



Ajuntament de Villalba Soleada: Disseny de la infraestructura informàtica

Sergio Morente Fernández

Treball Final de Carrera



Aquesta obra es troba sota [licència Creative Commons Atribució-CompartirIgual 3.0 Unported.](#)

Es permeten la lliure distribució i la creació d'obres derivades sempre que es respecti l'autor i es mantingui la llicència.

*“Les úniques persones que tenen alguna cosa per témer
el programari lliure són aquells els productes dels quals
tenen un valor encara menor.”*

David Emery

Índex

1. Introducció	7
1.1 Objectius.....	8
2. Requisites de maquinari	9
2.1 Estacions de treball.....	9
2.2 Impressores.....	12
2.3 Còpies de seguretat.....	14
3. Xarxa	15
3.1 Disseny físic.....	15
3.2 Polítiques de seguretat.....	18
4. Requisites de programari de les estacions	19
4.1 Sistema operatiu.....	19
4.2 Eines ofimàtiques.....	25
4.3 Clients d'aplicacions.....	29
Navegador web.....	29
Client d'impressió.....	31
Client VPN.....	32
Client LDAP.....	33
Client Kerberos.....	34
4.4 Còpies de seguretat.....	36
4.5 Antivirus.....	37
5. Requisites de programari als servidors	39
5.1 Sistema Operatiu.....	40
Debian.....	40
Ubuntu.....	40
RHEL (Red Hat Enterprise Linux).....	40
CentOS (Community Enterprise Operating System).....	40
SLES (SuSE Linux Enterprise Server).....	40
5.2 Servidor de fitxers i d'impressió.....	41
5.2 Sistema gestor de Bases de Dades.....	42
5.3 Servidor d'aplicacions.....	43
5.4 Servidor web.....	44
5.5 Servidor de correu.....	45
5.6 Servidor DNS.....	46
5.7 Autenticació i seguretat: VPN, LDAP i Kerberos.....	46
5.8 ERP.....	47
6. Fase d'implantació	48
Primera fase: Migració dels servidors.....	48
Segona fase: Creació de l'estació model i proves.....	49
Tercera fase: Clonació de l'estació model.....	49

7. Manteniment i actualitzacions	50
8. Pla de formació als usuaris	53
9. Web Interna	56
10. Web del municipi	58
11. Conclusions	59
12. Bibliografia	61

1. Introducció

L'ajuntament de Villalba Soleada vol modernitzar la infraestructura informàtica de les quatre seus de les que disposa. Degut a la difícil situació econòmica a la que es troba sotmès, el ple de l'ajuntament vol que aquest projecte sigui realitzat en la seva totalitat en programari lliure, optimitzant així els recursos del contribuent.

El món del programari lliure mica en mica va prenent força, i actualment existeix una àmplia varietat de productes destinats a un nombre cada cop més gran de màquines, ja siguin ordinadors de sobre-taula, portàtils, servidors, netbooks, tablets, smartphones, etc. A més, han sentit a parlar de diversos projectes similars, com el dut a terme a les administracions d'Extremadura i Saragossa amb bons resultats quant a rendiment, eficiència, seguretat i cost.

Aquest projecte té un abast relativament gran, ja que es tractarà de desenvolupar tota la infraestructura informàtica del consistori, el que inclou maquinari, programari i xarxa. També ha d'incloure altres aspectes, no menys importants, com són definir les polítiques de seguretat d'accés als arxius i xarxes, polítiques de manteniment i actualitzacions tant de maquinari com de programari i cursos de formació als usuaris.

S'hauran d'unificar tots aquests aspectes per tal de dotar de funcionalitat una web interna a que farà de punt d'accés al sistema per a la tasca diària dels empleats, és a dir, la intranet de l'organització.

Existeixen altres requisits en la funcionalitat demanada que s'aniran veient al llarg d'aquest treball.

Abans de continuar, fem una breu pinzellada sobre què és GNU/Linux. D'una banda, Linux és el nucli o *kernel* d'un sistema operatiu, i és l'encarregat d'aportar la funcionalitat entre el maquinari i el programari. Va ser dissenyat pel finlandès Linus Torvalds als anys 90, i actualment gaudeix d'una certa maduresa que li aporta estabilitat, versatilitat i seguretat. D'altra banda, el projecte GNU (*GNU is Not Unix*) forma part de la *free software foundation (FSF)*, una fundació encapçalada per Richard Stallman i que té com a principal objectiu el desplegament de programari de codi obert. Aporta a Linux tota la funcionalitat que no forma part del nucli, i per aquest motiu sempre se'ls anomena de manera conjunta. En conjunt, també es diu que GNU/Linux descendeix de UNIX. De fet, és un clon que manté compatibilitat amb UNIX.

La FSF també manté les llicències sota les quals es publica el programari lliure, la més comuna de les quals, i en la que ens basarem quan cerquem programari en aquest treball, és la coneguda GPL. Aquesta permet la lliure distribució del programari, estudiar el codi font, modificar-lo, etc.

1.1 Objectius

L'objectiu principal d'aquest projecte és dotar, almenys de manera teòrica, l'hipotètic ajuntament de la infraestructura informàtica que satisfaci els requeriments esmentats a l'enunciat. Es farà seguint criteris d'eficiència, flexibilitat, seguretat i cost. Evitant el pagament per llicències, el cost sempre tendirà a ser el mínim possible, que és el de l'adquisició del maquinari.

Aquest projecte implica la unió dels conceptes adquirits al llarg de tota la carrera d'Enginyeria Tècnica en Informàtica de Sistemes, en concret de les assignatures de sistemes operatius, xarxes, estructura de xarxes de computadors, seguretat de xarxes de computadors, i administració de xarxes i sistemes operatius.

No és l'objectiu, però, aprofundir massa en la tria de maquinari o programari degut a la rapidesa en què aquests canvien, i en la varietat que existeix en el mercat actual. A més, és un camp en el que la experiència és un factor determinant.

2. Requisits de maquinari

Per definir la infraestructura informàtica del consistori podem començar per identificar les necessitats de maquinari de les estacions de treball per després continuar amb l'estructuració de la xarxa. Per últim caldria integrar tota la funcionalitat del sistema amb el programari adient.

Com es pot preveure, existeixen milions de possibilitats en la tria de maquinari existent en el mercat. Aquest apartat no tractarà d'analitzar totes i cadascuna de les opcions per veure quina n'és la millor, sinó que ens centrarem en trobar-ne una que s'adapti el millor possible als requisits de l'enunciat.

2.1 Estacions de treball

La part més visible de tot el sistema informàtic són les estacions de treball, i suposem que volen canviar totes 100 estacions per màquines més modernes. Probablement podrien aprofitar-ne algunes d'elles ja que, tal com veurem més endavant, els sistemes GNU/Linux consumeixen pocs recursos i moltes podrien ser encara funcionals amb només 500 MB de memòria RAM i un disc dur de pocs *Gigabytes*.

Pel que fa als requisits de les estacions de treball, sabem que per realitzar la seva tasca diària, els empleats necessiten disposar de connectivitat amb els servidors interns, eines informàtiques i accés a recursos d'impressió. Un ordinador de sobretaula de gama mitjana pot ser més que suficient per satisfer aquests requisits. Es busquen màquines amb les següents característiques:

- Doble nucli
- Disc dur no gaire gran (la informació de l'ajuntament es guardarà al servidor per facilitar les còpies de seguretat)
- RAM 2 GB
- Targeta de xarxa
- Teclat i ratolí inalàmbric
- Monitor. Si és possible de LED (preu similar a TFT i menys consum)
- Targeta de vídeo compatible amb OpenGL.
- Lector de targetes intel·ligents per autenticació al sistema i signatures digitals (DNIe,...)

Es mostra una proposta de maquinari que compleix els requisits anteriors¹:



PC HP 500B microtorre [WU362EA]	
Compre ahora	
Precio €238 IVA no inc LLame al 902 234 468 para consultar opciones de compra	
Sistema operativo instalado	FreeDOS
Actualización de software recomendada	
Tipo de procesador	Procesador Intel® Celeron® Dual-Core E3400 (2,60 GHz, 1 MB de L2 caché, FSB 800 MHz)
Memoria de serie	SDRAM DDR3 de 2 GB 1333 MHz
Descripción de unidad de disco duro	320 GB 7200 rpm SATA 3 Gb/s
Unidades ópticas	Grabadora SATA SuperMulti DVD
Gráficos	Intel Graphics Media Accelerator 4500 integrado
Interfaz de red	Realtek RTL8103EL 10/100 Ethernet integrado Escritorio CT Gigabit Intel



**Monitor LCD iluminado WLED
HP x20LED de 50,8 cm (20")**

Ajustable

Cumplimiento

Rendimiento

enfoque de coste total de propiedad

**precio
€124 IVA no inc**

¹ Nota: S'ha triat el fabricant Hewlett-Packard degut a que és dels pocs que donen opció de compra amb programari lliure, sense cap versió de Windows pre-instal·lada. El preu es podria modificar si es féssin descomptes per volum.

Kits de teclado y ratón



[Ampliar imagen:](#)

Teclado inalámbrico y ratón de 2,4 GHz HP NB896AT

Nombre del producto Teclado inalámbrico y ratón de 2,4 GHz HP

Compatibilidad: [Ver lista completa de compatibilidad](#)

Precio
€25 IVA no inc

1 **Comprar en HP**

Entrega en cuatro semanas

**Características**

- Lector DNI electrónico USB
- Compatible con tarjeta ONA
- Lector/grabador universal de tarjetas inteligentes
- Detección automática al introducir y extraer la tarjeta
- Protocolos de comunicación soportados T=0 y T=1
- Compatible ISO-7816/1/2/3
- Certificado Microsoft WHQL, CE, EMV
- Compatible estándares API PC/SC, CSP y API PKCS#11
- Interfaz USB FullSpeed
- Sistemas operativos: Windows 98SE, Me, 2000, XP, 2003, Vista, Linux y MacOS 10.1, 10.2, 10.3, 10.4 y 10.5
- Instalador único para todos los sistemas operativos de Windows

Precio del lector dni 18,90 € (Iva no incl.)

[Solicitar más información](#)
902 170 600

Adreces

Torre: <http://h10010.www1.hp.com/wwpc/es/es/sm/WF06b/12454-12454-64287-3328893-3328893-4191793-4311939.html>

Monitor: <http://h10010.www1.hp.com/wwpc/es/es/sm/WF05a/382087-382087-64283-3923064-3923064-4190100.html>

Teclat+ratolí: http://h10010.www1.hp.com/wwpc/es/es/sm/WF2833c/A1-329290-69998-12454-12454-296719-4050763-4050763-3429268-3811362.html?jumpid=reg_R1002_ESES

DNIe: <http://www.dnielectronico.eu/>

I si alguns dels empleats volen tenir mobilitat dins l'edifici poden optar per aquest portàtil, demanant expressament que es vol sense sistema operatiu o amb SUSE Linux Enterprise 11.



PC portátil HP 630

Portabilidad	<input type="checkbox"/>
Vida batería	<input type="checkbox"/>
Conectividad	<input type="checkbox"/>
Rendimiento	<input type="checkbox"/>
Seguridad.	<input type="checkbox"/>

Windows® 7 Professional 64 [original](#)
 Windows® 7 Home Premium 64 [original](#)
 Windows® 7 Home Basic 64 [original](#)
 Windows® 7 Starter 32 [original](#)
 SUSE Linux Enterprise 11

Intel® Core™2 Duo
 Procesador Intel® Pentium®
 Intel® Celeron®

Ampliable a 8 GB

SATA II (7200 rpm)
 Hasta: 250 GB
SATA II (5400 rpm)
 Desde: 320 GB
 Hasta: 500 GB

39,6 cm (15,6 pulg.)

Integrados: Acelerador de Medios Gráficos Intel 4500MHD, Gráficos HD Intel®
 Discreto: Gráficos AMD Radeon HD 6370M con 512 MB de memoria de vídeo dedicada

**desde
 €375 IVA no inc**

Red: Puerto Realtek Ethernet (NIC de 10/100 o 10/100/1000)

Tecnologías inalámbricas: Atheros 802.11b/g/n Bluetooth 3.0 combinado

Font: <http://h10010.www1.hp.com/wwpc/es/es/sm/WF06b/321957-321957-64295-3955548-3955548-5086782-5109762.html>

2.2 Impressores

En principi no sabem de les necessitats quant a impressió de l'ajuntament per fer estimacions del nombre necessari de màquines. Es podria suposar que no necessitaran més d'una impressora per cada 10 estacions, o bé un parell per planta, alternant entre impressores làser, més ràpides i econòmiques de mantenir, i d'injecció de tinta -més qualitat i capacitat d'imprimir en color. El que sí que sabem és que tot empleat n'ha de tenir accés, almenys a les de la seva planta. Es poden connectar totes directament a la xarxa interna si disposen de targeta Ethernet o connectivitat wi-fi i configurar-ne només un parell a cada estació de treball.

Per evitar posteriors malsons de configuracions posteriors, podem consultar un llistat d'impressores compatibles amb GNU/Linux(i descarregar els controladors si cal) a la pàgina <http://www.linuxfoundation.org/OpenPrinting> o bé a <http://www.openprinting.org> . Si tenim el sistema operatiu instal·lat, abans de decidir-nos també pot ser d'utilitat consultar un llistat de fabricants i models d'impressores que ja suporta el sistema obrint l'arxiu `/usr/share/doc/package/ghostscript-library/catalog.devices`

Fent un cop d'ull a la pàgina d'HP, per aprofitar els possibles descomptes per volum, podem trobar un parell de propostes: una impressora multifunció làser -impressió, còpia i escàner- i una d'injecció de tinta.

Impresora HP LaserJet Pro serie M1132 multifunció



Compre ahora

Precio
€142
IVA no inc

**LLame al 902 234 468 para
consultar opciones de compra**

Adreça: http://h10010.www1.hp.com/wwpc/es/es/sm/WF05a/18972-18972-3328064-3328082-3328082-3965842.html?lang=es&jumpid=oc_R1002_ESESC-001_Impresora_multifuncin_HP_LaserJet_Pro_M113

Controladors: <http://hplipopensource.com/hplip-web/index.html>

Impresora HP Officejet Pro serie 8000



**Comprar en HP:
desde
€126 IVA no inc**

Adreça: http://h10010.www1.hp.com/wwpc/es/es/sm/WF06a/18972-18972-236251-3328074-3328074-3760400.html?jumpid=reg_R1002_ESES

Controladors: <http://hpoj.sourceforge.net/>

2.3 Còpies de seguretat

A la sala dels servidors s'hi pot instal·lar una unitat de *backup* d'alta capacitat d'emmagatzematge per evitar pèrdues accidentals d'informació.



HP Storageworks Ultrium 1760

3. Xarxa

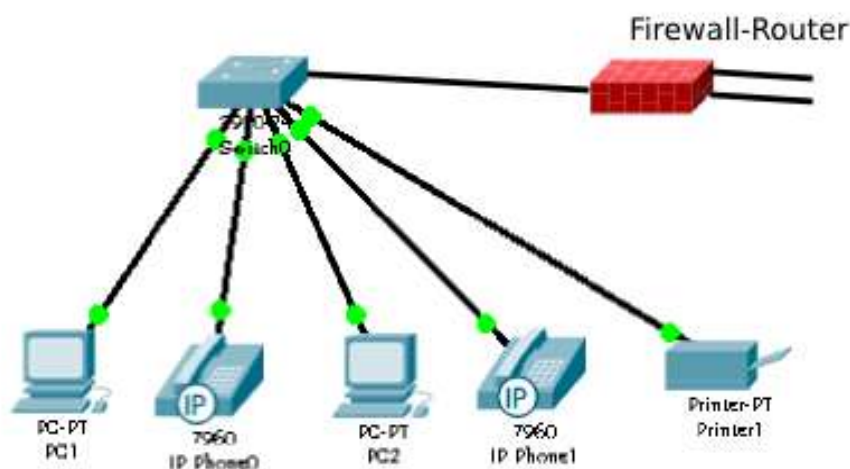
En aquest apartat veurem un disseny bàsic possible de la xarxa interna del consistori. Es dotarà l'organització de connectivitat, de manera que els empleats puguin compartir informació i recursos de manera segura entre totes les màquines de la xarxa interna, el que probablement augmentarà de manera considerable la productivitat dels empleats de l'organització pública.

No ens entretindrem gaire en els detalls del maquinari que implementa les xarxes locals, ja que ens diuen que l'ajuntament ja disposa d'una infraestructura funcional, i molt probablement, similar a la que aquí descriurem. Així, en la mesura que sigui possible, es reaprofitaran els concentradors, commutadors, punts d'accés, racks, firewalls, telèfons per veuIP i servidors de manera que el presupost en la migració del sistema es mantingui sempre el més baix possible. De tota manera, a nivell de xarxa ja no importa tant mantenir la homogeneïtat en el maquinari com era el cas de les estacions de treball, ja que, donat el cas que s'hagi de canviar una peça, aquesta es pot canviar sense afectar la resta.

3.1 Disseny físic

Un disseny força estès per connectar màquines dins un mateix edifici és el següent: un o diversos commutadors (*switch*) ubicats en un armari a cada planta als quals s'hi connecten les estacions de treball, els telèfons per veuIP i les impressores, i si es considera necessari, un punt d'accés per activar la connectivitat sense fils. Aquests *switch*s es connecten a l'altre extrem a un armari central a través d'un *backbone* de fibra òptica, i aquest a l'encaminador principal que serà l'encarregat de la connectivitat amb l'exterior.

