Administració d'usuaris

PID_00275590

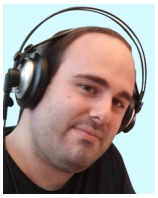
Miguel Martín Mateo
Javier Panadero Martínez
Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

Temps mínim de dedicació recomanat: 5 hores

Universitat Oberta de Catalunya

Miguel Martín Mateo

Llicenciat en Matemàtiques per la Universitat de Barcelona (UB). Màster en Programari Lliure per la Universitat Oberta de Catalunya (UOC). Des de 2006, col·labora amb la UOC en assignatures del màster de Programari Lliure i el seu TFM, i en l'assignatura Administració de xarxes i sistemes operatius i el seu TFG. Més de vint anys d'experiència professional. Actualment, és consultor sobre l'administració de sistemes en aspectes relacionats amb l'automatització de processos i en el compliment i auditoria en entorns Windows i Unix a la multinacional Accenture. També té una àmplia experiència en el desenvolupament d'aplicacions relacionades amb caixers automàtics.

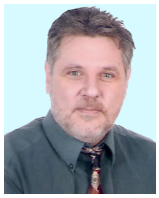


Javier Panadero Martínez

Enginyer informàtic i doctor en Computació d'Altes Prestacions per la Universitat Autònoma de Barcelona (UAB). Des de 2019, és professor dels Estudis d'Informàtica, Multimèdia i Telecomunicació de la Universitat Oberta de Catalunya (UOC). Director del màster universitari en Enginyeria Computacional i Matemàtica. Ha elaborat diversos materials sobre administració de sistemes i programació. Els seus interessos de recerca inclouen la computació paral·lela i distribuïda, l'optimització i simulació de sistemes complexos i els algorismes intel·ligents.

Jordi Serra Ruiz

Doctor en Informàtica per la Universitat Oberta de Catalunya (UOC). Enginyer superior en Informàtica per la Universitat Autònoma de Barcelona (UAB). Màster en Informàtica Industrial. Actualment, és professor de la UOC i és el director acadèmic del màster de Seguretat Informàtica de la UOC. Pertany al Grup de Recerca de Seguretat de la Informació KISON i és membre de l'IEEE.



Miquel Colobran Huguet

Doctor en Informàtica per la Universitat Autònoma de Barcelona (UAB). Consultor a la Universitat Oberta de Catalunya (UOC) d'assignatures sobre administració de sistemes i seguretat, i també d'informàtica i legislació en el grau i màster d'Informàtica i Multimèdia. Ha elaborat diversos materials i llibres sobre administració de sistemes, seguretat, informàtica forense i legislació aplicada a les tecnologies de la informació. La seva recerca s'emmarca dins de la seguretat, la influència de les TIC a la societat i l'enginyeria del coneixement.

Josep Maria Arqués Soldevila

Llicenciat en Informàtica per la Universitat Autònoma de Barcelona (UAB). Va fer el treball de recerca al Departament d'Enginyeria de la Informació i de les Comunicacions (DEIC) de l'esmentada universitat. Ha treballat com a professor ajudant i associat al DEIC, i ha exercit de consultor de diverses assignatures de la Universitat Oberta de Catalunya (UOC). Actualment, exerceix d'analista en informàtica forense.

Eduard Marco Galindo

Enginyer superior informàtic per la Universitat Politècnica de Catalunya (UPC). Des de 2003, col·labora amb la Universitat Oberta de Catalunya (UOC) com a tutor i professor col·laborador en el grau d'Informàtica i en el màster de Seguretat. Especialitzat en l'àmbit de l'Administració de Sistemes, ha format part de l'equip de redacció del temari de l'assignatura Administració de xarxes i sistemes operatius (AXSO) i ha exercit de consultor i tribunal en el seu TFG. En l'àmbit professional, treballa des de fa més de vint anys en el món dels sistemes informàtics, especialment en la capa *middleware* d'empreses i governs. Especialitzat en l'arquitectura de sistemes en l'àmbit empresarial, i també en la gestió d'equips de projecte i de serveis gestionats. Darrerament, iniciant una nova etapa professional i de recerca en projectes d'intel·ligència artificial en l'àmbit empresarial, forma part de l'equip tècnic de disseny i implementació de solucions.

Primera edició: setembre 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Autoria: Miguel Martín Mateo, Javier Panadero Martínez, Jordi Serra Ruiz, Miquel Colobran Huguet, Josep Maria Arqués Soldevila, Eduard Marco Galindo
Producció: FUOC

Índex

Introducció

En aquest mòdul ens centrarem en l'usuari i en tot el que hem de saber en relació amb el següent:

- Servidors
- Estacions de treball
- Programari
- Dades
- Incidències
- Formació

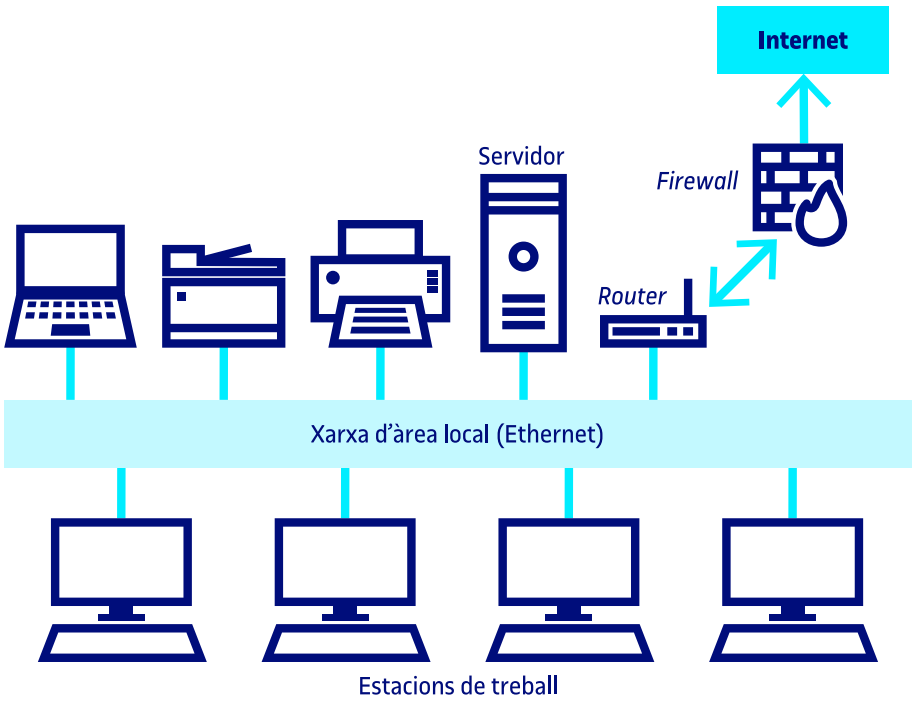
La funció del sistema informàtic és donar suport i servei als usuaris, i ajudar-los a fer la seva tasca dins l'organització.

La filosofia del departament

Hi ha autors que tendeixen a considerar el servei informàtic com a negoci i els usuaris com a clients. En aquests casos, la filosofia del departament informàtic és l'organització, el treball i l'actuació en tot moment.

La figura 1 mostra a grans trets un esquema on es poden veure totes les xarxes. Com es pot observar, hi ha dos elements diferenciadors: les estacions de treball i els servidors.

Figura 1. Esquema general d'una xarxa



Per tant, el tractament dels usuaris, des del punt de vista de l'administració, el podem dividir en uns serveis o funcions que necessàriament s'han de fer a la part «servidor» i uns serveis o funcions que s'han de fer a la part «usuari» o client.

Primer veurem com es fa el disseny de l'entorn d'usuaris per la part que afecta els servidors. Un bon disseny simplifica l'administració i ajuda els usuaris a tenir un entorn més coherent i robust. Això vol dir que a mitjà termini també es converteix per a ells en una eina més senzilla de fer servir.

Després seguirem amb la instal·lació, la configuració i el manteniment de les estacions de treball. Una configuració ben pensada i un mecanisme de recuperació de les configuracions permeten donar un bon servei d'avaries i, una vegada més, simplifiquen l'administració de les estacions de treball. Amb això s'acaba la part que afecta l'entorn de l'usuari.

Els punts següents tracten de la formació i l'atenció de les incidències de l'usuari. Són tan importants com els anteriors, i sovint es porten poc a la pràctica. La formació redueix costos a mitjà termini, ja que estalvia temps del departament d'informàtica, perquè forma el personal de l'organització i el fa autosuficient en moltes tasques, i una gestió correcta de les incidències[1] estalvia costos a l'organització i també, indirectament, al departament d'informàtica.

(1)Moltes vegades s'anomena CAU o *helpdesk*.

Objectius

Els materials didàctics d'aquest mòdul contenen les eines necessàries perquè l'estudiant assoleixi els objectius següents:

1. Saber dissenyar un entorn per als usuaris adient a l'organització.

2. Saber diferenciar les tasques que afecten els servidors de les que afecten les estacions de treball.

3. Saber dissenyar un entorn per a les estacions de treball útil per als usuaris i que sigui com més senzill d'administrar millor.

4. Saber fer del departament d'informàtica un servei àgil per respondre a les incidències dels usuaris.

5. Saber que les tasques es poden sistematitzar en procediments.

6. Conèixer les responsabilitats de l'administrador d'usuaris.

7. Conèixer eines per configurar, mantenir i recuperar les estacions de treball en situacions problemàtiques.

1. Disseny de l'entorn d'usuaris

Des del punt de vista de maquinari, el sistema informàtic té els servidors, la xarxa i les estacions de treball. Des del punt de vista de programari, té els sistemes operatius i les aplicacions. No n'hi ha prou amb ajuntar-los. Hem de dissenyar la manera que interactuaran entre si els diferents elements per obtenir el resultat desitjat.

Quan definim el que l'usuari trobarà quan es connecti als servidors de l'organització, es dissenya el que s'anomena entorn d'usuari, que afecta tant l'estètica com els recursos i les aplicacions disponibles.

Dissenyar l'**entorn d'usuari** vol dir preparar tot allò amb què es trobarà l'usuari quan faci servir la informàtica de l'organització.

Els criteris i objectius que cal seguir en el nostre disseny seran els següents:[2]

[(2)]La llista és aproximada.

- Ha de ser simple de fer servir i intuïtiu per a l'usuari.
- Ha de proporcionar un entorn homogeni a tots els usuaris.
- Si canvia d'ordinador o de lloc de treball, l'entorn (programari i maquinari) no li ha de resultar estrany.
- El sistema ha de ser ràpid, en temps de resposta dels servidors i en resposta de velocitat de la xarxa.
- Ha de donar un bon nivell de seguretat.
- Ha de ser fàcil d'administrar.
- Ha de ser fàcil d'actualitzar el programari.
- Si l'ordinador falla, ha de ser fàcil de reinstal·lar.
- Si l'ordinador es desconfigura, ha de ser fàcil de reconfigurar.
- Si l'ordinador falla, no s'ha de perdre informació (el mínim possible, i no hauria de ser crítica).
- Ha de ser senzill de fer còpies de seguretat.

Reflexió

Penseu que l'entorn de la vostra organització compleix aquests punts? Hi falta algun objectiu que considereu important? Comenteu-ho al fòrum de l'assignatura.

- Ha de ser fàcil de poder respondre davant d'una situació de desastre d'una estació de treball.

La utopia

Amb aquesta relació d'objectius i criteris de disseny, el primer que sembla evident és intentar aconseguir el següent:

- Que tot l'entorn de programari tingui una interfície homogènia.
- Que tot l'entorn de maquinari de les estacions de treball sigui homogeni.

Malgrat que són dos objectius molt interessants, difícilment es poden dur a terme a la pràctica, per tant, és més factible considerar que l'entorn d'usuari i de maquinari siguin el més homogenis possible.

Tenint presents aquests objectius, el nombre de servidors corporatius que hi ha, la xarxa existent, les estacions de treball instal·lades, el coneixement sobre els llocs de treball de l'organització, l'estructura dels departaments i de l'organització, etc., hem de dissenyar l'entorn en què els usuaris treballaran moltes hores diàries. Per tant, és important una planificació acurada.

Les contradiccions

Els criteris i objectius de disseny sovint entren en contradiccions. La seguretat acostuma a contradir-se amb la comoditat i la velocitat. El resultat final sempre és una solució de compromís entre aquests elements.

El disseny de l'entorn d'usuaris afecta tant els servidors com les estacions de treball i, per tant, s'ha de fer tenint en compte totes dues parts (com una unitat), ja que de fet treballen conjuntament, de manera que no és possible el disseny general d'una part sense tenir en compte l'altra. Una vegada establertes les línies mestres d'aquest disseny, es pot passar a detallar cadascuna de les parts.

1.1. Necessitats generals de l'usuari

Totes les organitzacions són diferents. Malgrat això, les necessitats informàtiques dels usuaris es poden generalitzar una mica. Podem dir que tots els usuaris tenen les necessitats següents pel que fa al sistema informàtic:

1) Una estació de treball. Generalment és un ordinador. És possible que alguns usuaris particulars necessitin dispositius especials com ara gravadores de DVD, escàners, impressores locals, impressores d'etiquetes, etc.

2) Un lloc on es pugui imprimir. Sigui una impressora local o en remot compartida amb altres usuaris. És habitual a les empreses tenir a cada departament una impressora compartida connectada a la xarxa, on els usuaris podem enviar els seus treballs, en comptes de tenir cada usuari la seva impressora local.

3) Espai per guardar la informació. Sigui en local al disc de l'estació de treball de l'usuari o a un espai remot als servidors.

4) Programari per treballar. Tots els programes i aplicacions que necessitarà l'usuari per treballar.

