



4 Configuración de sistemas operativos












Sumario

4 Configuración de sistemas operativos.....	1
4.1 Convencións empregadas.....	4
4.2 Administración básica do sistema Windows.....	5
4.2.1 Administración de usuarios e grupos.....	5
4.2.2 Contas de usuario en panel de control.....	6
4.2.3 "Usuarios e grupos" desde "Administración de equipos".....	8
4.2.3.1 Grupos en Windows.....	9
4.2.3.2 Cambiar nome ou contrasinal dun usuario.....	10
4.2.4 UAC (User Account Control, Control de Contas de Usuario).....	12
4.2.5 Seguridade local. Permisos locais ou NTFS.....	12
4.2.5.1 Lapela Seguridade.....	12
4.2.5.2 Modificar permisos estándar. Botón editar da lapela Seguridade.....	13
4.2.5.3 Botón Opcións avanzadas en lapela Seguridade.....	17
4.2.5.4 Recomendacións e exemplo final.....	21
4.2.6 Rexistro de Windows. Directivas de grupo e seguridade local.....	21
4.2.6.1 Rexistro de Windows.....	22
4.2.6.2 Directivas de grupo ou política local.....	24
4.2.6.3 Directivas de seguridade local.....	25
4.2.6.4 Ferramentas do sistema. Ferramentas administrativas.....	28
4.2.6.4.1 Cotas de disco.....	28
4.2.6.4.2 Desfragmentar e Comprobar unidade.....	29
4.2.6.4.3 Programador de tarefas.....	31
4.2.6.4.4 Protección do sistema. Puntos de restauración.....	31
4.2.6.4.5 Configuración. Actualización e seguridade.....	32
4.3 Administración básica do sistema Linux.....	36
4.3.1 Administración de usuarios e grupos.....	36
4.3.1.1 Creación de usuarios e grupos.....	36
4.3.1.2 Eliminación e modificación de usuarios e grupos. Propietarios de arquivos.....	39
4.3.2 Montaxe de dispositivos de almacenamento.....	41
4.3.3 Permisos de ficheiros e directorios.....	47
4.3.4 Xestión de procesos.....	49
4.3.5 Información do sistema e rexistro.....	53
4.3.6 Tarefas programadas.....	57

Material docente elaborado a partir da base dos materiais formativos de FP Online
propiedade do Ministerio de Educación e Formación Profesional.

[Aviso Legal](#)

4.1 Convencións empregadas

	Esta icona fai referencia a notas de introdución
	Esta icona indica aclaración
	Esta icona fai referencia a arquivos de configuración, de rexistro...
	Esta icona indica casos de uso
	Esta icona fai referencia a avisos o advertencias
	Esta icona indica incidentes
	Esta icona fai referencia a sección que inclúen instrucións paso a paso
	Esta icona fai referencia a sección que inclúen capturas de pantalla
	Esta icona fai referencia a actividades
	Esta icona fai referencia a documento esencial (licenza: http://www.ohmyicons.com)
	Referencia a ligazón recomendada (licenza: http://iconleak.com)

4.2 Administración básica do sistema Windows

4.2.1 Administración de usuarios e grupos

Nesta unidade, imos aprender a administrar Windows. Empezamos coa administración de usuarios e grupos.

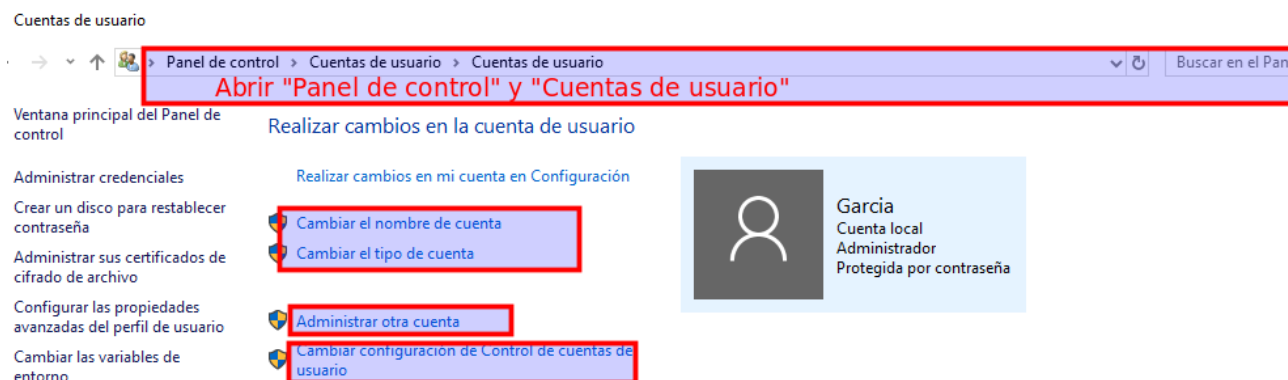
As contas de usuario están pensadas para uso individual, mentres que os grupos serven para facilitar a administración de varios usuarios.

En Windows hai 2 programas gráficos para a administración de usuarios e grupos:

- “Contas de usuario” desde “Panel de Control”
- “Usuarios e grupos” desde “Administración de equipos”

Este programa é máis completo para administrar usuarios e grupos, pero non está incluído nas versións Home. É o que utilizaremos por defecto nas versións Profesionais.

Móstrase unha imaxe de ambos os programas.

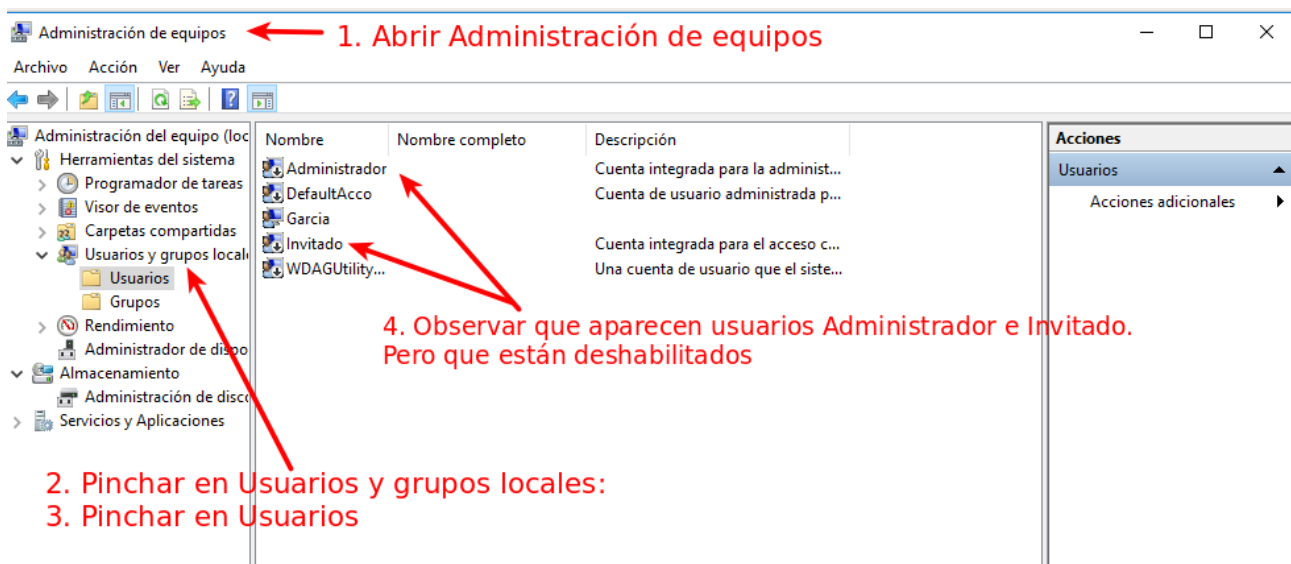


Miguel Ángel García Lara ([CC BY-NC-SA](#))

Na imaxe pódese observar que a instalación de Windows creou contas de usuario integradas, en concreto os usuarios Administrador e invitado, pero que ambos se atopan deshabilitados, polo que non poden iniciar sesión. Estes usuarios pódense habilitar, pulsando no seu menú contextual.

Habilitar o usuario invitado, permitiría que calquera persoa con acceso físico ao equipo, poida iniciar sesión.

Á parte destes usuarios creados automaticamente por Windows, atópase o usuario solicitado durante a instalación (Garcia na imaxe) con permisos de administrador.

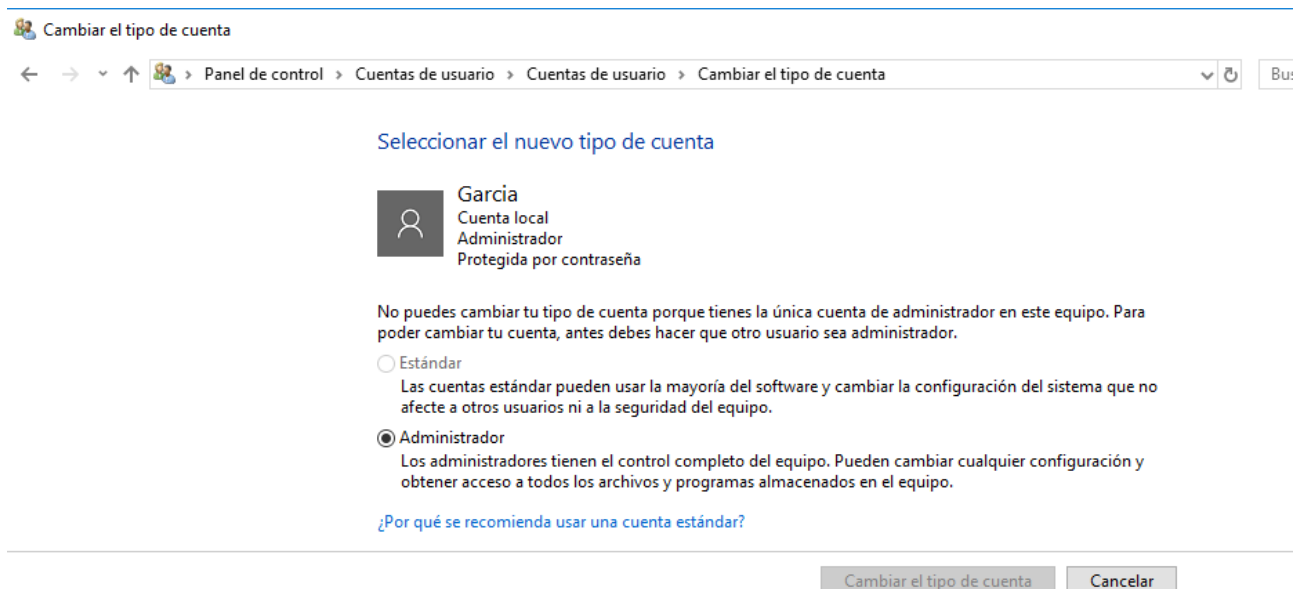


Miguel Ángel García Lara ([CC BY-NC-SA](#))

4.2.2 Contas de usuario en panel de control

Se pulsamos en “Cambiar o tipo de conta” podemos seleccionar 2 opciones: usuario estándar e administrador

Ilustración que mostra a conta pódese cambiar a usuario estándar ou administrador



Miguel Ángel García Lara ([CC BY-NC-SA](#))

- Conta de usuario estándar: Ten privilexios limitados, pódese usar a maioría dos programas instalados no equipo, pero non se pode instalar ou desinstalar software

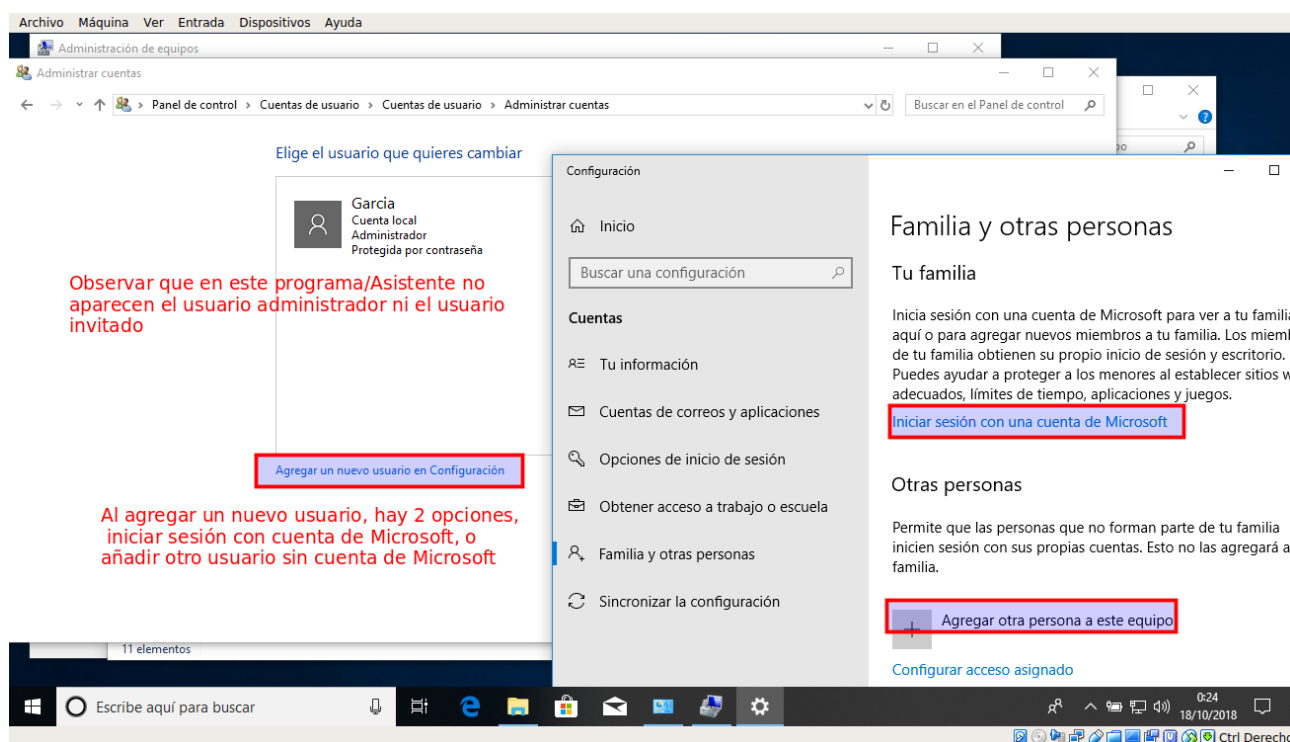
nin hardware, eliminar arquivos que son necesarios para que o equipo funcione, ou cambiar opcións de configuración no equipo que afecten a outros usuarios.

- Conta de administrador: Ten o máximo control sobre o equipo e só se debe utilizar cando leven a cabo tarefas de administración. Permite realizar cambios que afectan a outros usuarios. Son tarefas fundamentais dos administradores as relativas á configuración de seguridade, á instalación de software e hardware, e á obtención de acceso a todos os arquivos nun equipo.

Ademais, existe o tipo invitado, pero que por defecto vén deshabilitado e que nin sequera aparece na xanela de “Contas de usuario”

Se pulsamos en administrar outra conta, poderemos cambiar o seu tipo ou crear unha nova conta de usuario.

Ilustración Pulsar en administrar outra conta



Miguel Ángel García Lara ([CC BY-NC-SA](#))

Para crear unha conta de usuario, os pasos son:

1. Facer clic en Administrar outra conta.
2. Crear unha nova conta.
3. Escribir o nome que desexamos utilizar para a conta e, despois, facer clic en Seguinte.

4. Seleccionar o tipo de conta que desexamos e despois facer clic en Crear conta.

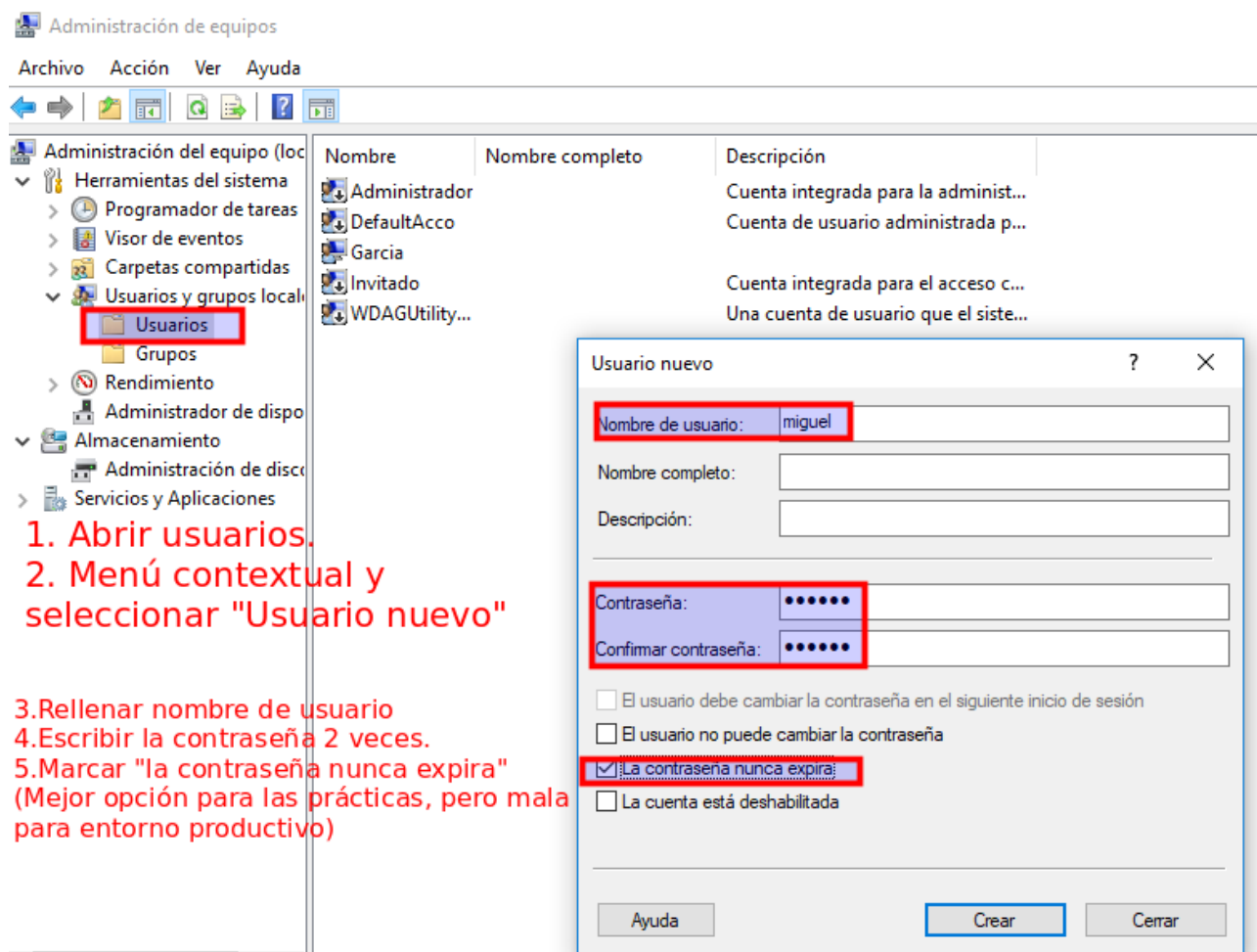
Cando eliminamos unha conta de usuario, esta bórrase definitivamente do sistema. Non podemos recuperala creando outra co mesmo nome co obxecto de conseguir os mesmos permisos da conta antiga. Isto é debido a que cando creamos outra conta nova o sistema asigna un novo SID distinto da conta antiga.

4.2.3 "Usuarios e grupos" desde "Administración de equipos"

Tamén se pode abrir este programa executando `lusrmgr.msc`

Para crear un usuario, púlsase menú contextual dentro da xanela usuarios ou en menú "Acción / Usuario novo"

Ilustración Menú contextual en Usuarios para crear usuario novo



Miguel Ángel García Lara (CC BY-NC-SA)

4.2.3.1 Grupos en Windows

Os grupos en Windows simplifican a administración de contas de usuario. Cando queiramos compartir un cartafol a un departamento enteiro, será máis cómodo introducir a todos os usuarios nun grupo e compartir o cartafol a ese grupo.

