El Administrador de Sistemas

Administración Avanzada de Sistemas Operativos

Eduardo Iniesta Soto (einiesta@ditec.um.es)

Departamento de Ingeniería y Tecnología de Computadores

UNIVERSIDAD DE MURCIA

CONTENIDOS

- Introducción
- Roles en la administración de sistemas informáticos
- Perfiles del administrador
- Contexto hardware
  - Servidores
  - Otros componentes
- Contexto software
  - Familia Windows Server
  - Distribuciones Linux
  - Comparativa

CONTENIDOS

- Aptitud y actitud
  - Competencia profesional
  - Código ético SAGE
- Estándar ISO 27000
  - Contexto normativo
  - Justificación
  - Catálogo de normas
  - Norma ISO 27002
- Documentación
  - Recomendaciones
  - Etiquetado del hardware

CONTENIDOS

- Sustitución de identidades
  - Windows
  - Linux
- Herramientas de instalación de software
  - Windows
  - Linux
- Herramientas de administración remota
  - Características generales
  - Conexión a Windows
  - Conexión a Linux

INTRODUCCIÓN

- Administrador de Sistemas: “Alguien que, como tarea principal, gestiona sistemas de computación y de red en nombre de otros” (definición de SAGE).
- Sistema: “Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto” (definición de la RAE).
- Sistemas de computación y de red...
  - Los ordenadores.
  - La red.
  - Los usuarios.
  - Las metas y políticas de la organización.

ROLES EN LA ADMINISTRACIÓN DE SISTEMAS

- Ciclo de vida de un sistema informático: concepción, diseño, construcción y operación.
- Roles profesionales que participan en ese ciclo de vida:
  - Arquitecto:
    - Obtiene los requisitos del nuevo sistema.
    - Traduce los requisitos en características.
    - Adopta las decisiones tecnológicas correspondientes.
  - Administrador:
    - Da de alta, mantiene y elimina cuentas de usuario.
    - Instala y actualiza el software.
    - Añade y quita hardware.
    - Diagnostica y resuelve problemas.
    - Monitoriza el sistema.

ROLES EN LA ADMINISTRACIÓN DE SISTEMAS

- Administrador (cont.):
  - Planifica las copias de seguridad.
  - Previene violaciones de seguridad.
  - Documenta las políticas de administración y el inventario.
  - Asiste a los usuarios.
- Operador:
  - Atiende incidencias de los usuarios.
  - Hace las copias de seguridad.
  - Otras tareas rutinarias.

- Una sola persona puede integrar dos o más perfiles.

PERFILES DEL ADMINISTRADOR

- Es una clasificación alternativa de las tareas del administrador de sistemas.
- Un mismo administrador de sistemas puede reunir varios perfiles.
- Perfiles profesionales más habituales en la administración de sistemas:
  - Administrador de bases de datos.
  - Administrador web.
  - Administrador de Linux/Windows.

CONTEXTO HARDWARE: Servidores

- Servidor: Máquina que presta servicios de diverso tipo a un rango de clientes que va desde 1 a varios millones.
- Un servidor va provisto de hardware de alta calidad, que permite que el servicio se preste ininterrumpida e indefinidamente (o “casi”).

CONTEXTO HARDWARE: Servidores

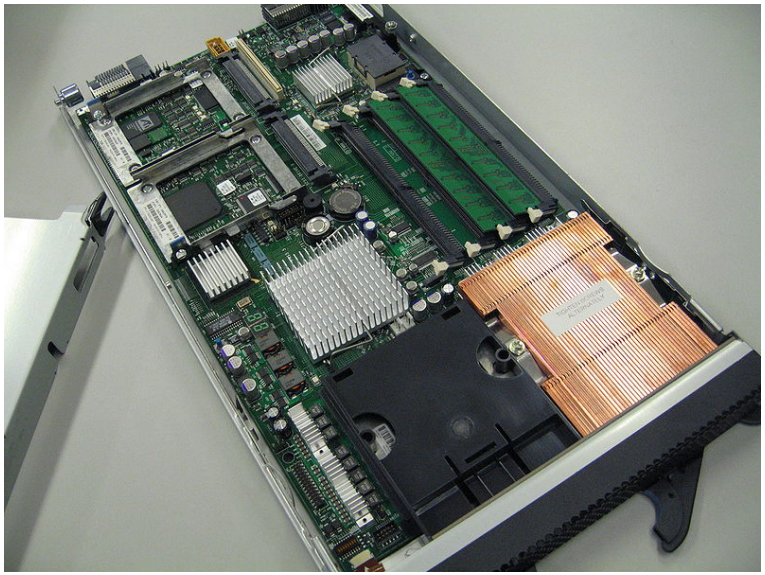
- Marcas comerciales más habituales: IBM, HP, Dell...
- Precio aproximado: 3000 – 6000 €.
- Ejemplo: IBM x3650 (año 2008).

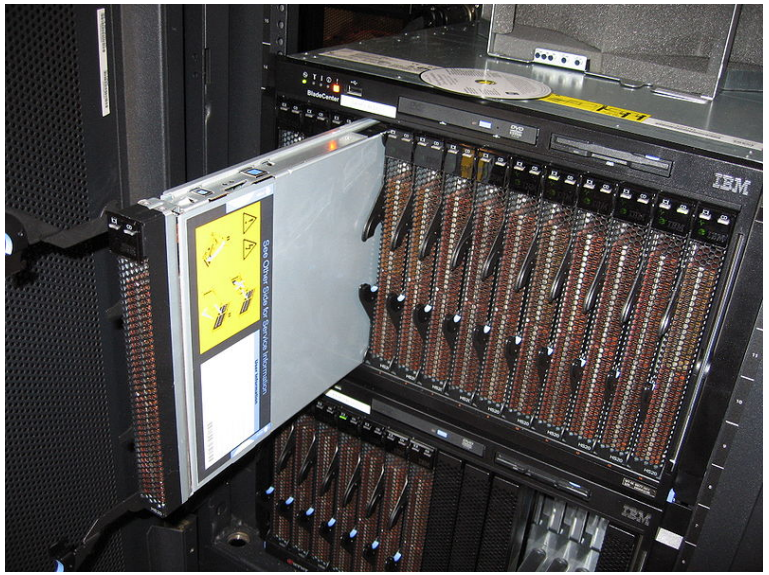
CONTEXTO HARDWARE: Servidores

- Ejemplo: IBM x3650 (cont.):
  - Procesador Intel Xeon X5460 (4 cores, 3 Ghz, ISA de 64 bits, 12 MB caché L2, bus frontal a 1.33 Ghz).
  - Memoria de 48 GB (módulos de 4 GB DDR-2 en 12 slots DIMM).
  - 8 discos duros SATA (6 TB).
  - Interfaz de red Ethernet Gigabit.
  - 4 slots PCI-Express.
  - 3 años de garantía.
  - Precio: 6000 €, aproximadamente.

CONTEXTO HARDWARE: Servidores

- A veces, los servidores son “blade”: sólo microprocesador, memoria y buses.
- Los servidores blade comparten fuente de alimentación, interfaces de almacenamiento y ventiladores.
- Ejemplo: IBM Blade HS20 (año 2006).





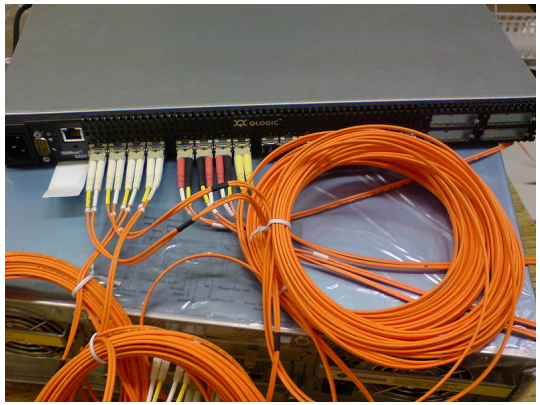
CONTEXTO HARDWARE: Otros componentes

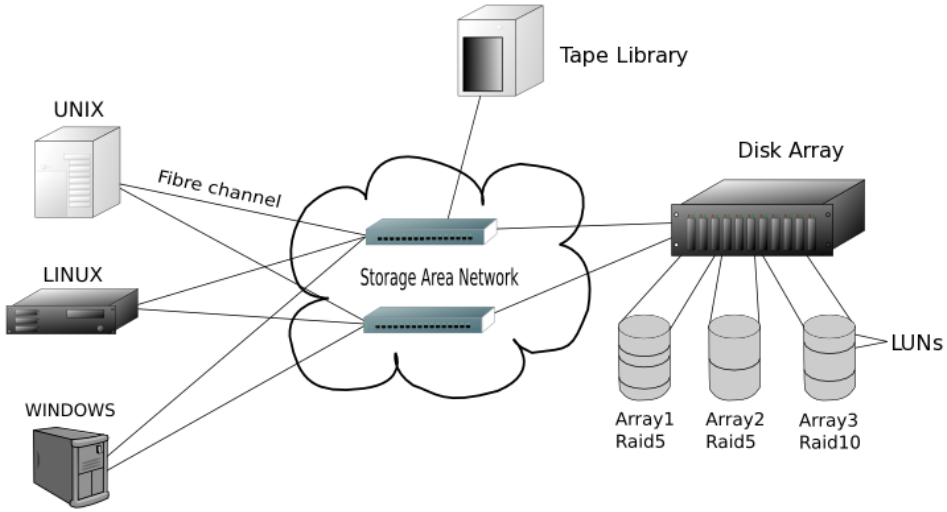
- Cajones para alojar discos duros.
  - Interfaz de canal de fibra.
  - Concebidos para albergar varios grupos de discos configurados en RAID.
  - Ejemplo: IBM DS4000 EXP, con capacidad para 16 discos.

- Discos con interfaz de canal de fibra.

CONTEXTO HARDWARE: Otros componentes

- Switches de canal de fibra.



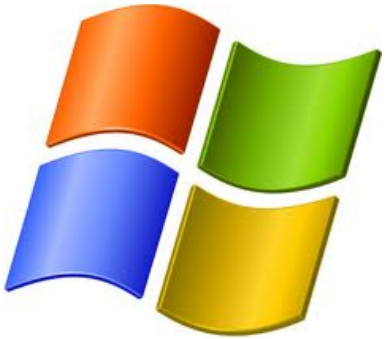


CONTEXTO HARDWARE: Otros componentes

- Equipos de interconexión de redes (hubs, switches, routers...)
- Sistemas de alimentación ininterrumpida.
- Armarios rack para alojar el hardware.
  - Cada componente queda sujeto sobre guías horizontales.
  - Fondo y altura variables, pero ancho normalizado (19").

CONTEXTO SOFTWARE: Familia Windows Server

- Ámbito de aplicación: todo tipo de servidores, pero sobre todo servidores web.
- Amplia difusión, por ser pionero en el ámbito de las arquitecturas Intel.



- Sistema operativo Microsoft Windows Server 2003:
  - Disponible para las arquitecturas ISA x86 (32 bits) e ISA x86_64 (64 bits).
  - Último service pack: SP2, de Marzo de 2007.