Genèricament, quant al programari que necessita l'usuari, el podem dividir en diverses categories:

- **Programari de base**: sistema operatiu i aplicacions bàsiques de comunicacions als servidors.
- **Programari d'ofimàtica**: són els paquets d'ofimàtica, que normalment inclouen un full de càlcul, un processador de textos, una base de dades i una agenda.
- **Programari de comunicacions**: generalment hi podem incorporar el correu electrònic, un visualitzador d'internet (Internet Explorer, Firefox, Chrome, etc.) i programari per fer videotrucades (Skype, Hangouts, etc.).
- **Aplicacions específiques**: és el grup d'aplicacions que engloba programes dependents de l'organització i, fins i tot, del departament, com ara programes de facturació, comptabilitat, disseny gràfic, control de la producció, nòmines, etc.

Reflexió

Penseu que hi falta alguna categoria de programari? Comenteu-ho al fòrum de l'assignatura.

Quan s'accedeix a la majoria d'aplicacions específiques, normalment demanen un usuari i una contrasenya (addicionals als que s'han posat quan s'entra a la xarxa) per accedir-hi. Aquesta identificació, que normalment és per a aplicacions que tenen bases de dades en servidors, serveix per assignar privilegis dins de l'aplicació, de manera que la part client és idèntica per a tothom i el que s'hi pot fer només depèn de l'usuari que hi entra.

Single sign on

Es busca identificar-se una sola vegada i poder accedir a tots els sistemes. Hi ha diversos mecanismes com ara:

- E-SSO
- Web-SSO
- Kerberos
- OpenID

L'accés a aquestes aplicacions (tant si són estàndards com específiques) ha d'estar controlat d'alguna manera, ja que no tothom té accés a tota la informació de l'organització. Per manipular la informació de l'organització (és a dir, crear-la, modificar-la o consultar-la), en principi, no cal que l'usuari sàpiga on està aquesta informació, sinó només la manera d'accedir-hi i com manejar-la per treballar.

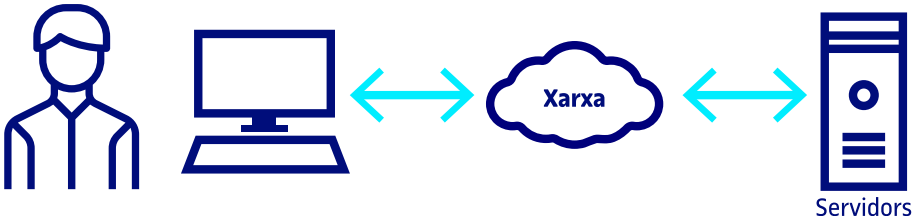
Perquè funcionin correctament, totes aquestes necessitats s'han de presentar en un entorn que sigui agradable i fàcil d'utilitzar. Altrament, el sistema, en lloc d'ajudar a la tasca, el que fa és dificultar-la, i, en comptes de complir l'objectiu global de millorar el rendiment, s'aconsegueix el contrari, disminuir-lo i dificultar el flux d'informació per tota l'organització.

Encara que els usuaris tenen rols molt diferenciats a l'empresa segons el seu càrrec, tots els usuaris d'una organització es poden unir en **grups de necessitats** molt similars. No hi haurà gaires grups i tampoc no seran gaire diferents.

1.2. El sistema informàtic i l'usuari

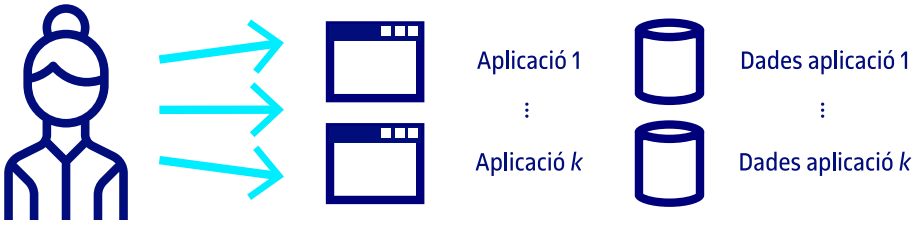
L'esquema global que es pot arribar a imaginar un usuari del sistema informàtic és semblant al que mostra la figura 2.

Figura 2. Esquema del sistema informàtic



Mentre que la imatge que es podria fer de les aplicacions és com la que mostra la figura 3.

Figura 3. Esquema de les aplicacions



Un usuari, però, no sap on estan instal·lades físicament les aplicacions ni on «viuen» realment les dades dins la xarxa informàtica de l'organització.

Misteris informàtics

Sovint un usuari considera sorprenent anar a un altre ordinador, connectar-se i trobar totes les dades i els programes. De la mateixa manera, si s'ha guardat alguna cosa (en local), quan es va a un altre ordinador i no hi és, no s'entén, ja que «ho ha guardat com sempre», i ensenya molts fitxers com a demostració i, en canvi, el que ha guardat fa una hora «ha desaparegut». Ningú no neix ensenyat i és molt normal que passi. A poc a poc es va educant l'usuari en aquestes noves eines de treball.

A partir de la llista d'objectius que hem fet abans i de la visió que sabem que els usuaris tenen de la xarxa informàtica, veurem diversos mecanismes de control d'accés que ens permetran dissenyar l'entorn d'usuari.

1.3. El control d'accés

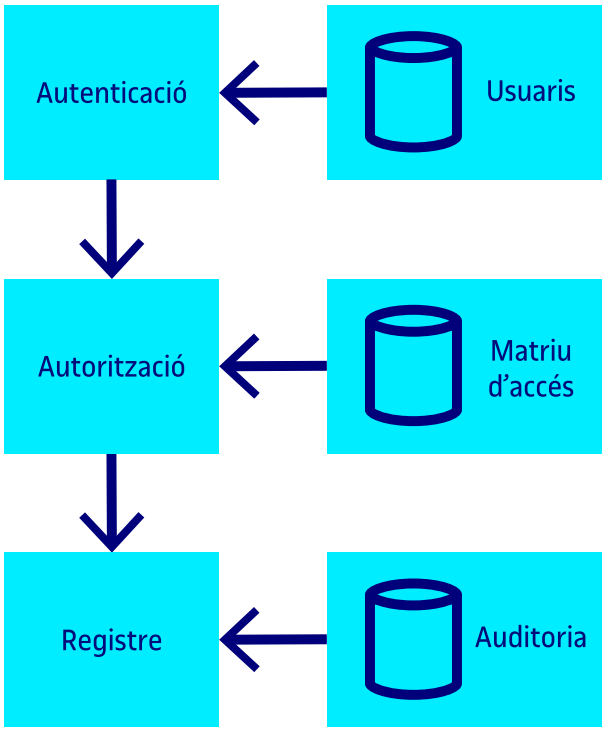
Una de les qüestions fonamentals en el disseny de l'entorn d'usuari és aconseguir que aquest accedeixi únicament a allò que necessiti. Per accedir a un recurs del sistema informàtic, l'usuari s'ha d'identificar (**autenticar**). Una vegada s'ha identificat, el sistema controla (**autoritza**) l'accés als recursos del sistema informàtic i registra (**audita**) com s'utilitza cada recurs,[3] com es veu reflectit a la figura 4.

[3] Es coneix com a model de seguretat AAA (*authentication, authorization* i *accounting*).

Nota

El tema del control d'accés és un tema molt extens de la seguretat i depassa els objectius d'aquests materials. Nosaltres només veurem aquella part que ens és útil per al disseny del sistema informàtic.

Figura 4. Esquema del model de seguretat AAA



Principi de privilegi mínim

Atorgar el conjunt de privilegis més restrictiu (l'autorització més baixa) necessària per dur a terme la seva tasca.

Font: **Departament de Defensa**. «Document de criteris d'avaluació dels sistemes informàtics de confiança del Departament de Defensa». *Llibre Taronja* (DOD-5200.28-STD).

L'**autenticació** és el procés de verificació de la identitat d'una persona o d'un procés que vol accedir als recursos d'un sistema informàtic. Habitualment es fa mitjançant el nom de l'usuari i contrasenya o *token* del procés.

Vegeu també

Vegeu més àmpliament l'autenticació al mòdul «Administració de la seguretat».

L'**autorització** és el procés mitjançant el qual el sistema autoritza l'usuari identificat a accedir als recursos d'un sistema informàtic.

L'autorització determina quin accés es permet a cada entitat. L'autenticació és el procés de verificació de la identitat d'una persona, mentre que l'autorització és el procés de verificació que una persona coneguda té l'autoritat per fer una certa operació. L'autenticació, per tant, ha de precedir l'autorització.

El **control d'accés** determina quins privilegis té un usuari dins el sistema informàtic i a quins recursos tindrà accés. Aquest control d'accés s'ha de pensar molt bé i acuradament, ja que podríem tenir problemes d'accés a informació privada d'altres persones o grups de l'empresa.

El **registre** de l'ús dels recursos és la informació de *log* guardada de l'activitat de l'usuari en el sistema informàtic.

1.3.1. Matriu de control d'accés

La matriu de control d'accés o matriu d'accés és un model formal de seguretat computacional usat en sistemes informàtics, que caracteritza els drets de cada subjecte respecte a tots els objectes del sistema. Els objectes són entitats que contenen informació i poden ser físics o abstractes. Els subjectes accedeixen als objectes i poden ser usuaris, processos, programes o altres entitats.

Els drets d'accessos més comuns són: accés de lectura (**L**), accés d'escriptura (**E**) i accés d'execució (**X**).

La taula 1 mostra un exemple de matriu d'accés. Les files de la matriu representen els dominis (o subjectes) i les columnes representen els objectes. Les entrades de la matriu consisteixen en una sèrie de drets d'accés. Per exemple, l'entrada $accés_{(i,j)}$ defineix el conjunt d'operacions que un procés, executant-se en el domini D_i, pot invocar sobre un objecte O_j.

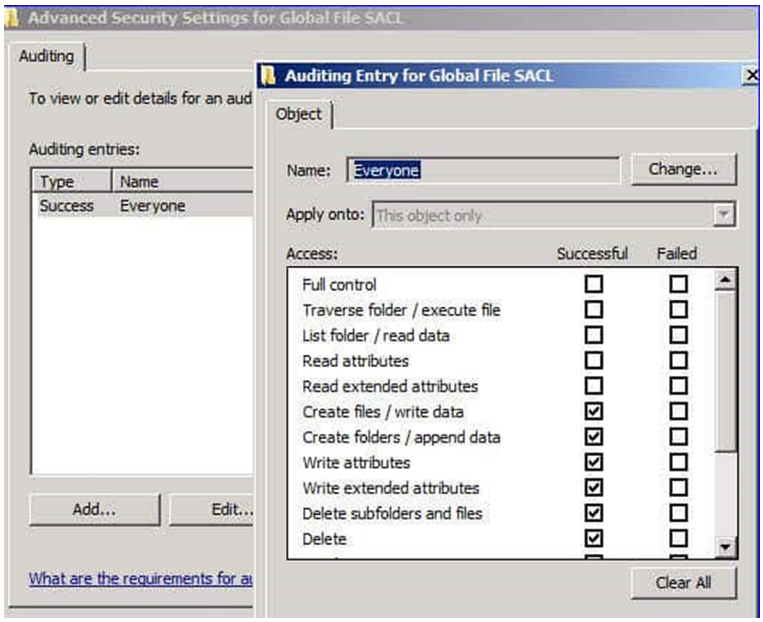
Taula 1. Exemple de matriu de drets d'accés

Domini	**Objecte**	
	Fitxer	**Directori**
D1	Lectura	Lectura Escriptura Execució
D2		Lectura Escriptura
D3	Execució	Lectura

1.3.2. Llista de control d'accés (ACL)

No s'acostuma a guardar la matriu ja que és molt gran. Una gran part dels dominis no tenen cap accés a la majoria dels objectes, per la qual cosa l'emmagatzematge d'una matriu enorme gairebé buida és un malbaratament de l'espai del disc. El que es fa és associar a cada objecte una llista (ordenada) amb tots els dominis que poden tenir-hi accés i la forma de fer-ho. Aquesta llista s'anomena **llista de control d'accés** (ACL) i un possible exemple es veu a la figura 5.

Figura 5. Llistat de control d'accés



1.3.3. *Single sign on*

Com ja s'ha comentat, és una expressió anglesa per identificar l'«inici de sessió únic» o «inici de sessió unificat» (*single sign on*, SSO), és a dir, un procediment d'autenticació que habilita un usuari determinat a accedir a diversos sistemes de l'organització amb una única instància d'identificació. Un exemple il·lustratiu podria ser que un cop ens autentifiquem a un equip no cal una nova autenticació per accedir al correu o a la missatgeria instantània.

Aquest sistema té els seus avantatges i inconvenients. Com a avantatge, podem dir que allibera l'usuari d'haver de fer múltiples inicis de sessió a les diferents aplicacions. Com a inconvenient, cal mencionar que si s'aconsegueix fer l'inici de sessió a l'estació de treball d'un usuari (o l'usuari ha deixat la sessió oberta) tenim accés a totes les aplicacions a què l'usuari té autorització sense haver de fer validacions.

1.4. Disseny del sistema informàtic

Veurem com podem aplicar la matriu d'accés en diversos dissenys i n'estudiarem els avantatges i inconvenients.

1.4.1. Mínima seguretat

Consisteix en un disseny que simplifica força l'administració, basant-se en els **criteris** següents:

Reflexió

Què en penseu, d'aquesta solució? Podeu opinar-ne al fòrum de l'assignatura.

- Tots els usuaris veuen tots els programes i totes les aplicacions.
- Tots els usuaris tenen permisos mínims (lectura i execució) per a tot.

- Les aplicacions específiques (com, per exemple, les bases de dades), que ja tenen permisos d'accés propis, queden controlades per la mateixa aplicació. No calen permisos especials.

- A les carpetes d'usuari només hi pot accedir el mateix usuari amb permisos de lectura, escriptura i execució.

Els **avantatges** d'aquest disseny són els següents:

1) Simplifica l'administració, ja que tots els usuaris són iguals i, per tant, crear un usuari no representa tenir res en compte.

2) Facilita la preparació de l'estació model.

3) Una vegada clonat un equip, gairebé no hi ha ajustament final.