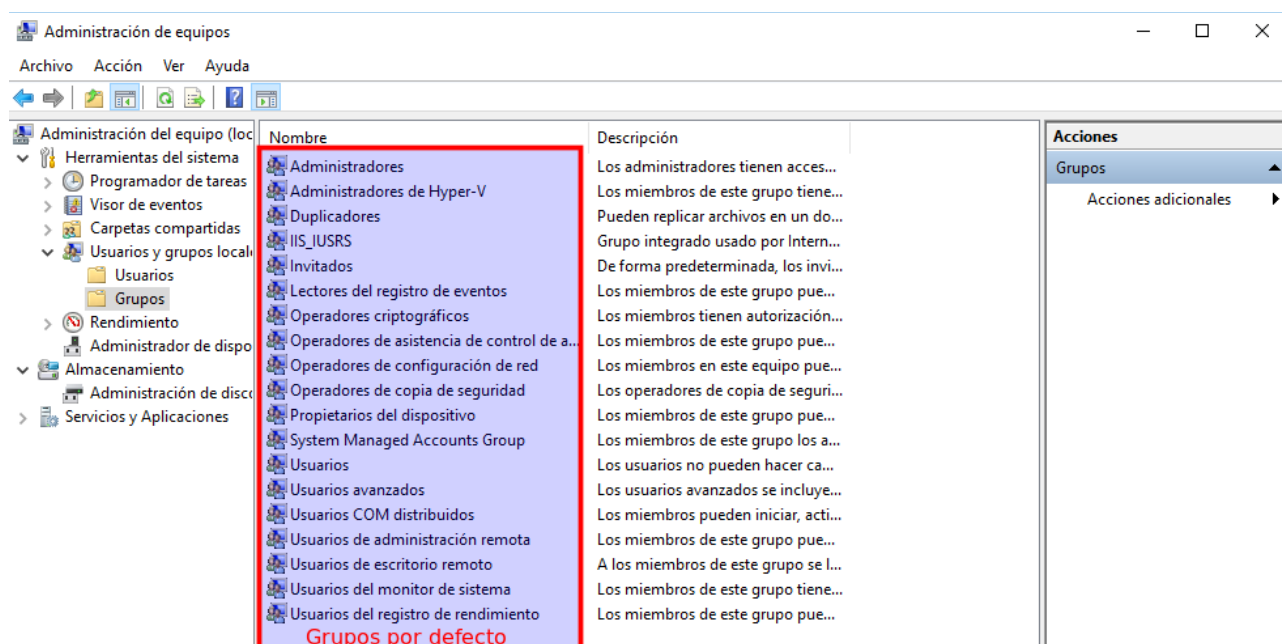
Cando se instala Windows créanse varios grupos de usuarios, estas contas de grupo dicir contas integradas. Ademais, o administrador poderá crear novos grupos.

Polo que hai tres tipos de grupos:

- Os grupos creados polo administrador
- Os grupos integrados (Administradores, Usuarios, Usuarios avanzados,...)
- Grupos de seguridade integrados ou especiais, ás que se pertence segundo a actividade realizada no momento. Por exemplo, atópanse o grupo Todos, Usuarios autenticados. Estes grupos non aparecen explicitamente, pero si que se lles pode dar permisos nun cartafol ou ficheiro.

Na seguinte captura, móstranse as contas de grupo integradas en Windows 10 Profesional.

Ilustración Grupos creados por defecto en Windows



Miguel Ángel García Lara (CC BY-NC-SA)

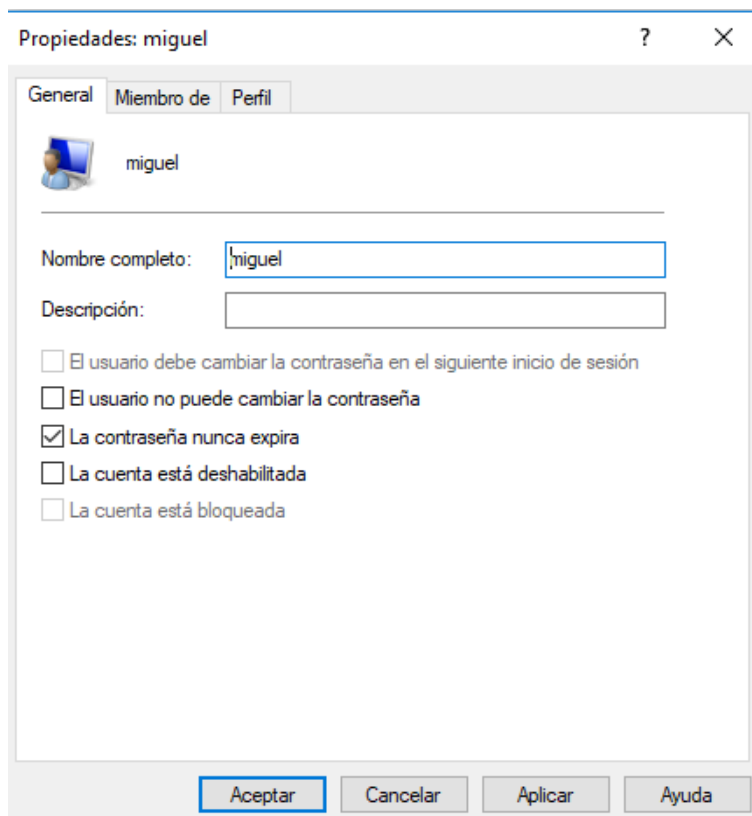
O nome dos grupos, adoita servir para entender o seu obxectivo. Por exemplo, o grupo “Operadores de copias de seguridade” terá aos usuarios que se lles permita realizar copias de seguridade.

Si que destacamos o grupo de “Usuarios avanzados” cuxa diferencia co grupo “Usuarios” é que permite instalar aplicacións.

4.2.3.2 *Cambiar nome ou contrasinal dun usuario*

Se accedemos co menú contextual ás propiedades dun usuario, temos tres lapelas:

Ilustración que mostra a lapela xeral das propiedades dun usuario



Miguel Ángel García Lara (CC BY-NC-SA)

Lapela “Xeral”:

Indícase o nome completo do usuario e a súa descrición. Hai que ter coidado con esta opción, se por exemplo, o usuario chámase juana, pero en nome completo escribimos “Juana López”, ao iniciar sesión gráfica, aparecerá “Juana López”, pero o nome do usuario é “juana”, polo que o seu cartafol de usuario é C:\Users\juana

Tamén se poden configurar as seguintes opcións sobre o contrasinal:

- O usuario debe cambiar o contrasinal no seguinte inicio de sesión. Obrígaselle ao usuario cambiar contrasinal a primeira vez.
- O usuario non pode cambiar o contrasinal.

- O contrasinal nunca caduco. É habitual ter desmarcada esta opción, para obrigar ao usuario cambiar a opción periodicamente.

Para as tarefas do módulo, recoméndase deixar marcada só a opción “O contrasinal nunca caduca” por comodidade, para non ter que cambiar o contrasinal constantemente dos distintos usuarios. Con todo, a nivel profesional, recoméndase deixar marcada a primeira opción, para obrigar ao usuario cambiar contrasinal a primeira vez. Desta forma, ademais o administrador non coñecerá o contrasinal do usuario.

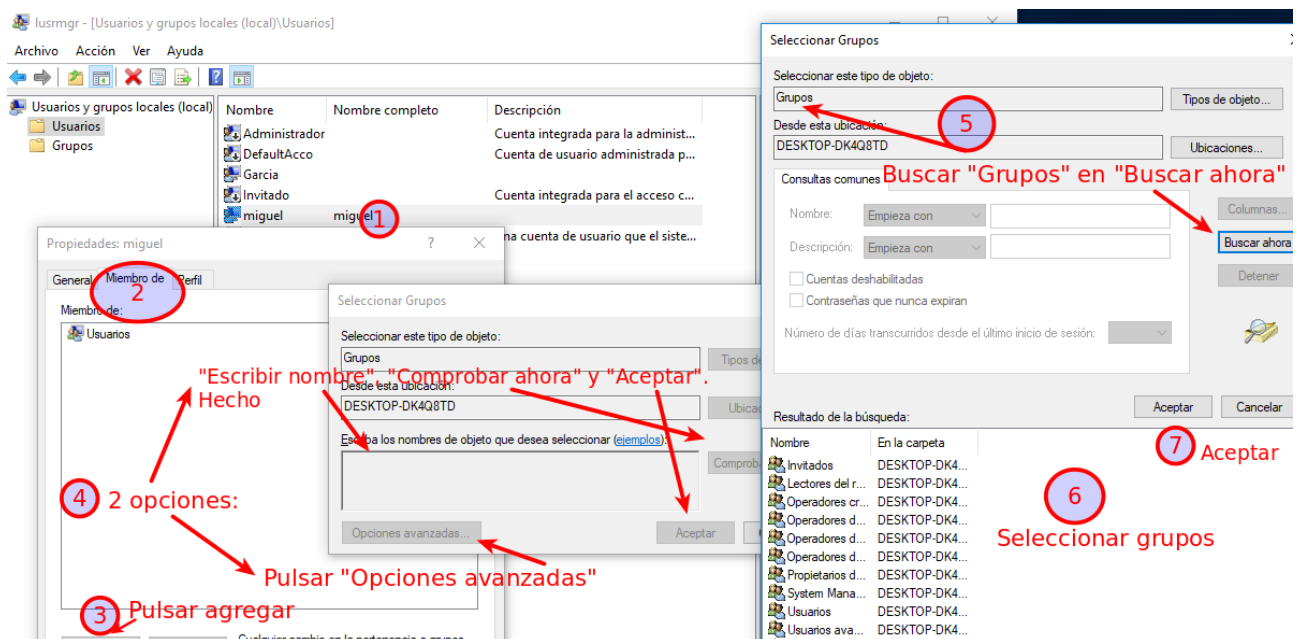
Finalmente, na lapela xeral, pódese deshabilitar ou habilitar a conta.

Lapela “Membro de”

Nesta pestana veremos todos os grupos aos que o usuario pertence actualmente. Podemos engadir ou eliminar ao usuario dos distintos grupos.

Na imaxe seguinte, móstrase como se pode incluír un usuario en distintos grupos.

En usuario seleccionado, pulsar "propiedades" e "membro de" para buscar grupo



Miguel Ángel García Lara (CC BY-NC-SA)

Se lle damos ao botón agregar poderemos escribir directamente o nome dun grupo onde agregalo. Se queremos escoller devandito grupo dunha lista dos grupos posibles, hai que escoller a opción Avanzada e logo Buscar agora, que nos mostrará unha lista de todos os grupos do sistema. Basta con seleccionar o que queiramos (ou os que queiramos) e pulsar aceptar.

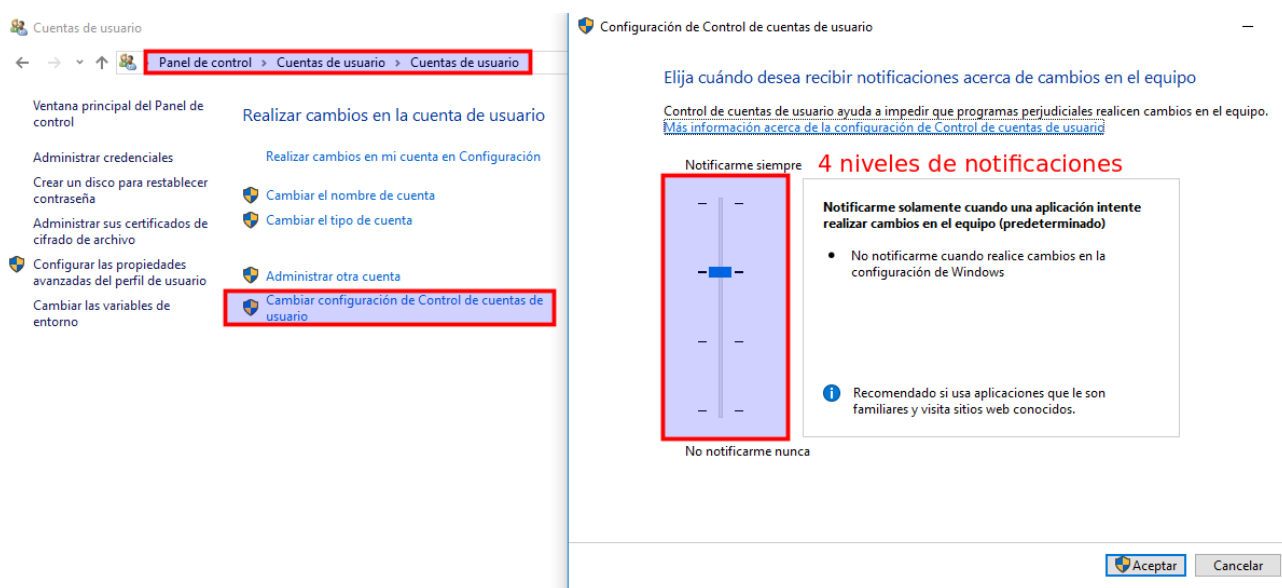
Do mesmo xeito que na xanela usuarios, na xanela Grupos, pódense crear e eliminar grupos; así como engadir ou quitar usuarios de grupos.

4.2.4 UAC (User Account Control, Control de Contas de Usuario)

Cada vez que se quere realizar algunha acción no sistema, como a instalación de programas, modifícanse o rexistro de Windows, etc. notifícase unha alerta de seguridade ao usuario. Esta alerta a lanza o UAC.

Pódense configurar 4 niveis de alerta, desde o nivel de alerta desexado. Isto realízase no panel “Contas de usuario”. Hai 4 niveis de alerta desde notificar sempre a non notificar nunca.

Ilustración onde se establece o nivel de alerta desexado en UAC



Miguel Ángel García Lara (CC BY-NC-SA)

4.2.5 Seguridade local. Permisos locais ou NTFS

4.2.5.1 Lapela Seguridade

Supoñamos un PC con Windows instalado, con 2 usuarios, Juan e María. Unha pregunta que nos facemos é se Juan pode protexer os seus arquivos sen que teña acceso María e viceversa. Estamos a falar de Seguridade local ou permisos locais, é dicir, no mesmo PC, sen utilizar a rede.

A resposta a esta pregunta é si, pero para iso a partición ten que ser NTFS.

En menú contextual Propiedades de ficheiro ou cartafol, aparecen 2 lapelas distintas: Compartir e Seguridade.

Compartir, son permisos para cando se acceden desde a Rede, é dicir, desde outro equipo.

Seguridade: son permisos para cando accede calquera usuario no equipo local. Estes permisos son os que imos configurar neste apartado.

Se non aparece a lapela Seguridade, é porque a partición é FAT 32. Pódese converter unha partición de FAT 32 a NTFS, sen necesidade de formatar nin eliminar os arquivos.

Para iso, executamos na terminal `convert unidade: /fs:ntfs`

Primeiras normas sobre permisos locais

- Podemos configurar permisos locais tanto a cartafol e ficheiros, en xeral falamos de obxectos.
- Por defecto, cando se crea un cartafol, hérdanse os permisos da cartafol pai.
- Os permisos concédense a usuarios e grupos.
- Todos os obxectos teñen un propietario, que por defecto é quen creou o obxecto.
- Os permisos aos obxectos pódenos cambiar os administradores e o usuario propietario do obxecto. A calquera usuario poderáselle dar dereito de cambiar permisos en calquera obxecto.
- Un administrador pódese converter en propietario de calquera obxecto

A lapela Seguridade incorpora 2 botóns: Estándar e Opcións avanzadas. Explícanse con detalle nos 2 apartados seguintes.

4.2.5.2 *Modificar permisos estándar. Botón editar da lapela Seguridade*

Pulsando o botón Editar na lapela Seguridade podemos modificar os **permisos estándar** (6 permisos para cartafol e 5 permisos para arquivos)

Os **permisos estándar** son (en orde de menos permisos a máis permisos):

- **Mostrar o contido do cartafol**
Só aparece en cartafol, permite ver os nomes de arquivos e subcarpetas.
- **Lectura**
En cartafol, permite "Mostrar o contido do cartafol" e ademais permite ver atributos, propietarios e os seus permisos.
En arquivos, permite ler os arquivos e ver os seus atributos, propietarios e os seus permisos.
- **Lectura e execución**
- **Ten os permisos de "lectura"**

Ademais en cartafol permite navegar por elas e en arquivos permite executar os programas (arquivos executables: exe, com, bat)

- Escritura

Inclúe todos os de lectura e execución, e ademais:

En cartafol, permite crear arquivos, subcarpetas e cambiar atributos.

En arquivos, permite cambiar o contido (sobrescribir o arquivo) e cambiar atributos.

- Modificar

Inclúe todos os de escritura, e ademais:

En cartafol permite borrar o cartafol

En arquivos permite borrar o arquivo

- Control total

Inclúe todos os de modificar, e ademais:

En cartafol permite borrar subcarpetas e arquivos, cambiar atributos e cambiar propietarios.

En arquivos, permite cambiar atributos e cambiar propietarios.

Estes permisos estándar divídense en 3 categorías principais:

Se queremos lectura e execución, concédense os permisos:

- Lectura e execución
- Mostrar o contido do cartafol
- Lectura

Se queremos modificar, ademais dos de lectura concédense os permisos:

- Modificar
- Escritura

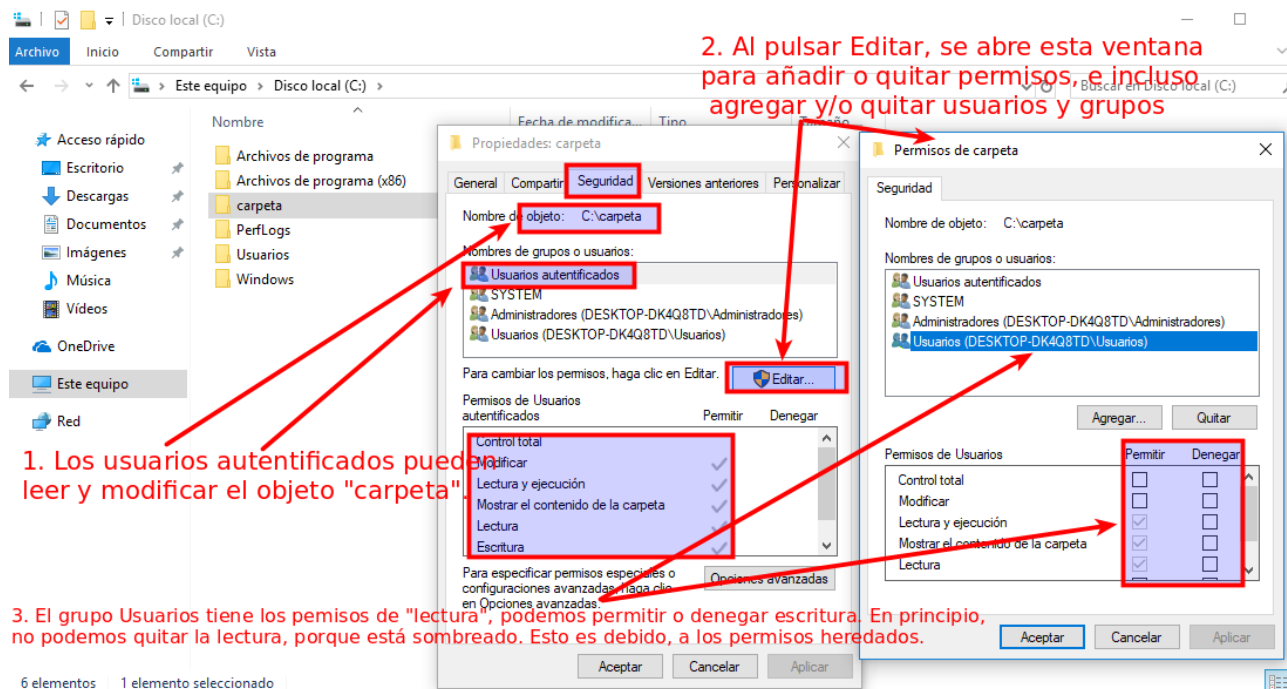
Se queremos control total, concédense todos salvos os permisos especiais. É dicir, ademais de modificar, concédese:

- Control total

Observar que Control total é un permiso moi potente. Se un usuario ten Control total nun cartafol, este usuario poderá eliminar calquera subcarpeta ou arquivo que haxa nese cartafol, mesmo se lle denegamos o permiso de escritura nesa subcarpeta ou arquivo; por tanto hai que ter moito coidado ao conceder este permiso.