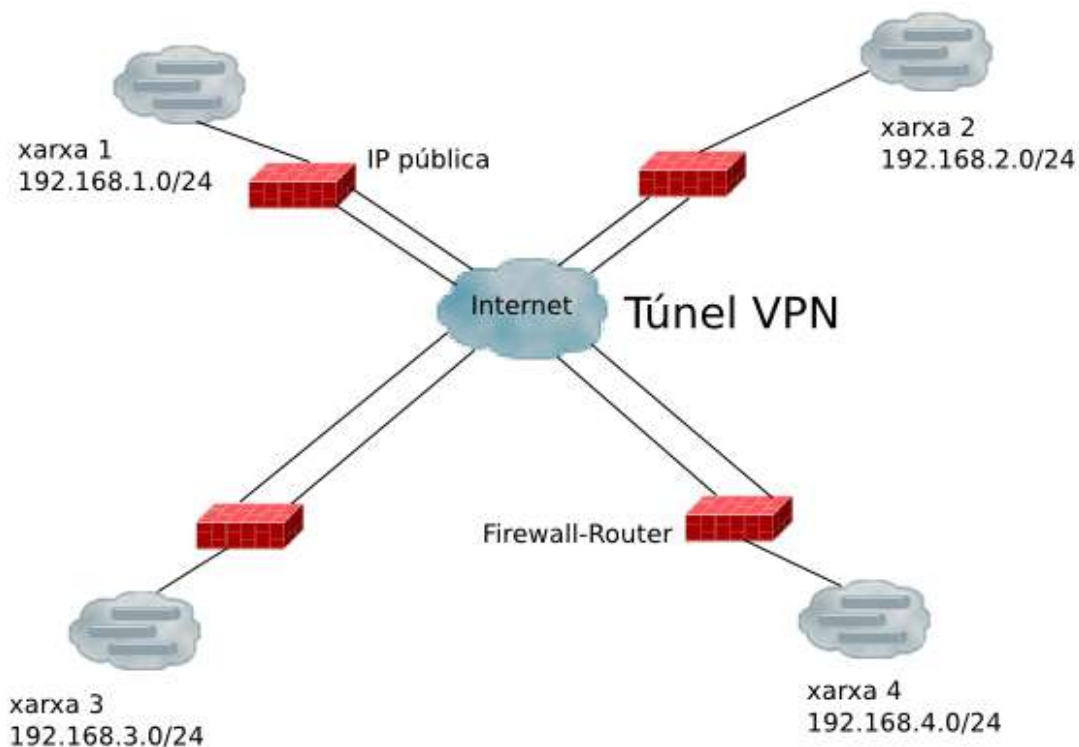
Es pot fer servir aquest mateix disseny per les quatre seus, amb l'excepció que un a d'elles haurà d'incloure els servidors. Podem veure'l de manera esquemàtica al gràfic següent:



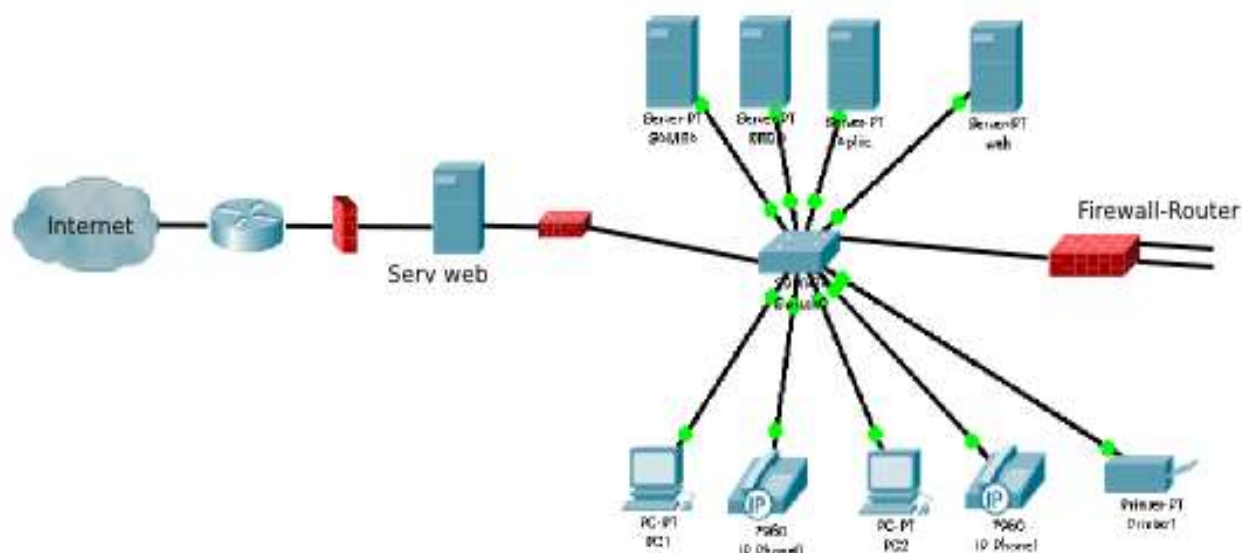
Ara cal connectar les quatre xarxes locals(LAN) entre elles per a què tots els empleats puguin tenir accés als recursos del consistori. Per fer-ho, s'opta per fer servir línies ADSL, aprofitant la infraestructura pública. D'aquesta manera no s'ha d'implementar cap línia dedicada, ni connectar directament per mòdem. Aquestes dues darreres opcions tindrien un cost major i no serien pas més eficients.

En aquest cas, cal emprar algun mecanisme de protecció addicional, ja que part de la informació que viatjarà entre els edificis es pot considerar sensible(dades de tributació, comptes bancaris de proveïdors o ciutadans, etc.) i recordem que ho farà per un canal insegur com és Internet. Per solucionar-ho, les seues faran servir encaminadors amb un firewall configurat per què creï túnels VPN. VPN són les sigles de xarxa privada virtual(*Virtual Private Network*) i consisteix en encapsular i xifrar tota la informació que viatja entre dos encaminadors configurats, a mode de túnel.

Per establir la VPN, cal que almenys un dels encaminadors tingui una adreça IP pública fixa per a què la resta d'encaminadors puguin crear el tunel per l'altre extrem. Un avantatge d'aquesta tecnologia és que un cop s'han establert els túnels, les quatre xarxes funcionaran a nivell lògic com si fossin una de sola, el que simplificarà la gestió de la seguretat. Podem veure aquesta infraestructura en l'esquema següent:



Abans s'ha avançat que una de les seus ha de allotjar els servidors. Seguint el disseny de les altres seus, aquests es poden connectar directament als commutadors sense cap protecció extra, amb una excepció, el servidor web de la web del municipi, tal com es pot veure en la figura següent:



El servidor de la web del municipi s'ha de col·locar fora de la VPN, perquè en cas contrari, els ciutadans necessitarien conèixer les claus de connexió per accedir-hi. A més, en cas de rebre moltes peticions, es podria arribar a col·lapsar la xarxa interna. A la figura veiem que aquest servidor es col·loca entre dos tallafocs, dins el que s'anomena una zona desmilitaritzada (DMZ). Aquesta estructura és útil en xarxes que disposen de servidors accessibles des d'Internet. El primer tallafoc, el més extern, protegeix la xarxa d'accessos hostils, però ha de permetre la connexió del servidor amb l'exterior. El segon tallafoc fa de barrera extra per als atacs amb destinació a la xarxa interna del consistori.

A la figura també es pot observar que aquesta és la única seu que disposa d'un punt d'accés a Internet (en crear els túnels VPN, els altres encaminadors han perdut aquesta capacitat). Aquest fet simplificarà la configuració de els tallafocs, amb l'inconvenient que aquests seran un punt clau en la seguretat de tot el sistema.

3.2 Polítiques de seguretat

Aquest és un bon moment per definir les polítiques de seguretat per implementar les que calgui a nivell de xarxa. En principi tots els empleats poden accedir a tots els servidors a nivell de xarxa, i seran els servidors els que gestionaran l'accés per grups o usuaris als recursos, com es veurà més endavant. A nivell de xarxa ens interessa més protegir la connexió a i des d'Internet, que és la principal font hostil. Aquestes polítiques es poden implementar als dos tallafocs que envolten el servidor web, amb l'ajut de programari adequat, com per exemple, *iptables*.

El més adient seria implementar una política restrictiva, és a dir, els tallafocs han d'impedir tot el trànsit excepte aquell que estigui explícitament autoritzat. Sense entrar gaire en detalls sobre adreces IP i ports, els quals poden canviar mentre es va implementant el sistema, els tallafocs han de filtrar tots el transit excepte:

- Les peticions al servidor de la web del consistori als ports http i https (tallafoc extern)
- Connectivitat entre el servidor de la DMZ i el servidor d'aplicacions per permetre tramitacions via internet. (tallafoc intern)
- Comunicació amb el servidor de correu. S'han de permetre correus professionals de i cap a l'exterior (tots dos tallafocs)
- Navegació web només per a determinats usuaris, aquells que no treballin cara el públic, el que es pot fer amb *subnetting*, col·locant-los en un rang d'adreces IP determinat (tots dos tallafocs)
- Port de gestió remota d'escriptori per ssh, en cas que l'assistència tècnica sigui externa (tots dos tallafocs)

4. Requisites de programari de les estacions

Recordem que els treballadors de l'ajuntament no necessiten una gran potència de càlcul ni un gran emmagatzematge per realitzar la seva tasca diària. La tria del programari es pot fer seguint criteris de popularitat, facilitat d'ús o seguretat i no tant per requeriments de maquinari.

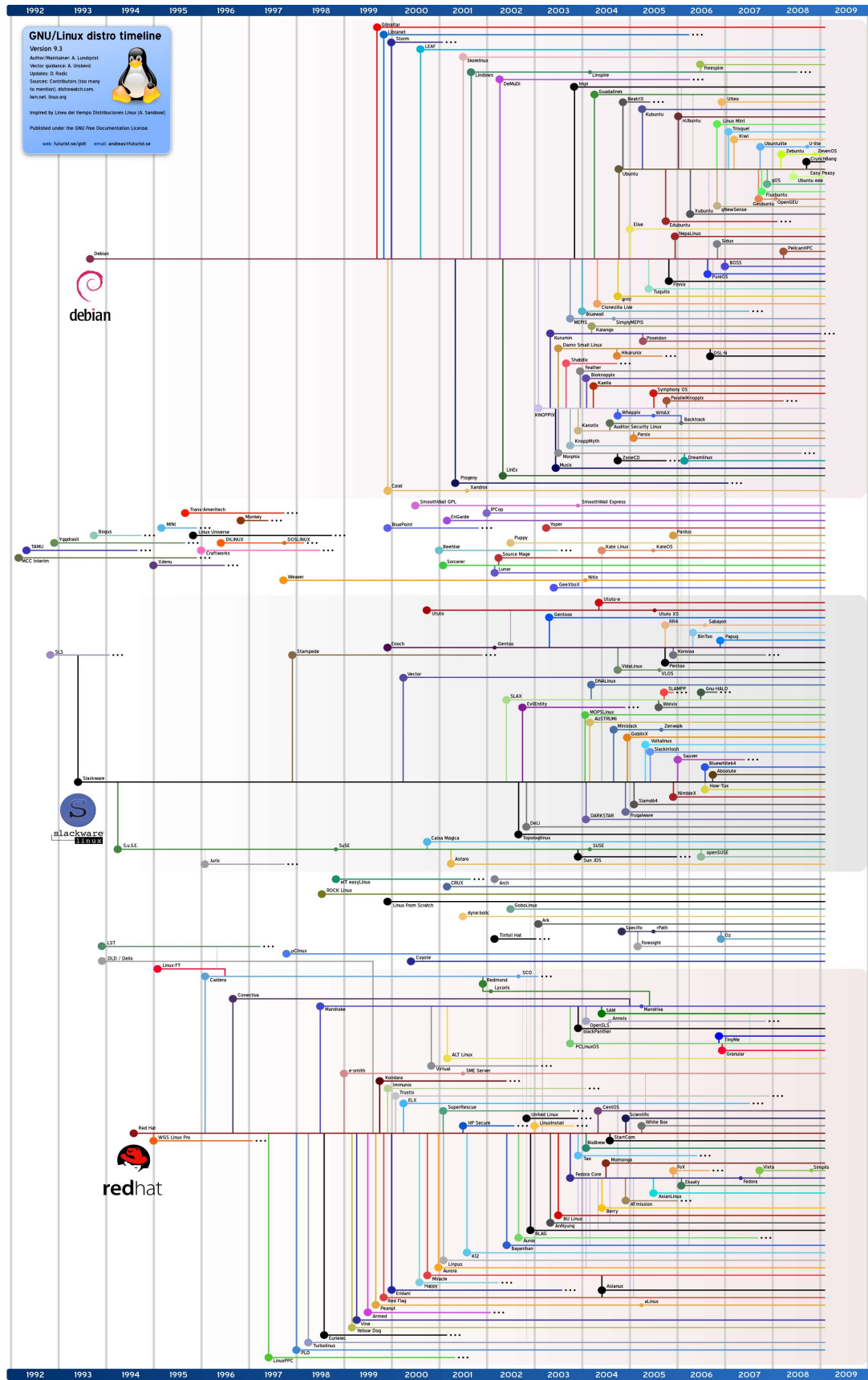
En aquest apartat analitzarem, sense entretenir-nos gaire en els detalls tècnics de les seves configuracions, les principals aplicacions que s'hauran d'instal·lar a cada estació de treball i que donaran la funcionalitat bàsica a les màquines dels treballadors. Bàsicament són les següents:

- Programari base: Sistema Operatiu
- Eines ofimàtiques: openOffice/LibreOffice
- Accés al portal intern: Navegador Mozilla Firefox
- Funcionalitat d'impressió: client CUPS
- Accés a la xarxa interna: client VPN
- Autenticació a la xarxa interna: clients LDAP i Kerberos

4.1 Sistema operatiu.

Tenim clar que volem instal·lar GNU/Linux a les estacions de treball, però un dels grans avantatges -o inconvenients, segons es miri- es l'elevada varietat de formes, aparences, programari i funcionalitats en les que es presenta. Cal triar una d'aquestes combinacions de característiques o programari, conegudes com distribucions o *distros* que s'adeqüi a les necessitats dels treballadors. Com es veurà en aquest apartat, triar-ne la que millor s'adapti a la funcionalitat demanada a l'enunciat pot arribar a estalviar molta feina en el moment de fer les configuracions particulars de les màquines.

Per fer-nos una idea de la quantitat de possibilitats diferents que GNU/Linux ens ofereix es mostra a la pàgina següent l'evolució de les diverses distribucions que van sorgir entre els anys 1992 i 2008.



Font: http://www.linux-es.org/files/distribuciones_en_el_tiempo.png

Una primera decisió que ens pot ajudar en la tria de la distribució adequada és la organització que presenta per a l'entorn d'escriptori (*Desktop Environment*). Aquest entorn aportarà les llibreries necessàries perquè les aplicacions puguin tenir propietats i un aspecte homogeni entre elles, l'anomenat *look and feel*. És important tenir present que aquesta serà la capa de programari amb la que interactuaran els usuaris i per tant serà determinant en el grau d'acceptació.

Actualment existeixen diversos entorns d'escriptori amigables, els més coneguts i complets són KDE, GNOME i XFCE. Vegem-los ràpidament.

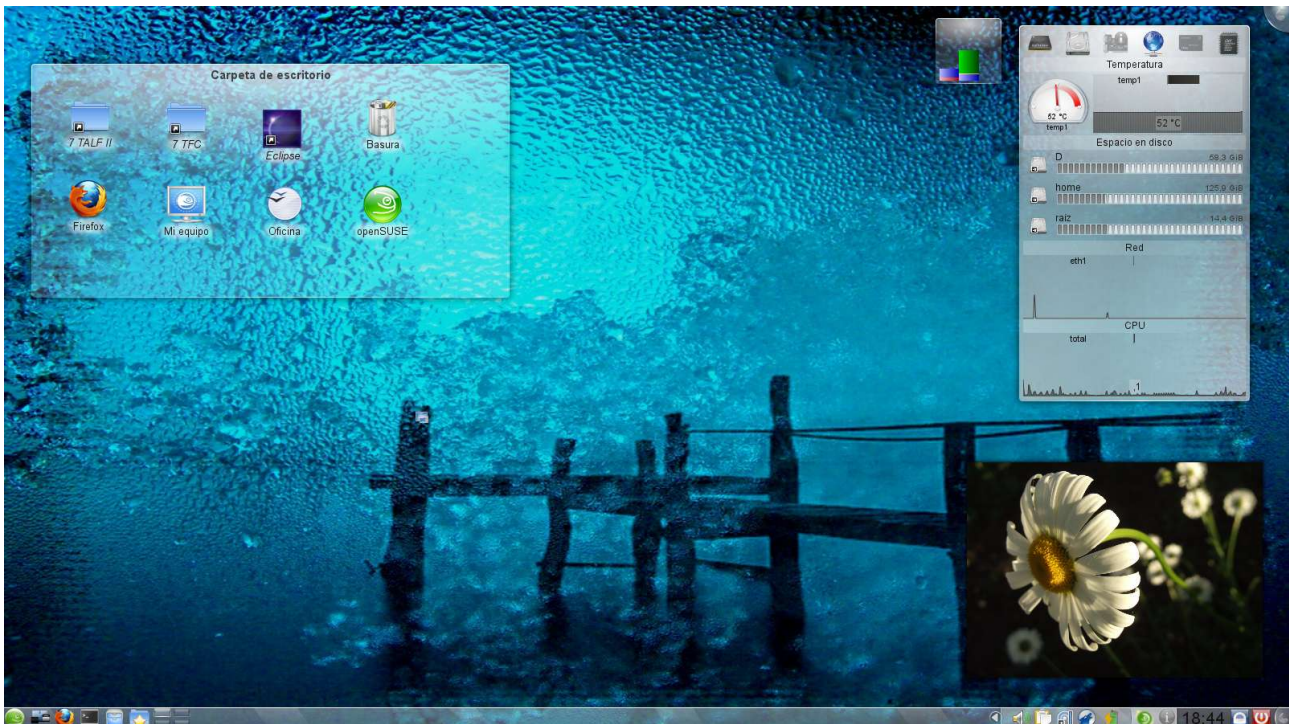


Fig openSUSE amb KDE.