4) Qualsevol usuari té permís per executar qualsevol aplicació, per la qual cosa la modificació dels esquemes de treball de l'organització no representa cap problema ni cap modificació en les estructures informàtiques creades.

5) El canvi de punt de treball no té el cost afegit d'instal·lar les aplicacions específiques per a aquell usuari, ja que totes estan disponibles a totes les estacions de treball.

6) L'entorn de treball és completament homogeni a tota l'organització, atès que tothom veu exactament el mateix.

7) Facilita la tasca de fer cerques d'informació dins el sistema informàtic, perquè tota la informació és «plana» (no està jerarquitzada ni protegida) dins el sistema.

8) L'usuari disposa de tot el potencial informàtic de l'organització.

9) Qualsevol canvi que comporti fer servir un nou programari no implica modificacions en el sistema informàtic.

Els **inconvenients** d'aquest disseny són els següents:

1) La idea de grup de treball, grup de persones, departament, etc., en definitiva, l'agrupació no queda inclosa en l'estructura informàtica, i això pot complicar l'administració en moments en què calgui incorporar-la per manipular la informació.

Vegeu també

Vegeu el subapartat «Creació de l'estació model».

2) La compartició d'informació entre grups d'usuaris no és fàcil, ja que el concepte de grup de persones no existeix. Per exemple, que tot un departament comparteixi la informació, sense que la resta de persones de l'organització no hi tinguin accés.

3) L'usuari es pot perdre una mica davant de tant programari, atès que pot no saber quin és «el seu» (quin ha de fer servir per treballar) i quin no.

4) Permetre que el directori d'un usuari, si l'usuari vol, sigui accessible a la gent del seu grup de treball no és possible. Si ho fa, quedarà automàticament obert a tota l'organització.

5) Pot ser negatiu que qualsevol persona de l'organització pugui executar qualsevol aplicació. Hi pot haver informació sensible que no ha d'estar a l'abast d'altres grups de l'organització.

6) Moltes peticions de grups d'usuaris respecte a la manipulació de la informació, especialment si és sensible, són molt complexes o, fins i tot, impossibles de fer.

7) Hi ha perill de manipulacions incorrectes amb resultats no desitjats.

1.4.2. Usuaris en grups

Es pot fer una segona solució modificant alguns dels criteris del disseny de seguretat mínima. Aquesta solució és més segura que l'anterior i es basa ens els **criteris** següents:

Reflexió

Què en penseu, d'aquesta solució? Podeu opinar-ne al fòrum de l'assignatura.

- Els usuaris s'uneixen en grups d'una manera natural dins l'organització, intentant reflectir aquesta situació dins el sistema informàtic.
- Un usuari només pot pertànyer a un grup.
- Una aplicació pot funcionar per a tothom o només per a un grup.
- Tots els usuaris tenen permisos mínims (lectura i execució) per als elements del grup.
- Tots els usuaris tenen permisos de lectura i execució per als elements generals (de tothom).
- Les aplicacions específiques (com, per exemple, les bases de dades), que ja tenen permisos d'accés propis, queden controlades per la mateixa aplicació. No calen permisos especials. Ara només veuen aquestes aplicacions els grups d'usuaris que les necessiten.

- A les carpetes d'usuari només hi pot entrar l'usuari amb permisos de lectura, escriptura i execució.

- Hem de tenir en compte les categories de programari que podríem trobar dins d'una organització.

Els **avantatges** d'aquest disseny són els següents:

1) Tots els usuaris són iguals per grups, per tant, crear un usuari representa tenir en compte a quin grup ha de pertànyer.

2) Qualsevol usuari només té permís per executar qualsevol aplicació del grup i totes les aplicacions comunes a tothom.

3) L'usuari només pot accedir a la informació del grup i a la informació comuna. Per tant, la informació de l'organització està molt més ben protegida.

4) No hi pot haver manipulacions incorrectes del programari, ja que ara només el poden executar els usuaris del grup.

5) L'entorn de treball és força homogeni a tota l'organització, però varia en la mesura que varien les aplicacions que veu l'usuari per treballar. Afortunadament, el paquet d'aplicacions comunes a tothom és el mateix, i això dona una sensació d'homogeneïtat molt important per a l'usuari.

6) L'usuari bàsicament disposa dels recursos de programari que necessita. Li facilita les coses saber que el programari que té a l'abast és el que ha de fer servir, i no com abans, que en veia algun que no havia d'utilitzar.

7) Ara la idea de grup de treball sí que s'inclou i és molt útil per compartir la informació en el grup i per treballar en aplicacions específiques d'una manera coordinada. Moltes vegades l'estructura de grups, com a conseqüència de les peticions que rep el departament d'informàtica, simplifica l'administració, perquè són per a qüestions característiques d'un grup de treball.

8) Ara es pot permetre que el directori d'un usuari, si l'usuari vol, sigui accessible a la gent del seu grup de treball. Si ho fa, queda automàticament obert només al seu grup de treball.

Vegeu també

Vegeu el subapartat «Necessitats generals de l'usuari».

Els **inconvenients** d'aquest disseny són els següents:

- Una modificació en els esquemes de treball pot representar modificar tots els permisos de les aplicacions i de les carpetes de treball dels grups, és a dir, haver de modificar les estructures informàtiques que s'han creat.

- El canvi de lloc de treball d'una persona, en cas que canviï de grup, implica modificar-ne el perfil, perquè passarà a tenir disponibles altres aplicacions i una part de les que tenia (les específiques del seu grup) les deixarà de tenir.

- La cerca d'informació dins el sistema és més complexa, atès que ara està organitzada per grups de treball dins l'organització.

- Instal·lar un programari nou pot ser un problema greu si l'han de fer servir diversos grups de treball.

- Compartir informació entre grups és complex.

1.4.3. Usuaris en múltiples grups

Aquesta solució és una extensió de l'anterior (usuaris en grup) i sorgeix del fet que alguns usuaris pertanyen a més d'un grup. El grup funciona molt bé per a la majoria dels casos, però per a alguns no és suficient. Si l'organització, per exemple, utilitza grups de treball dins el departament, o si es creen subgrups dins el grup de treball, es dona la situació que una persona pertany a més d'un grup a la vegada. Per tant, s'ha d'analitzar aquesta situació valorant, en primer lloc, els **criteris** que cal seguir:

Reflexió

Què en penseu, d'aquesta solució? Podeu opinar-ne al fòrum de l'assignatura.

- Els usuaris s'uneixen en grups d'una manera natural.

- Un usuari pot pertànyer a un grup o més.

- Una aplicació pot funcionar per a tothom o per a un o més grups.

- Tots els usuaris tenen permisos mínims (lectura i execució) per als elements del grup.

- Tots els usuaris tenen permisos de lectura i execució per als elements generals (de tothom).

- Les aplicacions específiques (com, per exemple, les bases de dades), que ja tenen permisos d'accés propis, queden controlades per la mateixa aplicació. No calen permisos especials. Ara només veuen aquestes aplicacions els grups d'usuaris que les necessiten.

- A les carpetes d'usuari només hi pot accedir l'usuari amb permisos de lectura, escriptura i execució.

Els **avantatges** d'aquest disseny són els següents:

1) Tots els usuaris són iguals per grups, per tant, donar d'alta un usuari representa tenir en compte a quins grups ha de pertànyer.

2) Qualsevol usuari només té permís per executar qualsevol aplicació dels grups als quals pertany i totes les aplicacions comunes a tothom. També té permís per accedir a la informació comuna del grup. Una modificació en els esquemes de treball pot representar haver de modificar tots els permisos de les aplicacions i de les carpetes de treball dels grups, és a dir, modificar les estructures informàtiques que s'han creat.

3) El canvi de lloc de treball d'una persona, en cas que canviï de grup, implica modificar-ne el perfil, perquè passarà a tenir disponibles altres aplicacions i una part de les que tenia (les específiques del seu grup) deixarà de tenir-les. Pot comportar modificar els grups a què pertany i la informació a la qual té accés.

4) L'entorn de treball és força homogeni a tota l'organització, però varia en la mesura que varien les aplicacions que l'usuari veu per treballar. Afortunadament, el paquet d'aplicacions comunes a tothom és el mateix, i això dona una sensació d'homogeneïtat molt important per a l'usuari.

Els **inconvenients** d'aquest disseny són els següents:

1) Ara sí que s'inclou la idea de grup de treball i és molt útil per compartir informació del grup i per treballar en aplicacions específiques d'una manera coordinada. Moltes vegades l'estructura de grups, com a conseqüència de les peticions que rep el departament d'informàtica, simplifica l'administració, perquè són per a qüestions característiques d'un grup de treball. L'usuari és conscient que pertany a diversos grups disjunts de treball (si és el cas) i, per tant, veu aplicacions i informació que el seu company de treball no ha de veure necessàriament.

2) Ara es pot permetre que el directori d'un usuari, si l'usuari vol, sigui accessible a la gent del seu grup de treball. Si ho fa, dependrà dels grups i privilegis que tingui, ja que és possible que quedi obert a tots els grups de treball als quals pertany.

El **disseny** ha de reflectir l'estructura de l'organització. Per contra, el disseny condiciona el funcionament del sistema informàtic en la mesura que el defineix.

Així doncs, el disseny que s'adoptarà s'ha de pensar acuradament i cal tenir en compte quins grups hi haurà a l'organització, quins permisos han de tenir per a les aplicacions i quines persones han de pertànyer a cada grup. Es pot fer

Reflexió

Teniu un disseny molt diferent a la vostra organització? Comenteu-ho al fòrum de l'assignatura.

mitjançant una taula de permisos com la que es mostra a continuació (taula 2), en què cal reflectir per a cada aplicació els permisos que té cadascun dels usuaris.

Taula 2. Taula de permisos per usuari

Grup	Persona	Persona
Aplicació	Permís	Permís
Aplicació	Permís	Permís

Després, s'ha de fer la taula d'aplicacions/grups (taula 3), en què hi ha totes les aplicacions i tots els grups. Aquesta taula, com que inclou totes les aplicacions de l'organització, dona una visió global de tot el programari que es fa servir. Això és especialment important per al programari que utilitza informació compartida o informació que accedeix a bases de dades.

Taula 3. Taula de permisos per grup

Programari	Grup	Grup
Aplicació	Permís	Permís
Aplicació	Permís	Permís

Per exemple, si es fes un estudi per a una organització pública, un hospital, una mostra de taules podria ser la següent:

Taula 4. Exemples de taules de permisos

Metges	Joan	Carme
Visites	L/E	L/E
Receptes	L/E	L/E

Administració	Maria	Pere
Comptabilitat	L/E	L/E
Facturació	L/E	L/E
Visites	L/E	L/E
Receptes	L/E	L/E

Programari	Metges	Administració
Comptabilitat	L/E	L/E
Facturació	L/E	L/E
Visites	L/E	L/E
Receptes	L/E	L/E

Programari	Metges	Administració
Ofimàtica	L/E	L/E

1.5. Distribució de les aplicacions

Amb les taules que s'acaben de fer tenim la llista d'aplicacions que els usuaris necessiten. La pròxima decisió que cal prendre és veure on han d'estar aquestes aplicacions. Només poden estar a dos llocs:

1) Local (a l'estació de treball): en aquest cas, l'aplicació estarà instal·lada a cada estació de treball i, per tant, l'estació de treball no haurà d'anar a buscar el programa al servidor. Ocupa més espai de disc a l'estació de treball, però carrega menys la xarxa i és més ràpid d'executar.

2) Remot: aquí l'aplicació està instal·lada a algun servidor. L'estació de treball fa peticions a un servidor en relació amb l'aplicació. Hi ha moltes variants possibles. Per exemple, que el programa estigui en remot (al servidor), però que s'executi en local, que només hi hagi un petit client (un navegador, per exemple) i, per tant, que només es facin peticions als servidors del que es necessita i tot el control el faci el servidor, que s'utilitzi una eina d'emulació de terminal i es connecti a un *host*, etc.

Llavors, depenent de l'aplicació de què es tracti, la decisió ja està presa. Pot passar que vingui donada pel fabricant del programari o que sigui molt clara la necessitat d'una base de dades que ha de funcionar sobre un servidor de bases de dades i, per tant, les coses hauran de funcionar bàsicament en remot.

En general, es tenen dos elements principals per decidir on posar l'aplicació i la informació que maneja aquesta aplicació, i tots dos poden estar en local o en remot. Les possibilitats són les que es mostren a la taula següent:

Taula 5. Taula de localització dades i aplicacions

		Informació	
		Local	**Remot**
Aplicació	Local		
	Remot		
Aplicació	Local		
	Remot		

A la taula 5, es pot veure que cada fila «Aplicació» té quatre possibilitats, de les quals només una és la millor per a cada aplicació que s'instal·la a l'organització.

Aquesta taula s'emplena amb totes les aplicacions de l'organització. Les aplicacions es posen a la primera columna. Ens cal saber quines haurem d'instal·lar a cada estació de treball i, per això, hem de decidir quines aplicacions aniran en local i quines en remot.

La decisió sobre si la informació la posarem en local o en remot depèn, bàsicament, de quantes persones hi accediran, de si la informació és crítica i de la possibilitat i la freqüència de fer-ne còpies de seguretat.

La llista d'aplicacions que es fan servir, i el fet de saber si estan en local o en remot, és fonamental per al disseny.

1.6. Taula d'aplicacions

Fent tots els passos de disseny que s'han explicat fins ara, tenim diverses taules petites i disperses. A la pràctica cal construir una taula, com la que mostra la taula 6, que en resumeix més d'una i que serveix per extreure tota la informació necessària.

Taula 6. Taula globalitzada

	Aplicació		**Informació**		**Grup**	**Grup**	**Grup**
	Local	**Remot**	**Local**	**Remot**			
Aplicació							
Aplicació					Permís		

El permís pot ser L, E o X (o una combinació), que indiquen lectura, escriptura o execució.

D'aquesta taula podem extreure la informació següent:

1) La llista de programari complet que s'utilitza a l'organització. Està a la primera columna de la taula.