CONTEXTO SOFTWARE: Familia Windows Server

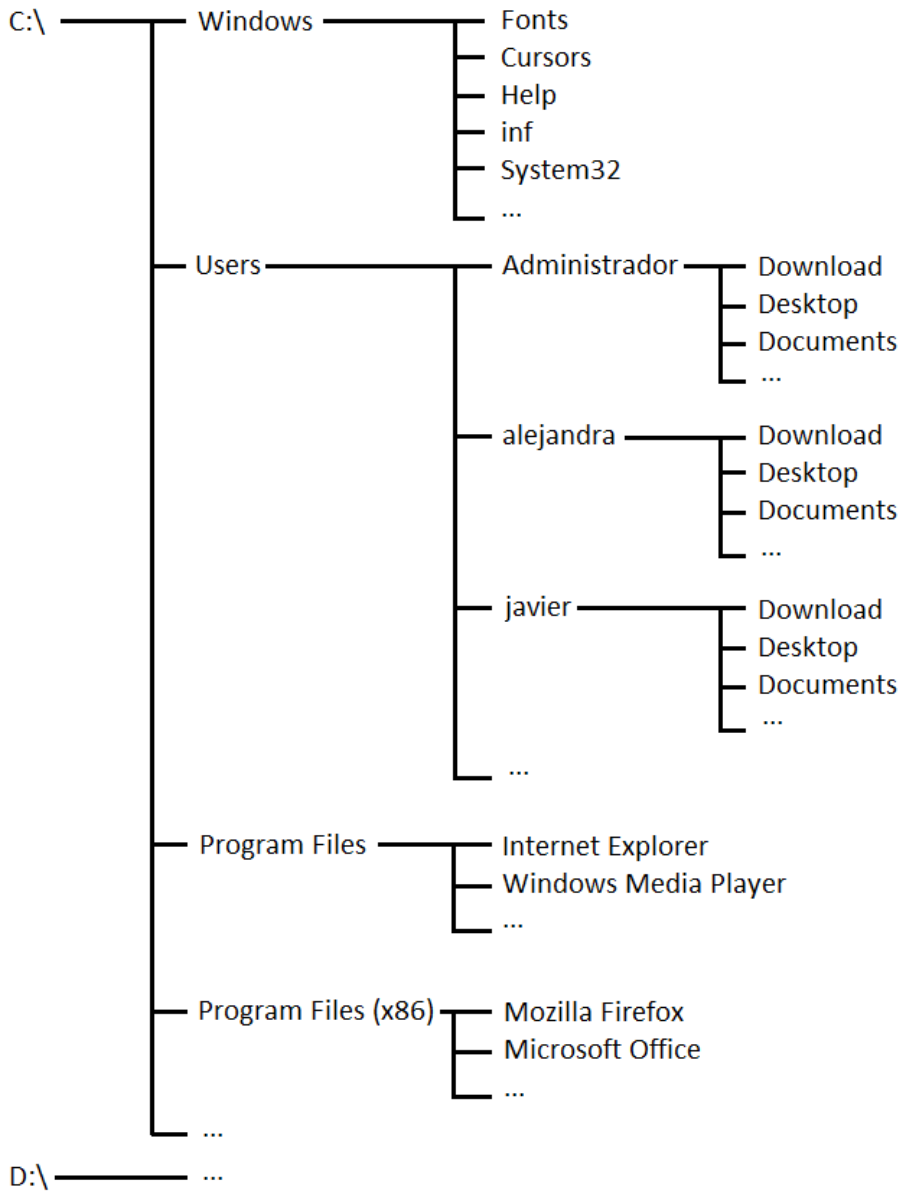
- Sistema operativo Microsoft Windows Server 2003 (cont.):
  - Versiones:
    - Standard: hasta 4 CPU's y hasta 4 GB de RAM.
    - Enterprise: hasta 8 CPU's y hasta 32 GB de RAM (64 GB en x86_64).
    - Datacenter: hasta 32 CPU's y hasta 64 GB de RAM (512 GB en x86_64).

CONTEXTO SOFTWARE: Familia Windows Server

- Sistema operativo Microsoft Windows Server 2008:
  - Disponible para las arquitecturas ISA x86 (32 bits) e ISA x86_64 (64 bits).
  - Último service pack: SP2, de Mayo de 2009.
  - Principales versiones:
    - Standard: hasta 4 CPU's y hasta 4 GB de RAM (32 GB en x86_64).
    - Enterprise: hasta 8 CPU's y hasta 32 GB de RAM (2 TB en x86_64).
    - Datacenter: hasta 64 CPU's y hasta 64 GB de RAM (2 TB en x86_64).
- Privilegios de administración:
  - Usuario “administrador”.
  - Cualquier otro usuario que forme parte del grupo “Administradores”.

CONTEXTO SOFTWARE: Familia Windows Server

- Jerarquía de directorios:



CONTEXTO SOFTWARE: Distribuciones Linux

- Ámbito de aplicación: todo tipo de servidores; en particular, suele ser la opción preferida en sistemas de cálculo intensivo (clusters y supercomputadores).
- Muy estable, seguro y eficiente.
- Linux es realmente sólo el kernel del sistema operativo GNU/Linux.
- Distribución Linux = sistema operativo GNU/Linux = Linux (kernel) + programas desarrollados bajo licencia GPL.

CONTEXTO SOFTWARE: Distribuciones Linux

- Siglas:
  - GNU (“GNU's Not Unix”): Proyecto para implementar un sistema operativo libre.
  - GNU, aparte del núcleo Linux, también ampara otros proyectos:
    - Compilador GCC.
    - Biblioteca para C GLIBC.
    - Escritorio GNOME.
    - Editor gráfico GIMP.
    - Etc.
  - FSF (“Free Software Fundation”): Organización que está a cargo del proyecto GNU.
  - GPL (“GNU Public License”): Licencia bajo la que se distribuye Linux y el software asociado (gratuidad y posibilidad de alterar y difundir el código fuente).

CONTEXTO SOFTWARE: Distribuciones Linux

- Distribución

  Red Hat Enterprise Linux (RHEL):

  - Última versión: 6.
  - Sitio web: http://www.redhat.com
  - Ámbito profesional: entornos de producción (distribución predominante).
  - Origen: Procede de la división de Red Hat en Fedora y RHEL. Año 2003.
  - El código fuente está bajo licencia GPL, pero por el resto (binarios, documentación, soporte) hay que pagar una licencia.
  - Disponible para el ISA x86 y el ISA x86_64.

CONTEXTO SOFTWARE: Distribuciones Linux

- Distribución Centos (“The Community ENTerprise Operating System”):

  - Última versión: 6.
  - Sitio web: http://www.centos.org
  - Ámbito profesional: entornos de producción.
  - Origen: Copia literal de RHEL (compilación de los fuentes de RHEL). Año 2004.
  - La distribución completa es GPL.
  - Disponible para el ISA x86 y el ISA x86_64.

CONTEXTO SOFTWARE: Distribuciones Linux

- Distribución Fedora

  (Fedora: sombrero a lo “Indiana Jhones”):

  - Última versión: 16.
  - Sitio web: http://fedoraproject.org
  - Ámbito profesional: entornos de desarrollo.
  - Origen: Procede, como su propio nombre sugiere, de Red Hat (división de Red Hat en Fedora y RHEL). Año 2003.
  - Licencia GPL.
  - Disponible para el ISA x86 y el ISA x86_64.

CONTEXTO SOFTWARE: Distribuciones Linux

- Distribución SUSE Linux Enterprise Server ("Software Und SystemEntwicklung"):

  - Última versión: 11.
  - Sitio web: http://www.suse.com
  - Ámbito profesional: entornos de producción.
  - Origen: Procede de la división de SUSE en dos distribuciones: SUSE Linux Enterprise Server y Open SUSE (este último es libre). Año 2004.
  - Licencia de pago, comercializado por Novell.
  - Disponible para el ISA x86 y el ISA x86_64.

CONTEXTO SOFTWARE: Distribuciones Linux

- Distribución Debian

  (“DEBorah and IAN Murdok”):

  - Última versión: 6.
  - Sitio web: http://www.debian.org
  - Ámbito profesional: entornos de desarrollo.
  - Origen: Proyecto GNU/Linux (una de las distribuciones más antiguas). Año 1997.
  - Licencia GPL.
  - Disponible para el ISA x86 y el ISA x86_64.

CONTEXTO SOFTWARE: Distribuciones Linux

- Distribución Ubuntu

  (“Igualdad y lealtad”, en zulú):

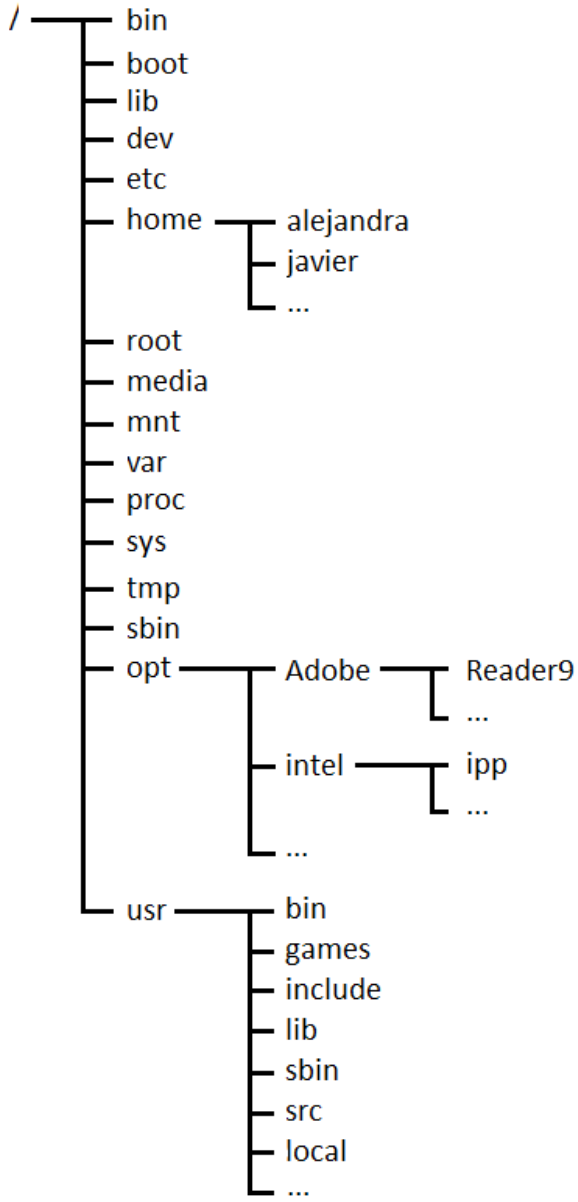
  - Última versión: 11.10.
  - Sitio web: http://www.ubuntu.com
  - Ámbito profesional: entornos de desarrollo (distribución predominante).
  - Origen: Debian y el patrocinio de la compañía británica Canonical. Año 2004.
  - Licencia GPL.
  - Disponible para el ISA x86 y el ISA x86_64.

CONTEXTO SOFTWARE: Distribuciones Linux

- Privilegios de administración:
  - Usuario “root”.
  - Cualquier otro usuario que forme parte del grupo “Administradores”.

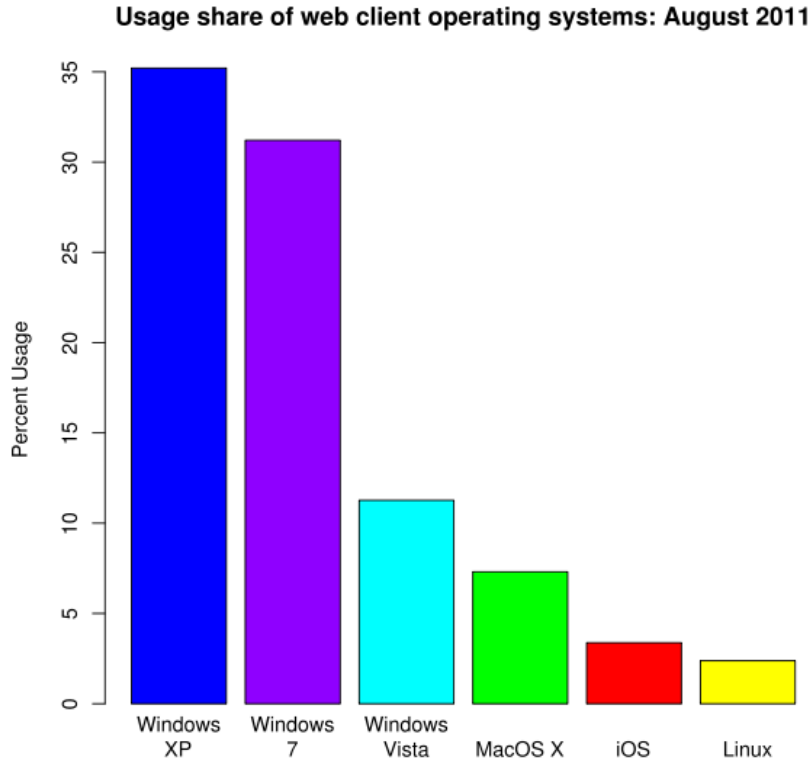
CONTEXTO SOFTWARE: Distribuciones Linux

- Jerarquía de directorios:



CONTEXTO SOFTWARE: Comparativa

- Ámbito de los ordenadores personales (2011): 90% Windows, 10% resto.



- Ámbito de los servidores (2008): 51% Linux, 36% Windows.
- Supercomputadores (2008): 85% Linux, 1% Windows.

APTITUD Y ACTITUD: Competencia profesional

- Aparte de los conocimientos que se irán adquiriendo aquí...
  - Sólida comprensión del funcionamiento interno de los sistemas operativos.
  - Conocimiento de las herramientas de administración básicas.
  - Conceptos básicos de redes locales y enrutamiento.
  - Saber implementar guiones shell.
- Habilidades y destrezas transversales:
  - Saber escuchar a los usuarios y ser capaz de hacerse entender.
  - Cierto grado de autonomía en la resolución de problemas.
  - Capacidad para redactar, de modo inteligible y formal, documentos técnicos.
  - Conocimiento alto del idioma inglés.

APTITUD Y ACTITUD: Código ético SAGE

- Profesionalidad.
- Integridad personal.
- Privacidad.
- Leyes y políticas.
- Comunicación.
- Integridad del sistema.
- Educación.
- Responsabilidad ante la comunidad informática.
- Responsabilidad social.
- Responsabilidad ética.