KDE (*K Desktop*) va ser creat l'any 1996 per Matthias Ettrich amb l'ajut d'altres *hackers* en resposta al notable èxit que va tenir Windows 95 a la seva estrena. L'objectiu era dotar els sistemes UNIX d'un sistema estàndard que implementés l'interacció amb l'usuari de manera gràfica -recordem que als anys 90 tot es feia des de la consola- i que a més fos eficient, estable i de confiança. El seu principal avantatge és el grau de personalització que ofereix als usuaris. Tanmateix, presenta un inconvenient important per als defensors més puristes del programari lliure: una de les llibreries que aporta per escriure aplicacions, l'anomenada biblioteca Qt, és propietat de l'empresa noruega *Trolltech*TM, el que significa que no és 100% de codi obert. Un exemple de distribució amb KDE és *Slackware*.

Deixant els detalls tècnics de banda, aquestes distribucions són potser les més indicades per a usuaris que s'inicien en el món GNU/Linux degut a que dels entorns que estem veient és el que més s'assembla en aparença dels escriptoris tipus *MS Windows*TM, i el pas a acceptar-lo podria ser més natural.



Fig: Fedora amb GNOME.

GNOME(*GNU Network Object Model Environment*) va néixer a l'estiu de 1997 en mans de Miguel de Icaza i Federico Mena Quintero, i forma part del projecte GNU. El que volien era desenvolupar un entorn completament lliure, sense cap restricció privativa, encara que fos amb una llicència GPL per derivats lliures com en el cas del KDE. Com es veu a la figura anterior, pretén ser senzill i intuïtiu.

Una distribució d'aquest tipus que es podria considerar instal·lar a les estacions de treball de l'ajuntament degut a la seva popularitat és *Ubuntu*, també coneguda com "la distribució de les persones". Del fet de ser tan popular, gaudeix de controladors per gairebé qualsevol perifèric existent en el mercat, i una comunitat de recolzament molt activa. Tot i que ha estat concebuda per a usuaris domèstics, cada cop està prenent més força en el món empresarial.

Per fer-nos una idea de la evolució d'aquesta *distro* podem veure el gràfic que ens ofereix *Google Trends* basat en el nombre de vegades que s'ha fet servir el seu nom per realitzar cerques al llarg dels anys, i el podem comparar amb cerques relatives a altres distribucions.



Fig: Evolució de les cerques referents a distribucions.

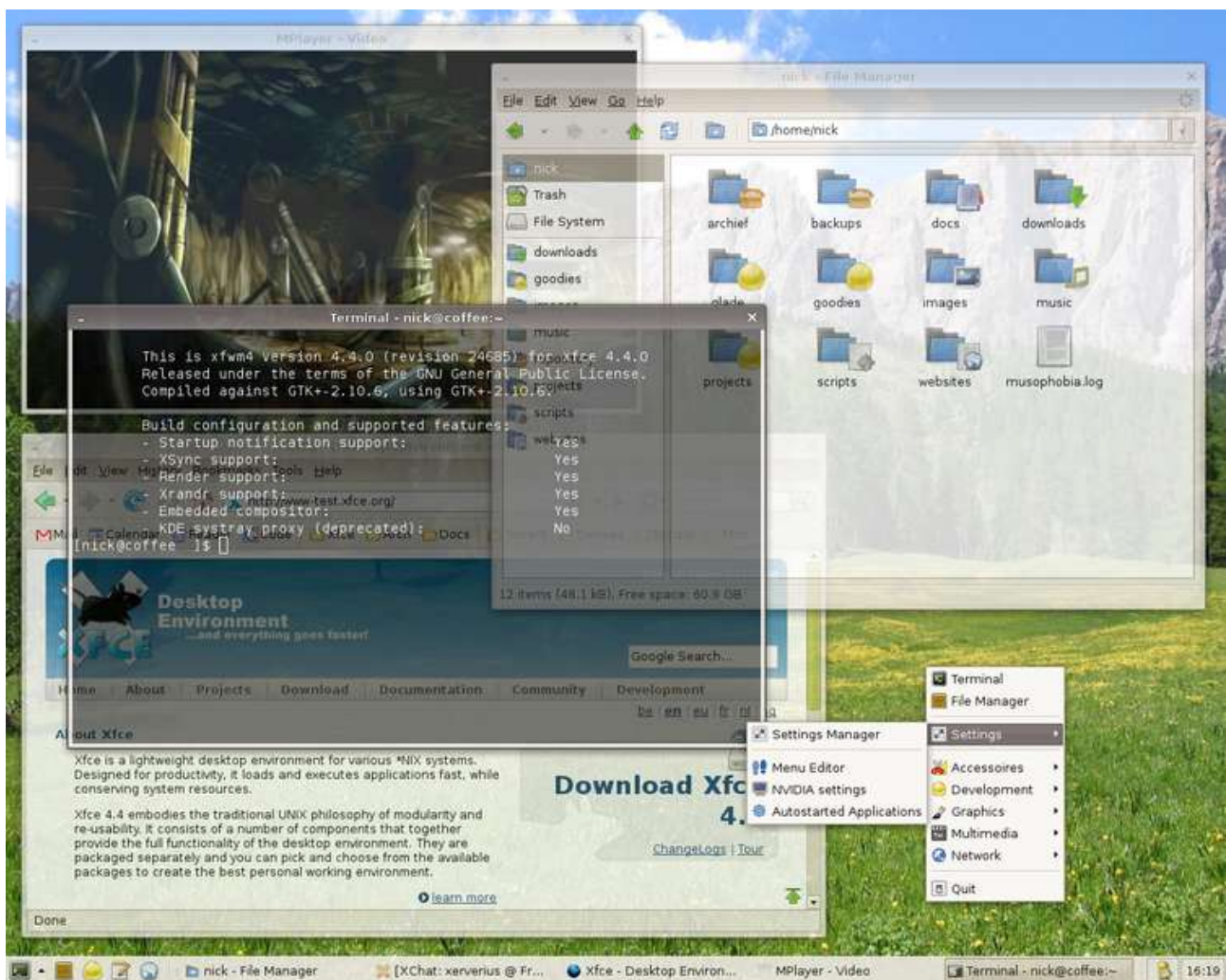


Fig: Escriptori XFCE

XFCE(originalment *XForms Common Enviroment*, i actualment *X Free Cholesterol Environment* o entorn X lliure de colesterol) és un entorn lleuger, que requereix pocs recursos, òptim per instal·lar en màquines antigues. Degut a que les estacions de treball que ens preocupen tenen recursos més que suficients per córrer amb KDE o GNOME, més agradables visualment, no cal considerar aquest entorn.

No és l'objectiu d'aquest treball analitzar totes i cadascuna de les distribucions existents per veure quina és la millor. Hem de tenir present que els treballadors de l'ajuntament només necessitaran eines ofimàtiques i accés a la intranet per fer les gestions pròpies d'un consistori, cosa que es pot fer amb un navegador web si el programa que gestiona les dades del consistori treballa seguint el model client/servidor. Amb tot plegat, l'elecció de la distribució no tindrà una importància vital pel que fa a la funcionalitat, sinó més aviat en l'acceptació o no per part dels usuaris.

Per triar-ne una, ens decidim per *openSUSE*, per diversos motius. En primer lloc, aquesta és l'evolució de *SUSE Linux*, la qual, junt amb *Red Hat Linux Enterprise*, han estat durant molts anys les distribucions de pagament més populars en el món empresarial gràcies al suport tècnic i les solucions que oferien. El fet que hagi estat dissenyada i provada amb escreix en sistemes informàtics d'organitzacions per un equip de desenvolupadors en exclusiva ja ens ha de donar una certa confiança. Avui dia, *openSUSE* és mantingut per comunitat de programari lliure, ja no és de pagament, tot i que rep el patrocini i el suport dels actuals desenvolupadors del propietari legítim de *SUSE Linux*, la corporació nord-americana Novell.

D'altra banda, encara que es considera de dificultat mitjana, es coneix com la distribució més "usable" del món, ja que inclou una interfície gràfica de configuració del sistema molt completa i intuïtiva (anomenada *yast*), actualitzacions automàtiques, tallafoc, i un gestor de paquets que simplifica enormement la tasca d'instal·lació de programes. A més, requereix pocs recursos. Funciona amb processadors Intel Pentium i AMD amb un mínim de 512MB de RAM. Un altre fet important és que es pot configurar amb els entorns GNOME, KDE o XFce, un fet interessant si es volgués canviar d'escriptori en el futur. A més, acaben d'incloure un entorn més lleuger per a *netbooks* i *tablets*, i així es deixa aquesta opció per si el consistori decideix incorporar-ne en un futur i no perdre homogeneïtat.



Fig: Escriptori d'openSUSE per *netbooks*

4.2 Eines ofimàtiques

En aquest apartat es fa inevitable parlar de *l'openOffice*, la *suite* d'ofimàtica lliure per excel·lència. Se sol pronunciar el seu nom quan es vol posar un exemple de programari lliure de qualitat, i de vegades se'l considera superior a altres paquets privatis de similar funcionalitat. El que ara ens interessa és que aporta la funcionalitat que necessitaran els empleats del consistori en la seva tasca diària: inclou un processador de textos (*Writer*), una aplicació de fulls de càlcul (*Calc*), un programa gestor de presentacions (*Impress*), funcionalitat com a client de bases de dades compatible amb SQL (*Base*) i un programa senzill de dibuix (*Draw*).

Una característica destacable d'aquesta *suite* és que el format nadiu que fa servir per guardar les dades de cada una d'aquestes aplicacions és un format obert, basat en XML². Aquest fet pot ser clau en el moment d'integrar i compartir la informació de la organització, ja que qualsevol aplicació pot saber amb detall com manipular-los correctament, el que no sempre és possible amb formats privatis. Dit d'una altra manera, es deslliga la informació emmagatzemada per una d'aquestes aplicacions de la pròpia aplicació. D'aquesta manera es simplifica la transferència de dades entre processos diferents i es garanteix la perennitat de les dades, ja que sempre es podran obrir, encara que no es disposi del programa amb què van ser creades. Recordem que aquestes aplicacions es faran servir per gestionar informació privada dels ciutadans, i per aquest motiu, fer servir formats oberts és la millor opció per garantir la integritat i la disponibilitat de les dades en el futur.

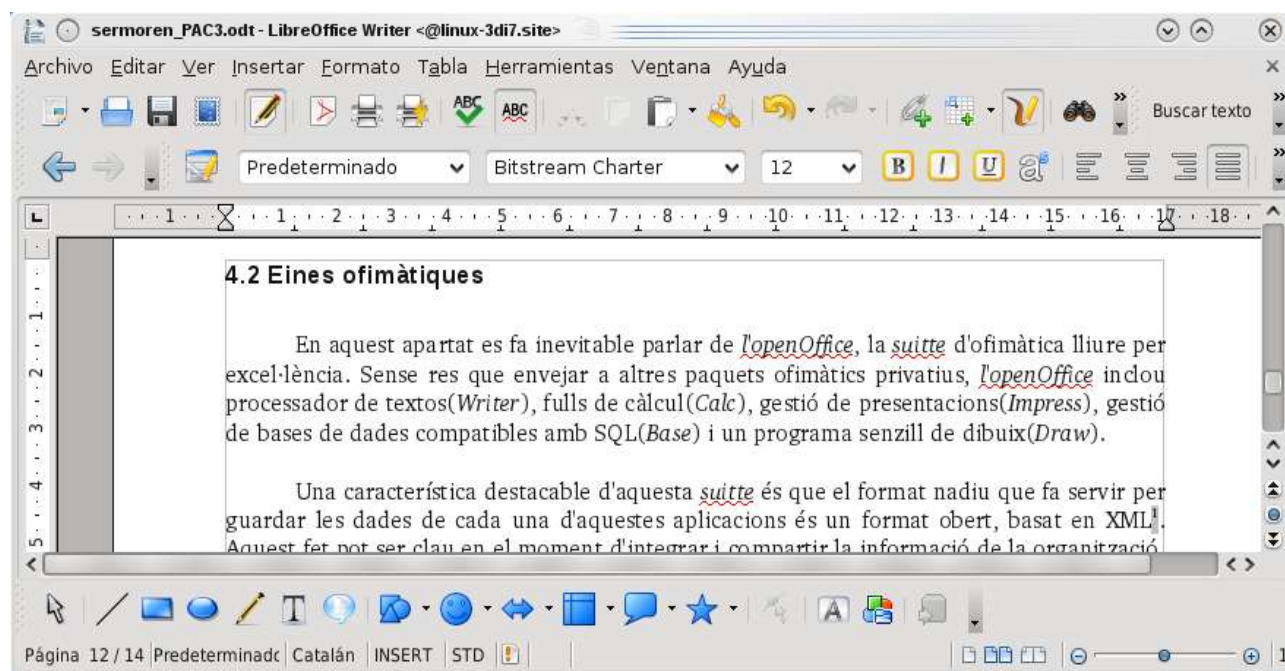


Fig: LibreOffice Writer

² XML o *eXtenible Markup Language* pretén ser un llenguatge estàndard per l'intercanvi d'informació entre diferents aplicacions i plataformes.

Darrerament aquest paquet ofimàtic va sofrir una escissió entre el propietari legítim(*Oracle*) i l'equip de desenvolupadors per les discrepàncies sorgides des que aquests es van fer amb el control de l'anterior propietari(*Sun Microsystems*). En el moment de la redacció d'aquest projecte, *Oracle* tot just decideix cedir el seu manteniment a la fundació *Apache software*, amb la qual cosa es preveu un retrobament entre *openOffice* i el nou derivat elaborat pels seus propis desenvolupadors, anomenat *LibreOffice*.

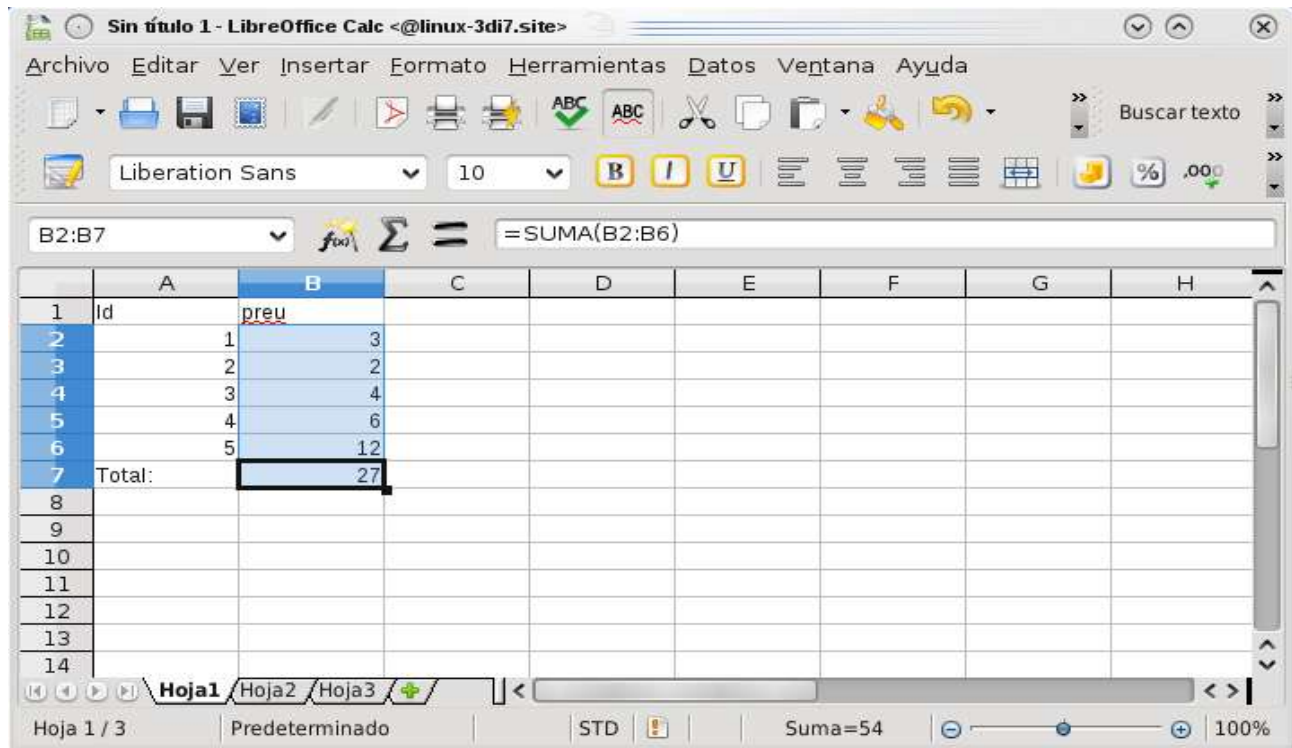


Fig: LibreOffice Calc per fulls de càlcul.

Com es pot veure en les imatges, la seva interfície gràfica és similar a la d'altres *suites* ofimàtiques, el que significa que els usuaris no han d'aprendre a fer servir les noves aplicacions des de zero, el que facilita l'acceptació. A més, gràcies a que és multiplataforma es pot anar provant abans de portar a terme la migració dels sistemes. També cal tenir present que *l'openOffice* és capaç d'obrir correctament arxius creats amb la *suite* de *Microsoft*, probablement la que feien servir amb els sistemes Windows, i per aquest motiu no cal patir per la pèrdua de dades.