2) On hi ha la informació de cada aplicació. Bàsicament, si està en local o en remot, és a dir, si està en servidors o dispersa a les estacions de treball. Serveix per als programes de còpies de seguretat, per establir permisos.

3) La relació de grups d'usuaris que s'han de crear als servidors.

4) També podem obtenir la llista del programari que s'utilitza per grups (i si els grups representen departaments, etc., també es pot saber per àrees de l'organització) amb els permisos que calen.

5) La relació d'aplicacions candidata per configurar l'estació de treball model, i també les aplicacions que cal instal·lar als servidors per tal que les facin servir els usuaris. Això ho extraurem a partir de les aplicacions que s'instal·len en remot o en local.

Tot aquest conjunt d'informació també ens dona el punt de partida per dissenyar la part servidor.

Vegem com quedaria aquesta taula amb les dades de l'exemple anterior:

Taula 7. Taula de permisos

	Aplicació		**Informació**		**Metges**	**Administració**
	Local	**Remot**	**Local**	**Remot**		
Comptabilitat	X			X		L/E
Facturació	X			X		L/E
Visites		X		X	L/E	L/E
Receptes	X		X		L/E	L/E

Com podem veure, a partir d'aquesta taula es pot conèixer: les aplicacions que s'han d'instal·lar en local, és a dir, a la màquina de l'usuari, les aplicacions que s'han d'instal·lar en remot, on residirà la informació que faran servir les aplicacions (local o remot), els grups de treball dels quals formarà part i amb quins permisos. Finalment, només ens quedaria preparar una cosa: el sistema operatiu de l'ordinador de l'usuari.

Amb la **taula d'aplicacions** extraiem molta de la informació per configurar l'entorn d'usuaris al servidor i als clients.

1.7. El sistema operatiu de l'estació de treball

Actualment, els sistemes operatius de les estacions de treball estan dissenyats per treballar en xarxa (en entorns corporatius) i aporten a l'usuari una interfície gràfica per facilitar-li l'ús de l'ordinador tant com sigui possible. Les contrapartides que tenen és que són complexos d'instal·lar, de configurar, molt flexibles i, desgraciadament, fàcilment desconfigurables en mans d'usuaris inexperts. Això últim sol complicar la tasca de l'administrador de sistemes. La seva gran flexibilitat també fa que moltes vegades els usuaris novells se sentin perduts davant de l'equipament informàtic. En qualsevol cas, els **sistemes operatius de xarxa** tenen uns punts en comú que val la pena tenir en compte:

Vegeu també

Vegeu l'apartat «Formació de l'usuari» per intentar evitar aquests problemes al màxim.

- L'usuari s'ha d'identificar forçosament. La identificació correcta li permetrà accedir als recursos de la xarxa, depenent de l'usuari, ja que hi ha privilegis per grups d'usuaris, i accedir a la seva informació privada (directori personal, correu electrònic, etc.).

- L'entorn s'ha de configurar perquè sigui tan homogeni i simple com sigui possible.

- Ha de tenir un accés fàcil i ràpid a les aplicacions que més utilitzi.

- En cas de pèrdua d'informació, el departament d'informàtica probablement li podrà resoldre.

- Si té un problema amb l'estació de treball, sap on ha de trucar perquè li resolguin com més aviat millor.

El sistema operatiu s'ha de poder comunicar bé amb els diferents servidors (recordem que poden ser heterogenis, poden tenir diferents versions i, fins i tot, ser de diferents fabricants).

2. Disseny dels servidors

Ara ja tenim les línies mestres de com es vol el disseny de les estacions de treball. És a dir, on hi haurà les aplicacions, amb quins permisos, amb quins grups i una mica com s'estructuraran els servidors.

A continuació, es veurà com es trasllada aquest disseny als servidors. Aquest disseny pot afectar els servidors en els punts següents:

- Nombre i capacitat dels discos.
- Contingut i nombre de particions dels discos.
- Disposició de la informació als servidors.
- Nombre de servidors.

Canvis per necessitats

No és la primera vegada que a una organització, quan s'analitzen les necessitats dels usuaris, es descobreix que cal, per exemple, una base de dades complexa, i que això fa que calgui un servidor de bases de dades que motiva l'aparició d'un ordinador servidor, d'un servidor de bases de dades i d'un programari client de bases de dades a totes les estacions de treball. Si aquestes coses es poden preveure abans que aparegui la necessitat o que la necessitat faci que la base de dades actual s'hagi de migrar, ens estalviarem molts maldecaps, problemes, temps, queixes dels usuaris i la sempre latent sensació que la informàtica és «allò que no acaba de funcionar mai bé».

Un possible **procediment** per detectar aquests punts podria ser:

1) Fer una relació de totes les aplicacions que caldrà instal·lar.

2) Veure on hi haurà la informació de totes aquestes aplicacions.

3) Veure amb quins permisos hauran de funcionar totes aquestes aplicacions.

Vegeu també

Recordeu que heu fet aquestes tres coses en l'apartat «Disseny de l'entorn d'usuaris».

4) Esbrinar, segons el nombre d'usuaris actuals i previstos, les necessitats del disc. Bàsicament, la partició d'usuaris i la partició on hi ha emmagatzemat el correu electrònic (les bústies dels usuaris).

5) Esbrinar, tenint en compte la informació que es manipula i la previsió de la informació que es preveu manipular, les necessitats del disc.

6) Esbrinar, considerant tots els elements anteriors, les necessitats del servidor i de la xarxa.

Finalment, cal adequar tota la infraestructura segons el que s'hagi detectat i veure si s'han de fer canvis i ampliar o canviar els servidors.

Cal **preveure** les necessitats reals dels usuaris per reflectir-les a l'estructura informàtica dels servidors.

2.1. Distribució dels discos

En apartats anteriors s'ha fet el disseny general, per la qual cosa ja s'ha identificat què ha de tenir el nostre ordinador per als usuaris: se sap, més o menys, el programari que ha d'integrar, les aplicacions que hi han de funcionar, els permisos, depenent de l'usuari i del grup al qual pertany, i on estaran les dades (al servidor, al client, en una base de dades, etc.). Amb aquest disseny present, es pot començar a dissenyar detalladament com serà la distribució dels servidors.

La distribució bàsica de particions de qualsevol servidor és la següent:

Vegeu també

Vegeu-ho al mòdul «Administració de servidors».

- Partició de sistema.
- Partició d'usuaris.
- Partició d'aplicacions.
- Partició de dades.

Amb la taula d'aplicacions que s'ha fet, es coneixen les aplicacions que necessiten els usuaris. Per tant, es pot establir si són suficients o si en necessitem de suplementàries. També podem descobrir si alguna aplicació requereix un servidor propi.

Si l'organització necessita una web per publicar informació a internet, ens cal un servidor web (una aplicació) corrent en un servidor, i les dades (tota la web) en algun servidor (normalment el mateix). Segurament tot en particions diferents (s'ha de decidir), i s'ha de saber si aquesta web accedirà a informació (bases de dades) de l'organització per decidir les qüestions de seguretat o, fins i tot, veure si es posa en un servidor corporatiu independent del servidor.

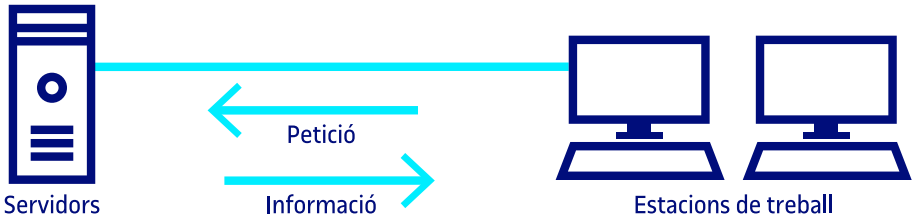
Per tant, pot passar que, en lloc de ser imprescindible distribuir la informació en particions, s'hagi de distribuir en discos dins el mateix servidor.

La relació d'aplicacions, la necessitat d'informació, el nombre potencial d'usuaris i el seu nivell de concurrència determinen la distribució dels discos.

2.2. Accés a la informació

La informació dels servidors es lliura als usuaris mitjançant peticions per la xarxa. Tal com mostra la figura 6, l'usuari, des de la seva estació de treball, fa una petició al servidor, la qual s'envia per la xarxa. Una vegada arriba la petició al servidor i la processa, li retorna la informació sol·licitada.

Figura 6. Esquema d'accés a la informació



Vegeu també

Vegeu el mòdul «Administració de servidors», on parla de com es pot optimitzar aquest problema amb el maquinari.

L'estructura física del disc del servidor fa que només pugui servir una informació cada vegada, per tant, les diverses peticions de lectura que es fan al disc es posen en una cua. Aquest problema pot arribar a ser molt greu i alentir el rendiment del servidor.

Detectar el problema

Aquests problemes són difícils de detectar, perquè normalment s'associen a problemes de la xarxa, ja que la percepció de l'administrador de sistemes i la dels usuaris és que les peticions de les estacions de treball triguen més del normal a ser ateses. L'anàlisi del temps de resposta del disc és correcta. Costa molt detectar que, en realitat, es fan massa peticions al disc.

Per evitar aquest problema, des del punt de vista del disseny, n'hi ha prou amb distribuir la càrrega de peticions en discos o controladores diferents (depenent de la tecnologia que s'utilitzi), fer peticions paral·leles i, si és possible, no tenir cues de peticions parades ni col·lapsades. Si el problema és crític, es pot arribar a haver de plantejar solucions de tipus servidors redundants.

Una vegada més, amb la llista d'aplicacions que hi ha d'haver al servidor, hem de veure quants usuaris concurrents tindrà cadascun per valorar la càrrega.

Cal fer el mateix amb la informació dels servidors. Si hi ha aplicacions o informació amb un gran volum d'accessos concurrents, són candidates a anar a un altre disc, o fins i tot, a una altra controladora de disc. Si la quantitat de peticions pot arribar a ser crítica, llavors han d'anar a un altre servidor independent.

Servidors web d'intranets

Un d'aquests casos són els servidors web d'intranets que accedeixen a les bases de dades de l'organització. S'ha d'anar amb compte amb les càrregues del disc. Una de les primeres solucions és posar-ho tot sobre la tecnologia més ràpida (tecnologia SCSI si es requereix una capacitat considerable o SSD si les necessitats d'espai no són molt altes) per evitar que el disc es converteixi en un coll d'ampolla del sistema. Tampoc no es descarten solucions RAID ni de servidors redundants.

L'accés a la informació es pot convertir en un problema si no mirem a fons quants usuaris simultanis intenten accedir a un dispositiu.

2.2.1. Privilegis

El sistema de fitxers és l'estructura que permet emmagatzemar la informació als discos. Aquesta estructura es compon de directoris, fitxers i la llista de control d'accés de cada element. A cada sistema operatiu el sistema de fitxers es gestiona d'una manera concreta pròpia del sistema operatiu, però això no vol dir que no es pugui accedir a la informació d'un sistema de fitxer d'un altre sistema operatiu.

El sistema de fitxers sobre el qual s'instal·li la informació ha de permetre seguir l'estructura que s'ha dissenyat amb els usuaris. És a dir, si hi ha grups d'usuaris i permisos sobre les aplicacions, a més de poder-se incloure en el sistema operatiu dels clients i dels servidors, també s'han de poder incloure en els sistemes de fitxers. Això permet una seguretat addicional en el sistema, perquè no en forma part solament el sistema operatiu, sinó que el mateix sistema de fitxers la porta «integrada».

3. Configuració de les estacions de treball

En aquest punt, tenim una idea de les aplicacions que necessiten els usuaris i sabem força bé amb quins permisos han de funcionar, i quines d'aquestes aplicacions ho faran al servidor i quines a l'estació de treball. El problema que cal resoldre ara és decidir on hi haurà guardades les aplicacions que hem decidit que funcionaran a l'estació de treball. Poden ser al servidor (es veuran com una unitat compartida, per exemple) o les podem instal·lar a cada estació de treball.[4]

(4)La manera de fer-ho s'explica més endavant.

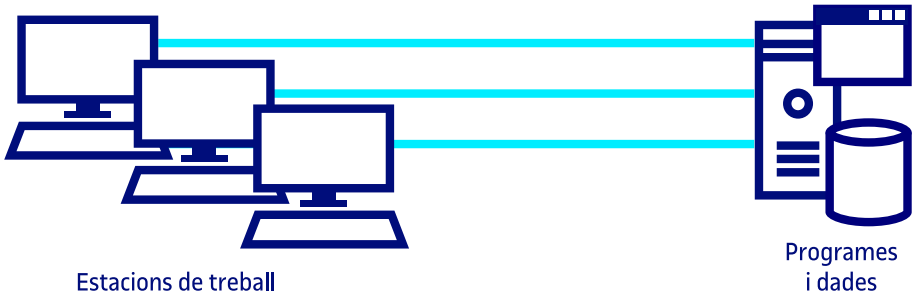
L'objectiu bàsic que ens ha de moure a l'hora de prendre aquestes decisions és aconseguir que el manteniment de les estacions de treball sigui el màxim de senzill possible.

Un canvi o actualització d'un programari a empreses amb centenars o milers d'ordinadors pot comportar molts dies de feina per tornar a configurar totes les estacions de treball.

3.1. Aplicacions comunes al servidor

Com menys coses hi hagi al disc de l'usuari, menys perill hi ha de pèrdua d'informació i de temps per recuperar l'equip.

Figura 7. L'emmagatzematge al servidor evita la pèrdua d'informació



Per tant, aparentment «tornem enrere» en una situació en què tot està als servidors i les estacions de treball es converteixen en «terminals» o dispositius «no intel·ligents», els quals es comuniquen constantment amb els servidors per accedir als programes i les dades, tal com es mostra a la figura 7.

Vegeu també

Vegeu en el mòdul «Administració de les dades» alguns criteris per decidir on guardar la informació.

