuelve el problema, solo puede ser leído por root.
De todas formas si deseamos guardar en **passwd** las contraseñas se utilizaría el comando **pwunconv.**

/etc/login.defs

En el archivo de configuración /etc/login.defs están definidas las variables que controlan los aspectos de la creación de usuarios y de los campos de shadow usadas por defecto. Algunos de los aspectos que controlan estas variables son:

- Número máximo de días que una contraseña es válida **PASS_MAX_DAYS**
- El número mínimo de caracteres en la contraseña **PASS_MIN_LEN**
- Valor mínimo para usuarios normales cuando se usa useradd **UID_MIN**
- El valor umask por defecto **UMASK**
- Si el comando useradd debe crear el directorio home por defecto **CREATE_HOME**

Basta con leer este archivo para conocer el resto de las variables que son autodescriptivas y ajustarlas al gusto. Recuérdese que se usaran principalmente al momento de crear o modificar usuarios con los comandos useradd y usermod que se explican a continuación.

2.1. Administración de Grupos

Dando de alta grupos

Para dar de alta grupos en el sistema usaremos el comando **groupadd** el cual deberá ser aplicado según la siguiente estructura

groupadd [opciones] nombreDelGrupo

Las opciones que pueden utilizarse con el comando **groupadd** son las siguientes:

Opciones	Descripcion
-g | --gid	Define un GID para un grupo
-r |	Define un grupo del sistema. Un grupo del sistema es aquel que tiene un numero de identidad (GID) de grupo por debajo del numero 500
-f | --force	Fuerza al sistema a crear el grupo aunque este ya exista.

Práctica 6: Dar de alta el grupo **ventas** asi como el grupo **contabilidad.** Dichos grupos tendrán las siguientes características:

- Nombre de los grupos → **ventas, contabilidad**
- Identificador para estos grupos → **520 y 530**

Comprueba el resultado en el fichero de configuración correspondiente.

Modificando grupos

Para modificar grupos dados de alta en el sistema usaremos el comando **groupmod** el cual deberá ser aplicado según la siguiente estructura

groupmod [opciones] nombreDelGrupo

Las opciones que pueden utilizarse en con el comando groupadd son las siguientes:

Opciones	Descripcion
-g | --gid	Define un nuevo GID para un grupo
-n | --new-name	Permite cambiar el nombre del grupo por otro

Práctica 7: Modificar el grupo **contabilidad** con las siguientes características Renombrar el grupo por **administracion y** cambiar su GID de **530 a 540**

Eliminando grupos

Para eliminar grupos en el sistema usaremos el comando **groupdel** el cual deberá ser aplicado según la siguiente estructura

gruopdel nombreDelGrupo

Práctica 8: Eliminar el grupo que se creó por defecto cuando instalamos el sistema.

2.2. Administración de cuentas de Usuario

Dando de alta cuentas de usuario

Para dar de alta cuentas de usuario en el sistema usaremos el comando **useradd** el cual deberá ser aplicado según la siguiente estructura:

useradd [opciones] nombreDelUsuario

Las **opciones** que pueden utilizarse con el comando **useradd** son las siguientes:

Opciones	Descripción
-d | --home	Carpeta de trabajo que sera asignado al usuario Ejemplos a) -d /home/usuario1 b) -d /home/cmartinez c) -d /home/icastillo

-s | --shell	Versión del Shell que se asigna al usuario, las opciones disponibles son: a) -s /bin/bash → Interprete de comandos de Linux equivalente a MS-DOS b) -s /sbin/nologin → El usuario no podrá logearse en el sistema. Ideal para usuarios con acceso a Samba o FTP sin acceso al interprete de comandos
-g | --gid	Grupo principal al cual puede ser asignado un usuario Ejemplos a) -g administracion b) -g Ventas
-G | --groups	Grupo secundario al cual puede ser asignado un usuario Ejemplos a) -G desarrolloJava b) -G ventasMedicas
-u | --uid	Identificador que sera asignado al usuario. Por defecto Linux asignara UID's a partir del numero 500 Ejemplos a) -u 501 b) -u 503
-e --expiredate	Se usa para especificar la fecha en la cual expira la cuenta. Debe especificarse en el siguiente formato Año-Mes-Dia. Ejemplos a) -e 20100506 b) -e 20081224
-m	Crea el directorio del usuario */home/usuario* y lo que haya en /etc/skel