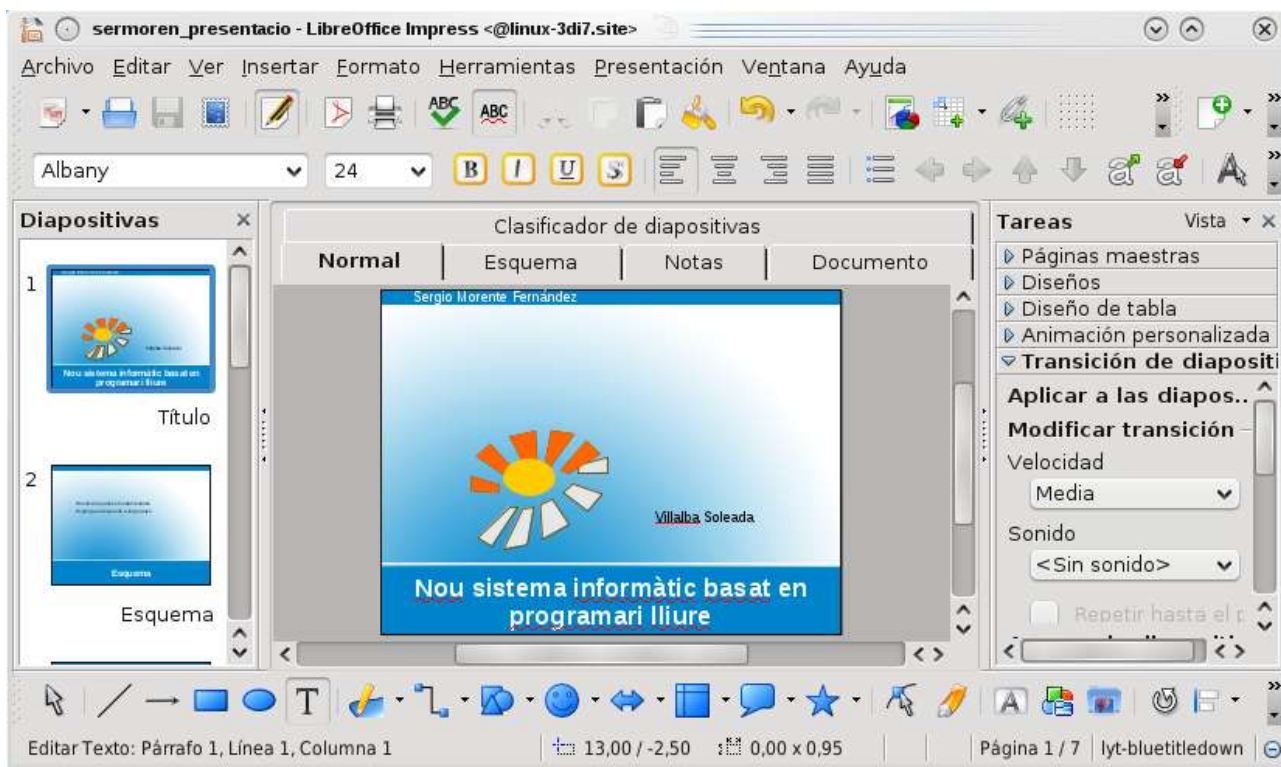


Fig. LibreOffice Impress per presentacions.

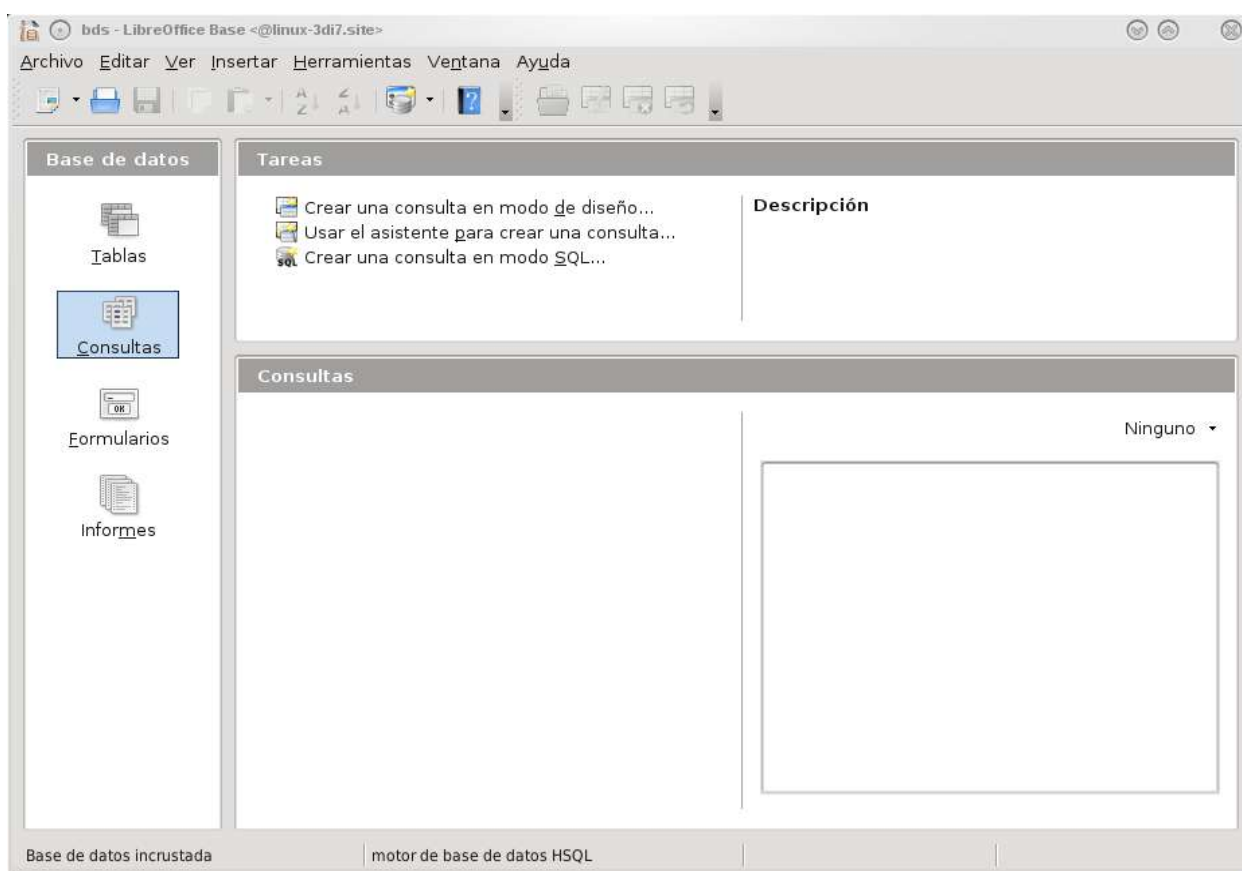


Fig: Sistema de Gestió de Bases de Dades locals o remotes amb LibreOffice Base

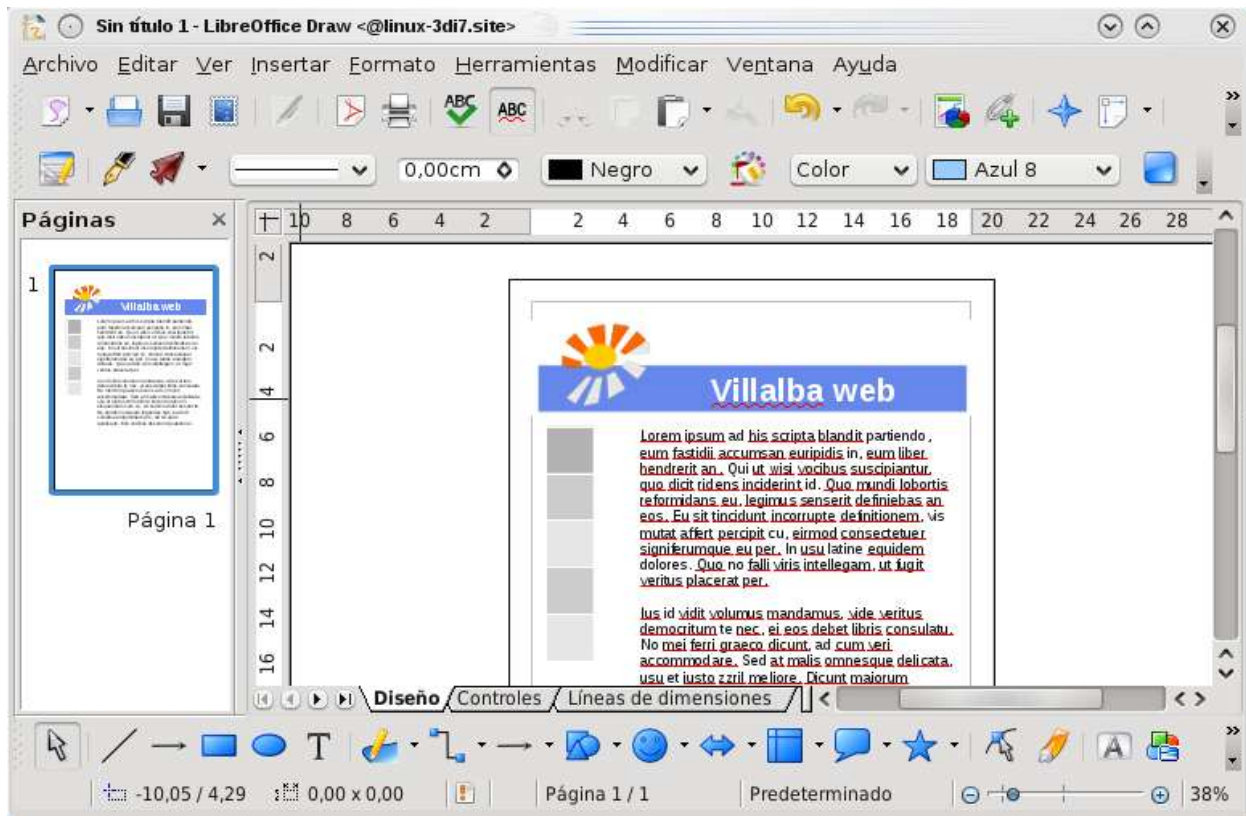


Fig: Dibujos senzills o maquetació web amb LibreOffice Draw

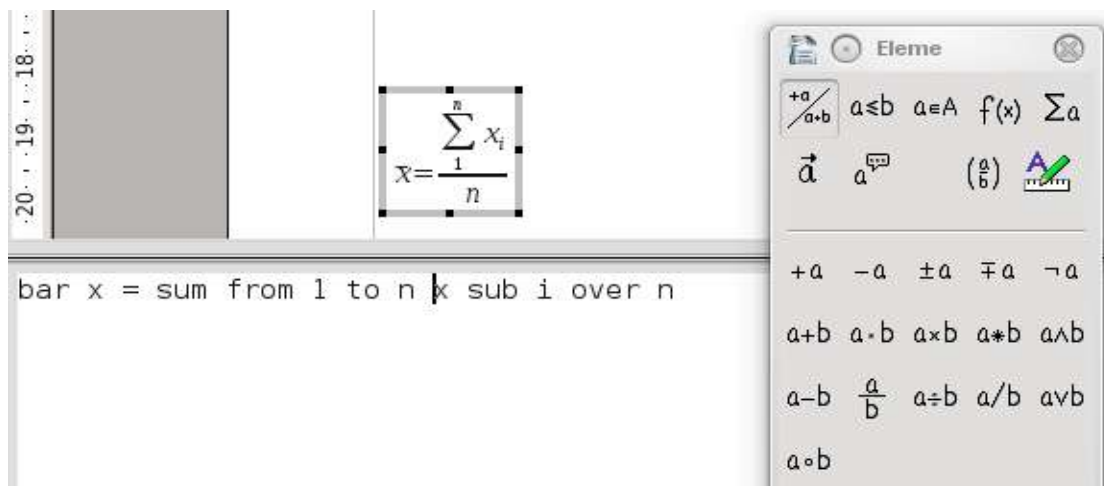


Fig: Suport per l'escriptura de fórmules a Writer.

4.3 Clients d'aplicacions

En aquest apartat hem d'estudiar les aplicacions que necessitin connectivitat amb els servidors o amb l'exterior i que s'hauran d'instal·lar en les estacions de treball dels empleats del consistori. De moment no s'instal·larà cap client de correu electrònic degut a que la direcció vol integrar aquest servei al portal intern i també que l'accés es faci mitjançant un aplicatiu *webmail* per raons de seguretat. La direcció també creu que d'aquesta manera l'usuari se sentirà més vigilat, el que el desmotivarà a l'hora d'enviar o llegir correus personals.

Navegador web

L'aplicació d'aquesta categoria més bàsica per a la tasca diària dels empleats és el navegador web. Recordem que l'ajuntament vol que tota la funcionalitat del seu sistema informàtic estigui integrada en el portal intern, la intranet, al qual s'accedirà via web. D'aquesta manera, per configurar l'estació d'un empleat només cal establir l'adreça del portal com a pàgina inicial del navegador, i així el treballador només ha d'obrir-lo per començar a treballar.

De navegadors web també hi ha força varietat. Actualment, els navegadors lliures més populars són Mozilla Firefox i el jove Google Chrome, tot i que existeixen d'altres com Konqueror o Camino. Es pot optar per Mozilla Firefox per la seva popularitat, seguretat, personalització i extensibilitat.

De la seguretat es pot destacar el control exhaustiu dels recursos que consumeixen les seves instàncies(aïllament de processos); el suport a les connexions xifrades SSL/TSL(https) i a l'autenticació amb targetes intel·ligents; la protecció contra el robatori de claus personals(phishing), de *malware* en general i també pel bloqueig als controls *ActiveX* ja que els consideren una font de vulnerabilitats.

Per últim, es pot esmentar que aquest navegador ja ve de sèrie en la majoria de DVDs d'instal·lació de distribucions GNU/Linux, *openSUSE* inclòs, pel que no ens haurem de preocupar. De tota manera, la elecció no té més importància si la generació del codi del portal es fa segons els estàndars de la W3C³, ja que tots aquests navegadors garanteixen la seva correcta implementació. Darrerament Firefox ha estat el navegador que més atacs maliciosos ha sofert, però gràcies a la extraordinària activitat dels seus desenvolupadors i de la pròpia comunitat és el que es recupera més ràpidament, el que ja indica una certa qualitat.

3 El consorci W3C elabora i promou l'ús de diversos estàndards per garantir la correcta visualització web amb independència de la plataforma, dispositiu o llengua de l'usuari.

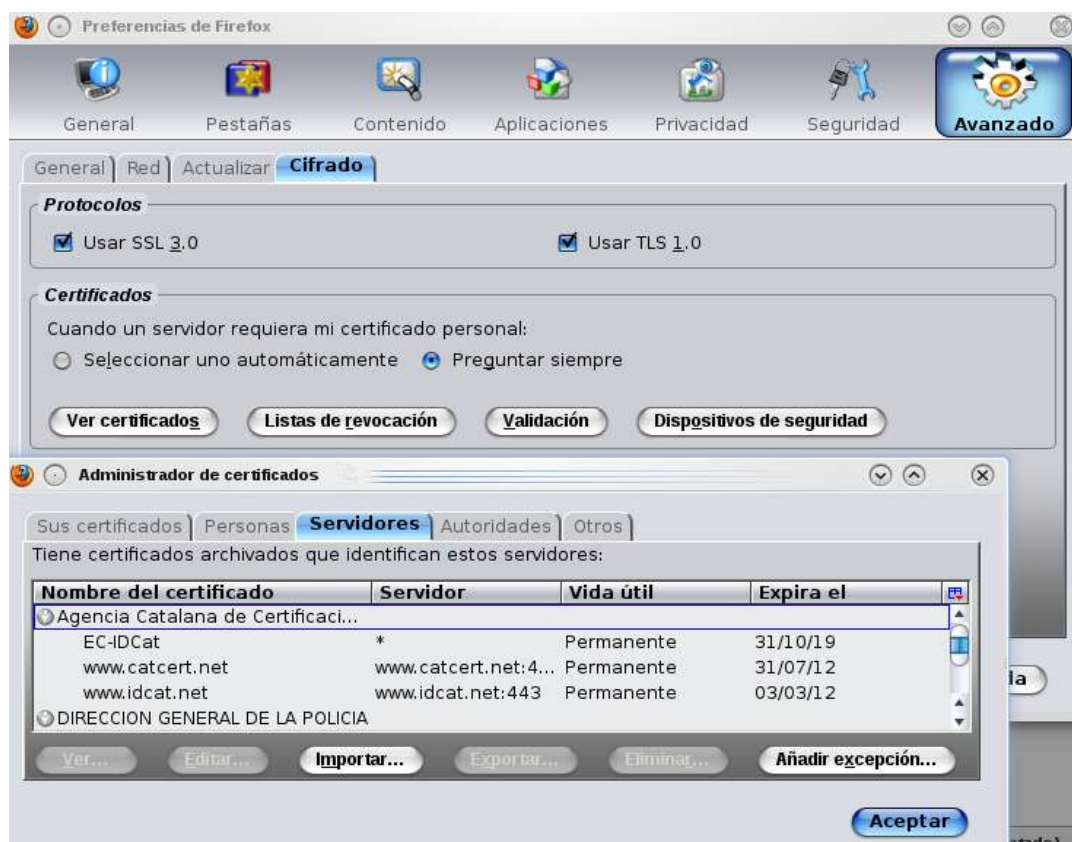


Fig: Navegador web Mozilla Firefox i gestió de la seguretat

Client d'impressió

Per dotar el consistori de capacitats d'impressió es pot habilitar un servidor d'impressores a una de les màquines que s'encarregui de gestionar la cua d'impressió de cada impressora compartida per xarxa. En sistemes tipus UNIX l'estàndard d'impressió més habitual és el que ofereix sistema CUPS o *Common Unix Printing System*, el qual ve inclòs en el sistema operatiu. El client d'aquest servei s'encarregarà de dirigir la petició d'impressió al servidor CUPS adequat.