Aquesta tendència pretén posar-ho tot als servidors per evitar la pèrdua d'informació (ja que ara està tota als servidors) i de temps per posar en marxa una estació de treball, atès que només té el sistema operatiu, perquè totes les aplicacions estan als servidors.

Aquesta estructura presenta molts **problemes**, alguns dels quals són els següents:

- Es col·lapsen els servidors.
- Es col·lapsa la xarxa.
- El sistema global va lent.
- Els usuaris tenen moltes queixes del rendiment general del sistema.

Malgrat tot, té alguns **avantatges**, que són els següents:

1) Com que no hi ha res als discos dels usuaris, no és perillós si hi ha algun problema a les estacions de treball.

2) Tot el control es fa des dels servidors i, per tant, no hi ha perill de problemes i desastres que provinguin dels clients.

3) Tampoc no hi ha problemes de fallades en la seguretat si tot està als servidors.

4) Tota la informació està als servidors.

Amb tot, no és una estructura que s'utilitzi a la pràctica, ja que els inconvenients que presenta superen amb escreix els avantatges. No obstant això, la idea és vàlida per a la instal·lació d'algun programari específic que pugui caldre. Aquest programari s'instal·larà al servidor i s'executarà remotament als clients. Valorant la necessitat i les càrregues que pot comportar en xarxa, en servidor i en temps d'execució, s'utilitza com a solució puntual, no com a solució generalitzada.

3.2. Aplicacions comunes als clients

S'intenta aplicar els **criteris** següents:

- Totes les estacions tenen el mateix als seus discos durs (això simplifica les instal·lacions).

- Totes les estacions tenen el programari de base, que comprèn el sistema operatiu, els paquets d'ofimàtica i el programari que utilitza tota l'organització.

Dissenyar amb aquests criteris té força **avantatges**. Aquests en són alguns:

1) Descarrega molt el trànsit de la xarxa.

2) Augmenta molt la velocitat d'execució del programari de les estacions de treball, ja que ara la majoria d'aplicacions s'executen en local.

3) Millora força el rendiment general de l'equip.

4) El servidor només guarda les dades i els programes especials (això últim si cal).

Per tant, els usuaris no tindran la sensació d'una xarxa pesant i lenta, perquè moltes de les aplicacions i utilitats funcionaran a l'estació de treball sense demanar res al servidor. Cal decidir si les dades les guardarà en local (al disc dur) o a la xarxa (en una unitat compartida o en un espai privat de l'usuari dins el servidor).

Espai per a l'administrador del sistema

Hi ha d'haver una part del disc del servidor, que no ha de ser visible per als usuaris, exclusivament reservada a l'administrador. Aquesta part del disc s'utilitzarà per refer les estacions de treball en cas de desastre i quan s'hagin de fer reinstal·lacions. La recuperació de les estacions de treball és una part de l'administració d'usuaris que ha d'estar prevista, ja que quan el nombre d'estacions de treball és considerable, és una activitat pràcticament diària.

Als discos dels clients hi instal·lem el programari que tenen tots els ordinadors.

3.3. Creació de l'estació model

Tenint clar quines aplicacions s'instal·len en local i quines en remot, en aquest punt la taula d'aplicacions hauria d'estar completa.

Ara ja es pot procedir a crear l'ordinador model de l'estació de treball que es vol posar a l'organització. A grans trets, el **procediment** és el següent:

1) Instal·lació del sistema operatiu.

2) Instal·lació de les aplicacions.

3) Instal·lació dels clients de les aplicacions que funcionen en remot.

4) Configuració de totes les opcions del sistema operatiu per ajustar-lo a les necessitats de l'organització.

5) Es fan proves durant un temps.

Una vegada s'han fet les proves amb tots els grups d'usuaris, privilegis, aplicacions, etc., i l'estació de treball funciona correctament, es dona per acabada l'estació model.

L'**ordinador model** és el disseny de programari i configuració que volem que tinguin tots els ordinadors de l'organització.

El seu disseny ha de ser molt acurat i cal tenir en compte molts punts, com per exemple:

- **Entorn d'usuari**. Amb què es trobarà quan engegui l'ordinador? Què li demanarà, quines finestres i quins colors tindrà? Què podrà modificar de l'entorn?

- **Xarxa**. Com s'identificarà la xarxa? Què podrà fer dins la xarxa? Quins grups d'usuaris hi haurà? Quins permisos tindrà?

- **Programari**. Quines aplicacions tindrà disponibles? Quines aplicacions estaran en local i quines en remot? On hi haurà el correu electrònic?

- **Facilitat d'ús**. Tot ha d'estar pensat per facilitar la feina a l'usuari i fer que s'acostumi ràpidament a aquesta eina de treball. Ha de servir per millorar-ne el rendiment.

- **Informació**. Una vegada l'administrador hagi decidit on guardar les dades i amb quin format, per a l'usuari això hauria de ser tan automàtic i transparent com fos possible, de manera que no s'hagi de preocupar del lloc real on estan les dades.

Tot plegat fa que sigui necessari dissenyar un ordinador model i, posteriorment, clonar-lo tantes vegades com estacions de treballs hi hagi a l'organització i, si cal, després l'estació de treball clonada s'ajustarà al lloc de treball al qual es destina.

Els passos, a grans trets, són els següents:

1) Es prepara l'estació de treball model. És a dir, es configura un ordinador tal com es vol que siguin totes les estacions de l'organització, amb el programari, les proteccions, les particions de disc, la configuració de xarxa, etc. Es prova a fons per veure si tot funciona correctament.

2) Amb el programari de clonació dels discos durs per xarxa es clona el disc de l'ordinador model i es guarda la imatge al servidor. Normalment aquesta imatge pot ocupar alguns centenars d'MB (algun GB i tot) i s'haurà de guardar en un servidor.

3) Els programaris de clonació poden crear un client portable per restaurar una imatge clonada des del servidor en una estació de treball. Amb aquesta operació s'obté una estació de treball amb el programari, les proteccions i la configuració de xarxa que s'ha establert a l'ordinador model, ja que en serà una duplicació.

4) Finalment, s'ha d'ajustar la configuració d'aquest ordinador per a l'usuari o el lloc de treball a què es destina.

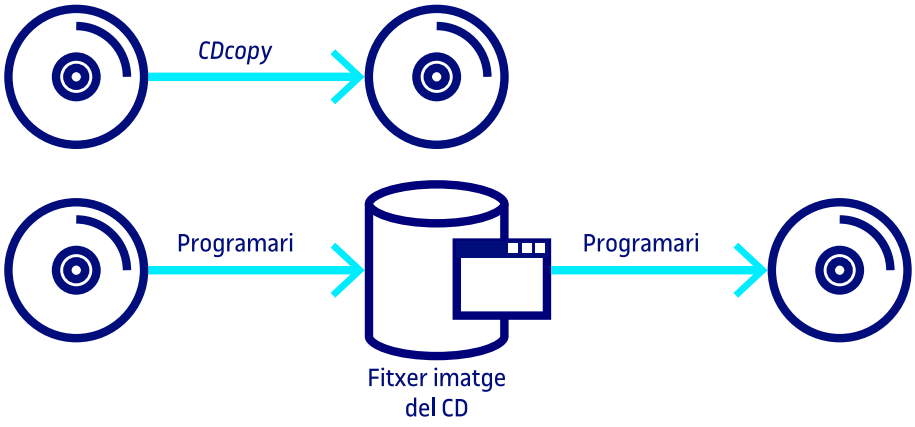
Per a l'administració del sistema informàtic, la situació ideal és que totes les estacions de treball siguin homogènies en programari i maquinari. Que ho sigui el maquinari facilita la compra, les reparacions, el recanvi i la substitució de material, ja que amb el pas del temps els ordinadors s'espatllen i necessiten reparacions. Com que a la pràctica això és impossible, almenys ha de ser un objectiu (que no s'assolirà mai).

El mateix passa amb el programari, que també hauria de ser homogeni, però això tampoc no és possible a la pràctica, ja que és un objectiu que mai no s'arriba a assolir.

3.3.1. Imatges de disc

Més o menys tothom coneix alguna utilitat per copiar un CD. La utilitat ens permet fer una còpia exacta del CD en un altre CD. D'aquesta manera, si desgraciadament es fa malbé el disc original, en tenim la còpia, que és un duplicat exacte de l'original. D'alguna manera és la idea de la fotocòpia en paper: **una copia fidedigna de l'original**. Ara bé, què passa si volem fer un duplicat d'un CD però no tenim un segon CD per fer-ho? Tal com mostra la figura 8, hi ha programaris que permeten fer una còpia del CD, però en lloc d'arxivar el resultat en un CD (el copiat), el posen en un fitxer. Aquest fitxer no el podem llegir ni escriure, ni tan sols executar-lo com un CD. L'únic que podrem fer, quan tinguem un CD, és traspassar el fitxer, i ja en tindrem la còpia.

Figura 8. Procés de duplicació d'un CD mitjançant una imatge



Amb aquest programari podrem fer tants duplicats del nostre CD com vulguem, sense necessitat de tenir el CD original, perquè el fitxer creat el podem tenir guardat al disc dur tant de temps com calgui. Del fitxer guardat al disc dur se'n diu **imatge de CD**.

Imatge d'un disc dur

Fer una imatge o còpia d'un disc dur també es diu *clonar un disc dur*.

Una imatge de CD pot semblar una cosa poc útil, però ho és molt si pensem que podem fer el mateix amb tot un disc dur. Podem fer una imatge d'un disc dur i és molt útil.

Amb el procediment de fer una imatge d'un disc dur obtenim un fitxer molt gran (de l'ordre de diversos GB) que conté la imatge del disc dur que hem copiat. Si tenim la desgràcia que es fa malbé el disc dur original (des del punt de vista de programari, és a dir, es desconfigura o es degrada el sistema fins al punt que cal reformatar el disc o reinstal·lar el sistema), es pot **restaurar la imatge del disc** al disc dur, de manera que en pocs minuts el disc dur i, per tant, l'ordinador, torna a ser completament funcional.

L'únic requisit necessari per fer una imatge de disc és un programari que creï el fitxer imatge a algun lloc. Lògicament no podem crear la imatge del disc al mateix disc. Si volem posar la imatge del disc dins el mateix disc físic, s'ha de posar en una partició diferent. En cas d'una fallada física o mecànica del disc, no podrem recuperar la imatge, per la qual cosa no és la solució més recomanable. Alguns llocs aconsellables són els següents:

- Al servidor, en alguna partició o tros de disc administratiu que no quedi a l'abast dels usuaris.
- Generar el fitxer imatge i, posteriorment, traspassar-lo a un DVD. Després, si s'ha de restaurar la imatge de disc, es pot fer des de qualsevol lector de DVD.
- En un compte destinat exclusivament a tasques d'administració d'usuaris.
- En un dispositiu extern de cinta magnètica del servidor (DAT, DLT, AIT, etc.).
- En dispositius de còpia externa com ara unitats USB o similars.

Cal remarcar que, igual que les còpies de seguretat, quan es restauren imatges de disc, l'estat d'aquest disc és el mateix que quan es van fer, per la qual cosa si hi havia dades es poden haver perdut. En aquest cas, s'hauria de recórrer a les còpies de seguretat per recuperar la informació. És per això que una de les grans utilitats de les imatges de discos és fer **ordinadors model**.

Per realitzar aquestes tasques podem utilitzar programaris coneguts com a gestors d'imatges. Alguns exemples són OpenGnsys, IBM Tivoli Provisioning Manager, FOG Project, Rembo Wizard & Rembo Toolkit. Aquestes eines proporcionen entorns per a la generació d'imatges, gestió i desplegament.

4. Manteniment de les estacions de treball

En aquest apartat, es parlarà de les accions que es duen a terme per garantir el correcte funcionament del maquinari i del programari que formen part de la estacions de treball.

Per **manteniment de les estacions de treball** entenem totes les accions necessàries perquè l'equipament estigui en òptimes condicions de funcionament per a l'usuari final.

Ara bé, a la pràctica això es divideix clarament en dues parts molt ben diferenciades. La primera és el manteniment de l'equipament de l'usuari (tant el maquinari com el programari) i la segona són les tasques necessàries perquè el sistema funcioni correctament.

4.1. Manteniment de l'equipament

Una de les parts importants de l'administració d'usuaris és el manteniment, la substitució o l'actualització del maquinari i del programari de les estacions de treball. Normalment aquesta part respon a diversos motius:

- Reparar per avaria de maquinari greu que requereix una substitució important de l'equip. De vegades, cal una reinstal·lació del programari de l'ordinador.
- Substituir l'ordinador per un de nou per actualització del maquinari.
- Instal·lar un maquinari per un pla de modernització o actualització.
- Canviar l'usuari de l'estació de treball i, per precaució, destruir la informació i tornar a instal·lar el programari d'usuari.
- Reinstal·lar l'equip com a conseqüència d'haver-lo traslladat per un canvi de funció dins l'organització.
- Reinstal·lar l'equip per un nou sistema de funcions dins l'estructura de l'organització.

En la majoria dels casos, el responsable d'informàtica n'està assabentat i el pla estratègic de l'organització és clau per dur a terme aquestes accions dins el pla global de l'organització. Però fora d'aquests casos, també podem trobar situacions com les següents:

- Desconfiguració completa de l'equip a causa de virus.
- Esborrament del disc a causa de virus.
- Esborrament parcial del disc a causa d'un mal ús involuntari per part dels usuaris.
- Fallada del corrent elèctric que ha provocat una desconfiguració de l'equip.
- Fallada del corrent elèctric que ha provocat un problema de maquinari que obliga a reinstal·lar el programari.