Práctica 9. Dar de alta al usuario **adan** el cual tendrá las siguientes características:

- Nombre de usuario → **adan**
- Directorio de Trabajo → **/home/adan**
- Shell asignado → **BASH**
- Identificador para este usuario → **512**
- Grupo principal de trabajo → **ventas**
- Grupo secundario de trabajo → **administracion**

NOTA.- El nombre del usuario tiene que ser exactamente igual al nombre especificado en el directorio de trabajo de otra forma no sera posible ejecutar correctamente el comando.Asi mismo, no sera necesario crear antes el directorio de trabajo /home/adan, esto es debido a que el comando useradd lo creara por defecto .

Practica 10. Dar de alta al usuario **eva** el cual tendrá las siguientes características:

- Nombre de usuario → **eva**
- Directorio de Trabajo → **/home/eva**
- Shell asignado → **BASH**

- Identificador para este usuario → **515**
- Grupo principal de trabajo → **administracion**
- Grupo secundario de trabajo → **ventas**
- Tiempo de vida de la cuenta → **5 años**

Asignando contraseñas a las cuentas de usuario

Para asignar contraseñas a las cuentas de usuario haremos uso del comando **passwd** el cual deberá ser aplicado según la siguiente estructura

passwd nombreDelUsuario

Práctica 11: Asignar contraseña a los usuarios **adan y eva.**

Eliminando cuentas de usuario

Para eliminar cuentas de usuario en el sistema usaremos el comando **userdel** el cual deberá ser aplicado según la siguiente estructura

userdel [opciones] nombreDelUsuario

Las opciones que pueden utilizarse con el comando useradd son las siguientes:

Opciones	Descripción
-f | --force	Fuerza a remover el usuario del sistema aunque este este activo.
-r | --remove	Elimina la carpeta de trabajo del usuario y todo su contenido.

Práctica 12.- Elimina el usuario que se creó por defecto durante su instalación así como su directorio de trabajo.

Práctica 13.- Busca en internet la diferencia entre el comando **useradd y adduser.**

Modificando cuentas de usuario

El comando **usermod** permite modificar o actualizar un usuario o cuenta ya existente. Sus opciones más comunes o importantes son las siguientes:

Opciones	Descripción
-c | --change	añade o modifica el comentario o campo 5 de /etc/paswd
-d | --directory	modifica el directorio de trabajo del usuario, campo 6 de /etc/passwd
-e	cambia o establece la fecha de expiración de la cuenta, formato AAAA-MM-DD, campo 8 de /etc/shadow
-g | --group	cambia el número de grupo principal del usuario (GID), campo 4 de /etc/passwd
-G	establece otros grupos a los que puede pertenecer el usuario, separados por comas.

-l | --login	cambia el login o nombre del usuario, campo 1 de /etc/passwd y de /etc/shadow
-L	bloquea la cuenta del usuario, no permitiéndole que ingrese al sistema. No borra ni cambia nada del usuario, solo lo deshabilita.
-s	cambia el shell por defecto del usuario cuando ingrese al sistema.
-u	cambia el UID del usuario.
-U	desbloquea una cuenta previamente bloqueada con la opción -L.

Práctica 14. Deshabilita el usuario **adan,** compruébalo y vuelvo a habilitarlo.

2.3. Archivos de configuración

Los usuarios normales y root en sus directorios de inicio tienen varios archivos que comienzan con "." es decir están ocultos.

.bash_profile aquí podremos indicar alias, variables, configuración del entorno, etc. que deseamos iniciar al principio de la sesión.

.bash_logout aquí podremos indicar acciones, programas, scripts, etc., que deseemos ejecutar al salirnos de la sesión.

.bashrc es igual que .bash_profile, se ejecuta al principio de la sesión, tradicionalmente en este archivo se indican los programas o scripts a ejecutar

Lo anterior aplica para terminales de texto 100%.

Si deseamos configurar archivos de inicio o de salida de la **sesión gráfica** entonces, hay que buscar en el menú del ambiente gráfico algún programa gráfico que permita manipular que programas se deben arrancar al iniciar la sesión en modo gráfico. En la mayoría de las distribuciones **existe un programa llamado "sesiones" o "sessions",** generalmente esta ubicado dentro del **menú de preferencias**. En este programa es posible establecer programas o scripts que arranquen junto con el ambiente gráfico.