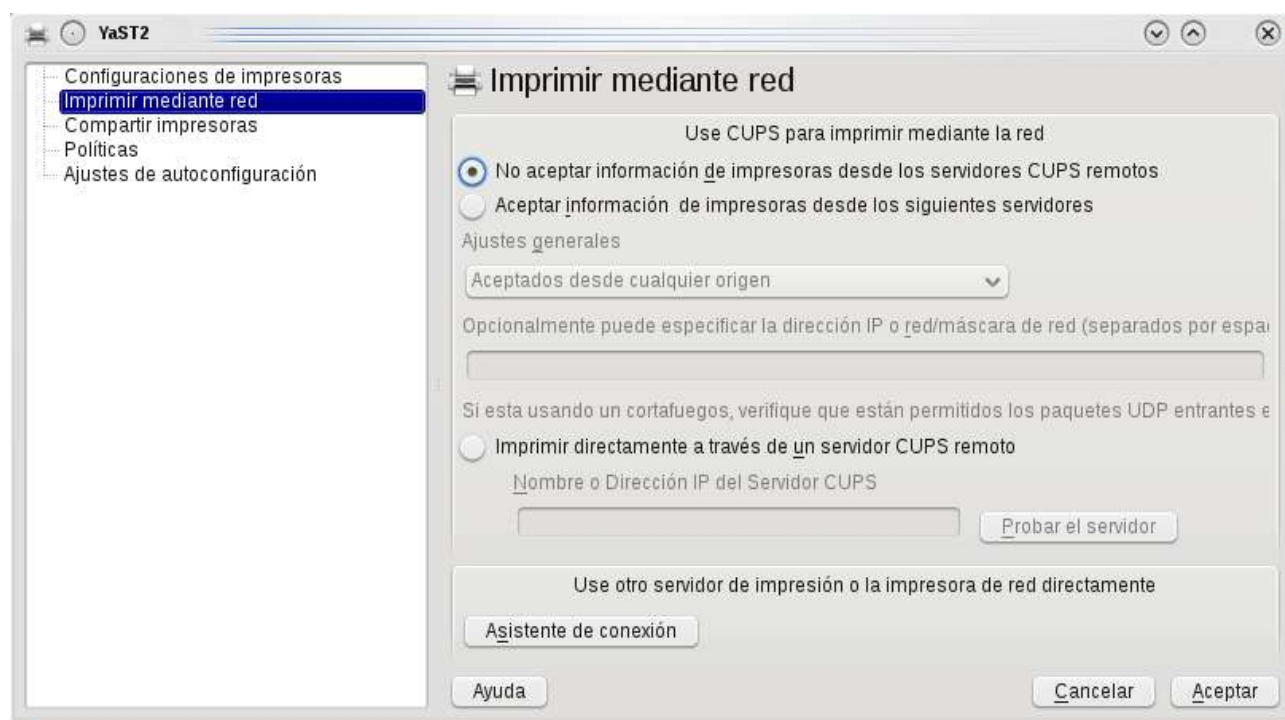


Fig: Panell de configuració del servei d'impressió CUPS

La finestra d'opcions de CUPS permet configurar les impressores connectades a la xarxa(remotes) i indicar-hi si es volen compartir aquelles que estiguin directament connectades a les estacions de treball(locals). També inclou la possibilitat d'obtenir d'un repositori de *drivers* el controlador del dispositiu en cas que ens calgui, i especificar la política a seguir en cas d'error d'impressió.

Client VPN

En l'apartat de disseny de la xarxa s'ha vist que la comunicació entre les xarxes privades locals de cada edifici es realitzarà mitjançant túnels VPN, establint una única xarxa lògica, una xarxa privada virtual o VPN. En aquest tipus de xarxes les dades van xifrades i autenticades quan viatgen entre els diferents edificis per Internet, de manera que s'impedeix que tercers no autoritzats puguin tenir accés a aquesta informació.

Degut a que es fan servir tècniques criptogràfiques per protegir l'accés, cal instal·lar un client VPN a les màquines dels empleats per l'autenticació davant el servidor, i cal que ho faci de manera completament transparent per l'usuari. De clients VPN per programari es pot anomenar l'openVPN, inclòs de sèrie en els sistemes GNU/Linux. L'openVPN permet xifratge asimètric de les dades(RSA) fent servir els protocols SSL/TSL, el que el converteix en un mecanisme de protecció molt robust i flexible, gràcies a que també es pot fer servir en combinació amb firewalls i proxys.

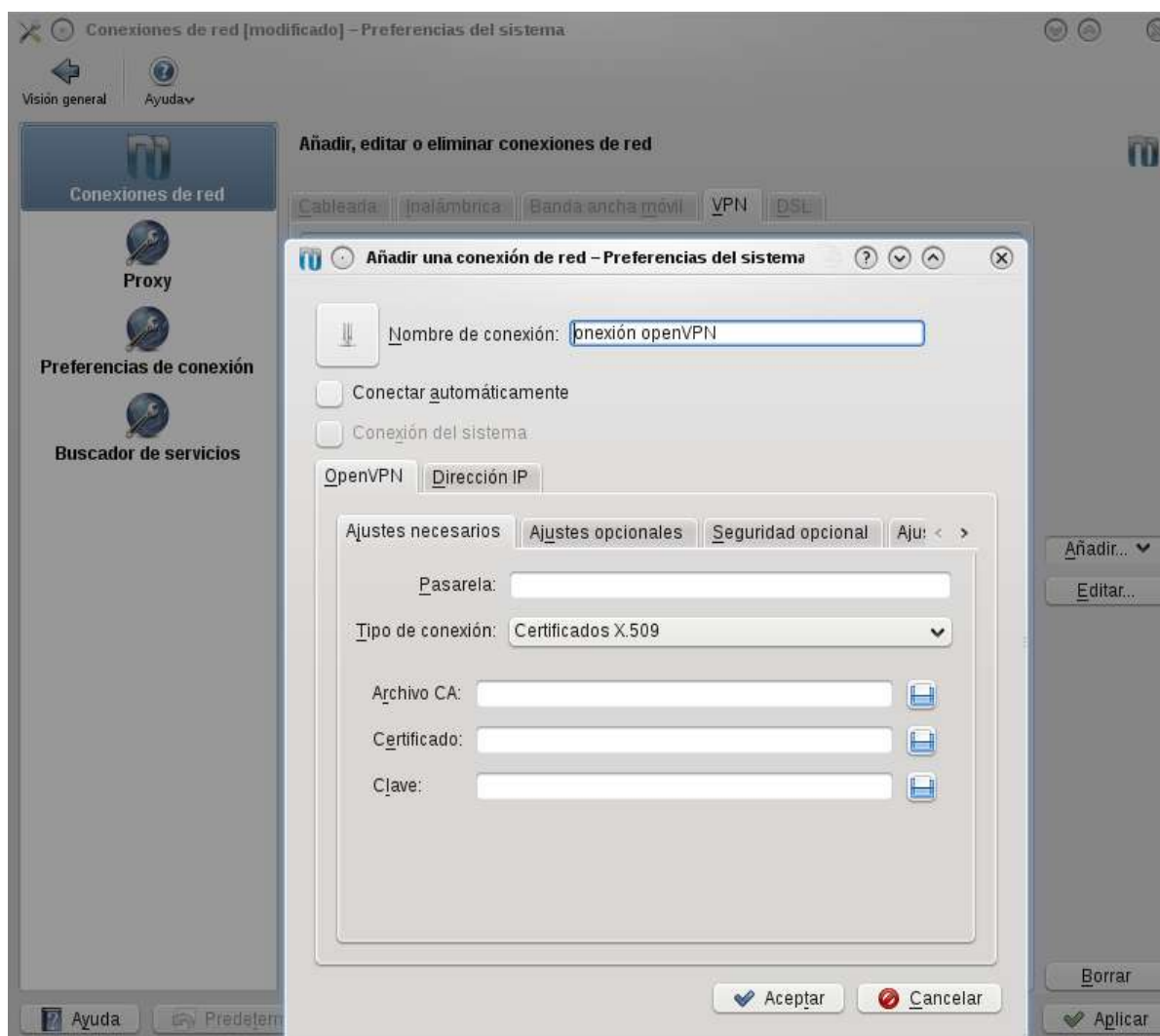


Fig: Interfície gràfica de configuració per l'openVPN inclòs a KDE.

Client LDAP

Sabem que el consistori té oficines situades en quatre edificis diferents que es comuniquen mitjançant una xarxa privada i que ofereix accés al sistema informàtic a uns 100 equips distribuïts. Com era d'esperar, el sistema està protegit d'accessos indeguts i cada empleat s'ha d'autenticar amb un nom d'usuari i una contrassenya, però, on es guarda aquesta informació d'accés per a poder ser verificada?

Una opció cada cop més habitual en aquests tipus de sistemes consisteix en fer servir els anomenats directoris LDAP. Aquests directoris funcionen de manera similar a una base de dades amb una estructura jeràrquica -com l'utilitzada pels servidors DNS- on s'organitza la informació relativa a cada usuari en un registre. Aquests registres poden contenir qualsevol mena d'informació en format de cadenes de text, com el nom d'usuari, contrassenya, nom complet, adreça de correu, extensió, certificats públics, etc. D'aquesta manera es pot implementar un únic punt d'accés per cercar informació de la organització i dels empleats accessible des de qualsevol punt de la xarxa interna. A més, el fet d'emmagatzemar la informació de *login* de manera centralitzada permet als usuaris autoritzats autenticar-se des de qualsevol màquina connectada a la xarxa privada.

És important esmentar que la informació que s'hi emmagatzemi ha de ser poc canviant, ja que, a diferència de les bases de dades pròpiament dites, els directoris LDAP estan optimitzats per a suportar un gran nombre de peticions de lectura, però no de modificacions; el que significa que els accessos concurrents d'escriptura poden acabar provocant inconsistències.

Per accedir a la informació d'aquesta estructura de dades existeix un estàndard elaborat per l'IETF⁴, el Protocol d'Accés Lleuger a directori, *Lightweight Directory access Protocol* o LDAP. Per garantir l'accés a les dades, aquest protocol estableix mecanismes per facilitar l'intercanvi d'informació entre diferents aplicacions i plataformes, el que resulta especialment útil en xarxes heterògenies. Per protegir el directori d'accessos indeguts es promou l'ús de llistes de control d'accés, on es pot indicar quins usuaris tenen accés a la informació, què poden llegir i si poden realitzar canvis en els registres o no. També s'estableixen mecanismes per establir-hi connexions segures fent servir tècniques de comunicacions xifrades com TSL o SSH.

Existeixen diverses implementacions d'aquesta tecnologia, de les quals la que més ens interessa és la coneguda com openLDAP, ja que és completament lliure, independent de la plataforma que la implementa i a més es troba inclosa en la majoria de distribucions GNU/Linux.

4 L'Internet Engineering Task Force promou estàndards per la normalització a Internet.

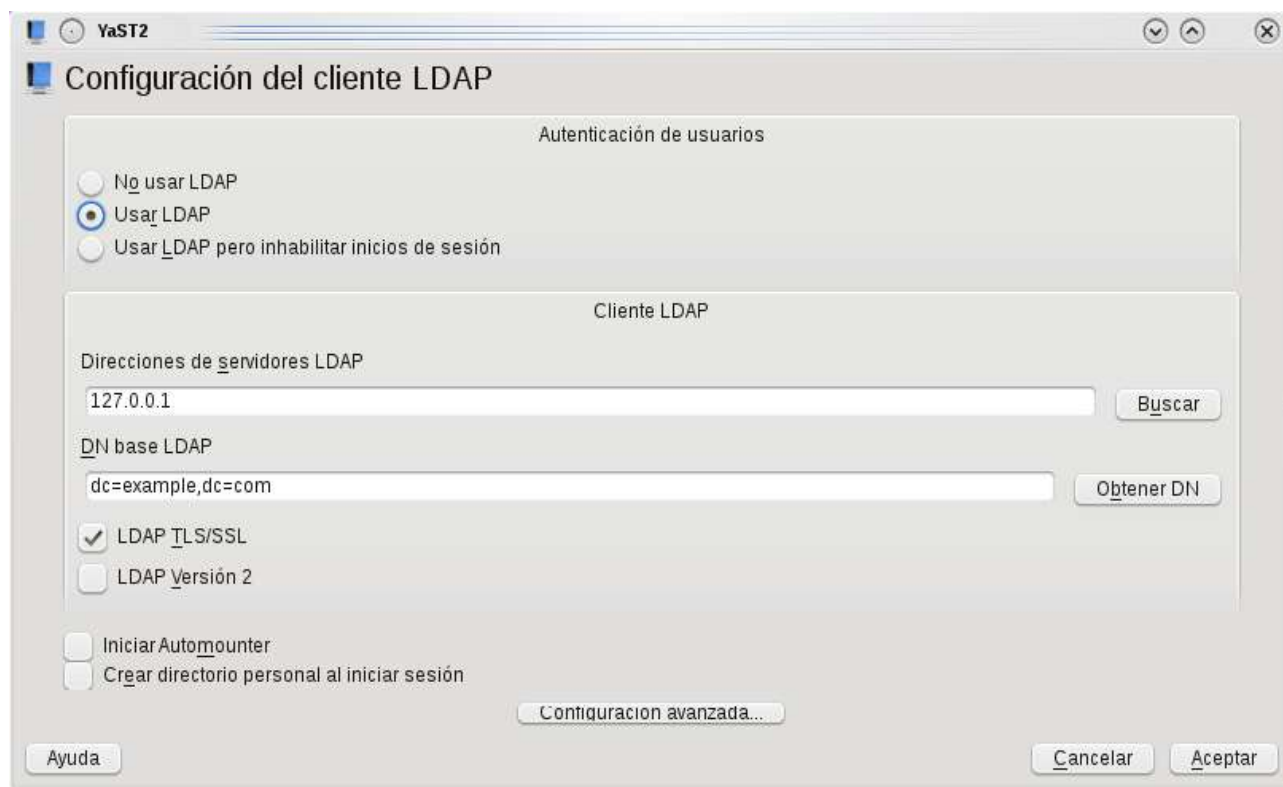


Fig: Pantalla de configuració del client LDAP en openSUSE.

El que hem de tenir clar és que gràcies a LDAP podem tenir una base de dades lleugera amb dades dels usuaris i potser alguna altra informació de la xarxa com rutes d'encaminament de servidors. Podrem fer servir aquesta base de dades a mode de guia telefònica amb informació de contacte dels empleats o amb intencions d'autenticació. També la podrem fer servir per emmagatzemar la estructura de grups i usuaris dins l'organització per tal que el servidor d'aplicacions o de fitxers gestioni els permisos adients. Com a exemple, el servidor on s'emmagatzema la informació dels empleats podria consultar el registre d'un usuari concret per obtenir el límit màxim d'espai assignat(quota) i comprovar així que no l'excedeixi, un dels requisits de l'enunciat.

Client Kerberos

A fi d'evitar la suplantació d'identitat dins una xarxa interna el client Kerberos estableix mecanismes per facilitar l'autenticació mútua entre usuari i servidor. Per realitzar l'autenticació de totes dues entitats fa servir un mecanisme basat en el protocol de Needham-Schroeder en el qual Kerberos actua com a intermediari en la distribució de les claus. La seva tasca és verificar amb protocols criptogràfics de clau asimètrica i de tipus repte-resposta la veracitat de les identifications, i un cop comprovades, es guarda una base de dades una clau de sessió que només coneix ell i la entitat interessada, tant del client com del servidor.

Aquest mecanisme permet que l'usuari només s'hagi d'autenticar un sol cop en tota la sessió, ja que si la identificació es fa correctament, el client obté un tiquet que li permetrà obtenir les credencials necessàries per accedir a serveis protegits. I aquesta és precisament la raó d'incloure el client Kerberos en la configuració de les estacions, ja que utilitzat de manera conjunta amb LDAP es pot implementar l'anomenat *Single sign on*(SSO).

Gràcies a aquesta autenticació única, l'empleat només haurà d'autenticar-se a l'inici de la sessió, i no li caldrà tornar a introduir nom d'usuari i contrassenya per cada servei que demani, com l'accés al portal, al servidor de correu o a les aplicacions internes que ho requereixin.



Fig: Configuració avançada del client Kerberos a openSUSE, basada en la implementació de Kerberos 5 del MIT.

4.4 Còpies de seguretat

Hem vist que les estacions noves incorporen una gravadora de DVD a les torres. Per aprofitar-les, s'hi podria instal·lar programari de gravació de CD-ROM i així donar la capacitat als empleats de fer còpies de seguretat dels seus arxius de manera manual, entre altres usos.

Existeix per KDE un aplicatiu de gravació de discos compactes i DVD molt complet anomenat k3b(acrònim de *KDE burn, baby, burn*). Suporta discos regravables i multisessió -gravació en diversos cops, sense esborrar continguts anteriors. Té una interfície gràfica d'usuari basada en la interacció *arrossegat i deixar anar*(*drag & drop*) amb la que es pot crear fàcilment tot tipus de discos multimèdia. També permet crear imatges d'un disc, és a dir, “treure una foto del sistema de fitxers” per fer-ne còpia de seguretat.