Hi ha moltes situacions que poden provocar que un equip funcioni malament. Ara bé, de la mateixa manera que hem de tenir cura de com s'ha de preparar l'equip per a l'usuari, també s'ha de tenir molta cura a l'hora d'establir com s'ha de recuperar un equip davant d'un desastre que ens deixa l'ordinador inoperatiu, per tal que sigui operatiu al més aviat possible. Un bon disseny de l'equip model ens permet recuperar correctament els equips amb problemes. El mètode de disc d'imatge/clonació és perfectament aplicable al manteniment de l'equipament, ja que ens permet restablir en molt poc temps l'operativitat d'un equip que ha deixat de ser funcional per a l'organització, sempre que només es tracti de problemes de programari. En cas que els problemes siguin de maquinari, hem de tenir un petita quantitat de peces de substitució per a les avaries freqüents i fàcils de reparar (si també volem donar servei de reparació de maquinari).

Reflexió

Us heu trobat amb altres situacions que us hagin fet reinstal·lar equips? Comenteu-ho al fòrum de l'assignatura.

Hi ha una gran quantitat de causes que poden deixar una estació de treball inoperant. Hem d'estar preparats per a les més usuals.

4.2. Extreure dades d'un equip

Hi ha molts escenaris de problemes possibles. Molts tenen solució, fins i tot sense haver d'anar físicament davant de l'equip. Però n'hi ha un d'especialment conflictiu. Malgrat que hem procurat que les dades estiguin als servidors i que no hi hagi informació a les estacions de treball, moltes vegades no és així. Si un equip té el sistema operatiu corromput (i, per tant, necessitem aplicar la tècnica de la clonació per restaurar l'ordinador i tornar-lo a l'estat original), de manera que no és possible connectar-se a la xarxa per copiar la informació i té informació dins el disc dur que necessitem extreure, hem de buscar alguna manera de copiar-la. Potser l'equip no és ni capaç d'arrencar,

però nosaltres, amb qualsevol mètode (un DVD o un llapis de memòria per arrencar l'ordinador, per exemple), aconseguim engegar l'ordinador i accedir a la informació. Com la podrem extreure, ara que sabem que està en bon estat? Hi ha dues maneres de fer-ho:

1) Moure el disc dur. La idea és senzilla: extraiem el disc dur de l'ordinador i el posem en un altre ordinador que funcioni. L'instal·lem com a disc no principal i posem en marxa l'ordinador. El sistema operatiu hauria de detectar aquest altre disc dur i se n'haurien de veure tots els fitxers. Copiem els fitxers que ens interessen al disc dur principal, i després ja podrem fer l'operació de clonació sobre aquest disc dur (que en destruirà el contingut).

2) Fer servir una unitat DVD, Blu-Ray o *linear tape open* (LTO). Si s'ha fet tot el disseny dels servidors, els discos dels usuaris contenen poca informació. Això permet, amb els dispositius de memòria massiva de reduïdes dimensions i gran capacitat, fer fàcilment una còpia de seguretat de les dades. Per tant, el procediment és el següent: una d'aquestes unitats (una gravadora Blu-Ray2 de 50 GB, per exemple) es connecta al port USB. S'arrenca l'ordinador amb un llapis de memòria i, des d'aquest mateix llapis, es fa reconèixer el dispositiu Blu-Ray. Per tant, es té configurada una unitat, com un disc dur més, de capacitat 50 GB. Ara, com que es pot accedir al disc dur, és possible copiar a cada Blu-Ray fins a 50 GB. Una vegada s'ha fet la còpia, es pot procedir a reparar l'equip. Mentrestant, per exemple, es pot posar aquesta informació a l'espai de l'usuari del servidor. D'aquesta manera, tan bon punt estigui solucionat el problema, trobarà la informació que, lògicament, s'haurà de tornar a col·locar al lloc adient.

Això implica temps i pressupost per tenir aquestes eines addicionals que ens permetin mantenir i recuperar les dades el més ràpid possible i amb una pèrdua mínima d'informació.

Davant d'un ordinador que té informació i no s'engega, hem de buscar maneres d'extreure'n aquesta informació important.

4.3. Tasques periòdiques de manteniment

Les tasques de manteniment són molt importants per al funcionament correcte del sistema global, però no responen a cap situació extraordinària. S'han de fer forçosament cada cert temps i la majoria són transparents per a l'usuari, el qual només sap que hi són quan no funcionen correctament.

4.3.1. Manteniment del servidor

Tal com ja hem comentat, hi ha un seguit de tasques que se situen en una línia divisòria molt fina. Són responsabilitat de l'administrador d'usuaris o de l'administrador de servidors? Afecten el servidor, però molt directament l'usuari. Uns exemples d'aquestes tasques podrien ser:

- **Controlar que no s'omplin les bústies de correu dels usuaris**. Generalment hi ha un *script* (guió) que permet controlar l'espai de les bústies dels usuaris i, en cas que alguna estigui excessivament plena i abans que el servidor de correu es col·lapsi per falta d'espai, s'avisa l'usuari (o els usuaris) perquè faci neteja dels correus. Aquesta tasca s'ha de dur a terme periòdicament.

- **Controlar que no s'omplin els directoris dels usuaris**. Amb el mateix criteri d'abans, cal evitar quedar-se sense espai en la partició dels usuaris. S'ha de vigilar periòdicament la mida d'aquesta partició. També cal avisar els usuaris dels directoris que sobrepassen una mida perquè en facin neteja.

Reflexió

Penseu que hi ha altres tasques? Comenteu-ho al fòrum de l'assignatura.

4.3.2. Virus

Els virus són un dels problemes amb què s'enfronten tots els administradors d'usuaris. Avui hi ha antivirus que funcionen d'una manera centralitzada, és a dir, s'instal·la l'antivirus «servidor» en un ordinador que farà el paper de «servidor», es defineixen els ordinadors, els usuaris, els permisos, etc. i quan l'usuari entra dins el sistema, automàticament, s'instal·la el programari antivirus a l'ordinador. L'administrador actualitza diàriament el **fitxer de signatures** de l'antivirus, que s'actualitza automàticament a tots els ordinadors de l'organització quan l'usuari s'identifica. També actualitza periòdicament el programari, el qual, seguint el mateix procediment, s'actualitza a tota l'organització.

Vegeu també

Vegeu el mòdul «Administració de la seguretat» per a més informació sobre els virus.

Quan es posa en marxa, el programa antivirus es dedica a controlar tota la informació que entra a l'estació de treball (especialment per internet), per correu electrònic, i a buscar constantment virus en el sistema dels discos locals de l'estació de treball. Què passa si en troba?

1) El pot eliminar.

2) No el pot eliminar. En aquest cas potser proposa esborrar el fitxer. Si el fitxer és crític per al sistema operatiu (moltes vegades l'usuari no ho sap), pot ser que esborrar-lo sigui perillós per al seu funcionament, per la qual cosa en aquests casos el millor sempre és avisar l'administrador d'usuaris.

Sigui com sigui, si detectem o sospitem que hi ha un virus al nostre ordinador, és convenient avisar telefònicament l'administrador d'usuaris, perquè té coneixement de la perillositat i la capacitat de propagació del virus. Si l'antivirus l'ha eliminat i no en diem res, pot ser una mesura insuficient, perquè el virus ja es pot haver propagat per l'organització (o encara pitjor, haver-ne sortit fora).

Aquest és el missatge que cal difondre als usuaris per evitar propagacions. Com en molts casos, se'ls ha d'educar en l'ús d'eines informàtiques.

4.3.3. Control remot

El control remot és un programari fonamentat en la tecnologia client/servidor que permet accedir, mitjançant la xarxa a un ordinador físicament distant, a les seves dades, administrar el seu sistema i facilitar ajuda al seus usuaris davant possibles problemes.

Vegeu també

Vegeu l'apartat «Centre d'atenció a l'usuari (CAU)».

Seguint la tecnologia client/servidor, aquest programari té la seva part servidora a l'estació de treball de l'usuari dedicada a servir les ordres dictades des de l'estació client situada a l'estació de treball de l'administrador d'usuaris.

Gràcies a la seva gran utilitat, els programaris de control remot han incorporat noves capacitats com ara: cerca d'elements dins la xarxa, autoinstal·lació en estacions servidores, connexions compartides a estacions de treball, facilitat de transferència de dades i moltes altres.

Hi ha, doncs, molts **avantatges** que recomanen la utilització del control remot:

1) Econòmics. Gràcies a la reducció de personal, de temps i de desplaçaments, la recuperació de la inversió és garantida.

2) Treball a distància. Permet treballar a distància flexibilitzant tasques específiques, per exemple en caps de setmana via teletreball.

3) Assistència ràpida i eficaç. Millora molt el suport a l'usuari, ja que permet als tècnics accedir al sistema i comprovar personalment els problemes existents. A la vegada, permet solucionar-los sense necessitat de desplaçaments.

4) Formació. Permet formar remotament mitjançant la connexió compartida a una estació de treball.

5) Manteniment. Millora substancial en el manteniment de les estacions de treball.

Hi ha, però, aspectes que poden dificultar les tasques de l'administrador:

1) Seguretat. La informació entre l'estació client (servidor) i l'estació administradora (client) es transmet mitjançant la xarxa. Si aquesta no és segura, compromet el control.

2) Recursos de xarxa. Consumeixen una amplada de banda important, atès que les pantalles de les estacions de treball viatgen per la xarxa. Els programaris de control remot incorporen eines que permeten triar la resolució i el color de la pantalla per evitar-ne el consum desmesurat.

3) Comunicació específica. La comunicació s'estableix per ports que moltes vegades no són visibles des de les xarxes remotes a causa de l'existència d'elements de la xarxa que impedeixen la comunicació, normalment per seguretat.

4) Aspectes legals. Molt importants. Es podria incórrer en incompliments de la normativa legal si l'usuari no és avisat sobre la connexió a la seva estació de treball. Es podria violar el seu dret a la intimitat.

Aquests programaris, que s'utilitzen molt a les organitzacions, pretenen millorar el servei que es dona a l'usuari.

4.3.4. Actualització diferida

Quan hi ha instal·lacions geogràficament allunyades o un nombre elevat d'estacions de treball, com podem actualitzar un programari que està a les estacions de treball?

Hi ha programaris capaços de fer-ho. Permeten seleccionar el programari i les estacions de destinació i procedir a l'actualització massiva, sense haver-nos de traslladar físicament davant de cap equip o haver de fer l'operació i repetir-la cada vegada.

4.4. Documentació i procediments

Un dels aspectes que sovint s'oblida és la documentació i els procediments. Els procediments són una qüestió de documentació tècnica per als administradors de sistemes.

4.4.1. Procediments

Atès que hi ha molts usuaris, moltes de les tasques acostumen a ser repetitives, molt més que no pas a l'administració de servidors. Això fa que sovint sigui convenient descriure els passos per fer una tasca, ja que de vegades una tasca consta de molts passos i, malgrat que es fa moltes vegades, es duu a terme en

intervals de temps prou espaiats perquè s'oblidi. D'aquest conjunt de passos per fer una tasca en direm *procediment* i, perquè ens sigui senzill dur-lo a terme quan s'hagi de fer el tindrem escrit, és a dir, documentat.

La definició formal (algorítmica) de procediment és la següent: descripció no ambigua i precisa d'accions que cal dur a terme per resoldre un problema ben definit en un temps finit.

L'**acció** és l'esdeveniment finit en el temps i que té un efecte definit i previst.

El **procés** és l'execució d'una o diverses accions.

Adaptant-la a les nostres necessitats d'aquest moment, la podem definir de la manera següent:

Un **procediment** és una descripció del conjunt d'accions per fer una tasca determinada.

Tots els procediments haurien d'estar reflectits en un document.

Document del procediment

El document pot ser en format paper, HTML o qualsevol altre.

Per tant, cadascun dels procediments haurien d'estar escrits en un document. D'aquesta manera, cada vegada que hàgim de fer qualsevol tasca, només caldrà consultar aquest «manual de procediments» i fer les accions que hi ha especificades per dur a terme la tasca encomanada.

Hi ha moltes maneres de tenir recollida aquesta informació. Una és en forma de PMF (FAQ),[5] penjada en format HTML en algun servidor web, de manera que el personal tècnic la pot consultar en qualsevol moment i des de qualsevol lloc. Moltes vegades, juntament amb els documents, s'adjunten fitxers, perquè el format de web permet transferir fitxers alhora.

(5)Acrònim de preguntes més freqüents (en anglès, *frequently asked questions*).

Exemples de procediments

Els següents són exemples de procediments:

- Donar d'alta un usuari.
- Configurar una impressora.
- Configurar una estació de treball.
- Configurar el correu electrònic.
- Restaurar una imatge en una estació de treball.

Reflexió

A la vostra organització, hi ha alguna manera de documentar els procediments habituals? Penseu que hi ha alguna altra manera de fer-ho? Podeu comentar-ho al fòrum de l'assignatura.

Cap d'aquestes tasques no es pot fer amb una sola acció. Cal tenir present que algunes vegades un procediment pot implicar accions sobre el servidor i sobre l'estació de treball.

4.4.2. Programari

De la mateixa manera, de tot el programari que s'utilitza, l'administrador d'usuaris hauria de tenir cura que els usuaris tinguessin accés a algun tipus de documentació (en algun format) sobre la utilització d'aquests programaris. Això facilita el fet de poder conèixer les eines amb què treballen. És millor que la documentació estigui en diversos formats a la vegada. En qualsevol cas, ha de ser fàcilment accessible per als usuaris. També és molt interessant poder tenir tutorials d'aquest programari. Molts programes n'incorporen, però d'altres es poden trobar gratuïtament, fins i tot, a internet. És important poder facilitar algun tipus de documentació als usuaris sobre les eines que utilitzen. La seva percepció és que els administradors es preocupen d'ells. Malgrat tot, no s'ha d'oblidar la formació, ja que això no pretén substituir-la, sinó complementar-la.

5. Formació de l'usuari

Un aspecte sovint oblidat a les organitzacions és el **pla de formació** dels usuaris, que ha d'estar dirigit pel responsable d'informàtica d'acord amb les directrius de l'organització i el pla estratègic.

Reflexió

Què en penseu, de la formació per als usuaris? Què us semblen els cursets d'autoaprenentatge? Porteu la vostra reflexió al fòrum de l'assignatura.