Na captura seguinte, móstrase a lapela Seguridade do obxecto cartafol, onde ven os grupos e usuarios que teñen algún permiso. Tamén se visualiza a xanela que se abre ao pulsar Editar.

Ilustración que mostra a lapela Seguridade e a xanela ao pulsar Editar



SolapaSeguridadEditarPermisos (CC BY-NC-SA)

Como calcular os permisos dun obxecto

Cando configuramos permisos, podemos permitir, denegar e non marcar opción. A diferenza entre permitir e denegar, está clara, pero cal é a diferenza de denegar un permiso explicitamente, e non deixar marcado nin permitir nin denegar?

Supoñamos un usuario que pertence a varios grupos. Que permiso ten ese usuario?

2 regras:

Regra 1. Mirarase o permiso que ten o usuario e os grupos aos que pertence, se algún deles ten denegado o permiso, a denegación manda, e o usuario non terá ese permiso.

Regra 2. Se non hai denegación, mirarase os permisos permitidos ao usuario e os seus grupos, o usuario terá o máximo de permisos permitidos.

- Exemplo 1. Supoñamos que Juan pertence aos grupos contabilidade e informática. E que os permisos configurados corresponden a:
 - Juan ten concedida lectura no cartafol apuntes
 - O grupo contabilidade ten denegada a lectura

- O grupo informatica ten permiso escritura no cartafol apuntes
- Cales son os permisos?
- Resposta: o usuario non ten ningún permiso, pois o grupo contabilidade ao que pertence ten denegada a lectura.
- Exemplo 2. Que cambiaría en exemplo 1, se o grupo contabilidade non ten permisos aceptados nin denegados no cartafol apuntes.
 - Cales son os permisos?
 - Resposta: o usuario juan tería permiso escritura. Pois non hai ningunha denegación, polo que se mira o máximo de permisos, juan só ten lectura, pero o seu grupo informatica ten escritura, polo que juan terá permisos de escritura.

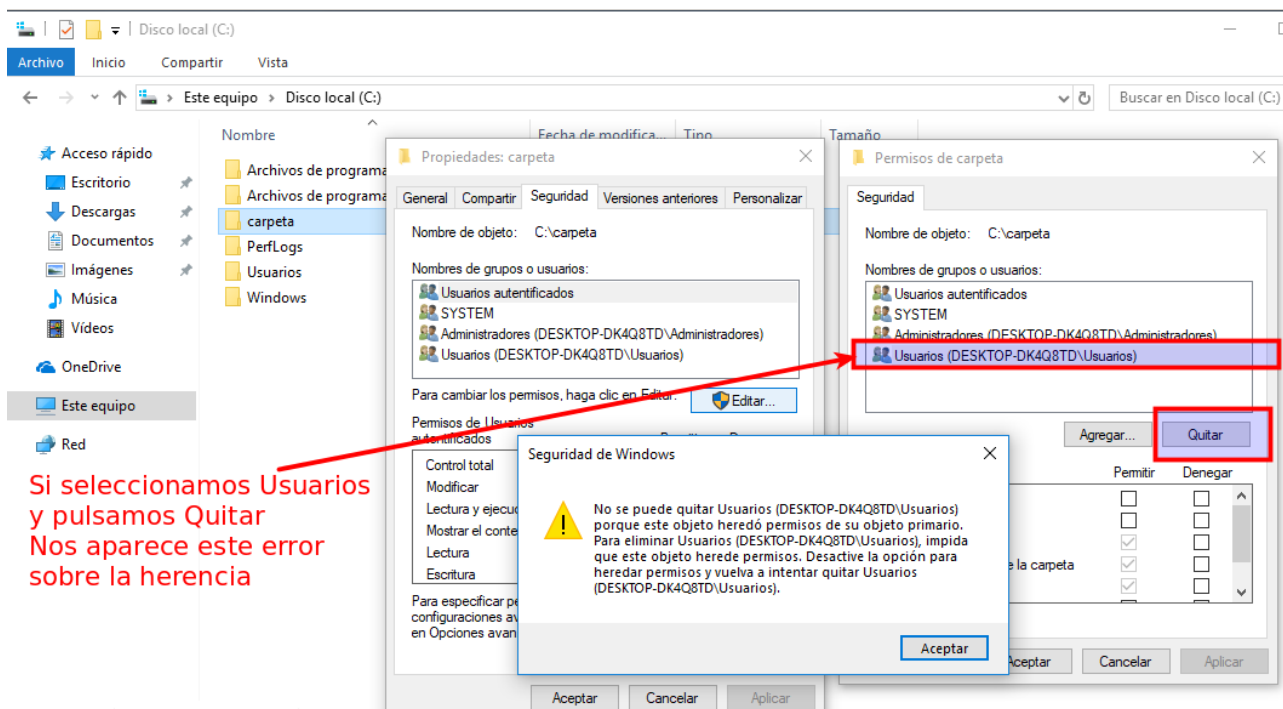
Herdanza

Ao crear un arquivo ou cartafol; créase cos permisos do seu cartafol pai. **Por defecto a herdanza está habilitada.** Por iso, en moitos casos, non podemos quitar usuarios que teñen permisos, ou desmarcar permisos que aparecen sombreados. Nestes casos, teremos que deshabilitar a herdanza.

Na imaxe seguinte, téntase quitar ao grupo **Usuarios**, para que non teñan permisos no obxecto **cartafol**. Ao facelo, sae mensaxe de erro, que nos indica que para podelo quitar, é necesario quitar a herdanza.

Para quitar a herdanza, non se pode realizar no botón Editar, senón en Opcións Avanzadas. Vémolos a continuación.

Ilustración que mostra o erro que aparece por herdanza ao quitar permisos a Usuarios



Miguel Ángel García Lara (CC BY-NC-SA)

4.2.5.3 Botón Opcións avanzadas en lapela Seguridade

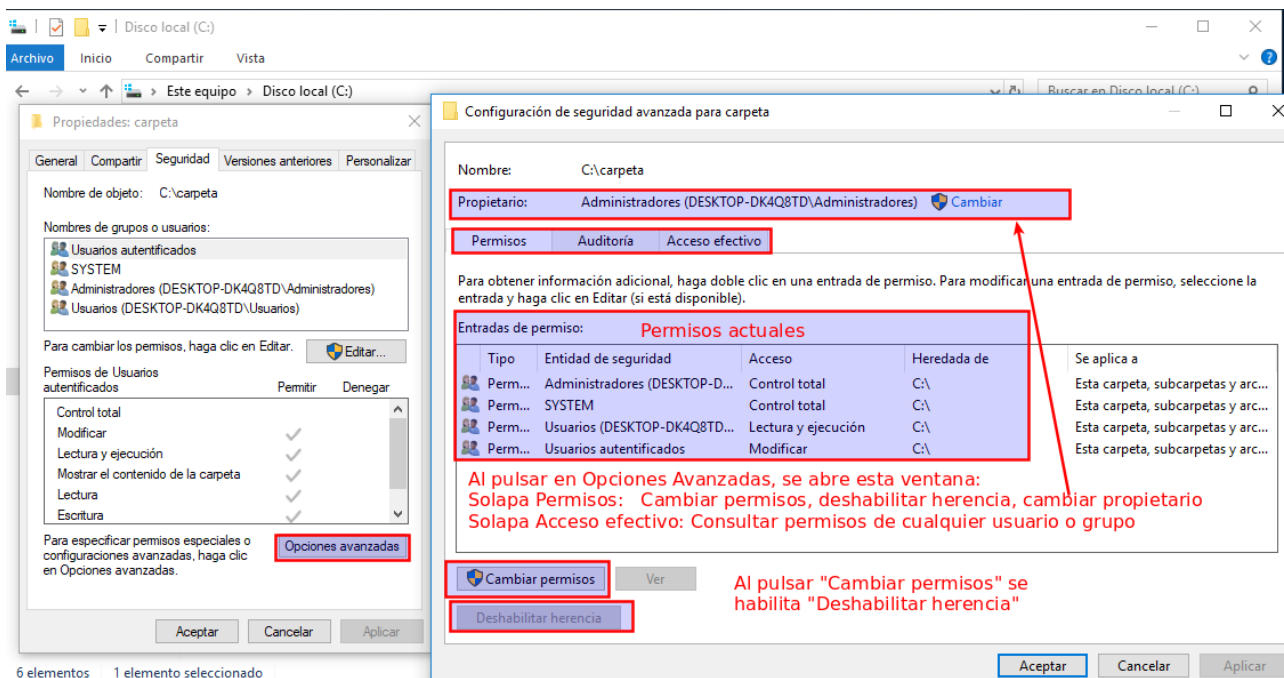
En Opcións Avanzadas da lapela Seguridade podemos:

- Deshabilitar e/ou habilitar a herdanza
- Cambiar os permisos de calquera usuario ou grupo.
- Coñecer e cambiar o propietario do obxecto
- Consultar os permisos efectivos dun obxecto concreto

Ao pulsar **Opcións Avanzadas**, ábrese unha nova xanela con 3 lapelas: **Permisos**, **Auditoría** e **Acceso efectivo**. Na lapela **Permisos** ven todos os permisos actuais no obxecto, é o mellor sitio, para ver dunha ollada os permisos concedidos a cada usuario ou grupo.

Móstrase unha captura da xanela.

Ilustración que muestran as distintas lapelas ao pulsar Opcións Avanzadas

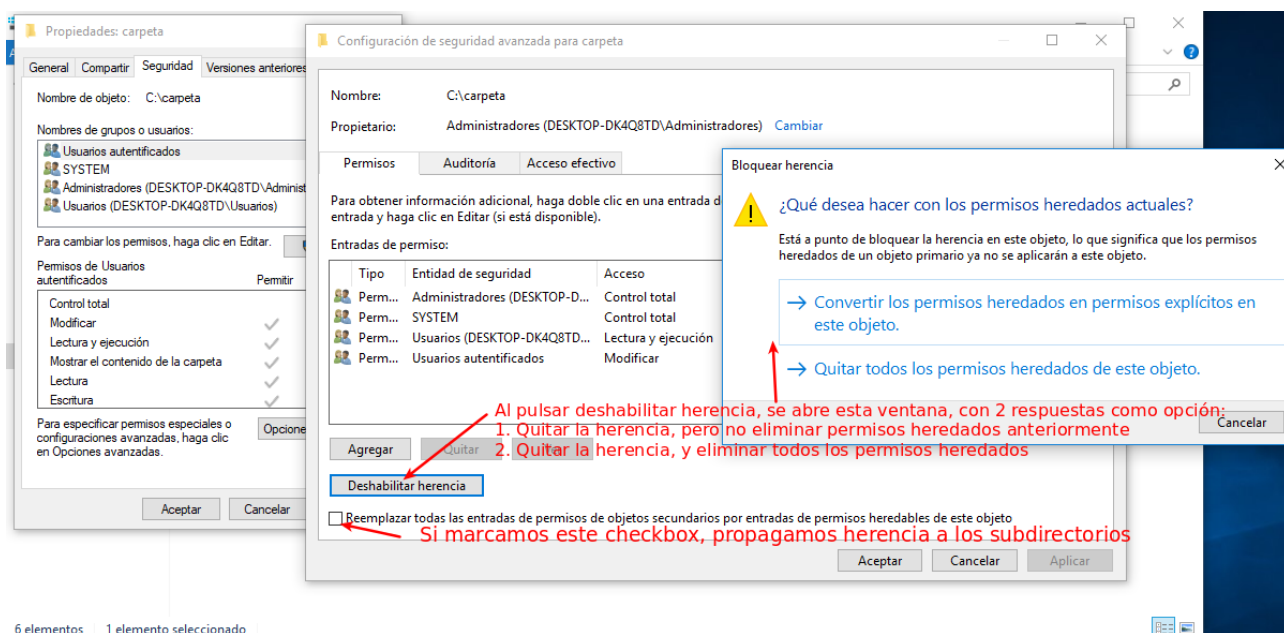


Miguel Ángel García Lara (CC BY-NC-SA)

Quitar a herdanza nun obxecto

Para quitar a herdanza a un obxecto, hai que ir a "Opcións Avanzadas" e pulsar "Cambiar permisos", nese momento, habilítase o botón "Deshabilitar herdanza"

Ilustración que mostra como deshabilitar herdanza



Miguel Ángel García Lara (CC BY-NC-SA)

Se pulsamos “Deshabilitar herdanza”, ábrese a xanela emerxente que se ve na captura anterior. Temos 2 opcións para responder:

- Se respondemos “**Converter os permisos herdados en permisos explícitos**” significa que quitamos a herdanza, pero non eliminamos ningún permiso herdado anterior. En xeral, recoméndase esta opción, pois hai permisos que non debemos modificar, como os permisos concedidos a System, Creator Owner...
- Se respondemos “**Quitar todos os permisos herdados**”, quitamos a herdanza, e eliminamos os permisos herdados ata o de agora nese obxecto.

Permisos especiais

Tamén se poden modificar os permisos pulsando “Opcións avanzadas” na lapela “Seguridade”. Nesta xanela, chámanse permisos especiais, pois son distintos aos permisos estándar vistos antes.

Nesta xanela de Opcións avanzadas, no canto dos 6 permisos estándar, hai 13 permisos especiais. Por exemplo, o permiso estándar de “Lectura”, equivale aos permisos especiais “Ler datos”, “Ler atributos”, “Ler permisos” e “Ler atributos estendidos”.

Por ese motivo, salvo que se teña bastante experiencia, recoméndase administrar os permisos, no botón “Editar” da lapela “Seguridade” pois é máis sinxelo administrar 6 permisos que 13 permisos.

Na seguinte páxina de soporte de Microsoft, móstrase a equivalencia entre permisos especiais e permisos estándar:

<https://technet.microsoft.com/é-é/library/cc732880.aspx>

Para ver que permite cada permiso especial, mirar vínculo:

<https://technet.microsoft.com/é-é/library/cc753992.aspx>

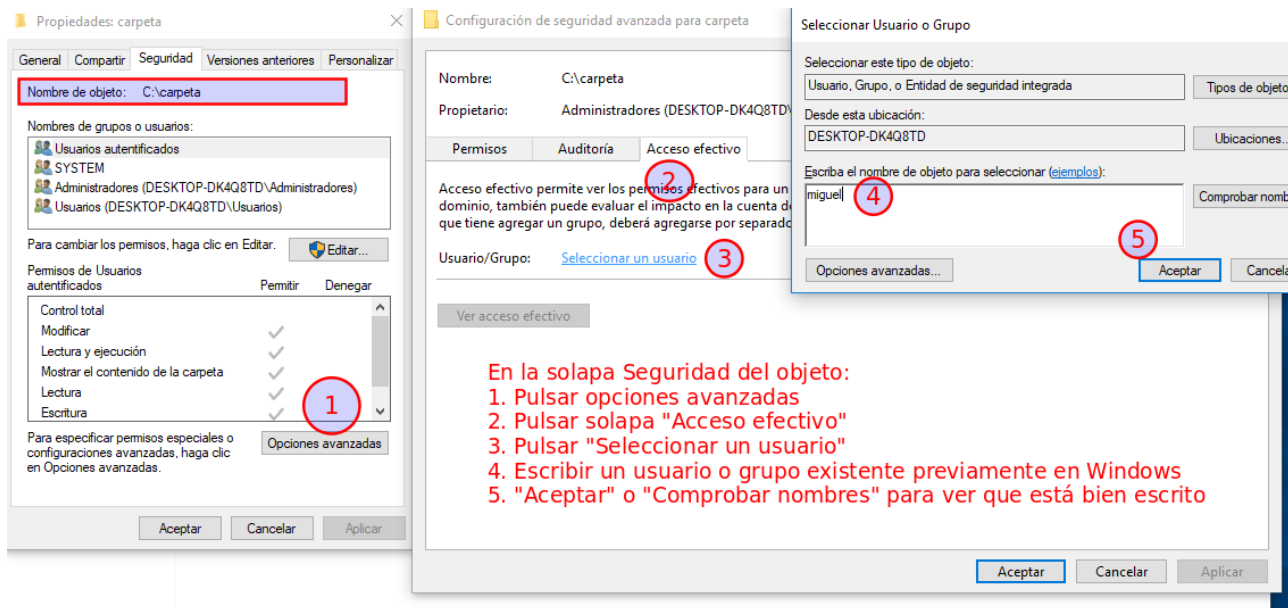
Lapela “Acceso efectivo” en “Opcións avanzadas”

A lapela **Acceso efectivo**, serve para ver os permisos concretos dun usuario ou grupo nun cartafol ou arquivo. Nesta lapela, non se pode cambiar ningún permiso.

A administración de permisos, é moi completa, o que pode dar lugar a algún erro de configuración. De aí, que se incorpora esta lapela, como forma de pescudar que permisos concretos ten un usuario ou grupo. Esta lapela, en anteriores Windows chámase Permisos efectivos.

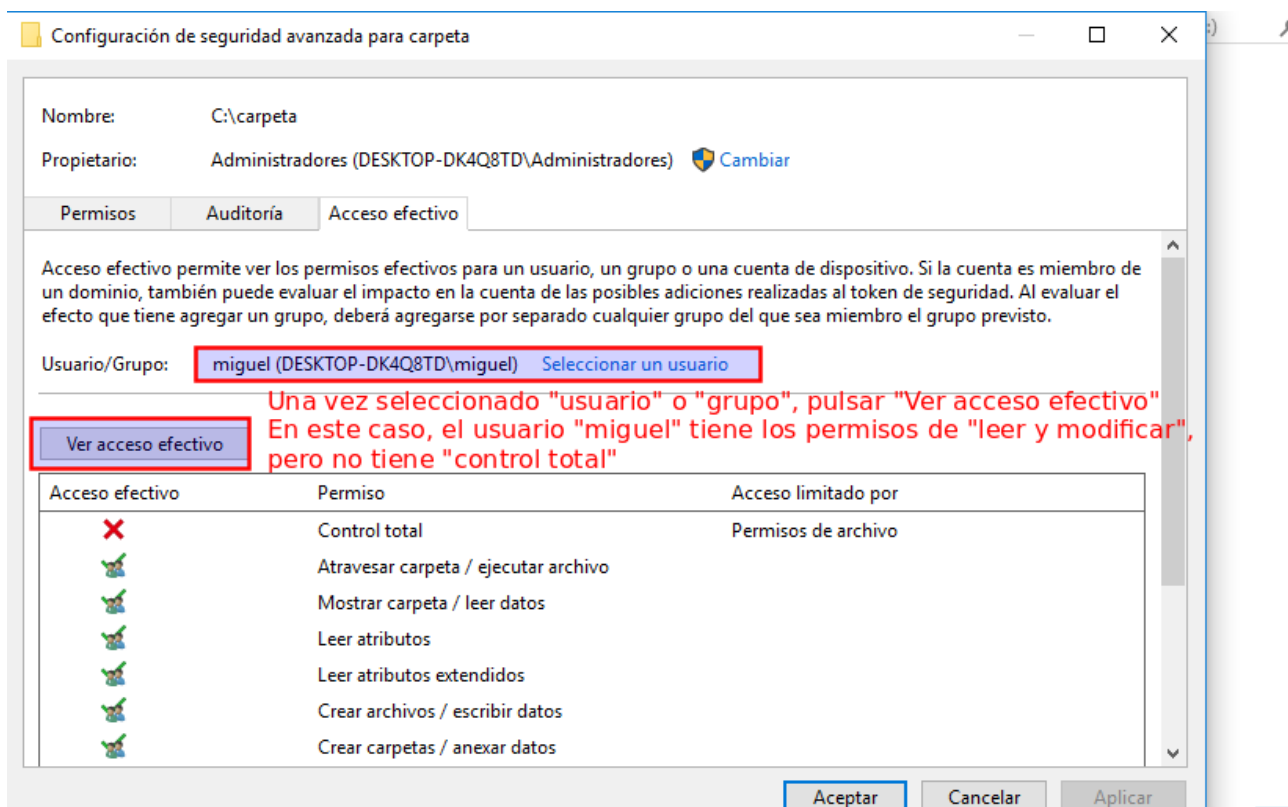
Púlsase en “seleccionar” para buscar un usuario ou grupo, e devólvenos os permisos nese obxecto (cartafol ou ficheiro). Ver as 2 capturas incluídas de como facelo. Basicamente, trátase de entrar na lapela **Acceso efectivo** e seleccionar un usuario ou grupo para buscar os seus permisos.