ESTÁNDAR ISO 27000: Contexto normativo

- ISO (“International Standarization Organization”):

  - Dicta normas industriales reconocidas internacionalmente.
  - Compuesta por 162 institutos nacionales de normalización:
    - ANSI en EE.UU.
    - DIN en Alemania.
    - BSI en Reino Unido.
    - AFNOR en Francia.
    - AENOR en España.
    - ...

ESTÁNDAR ISO 27000: Contexto normativo

- Algunas de las normas ISO más relevantes a nivel general:
  - ISO 9001: Sistema de gestión de la calidad.
  - ISO 14001: Sistema de gestión medioambiental en entornos de producción.
  - ISO 18001: Sistema de gestión de salud y seguridad laboral.

- Algunas de las normas ISO más relevantes en el ámbito de las TIC:
  - ISO 20000: Conjunto de normas relativas al sistema de gestión de servicios de las tecnologías de la Información.
  - ISO 27000: Conjunto de normas relativas al sistema de gestión de la seguridad de la Información.

ESTÁNDAR ISO 27000: Acreditaciones ISO

- Justificación de las acreditaciones:
  - Objetivos endógenos:
    - Asegurar la calidad, integridad y fiabilidad de algún producto, servicio o empresa.
  - Objetivos exógenos:
    - Mejorar la imagen de marca.
    - Satisfacer requisitos en determinados contratos.
- ¿Quién puede conceder acreditaciones?
  - En España, todas aquellas empresas u organizaciones auditoras que hayan obtenido el reconocimiento de ENAC ("Entidad Nacional de Acreditación"): AENOR, Bureau Veritas, TUV...

ENAC Entidad Nacional de Acreditación

AENOR ER Empresa Registrada

BUREAU VERITAS 1828

TÜVRheinland®

ESTÁNDAR ISO 27000: Acreditaciones ISO

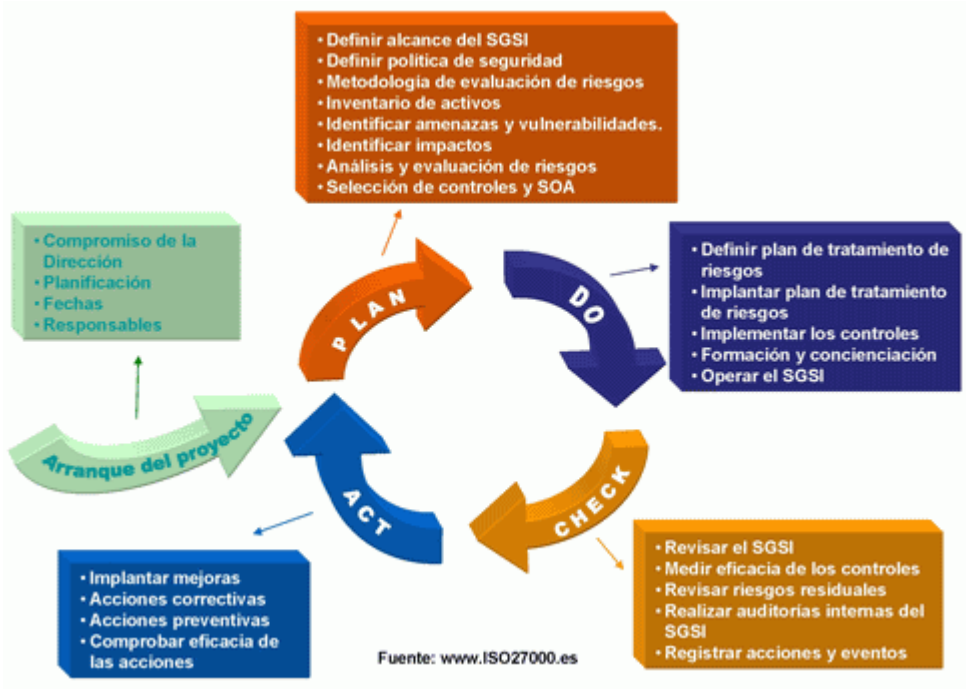
- Caso de AENOR:
  - Es una organización privada y sin ánimo de lucro.
  - Representante de España en ISO.
  - Cometidos:
    - Elaborar normas UNE (“Una Norma Española”), algunas de las cuales pueden ser asumidas internacionalmente por ISO.
    - Conceder certificaciones ISO.
  - Tipos de normas UNE:
    - UNE: Una Norma Española.
    - UNE-EN: Una Norma Española - European Norm.
    - UNE-EN-ISO: Una Norma Española - European Norm - International Standarization Organization.

ESTÁNDAR ISO 27000: Acreditaciones ISO

- Caso de AENOR (cont.):
  - Proceso de certificación:
    - Cuestionario previo de solicitud.
    - Planificación de la auditoría.
    - Análisis de la documentación.
    - Visita previa.
    - Auditoría del sistema.
    - Plan de acciones correctoras.
    - Concesión de la certificación.
    - Auditorías anuales de seguimiento.
    - Auditorías trienales de renovación del certificado.

ESTÁNDAR ISO 27000: Catálogo de normas

- ISO 27000:
  - Visión general de las normas de la serie 27000: “Sistema de Gestión de Seguridad de la Información” (SGSI).
  - Describe someramente el proceso de implantación ISO 27000.



  - Serie ISO 27000: ISO 27001, ISO 27002, ISO 27003 ...

ESTÁNDAR ISO 27000: Catálogo de normas

- ISO 27001:

  - Año 2005.
  - Origen: norma británica BS-7799-2 (1998), transformada en 2005 en ISO 27001.
  - Norma principal de la serie 27000.
  - Contiene los requisitos de un SGSI.
  - Anexo A: Guía de buenas prácticas y controles relativos a la seguridad de la información. Desarrollado en profundidad en la norma ISO 27002.
  - No obligatoriedad de implantar todos los controles del anexo A, pero con argumentos.

ESTÁNDAR ISO 27000: Catálogo de normas

- ISO 27002:

  - Año 2007.
  - Origen: norma británica BS-7799-1 (1995), transformada en 2000 en ISO 17799 y en ISO 27002 en 2007.
  - ISO 27002 e ISO 17799 son, en la práctica, equivalentes.
  - Implementa una guía de buenas prácticas y controles relativos a la gestión de la seguridad (desarrolla el anexo A de la norma ISO 27001).
  - 133 controles de gestión de la seguridad, agrupados en 11 dominios.
  - Publicada en España como UNE-ISO/IEC 27002:2009.

ESTÁNDAR ISO 27000: Norma ISO 27002

- Dominio nº 1: “Política de seguridad de la información”.
- Dominio nº 2: “Aspectos organizativos de la seguridad de la información”.
  - Organización interna.
  - Seguridad en los accesos de terceras partes.
- Dominio nº 3: “Gestión de activos”.
  - Inventario de activos hardware.
  - Clasificación de la información.
- Dominio nº 4: “Seguridad en recursos humanos”.
  - Seguridad antes del empleo.
  - Seguridad durante el empleo.
  - Finalización del empleo.

ESTÁNDAR ISO 27000: Norma ISO 27002

- Dominio nº 5: “Seguridad física y ambiental”.
  - Áreas seguras.
  - Seguridad de los equipos.
- Dominio nº 6: “Gestión de comunicaciones y operaciones”.
  - Procedimientos de operación.
  - Tareas de planificación.
  - Protección contra software malicioso.
  - Gestión de copias de seguridad.
  - Seguridad telemática.
  - Gestión de medios removibles.
  - Supervisión de accesos y actualizaciones.
  - ...

ESTÁNDAR ISO 27000: Norma ISO 27002

- Dominio nº 7: “Control de accesos”.

  - Gestión de accesos por parte de los usuarios.
  - Responsabilidades de los usuarios.
  - Control de acceso al sistema operativo.
  - Control de acceso a las aplicaciones.
  - Control de acceso a la red.
  - Comunicaciones inalámbricas.
  - ...

ESTÁNDAR ISO 27000: Norma ISO 27002

- Dominio nº 8: “Adquisición, desarrollo y mantenimiento de sistemas de información”.

  - Requisitos de seguridad de las aplicaciones.
  - Robustez de las aplicaciones.
  - Controles criptográficos.
  - Seguridad y estabilidad del sistema operativo y de las aplicaciones.
  - Procesos de desarrollo y soporte.
  - ...

ESTÁNDAR ISO 27000: Norma ISO 27002

- Dominio nº 9: “Gestión de incidentes de seguridad”.
  - Notificación de incidencias.
  - Gestión de mejoras.
- Dominio nº 10: “Gestión de la continuidad del negocio”.
- Dominio nº 11: “Cumplimiento”.
  - Cumplimiento de la legislación nacional.
  - Cumplimiento de las normas internas.

DOCUMENTACIÓN: Recomendaciones

- ¿Qué se documenta?
  - Procedimientos operativos.
  - Inventario de software.
  - Inventario de hardware.
  - Incidencias.
  - Contactos.
  - Teléfonos de emergencias.
  - ...
- ¿Por qué se debe documentar?
  - Para recordar procedimientos no rutinarios.
  - Para facilitar la tarea de otros posibles administradores.

DOCUMENTACIÓN: Recomendaciones

- ¿Dónde se documenta?
  - Opcionalmente, en formato electrónico; obligatoriamente, en papel.
  - Comentarios en guiones shell y en ficheros de configuración.

- ¿Cuáles son los formatos recomendados?
  - Formato estándar compartido por todos los documentos.
  - Explicaciones breves y sencillas.
  - A ser posible, documentos de no más de una página.

DOCUMENTACIÓN: Etiquetado del hardware

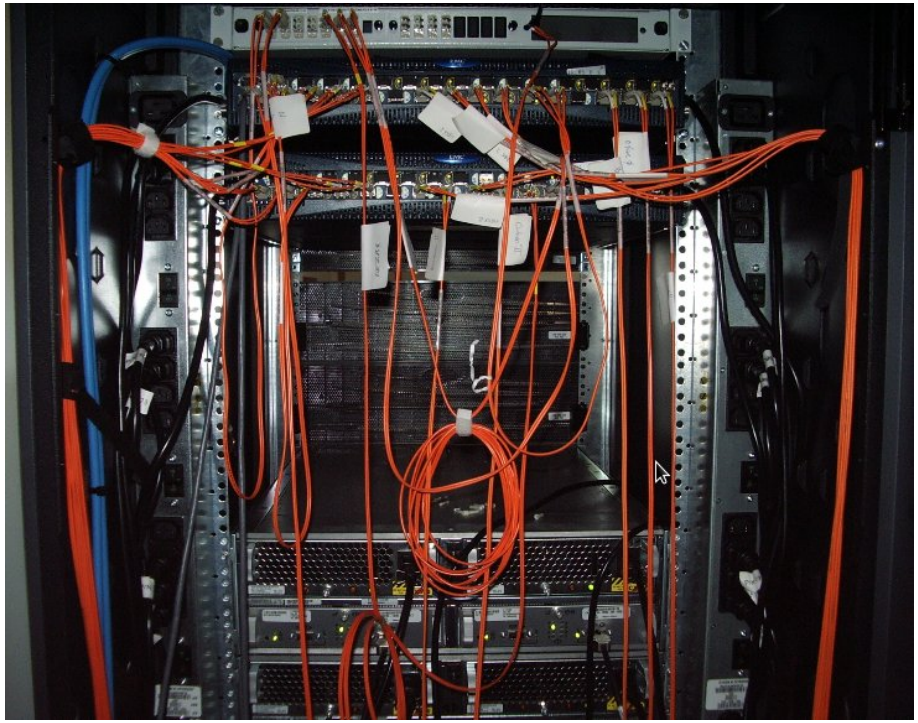
- ¿Por qué etiquetar?
  - Facilitar la localización del hardware.
- ¿Cómo etiquetar?
  - Etiquetas adhesivas de pequeño tamaño y lectura fácil.
  - Copia de la información de la etiqueta en el inventario hardware.
  - Mantener permanentemente actualizadas las etiquetas.
  - En caso necesario, incluir en el inventario hardware las ubicaciones de elementos poco visibles de la sala de servidores.

DOCUMENTACIÓN: Etiquetado del hardware

- ¿Qué hardware se debe etiquetar?
  - Servidores:
    - Nombre.
    - Dirección (o direcciones) IP.
    - Arquitectura y sistema operativo.
    - Información de contacto del responsable del equipo.
  - Arrays de discos:
    - Grupo RAID.
    - Particiones.
    - Puntos de montaje.
  - Unidades de cinta.
  - Impresoras.
  - Discos USB.