Els **avantatges** d'un pla de formació es poden resumir en els següents:

1) Millora en l'ús de les eines de programari.
2) Augment de l'efectivitat i l'eficiència del personal.
3) Disminució de les incidències al departament d'informàtica.
4) Satisfacció del personal.
5) Disminució de costos del departament d'informàtica.

Algunes de les **conseqüències indirectes** que s'esdevenen són les següents:

- Detecció de noves necessitats informàtiques a l'organització.
- Augment de la informació en els sistemes informàtics. Això permet nous mètodes de recerca de dades per prendre decisions en els estaments directius.

Ningú no neix ensenyat

De la mateixa manera que per conduir un cotxe ens han de formar (i, al final, ens donen un títol que reconeix els coneixements que tenim), per fer anar un telèfon mòbil o una rentadora també ens han d'explicar com funciona com a usuaris, és a dir, d'una manera simple, didàctica i sense tecnicismes.

Moltes organitzacions tenen la sensació que un pla de formació és malgastar el temps, però no seguir-lo ocasiona els problemes següents:

1) Pèrdues de temps dels usuaris que s'enfronten a programari o maquinari nou sense coneixements i, per tant, la corba d'aprenentatge és molt elevada.

2) La probabilitat d'error en aquesta fase d'autoaprenentatge és molt important, amb conseqüències de temps i de cost per solucionar-ho impredictibles.

3) Les probabilitats que els errors involuntaris produeixin problemes, fallades, mals funcionaments, desconfiguracions, etc., en els equips o servidors és alta, amb el temps i el cost per al personal del departament informàtic que això pot comportar.

4) La possibilitat, que una gran part del volum de treball (fins i tot es pot arribar a una situació de col·lapse) del departament d'informàtica es degui a problemes indirectes de formació del personal, s'ha de tenir en compte.

5) El desconcert, les queixes, la sensació de mala instal·lació del programari o de maquinari incorrecte o defectuós, que no s'adiu a les necessitats reals de l'organització, és molt possible que apareguin, amb el perill de poder fer fracassar els plans d'informatització o els plans d'actualització que es procuren dur a terme.

Tot això tampoc no vol dir que el pla de formació hagi de ser sempre igual i general per a tothom. Un bon pla de formació està estudiat i es té molt en compte què s'explica i a quin col·lectiu s'explica.

La mateixa aplicació genera cursos de formació diferents per a col·lectius diferents.

Una aplicació de nòmines integrada tindrà un curset de formació diferent per al departament de recursos humans, per al de comptabilitat, per a tots els treballadors que han de fitxar a l'entrada i a la sortida, i que poden consultar per mitjà d'una web de la intranet el seu registre d'entrades i sortides, etc. Finalment, com és lògic, el curset de formació per al departament informàtic sobre aquesta aplicació també ha de ser diferent.

Així, doncs, hi ha diversos plans de formació:

1) Plans de formació per a actualitzacions

Els plans de formació per a actualitzacions es limiten simplement a posar al dia els usuaris sobre canvis que s'han fet en el programari o maquinari. Són curts i permeten tenir la plantilla al dia. Un gran avantatge és que eviten força problemes al departament informàtic.

Són molt curts, per aquest motiu moltes vegades també s'anomenen *sessions*, *seminaris*, *cursets*, *xerrades*, etc. Tenen una altra funció secundària molt important, que és la de mantenir la imatge del departament d'informàtica de preocupació pels usuaris.

2) Plans de formació per a la implantació de programari nou

Implantar programari

Implantar programari pot voler dir: desenvolupar una aplicació nova dins la mateixa organització, subcontractar-la o instal·lar-hi un programari estàndard (parametritzable).

Són realment els més complexos, ja que normalment s'han de fer sessions prèvies per escoltar les idees, els suggeriments i les propostes del col·lectiu implicat, i tot això integrar-ho en el programari que s'està implantant. El més complex d'aquestes sessions és que implantar sistemes nous implica canviar processos i maneres de treballar, i generalment això costa d'acceptar als col·lectius d'usuaris. És millor parlar-ne en aquesta fase perquè:

- Els usuaris senten que ells participen en el projecte, i això els predisposa més a acceptar-lo.

- És més fàcil canviar l'oposició inicial si s'argumenten els avantatges que obtindran amb el nou sistema (que encara no tenen i, per tant, continuen

treballant de la manera usual) i es diu que les propostes que es facin es tindran en compte en el desenvolupament del projecte.

- Es poden argumentar els inconvenients del mètode de treball actual, perquè com que el segueixen cada dia, i encara ho faran durant un cert temps, s'adonaran de la diferència.

- Com que no és un sistema imposat, sinó que s'hi fa participar per aconseguir que sigui àgil, útil i còmode per als usuaris, s'evita la sensació que tindrà errors bàsics.

- S'han de demanar opinions, propostes, idees, queixes, etc., sobre com hauria de treballar el sistema. Però també s'ha de deixar clar que no sempre és possible fer tot el que es demana i que, per tant, no es podran dur a terme totes les peticions.

Una vegada desenvolupat el programari, s'hauria de fer una formació pilot a un grup representatiu. Això serviria per ajustar el pla de formació i per detectar i corregir anomalies en els procediments d'instal·lació i configuració.

Si tot va bé, després es poden formar els usuaris i, seguidament, instal·lar el programari. D'aquesta manera, tan bon punt el trobin instal·lat a les estacions de treball, el podran començar a fer servir sense que els sigui estrany i sense causar incidències motivades pel desconeixement del programari.

3) Plans de formació per a usuaris nous

El pla de formació per a usuaris nous ha de ser un curset amb un fort component estàndard, perquè implica bàsicament ensenyar als usuaris tota l'operativa comuna que s'utilitza a l'organització. Fent-ho d'aquesta manera s'eviten molts errors i es guanya molt de temps, ja que es familiaritza l'usuari amb l'entorn de treball amb què es trobarà. Si és possible, s'hauria de fer un petit apartat més específic per al lloc de treball que haurà d'ocupar, quines eines específiques utilitzarà i com, quines bases de dades farà servir, etc.

És molt important per als responsables del departament d'informàtica i per als propietaris i gerents de les empreses reduir al màxim els problemes d'usabilitat amb què es troben els usuaris a causa dels canvis de programació. És important fer cursos de formació continuada als treballadors.

6. Centre d'atenció a l'usuari (CAU)

Avui en dia, la gran majoria de les empreses disposen de serveis TI amb les quals els seus empleats han d'interactuar en més o menys grau. Aquests empleats són simplement usuaris d'una tecnologia, de la qual no han de conèixer necessàriament els fonaments. Els serveis TI són per a aquests empleats una eina indispensable en molts casos, que ha d'estar disponible el major temps possible.

Què succeeix quan un d'aquests serveis o eines no treballen correctament, o simplement no treballen? L'usuari detecta un problema o incidència en una de les seves eines, però no té una noció clara (ni una explicació tècnica) de què passa.

Per a l'usuari, l'ordinador és una eina per augmentar el seu grau d'organització o eficiència i no té la necessitat de conèixer els detalls tècnics de l'equipament que fa servir.

De la mateixa manera que utilitza un fax, una fotocopiadora, el cotxe, un ascensor o el caixer automàtic sense conèixer el seu funcionament intern, aquest hauria de ser l'objectiu d'un bon sistema informàtic des del punt de vista de l'usuari.

En aquest punt apareix el concepte CAU per resoldre la següent pregunta que ens podem formular. Si l'usuari detecta un problema en una eina i no té els coneixements necessaris per solucionar-lo, què ha de fer?

Quan un usuari té un problema informàtic, s'ha d'adreçar a un únic punt per resoldre'l, el **centre d'atenció a l'usuari (CAU)**.

CAU

El centre d'atenció a l'usuari (CAU), de vegades, també rep el nom de *helpdesk*.

Un CAU és un servei integral que, mitjançant un punt de contacte, ofereix la solució de les incidències i l'atenció dels requisits relacionats amb les TI, com ara: computadores, perifèrics, recursos informàtics, programaris i plataformes en què treballen la majoria de les organitzacions.

El CAU juga un important paper en la provisió dels serveis TI. És un únic punt d'accés per als empleats o usuaris que necessiten ajuda. Sense un CAU, una organització certament podria afrontar pèrdues a causa de la ineficiència.

Tot i que hi ha diferents tipus de CAU, com els *call centre*, CAU experts i d'altres, en aquest apartat comentarem el més comú de tots, el CAU de **tres nivells**.

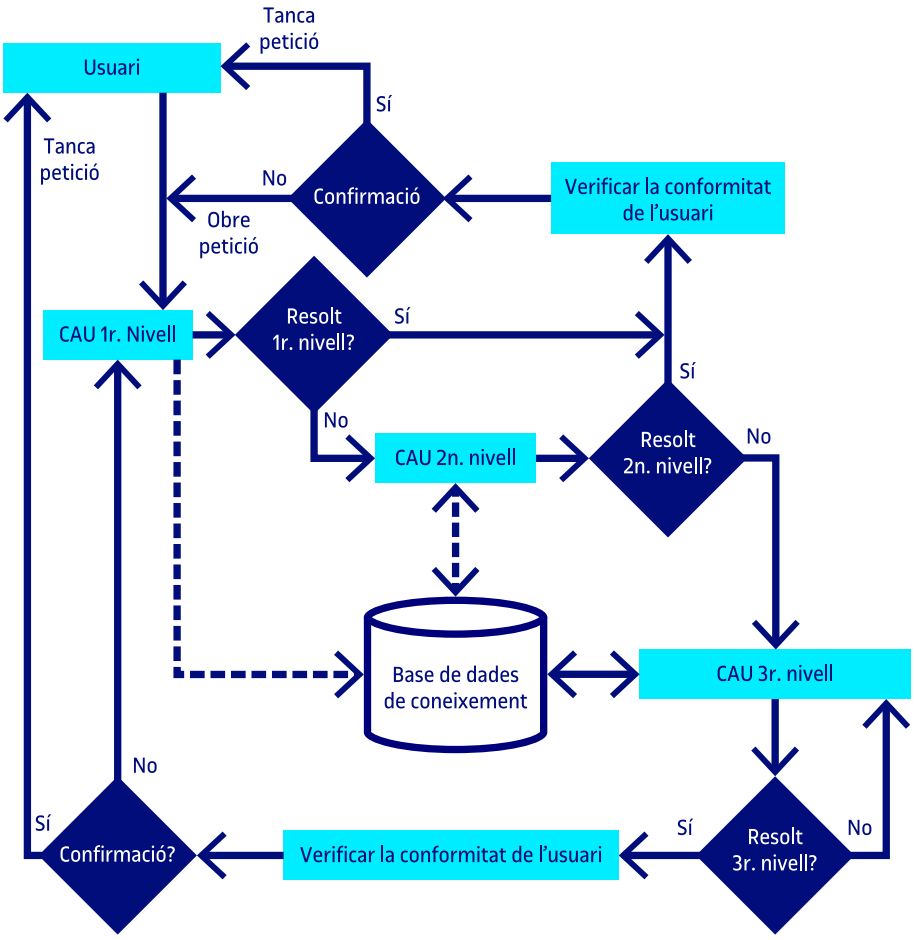
Quan un usuari detecta un problema, es posa en contacte amb el punt central de suport, sigui per telèfon, correu o altres mètodes. En aquest punt, la seva petició serà rebuda pel **primer nivell** de suport, que registrarà les seves dades, el problema i obrirà una **petició**.

Un cop oberta la petició, el primer nivell intentarà resoldre la petició revisant la **base de dades de coneixement**, on trobarà la informació i mètodes de resolució de les incidències ja tractades o comunes. Si el primer nivell pot resoldre la petició, la verificarà amb l'usuari i la tancarà. Si no pot solucionar la petició, aquesta serà assignada al segon nivell.

El **segon nivell**, format per personal amb un perfil tècnic més avançat i especialitzat (xarxes, servidors, programari, etc.), intentarà resoldre la petició. Si el tècnic assignat pot resoldre la petició, la verificarà amb l'usuari i la tancarà, i a més a més actualitzarà la base de dades de coneixement per a futures consultes. Si no pot solucionar la petició l'assignarà al **tercer nivell**.

Aquest últim nivell és el més especialitzat i moltes vegades és personal extern a l'organització. Aquests resoldran la petició, ho comunicaran a l'usuari i actualitzaran la base de dades de coneixement perquè aquesta informació serveixi per a futures consultes.

Figura 9. Esquema de funcionament d'un CAU de tres nivells



Així doncs, cada nivell d'un CAU té assignades funcions específiques, com es veu a la figura 9 i es descriu a continuació.

1) Primer nivell. Segons l'esquema presentat i la funcionalitat del CAU, el primer nivell d'assistència haurà de gestionar les activitats següents:

a) Rebre les incidències dels usuaris, sigui via telefònica, correu electrònic o programari específic.

b) Crear una petició o tiquet en el sistema de control de peticions. Imprescindible per a una bona gestió i seguiment de les incidències.

c) Classificació de la petició o incidència, en què cal especificar grup afectat: comunicacions, servidors o altres.

d) Priorització de la petició o incidència segons la seva criticitat, que pot venir donada pel nombre d'usuaris afectats, per l'afectació als sistemes productius i altres depenent de l'organització.

e) Escalar la petició al grup adient de segon nivell, si cal.

f) Cerca d'informació de resolució a la base de dades de coneixement per resoldre la petició al primer nivell.

g) Actualitzar les dades de l'usuari i del grup TI, si s'escau.

h) Verificació periòdica de l'estat de les incidències obertes i comunicació amb l'usuari.

i) Preparar documentació de gestió de la incidència.