Ilustración que mostran os permisos efectivos



Miguel Ángel García Lara (CC BY-NC-SA)

Ilustración que muestra Permisos concretos dun usuario



Miguel Ángel García Lara (CC BY-NC-SA)

4.2.5.4 *Recomendacións e exemplo final*

Recomendacións ao administrar permisos

Se non se ten coidado na administración de permisos, é moi fácil obter un caos. Para evitalo, fanse as seguintes recomendacións:

- Evitar no posible denegar permisos.
- Administrar preferiblemente permisos a grupos, que permisos a usuarios.
- Administrar preferiblemente permisos en cartafol, que permisos en arquivos.

É máis fácil administrar permisos de forma global a cartafol e grupos. E trátase de poñer o mínimo de denegacións, normalmente para excluír a alguén ou pequenos grupos. Por exemplo, se queremos que un grupo enteiro poida ler, salvo un usuario do grupo, concedemos a lectura ao grupo e denegamos ao usuario.

Que permisos créanse cando copiamos ou movemos cartafol ou arquivos?

Copiar obxectos en particións NTFS:

Cando copiamos un obxecto, sexa na mesma partición NTFS ou noutra, considérase un obxecto novo, polo que herda os permisos do cartafol de destino.

Mover obxectos en particións NTFS:

Cando movemos un obxecto dentro unha partición NTFS, o obxecto conserva os seus permisos orixinais.

Cando movemos un obxecto entre distintas particións, o obxecto herda os permisos do cartafol de destino.

Talvez axúdecche a comprender por que é así, que se moves un arquivo grande na mesma partición, non se tarda nada, pois non se escribe no disco. Só cámbiase o roteiro do arquivo. Con todo, se o movemos dunha partición a outra, se se tarda bastante, pois realmente hai unha escritura na partición nova.

4.2.6 *Rexistro de Windows. Directivas de grupo e seguridade local*

Sempre desde unha conta con privilexios de administrador Windows 10 proporcionanos a posibilidade de xestionar de forma centralizada a configuración da seguridade do noso sistema, a través das Directivas de seguridade local e as Directivas de grupo local. Ambas as opcións contan con consolas para facilitar a configuración das directivas. Unha directiva é un conxunto de regras de seguridade que se poden implementar nun sistema.

Coas Directivas de seguridade local veremos como aplicar distintas restricións de seguridade sobre as contas de usuario e contrasinais. Doutra banda, as Directivas de grupo local permítennos configurar equipos de forma local ou remota, instalar ou eliminar aplicacións, restrinxir os dereitos dos usuarios, entre outras accións.

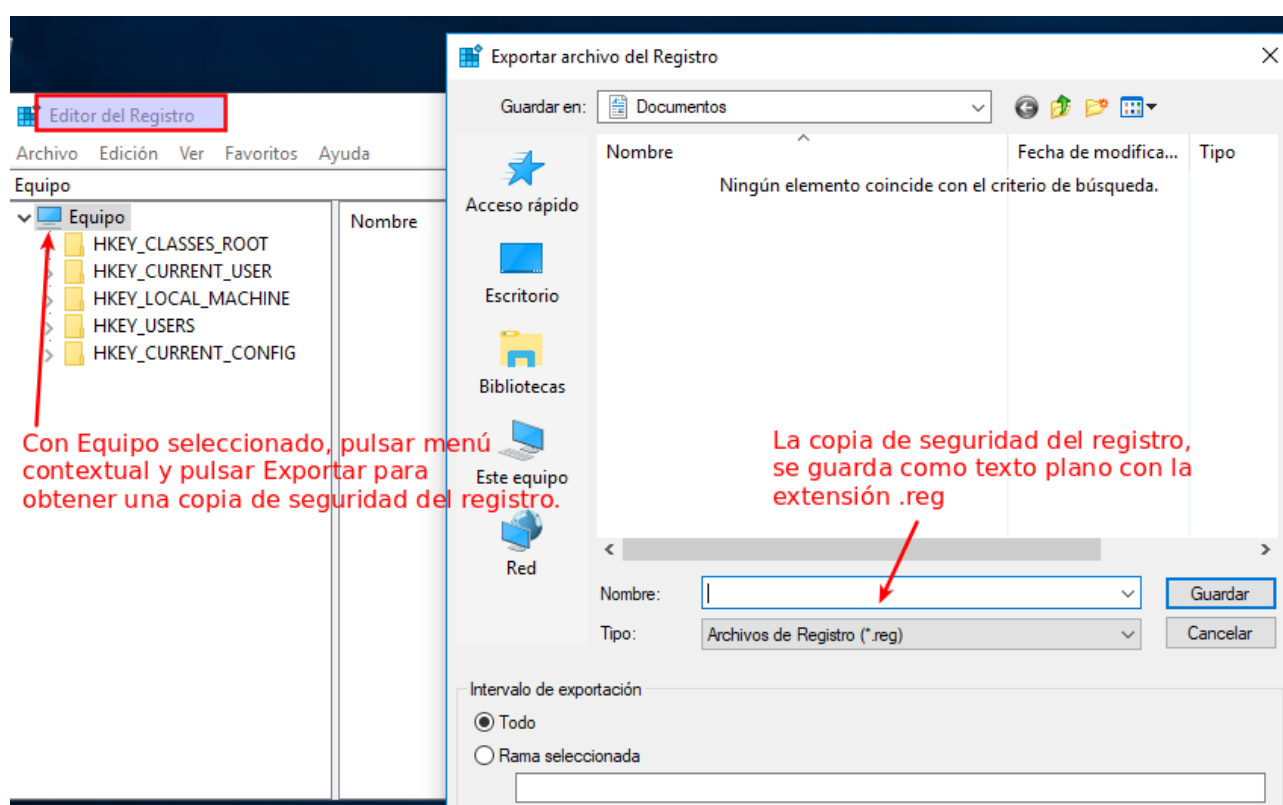
4.2.6.1 Rexistro de Windows

O rexistro de Windows ten todo o historial desde que se instalou o Sistema Operativo. Por exemplo, se instalamos un programa, e a continuación desinstalamos, no rexistro quedan escritas as 2 cousas, aínda que o cartafol de instalación elimínouse. Por iso, cando utilizamos un shareware con 30 días de avaliación, se pasado ese tempo, se desinstala e vólvese a instalar, o Sistema Operativo informa que xa se instalou ese software anteriormente.

O rexistro de Windows, faise cada vez máis grande, e é o principal motivo de que o computador cada vez tarde máis en arrincar.

O rexistro de Windows, non se debe tocar, salvo que saibamos o que facemos. Pero ás veces, prodúcense situacións nas que é necesario modificar o rexistro.

Ilustración que mostra xanela do editor de rexistro, e impórtase copia



Miguel Ángel García Lara (CC BY-NC-SA)

Aquí móstranse algunhas situacións de porque pode ser necesario tocar o rexistro:

Ás veces ocorre, que un programa instálase e polo que sexa non acaba de instalarse. É posible, que se entre nun bucle, porque o programa non se deixa instalar porque xa se instalou, e tampouco se poida desinstalar, porque di que xa está instalado.

Moitos virus, tocan valores no rexistro. Pode ocorrer que aínda que eliminemos o virus ou software espía, o rexistro non volva ao seu valor orixinal.

Execución do editor de rexistro e copia de seguridade

O rexistro édítase de forma manual co programa **regedit**. Temos varios cartafoles, onde en cada unha delas hai moitas claves, cada un cun valor.

Antes de modificar un valor do rexistro, é **moi importante realizar unha copia de seguridade** do rexistro.

Para iso, despois de escribir regedit, ábrese o “Editor de rexistro”, e comprobando que está seleccionado o total do equipo e non una dos 5 cartafoles, seleccionamos **Arquivo / Exportar**. Esta utilidade, obterá un ficheiro de texto, extensión reg, con todo o contido do rexistro.

Desa forma, en caso de cometer algún **erro grave ao cambiar valores no rexistro**, temos a copia de seguridade, e utilizaríamos o menú Arquivo / Importar

Limpadores de rexistro

Existen varios limpadores de rexistro, máis amigables que o editor de rexistro de Windows, cuxo fin é borrar todas as entradas innecesarias e tentar corrixir posibles valores erróneos.

Exemplo de limpadores de rexistro son: RegClean, CCleaner, Regseeker. A maioría destes programas é software privativo.

Exemplo concreto: Regseeker (freeware)

A versión actual é a versión 4.7. Pódese baixar desde a súa páxina oficial:

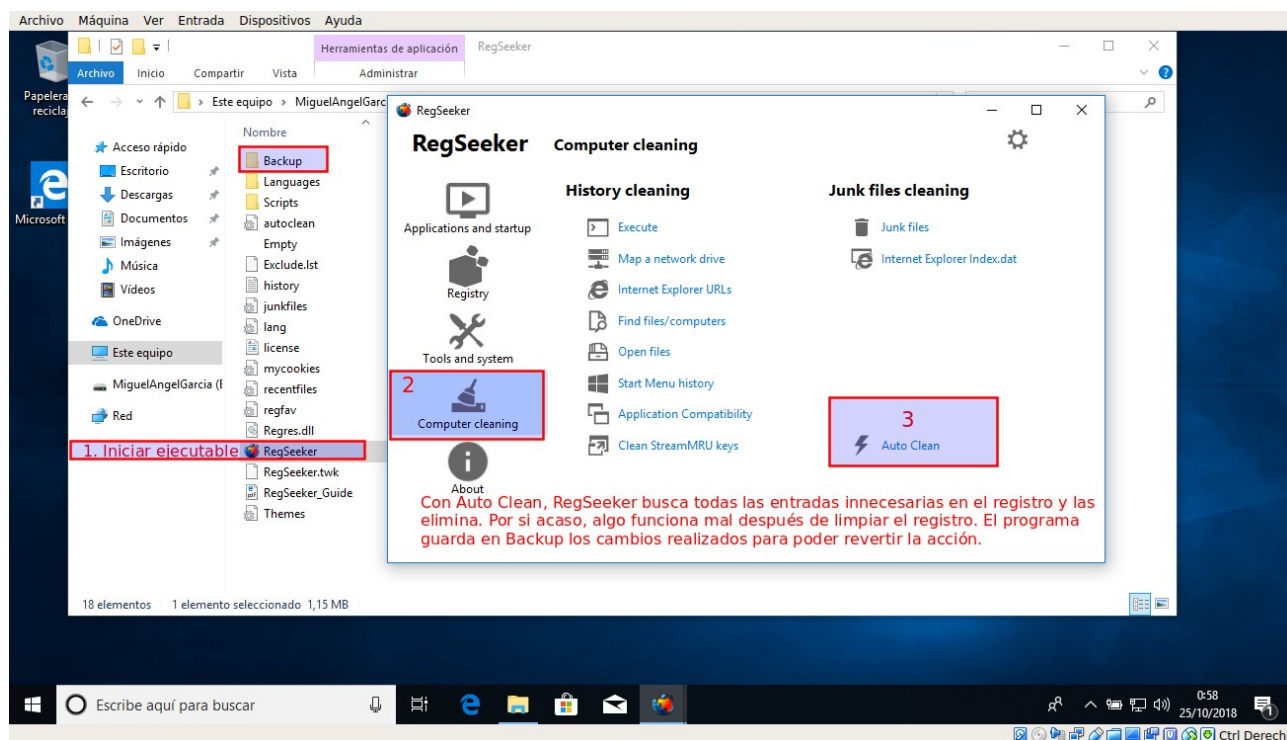
<http://www.hoverdesk.net/download.php>

Se baixa en versión portable nun arquivo .zip, o que significa, que unha vez descomprimido non fai falta realizar instalación. Arríncase co executable e é moi fácil de utilizar. Tan simple que se pode realizar unha limpeza de forma automática co botón Auto Clean.

RegSeeker comprobará as entradas erróneas ou entradas innecesarias, e corríxeas. Mesmo, se se limpa varias veces, séguense eliminando entradas.

Outro uso importante de Regseeker, é desinstalar aplicacións. Hai moitas pequenas aplicacións, que non teñen opción de desinstalar no seu propio menú, igualmente non se poden eliminar desde “Agregar ou quitar programas”, e con todo se poden desinstalarse desde a opción de Aplicacións instaladas de Regseeker.

Ilustración de RegSeeker e se ejecuta AutoClean



Miguel Ángel García Lara (CC BY-NC-SA)

4.2.6.2 Directivas de grupo ou política local

Para abrir nun equipo Windows o editor de directivas de grupo local, execútase o programa gpedit.msc como administrador.

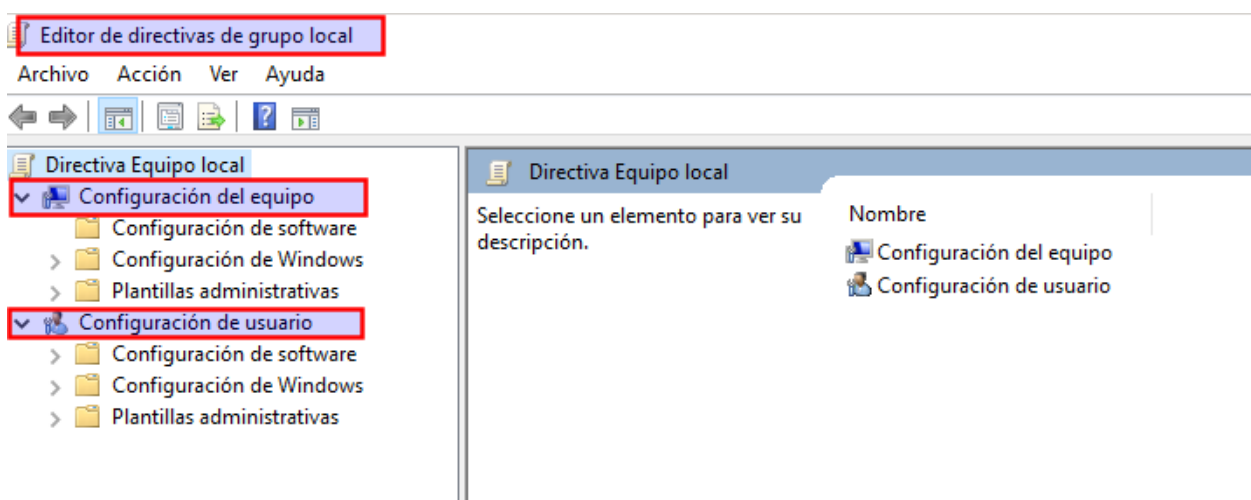
Usando as “directivas de grupo local” nunha maquina Windows, podemos:

- Modificar políticas ou directivas como deshabilitar o Administrador de equipos, deshabilitar a configuración da rede, obrigar a un fondo de escritorio...
- Asignar arquivos executables ou scripts que se executasen automaticamente cando o sistema acéndase, apáguese, inicie sesión un usuario ou peche sesión.
- Especificar opcións especiais de seguridade.

Ao modificar as directivas locais, o que estamos a realizar é modificar o rexistro, pero dunha forma máis amigable que utilizando o editor de rexistro. É bastante máis simple utilizar gpedit.msc, que regedit. No editor de políticas locais, explícase o significado de cada directiva.

Se estamos a traballar nunha rede Windows baixo un dominio (cun Windows Server administrando devandito dominio) as políticas de grupo cobran maior protagonismo. Pero nun ambiente de rede de grupo de traballo (sen Windows Server), as políticas de grupo son locais, é dicir controlan só os aspectos da propia máquina.

Ilustración que mostra editor de directivas, con 2 configuracións principais: equipo e usuario



Miguel Ángel García Lara (CC BY-NC-SA)

Dentro das **directivas de grupo locais** hai dúas **opcións**: **Configuración do equipo** e **Configuración do usuario**. No caso de directivas locais é practicamente indistinto traballar cunha opción ou outra.

Algunhas directivas aparecen tanto na configuración do equipo como na configuración do usuario. En caso de conflito, a configuración do equipo sempre ten preferencia.

Respecto a a configuración, cada directiva ten 3 posibles valores:

- Non configurar a directiva, co que se comportará segundo o criterio por defecto para dicha directiva.
- Habilitala, co que a poñeremos en marcha no sistema.
- Deshabilitarla, co que impediremos que se poña en marcha dita directiva.

Para modificar a configuración dunha directiva, simplemente temos que realizar dobre clic sobre dicha directiva para que nos apareza o cadro de dialogo que nos permite modificar dicha directiva. No devandito cadro de dialogo mostraranos unha explicación da funcionalidade de dicha directiva.

4.2.6.3 *Directivas de seguridade local*

Coas Directivas de seguridade local aplícanse distintas restricións de seguridade sobre as contas de usuario e contrasinais.