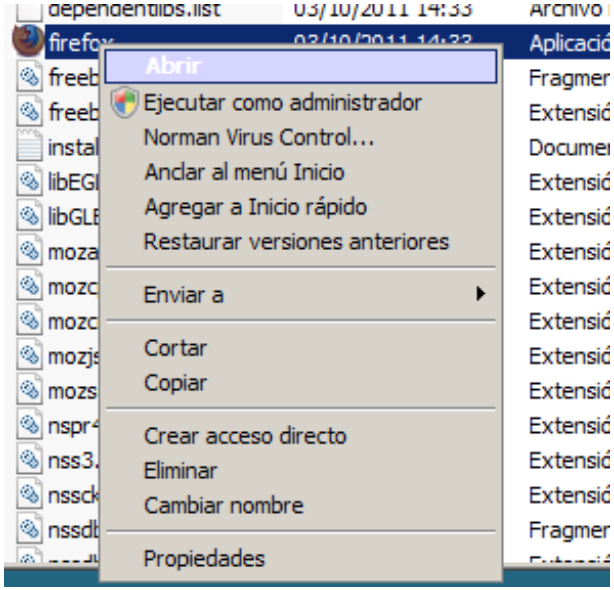
DOCUMENTACIÓN: Etiquetado de hardware

- ¿Qué hardware se debe etiquetar? (cont.)
  - Elementos de interconexión:
    - Routers, switches, hubs...
    - Cableado (ethernet y fibra).



SUSTITUCIÓN DE IDENTIDADES: Windows

- Recomendación de seguridad: intentar, en la medida de lo posible, no iniciar sesión como administrador.
  - Entrar en una cuenta convencional, y recurrir a utilidades de administración sólo cuando sea necesario.
- ¿Qué hacer cuando se requiera alguna tarea administrativa?
  - Opción 1: ejecutar esa tarea con privilegios de administración mediante la opción “Ejecutar como Administrador”.



SUSTITUCIÓN DE IDENTIDADES: Windows

- ¿Qué hacer cuando se requiera alguna tarea administrativa?
  - Opción 2: ejecutar "`runas`".

Sintaxis: `runas /user:<equipo>\<usuario>`

Y si es un dominio: `runas /user:<usuario>@<dominio>`

Ejemplos:

Abrir un shell de administración en el equipo ASO19:

```
runas /user:aso19\administrador cmd
```

Abrir un shell de administración en el dominio dom19.sala27:

```
runas /user:administrador@dom19.sala27 cmd
```

SUSTITUCIÓN DE IDENTIDADES: Windows

- ¿Qué hacer cuando se requiera alguna tarea administrativa?
  - Opción 2: ejecutar "`runas`".
    - Ejemplos (cont.):

Abrir el administrador de tareas como usuario Administrador:

```
runas /user:aso19\administrador taskmgr
```

Abrir el administrador de discos como usuario Administrador:

```
runas /user:aso19\administrador "mmc %SystemRoot
%\system32\diskmgmt.msc"
```

SUSTITUCIÓN DE IDENTIDADES: Linux

- Recomendación de seguridad: al igual que en Windows, intentar no iniciar sesión como administrador (al menos en un terminal gráfico).
  - Fedora 15 por defecto no permite el inicio de sesión como **root** en el terminal gráfico.
  - Como en Windows, trabajar con una cuenta normal y recurrir puntualmente a utilidades de administración.
- ¿Qué hacer cuando se requiera alguna tarea administrativa?
  - Abrir un shell como root: `su`
  - Abrir un shell como root simulando una apertura de sesión: `su -`
  - Abrir un shell como otro usuario: `su <usuario>`
  - Ejecutar una orden sin abrir un shell: `su -c <orden>`

SUSTITUCIÓN DE IDENTIDADES: Linux

- sudo:
  - Permite delegar tareas administrativas que normalmente sólo haría **root**.
  - Permite ejecutar como otro usuario un determinado programa.
- Sintaxis:

```
sudo [-u <usuario>] <comando>
```

- Ejemplo 1: delegación de tarea administrativa.

```
sudo /bin/cat /etc/shadow
```

- Ejemplo 2: ejecutar como otro usuario un determinado programa.

```
sudo -u operadorcopias /sbin/dump 0uf
/media/discousb/copia.dump /dev/sda2
```

SUSTITUCIÓN DE IDENTIDADES: Linux

- En `<comando>` es aconsejable indicar la ruta completa, para prevenir la ejecución inadvertida de otros programas.
- Fichero `/etc/sudoers`:
  - Permisos:

    ```
    -r--r-----. 1 root root 3338 nov 30  2010 /etc/sudoers
    ```

  - Establece quién puede ejecutar `sudo`, qué comandos puede ejecutar, en qué máquinas puede hacerlo y a qué usuarios puede suplantar.
  - Cuando un usuario ejecuta `sudo`, el sistema le vuelve a pedir sus credenciales.
  - Es conveniente que **root** actualice `sudoers` sólo mediante la herramienta `visudo`.

SUSTITUCIÓN DE IDENTIDADES: Linux

- Sintaxis de `/etc/sudoers`: Lista de líneas (una por permiso)...
  - `<usuarios_o_grupos> <host> = <comandos>`
  - <usuarios_o_grupos>
    - Usuario, grupo, lista de usuarios o lista de grupos.
    - Ejemplo 1: `alumno,alumno2` => usuarios **alumno** y **alumno2**.
    - Ejemplo 2: `%profesores` => grupo **profesores**.
  - <host>
    - Máquina o lista de máquinas para las cuales el permiso es válido.
    - Es posible agrupar varias máquinas bajo un mismo alias.
    - Ejemplo 1: `ALL` => Permisos válidos para cualquier máquina.
    - Ejemplo 2: `Host_Alias DITEC = sig, oracle`
      `DITEC` => Válidos sólo para **sig** y **oracle**.
    - Ejemplo 3: `ALL, !DITEC` => Válidos para todas, excepto **sig** y **oracle**.

SUSTITUCIÓN DE IDENTIDADES: Linux

- Sintaxis de `/etc/sudoers` (cont.)
  - <comandos>: `[(ALL | <usuario>)] <rutas_comandos>`
    - La primera parte es opcional; se indica si se quiere permitir suplantar a una identidad distinta de la de **root** (`sudo -u`).
      - Si se quiere dejar que se suplante a cualquier identidad, elegir `ALL`.
      - Si se quiere filtrar las identidades admisibles, indicar el nombre o nombres de usuario.
    - La segunda parte es obligatoria: son los comandos permitidos.
      - Si se quiere permitir la ejecución de cualquier comando, indicar `ALL`.
      - Se pueden indicar directamente, o agrupar bajo un alias.
    - Ejemplo 1: `ALL` => Se puede ejecutar cualquier comando, pero sólo como **root**.
    - Ejemplo 2: `(ALL) ALL` => Idem, pero ahora es posible elegir cualquier usuario con `sudo -u`.

SUSTITUCIÓN DE IDENTIDADES: Linux

- Sintaxis de `/etc/sudoers` (cont.)
  - <comandos>: `[(ALL | <usuario>)] <rutas_comandos>`
    - Ejemplo 3: `(adminsudo) /usr/bin/kill, /sbin/modprobe`
      => comandos ejecutables sólo como usuario **adminsudo**.
    - Ejemplo 4: `Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/yum`
      `SOFTWARE` => Se puede ejecutar (como **root**) `rpm` y `yum`.
    - Ejemplo 5: `ALL, !SOFTWARE` => Se puede ejecutar (como **root**) todo menos `rpm` y `yum`.
    - Ejemplo 6: `NOPASSWD:SOFTWARE` => Idem `SOFTWARE`, pero ahora **sudo** no pedirá password.

SUSTITUCIÓN DE IDENTIDADES: Linux

- Ejemplo de `/etc/sudoers`:
  - Configuración requerida: en cualquier máquina en la que esté el siguinte `sudoers` ...
    - **root** puede hacer lo que quiera y suplantar a cualquiera.
    - **alumno**, en el papel de **root** y mediante `sudo`, únicamente podrá instalar y desinstalar programas.
  - Contenido de `/etc/sudoers`:

```
Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/yum
root    ALL=(ALL) ALL
alumno  ALL=SOFTWARE
```

SUSTITUCIÓN DE IDENTIDADES: Linux

- De cualquier comando que se ejecute o se intente ejecutar con `sudo` queda constancia en la bitácora `/var/log/secure`.
  - Permisos:

    ```
    -rw-------. 1 root root 25818 dic 10 18:59 /var/log/secure
    ```

  - En `secure` también se almacenan las sesiones que se han abierto, así como los intentos fallidos.
  - Los contenidos “antiguos” de `secure` se van separando en otros ficheros `secure-<AAAAMMDD>`.

SUSTITUCIÓN DE IDENTIDADES: Linux

- Ejemplo (fragmento de un `/var/log/secure`):

```
Dec  7 20:30:02 localhost sudo:   alumno : user NOT in
sudoers ; TTY=pts/1 ; PWD=/home/alumno ; USER=root ;
COMMAND=/bin/cat /etc/sudoers

Dec  7 20:43:25 localhost sudo:   alumno : 3 incorrect
password attempts ; TTY=pts/1 ;
PWD=/home/alumno/Descargas ; USER=root ; COMMAND=/bin/rpm
-i AdobeReader_esp-8.1.7-1.i486.rpm

Dec  7 20:44:53 localhost sudo:   alumno : command not
allowed ; TTY=pts/1 ; PWD=/home/alumno/Descargas ;
USER=root ; COMMAND=/bin/rpm -i AdobeReader_esp-8.1.7-
1.i486.rpm

Dec  7 20:45:31 localhost sudo:   alumno : TTY=pts/1 ;
PWD=/home/alumno/Descargas ; USER=root ; COMMAND=/bin/rpm
-i AdobeReader_esp-8.1.7-1.i486.rpm
```

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Windows

- Software ajeno al sistema operativo:
  - Instalación: cada nuevo programa aporta su propia herramienta de instalación.
  - Desinstalación: desde el panel de control, en “Programas y Características”.
  - En todo caso, hay que actuar como **Administrador**.
- Software del sistema operativo:
  - Hay que ser el usuario **Administrador**.
  - Herramienta de instalación automática de parches: “Windows Update”.
    - Es configurada desde el panel de control, en “Windows Update”.
    - Se recomienda elegir otra opción distinta de la que hay por defecto: “Instalar actualizaciones automáticamente” (*ISO 27002, control 12.5.1 -dominio 8-*).

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Windows

- Software del sistema operativo (cont.):
  - Instalación de Service Packs:
    - Ser cauto y no instalar si no es necesario (algunos programas podrían dejar de funcionar).
    - Mejor la instalación desde el sitio de Microsoft.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Para todas las distribuciones...
  - Instalación y actualización del software mediante un sistema de paquetes.
  - Para instalar hay que ser **root**.
  - Si lo hubiere, retirar cualquier control de actualizaciones automáticas (*ISO 27002, control 12.5.1 -dominio 8-*).
  - Mejor probar en desarrollo antes que en producción (*ISO 27002, control 10.1.4 -dominio 6-*).
  - Ventajas del sistema de paquetes:
    - Atomicidad y reversibilidad (como las transacciones de las BBDD).
    - En sistemas de manejo de paquetes de alto nivel, transparencia para el usuario.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Antes de instalar un paquete...

  - Podemos comprobar si ya está instalado,
    - Familia Red Hat: `rpm -qa`
    - Familia Debian: `dpkg -l`

  - Podemos intentar encontrar algún fichero relacionado con el paquete a instalar:
    - Si es un binario, `which <programa>` => Busca en `$PATH`.
    - Para cualquiera, `whereis <fichero>` => Busca en todas partes.
    - Para cualquiera, `locate <fichero>` => Busca en todas partes.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistemas de gestión de paquetes:
  - RPM (“Red-hat Package Manager”).
    - Sistema característico de RHEL, Centos, Fedora y Suse.
    - Los paquetes son ficheros con extensión “`.rpm`”.
    - Herramientas de instalación basadas en línea de comandos:
      - `rpm`: instala y desinstala ficheros “`.rpm`”.
      - `yum`: instala y desinstala telemáticamente el contenido de los paquetes, sin ser necesario el “`.rpm`”.
  - DEB (“DEBian package manager”).
    - Sistema característico de Debian y Ubuntu.
    - Los paquetes son ficheros con extensión “`.deb`”.
    - Herramientas de instalación basadas en línea de comandos:
      - `dpkg`: instala y desinstala ficheros “`.deb`”.
      - `apt-get`: instala y desinstala telemáticamente el contenido de los paquetes, sin que se requiera el “`.deb`”.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Nomenclatura de los ficheros rpm:

  `<Nombre>-<Versión>-<Revisión>.<Arquitectura>.rpm`

  - Ejemplo: `AdobeReader_esp-8.1.7-1.i486.rpm`
  - `<Arquitectura>`: si acaba en `86`, es de 32 bits; si acaba en `86_64`, es de 64.
  - Una vez instalado, el sistema sólo reconocerá el nombre del paquete. Ejemplo:

```
[root@asus Descargas]# ls -l ./AdobeReader_esp-8.1.7-1.i486.rpm
-rw-rw-r--. 1 aaso aaso 52475467 dic 11 00:14 ./AdobeReader_esp-8.1.7-1.i486.rpm
[root@asus Descargas]# rpm -qpi ./AdobeReader_esp-8.1.7-1.i486.rpm
Name        : AdobeReader_esp
Version     : 8.1.7
...
[root@asus Descargas]# rpm -qi AdobeReader_esp
Name        : AdobeReader_esp
Version     : 8.1.7
...
```

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Comando `rpm`:
  - Tiene cinco usos principales:

    `rpm -i <fichero_rpm>` => Instala el contenido de `<fichero_rpm>`.