Además Linux permite que el usuario decida que tipo de entorno Xwindow a utilizar, ya sea algún entorno de escritorio como KDE o Gnome o algún manejador de ventanas como Xfce o Twm. Dentro del **home del usuario**, se creará un directorio o archivo escondido "." , por ejemplo '.gnome' o '.kde' donde vendrá la configuración personalizada del usuario para ese entorno. Dentro de este directorio suele haber varios directorios y archivos de configuración. Estos son sumamente variados dependiendo de la distribución y del entorno. No es recomendable modificar manualmente es mucho mas sencillo modificar vía las interfases gráficas que permiten cambiar el fondo, protector de pantalla, estilos de ventanas, tamaños de letras, etc.

Practica 15.- Modifica el fichero .bashrc para que al iniciar sesión de la Bienvenida.

2.4. Administración de Permisos

Los comandos que usaremos para asignar permisos tanto a carpetas como a ficheros serán los siguientes:

chmod

Para modificar permisos de escritura, lectura y/o ejecución sigue la siguiente estructura

chmod [UGO] archivo/directorio

Las letras U,G y O son interpretadas de la siguiente manera

U.-Permisos para el usuario
G.-Permisos para el grupo
O.-Permisos para otros

Los permisos para usuario, grupo y otros se forman de la siguiente manera

U= rwx G= rwx O= rwx

Las letras 'r' 'w' y 'x' tienen la siguiente funcion:

	Descripcion
r | read	Lectura de un archivo
w | write	Escritura de un archivo
x | execute	Ejecución de un archivo

Las letras '**r**' '**w**' y '**x**' tendrán que ser substituidas por un numero **1** o un numero **0** dependiendo del tipo de permisos que se asignen.

	Descripcion
1	Permite leer, escribir o ejecutar un archivo
0	Restringe leer, escribir o ejecutar un archivo

Una vez subtituidas las letras por números tendremos como resultado un numero binario el cual se transforma a base 10 y finalmente deberá ser asignado a la letra '**U**' '**G**' u '**O**'.

Una forma mas rápida de asignar permisos tanto a archivos como a carpetas es mediante la aplicación del mismo comando pero con la siguiente nueva estructura.

chmod u=rwx,g=rwx,o=rwx [archivo/directorio]

En donde las letras '**u**' , '**g**' , '**o**' , '**w**' , '**r**' y '**x**' tienen la siguiente funcion:

	Descripcion
u | usuario	Usuario
g | grupo	Grupo
o | otros	Otros
r | read	Lectura de un archivo
w | write	Escritura de un archivo
x | execute	Ejecución de un archivo

chown

Para modificar el grupo y/o propietario de un archivo o directorio se deberá seguir la siguiente estructura

chown [nuevoPropietario:nuevoGrupo] [archivo/directorio]

Practica 16. Realiza los pasos siguientes para comprobar el uso del comando.

Paso 1

Dar de alta al usuario **moises** el cual tendrá las siguientes características:

- Nombre de usuario → **moises**
- Directorio de Trabajo → /home/moises
- Shell asignado → BASH
- Identificador para este usuario → 512
- Grupo principal de trabajo → ventas

Paso 2

Logearse con la cuenta de “root” y una vez dentro crear un archivo con la ayuda del editor de textos **nano** el cual deberá ser guardado con el nombre de “**prueba1.txt**”

Paso 3

Verificar los permisos del archivo “prueba 1”

[root@localhost]# ls -l prueba1.txt

Paso 4

Hacer los siguientes cambios al archivo **prueba1.txt**

Nuevo propietario → **adan**

Nuevo grupo → **administracion**

Permisos para el propietario → **Lectura,Escritura y Ejecución = 7**

Permisos para el grupo → **Lectura y Ejecución = 5**

Permisos para otros → **ninguno**

Para comprobar los cambios solo basta ejecutar nuevamente el comando ls -l

chgrp

A diferencia de chown este comando solo sirve para modificar el grupo de un archivo o directorio , para hacer uso de este comando se debe seguir la siguiente estructura.