Hai 3 formas de chegar ás Directivas de seguridade local:

- Executando **SecPol.msc**
- Abrir directamente **Directiva de seguridade local**

- Forman parte das directivas de grupo, polo que tamén hai acceso desde **gpedit.msc**

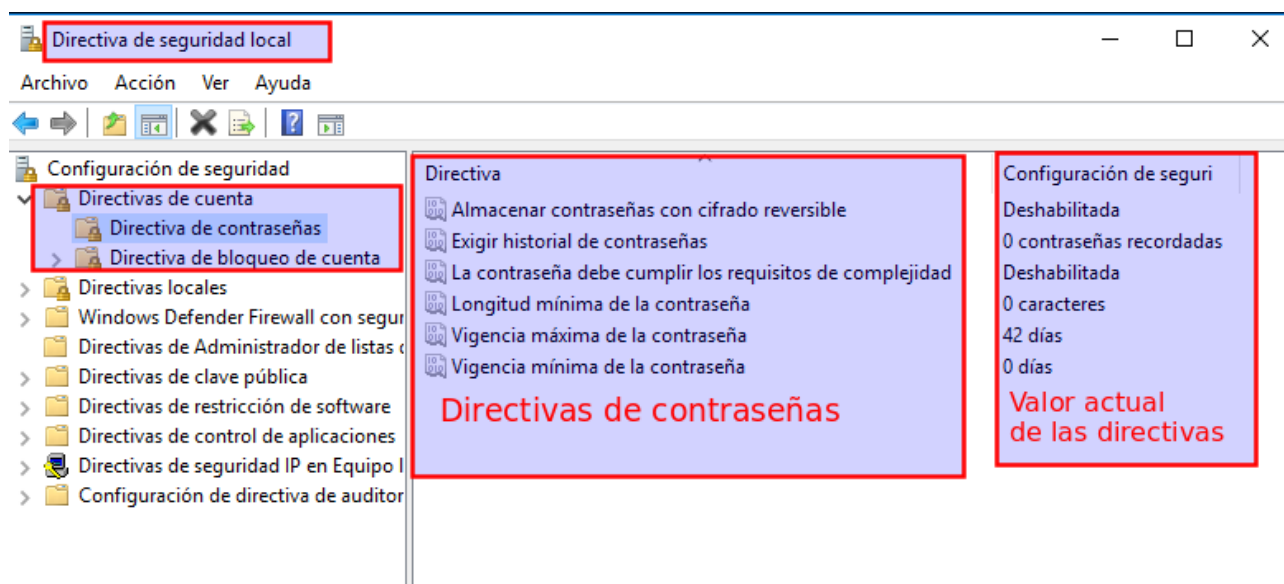
En gpedit.msc, habería que ir a Configuración de equipo / Configuración de Windows / Configuración de seguridade / Directiva de seguridade / Directivas de conta

Nas Directivas de conta, hai 2 tipos de directivas: **Directivas de contrasinal** e **Directivas de bloqueo de contas**

Directivas de contrasinal

Unha vez aberto SecPol.msc, para ver as directivas de contrasinal, facemos clic en Directivas de Conta - **Directivas de Contrasinais**

Ilustración que mostran as directivas de contrasinal en xanela directivas de seguridade



Miguel Ángel García Lara (CC BY-NC-SA)

As **configuracións** máis útiles que podemos xestionar desde aquí son:

- **Esixir o historial de contrasinais.** Impide que un usuario cambie o seu contrasinal por un contrasinal que usase anteriormente. Por defecto aparece configurado a 0. Se queremos que non se poidan repetir as últimas 3 contrasinais, cambiaríamos o 0 a 3 pulsando o menú contextual en “Esixir o historial de contrasinais”.
- **Os contrasinais deben cumprir os requirimentos de complexidade.** Obriga a que os contrasinais deban cumprir certos requirimentos, como son mesturar letras maiúsculas, minúsculas e números, non parecerse ao nome da conta, etc.

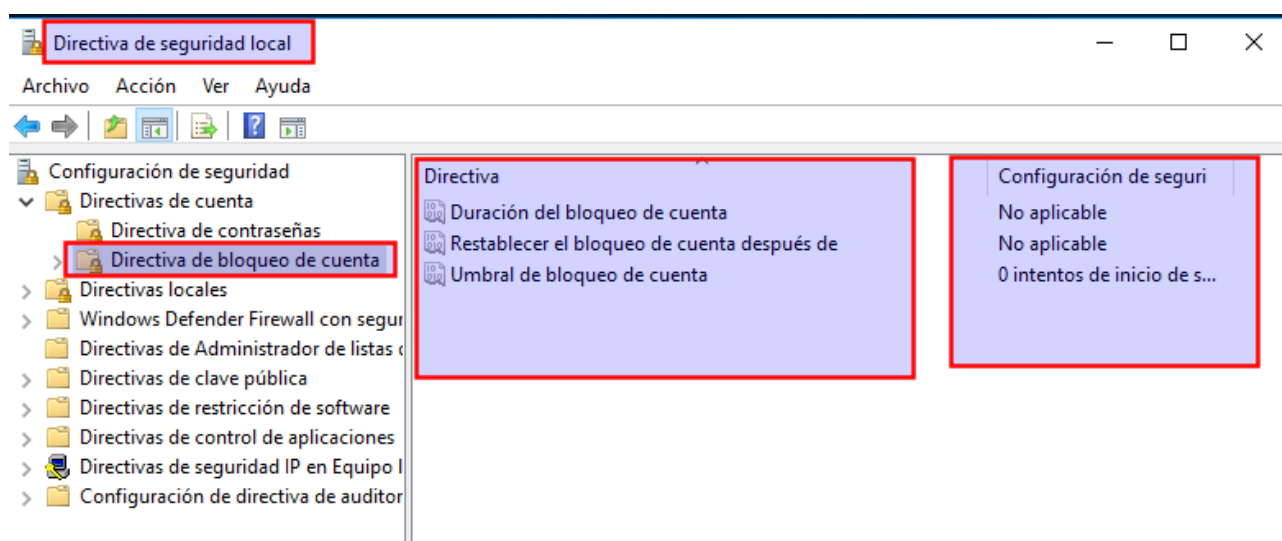
- **Lonxitude mínima do contrasinal.** Indica cuantos caracteres debe ter o contrasinal como mínimo, un valor cero neste campo indica que poden deixarse os contrasinais en branco.
- **Vixencia máxima do contrasinal.** Os contrasinais dos usuarios caducan e deixan de ser validas despois do número de días indicados nesta configuración, e o sistema obrigará ao usuario para cambialas. (Lembremos que ao crear unha conta de usuario podemos indicar que o contrasinal nunca caduco para esa conta).
- **Vixencia mínima do contrasinal.** Indica canto tempo debe transcorrer desde que un usuario cámbiase o contrasinal, ata que pode volver cambiala. Esta configuración de seguridade local úsase para evitar que un usuario cambie continuamente o seu contrasinal a fin de volver quedar co seu contrasinal orixinal caducado.

Directiva de bloqueo das contas

Podemos bloquear as contas se se usan contrasinais incorrectos.

Unha vez aberto SecPol.msc, para ver as directivas de bloqueo de contas, facemos clic en Directivas **de Conta – Bloqueo de contas**

Ilustración que mostran as directivas de limiar de bloqueo en xanela directivas de seguridade



Miguel Ángel García Lara (CC BY-NC-SA)

Aquí podemos configurar:

- **Duración do bloqueo de conta.** Durante canto tempo permanecerá unha conta bloqueada se se supera o limiar de bloqueo. Un valor cero indica que a conta se bloqueará ata que un Administrador desbloqueea.

- **Restablecer o bloqueo de conta despois de.** Indica cada canto tempo ponse o contador de intentos erróneos a cero.
- **Limiar de bloqueo da conta.** Indica cuantos intentos erróneos permítense antes de bloquear a conta.

4.2.6.4 *Ferramentas do sistema. Ferramentas administrativas*

A primeira vista, o aspecto de Windows cambia bastante entre as distintas versións de Windows: Windows 7, Windows 8 e Windows 10. Pero, as diferenzas están principalmente en como chegar ás distintas ferramentas ou programas integrados. Pois, as distintas ferramentas vistas neste tema e as que quedan utilízanse da mesma forma, en xeral existen tanto en Windows 7, 8 e 10, como nas distintas versións de Windows Server.

No **menú contextual de Equipo**, temos acceso a Propiedades e **Administrar**.

Tamén son importantes **Panel de Control** e **Configuración**.

Ao desaparecer o típico Inicio / Programas en Windows 7, en Windows 8 e Windows 10, gañan moito peso 2 formas de chegar a bastantes ferramentas:

- **Tecla Windows + R** abre executar, onde podemos escribir calquera nome de programa.
- Pulsando o **menú contextual en Inicio**, tense acceso a bastantes ferramentas de Windows. Móstrase captura.

A continuación imos ver ferramentas para administrar Windows: tarefas programadas, desfragmentador, cotas de disco, recuperar o sistema, reinstalación Windows 10, etc.

4.2.6.4.1 *Cotas de disco*

A ferramenta cota de discos consiste en limitar o espazo que ten cada usuario para gardar os seus datos.

Pódense habilitar cotas de disco ao ter acceso ás propiedades do volume de disco no Explorador de Windows ou mediante o obxecto de directiva de grupo. Vexamos cada un destes métodos:

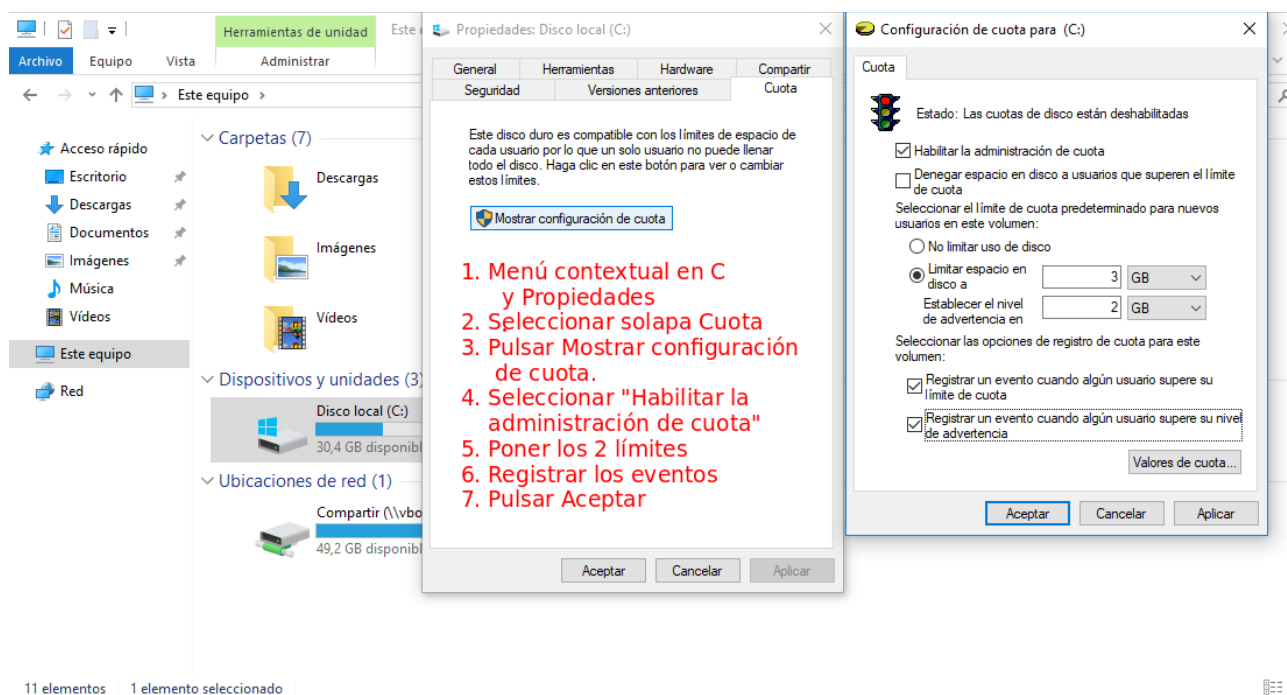
A través do Explorador de Windows:

- No explorador de Windows, seleccionar Propiedades no menú contextual da unidade que se desexen habilitar cotas de disco.
- Seleccionar lapela cota, e facer clic en “Mostrar a configuración de cota”.
- Ábrese unha nova xanela, onde pulsamos a casa “Habilitar a administración de disco” e enchamos os 2 límites de espazo:
- “Limitar espazo en disco a ...” é o límite que non se poderá superar.
- “Establecer o nivel de advertencia en ...” avisarase cunha mensaxe ao usuario, de que se achega ao seu límite de espazo.

- Pódese marcar as casas para rexistrar os eventos relacionados coas cotas de disco. Pulsar Aceptar.

En a seguinte imaxe, establécense cotas na unidade C, con límites de 2GB como advertencia e 3GB que non se pode exceder.

Ilustración que establece unha cota na unidade C, de 3GB por usuario, con nivel de advertencia a 2GB.



Miguel Ángel García Lara (CC BY-NC-SA)

A través de directivas de grupo:

Nas Directivas de equipo local, expande Configuración do equipo, expande Persoais administrativos , expanda sistema e, a continuación, feixe dobre clic en Cotas de disco.

A diferenza para realizalo en directivas de grupo, é que as cotas que se establezan é a suma do admitido entre todas as unidades do PC.

4.2.6.4.2 Desfragmentar e Comprobar unidade

Desfragmentar e optimizar unidades

Con anterioridade habemos visto que os arquivos gárdanse en unidades de asignación ou agrupación industrial non contiguos. Se os arquivos están demasiado torar, redúcese o rendemento da partición, como vimos porque o cabezal do disco ríxido ten que saltar moitas veces de pista e/ou superficie. A función de "desfragmentar **unidade**", é axudar a que as **unidades de asignación dun arquivo queden contiguas**, aumentando o rendemento.

É moi recomendable desfragmentar o disco ríxido cando notes que o rendemento do disco ríxido estea a decaer, é dicir, que o sistema operativo tarde moito en atopar a información no disco ríxido porque esta atópase moi dispersa.

Sinalar tamén, que o desfragmentador, non vai gañar espazo no disco ríxido, é dicir, o espazo perdido nas agrupacións industriais ou unidades de asignación, por ser máis pequeno o anaco de arquivo que a agrupación industrial. Para explicalo doutra forma, o que realiza "desfragmentar unidade" é compactar o arquivo, nunca recuperar espazo.

Se acede executando directamente **Desfragmentar e optimizar unidades**, ou con menú Propiedades na unidade e lapela Ferramentas. Por defecto, execútase segundo unha programación semanal, pero pódese executar en calquera momento.

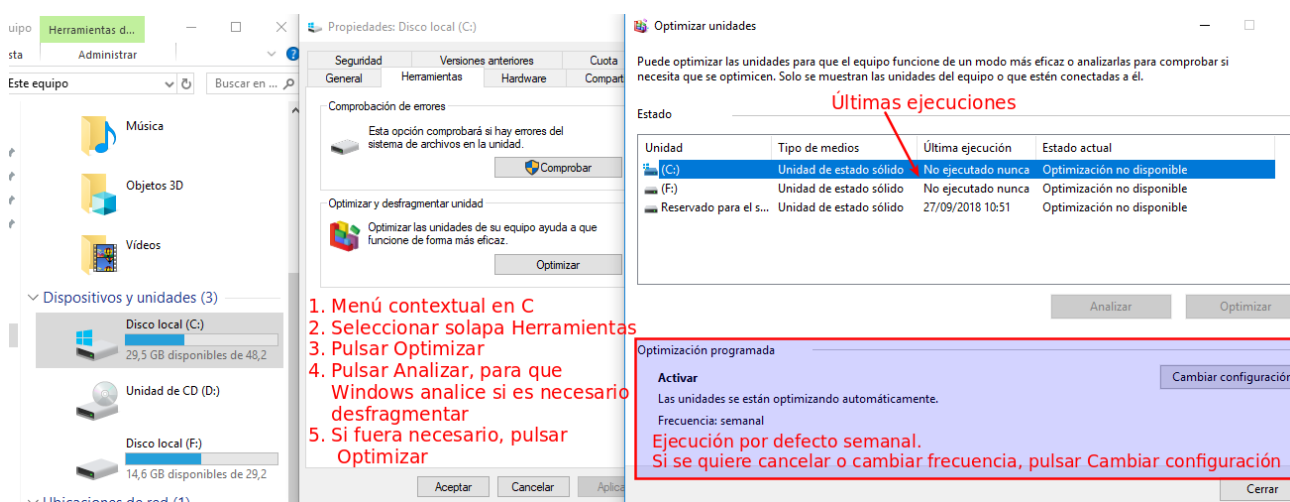
Cambiou lixeiramente o nome con respecto aos anteriores Windows, onde se chamaba "desfragmentador de disco" por "desfragmentador de unidade", sendo máis correcto este último porque se desfragmenta unha unidade lóxica..

Tamén se pode executar na terminal co programa:

defrag [unidade:]

Así mesmo, as unidades SSD non se deben desfragmentar, pois debido ás súas características están optimizados tanto para lectura secuencial como aleatoria. Mesmo, pódese dicir que é prexudicial, polo número de escrituras en SSD que é moi alto, pero limitado. Neste caso, pulsando Cambiar configuración pódese anular a Execución programada.

Ilustración que mostra o desfragmentador



Miguel Ángel García Lara (CC BY-NC-SA)

Comprobar erros

Observar, que na mesma lapela Ferramenta, temos a opción “Comprobar erros” que corresponde á forma gráfica de executar chkdsk /F [unidade:] que vimos nos comandos da unidade 3.

4.2.6.4.3 Programador de tarefas

O Programador de tarefas permite programar a execución automática de aplicacións ou outras tarefas.

Poderemos programar para que calquera utilidade executésemos semanalmente, ao acender o computador, ao apagalo. Así mesmo, poderase executar periodicamente calquera arquivo por lotes.

Accédese ao **Programador de tarefas** desde **Administración de equipos**.

Para utilizalo é necesario iniciar sesión como administrador. Se non se iniciou sesión como administrador, só se poden cambiar as configuracións que se apliquen á súa conta de usuario.

4.2.6.4.4 Protección do sistema. Puntos de restauración

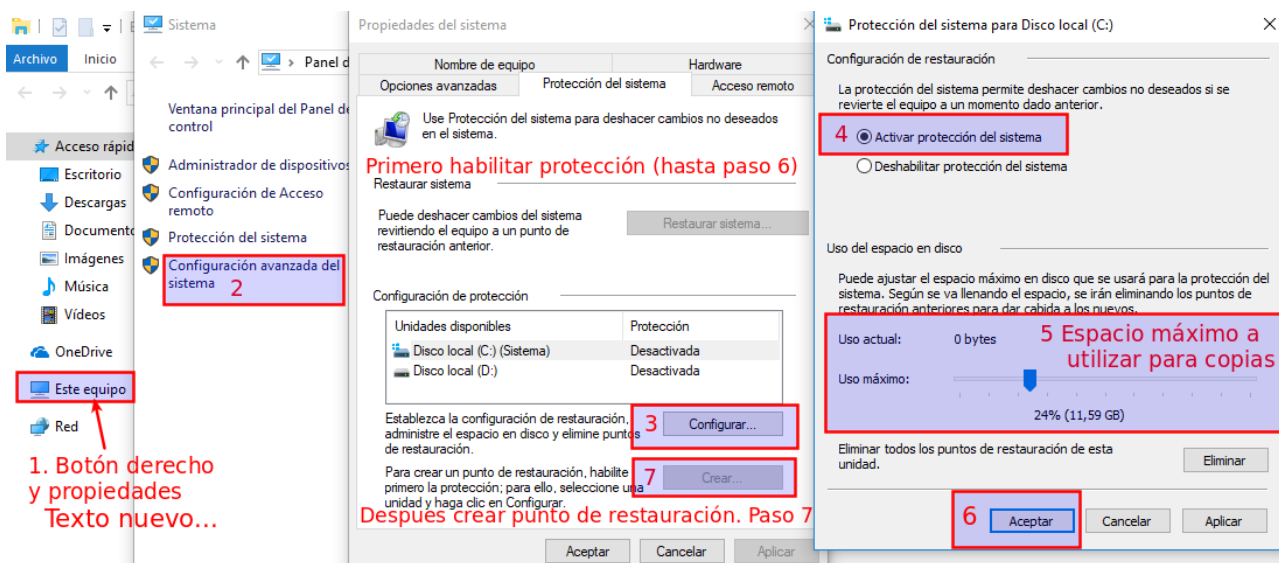
En ocasións, o noso sistema pode volveirse inestable ou mesmo deixar de funcionar totalmente. Isto pode deberse a numerosas causas, tales como un controlador mal deseñado, un programa malintencionado ou mal programado, un erro do usuario, unha corrupción do rexistro, etc. Nestes casos, unha axuda fundamental é a capacidade de Windows de Restaurar o sistema a un punto anterior, o que eliminará automaticamente todos os cambios que realizásemos no noso equipo desde o momento en que se creou devandito punto de restauración.

Por defecto vén deshabilitado Protección do Sistema, pois ao crear puntos de restauración ocúpase disco ríxido.

Pasos para habilitar a protección e crear un punto de restauración en Windows 10:

- Abrir Propiedades en Equipo
- Seleccionar a pestana Protección do sistema da xanela Propiedades do sistema.
- De momento, está deshabilitada a protección, polo que o botón Crear atópase deshabilitado. Para habilitala, pulsar Configurar e ábrenos unha nova xanela.
- Seleccionar Activar protección do sistema.
- Seleccionar espazo máximo a ocupar polos puntos de restauración.
- Pulsar en Aceptar. Xa está habilitada a protección. Péchase esta xanela.
- Agora, o botón Crear que estaba deshabilitado no paso 3, xa está habilitado. Pulsamos Crear para crear o punto de restauración.
- Insérese un nome ao momento de restauración e Crear.