    `rpm -U <fichero_rpm>` => Actualiza un paquete ya instalado.

    `rpm -e <nombre_paq>` => Elimina el paquete <nombre_paq>.

    `rpm -qp<subopciones> <fichero_rpm>` => Obtiene información de `<fichero_rpm>` (instalado o no).

    `rpm -q<subopciones> <nombre_paq>` => Obtiene información del paquete `<nombre_paq>` (instalado, necesariamente).

  - Ejemplos de uso de `rpm -qp` y `rpm-q`:

    `rpm -qa` => Lista todos los paquetes instalados.

    `rpm -q[p]i <paq>` => Obtiene información sobre un paquete.

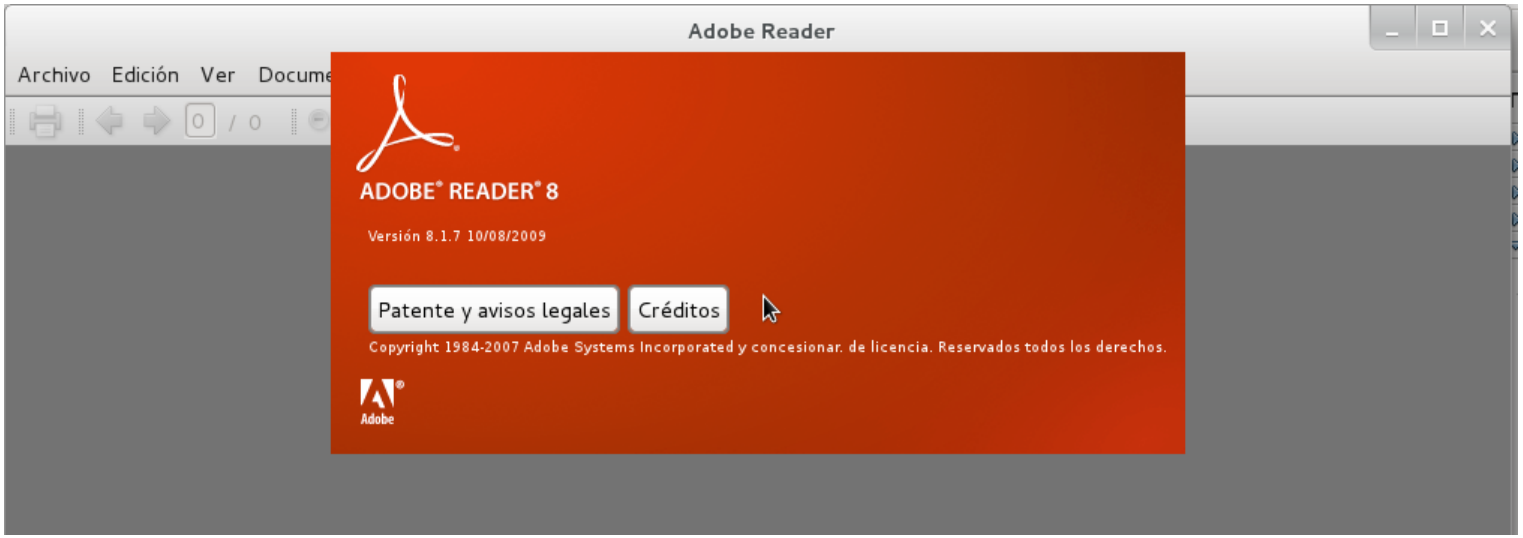
    `rpm -q[p]l <paq>` => Lista los ficheros instalados por un paquete.

    `rpm -qf <fich>` => Indica el paquete del que forma parte un fichero.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Comando `rpm` (cont.):
  - Ejemplos de uso de las opciones `-i`, `-e` y `-U`:

```
[root@asus Descargas]# acroread &
```

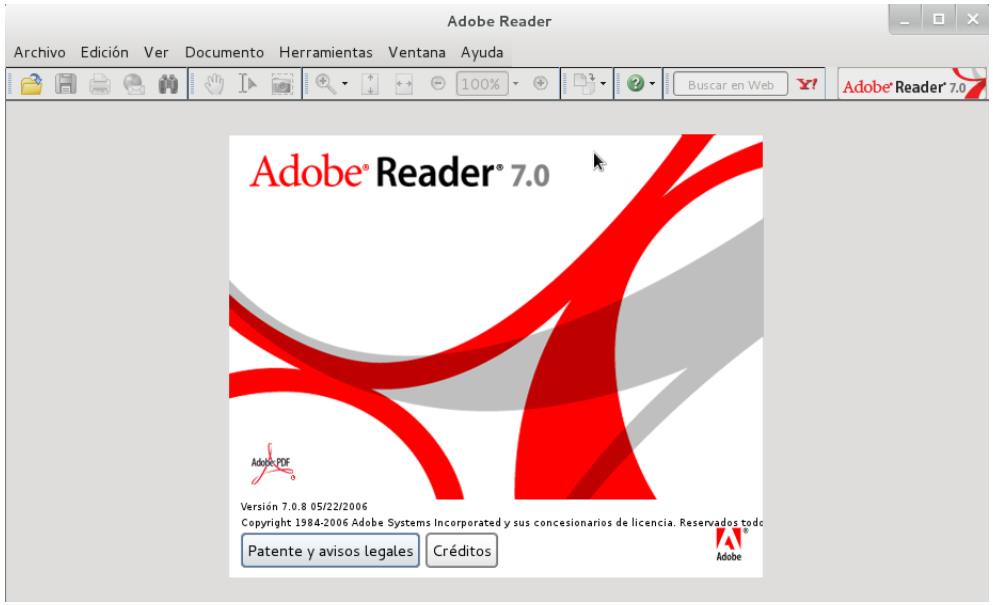



```
[root@asus Descargas]# which acroread
/usr/bin/acroread
[root@asus Descargas]# rpm -qf /usr/bin/acroread
AdobeReader_esp-8.1.7-1.i486
```

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Comando `rpm` (cont.):
  - Ejemplos de uso de las opciones `-i`, `-e` y `-U`:

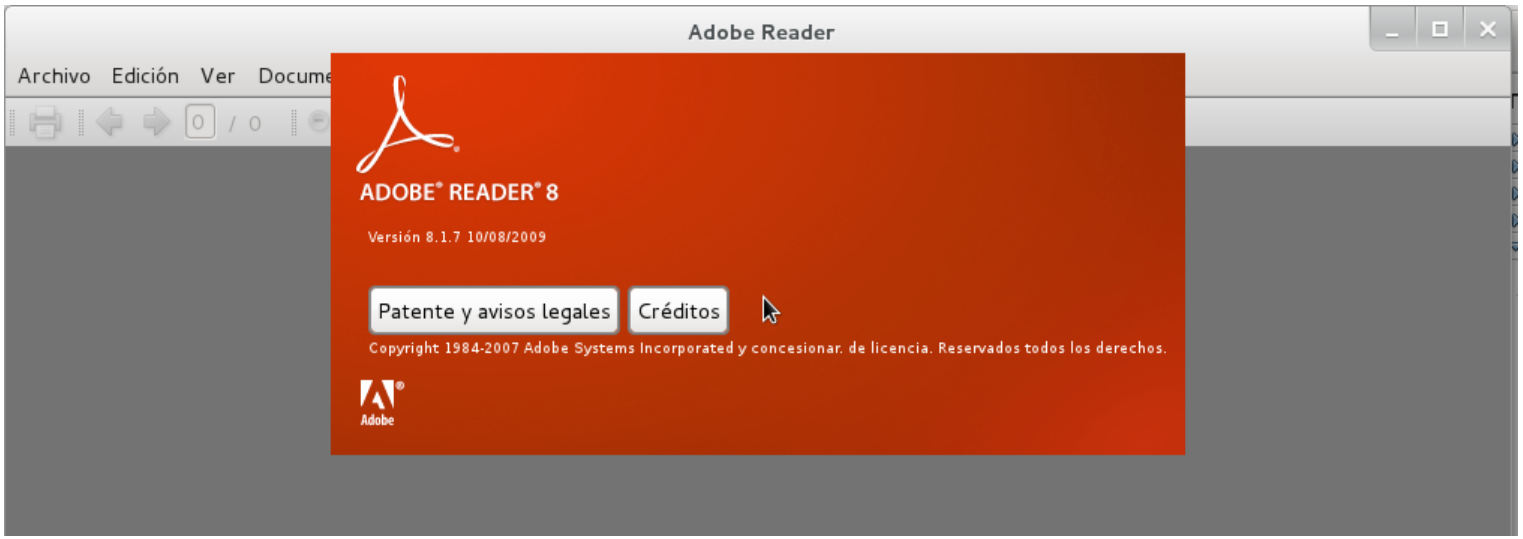
```
[root@asus Descargas]# rpm -e AdobeReader_esp
[root@asus Descargas]# which acroread
/usr/bin/which: no acroread in
(/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin)
[root@asus Descargas]# rpm -i ./AdobeReader_esp-7.0.9-1.i386.rpm
[root@asus Descargas]# acroread &
```



HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

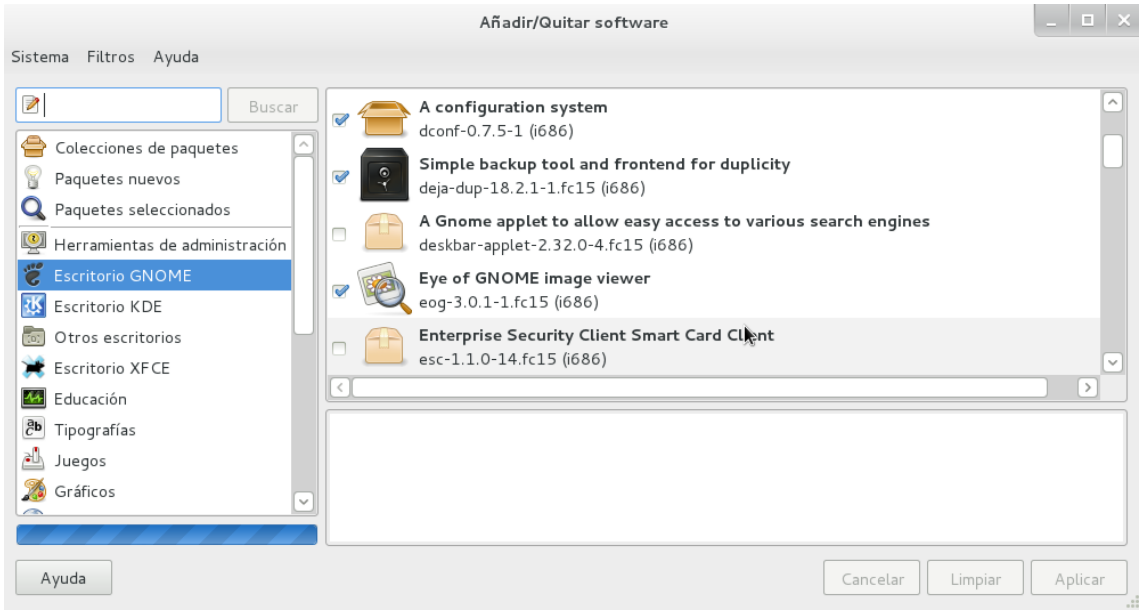
- Comando `rpm` (cont.):
  - Ejemplos de uso de las opciones `-i`, `-e` y `-U`:

```
[root@asus Descargas]# rpm -qf /usr/bin/acroread
AdobeReader_esp-7.0.9-1.i386
[root@asus Descargas]# rpm -U ./AdobeReader_esp-8.1.7-1.i486.rpm
[root@asus Descargas]# rpm -qf /usr/bin/acroread
AdobeReader_esp-8.1.7-1.i486
[root@asus Descargas]# acroread &
```



HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (“Yello Updater Modified”):
  - Sistema gestor de paquetes RPM, basado en un esquema cliente-servidor.
    - Lado servidor: Repositorios de paquetes.
    - Lado cliente:
      - Comando `yum`.
      - Interfaz gráfica `gpk-application` (servicio **packagekitd**).



HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (cont.):
  - Ventajas del sistema YUM:
    - Simplifica la localización y descarga de paquetes.
    - Automatiza el proceso de actualización de paquetes.
    - Resuelve automáticamente las dependencias entre paquetes.
  - Repositorios:
    - En /etc/yum.conf está la configuración del lado cliente.
      - `logfile = /var/log/yum.log`
      - `reposdir = /etc/yum.repos.d`
      - ...