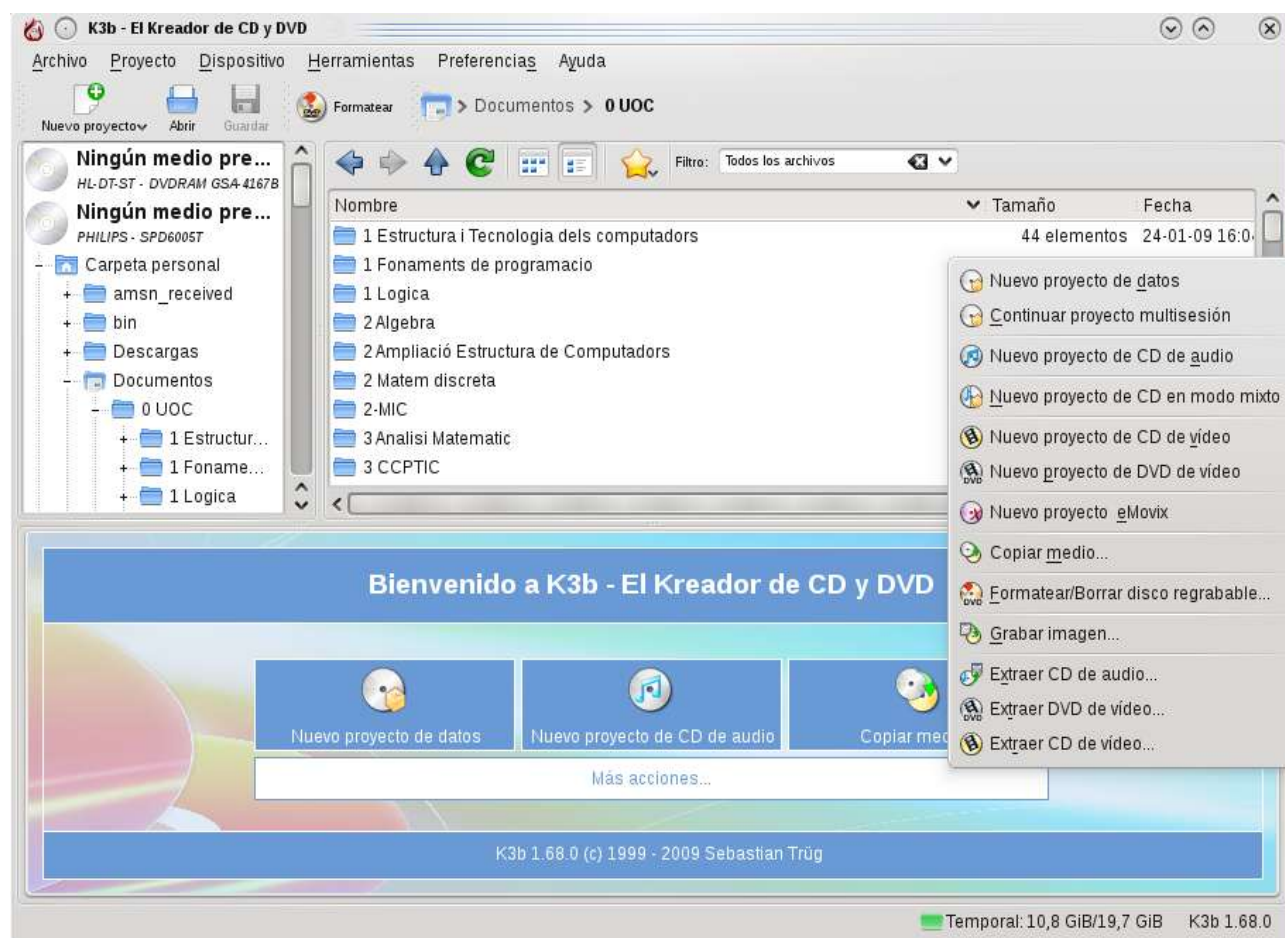


Fig: Pantalla inicial de l'aplicació multimèdia k3b

4.5 Antivirus

Els sistemes GNU/Linux són coneguts per la seva robustesa envers els virus informàtics, però seria un error per la nostra part pensar que són invulnerables. Cada cop existeixen més variants de programari maliciós o *malware*, ja sigui com a virus, cucs, troians o programes espies, i encara que per a GNU/Linux només hi hagi una part molt petita que l'afecti i amb poc poder destructiu no s'ha d'obviar aquesta amenaça. De fet, el primer cuc⁵ documentat, el cuc Morris, va deixar fora de servei el 10% de màquines connectades a Internet l'any 1988, totes màquines UNIX, les quals feien servir un sistema de protecció similar al que utilitza GNU/Linux en l'actualitat.

Per saber una mica més, un virus necessita poder accedir a la totalitat de la memòria RAM o bé modificar arxius executables per poder-se replicar i infectar les màquines. El primer mètode no és viable a GNU/Linux per l'aïllament de l'espai d'adreces dels processos, inclús per a l'usuari amb més privilegis, l'usuari *root*. Això vol dir que en cas que el virus arribés a executar-se no podria pas propagar-se. D'altra banda, la protecció dels arxius del sistema bloqueja les modificacions que en facin els usuaris que no siguin l'administrador, com els virus, deixant el sistema operatiu blindat per a modificacions no autoritzades.

De tota manera, encara que patir un desastre per virus em sistemes GNU/Linux és poc probable, no està de més pensar en una mica de protecció extra i instal·lar a cada estació una aplicació antivirus. El més adient seria que a més de virus detectés cucs i troians, i que actualitzés sovint la seva Base de Dades. Per a GNU/Linux n'hi ha de gratuïtes com l'Avira o l'Avast!, però si volem un antivirus 100% lliure i mantingut per la comunitat ens haurem de decidir pel ClamAV.

5 A diferència d'un virus, un cuc no provoca danys en el sistema de fitxers però si es propaga entre màquines i pot arribar a absorbir una gran quantitat de recursos de xarxa.

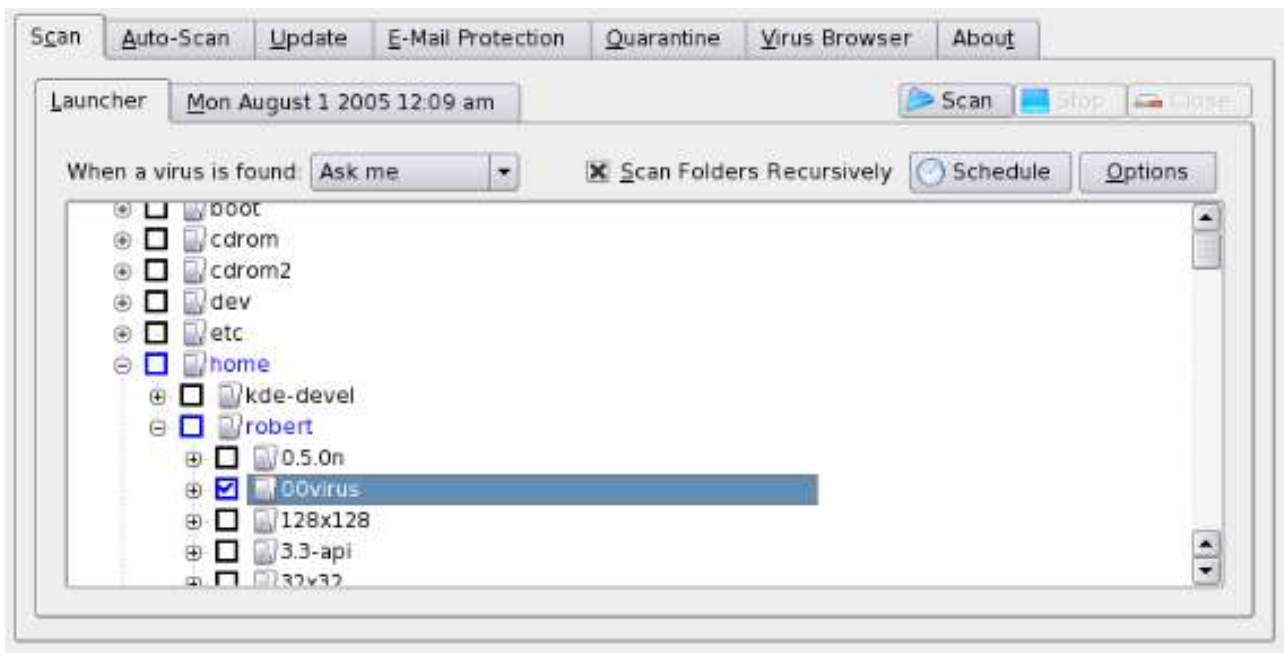


Fig: Interfície de ClamAV per GNU/Linux

5. Requisits de programari als servidors

Seguint els objectius del projecte es cerca programari lliure per instal·lar als servidors. Per aquestes màquines la cosa canvia i tot i que es troba programari que permetrà oferir els serveis desitjats en codi obert, el més habitual és que aquest no sigui gratuït. Seguint un dels objectius del projecte, busquem un cost zero per al programari, no cal el suport del fabricant, ja que de la instal·lació i de la configuració se n'encarrà l'equip tècnic.

Les funcionalitats que s'han de cobrir són les següents:

- Sistema operatiu
- Servidor de fitxers
- Servidor d'impressió
- Gestor de Bases de dades
- Servidor d'aplicacions
- Servidor web
- Servidor de correu
- Servidor DNS (Domain Name Server)
- Autenticació i seguretat: VPN, LDAP i Kerberos
- Programari ERP

5.1 Sistema Operatiu

Triar la distribució i versió del sistema operatiu per als servidors és un punt clau per a la funcionalitat i seguretat del sistema informàtic i la que més debats ha generat entre professionals. Fem una descripció ràpida dels sistemes més populars per a servidors, recordant que tots aquests serviran per cobrir la funcionalitat demanada -es centren en eines de connectivitat- i disposen d'un entorn gràfic que en facilita l'administració dels recursos compartits.

Debian

De les més antigues(1993) i completament mantinguda per la comunitat. No hi ha cap empresa al darrere que la mantingui, per la qual cosa és gratuïta.

Ubuntu

La distribució que més ha crescut en els darrers anys, inclús en el món dels servidors. Es basa en Debian i és gestionada per l'empresa *Canonical*. Compta amb el recolzament del gegant de programari *Oracle*.

RHEL (Red Hat Enterprise Linux)

Aquesta és la distribució més veterana i coneguda en el món empresarial. Va ser concebuda per ser instal·lada en empreses, i ha contribuït de manera molt activa en el desenvolupament de moltes de les solucions de connectivitat lliures existents en el mercat actual. Tot i que ofereix suport i actualitzacions gratuïtes als usuaris, requereix el pagament de certes llicències.

CentOS (Community Enterprise Operating System)

CentOS és una versió lliure del sistema operatiu de Red Hat, de la qual modifica només alguns logotips i marques registrades. És 100% compatible amb l'original i no cobra per les actualitzacions de seguretat.

SLES (SuSE Linux Enterprise Server)

Podríem dir que aquesta és la versió Europea de Red Hat, ja que d'aquesta agafa el model de negoci(és de pagament) i la gestió de paquets. En 2003 va ser adquirida per Novell, i actualment també ofereix una versió completament oberta i descarregable des de la seva pàgina anomenada *Novell Open Enterprise Server*.

5.2 Servidor de fitxers i d'impressió

En sistemes tipus UNIX, el servidor que permet compartir recursos per excel·lència és el servidor SAMBA. Es basa completament en codi obert i gràcies al seu protocol SMB permet compartir fitxers i impressores entre una xarxa multiplataforma d'usuaris. Recordem que als sistemes GNU/Linux la interacció amb els dispositius s'implementa com si aquests fossin arxius per integrar-los en el sistema de fitxers.

Degut a que ha estat concebut per funcionar en sistemes UNIX, SAMBA és completament compatible amb el seu sistema de privilegis i permisost. Gràcies als mecanismes d'autenticació d'usuaris que incorpora, els quals pot gestionar de manera conjunta amb les definicions de grups i usuaris establertes en el directori LDAP, pot protegir arxius i impressores d'usuaris no autoritzats, un dels requisits demanats a l'enunciat.

Es pot configurar SAMBA en el servidor de fitxers, que és bàsicament un disc dur compartit, per a què els usuaris només tinguin accés als directoris que els pertocuin. L'organització dels directoris es pot fer per àrees funcionals, per departaments, per seus, creant una carpeta per cada usuari o bé com es consideri oportú. Quan un usuari vulgui accedir als recursos, el servidor SAMBA consultarà el seu nom d'usuari i els grups als què pertany al directori LDAP per deixar-lo entrar amb una autenticació automàtica o no. Un cop sigui a dins, SAMBA també pot gestionar els permisos de lectura, modificació o execució que tingui l'usuari sobre els arxius, directoris o dispositius.



Fig: Esquema de funcionament del Servidor SAMBA.

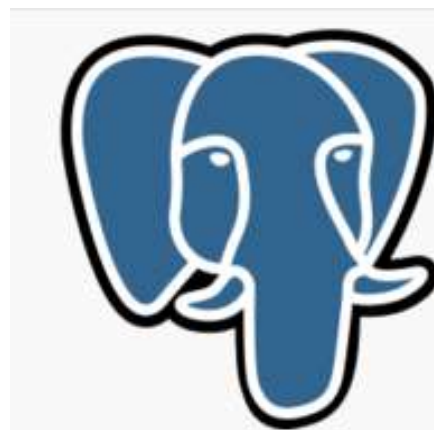
5.2 Sistema gestor de Bases de Dades

Qualsevol organització, per petita que sigui, necessita emmagatzemar i gestionar les dades dels clients o usuaris, personal, proveïdors, etc., de manera centralitzada, i això es pot fer gràcies a les conegudes bases de dades. Cal tenir present que les dades en sí no són gaire útils si no hi ha un programa gestor que atengui les peticions de les aplicacions que les demanen, i que a més protegeixi la informació d'accesos indeguts i d'incoherències provocades per modificacions simultànies. Aquesta és la tasca primordial del Sistema gestor de Bases de Dades o SGBD.

Val a dir que acualment es fan servir les bases de dades per altres usos i no només per emmagatzemar informació d'una l'organització. Aquesta tecnologia també permet que un usuari pugui emmagatzemar informació en un servidor operatiu, i aquesta pot ser utilitzada a l'hora de crear el contingut d'una pàgina web. D'aquesta manera, amb SQL i una aplicació executada en el servidor(anomenada *servlet*) es poden crear tota mena de pàgines amb contingut dinàmic, com les botigues on-line, fòrums, pàgines de notícies en temps real, xarxes socials, o blogs. Aquesta serà la tecnologia bàsica que es farà servir en el portal intern per la comunicació interna.

L'estàndard més utilitzat darrerament en qualsevol sistema informàtic per realitzar consultes a les Bases de dades és l'SQL(*Standard Query Language*). Gairebé tots els SGBD del mercat són compatibles amb aquest llenguatge. Si fem una cerca de SGBD lliure i compatible, ens trobarem de ple amb al PostgreSQL.

PostgreSQL és un SGBD relacional, de codi obert, i mantingut per una comunitat d'usuaris. És compatible amb la majoria de programari empresarial ja que el codi s'executa en el propi servidor, i a més, permet una alta concurrència. Accepta diversos llenguatges de programació per implementar-ne la interacció, el que el facilitarà la migració al nou sistema.



5.3 Servidor d'aplicacions

De la mateixa manera que es pot mantenir centralitzada tota la informació de l'organització també es pot mantenir centralitzada tota la funcionalitat, per permetre'n l'accés als usuaris a través del portal intern. En aquest sentit, els servidors d'aplicacions són una bona opció ja que permeten l'execució d'aquells programes comuns per a tots els empleats -amb connectivitat a les bases de dades internes- encara que no els tinguin instal·lats en les seves màquines.

Gairebé tota la funcionalitat de la intranet s'ha d'implementar mitjançant un conjunt de mini-aplicacions molt concretes amb connectivitat a les bases de dades. Mantenir-les centralitzades en un mateix punt facilita el seu desenvolupament i manteniment, a la vegada que s'assegura que l'usuari sempre executarà la versió més actual, sovint la més segura. Aquest fet també facilita el manteniment del sistema, ja que no cal anar màquina per màquina instal·lant les darreres versions.

Els servidors d'aplicacions funcionen com a contenidors de components necessaris per a construir les aplicacions, els quals fan servir l'estandart Java EE per facilitar la portabilitat dels programes. A aquests components se'ls anomena *Servlets*, *Java Servlet Pages (JSPs)* o *Enterprise Java Beans (EJBs)* segons la funcionalitat que implementin (els servlets es fan servir per la generació dinàmica de contingut web, i els EJBs per implementar les diferents capes de les aplicacions, com la interfície d'usuari, gestió d'usuaris, organització de les aplicacions i accés a les bases de dades). També inclouen programari de connectivitat o *middleware* que aporta una interfície per permetre la comunicació amb altres aplicacions, maquinari, xarxes o sistemes operatius, el que facilita el desenvolupament de les aplicacions.

Glassfish Server open source Edition és un servidor d'aplicacions completament lliur, basat en codi font donat per Sun Microsystems (el seu creador) i Oracle Corporation. És compatible amb la plataforma Java EE 6, modular, i permet l'execució d'aplicacions en clústers⁶.



⁶ Un clúster és un grup de màquines que treballen de manera conjunta, unint les seves capacitats de càlcul

5.4 Servidor web

Per implementar l'accés web a la pàgina del consistori, i també per al portal intern, caldrà instal·lar un servidor web que s'encarregui de servir arxius als usuaris seguint el protocol HTTP. El servidor web lliure per excel·lència és el que ofereix la fundació *Apache Software* per la seva popularitat i implantació, si tenim present que es troba funcionant en la gran majoria de servidors arreu del món.



**The Apache Software
Foundation**

El servidor apache és modular, extensible i multiplataforma. Dels mòduls que incorpora se'n pot destacar el mòdul per a donar suport a connexions http segures o https(fent servir el protocol TLS), autenticació d'usuaris mitjançant LDAP i connectivitat amb el servidor d'aplicacions per implementar pàgines dinàmiques amb servlets i JSP. També permet la incorporació d'un mòdul que dona suport a PHP(*PHP Hypertext preprocessor*), i que permet crear pàgines dinàmiques amb connectivitat a bases de dades sense haver de fer servir aplicacions java.



Fig: Esquema de funcionament d'un servidor web.

5.5 Servidor de correu

Per dotar al consistori de la capacitat d'enviar i rebre correus electrònics amb el seu propi domini caldrà instal·lar un servidor de correu. A més, s'aconsegueix independència de servidors externs insegurs. Aquesta aplicació pot actuar com un un agent MTA (*Mail Transport Agent* o agent de transport de correu), que és l'encarregat de negociar amb altres servidors o MTAs l'enviament o recepció dels arxius.

Ha d'incloure suport al protocol estàndard i oficial per a l'enviament de correus electrònics, l'SMTP (*Simple Mail Transfer Protocol* o protocol simple de transferència de correu) i als protocols utilitzats per rebre'ls, que són el POP3 (*Post Office Protocol*, protocol d'oficina de correus) i IMAP (*Internet Message Access Protocol*, protocol d'accés a missatges d'Internet), els quals s'implementaran en l'aplicatiu de *webmail* del portal intern.