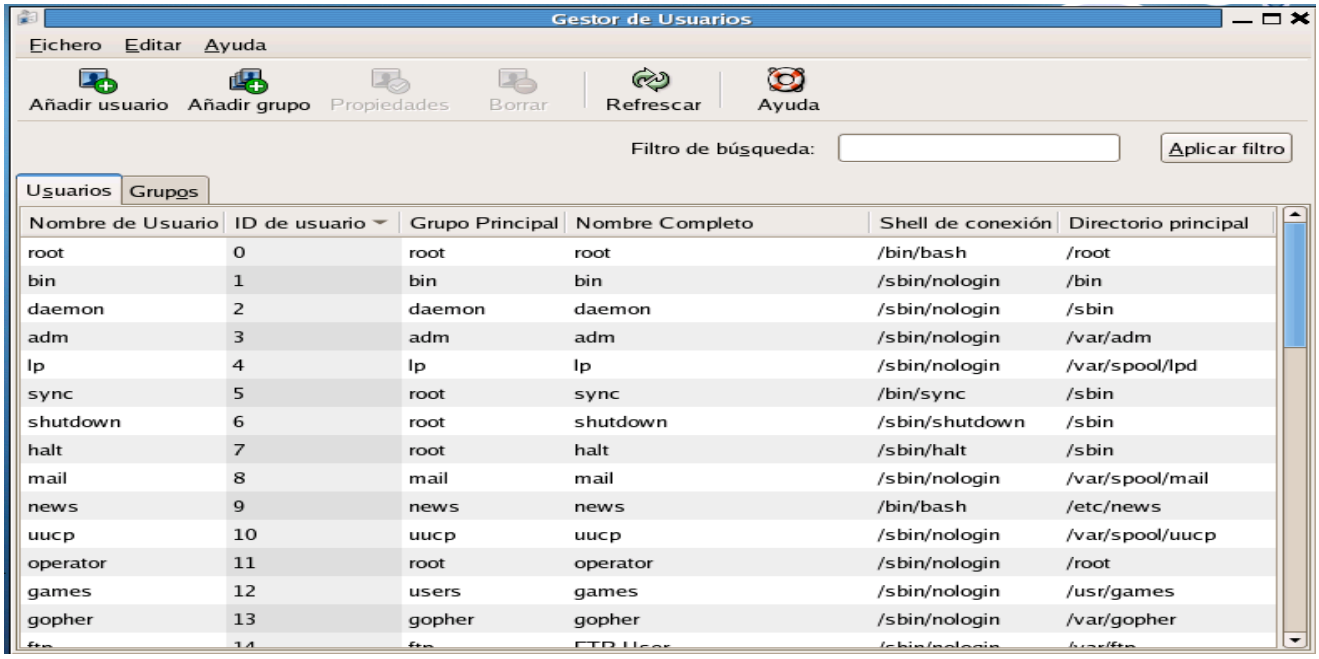
chgrp [nuevoGrupo] [archivo/directorio]