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (cont.):
  - Repositorios:
    - Cada fichero de `/etc/yum.repos.d` con extensión "`.repo`" establece el modo de acceso a un repositorio (o a un grupo de repositorios relacionados).
      - Contenido de `/etc/yum.repos.d/fedora.repos`:

```
[fedora]
name=Fedora $releasever - $basearch
mirrorlist=https://mirrors.fedoraproject.org/metalink
?repo=fedora-$releasever&arch=$basearch
...
```

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (cont.):
  - Comando `yum`:
    - Búsqueda de software en los repositorios:
      - `yum list available` => Búsqueda “bruta”.
      - `yum search <patrón>` => Búsqueda algo más refinada.
      - `yum provides <fich>` => Búsqueda exacta.
    - Información sobre lo que ya tenemos instalado:
      - `yum repolist` => Muestra los repositorios accesibles.
      - `yum list installed` => Muestra los paquetes instalados.
    - Información sobre un paquete en particular (tanto si está instalado como si no):
      - `yum info <paquete>` => Muestra si está o no instalado, y sus características generales.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (cont.):
  - Comando `yum`:
    - Instalación de paquetes:
      - `yum install <paquete> [<paq_sup1> <paq_sup2> ...]`
      - `<paquete>` es sólo el nombre (se excluye la versión, revisión, arquitectura, etc). Se instalará automáticamente la última versión.
      - `<paquete>` puede ser una expresión regular.
    - Actualización de paquetes:
      - Comprobación de actualizaciones: `yum check-update`
      - Implantación de una actualización: `yum update [<paquete>]`
      - Si se omite `<paquete>`, se actualizarán todos los paquetes (**¡cuidado!**).
    - Eliminación de paquetes:
      - `yum remove <paquete> [<paq_sup1> <paq_sup2> ...]`
      - Mismas consideraciones que con `yum install`.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (cont.):
  - Ejemplo: compilación de textos con **latex**.
    - 1. Buscamos paquetes candidatos:

```
[root@asus ~]# yum search latex
Complementos cargados:langpacks, presto, refresh-packagekit
========= N/S Matched: latex =========
dblatex.noarch : DocBook to LaTeX/ConTeXt Publishing
...
texlive-latex.i686 : LaTeX front end for the TeX text formatting system
texlive-texmf-errata-latex.noarch : Errata for texlive-texmf-latex
texlive-texmf-latex.noarch : Texmf files needed for texlive-latex
...
```

    - 2. Una vez localizado un candidato, confirmamos su idoneidad:

```
[root@asus ~]# yum info texlive-latex
Nombre      : texlive-latex
...
Repositorio : fedora
URL         : http://tug.org/texlive/
Licencia    : GPLv2 and BSD and Public Domain and LGPLv2+ and GPLv2+ and LPPL
Descripción : LaTeX is a front end for the TeX text formatting system...
```

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (cont.):
  - Ejemplo: compilación de textos con **latex**.
    - 3. Por último, instalamos el paquete:

```
[root@asus ~]# yum install texlive-latex
Complementos cargados:langpacks, presto, refresh-packagekit
Configurando el proceso de instalación
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Package texlive-latex.i686 0:2007-62.fc15 will be instalado
...
Instalado:
  texlive-latex.i686 0:2007-62.fc15

Dependencia(s) instalada(s):
  kpathsea.i686 0:2007-62.fc15
  ...
  texlive-utils.i686 0:2007-62.fc15

¡Listo!
```

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (cont.):
  - Gestión de grupos de paquetes:
    - Concepto:
      - Conjunto, con entidad propia, de paquetes relacionados.
      - Los paquetes de un grupo pueden ser instalados o eliminados simultáneamente.
      - Ejemplos: **Entorno de escritorio GNOME (gnome-desktop)**, **Java (java)**, **Servidor web (web-server)**, etc.
    - Información sobre grupos:
      - `yum –v grouplist` => Muestra la descripción y el identificador de cada grupo (instalado o no -repositorio-).
      - `yum groupinfo <id_grupo>` => Muestra los paquetes de que se compone un grupo.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Sistema **YUM** (cont.):
  - Gestión de grupos de paquetes:
    - Instalación y desinstalación de grupos:
      - `yum install @<id_grupo>` => Instalación.
      - `yum remove @<id_grupo>` => Desinstalación.

HERRAMIENTAS DE INSTALACIÓN DE SOFTWARE: Linux

- Actualización de software crítico:
  - A ser posible, probarlo antes en otro entorno diferente del de producción.
  - Si lo anterior no es posible y se van a sobreescribir ficheros de configuración, antes hacer copia de seguridad del resultado de `rpm -ql <paquete_a_sobreescribir> | grep -i "/etc/"`.
  - En el caso del paquete `kernel`, (o `kernel-PAE`, si tenemos más de 4 GB de RAM) no actualizar nunca, sino instalar nuevas versiones (**GRUB** lo mostrará como una opción más del menú de arranque).

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Características generales

- Sistemas multiusuario:
  - Adquieren sentido cuando se permiten conexiones telemáticas simultáneas.
  - Cada usuario sólo utiliza de su máquina el teclado, el ratón y la pantalla.
- Requisitos:
  - Se debe mantener el aislamiento entre sesiones.
  - Ha de garantizarse la confidencialidad de la comunicación (*ISO 27002, control 10.6.1 -dominio 6-*).
  - La máquina ha de disponer de suficientes recursos.
- Participantes:
  - Un servidor.
  - Varios clientes.

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Características generales

- Sobre la administración remota...
  - Es sólo una de las posibilidades de los sistemas multiusuario (otras: compartir hardware y/o software entre varios usuarios).
  - Punto de vista del administrador: evita muchas incomodidades.

- Administración remota de Microsoft Windows:
  - Desde clientes Windows: Escritorio Remoto, VNC...
  - Desde clientes Linux: rdesktop, VNC...

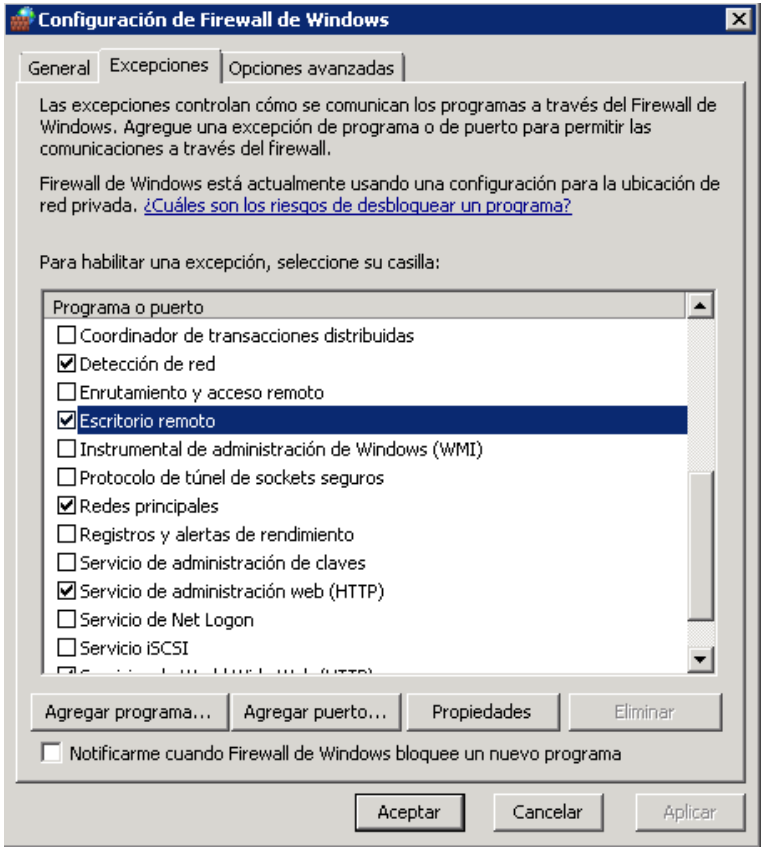
- Administración remota de GNU/Linux:
  - Desde clientes Windows: putty, VNC...
  - Desde clientes Linux: ssh, VNC...

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- rdesktop:
  - Conexiones desde clientes Linux a Windows Server.
  - Se utiliza el protocolo RDP (“Real Desktop Protocol”):
    - Desarrollado por Microsoft.
    - Comunicación cifrada (cifrado simétrico RC4).
    - Puerto utilizado por el servidor: 3389.
  - Requisitos en el cliente:
    - Tener instalado el paquete **rdesktop**.
  - Requisitos en el servidor:
    - Levantar el servicio **Terminal Services**.

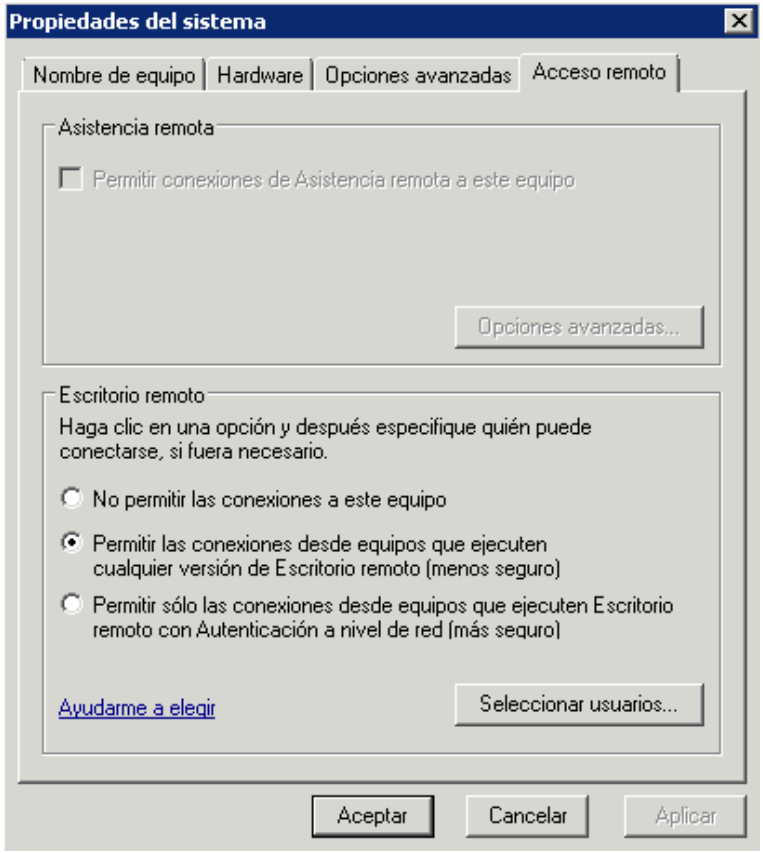
HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- rdesktop (cont.):
  - Requisitos en el servidor:
    - Si está en marcha el cortafuegos, comprobar el puerto 3389.



HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- rdesktop (cont.):
  - Requisitos en el servidor:
    - Evitar la autenticación a nivel de red.



HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- rdesktop (cont.):
  - Conexión desde el cliente:

```
rdesktop  <ip> [-d <dominio>] [-u <usuario>] [-p passw]
          [-a 8|15|16|24] [-f | -g <width>x<height>]
          [-r disk:<dir_en_servidor>=<dir_en_cliente>]
```

Ejemplos:

- Introducción de credenciales en el diálogo de conexión:

```
rdesktop 155.54.225.20
```

- Modo pantalla completa, 16 bits de profundidad de color y nos conectamos como **Administrador**:

```
rdesktop 155.54.225.20 -u administrador -p practicas -a 16 -f
```

- A 1024x768, y nos conectamos como el usuario **alumno** del dominio **aso20.sala27**:

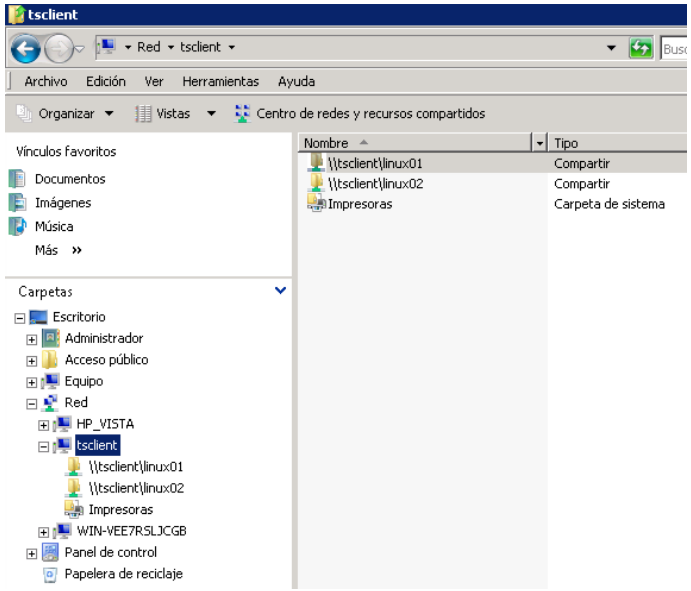
```
rdesktop 155.54.225.20 -d aso20.sala27 -u alumno -p alumno -g 1024x768
```

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- rdesktop (cont.):
  - Ejemplos:
    - Hacemos visibles **/root/winremoto01** y **/root/winremoto02** desde el nodo **tsclient** del explorador de windows del servidor:

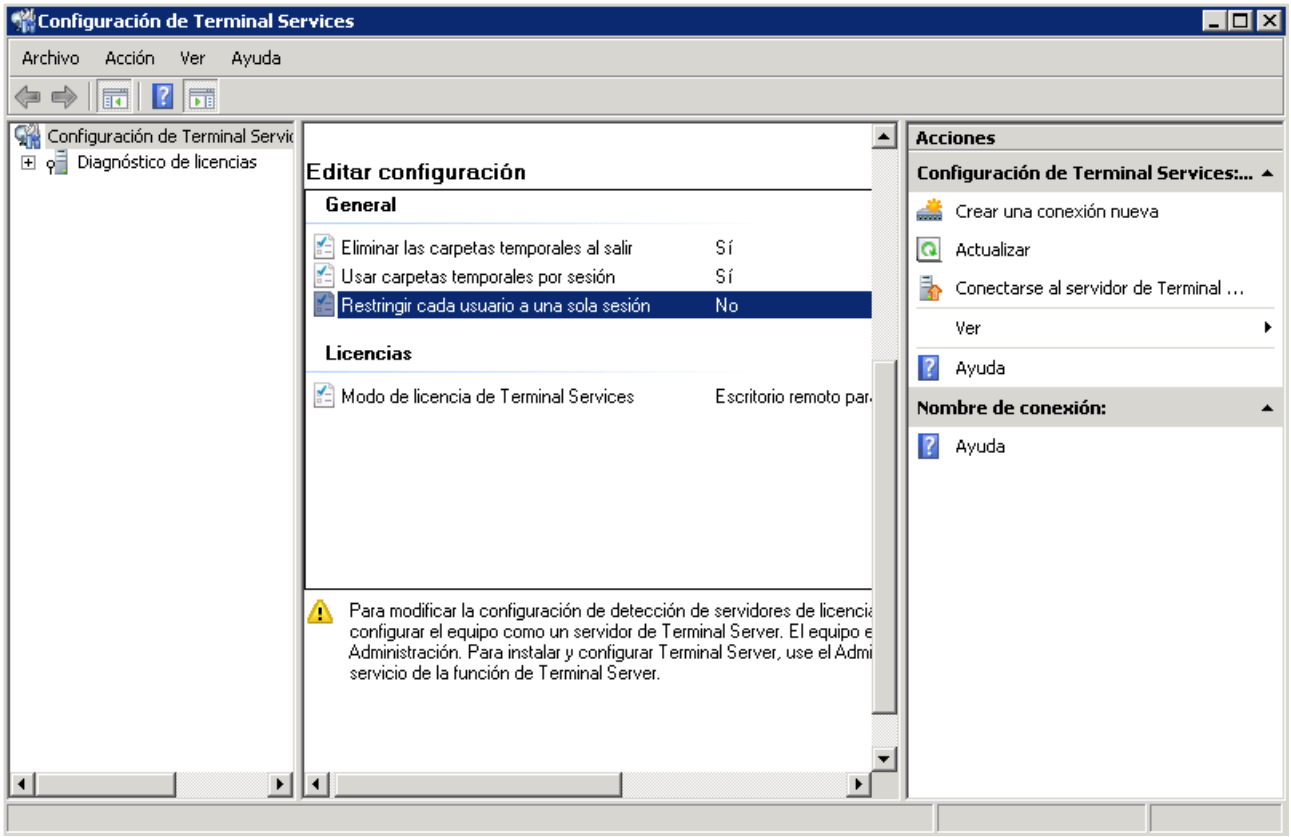
```
rdesktop 192.168.1.245 -u administrador -p practicas -g 1024x768 -a 16
         -r disk:linux01:/root/winremoto01,linux02:/root/winremoto02
```

    - Y en el servidor se observa...



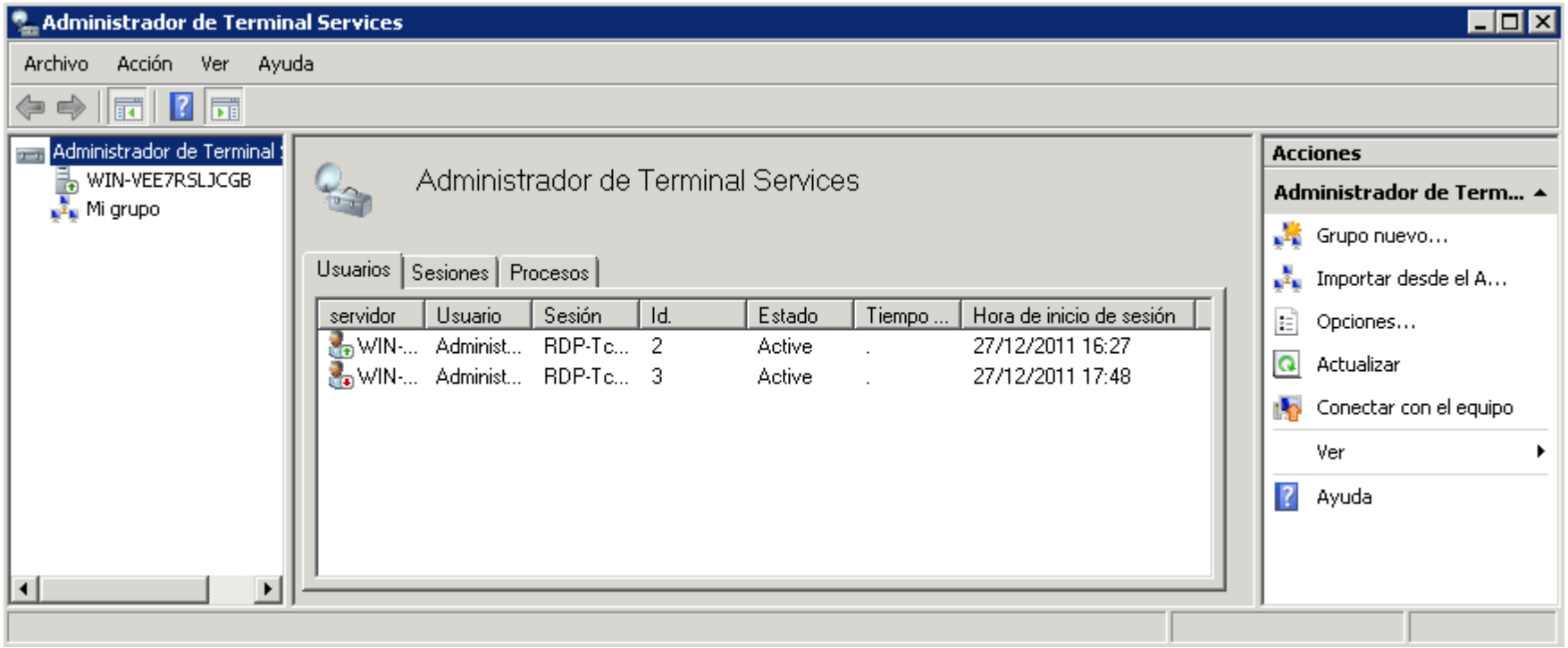
HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- rdesktop (cont.):
  - Configuración del servidor: panel de control – herramientas administrativas – terminal services: **Configuración de Terminal Server**.



HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- rdesktop (cont.):
  - Administración de conexiones: panel de control – herramientas administrativas – terminal services: **Administrador de Terminal Services**.

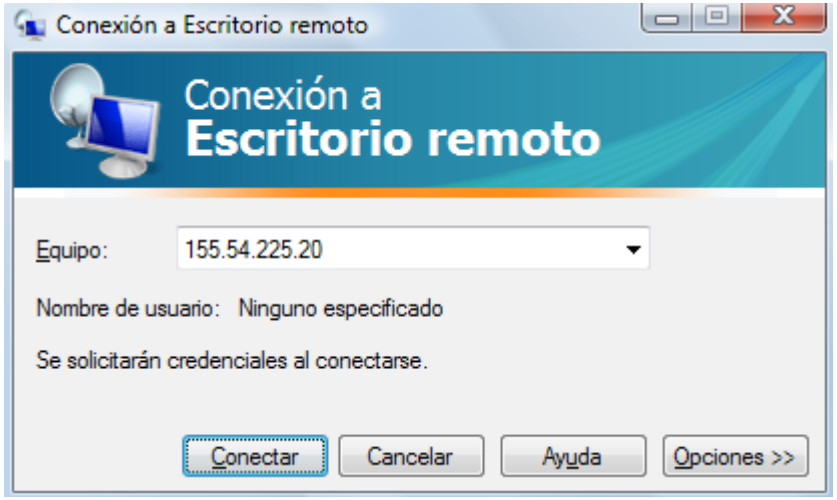


HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- Escritorio Remoto:
  - Conexiones desde clientes Windows a Windows Server.
  - Se utiliza el protocolo RDP.
  - Requisitos del cliente: accesorio **Conexión a Escritorio remoto**.
  - Requisitos en el servidor:
    - Tener en marcha el servicio Terminal Services.
    - Tener abierto el puerto 3389.
    - Permitir las conexiones desde el escritorio remoto, desde la pestaña **Acceso remoto** del diálogo de **Propiedades del sistema**:
      - Hay tres opciones; sólo las dos últimas permiten las conexiones.
      - De esas dos últimas opciones, es preferible la última, la **autentiación a nivel de red**, por su mayor seguridad y menor consumo de recursos en el servidor (recordar que si el cliente es linux, sólo sirve la primera opción).

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

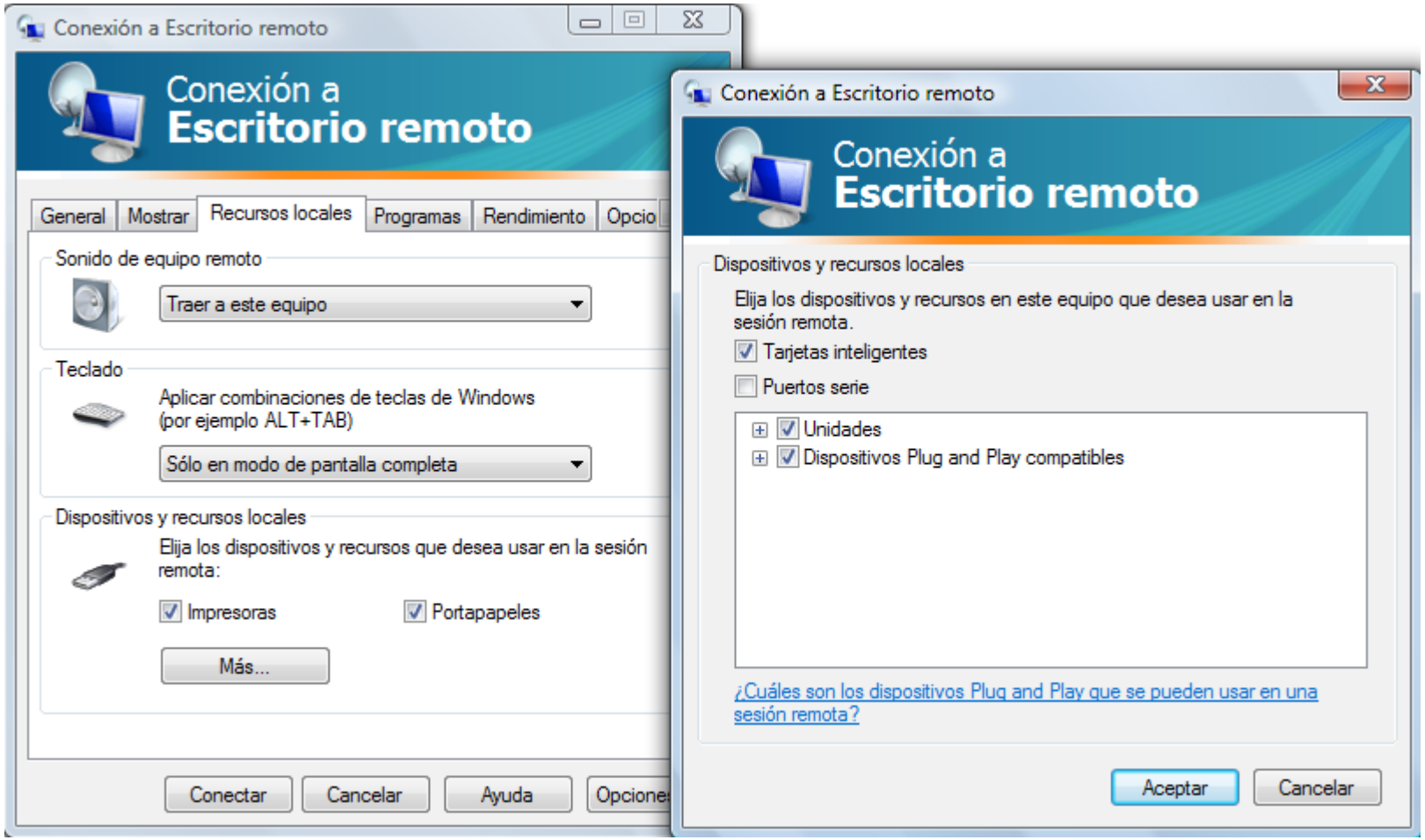
- Escritorio Remoto (cont.):
  - Conexión desde el cliente (Accesorios: Conexión a **Escritorio remoto**).