Ilustración que muestra como habilitar a protección, para crear punto de restauración



Miguel Ángel García Lara (CC BY-NC-SA)

Para verificar que o punto se ha creado correctamente, facer clic no botón **Restaurar sistema**, logo seleccionar **Elixir outro punto de restauración** e o punto creado mostrase na lista de puntos existentes.

Cada punto de restauración de sistema que cremos, consome un espazo en disco. Cada certo tempo, Windows crea automaticamente os seus propios puntos de restauración, e tamén son creados automaticamente cando instalamos novo software ou controladores, sempre que estes sexan considerados importantes polo sistema.

O total do espazo en disco que poden ocupar entre todos os puntos restauración, pódese reaxustar en Configurar.

Cando se crea un punto de restauración, e non existe espazo suficiente, Windows elimina o punto de restauración máis antigo que atope.

4.2.6.4.5 Configuración. Actualización e seguridade

Menú Actualización e Seguridade

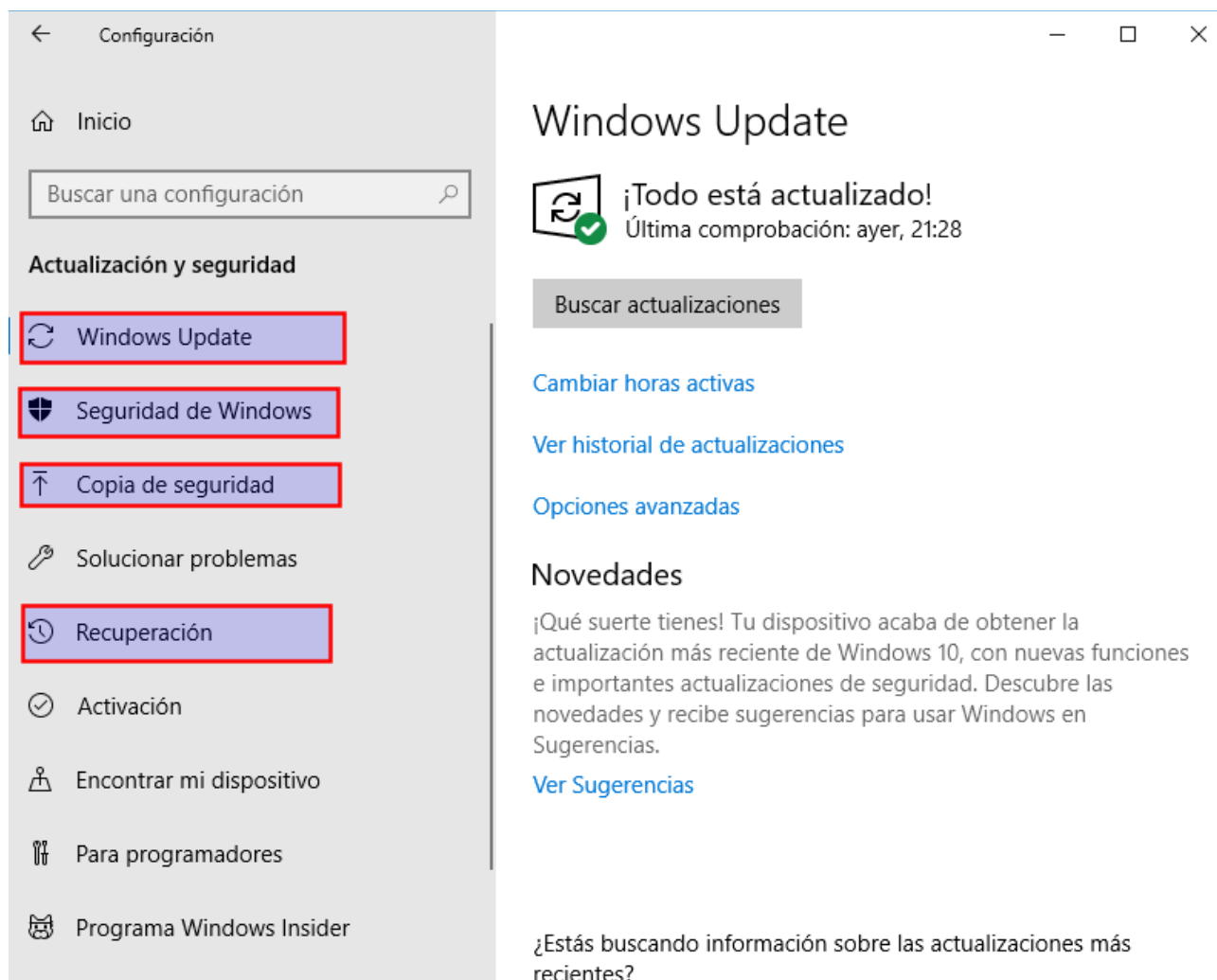
O programa Actualización e Seguridade, ábrese executando **Configuración** e seleccionando na xanela que se abre, abaixo, **Actualización e Seguridade**.

Nesta utilidade, centralizáronse en Windows 10 algunhas ferramentas importantes:

- Windows Update: acceso ás actualizaci3ns de Windows
- Seguridade de Windows: acceso á configuraci3n de Windows Defender
- Copias de seguridade: para crear copias de seguridade de cartafoles como da instalaci3n de Windows. Na unidade 7 falaremos desta utilidade.
- Recuperaci3n: Posibilidade para reinstalar Windows 10

Vexamos algunhas delas.

Ilustración que mostra xanela de "Actualización e seguridade"



Miguel Ángel García Lara (CC BY-NC-SA)

Windows Update

Windows Update é o servizo que se encarga das actualizacións automáticas de Windows. En Windows 7 e Windows 8, tamén se chama Windows Update, pero cambiou a forma de configuralo en Windows 10.

- Se pulsamos **Buscar actualizaciones** o sistema buscará neste momento as actualizacións publicadas.
- Se pulsamos **Cambiar horas activas**, son as horas nas que o sistema non se reiniciará por actualizacións. Pódese configurar ata un máximo de 18 horas ao día.

- Se pulsamos Opcións avanzadas, pódense desactivar as actualizacións automáticas de Windows. Microsoft habilitou en Windows 10 un máximo de tempo sen actualizar, no caso da versión Windows 10 Profesional o máximo é de 35 días.

É moi importante ter un equipo actualizado, pois os parches que se obteñen en Windows Update, moitas veces son parches de seguridade para reparar posibles buracos de seguridade atopados por Microsoft no Sistema Operativo.

Independentemente da configuración do propio servizo Windows Update, como servizo que é, pódese deshabilitar. Para iso, en "Administración de Equipos" ir a "Servizos". Buscar o servizo "Windows Update" e no seu menú contextual seleccionar propiedades. Na nova xanela, en "Tipo de inicio", pulsar Deshabilitar. Desta forma, o servizo queda deshabilitado, de forma que ao iniciar o equipo non se actualizaría nunca. Isto, en xeral non é recomendable, pero hai situacións nas que é útil.

Por exemplo, nas máquinas virtuais, pódese perder moito tempo polas actualizacións de Windows. Outro exemplo, sería en computadores de aeroportos, hoteis, cibercafés, onde os computadores inician sempre igual, (dise que están conxelados), non ten sentido que se actualicen, pois cando se reinicie perderanse e volverase a perder tempo.

Seguridade de Windows. Windows Defender

En Windows 10, inclúese **Windows Defender** como centro de seguridade de Windows. Inclúe un **antivirus e o firewall de Windows (devasa)**. Polo que é elección do usuario, utilizar Windows Defender ou calquera outro antivirus do mercado.

Ata o de agora, a instalación de Windows non incluía antivirus. Ata Windows 7, incluíase Windows Defender como programa antiespía (antispysware). Tamén se incluía o **firewall de Windows**. Pero como antivirus, había que instalar Microsoft Security Essentials ofrecido gratuitamente por Microsoft, ou calquera outro antivirus do mercado. Windows Defender en Windows 10, é a unión de todos estes programas.

Por suposto, o usuario pode preferir utilizar outro antivirus distinto a Windows Defender. Se é importante coñecer, que se se instala outro antivirus, debemos desactivar o antivirus de Defender, pois adoita crear conflitos ter 2 antivirus no mesmo equipo.

Para que un computador estea protexido, é moi recomendable ter un antivirus, complementado cun software antimalware.

Reinstalación de Windows. Xanela Recuperación

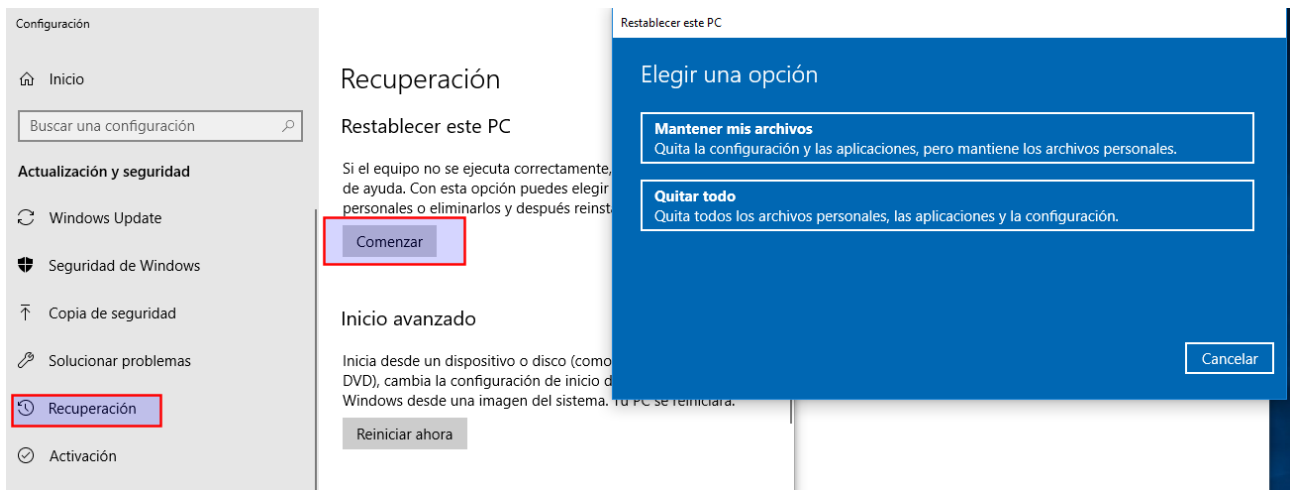
En Windows 10, incorporouse por primeira vez, unha ferramenta que permite reinstalar Windows 10 sen necesidade de utilizar ningún CD ou arquivo iso. Mesmo se pode reinstalar Windows 10, salvando os ficheiros do usuario. Para iso, hai que abrir o programa Recuperación.

Temos 2 formas de abri-lo:

- Execútase Configuración / Actualización e Seguridade / Recuperación

- Abrir Panel de Control / Recuperación. Ábrese unha xanela con acceso a Recuperación Avanzada. Temos que pulsar abaixo, onde pon “Se tes problemas co equipo, ve a Configuración e proba a restablecela”

Ilustración que mostra a pantalla de recuperación, púlsase Comezar para reinstalar Windows



Miguel Ángel García Lara (CC BY-NC-SA)

Unha vez aberta a xanela, púlsase Comezar para restablecer o PC. Ábrese unha nova xanela con 2 opcións:

- Manter os meus arquivos

Restáurase Windows, eliminando as aplicacións e conservando os arquivos.

- Quitar todo

Ábrese outra xanela, preguntando se se quere eliminar:

- Só a unidade onde está instalado Windows (esta opción utilizaríamola, se temos unha partición de Datos, que non queremos eliminar)
- Todas as unidades (borraríanse todas as particións)

Esta opción de “Quitar todo” volvería deixar a partición, tal como estaba ao instalar Windows 10.

4.3 Administración básica do sistema Linux

4.3.1 Administración de usuarios e grupos

4.3.1.1 Creación de usuarios e grupos

Nesta unidade imos estudar varios aspectos da administración de Linux. Neste primeiro libro vai estudar a creación de usuarios e grupos, a pertenza do usuario a distintos grupos e a eliminación de usuarios.

Para administrar contas de usuarios e contas de grupos debemos ser superusuario.

Crear novos usuarios (nun grupo novo)

adduser nome_usuario

Este comando crea un usuario, pero tamén un grupo. Ao executar o comando, realízanse 3 tarefas de forma automática:

1. Créase un usuario co nome introducido.
2. Créase un grupo co mesmo nome.
3. Introdúcese a ese usuario nese grupo.

Ao executar o comando adduser, solicítase a password (hai que introducila 2 veces) e a información completa do usuario (descrición do usuario)

Lembrar lenda de cores nos exemplos:

O prompt do sistema, chamado shell, móstrase en cor negra e os comandos introducidos en negra

As liñas devoltas pola máquina móstranse en cor verde

Os comentarios póñense en cor vermella

Exemplo

```
miguel@sistemasubuntu:$ sudo adduser juan
```

```
[sudo] password for miguel:
```

```
Engadindo o usuario `juan' ...
```

```
Engadindo o novo grupo `juan' (1004) ...
```

```
Engadindo o novo usuario `juan' (1004) con grupo `juan' ...
```

```
Creando o directorio persoal `/home/juan' ...
```

```
Copiando os ficheiros desde `/etc/skel' ...
```

```
Introduza o novo contrasinal de UNIX:
```

Volva escribir o novo contrasinal de UNIX: **Introdúcese o contrasinal**

passwd: contrasinal actualizado correctamente **desexada 2 veces**

Cambiando a información de usuario para juan

Introduza o novo valor, ou presione INTRO para o predeterminado

Nome completo []: Juan Lopez **Aquí pódese encher**

Número de habitación []: **ou deixar todo en branco**

Teléfono do traballo []: 987654321

Teléfono de casa []:

Outro []:

É correcta a información? [S/n] s

Vimos a primeira diferenza con Windows. En Windows hai un grupo “Usuarios”, de forma que cando se crea un usuario introdúceselle nese grupo.

En Linux, non existe ese grupo usuarios, e por defecto, ao usuario introdúceselle nun grupo con igual nome que o usuario, que é o seu grupo principal.

Comandos para crear grupos, introducir a un usuario novo nese grupo e crear password:

Crear novos grupos

addgroup nome_grupo

Ao executar o comando, créase un grupo co nome introducido

Crear novo usuario (nun grupo xa existente)

adduser nome_usuario --ingroup nome_grupo

Cambiar o contrasinal a un usuario:

passwd nome_usuario

Haberá que introducir 2 veces o password novo. Cada usuario pode cambiar o seu password e o root poderá cambiar a de todos os usuarios.

Ficheiros moi importantes de usuarios e grupos:

Cando creamos usuarios e grupos, escribimos nestes ficheiro

O ficheiro **/etc/passwd** contén unha liña para cada usuario.

O ficheiro **/etc/shadow** contén os contrasinais dos usuarios, encriptadas.

O ficheiro **/etc/group** contén unha liña para cada grupo

Significado de /etc/passwd

O ficheiro `/etc/passwd` ten tantas liñas como usuarios. Aparecen bastantes máis usuarios á parte dos creados por nós, pois hai bastantes servizos co seu usuario asignado.

```
miguel@sistemasubuntu:~$ cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
```

 O usuario root sempre aparece en primeira liña

```
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```

 usuario do servizo mail

```
.....
```

```
miguel:x:1000:1000:miguel,,,:/home/miguel:/bin/bash
```

```
alumno:x:1001:1001:,,,:/home/juan:/bin/bash
```

```
juan:x:1002:1002:Juan Lopez,,987654321:/home/juan:/bin/bash
```

```
pablo:x:1003:1003:,,,:/home/pablo:/bin/bash
```

```
juana:x:1004:1003:JuanaGarcia,,765432198:/home/juana:/bin/bash
```

Hai 7 campos separados polo carácter ":" O significado de cada campo é:

O 1 (juana) representa o nome de usuario.

O 2 (x) é unha x que serve para dicir que o usuario está habilitado e o seu contrasinal encriptado.

O 3 (1004) é o identificador de usuario UID (User IDentifier). Este identificador é único para cada usuario. En Ubuntu, este número empeza a partir do 1000 nos usuarios normais. O UID do usuario root, sempre é o 0, de forma que o usuario root sempre aparece na primeira liña do ficheiro.

O 4 (1003) representa o identificador de grupo GID (Group IDentifier). É o grupo principal do usuario. Un usuario poderá pertencer a varios grupos, pero pertence a un grupo de forma principal.

O 5 (JuanaGarcia,,765432198) son os datos que se introduciron na descrición do usuario: nome completo, teléfonos,...

O 6 (/home/juana) representa o directorio \$HOME do usuario.

O 7 (/bin/bash) informa da shell por defecto que utiliza o usuario. Na maioría de Linux actuais, adoita ser a bash (Bourne again shell) que derivou de sh (Bourne shell)

<http://es.wikipedia.org/wiki/bash>

Observación: Á parte dos usuarios normais, tamén aparecen todos os servizos. Por exemplo, na captura, a segunda liña é o servizo mail. Nos servizos, a shell ponse nologin. Isto significa que non se poderá iniciar sesión en terminal ou gráfica con ese usuario (utilizarao só o servizo correspondente)

Significado das liñas de `/etc/group` (Tantas liñas como grupos)

Cada liña representa un grupo

alumno@pcubuntu:\$ **cat /etc/group**

root:x:0:

miguel:x:1000:

alumno:x:1001:

juan:x:1002:

electricista:x:1003:

Hai 4 campos separados polo carácter ":" O significado de cada campo é:

O 1 representa ao nome do grupo.

O 2 non ten un significado especial

O 3 no GID, identificador do grupo

O 4, especifícanse os usuarios que pertencen a ese grupo de forma secundaria, separados por comas. Utilízase só cando un usuario pertence a varios grupos. Por iso, neste exemplo todos os grupos teñen este cuarto campo baleiro (Non aparece nada despois do carácter ":")

No exemplo concreto anterior, vemos en /etc/passwd que os usuarios pablo e juana, pertencen ao mesmo grupo con GID 1003. Para ver como se chama ese grupo, miramos en /etc/group onde vemos que o grupo se chama electricista.

4.3.1.2 Eliminación e modificación de usuarios e grupos. Propietarios de arquivos

Eliminación de usuarios: **userdel [-r]**

A opción -r significa que tamén se vai a eliminar o directorio \$HOME correspondente

#userdel juan Elimina o usuario juan, pero sen borrar o seu \$HOME

#userdel -r juan Elimina o usuario juan e o seu directorio \$HOME (/home/juan)

Eliminación de grupos: groupdel

Só permítese borrar un grupo se ningún usuario pertence xa ao grupo.

#groupdel contable Borra o grupo contable.

O que fan estes comandos, userdel e groupdel é borrar as liñas correspondentes en /etc/passwd e /etc/group

Cambiar a un usuario de grupo ou o seu \$HOME.

Pódense realizar cambios a un usuario, como cambiarlle o grupo principal ou cambiar o roteiro do seu \$HOME. Estes cambios, podémolos realizar manualmente no arquivo /etc/passwd, pero quedarían cousas pendentes, por exemplo unha vez cambiada o roteiro de \$HOME en /etc/passwd, habería que mover o directorio con mv e cambiar permisos.. Realizalo desta forma é moi didáctico, pero para facilitar esa administración, Linux proporciónanos o comando usermod.

usermod [-dgm] nome_usuario

-d Serve para cambiar o directorio home do usuario

-g Sire para cambiar ao usuario de grupo principal

-m Serve para mover os arquivos do directorio home antigo ao home novo (só pódese usar, se á vez usouse -d)

Introducir a un usuario noutros grupos suplementarios ou secundarios

Todos os usuarios poden pertencer á parte do grupo principal, a varios grupos secundarios. Para iso, execútase:

#adduser usuario grupo

Observar que xa debe existir previamente o usuario e o grupo.

Comando groups para ver grupos aos que pertence un usuario

O comando groups mostra os grupos aos que pertence o usuario `miguel@sistemasubuntu:$ groups`