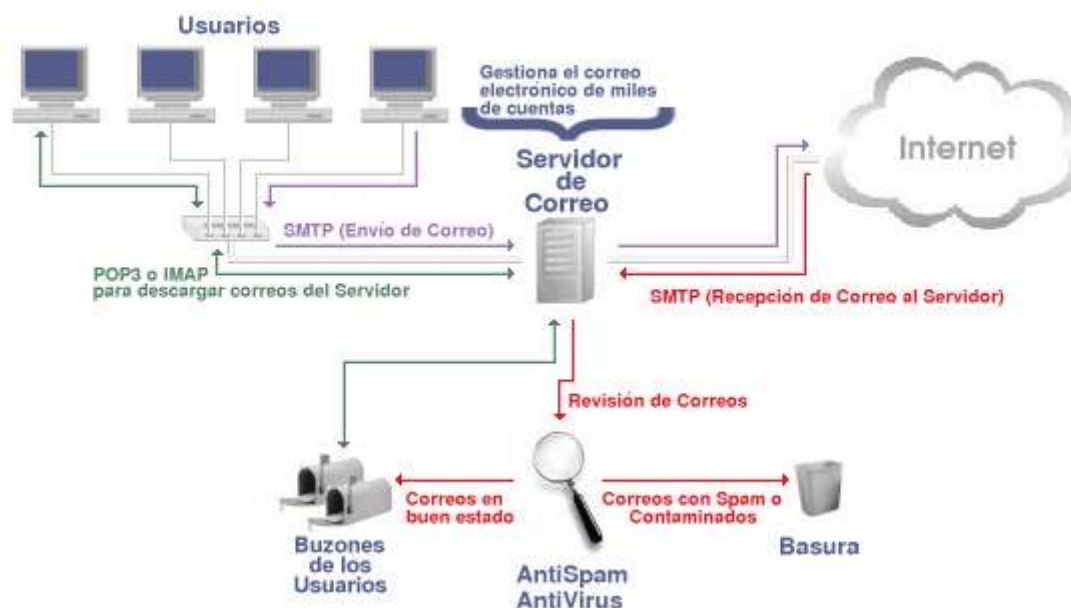


Fig: Funcionament de l'enviament de correus electrònics

Hi ha diversos sistemes GNU/Linux que incorporen un agent MTA per defecte anomenat PostFix, que implementa tota aquesta funcionalitat; i a més, permet l'extensió per incorporar filtres de correu brossa o antispam, ús de llistes de correu, establiment de la capacitat màxima d'emmagatzematge per usuaris (quotes) i creació d'una interfície web per a clients de correu.

5.6 Servidor DNS

El servei DNS(*Domain Name Server* o servidor de noms de domini) es fa servir des dels inicis d'Internet per crear un índex de màquines connectades a una xarxa i les seves adreces IP per poder-les localitzar i encaminar la informació. Fa servir una base de dades jeràrquica per permetre que donat un nom de màquina tractable per humans, es pugui obtenir la seva adreça IP, en format numèric i difícil de recordar. En el nostre cas es fa necessari per localitzar els servidors dins la xarxa.

Als sistemes servidors tipus UNIX s'inclou de sèrie un servidor DNS que s'ha proclamat un estàndard *de facto* anomenat BIND(*Berkeley Internet Name Daemon*). A més de permetre la creació i manipulació d'aquesta base de dades, suporta la gestió d'adreces IP versió 6, LDAP, MySQL i PostgreSQL.

5.7 Autenticació i seguretat: VPN, LDAP i Kerberos

Hem vist en l'apartat sobre els requisits de maquinari per les estacions de treball que els serveis VPN, LDAP i Kerberos són necessaris per protegir la xarxa d'accesos indeguts, sigui codificant la informació, gestionant una llista d'usuaris autoritzats o autenticant els usuaris de manera automàtica, respectivament. Ara cal instal·lar les versions d'aquests clients en el costat del servidor.

En tots tres casos es pot fer servir el mateix programari, ja que openVPN, openLDAP i Kerberos poden executar-se en el costat del servidor per acabar d'implementar la funcionalitat que ofereixen.

5.8 ERP

A fi de coordinar totes aquestes tecnologies es pot fer servir un programa dels anomenats ERP (*Enterprise Resource Planning* o Planificadors de recursos per a l'empresa). Aquests programes faciliten la creació d'aplicacions web destinades a la gestió dels recursos de les organitzacions, ja siguin de comptabilitat, de producció, inventaris, proveïdors, recursos humans, etc. i centralitzar tota aquesta informació en el servidor adient.

Dins d'aquesta categoria podem trobar l'aplicació *OpenBravo ERP Community Edition*, un aplicatiu de codi obert destinat a petites i mitjanes empreses o organitzacions. Funciona sobre el servidor web Apache i suporta la interacció amb les bases de dades gestionades per PostgreSQL. Resultarà una eina útil en el moment de construir el portal intern de l'ajuntament. Com es pot veure a la figura següent, aporta una interfície gràfica per al desenvolupament de les aplicacions.

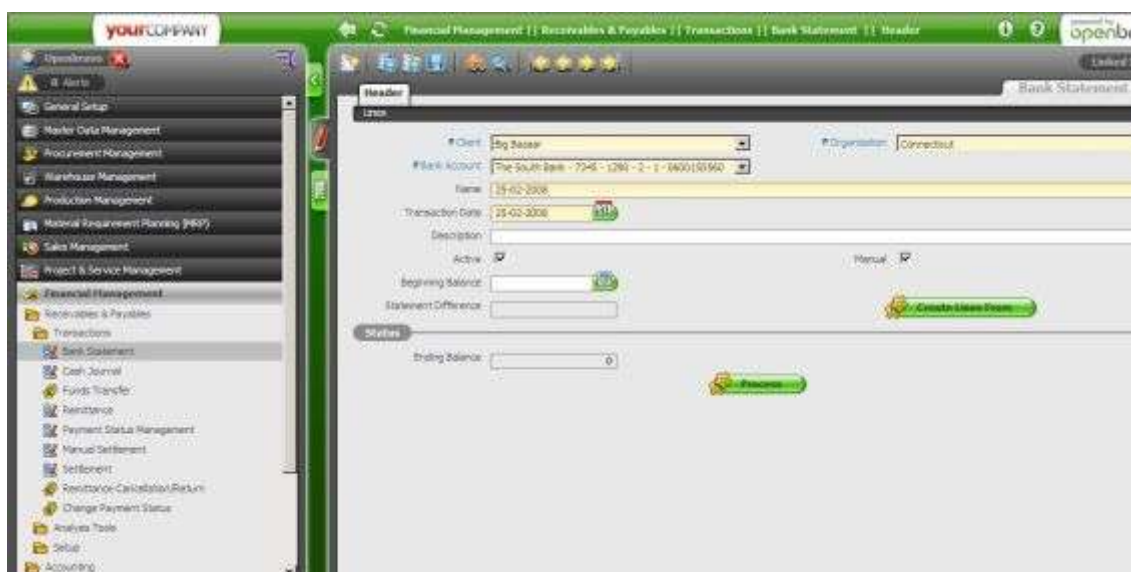


Fig: Panell d'administració d'openBravo.

6. Fase d'implantació

Un cop s'hagi adquirit el maquinari necessari i es tingui clar quin és el programari exacte que es vol fer servir, es pot començar amb el desplegament. A fi d'evitar haver d'aturar tot el sistema durant la migració al nou sistema es pot dividir la tasca en fases de manera que ambdós sistemes coexistiran un temps determinat.

Aquesta fase també es pot dividir en fases diferenciades: migrar els servidors i canviar les estacions de treball. Per garantir la coèxistència temporal dels sistemes s'haurà de fer en aquest ordre.

Primera fase: Migració dels servidors

Primer de tot s'ha de canviar el programari dels servidors cap a les versions lliures. Degut a que s'han d'aturar completament els servidors per a fer el canvi, s'haurà de fer fora de l'horari laboral, això si no s'han adquirit servidors nous.

La migració dels servidors SAMBA, Apache, correu i DNS no tindrà complicació afegida en el sentit que aquests poden conviure perfectament amb les màquines Windows actuals, i en principi no caldrà reconfigurar cap estació de treball per mantenir la interactivitat. També es poden implementar com a nous els servidors de VPN, LDAP i Kerberos, si no existien.

Potser cal parar especial atenció en la migració del servidor d'aplicacions i Base de Dades, degut a que els canvis poden alterar el seu funcionament, i encara que siguin multiplataforma algunes de les aplicacions poden requerir modificacions per a poder funcionar sota els dos sistemes.

Aquesta fase és, doncs, un bon punt per començar a implementar el portal nou del consistori, el que es pot fer en paral·lel a la segona fase. També és un bon moment per establir les polítiques d'accés als recursos del sistema informàtic per usuaris i grups, configurant el directori LDAP i el servidor SAMBA.

Segona fase: Creació de l'estació model i proves.

Un cop hem decidit el programari que s'executarà de manera local a cada màquina es procedeix a instal·lar-lo en una màquina que ens servirà de prototip. En aquest punt també es configuraran tots els clients de les aplicacions que requereixin connectivitat a fi de provar el correcte funcionament de tot el sistema.

En aquesta fase s'han de detectar els errors de connectivitat amb tots els servidors, el que es pot fer simplement amb la comanda ping. També és bo provar els mecanismes d'autenticació en els diferents recursos compartits. Detectar els errors en aquesta fase evitarà que es propaguin i s'hagin de corregir posteriorment en totes les altres estacions de treball.

Tercera fase: Clonació de l'estació model.

Un cop sabem que els servidors estan preparats i tenim una estació model completament funcional podem clonar-la. Aquest procediment consisteix a “fer una fotografia” del disc dur d'aquesta màquina per després clonar-lo per xarxa a la resta d'estacions. D'aquesta manera es pot reduir considerablement el temps necessari per deixar operativa una màquina nova. Una nova instal·lació i configuració dels clients pot necessitar un parell d'hores, especialment si es fan les actualitzacions de seguretat per internet, acumulades des de el moment de llançament del DVD d'instal·lació. Amb un programa de clonació aquest temps es pot reduir a uns pocs minuts.

Per la clonació es pot fer servir el programari, també de codi obert, *CloneZilla*. Aquesta aplicació permet fer imatges de discos sencers o de particions, pujar la imatge resultant a un servidor SAMBA i crear un Live-CD amb la funcionalitat necessària perquè una màquina nova sense sistema operatiu sigui capaç d'obtenir l'arxiu de la xarxa i el copii al seu disc dur.

7. Manteniment i actualitzacions

Com ja s'ha vist a la secció d'antivirus, cada cop existeixen més amenaces que poden provocar danys greus en el sistema, i no són només virus. També s'ha vist que GNU/Linux és fort davant aquestes amenaces, però sí que es vulnerable als errors en la programació. Els errors en el codi dels programes impliquen un forat en la seguretat del sistema, i n'hi ha atacants disposats a aprofitar-se'n. Aquest és el cas dels anomenats *exploits*, construïts a partir d'unes poques línies de codi i que en executar-se són capaços d'exploitar una vulnerabilitat coneguda, obrir una consola com a administrador i fer-se'n amb el control de la màquina.

La millor manera de prevenir aquest tipus d'atac és mantenint tot el programari actualitzat. Qualsevol aplicació és susceptible de tenir errors en el seu codi, els anomenats *bugs*, els quals es van corregint a mesura que es van reportant. Aquest és precisament un dels punts forts del programari lliure: en cas de detectar-se una vulnerabilitat en una aplicació, la mateixa persona que l'ha detectat pot corregir-lo gràcies a que disposa del seu codi font, o bé pot reportar l'error en la comunitat corresponent per a què algú s'ofereixi a solucionar-lo.

El que ara ens interessa, és que es poden configurar les actualitzacions de programari, els coneguts "*parxes*", per a que es facin de manera automàtica en engegar el sistema. Per fer-ho, cal introduir una llista d'adreces de repositoris on es faran les cerques de paquets nous i el dimoni "Update Applet" s'encarregarà de la resta.

En el nostre cas, caldria afegir els repositoris oficials de la distribució (opensuse-oss), els de KDE, openOffice, Mozilla Firefox i potser algun de programari genèric com el conegut packman.



Gràcies a mantenir centralitzades en servidors les dades i la funcionalitat bàsica de la organització, un cop instal·lat l'antivirus i les configuracions automàtiques no es necessitarà més manteniment que el que requereixin els propis servidors interns o els provocats per canvis substancials en la infraestructura de la xarxa. Per facilitar el manteniment del maquinari seria convenient tenir sempre disponible algunes peces de recanvi, com un parell de targetes Ethernet, discos durs, ventiladors de CPU i algun teclat; és a dir, aquelles peces que puguin ser bescanviades ràpidament per qualsevol informàtic.

Cal tenir present que en el moment d'instal·lar qualsevol actualització, l'Updater Applet demanarà la clau d'administrador per poder modificar els arxius en qüestió. Per tant, cada empleat ha de conèixer la clau de *root* del sistema i caldrà avisar-los del perill que això suposa en els plans de formació, com es veurà més endavant. Es pot considerar un fet positiu donar la llibertat i motivació necessària a cada usuari perquè pugui mantenir al dia el programari de la seva pròpia màquina.

En cas que no es vulgui que els empleats coneguessin la clau de *root* per motius de seguretat, les actualitzacions les podrien fer els tècnics de manera remota. Es poden realitzar fent servir un dels programes tipus VNC (*Virtual Network Computing* o programació virtual per xarxa) els quals permeten també l'assistència remota en cas de problemes tècnics. Aquests programes fan servir el model client/servidor per controlar a distància una màquina, i en cas que sigui necessari, permeten reparar una estació de treball des de qualsevol punt connectat a Internet de manera immediata. Resulta lògic pensar que el fet que els usuaris disposguin de servei tècnic immediat augmenta en gran mesura el grau de satisfacció dels propis empleats i la direcció.

Els sistemes GNU/Linux solen incloure un servidor VNC per defecte, que cal que l'usuari activi quan vulgui rebre assistència tècnica remota. Per raons de seguretat, no sembla bona idea deixar-lo activat per defecte, encara que la màquina no sigui visible a Internet.



Fig: Activació de la gestió remota al panell de configuració del sistema

A l'altra banda de la comunicació, el tècnic pot controlar la màquina fent servir un client de VNC degudament autenticat. A la figura següent es mostra la interfície gràfica d'un d'aquests clients d'escriptori remot, el que inclou KDE anomenat KDRC (*KDE Desktop Remote Client*).

És important tenir en compte que aquests programes són perillosos en el sentit que si un atacant es fa amb el control d'una sola màquina pot arribar a comprometre la integritat de tot el sistema. Per aquest motiu no sembla una mala idea fer servir clients VNC que xifrin i autèntiquin les dades que viatgen entre totes dues màquines per evitar suplantacions, i aquest no és el cas del KDRC. De totes maneres, el tècnic que dona assistència pot redirigir el port de la connexió TCP/IP d'aquest programa a un port segur, a fi d'establir-hi un túnel SSH (Secure Shell). Curiosament, SSH va ser creat precisament per controlar màquines de manera segura des d'una consola del sistema.



Fig: Client de connexió remota KRDC

El programa de manteniment també ha de definir les polítiques pel que fa a les còpies de seguretat. Ja s'ha vist que es pot fer directament en unitats de *backup* de gran capacitat. Cal decidir quan es faran les còpies -diàries, setmanals, mensuals,etc- i quines seran les dades que s'emmagatzemaran. També es pot definir un procés de copia total o incremental, és a dir, guardar només les dades que hagin canviat des que es va fer la darrera còpia de seguretat.

8. Pla de formació als usuaris

Un punt bàsic per a l'acceptació del nou sistema per part dels empleats és elaborar un pla lleuger de formació als usuaris per treure'ls la por i la creença que GNU/Linux és un sistema operatiu difícil, lleig, i només per a informàtics.

El primer que cal explicar és el perquè de la migració: eficiència, seguretat, estabilitat, millores en la productivitat, optimització dels recursos, cost, recuperació d'arxius en cas de tall elèctric gràcies al *journaling* del sistema de fitxers ext3, etc. En altres paraules, s'han d'explicar les millores que incorporà a la seva feina.

Es pot continuar explicant la funcionalitat més bàsica de l'entorn d'escriptori instal·lar amb les similituds i millores respecte al sistema operatiu anterior: arrossegar i deixar anar icones entre finestres per copiar o moure arxius, entendre el sistema de permisos dels arxius a GNU/Linux, moure's pel menú d'aplicacions organitzades per categories, etc. També se'ls pot ensenyar a canviar l'aparença i interactivitat amb l'escriptori per millorar-ne l'experiència: crear llançadors d'aplicacions a la carpeta d'escriptori, canviar el fons de pantalla o incorporar efectes 3D amb OpenGL, afegir mini-aplicacions d'escriptori o gadgets, etc.

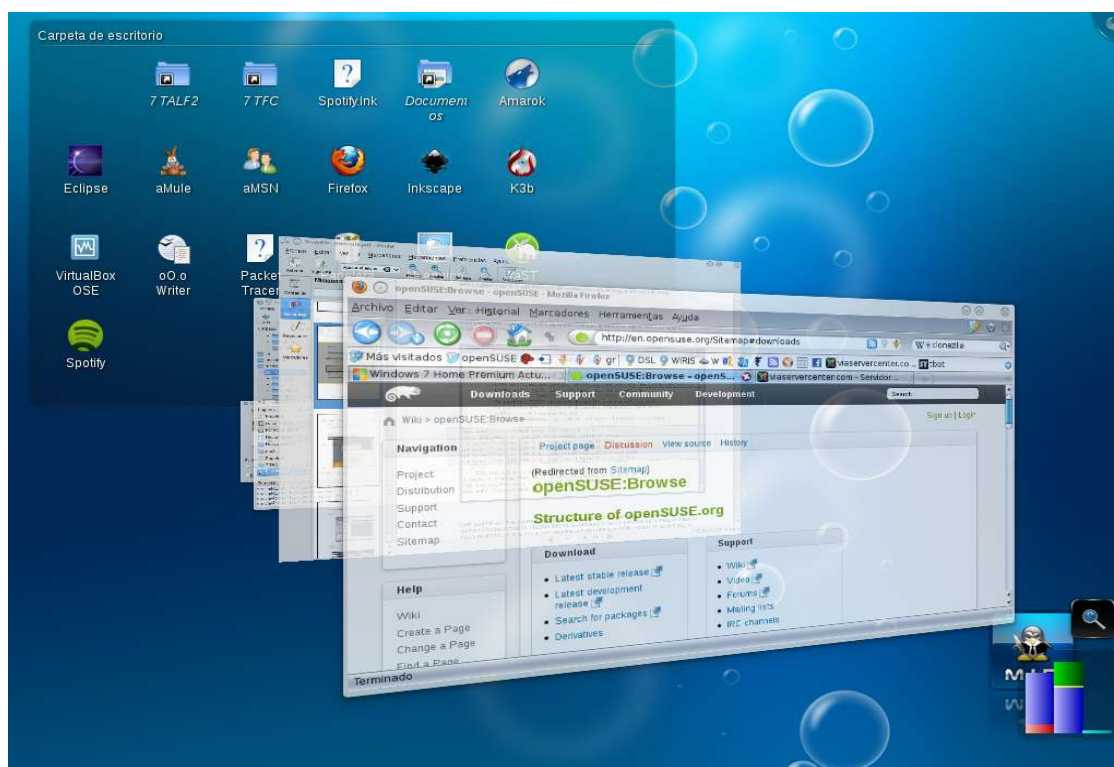


Fig: Efectes d'escriptori basats en OpenGL inclosos a KDE

En principi els empleats no necessiten instal·lar programari degut a que ja disposen de tot allò que necessiten. Però en cas que necessitin instal·lar-ne, se'ls pot indicar els millors llocs d'on trobar-lo (repositoris de confiança). openSUSE permet cercar i descarregar tota mena de paquets "auto-instal·lables" directament d'internet. No és necessari compilar el codi dels programes més comuns.