IMPORTANTE: Si queremos ver desde el servidor los discos de nuestro equipo, hemos de indicarlo en las opciones de conexión (ver imagen siguiente).

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- Escritorio Remoto (cont.):
  - Conexión desde el cliente (opciones de conexión):



HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Windows

- Escritorio Remoto (cont.):

  - Configuración del servidor: panel de control – herramientas administrativas – terminal services: **Configuración de Terminal Server**.

  - Administración de conexiones: panel de control – herramientas administrativas – terminal services: **Administrador de Terminal Services**.

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- ssh / scp:
  - Conexiones desde clientes Linux a Linux.
  - Se utiliza el protocolo SSH (“Secure SHell”):
    - Desarrollado por OpenBSD, e implantado en todas las distribuciones GNU/Linux.
    - Comunicación cifrada (cifrado asimétrico RSA).
    - Puerto utilizado por el servidor: 22.
  - Requisitos del cliente:
    - Tener instalado el paquete **openssh-clients**.
  - Requisitos del servidor:
    - Tener instalado el paquete **openssh-server**.
    - Tener en marcha el demonio **sshd**.

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- ssh / scp (cont.):
  - Requisitos del servidor:
    - Tener abierto el puerto por el que se atienden las conexiones SSH.

```
[root@asus ssh]# cat /etc/sysconfig/iptables | grep 22
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

  - Configuración del servidor (`/etc/ssh/sshd_config`):

```
port 22
Protocol 2
LoginGraceTime 30
PermitRootLogin no
AllowUsers <usuario01>[@<ip01>]
           <usuario02>[@<ip02>] ...
MaxStartups 10
PasswordAuthentication yes
```

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- ssh / scp (cont.):
  - Programas cliente que utilizan el protocolo SSH:
    - `/usr/bin/ssh`: Conexión remota.
    - `/usr/bin/scp` y `/usr/bin/sftp`: Copia remota.
  - Claves RSA utilizadas por SSH:
    - Clave pública: `/etc/ssh/ssh_host_rsa_key.pub` (puede ser leída por todos los usuarios, pero sólo puede ser alterada por **root**).
    - Clave privada: `/etc/ssh/ssh_host_rsa_key` (no puede ser leída ni alterada por ningún usuario, a excepción de **root**).

```
[root@asus ~]# ls -l /etc/ssh/ssh_host_rsa_key.pub
-rw-r--r--. 1 root root 382 nov  5 10:42 /etc/ssh/ssh_host_rsa_key.pub
[root@asus ~]# ls -l /etc/ssh/ssh_host_rsa_key
-rw-------. 1 root root 1679 nov  5 10:42 /etc/ssh/ssh_host_rsa_key
```

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- ssh / scp (cont.):
  - Funcionamiento básico del protocolo SSH:

1. Cuando el programa cliente SSH se intenta conectar a un servidor remoto por vez primera, éste le facilita al cliente su clave pública.

2. El cliente guarda la clave pública del servidor en `$HOME/.ssh/known_hosts` (en sucesivas conexiones, el paso 1 ya no se llevará a cabo).

3. El usuario del servidor se autentica desde el cliente y comienza la comunicación cifrada (el cliente encripta con la clave pública del servidor, y este último desencripta con su propia clave privada).

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- ssh / scp (cont.):
  - Funcionamiento básico del protocolo SSH (ejemplo):

```
[aaso@asus ~]$ ls -l .ssh
total 0
[aaso@asus ~]$ ssh asop@155.54.225.20
The authenticity of host '155.54.225.20 (155.54.225.20)' can't be established.
RSA key fingerprint is c2:b5:4e:9c:4f:33:d1:b5:b0:38:17:09:f3:d8:a2:aa.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '155.54.225.20' (RSA) to the list of known hosts.
asop@192.168.1.36's password:
Last login: Wed Dec 28 18:15:58 2011 from 155.54.225.19
[asop@unknown00123fd08ab3 ~]$ exit
logout
Connection to 155.54.225.20 closed.
[aaso@asus ~]$ cat .ssh/known_hosts
155.54.225.20 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA6OWeLTp5FnMp28OvqZGWeyjfrrT/b5SGAdaIRn...
```

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- ssh / scp (cont.):
  - Conexión remota mediante ssh:

```
ssh   <cuenta_remota>@<maquina_remota>
      [-p <puerto>] [-X]
      [<comando_remoto>]
```

  - Ejemplos:
    - Conexión a la cuenta **alumno** del host **pc20**:

```
ssh alumno@pc20
```

    - Conexión a la cuenta **alumno** y ejecución de un “ls -l”

```
ssh alumno@155.54.225.20 ls -l /home
```

    - Conexión a la cuenta **alumno**, con posibilidad de utilizar aplicaciones gráficas:

```
ssh alumno@pc20 -X
```

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- ssh / scp (cont.):
  - Copia remota mediante scp:

    `scp [-P <puerto>] [-r] <origen> <destino>`

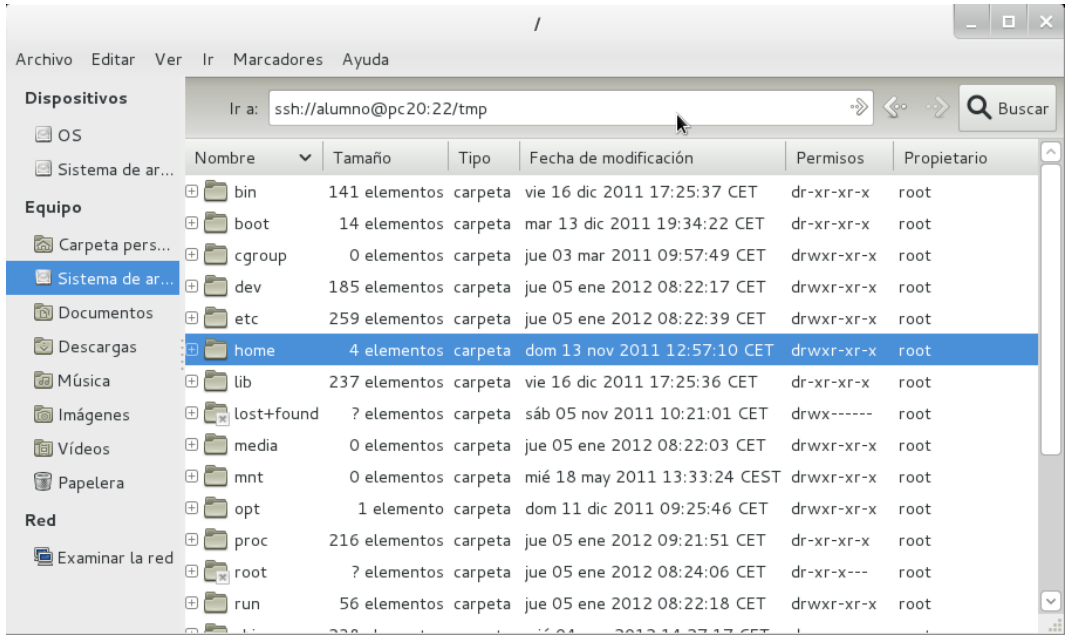
    - Tanto `<origen>` como `<destino>` pueden ser archivos o directorios, y cada uno de ellos ha de estar en una máquina distinta.
    - Para hacer referencia a un elemento (origen o destino) que esté en la otra máquina, debe utilizarse la sintaxis `<cuenta>@<maquina>:<ruta>`.
  - Ejemplos:
    - Copiar, desde un terminal del equipo local, el archivo `dibujos.jpg`, que está en el directorio `Descargas` de la cuenta **alumno** de la máquina remota **pc20**:

      ```
      [alumno@pc19 ~]$ scp alumno@pc20:/home/alumno/Descargas/dibujos.jpg
                       /home/alumno
      ```
    - Copiar, desde un terminal de la máquina remota (al que previamente nos hemos conectado mediante **ssh**), el directorio `Documentos` (y sus subdirectorios) a un directorio temporal del usuario **alumno** de la máquina local (**pc19**):

      ```
      [alumno@pc20 ~]$ scp -r /home/alumno/Documentos
                       alumno@pc19:/home/alumno/tmp
      ```

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- ssh / scp (cont.):
  - Navegación con **Nautilus** sobre el sistema de archivos de una máquina remota:
    - Configurar **Nautilus** para que se muestre la barra de direcciones.
    - Introducir: `ssh://<cuenta>@<máquina>[:puerto/directorio]`
    - Ejemplo: `ssh:alumno@pc20:22/tmp`

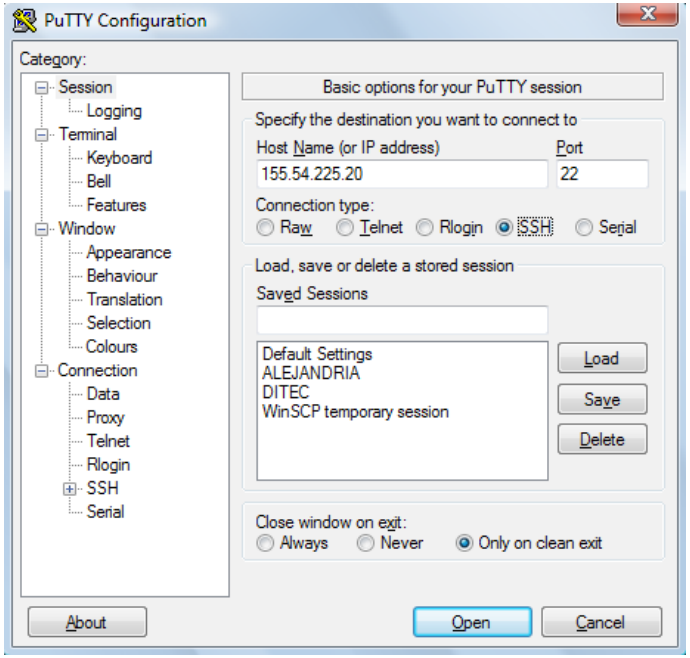


HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- putty / winscp:
  - Conexiones desde clientes Windows a Linux.
  - Se utiliza el protocolo SSH.
  - Requisitos del cliente: descarga e instalación de los programas **putty** / **winscp** (libres).
  - Requisitos del servidor: los ya conocidos (paquete **openssh-server**, demonio **sshd** en marcha, etc).
  - Configuración del servidor: la ya conocida (fichero `/etc/ssh/sshd_config`).
  - Conexión remota:**putty**, similar a **ssh**.
  - Copia remota:
    - **pscp**: similar a **scp**.
    - **winscp**: interfaz gráfica.

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- putty / winscp (cont.):
  - **putty** en... http://www.chiark.greenend.org.uk/~sgtatham/putty
  - Diálogo de conexión de **putty**:



  - En la página de descarga de **putty** también está el programa **pscp**, siendo su sintaxis y funcionamiento idénticos a los de **scp**.

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- putty / winscp (cont.):
  - Ejecución de aplicaciones gráficas con **putty**:
    - Condiciones:
      - En el servidor:
        - En `/etc/ssh/sshd_config`, comprobar lo siguiente: `X11Forwarding yes`
      - En el cliente:
        - Tener instalado un servidor X11 (**xming**, por ejemplo).
        - En el diálogo de conexión de **putty**, activar el checkbox **Enable X11 forwarding** (**Connection – SSH – X11**).
    - Cómo ejecutar las aplicaciones gráficas: tecleando sobre el terminal **putty** el nombre de la aplicación (`firefox &`, por ejemplo).

HERRAMIENTAS DE ADMINISTRACIÓN REMOTA: Conexión a Linux

- putty / winscp (cont.):
  - **winscp** en... http://winscp.net
  - Permite la copia de archivos entre Linux y Windows mediante una intefaz gráfica.