```
miguel sudo electricista
```

Observación

O propio sudo é un grupo do linux, onde por defecto está o usuario que instala Linux. Se queremos que calquera outro usuario, poida executar sudo, por exemplo juan, executaríamos:

sudo adduser juan sudo

Cambiar o usuario e grupo propietario dun arquivo ou directorio

Todo arquivo ten un usuario e un grupo propietario.

Recodar que ao listar en formato longo `ls -l`, obtéñense ambos:

```
-rw-r--r-- 1 juana electricista 5 2012-05-22 00:00 arquivo.txt
```

O usuario propietario de arquivo.txt é juana e o grupo propietario é electricista.

Cando se crea un arquivo, o propietario é quen o crea, e o seu grupo é o grupo principal do usuario.

Cambiar usuario propietario:

chown [-R] nuevoUsuarioPropietario fichero/directorio

Serve para cambiar a un fichero ou directorio o usuario propietario

A opción -R de recursivo, serve para cambiar o propietario a un directorio coa súa árbore.

Cambiar grupo propietario:

chgrp [-R] nuevoGrupoPropietario fichero/directorio

Serve para cambiar a un fichero ou directorio o grupo propietario

A opción -R de recursivo, serve para cambiar o propietario a un directorio coa súa árbore.

Cambiar nun só comando usuario e grupo propietario

chown [-R] nuevoUsuarioPropietario:nuevoGrupoPropietario fichero/directorio

Diferenzas de comandos de crear usuarios e grupos entre distintos LINUX

adduser ou useradd?

Se probamos en Ubuntu, funcionan os 2 comandos. Pero debemos usar adduser pois realiza moitas máis tarefas que useradd, que só crea o usuario, pero non crea nin o seu \$HOME.

Na maioría das distribucións funcionan os 2 comandos, pero nunhas distribucións é máis completo adduser (en Ubuntu) e noutras o é useradd (Red Hat).

4.3.2 Montaxe de dispositivos de almacenamento

Para utilizar calquera partición, pendrive, CD, temos que telo montado. Para montar unha partición, temos que coñecer onde está o seu arquivo de dispositivo.

Os dispositivos atópanse en directorio /dev (device)

Para montar unha partición, temos que coñecer onde está o seu arquivo de dispositivo. Equivale a dicir que en /dev atópanse os drivers. É necesario saber a nomenclatura dos medios de almacenamento.

Nomenclatura dos distintos dispositivos

Primeiro disco: /dev/sda

Segundo disco: /dev/sdb (así sucesivamente, terceiro disco sdc...)

Particións: Números 1 a 4 primarias. A partir do 5 é lóxica.

Por exemplo, /dev/sdb7 representa a terceira partición lóxica do segundo disco

Disqueteira: /dev/fd0 (noutras versións de unix-linux é /dev/floppy). Miramos que fichero existe con ls -l /dev/f*

Cd-Rom e DVD: /dev/sr0 (noutras versións de unix-linux é /dev/floppy)

Punto de montaxe: /media ou /mnt

En Windows, as particións móntanse en letras: D, E,... En Linux, díxose que só hai unha árbore de directorios: a árbore /.

Os dispositivos de almacenamento como pendrive, discos ríxidos externos, cd móntanse automaticamente no directorio /media

Pero hai veces que os temos que montar de forma manual, (disquetes, particións posteriores á instalación...); neste caso montámolo manualmente no directorio /mnt (directorio mount. Aínda que se pode montar en calquera outro sitio)

Denominación dos distintos sistemas de arquivos en Linux

Os posibles **sistemas_ficheiros** dunha unidade lóxica son:

ext2, ext3, ext4 (os de Linux)

msdos (se é FAT16)

vfat (se é FAT32)

ntfs

iso9660 (en CDROM)

Comando de montaxe: mount

mount dispositivo punto_montaxe

Antes de montar co comando mount, debe existir o punto de montaxe (directorio de destino)

Exemplos

Montar primeira partición lóxica do terceiro disco na cartafol Datos dentro do directorio /mnt

```
miguel@sistemasubuntu:$ sudo mkdir /mnt/Datos      #Creamos o punto de montaxe (cartafol destino)
```

```
miguel@sistemasubuntu:$ sudo mount /dev/sdc5 /mnt/Datos      #Montamos, utilizando o dispositivo e o cartafol de destino)
```

Montar un CD de Windows no cartafol win10 dentro de /mnt

```
miguel@sistemasubuntu:$ sudo mkdir /mnt/win10
```

```
miguel@sistemasubuntu:$ sudo mount /dev/sr0 /mnt/win10
```

Ás veces **mount** non pode determinar de forma automática o sistema de ficheiros do dispositivo. Nese caso, habería que engadir ao comando a opción **-t**

Así, por exemplo, para montar o cd de Windows 10, a liña completa sería:

```
miguel@sistemasubuntu:$ sudo mount -t iso9660 /dev/sr0 /mnt/win10
```

Comando df

O comando df mostra os dispositivos montados, co espazo total, ocupado e libre. Coa opción -h dá a información con unidades.

```
miguel@sistemasubuntu:$ df -h
```

S.ficheiros Tamaño Usados Disp Uso% Montado en

```
/dev/sda1 46G 5,3G 38G 13% /
```

```
Compartir 440G 379G 62G 87% /media/sf_Compartir
```

```
/dev/sdb1 59G 56G 2,7G 96% /media/miguel/LabelPendrive
```

```
/dev/sr0 4,4G 4,4G 0 100% /mnt/win10
```

A primeira liña, é a primeira partición do primeiro disco (dispositivo /dev/sda1) que está montado en /. Esta partición ten 46 GB, dos que están ocupados 5,3 GB.

A segunda liña, é o cartafol compartido coa máquina anfitrión

A terceira liña, é a primeira partición do segundo disco (/dev/sdb1) que corresponde a un pendrive de 59 GB montado automaticamente en /media/miguel/LabelPendrive

A cuarta liña, é un CD-Rom (/dev/sr0) que está montado en /mnt/win10 (O DVD ten 4,4 GB)

Desmontar dispositivo. Comando umount

É obrigatorio desmontar un dispositivo antes de extraelo do PC. Se non poderíamos ter algunhas incoherencias, xa que moitas escrituras non se realizan no momento se non cando ao procesador dispón de tempo.

Para desmontar utilízase o comando umount. Admite 2 sintaxe, pois se pode desmontar o dispositivo ou o punto de montaxe:

#umount dispositivo

#umount punto_de_montaxe

Para desmontar o CD montado de Windows do anterior exemplo, execútase unha das 2 instrucións seguintes:

#umount /dev/sr0

#umount /mnt/win10

Ficheiro /etc/fstab

O comando mount equitación o dispositivo, pero cada vez que se inicie o equipo haberá que executar mount.

No ficheiro `/etc/fstab` atópanse os dispositivos que se montan ao iniciar o equipo e en que punto de montaxe.

Podemos engadir unha liña por cada dispositivo que queiramos que se monte ao iniciar o equipo.

Exemplo

Engadir as liñas correspondentes en `/etc/fstab` para montar sempre:

En `/mnt/Datos1` a primeira partición lóxica do segundo disco, formatada `fat32`

En `/mnt/Datos2` a segunda partición lóxica do segundo disco, formatada `ntfs`

miguel@sistemasubuntu:~\$ sudo nano /etc/fstab

<file system> <mount point> <type> <options> <dump> <pass>

..... Engadimos ao final do ficheiro as 2 liñas seguintes:

`/dev/sdb5 /mnt/Datos vfat user,rw 0 0`

`/dev/sdb6 /mnt/Datos2 ntfs user,rw 0 0`

Opcións: Vexamos que significan as opcións escritas:

`user/nouser`: permite utilizar a partición todos os usuarios ou só root.

`rw/ro`: montar lectura-escritura (read-write) ou só lectura (read only)

`defaults`: aplica as opcións `rw`, `suid`, `dev`, `exec`, `auto`, `nouser`, `async`

dump é unha utilidade de copia de seguridade, normalmente, poñemos 0.

pass ten que ver coa comprobación de erros, normalmente, poñemos 0.

man `fstab` mostra o manual de `/etc/fstab`

Administración de discos e particións

Crear particións: programa `fdisk`

`fdisk` é a ferramenta nativa de Unix / Linux (polo que se atopa en todas as distribucións Linux)

Só necesita interface de texto, polo que é unha boa opción cando se accede por acceso remoto (habitualmente con servizo `ssh`) a distintos equipos ou servidores. Na actualidade, isto gaña moita importancia, pois equipos servidores e estacións de traballo atópanse na nube en máquinas virtuais, que adoitan traballar sen contorna gráfica.

Exemplos de `fdisk`:

`#fdisk -l` Mostra en pantalla a información de todas as particións de todos os discos.

#fdisk -l /dev/sda Mostra en pantalla a información de todas as particións do primeiro disco.

#fdisk /dev/sda Ao non utilizar a opción **-l** ábrese o programa fdisk para administrar as particións. Se pulsamos **m**, dános as distintas opcións. As principais opcións son:

m mostra as posibles opcións

p mostra en pantalla as particións actuais (print)

n para engadir unha nova partición (new)

d para borrar unha partición (delete)

w para gardar os cambios realizados e saír de fdisk (write)

Interpretación da información de fdisk

Ponse unha captura da información obtida nunha máquina virtual (é unha maquina distinta a SistemasUbuntu)

```
miguel@virtual:$ sudo fdisk -l
```

```
[sudo] password for miguel:
```

```
Disco /dev/sda: 42.9 GB, 42949672960 bytes #Primeiro disco de 43GB é unha máquina virtual)
```

```
255 cabezas, 63 sectores/pista, 5221 cilindros, 83886080 sectores en total #83 millóns de sectores
```

```
Unidades = sectores de 1 * 512 = 512 bytes #tamaño do sector, 512 bytes
```

```
Tamaño de sector (lógico / físico): 512 bytes / 512 bytes
```

```
Tamaño E/S (mínimo/óptimo): 512 bytes / 512 bytes
```

```
Identificador do disco: 0x00096458 #Fixarse que en cada partición pon sector de inicio e sector final.
```

```
Dispositivo Inicio Comezo Fin Bloques Ide Sistema #Tamén aparece sistema de arquivos
```

```
/dev/sda1 * 2048 29296639 14647296 83 Linux #Primeira partición primaria con sistema arquivos Linux (a partición raíz) O * na primeira partición significa que é a activa.
```

```
/dev/sda2 29296640 31297535 1000448 82 Linux swap / Solaris #Segunda partición primaria (a swap ou área de intercambio)
```

```
/dev/sda3 43585536 83886079 20150272 5 Estendida #Terceira partición primaria que é a estendida
```

```
/dev/sda5 43587584 64067583 10240000 b W95 FAT32 #Dentro de estendida, primeira lóxica tipo fat32
```

```
/dev/sda6 64069632 83886079 9908224 7 HPFS/NTFS/exFAT #Segunda lóxica, tipo ntfs
```

```
Disco /dev/sdb: 62.7 GB, 62742792192 bytes #Segundo disco, é un pendrive de 64GB
```

13 cabezas, 4 sectores/pista, 2356625 cilindros, 122544516 sectores en total

Unidades = sectores de 1 * 512 = 512 bytes

Tamaño de sector (lógico / físico): 512 bytes / 512 bytes

Tamaño E/S (mínimo/óptimo): 512 bytes / 512 bytes

Identificador do disco: 0x000e76a6

Dispositivo Inicio Comezo Fin Bloques Ide Sistema

/dev/sdb1 2048 122544515 61271234 7 HPFS/NTFS/exFAT #Unha partición NTFS ocupando todo o pendrive

Observacións:

Os primeiros 2048 sectores, (equivalen a 2048*512bytes = 1MB) están reservados para MBR, GPT ou futuras estruturas.

Preguntámonos, Queda espazo libre en disco /dev/sda?

Se nos fixamos, en sectores de inicio e final, Vemos que sda2 termina en sector 31 millóns e sda3 comeza en sector 43 millóns (en número redondos). A estendida sda3, vai dos 43 millóns aos 83 millóns que coincide co total de sectores do disco. Ademais, as lóxicas sda5 e sda6 ocupan totalmente a estendida.

Por tanto, o espazo libre é do sector 31 millóns aos 43 millóns, é dicir uns 6GB.

No exemplo final deste libro, execútase fdisk, para crear unha partición nese espazo de 4GB e acábase formatando a partición.

Formatar particións: Comando mkfs

Cando as particións están creadas, antes de podelas utilizar é necesario formatar. Unha vez creada a partición con fdisk, é necesario reiniciar o equipo, e a continuación formatar a partición.

Exemplo

#mkfs -t ext4 /dev/sda6 Formata a partición sda6 con formato ext4

#mkfs /dev/sda6 Formata a partición sda6 con formato ext3 (formato por defecto ao non utilizar a opción -t)

4.3.3 Permisos de ficheiros e directorios

Lembremos que ao listar as propiedades dun arquivo con ls -l, aparece o primeiro campo con 10 caracteres. Despois do primeiro carácter para dicir se é directorio ou ficheiro, os 9 caracteres seguintes son os permisos. Se un ficheiro tivese todos os permisos, os 9 caracteres serían: rwxrwxrwx

Neses caracteres poden aparecer os símbolos “r”, “w”, “x” “-“

Interpretación dos permisos

Os 9 caracteres son 3 grupos de 3 caracteres cada un. (rwxrwxrwx)

Significado dos 3 caracteres rwx

- “r” significa permiso de lectura (read)
- “w” significa permiso de escritura (write)
- “x” significa permiso de execución (execute)
- Se aparece un “-” en lugar da letra, significa que non se ten ese permiso

Por que son 3 grupos de letras? Cada grupo vai dirixido a uns usuarios:

- Primeiro grupo: (user) permisos do usuario propietario do ficheiro.
- Segundo grupo: (group) permisos do grupo propietario do ficheiro excluído o propietario, que pode mesmo non pertencer ao grupo.
- Terceiro grupo: (other) permisos do resto de usuarios

Exemplo

No arquivo listado a continuación, quen pode ler e quen pode facer modificacións? Alguén o pode executar?

```
- r w - r - - - - 1 pablo electricista 40 2018-02-01 22:27 arquivo.txt
```

Resposta:

- O usuario propietario é pablo e os seus permisos son lectura e escritura (r w -)
- O grupo propietario é electricista, e os usuarios do grupo electricista (salvo pablo), só poden ler o ficheiro (r - -).
- O resto dos usuarios non poden nin lelo (- - -)
- Ninguén pode executar o ficheiro

Observación:

Lembrar que en Windows un ficheiro é executable, cando ten a extensión exe, com ou bat. Con todo en Linux non teñen ningunha extensión. O importante é que teña a x nos permisos.

Mesmo, se no anterior exemplo o grupo electricista tivese maiores permisos que pablo, pablo non tería eses permisos aínda que pertenza ao grupo. Observa a diferenza con Windows onde os permisos eran acumulativos.

Significado dos permisos en directorios

Para un ficheiro é trivial diferenciar que significa ler, escribir ou executar, pero que significa que un directorio pódase ler ou executar? Para os directorios estes permisos significan o seguinte:

- r: Permiso para listar o contido do directorio. (Non se pode executar ls senón tense este permiso)
- w: Permiso para crear ou borrar entradas no directorio, é dicir, que quen protexe o borrado dun ficheiro é a escritura do directorio ao que pertence.
- x: Permiso para acceder ás entradas. (Non se pode executar cd senón tense este permiso)

Nos directorios, a r e a x van relacionadas, de forma que se permiten ambas as ou ningunha, pois non ten moito sentido permitir listar un directorio (ls), e non permitir cambiar a ese directorio (cd).

Cambiar permisos: comando chmod

Os permisos só pódenos cambiar 2 usuarios: o usuario propietario do ficheiro e o usuario root.

Sintaxe: # chmod permisos nome_ficheiro

Hai dúas notacións distintas para cambiar os permisos.

1ª Forma (Notación octal)

Convértese cada grupo de permisos (rwx) a un número octal. Como?

Substitúese cada letra por 1 ó 0. Despois sumamos aos que son 1, o valor seguinte: lectura(4) + escritura(2) + execución (1)

Exemplo

Queremos que arquivo.txt teña os permisos seguintes: r w - r w x - -x

Para calcular os permisos, substituímos as letras por 1 e os guións por 0:

r w - r w x - - x

1 1 0 1 1 1 0 0 1

(4+2) (4+2+1) (1)

6 7 1

A liña para executar é: **# chmod 671 arquivo.txt**

2ª Forma (Notación simbólica)

Utilízase un patrón de texto formado por:

1. As categorías afectadas:

u: para o propietario

g: para o grupo

o: para o resto de usuarios

2. Un carácter para retirar os permisos (-), deixalos igual (=) ou engadir (+)

3. As abreviaturas dos tipos de permisos:

r: lectura

w: escritura

x: execución

Exemplos

1. Dar permisos de escritura ao resto de usuarios sobre o ficheiro 'proba': `# chmod o+w /home/usuario1/proba`
2. Quitar todos os permisos de escritura do ficheiro a todos excepto ao propietario:
`# chmod go-w /home/usuario1/proba`

4.3.4 Xestión de procesos

Proceso de arranque

Cando se inicia o equipo primeiro inicia a BIOS que permite detectar e acceder ao hardware do sistema. A partir de aí, carga o xestor de arranque (que en Linux chámase GRUB) e no caso de iniciar un sistema GNU/Linux accede ao directorio /boot onde carga o kernel ou núcleo do sistema operativo e executa o proceso init con PID 1 que será o encargado de iniciar todos os servizos para que o sistema funcione correctamente. Tradicionalmente, o arranque e xestión de procesos de Linux estaba baseado en Unix System V, pero nos últimos anos, a maioría dos Linux adoptaron systemd.

O servizo systemd inicia o proceso kthreadd con PID 2, que xestiona o resto dos servizos relacionados co inicio. Todos os procesos posteriores son fillos, netos,... do init ou do kthreadd.

Comandos de procesos

Comando ps [-efl]

O comando ps lista os procesos vivos (activo, en espera ou bloqueados. Os procesos xa terminados non aparecen.

As opcións habituais son executar ps -ef ó ps -fl

miguel@sistemasubuntu:~\$ **ps -ef**

```

UID PID PPID C STIME TTY ESTAFE CMD
root 1 0 1 23:41 ? 00:00:02 /sbin/init splash
root 2 0 0 23:41 ? 00:00:00 [kthreadd]
root 3 2 0 23:41 ? 00:00:00 [kworker/0:0]
.....
miguel 1387 1 0 23:42 ? 00:00:00 /lib/systemd/systemd --user
.....
miguel 2054 1387 1 23:43 ? 00:00:00 /usr/bin/gnome-calendar --gapplication-service
miguel 2055 1387 1 23:43 ? 00:00:00 /usr/lib/gnome-terminal/gnome-terminal-server
miguel 2142 2055 0 23:43 pts/0 00:00:00 bash
miguel 2153 1418 0 23:43 tty2 00:00:00 update-notifier
miguel 2162 2153 13 23:43 tty2 00:00:01 /usr/bin/python3 /usr/lib/update-notifier/apt-check
miguel 2177 2142 0 23:43 pts/0 00:00:00 ps -ef      #O último proceso é o PID 2177, é a
propia execución do comando ps -ef. O seu pai (PPID) é o PID 2142, que é a propia
terminal bash e o seu pai é o 2055. O pai do 2055 é o 1387, que á vez é fillo do PID 1 que
é o proceso init.

```

Significado de cada columna do comando ps -ef

UID: Usuario que executou o proceso

PID: Identificador de proceso. Son correlativos, executáronse tantos procesos como o último PID. Todos os que faltan, son procesos terminados.

PPID: Identificador de proceso do pai, é dicir, PID do pai

C: Porcentaxe de utilización da CPU para ese proceso

STIME: Hora que se iniciou a executar o proceso

TTY: Terminal ou consola onde se executou o proceso

TIME: Tempo utilizado do procesador para a execución deste proceso

CMD: Comando ou nome do proceso que se executou

Terminar procesos. Comando kill

Para terminar ou matar un proceso, liberando a memoria, utilízase o comando seguinte:

```
$ kill -9 PID
```

Un proceso pódoo terminar o usuario que executa o proceso e o administrador.

Co -9, estamos a executar kill co sinal 9. Senón poñemos -9, kill execútase co sinal por defecto que é a 15. É dicir, é o mesmo executar **\$kill PID** que **\$kill -15 PID**

O sinal -9 é máis potente que a -15. É dicir, cando un proceso bloqueouse, adoita ser máis garantía eliminar o proceso con kill -9

Para ver todos os sinais admitidos polo comando kill, ver a axuda con **\$ man kill**

Comando yes

O comando yes manda o carácter e infinitamente, ata que o finalicemos. Se se executa \$ yes ola devolve ola infinitamente.

Este comando vai utilizar para realizar de forma didáctica algúns exemplos de procesos. É interesante, ver como se pode encher unha partición en minutos, cun comando aparentemente inofensivo como \$ yes > arquivo.txt

Comando top

O comando top, mostra os procesos ordenados por consumo de recursos.

Exemplo. Executar yes nunha terminal e desde outra terminal descubrir PID, consumo de recursos e matar yes

Paso 1.

En primeira terminal, executar yes:

```
miguel@sistemasubuntu:$ yes
```

y

y **#Mostra e infinitas, ata que paremos o proceso. Consume moito procesador**

Paso 2.

Sen pechar a primeira terminal, abrir unha segunda terminal, executar ps -ef ou top (en ambos os comandos, pódese ver PID e consumo de procesador)

```
miguel@sistemasubuntu:$ top
```

```
top - 00:46:15 up 13 min, 2 users, load average: 3,84, 2,90, 1,52
```

```
Tarefas: 209 total, 5 executar, 174 hibernar, 0 deter, 0 zombie
```

```
%Cpu(s): 29,1 usuario, 16,2 sist, 0,2 adecuado, 53,9 inact, 0,3 en espera, 0,0 hardw int, 0,2 sof
```

```
KiB Mem : 2041304 total, 241500 libre, 1124408 usado, 675396 búfer/caché
```

```
KiB Intercambio: 3999740 total, 3999740 libre, 0 usado. 744020 dispon Mem
```

```
PID USUARIO PR NIN VIRT RES SHR S %CPU %MEM HORA+ ORDE
```

```
1076 miguel 20 0 447168 100404 47388 R 20,0 4,9 0:31.35 Xorg
1634 miguel 20 0 802324 39420 28316 R 20,0 1,9 2:14.02 gnome-terminal-
31 root 20 0 0 0 0 R 15,0 0,0 0:29.58 kworker/ou2:1
1964 miguel 20 0 14576 732 668 S 15,0 0,0 1:14.99 yes
2214 miguel 20 0 49020 3860 3236 R 15,0 0,2 0:00.03 top
```

#Neste exemplo, o comando yes ten o PID 2214 e está a consumir o 15% de CPU (a velocidade ás que manda e é moi grande)

Paso 3. Terminar o proceso yes definitivamente:

```
miguel@sistemasubuntu: $ kill -9 2214
```

Este exemplo, mostrou os pasos para seguir para finalizar un programa que se bloquee. Nunha terminal, pescúdase o PID do proceso bloqueado, e execútase kill.

Prioridade de procesos: nice e renice

En Linux, a prioridade dun proceso está entre **-20 que é a prioridade máxima e 19 que é a prioridade mínima**.

As prioridades asignadas a cada proceso visualízanse na columna “NIN” cando executamos `ps -efl` (incorporamos a opción `-l`)

Comando nice. Executar un proceso cunha prioridade concreta

Por defecto todos os procesos execútanse coa prioridade 0. Para executar un proceso con outra prioridade, utilízase nice. Sintaxe do comando nice:

nice [-n prioridade] comando

Exemplos:

```
# nice yes Executa yes con prioridade 10 (nice sen opcións)
```

```
# nice -n -10 yes Asigna a prioridade -10 ao proceso yes
```

Observación

Todos os usuarios poden utilizar a instrución nice, pero só root pode utilizar os negativos. Para o resto dos usuarios a máxima prioridade é 0.

Comando renice. Cambiar prioridade a un proceso que xa está en execución.

O comando renice serve para cambiar a prioridade a un proceso que xa se está executando. A súa sintaxe é:

renice [prioridade] -p PID

Exemplo:

```
$ renice 10 -p 3183 Cambia a prioridade 10 o proceso con PID 3183. Se non se especifica ningunha prioridade, cámbiase a prioridade a 0.
```

Observacións:

Os usuarios só poden utilizar renice para baixar a prioridade.

O superroot pode subir e baixar a prioridade.

4.3.5 Información do sistema e rexistro

Neste punto vemos algúns comandos para obter versión do kernel, información do procesador, memoria, particións, directorios, así como directorios dos eventos producidos no sistema.

Información do sistema e kernel: comando `uname[-ra]`.

O comando `uname` devolve información do sistema. Coa opción `-r` devolve a versión de kernel instalada. Coa opción `-para` devolve información de Linux instalado, coa súa kernel, nome de equipo e se o procesador e Linux instalados son de 32 ou 64 bits.

```
miguel@sistemasubuntu:$ uname -r
```

```
4.15.0-43-generic kernel 4.15
```

```
miguel@sistemasubuntu:$ uname -a
```

```
Linux SistemasUbuntu 4.15.0-43-generic #46-Ubuntu SMP Thu Dec 6 14:45:28 UTC 2018  
x86_64 x86_64 x86_64 GNU/Linux      #Linux instalado en máquina con nome  
SistemasUbuntu. É Ubuntu do 2018 con kernel 4.15 de 64 bits, instalado en procesador  
de 64 bits
```

Importancia da versión do kernel

O kernel ou núcleo de GNU-Liux é independente da distribución (Fedora, Ubuntu, Suse,...) Ao comprar calquera hardware, por exemplo unha impresora, dinos nas especificacións para que Windows é compatible, tamén di se é compatible para Linux, e cal é o kernel mínimo requirido. Por exemplo, nas especificacións virá que é compatible para kernel 2.8 ou posterior.

Kernel 2.8 significa versión 2, e dentro dela a revisión 8. De forma que o kernel 2.8 é anterior ao kernel 4.4.

Información da memoria principal e swap: comando `free`

Mostra información sobre a memoria principal (memoria RAM) e memoria de intercambio total, utilizada e libre

```
miguel@sistemasubuntu:$ free -h
```

```
total usado libre compartido búfer/caché dispoñible
```

```
Memoria: 1,9G 1,1G 169M 19M 665M 666M
```

```
Swap: 3,8G 0B 3,8G
```

O equipo ten 1,9GB, con 1,1GB ocupados e 169MB libres.

A memoria swap ten 3.8GB, toda libre.

Características do procesador: comando lscpu.

Devolve información do procesador. Vese os núcleos que ten, velocidade,...

miguel@sistemasubuntu:~\$ **lscpu**

Arquitectura: x86_64 **#procesador de 64 bits**

modo(s) de operación das CPUs: 32-bit, 64-bit

Orde dos bytes: Little Endian

CPU(s): 8 **#8 CPU? Son 8 fíos de execución en total, que se chama tamén 8 CPU lóxicas ou 8 CPU virtuais.**

Lista da(s) CPU(s) en liña: 0

Fío(s) de procesamento por núcleo: 2 **#2 fíos de execución por núcleo. Hai moitos procesadores que só teñen 1 fío de execución por núcleo.**

Núcleo(s) por «socket»: 4 **#4 núcleos.**

«Socket(s)» 1

Modo(s) NUMA: 1

IDE de fabricante: GenuineIntel

Familia de CPU: 6

Modelo: 60

Nome do modelo: Intel(R) Core(TM) i7-4702MQ CPU @ 2.20Ghz **#Procesador Intel i7 de cuarta xeración (4702)**

Revisión: 3

CPU MHz: 2194.914 **#Velocidade procesador 2194MHz**

BogoMIPS: 4389.82

Fabricante do hipervisor: KVM

Tipo de virtualización: VT-x **#Procesador con instrucións específicas para virtualización**

Caché L1d: 32K

Caché L1i: 32K **#L1: 32KB de datos + 32KB de instrucións**

Caché L2: 256K **#L2: 256KB**

Caché L3: 6144K **#L3: 6144KB**

CPU(s) do nodo NUMA 0: 0-7

.....

Comando df [-h]. Información das particións montadas.

O comando df devolve o espazo total, libre e utilizado dos dispositivos ou particións montadas.

A opción -h fai a información máis lexible en MB ou GB. Sen opción -h a información aparece en KB

```
miguel@sistemasubuntu:$ df -h
```

S.ficheiros Tamaño Usados Disp Uso% Montado en

```
/dev/sda1 46G 5,3G 38G 13% / #sda1 ten montada a partición / con 46GB dos que hai ocupados 5.3GB.
```

.....

```
Compartir 440G 380G 61G 87% /media/sf_Compartir #Montada o cartafol compartir coa máquina anfitrión en /media/sf_Compartir
```

```
/dev/sr0 56M 56M 0 100% /media/miguel/VBox_Gas_5.2.16 #Está montado sr0 que é o CD de Guest additions
```

```
/dev/sdb1 15G 14G 1,5G 91% /media/miguel/NOVO VOL #Está montado un pendrive, como segundo disco sdb de 15GB e 1,5GB libres
```

Comando du [-sh]. Información dos directorios.

O comando du informa do espazo utilizado polo directorio especificado, incluíndo o que ocupan os subdirectorios. O espazo utilizado está en KB.

Opcións:

-s devolve só a liña do directorio e non os subdirectorios

-h devolve a información máis lexible utilizando MB ou GB

Exemplos

```
miguel@sistemasubuntu:$ du -sh /home/miguel
```

3G/home/miguel #O directorio \$HOME do usuario miguel está a ocupar 3GB.

Directorio /proc

É un directorio cargado en memoria RAM, o seu contido non se garda en disco. É dicir, en cada inicio, créase o directorio /proc.

Información do procesador: **cat /proc/cpuinfo** (información parecida a lscpu)

Información de memoria: **cat /proc/meminfo**

Nel gárdase información de cada proceso. Para cada PID créase un cartafol /proc/PID.

Rexistro do sistema: syslog

Tanto en Windows como en Linux os arquivos log son arquivos de texto plano que rexistran o que ocorre no sistema. Cada vez que se inicia o PC escíbese nos devanditos arquivos.

En Linux, o directorio de rexistros é /var/log

Dentro do cartafol /var/log adoita haber un cartafol para cada servizo, onde se gardan os arquivos .log sobre cada servizo.

Arquivo rexistro principal /var/log/syslog

Este arquivo recolle todo o que ocorre no sistema. Gárdanse todos os eventos desde que se instalou Gnu-Linux, polo que normalmente mírase o contido das últimas liñas co comando tail.

Móstrase como exemplo o **arquivo de rexistro** dunha máquina anfitrión Linux con 2 impresoras instaladas:

```
miguel@portatil:$ tail -20 /var/log/syslog #móstranse últimas 20 liñas do arquivo de rexistro
```

```
Feb 9 10:05:57 portatil colord: Profile added: DCP9020CDW-Gray.. #mensaxes relacionadas con impresoras
```

```
Feb 9 10:05:57 portatil colord: Profile added: DCP9020CDW-RGB.. #brother DCP e HP instaladas no equipo
```

```
Feb 9 10:05:57 portatil colord: Device added: cups-DCP9020CDW #cups é o servizo de impresoras de GNU-Linux
```

```
Feb 9 10:05:57 portatil colord: Profile added: hp-LaserJet-1000-Gray..
```

```
Feb 9 10:05:57 portatil colord: Profile added: hp-LaserJet-1000-RGB..
```

```
Feb 9 10:05:57 portatil colord: Device added: cups-hp-LaserJet-1000
```

```
Feb 9 10:09:43 portatil kernel: [ 260.532054] capability: warning: `VirtualBox' uses 32-bit capabilities (legacy support in use) #Esta liña e seguintes relacionadas con inicio VirtualBox
```

```
Feb 9 10:09:51 portatil kernel: [ 268.747435] vboxdrv: ffffffff09e5020 VMMDR0.r0
```

```
Feb 9 10:09:51 portatil kernel: [ 268.860732] vboxdrv: ffffffff0adf020 VBoxDDR0.r0
```

```
Feb 9 10:09:51 portatil kernel: [ 268.863287] vboxdrv: ffffffff0408020 VBoxDD2R0.r0
```

```
Feb 9 10:09:51 portatil kernel: [ 268.894066] vboxdrv: ffffffff0135020 VBoxEhciR0.r0
```

#próximas liñas relacionadas con cron: traballos programados. Execución automática diaria (cron)


```
Feb 9 10:10:27 portatil anacron[1107]: Job `cron.daily' started
Feb 9 10:10:27 portatil anacron[2765]: Updated timestamp for job `cron.daily' to 2018-02-09
Feb 9 10:11:04 portatil anacron[1107]: Job `cron.daily' terminated (exit status: 1) (mailing output)
Feb 9 10:11:04 portatil anacron[1107]: Can't find sendmail at /usr/sbin/sendmail, not mailing output
Feb 9 10:11:04 portatil anacron[1107]: Normal exit (1 job run)
Feb 9 10:17:01 portatil CRON[3150]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Feb 9 10:20:02 portatil udisksd[2245]: Cleaning up mount point /media/miguel/MiguelAngelGarcia (device 8:17 non longer exist) #desmontando pendrive
Feb 9 10:20:02 portatil ntfs-3g[2292]: Unmounting /dev/sdb1 (MiguelAngelGarcia)
```

4.3.6 Tarefas programadas

Demo cron e arquivo /etc/crontab

En Linux programaranse as tarefas con cron. Así por exemplo, poderase reaizar unha copia de seguridade todos os días á mesma hora.

O programa cron componse de 2 elementos: **cron**, o demo (un executable que está a correr todo o tempo) e o arquivo de configuración **/etc/crontab**.

Se vemos os procesos en execución debe aparecer cron. Na liña seguinte execútase `ps -ef` e filtramos con `grep` para obter só as liñas que apareza **cron**:

```
miguel@sistemasubuntu:~$ ps -ef | grep cron #devolvemos só liñas que apareza cron (en Windows, utilizabamos “| find” no canto de “| grep”)
```

```
root 580 1 0 06:51 ? 00:00:00 /usr/sbin/cron -f #efectivamente estase executando o demo cron
```

```
miguel 4517 2179 0 09:05 pts/1 00:00:00 grep --cor=auto cron #esta liña non teñen ningún valor, só está relacionada coa execución do ps
```

Arquivo de configuración das tarefas programadas: /etc/crontab

Para engadir as tarefas programadas, pódense engadir directamente no arquivo **/etc/crontab** con calquera editor.

Normalmente, utilízase o comando: **nano /etc/crontab**

A diferenza entre editar o arquivo directamente con `nano /etc/crontab` e utilizar o comando **crontab -e** radica en que con este último non fan falta privilexios de root (automaticamente Linux configura que esa tarefa execútese cos permisos concretos do usuario)

A primeira vez que se executa **crontab -e** solicítase o editor para utilizar (nano no noso caso)

Sintaxe de cada liña:

m h dom mon dow command **#cabezallo do arquivo**
10 8 * * 3 /home/miguel/script.sh **#Execútase script.sh todos os mércores ás 8:10. Ver significado de cada campo:**

Significado de cada campo:

m: minuto

h: hora, as horas utilizan o formato de 24 horas, sendo válido entre 0 e 23

dom: day of month, día do mes

mon: month, mes

dow: day of weak, día da semana, son válidos os valores 0 (domingo) a 6 (sábado). É así pois en EEUU as semanas empezan por domingo.

Comodíns a utilizar: - , * /

Na anterior liña, utilizouse o comodín *

A continuación, explícanse os comodíns para utilizar cun exemplo:

- * Todos os valores
- 3-6 Valores 3, 4, 5 e 6
- 3,6 Valores 3 e 6
- */10 Cada 10

Exemplos

1. Apagar o computador todos os días ás 21.50. Engadir a seguinte liña:
50 21 * * * poweroff
2. Executar script.sh, cada 20 minutos desde as 9 horas ata as 10 de luns a venres. 2 opcións:
00,20,40 9 * * 1-5 /home/miguel/script.sh
*/20 9 * * 1-5 /home/miguel/script.sh
3. Crear unha copia de seguridade cada 2 días ás 23.50 do home de todos os usuarios:
50 23 /2 * * tar -cvzf /root/home.tar.gz /home/*

O comando tar utilizado aquí estudarase na unidade 7. Serve para obter un arquivo comprimido home.tar.gz con todo o que hai en /home

Outras opcións do comando crontab:

Ver as tarefas programadas dun usuario: **crontab -l -ou nome_usuario**

Eliminar as tarefas dun usuario: **crontab -r -ou nome_usuario**

Cartafoles predefinidas para a execución periódica de tarefas programadas no directorio /etc

En versións actuais de Linux, en /etc atópanse os seguintes subdirectorios:

cron.hourly

cron.daily

cron.weekly

cron.monthly

Os scripts que se poñan en cada subdirectorio executaranse unha vez cada hora, día, semana ou mes segundo subdirectorio utilizado.

Observacións sobre os scripts

Os script de Linux son os equivalentes aos arquivos por lotes de Windows. Mentres que en Windows, tiñamos que chamalos .bat, en Linux o importante é que teñan os permisos de execución. Aínda así, en Linux, aínda que non é obrigatorio, para diferencialos ao listar un directorio, adoitamos poñer aos scripts a extensión .sh

Un script de Linux tamén recibe os nomes de Shell-script e guións Shell, no sentido que se interpretan pola Shell do sistema.

A primeira liña dun script.sh é:

```
#!/bin/bash
```

Esta liña serve para dicir, que o script vai interpretar a shell bash.

A programación de scripts de Linux non está incluída no módulo.

Exemplo de execución dun script

Realizar un script que cre un directorio, direccione contido a un ficheiro dentro do directorio, limpe a pantalla e mostre a listaxe do directorio e o contido do ficheiro.

```
miguel@sistemasubuntu:$ nano exemplo.sh
```

#Con nano escríbese o contido do script. Móstrase o seu contido con cat.

```
miguel@sistemasubuntu:$ cat exemplo.sh
```

```
#!/bin/bash
mkdir /home/miguel/cartafol
boto liña1 do ficheiro.txt > /home/miguel/cartafol/ficheiro.txt
clear
ls -l /home/miguel/cartafol
boto Móstrase contido do ficheiro.txt:
cat /home/miguel/cartafol/ficheiro.txt
miguel@sistemasubuntu:~$ ls -l exemplo.sh
-rw-r--r-- 1 miguel miguel 218 ene 25 02:33 exemplo.sh
#O arquivo non é executable, polo que se se executa, devolve "Permiso denegado"
miguel@sistemasubuntu:~$ ./exemplo.sh
bash: ./exemplo.sh: Permiso denegado
#Ponse permiso de execución ao usuario propietario (miguel)
miguel@sistemasubuntu:~$ chmod ou+x exemplo.sh
#Execútase sen problemas. Limpa a pantalla.
miguel@sistemasubuntu:~$ ./exemplo.sh
#Limpa a pantalla, e devolve listaxe do cartafol e o contido de ficheiro.txt
total 4
-rw-r--r-- 1 miguel miguel 24 ene 25 02:34 ficheiro.txt
Móstrase contido do ficheiro.txt:
liña1 do ficheiro.txt
miguel@sistemasubuntu:~$
```