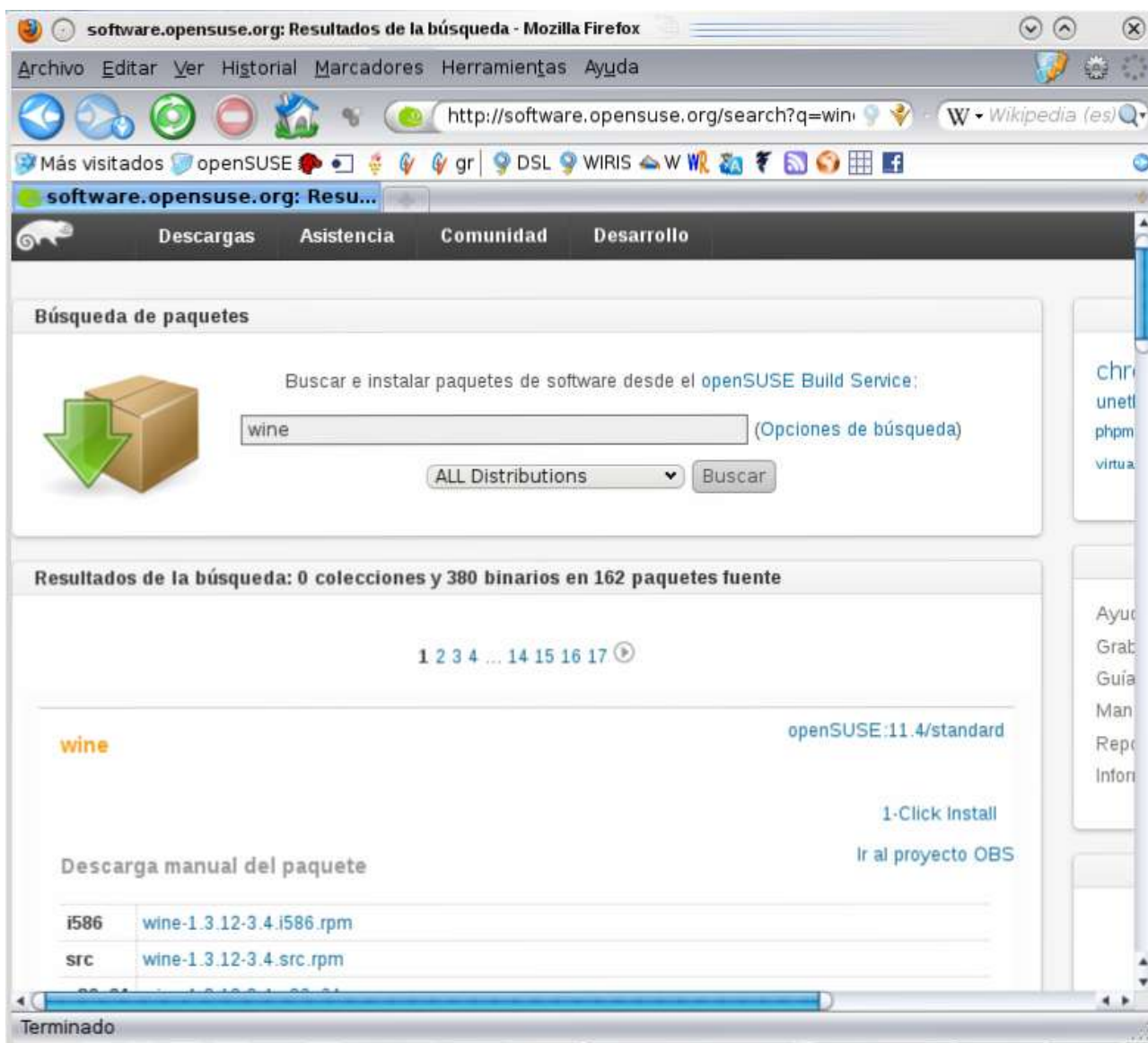


Fig: Descàrrega de paquets "1-click Install" per openSUSE des de la pàgina <http://software.opensuse.org>

I en cas de necessitar instal·lar i executar programes basats en la plataforma Windows ho poden fer a través de l'interpret Wine (Wine Is Not an Emulator).



Fig: Instal·lació i execució de programes per MS Windows amb Wine

Es pot continuar amb unes pinzellades de *l'openOffice* i *Firefox*, encara que degut a la seva popularitat segur que ja els coneixeran. Per acabar, caldria explicar com s'estructura el portal intern, com es poden trobar les aplicacions més generals que incorpora, la documentació, i com es poden compartir i protegir els arxius per la xarxa.

9. Web Interna

Com s'ha dit varies vegades al llarg d'aquest text, el portal intern serà el punt d'accés principal per a la interacció amb el sistema informàtic del consistori i per tant, la primera pàgina que mostrarà el navegador tot just obrir-se.

El portal ha d'implementar una secció comuna i accessible per tots els empleats, on apareixeran les circulars o notícies de comunicació interna. També es pot implementar l'accés als arxius comuns a tota la organització (documentació, formularis, plantilles, manuals d'ajuda, banc d'imatges, etc) i una secció a mode de "xarxa social" que permet cercar perfils d'altres usuaris i deixar comentaris.

The screenshot shows a web browser window displaying the internal portal of the Ayuntamiento de Villalba Soleada. The browser's address bar shows the file path: file:///media/FLASH DRIVE/7 TFC/Portal 2.0/Home1024.html. The page layout includes a navigation menu with items like 'Acercade', 'Comunicación', 'Archivos', 'Nuestra organización', and 'Personas'. A user profile for Sergio Morente Fernández is visible, along with a calendar for June 2011 and a news section titled 'Elecciones' featuring a large star graphic. The page also contains a workflow section and a project section for 'Proyecto Intranet'.

Fig: Exemple de portal corporatiu

També incorpora accés a recursos exclusius per cada usuari, com accés als arxius privats o als arxius corresponents al seu grup o grups d'usuaris guardats al servidor SAMBA, i de manera anàloga, les aplicacions corresponents al seu grup. A més, inclou via webmail accés a la bústia personal de correu intern, tal i com fa, per exemple, el servei de correu de Google. Es pot implementar tota mena d'eines, com per exemple una agenda de tasques per fer o un blog personal.

Tot això es pot realitzar fent servir LDAP per l'autenticació davant el servidor adequat i l'us d'una aplicació que gestioni l'intercanvi de dades amb el servidor de fixers, de correu o de base de dades, i que generi una sortida en HTML per poder-la mostrar en el navegador(servida per Apache). Moltes d'aquestes funcionalitats ja les inclou el programa ERP que hem vist anteriorment.

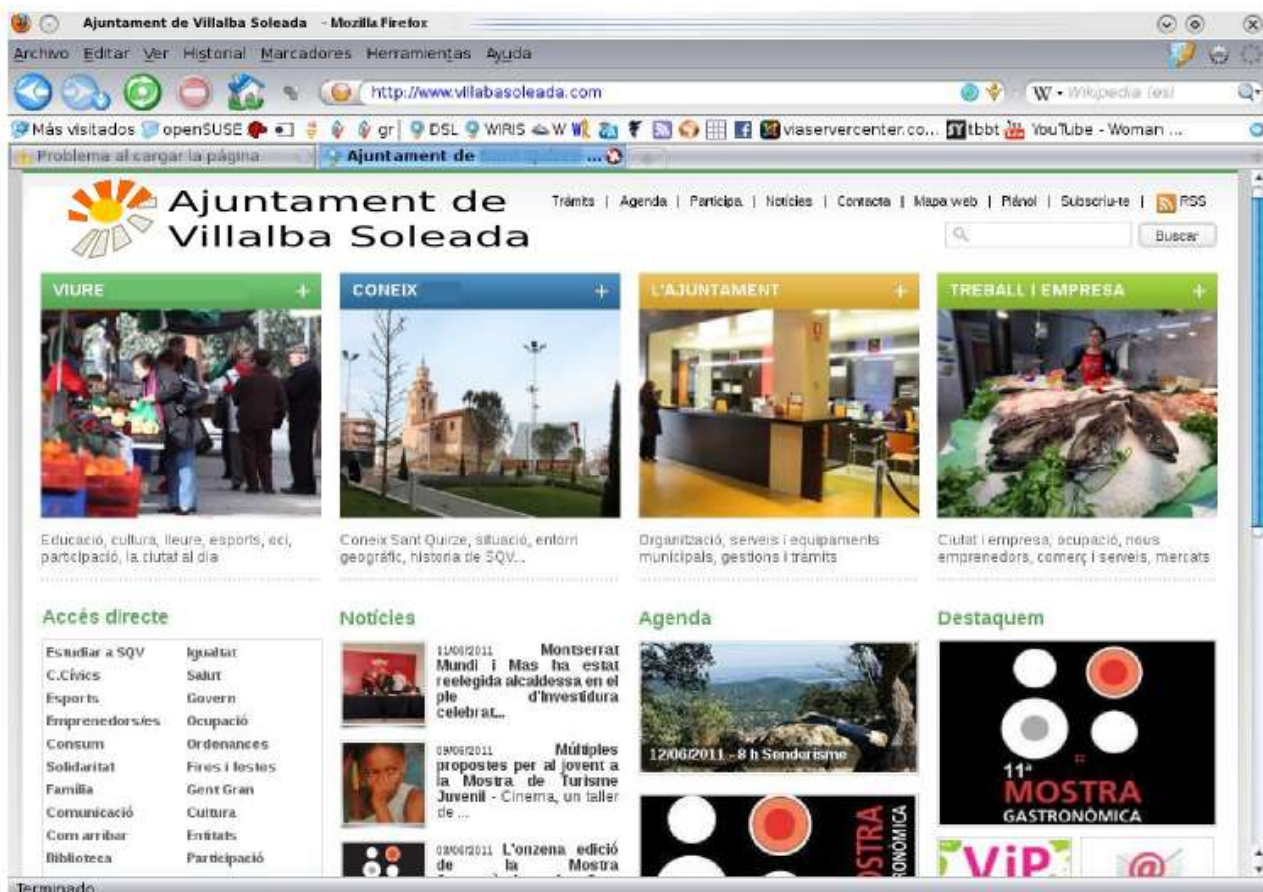
The screenshot shows a web application interface. On the left is a sidebar with a 'Menú' section containing links: 'Aplicaciones y software', 'Herramientas externas', 'Herramientas online', 'Procedimientos internos', 'Servicios internos', and 'Soporte y foros de ayuda'. Below this is a dropdown menu for 'Procedimientos internos'. Underneath is an 'Enlaces relacionados' section with links: 'Políticas', 'Procedimientos', and 'Mis procedimientos'. The main content area is titled 'Reserva de salas' and contains the text 'Desde aquí puedes reservar una sala en tu oficina'. It features a form with the following fields: 'Ubicación' (a dropdown menu set to 'Edificio'), 'Día' (a text input field with a calendar icon), and 'Hora' (a time range selector set to 'de 10:10 a 10:10'). An 'Enviar' button is located at the bottom of the form.

Fig: Aplicació “Reserva de salas” integrada en el portal.

10. Web del municipi

En aquest web s'ofereix tota la informació d'interès, de caire general, als ciutadans i turistes que visitin el municipi. Degut a que ofereix informació pública, s'ha de garantir l'accés des d'Internet, i és per aquest motiu que el servidor que ofereix aquest servei es col·loca fora de la VPN. A més, ens diuen que aquest web reporta uns 4.000 accessos diaris, i per aquest motiu, si es col·loqués en el mateix segment que els altres servidors es podria arribar a col·lapsar la xarxa interna.

Es pot oferir aquest servei mitjançant un servidor Apache amb una connexió HTTP publica per a les dades generals, i a través d'una connexió segura HTTPS, també oferta per Apache, per permetre als ciutadans realitzar els seus tràmits per internet.



11. Conclusions

Al llarg de tot aquest treball hem vist que GNU/Linux és perfectament vàlid i funcional per cobrir la funcionalitat informàtica que necessita una petita o mitjana organització. És un sistema madur, amb gairebé aplicacions per a qualsevol ús, i ben estudiat, i per aquest motiu sol incorporar la solució més eficient, i corregir les vulnerabilitats més ràpidament.

També hem pogut deduir que l'estalvi en llicències pot arribar a ser considerable. Si ens centrem només en el que hauria costat l'actualització a MS windows 7 i la llicència de MS Office tindriem un cost de $379+285=664$ euros per estació, un preu que com s'ha vist, és fins i tot superior al de l'adquisició del maquinari (dades extretes de la botiga en línia de Microsoft, <http://emea.microsoftstore.com/es/es-ES>).

A mode de resum, vegem com s'han solucionat els requisits de l'enunciat:

- *Dissenyar la infraestructura informàtica per connectar 100 màquines distribuïdes en quatre edificis:* S'implementa una LAN per edifici i aquestes s'interconnecten mitjançant túnels VPN.
- *Servidors:* Es necessita un servidor de fitxers (SAMBA), un de Bases de dades (PostgreSQL), un parell de servidors web (Apache, un per la intranet i un altre per la web del municipi), un servidor d'aplicacions (Glassfish), un de correu (Postfix), un DNS (Bind), VPN (openVPN) i LDAP (openLDAP). Tots s'ubiquen a la seu central.
- *Emmagatzematge remot de les dades dels usuaris amb limitació d'espai i informació comuna:* Es configura el servidor SAMBA per gestionar els privilegis per usuaris i grups emmagatzemats al directori LDAP, on es guarda per cada usuari els grups als què pertany i la quota de disc.
- *Recursos d'impressió per tots els empleats:* Impressores compartides per xarxa i gestionades per servidors CUPS.
- *Polítiques de seguretat: Filtratge de la navegació per equip i usuari:* s'estableixen regles restrictives als tallafocs i es permet la navegació a un rang determinat d'adreces (subnetting).
- *Restricció de correus personals:* L'accés al servei de correu electrònic es farà exclusivament via webmail intern.
- *Eines ofimàtiques:* S'instal·la la suite openOffice o LibreOffice a cada estació.
- *Web interna:* Punt d'accés centralitzat a tot el sistema informàtic, incloent les aplicacions d'ús més habitual. S'accedeix a través d'un navegador (Firefox) instal·lat a cada estació.

S'implementa amb l'ajut d'un ERP(*openBravo*). Funciona sobre el servidor Apache intern, amb connectivitat amb els servidors d'aplicacions, bases de dades, fitxers i correu electrònic.

- *Web del municipi*: Ofert per un servidor Apache dins una DMZ per permetre l'accés des de l'exterior i protegir la xarxa interna. Admet connexions segures i connexió amb el servidor d'aplicacions per les gestions dels ciutadans.
- *Manteniment i actualitzacions*: Configuració de les actualitzacions automàtiques a cada estació o actualitzacions diferides per gestió remota. Còpies de seguretat periòdiques a una unitat de *backup* de gran capacitat.
- *Pla de formació als usuaris*: Avantatges dels sistemes GNU/Linux, funcionalitat bàsica de l'entorn d'escriptori, personalització de la interfície gràfica, instal·lació de programari, ús d'un intèrpret de programes per *MS Windows* i funcionalitat bàsica de les eines ofimàtiques i el navegador.

12. Bibliografia

[1] **González Barahora, J.; Seoane Pascual, J.; Robles, G.**(2003) *Introducción al Software libre*. Barcelona: Fundació per la Universitat Oberta de Catalunya

[2] **Novell, Inc. and contributors** (2006-20011) *openSUSE 11.4 Start-up; Reference Guide; security Guide*

[3] **Perramon Tornil, X.** (2008) *Mecanismes de protecció; Mecanismes de prevenció*. Barcelona: Fundació per la Universitat Oberta de Catalunya

[4] **García Alfaro, J.** (2008) *Filtrado y registro de paquetes con Iptables*. Barcelona: Fundació per la Universitat Oberta de Catalunya

[5] **Serra Ruiz, J.; Colobran Huguet, M.; Arqués Soldevila. J.M.; Marco Galindo, E.** (2008) *Administració d'usuaris*. Barcelona: Fundació per la Universitat Oberta de Catalunya

[6] **López Jiménez, W.** (2006-2007) *VPN en servidor Linux y clientes Windows/Linux con OpenVPN + Shorewall* [en línia] <http://www.alcancelibre.org/staticpages/index.php/openvpn-clients-win-linux-shorewall-P1>

[7] **Michael Donnelly** (2000), Una introducció a LDAP [en línia] http://www.ldapman.org/articles/sp_intro.html

[8] **Santo Otero, D.** (2007) *Mitos y realidades: Linux y los virus*. Todo Linux número 90.