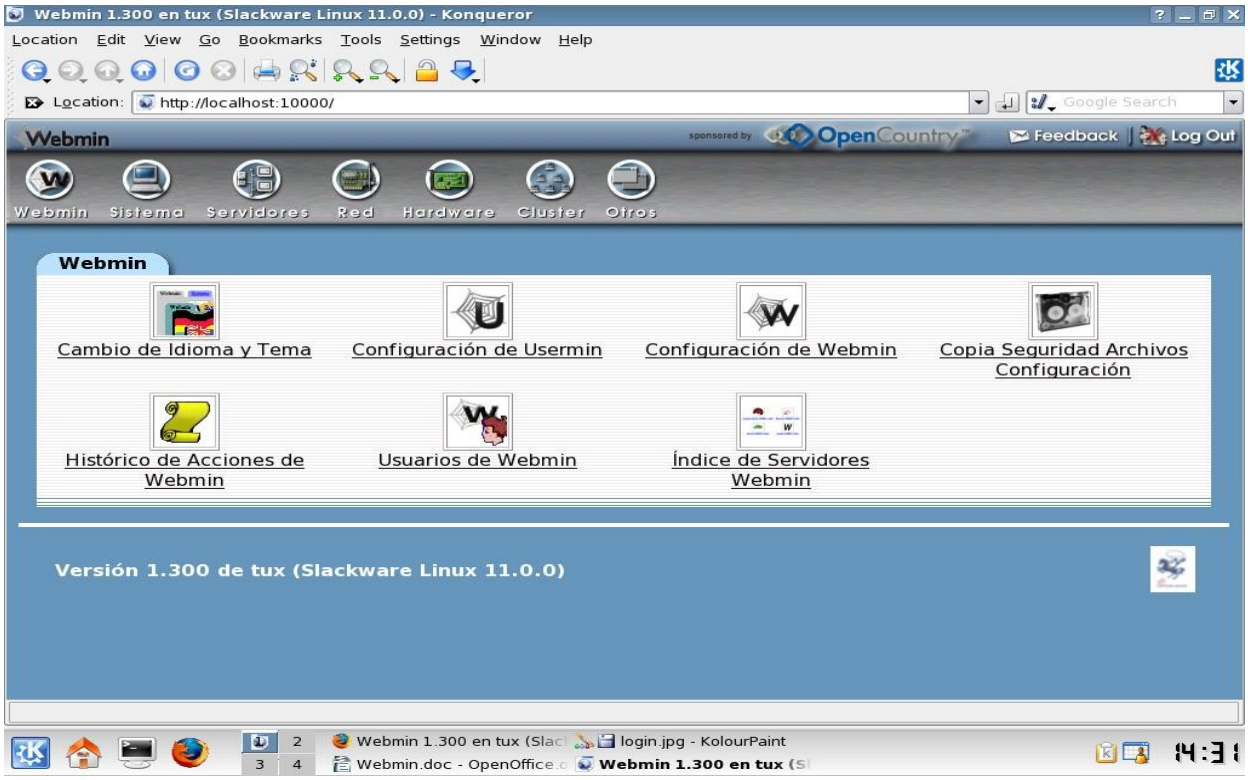
Practica 17 En base al ejemplo 9 asignaremos al archivo **prueba1.txt** el grupo → **administracion**

Para comprobar los cambios solo basta ejecutar nuevamente el comando ls -l

2.5. Ambientes gráficos y Web

Si usas Linux con Xwindow (gnome, kde, etc.) encontrarás dentro de los menús una o varias opciones gráficas de administración de usuarios, así como programas basados en **Web como webmin (muy recomendable)** que entre muchas otras cosas te permiten un control total de la administración de usuarios y grupos. Estos programas de gestión de usuarios son sumamente intuitivos y en una sola pantalla a través de sus opciones puedes controlar prácticamente todas las funciones.





2.5. Estableciendo límites a lo usuarios.

En los sistemas UNIX/LINUX existe la posibilidad de limitar recursos a los usuarios o grupos, por ejemplo, máximo numero de logins que puede realizar simultáneamente un usuario, el máximo tiempo de CPU, el máximo numero de procesos etc. Estos límites se controlan en LINUX a través del fichero **/etc/security/limits.conf**. También es posible limitar los tiempos de acceso a los usuarios. Una de las formas de hacerlo es con el servicio **timeoutd**. Este servicio se instala a través de la distribución y, una vez instalado aparece un fichero de configuración /etc/timeouts. Una línea del fichero podría ser esta:

```
TIMES:TTYS:USERS:GROUPS:MAXIDLE:MAXSESS:MAXDAY:WARN
```

o bien

```
TIMES:TTYS:USERS:GROUPS:LOGINSTATUS
```

Practica 18. Ejemplos de límites horarios

- El usuario **adan** no puede hacer login durante el fin de semana:

```
SaSu:*:curso:*:NOLOGIN
```

- Sólo el usuario **root** puede acceder desde las consolas tty1–tty6:

```
Al:tty1,tty2,tty3,tty4,tty5,tty6:root:*:LOGIN
Al:tty1,tty2,tty3,tty4,tty5,tty6:*:*:NOLOGIN
```

- Sólo el usuario **root** puede acceder entre las 22:00 y las 23:00h de cada día:

```
Al1500-1600:*:root:*:LOGIN
Al1500-1600:*:*:*:NOLOGIN
```

Una vez preparado el fichero /etc/timeouts **es necesario reiniciar el servidor timeoutd:**

..# /etc/init.d/timeoutd restart
Stopped /usr/sbin/timeoutd (pid 2412).
Starting /usr/sbin/timeoutd...

Es importante destacar que este proceso **no actúa durante el proceso de login** lo que da lugar a que, aunque un usuario tenga prohibido el acceso a una máquina en un momento determinado, inicialmente puede entrar y sólo, una vez que se ejecute el proceso timeoutd, será expulsado del sistema. **Para conseguir que durante el proceso de login se revisen las condiciones de timeouts** se debe incluir las siguientes lineas en el fichero /etc/profile:

```
# Comprueba restricciones de timeoutd (ver timeoutd, timeouts(5))
 /usr/sbin/timeoutd ‘whoami‘ ‘basename \‘tty\‘‘ || exit
```

Con esta línea incluso aunque el servicio timeoutd este parado si en el fichero

/etc/timeouts se prohíbe el acceso a un usuario éste no podrá entrar en el sistema.

Límites de quotas

El sistema de quotas provee un m**ecanismo de control y uso del espacio de disco duro disponible en un sistema**. Se pueden establecer limites en la cantidad de espacio y el número de ficheros de que puede disponer un usuario o grupo. En las quotas hay cuatro números para cada límite: la cantidad actual ocupada; el límite soft (quota propiamente dicha); el límite hard (espacio sobre quota), y el tiempo que resta antes de eliminar el exceso entre soft y hard. Mientras que el límite soft puede ser superado temporalmente, el límite hard nunca puede rebasarse.

Administrando el sistema de quotas

Para implementar el sistema de quotas es necesario instalar algún paquete de control de dicho sistema. En **Ubuntu hay un paquete denominado quota** que instala todo lo necesario para implementar todo el sistema. Una vez instalado tenemos que realizar una serie de pasos para activar el mecanismo de quotas. Estos pasos son:

- Configuración de kernel

Antes de instalar el sistema de quotas **debe disponerse de un kernel con la opción de quota–system habilitada**. Esto se consigue en el proceso de compilación de un nuevo kernel respondiendo yes a la pregunta de Disk QUOTA support Los **kernels precompilados que se distribuyen con Debian (paquetes kernel-image.ya tienen esta opción habilitada**.

- Elección del sistema de ficheros sobre el que se aplican las quotas

Lo normal es que solo el sistema donde están las cuentas de usuarios tengan quotas, aunque **es recomendable que tenga quotas todo sistema de ficheros donde los usuarios puedan escribir.** Para habilitar las quotas en un sistema de ficheros hay que editar el fichero /etc/fstab e incluir las opciones usrquota y grpquota:

```
# /etc/fstab: static file system information.
# file system mount     point          type options                                    dump pas
/dev/hda5 /                 ext2       defaults,errors=remount-ro,usrquota,grpquota    0
```

- Habilitar las quotas

Para instalar los ficheros de quotas se debe ejecutar el comando:

 # quotacheck -avug

Scanning /dev/hda5 [/] done
Checked 4943 directories and 57624 files
Using quotafile /quota.user
Updating in-core user quotas
Using quotafile /quota.group
Updating in-core group quotas

A continuación establecer o activar el sistema de cuotas

 # quotaon -f /dev/hda5 (en nuestro caso es /dev/hda5)

A veces se hace necesario volver a ejecutar el programa sin la -f

 # quotaon /dev/hda5

La primera vez que se ejecuta este comando sirve para crear los ficheros de quotas: **quota.user y quota.group.**

- Especificar quotas para usuarios o grupos

Para editar la quota de un usuario o grupo s**e usa el programa edquota con la opción -u para editar las quotas de usuarios y con la opción -g para editar las opciones de grupo.** Sólo hay que editar los números que están detrás de soft y hard. El **período de gracia que hay entre** el límite soft y el hard puede cambiarse con:

 # edquota -t

La mayoría de las veces los usuarios tienen la misma quota. Una forma rápida de editar la quota de todos los usuarios es colocarse en el directorio **donde tienen sus directorios raíz cada usuario. Editar la quota de uno de estos usuarios con los valores apropiados y, posteriormente, ejecutar**:

 # edquota -p *usuarioprototipo* *

Para verificar las quotas que tiene un usuario se utiliza el comando:

 # quota -v

El **superusuario puede ver** las quotas de todos los usuarios con el comando:

#repquota filesystem

- Desabilitar quotas para usuarios o grupos

Para deshabilitar las quotas de un usuario o grupo solo hay que editarlas quotas y poner los limites a 0. Así un usuario puede usar tantos bloques e inodos como quiera.