2) Segon nivell. Tal com s'ha comentat al primer nivell, comentem les accions pertinents a aquest segon nivell (tècnics especialitzats):

a) Reclassificació de la petició o incidència si aquesta està definida de forma errònia.

b) Escalar la incidència al grup correcte, si ha estat assignada a un grup erroni.

c) Investigació i resolució de la incidència. Cal posar-se en contacte amb l'usuari, si cal.

d) Manteniment de la base de dades de coneixement respecte a la resolució de la incidència, si s'ha pogut resoldre. Cal documentar correctament els passos a seguir per solucionar una petició com la que s'acaba de resoldre.

e) Desenvolupar mecanismes per tal d'evitar peticions i incidències com les s'han pogut solucionar. Millora del sistema TI.

f) Tancament de la petició o tiquet, si s'ha pogut resoldre.

g) Escalar al tercer nivell, si no s'ha pogut resoldre la incidència.

3) Tercer nivell. En aquest tercer nivell trobarem els especialistes de cada àmbit que, moltes vegades serà personal extern a l'organització, i que donarà servei en moments puntuals davant d'una petició o problema d'un nivell de resolució molt alt.

a) Reclassificació de la petició o incidència, si aquesta està definida de forma errònia.

b) Investigació i resolució de la incidència. Cal posar-se en contacte amb l'usuari, si cal.

c) Manteniment de la base de dades de coneixement respecte a la resolució de la incidència, si s'ha pogut resoldre. Cal documentar els passos a seguir per solucionar una petició com la que s'acaba de resoldre.

d) Desenvolupar mecanismes per tal d'evitar peticions i incidències com les s'han pogut solucionar. Millora del sistema TI.

e) Tancament de la petició o tiquet quan s'hagi resolt.

6.1. Control de les incidències pendents

Alguna persona s'ha d'encarregar de veure diàriament quines incidències hi ha pendents i fer el seguiment de l'estat en què les tenen els tècnics. Això normalment ho fa una persona del primer nivell del CAU, ja que d'aquesta manera està en contacte amb els tècnics per consultar l'estat de les incidències, actualitzar la base de dades, si cal, i informar l'usuari. Mantenir l'usuari informat sobre l'estat de la incidència (especialment si és complexa o llarga de resoldre) és important per tranquil·litzar-lo i transmetre-li la impressió que el departament d'informàtica es preocupa del seu problema.

Petició al CAU

Una petició d'un usuari al CAU: «Necessito que s'instal·li el programa ABC al meu ordinador». El CAU, sense gaires problemes, s'adona que és un programari que no està a l'organització. Per tant, aquesta petició no pot prosperar per mitjà del CAU, sinó que com que el programari s'ha de comprar ha d'anar vehiculat per mitjà dels caps de departament, per exemple. S'ha d'explicar així a l'usuari i, per tant, no es pot atendre la seva petició.

Una altra funció molt important del personal d'atenció del CAU és fer de filtre de les peticions que hi ha, més enllà de les funcions o capacitats del departament d'informàtica o del sistema informàtic implantat a l'organització (això no vol dir que no es puguin recollir suggeriments). Tanmateix, el CAU ha de tenir la capacitat de denegar la gestió de les incidències.

Resum

Hem vist que l'usuari és una de les parts que dona sentit al sistema informàtic. Sense usuaris, la majoria de sistemes informàtics no tindrien sentit.

Un bon disseny de l'entorn facilita l'administració posterior dels servidors i simplifica els processos. Aquí la planificació prèvia és clau.

De la mateixa manera, una bona planificació de les configuracions i instal·lacions de les estacions de treball permet una administració eficaç per resoldre problemes dels usuaris i simplifica tots els processos i accessos posteriors. També tenim un bon conjunt d'eines que ens ajuden molt a dur a terme aquesta tasca. Una vegada més, la planificació prèvia és essencial.

L'usuari ha de tenir un punt de referència únic en cas de problemes informàtics. Aquest punt de referència permetrà resoldre ràpidament els problemes immediats, respondre les consultes sobre situacions conegudes, emetre una resposta en un temps raonable si el problema és singular i, sobretot, la sensació que algú es preocupa d'ell. Aquest punt de referència és el centre d'atenció a l'usuari (CAU).

La instal·lació d'un nou programari canvia la manera de treballar i s'ha de tractar amb molt de compte per tal de no crear un mal ambient laboral i perquè els usuaris utilitzin correctament el nou programari, ja que altrament poden fer fracassar aquesta instal·lació.

La formació dels usuaris és una qüestió sovint oblidada, però clau per a una organització que utilitza el sistema informàtic d'una manera eficient. Hi ha diferents tipus de formació depenent de la situació de l'usuari. Cal tenir-les en compte per aprofitar, al màxim, la seva utilitat.

Sigui com sigui, l'usuari sempre ha de tenir la sensació que té el suport i l'ajuda del departament d'informàtica per dur a terme la seva tasca. D'aquesta manera emetrà el judici que el departament d'informàtica «funciona correctament».

Activitats

1. Com a responsables de la gestió d'usuaris de la vostra organització, la primera tasca que voleu fer és definir la matriu de control d'accessos. Podríeu confeccionar aquesta matriu per als grups d'usuaris i objectes més representatius de la vostra organització.

2. Cerqueu per la xarxa algunes de les múltiples aplicacions de control remot de les estacions de treball que tenen una versió de proves i instal·leu-la per fer proves de la seva utilitat. Quins avantatges penseu que aportaria a la vostra organització?

3. Si teniu la possibilitat de disposar d'una estació de treball de proves, creeu la vostra pròpia estació de treball seguint els passos que s'indiquen en aquest mòdul. Si no teniu aquesta possibilitat, intenteu definir quins són aquests passos adaptats a la vostra pròpia organització.

4. Si disposeu d'un CAU a la vostra organització, intenteu definir el *graf* de nivells sobre el qual es basa el seu funcionament. Si no teniu cap CAU a la vostra organització, intenteu definir com us agradaria que funcionés i dibuixeu el *graf* de nivells. Com a tasca addicional, podeu cercar a la xarxa programaris de demostració dedicats a gestionar CAU per tal de triar-ne un d'adient.

Exercicis d'autoavaluació

1. Tenint en compte els grups d'usuaris i aplicacions següents que formen part de la vostra organització (institut de secundària), feu la taula d'aplicacions i comenteu la informació que se'n desprèn.

Grups:

Alumnes
Professors
Equip directiu
Gestió del centre

Aplicacions:

Ofimàtica
Eines d'aprenentatge
Aplicació d'avaluació (gestor de notes d'alumnes)
Comptabilitat del centre
Control centre (gestor horaris, entrades i sortides de personal, registre, etc.)

2. La direcció ha demanat posar en marxa un sistema de control horari a l'organització. El vostre cap d'informàtica es reuneix amb vosaltres, que sou tècnics de sistemes, perquè li doneu la informació tècnica per posar en marxa un paquet informàtic que controli l'entrada i la sortida dels treballadors. Així ho feu, però li recordeu que s'hauria de fer un pla d'informació i formació dels usuaris. El cap us diu que d'acord, però us demana l'opinió. Què li diríeu?

3. En una organització es crea un lloc de treball nou. Han posat una taula nova i a vosaltres, administradors de sistemes, us comuniquen l'arribada d'aquesta persona. Elaboreu el procediment complet perquè aquesta persona, quan arribi la setmana que ve, es pugui asseure a la taula nova, engegar l'ordinador i començar a treballar.

4. Com a responsable del CAU de tres nivells de la teva organització, defineix tots els passos que se seguiran fins al segon nivell des del moment en què rebeu la incidència d'un usuari d'una delegació que està, aproximadament, a 200 km de la seu central.

Solucionari

Exercicis d'autoavaluació

1. Creem la taula d'aplicacions. Aquesta és una de les possibilitats.

	Aplicació		Informació		Alumnes	Professors	Equip directiu	Gestió centre
	Local	Remot	Local	Remot				
Ofimàtica	X			X	L/E/X	L/E/X	L/E/X	L/E/X
Eines aprenentatge	X		X		L/E/X	L/E/X	L/E/X	
Aplicació avaluació		X		X		L/E/X	L/E/X	
Comptabilitat		X		X			L/E/X	L/E/X
Control centre		X		X				L/E/X

Extraiem la informació:

- **Llista de programari** complet que s'utilitza a l'organització (que, de fet, ja coneixíem). És la primera columna de la taula.
  - Programari d'ofimàtica
  - Programari eines d'aprenentatge
  - Programari d'avaluació
  - Programari de comptabilitat
  - Programari de control del centre

- **On hi ha la informació de cada aplicació**. Veiem que hem decidit que estigui tota en remot, excepte les dades de les eines d'aprenentatge, ja que són aplicacions que no actualitzen les seves dades un cop han interactuat amb l'usuari.
- **Relació de grups d'usuaris**. Amb la relació de grups que tenim, veiem que hi haurà usuaris que podran pertànyer a, com a mínim, un parell de grups: professors i equip directiu.
- **Llista de programari que s'utilitza per grups**. L'organització tindrà el programari que sembla que necessita tothom, i cada grup tindrà el que és específic per a cada departament. Cal anar amb compte amb la informació, ja que l'ofimàtica requereix un estudi detallat, perquè si no, amb permisos per a tothom, tots els usuaris veurien tota la informació.
- La relació d'aplicacions candidata per crear l'**estació de treball model**.
  Ofimàtica: sí.

2. Com a tècnic de sistemes (o administrador dels servidors o dels usuaris), se suposa que l'hem informat d'una aplicació que s'ajusta a les necessitats de l'organització, des del punt de vista tècnic i des del punt de vista de la necessitat que s'ha de cobrir. Ara bé, es tracta de donar l'opinió sobre com pensem que s'ha de desenvolupar el pla de formació, per tant, li explicaríem les línies mestres amb què el faríem.

Formació general

- Que el personal de l'organització conegui l'eina de la gestió horària.
- Que entengui els avantatges que es desprenen d'aquesta nova eina.
- Que no la vegi com un mecanisme de control.
- Enumerar els avantatges que comporta. Per exemple:
  - Consulta del temps d'entrada i sortida des de qualsevol ordinador (controlat per contrasenya) individualitzat per a cada persona.
  - Petició de dies per a assumptes personals des de qualsevol ordinador en qualsevol moment.
  - Recuperació automàtica de les hores per mitjà del sistema, en cas que algun dia s'arribi tard.
  - Es poden introduir incidències (dir que s'ha arribat tard) directament des de qualsevol ordinador.

– Ara –abans no era possible– el temps sobrer es podrà fer servir per a assumptes personals, gràcies a aquest nou sistema.
– I altres coses.

Formació d'administració

Aquest programari necessita formació addicional per a les persones que en gestionen les incidències i detecten les anomalies horàries. Com que utilitzen una altra part del programari que no fa servir tota l'organització, necessiten una formació complementària.

Formació de nòmines

Lògicament un programari d'aquestes dimensions ha d'enllaçar amb nòmines, i com que es fan mensualment i se n'ocupa un altre departament, es fa servir una part del programari que no utilitza ningú mes. Necessiten una formació complementària.

Formació d'informàtica

L'aplicació maneja dades sensibles, té dispositius per fitxar en un o diversos llocs de l'organització i sembla que enllaça elements diferents (almenys nòmines i administració). Per tant, és una aplicació força complexa. Cal la formació d'alguna o algunes persones del departament per assegurar que la instal·lació es fa correctament, que davant d'un problema es pot resoldre, i que les còpies de seguretat es fan de la manera adient.

Segurament un possible ordre de la formació seria:

1) Jornada inicial amb el personal de l'organització per avaluar-ne l'opinió.
2) Formació d'informàtica.
3) Formació de nòmines.
4) Formació d'administració / formació de l'organització.

Per tant, faria unes jornades de dues hores per explicar al personal el funcionament del sistema, com s'utilitza, els avantatges que té i els canvis i les millores que s'introduiran a l'organització gràcies a la implantació d'aquest programari.

3. En línies generals, les tasques poden ser les següents:

- Comprar un ordinador complet (pantalla, teclat, caixa, placa de comunicacions, etc.).
- Preguntar al departament adient el lloc de treball i les responsabilitats d'aquesta persona, per determinar:
  – El lloc físic on ha d'instal·lar l'ordinador.
  – El grup o els grups als quals pertany la persona.
  – Per tant, els permisos que tindrà dins el sistema.
  – Per tant, el programari que necessita utilitzar.

- Establir la connexió de la xarxa física fins al lloc de treball.
- Donar d'alta l'usuari als servidors.
- Crear-li un compte de correu.
- Habilitar el seu espai privat.
- Donar-li, si cal, permisos especials per als servidors de les bases de dades.
- Habilitar encaminadors (*routers*) i commutadors (*switches*), amb l'adreça en placa perquè aquesta placa de comunicacions pugui enviar i rebre informació per la xarxa de l'organització.
- Clonar la imatge de les estacions de treball en aquest ordinador nou.
- Ajustar la configuració, atès que tenim l'ordinador model: ajustar els paràmetres de la xarxa com ara el nom de l'ordinador, l'adreça IP, configurar les impressores que utilitzarà, etc.
- Instal·lar, si cal, programari específic.
- Provar l'ordinador com si fóssim aquesta persona.
- Si tot ha anat bé, portar l'ordinador al lloc de treball de la persona, perquè quan arribi l'hi trobi.

No és sobrer enviar-li un correu electrònic que expliqui quina és l'operativa bàsica (si no ha fet cap formació a l'organització) i on es pot adreçar per solucionar els problemes. També és recomanable fer-ho en suport paper, telefònic o presencial, perquè, si no sap fer servir l'eina de correu electrònic, un missatge de correu no serveix de gran cosa.

4. Tenint en compte que tenim un CAU de tres nivells:

Primer de tot rebrem la incidència per un únic punt de control que gestionarà el primer nivell del CAU. Aquests obriran el tiquet identificatiu de la incidència a la base de dades del CAU i informaran l'usuari.

Des del primer nivell s'accedirà a la base de dades de coneixement per intentar cercar solucions ja certificades per al problema. Si se soluciona el problema, es tancarà la incidència d'acord amb l'usuari. En cas contrari, aquesta s'escalarà al segon nivell.

Al segon nivell, un tècnic especialitzat de l'àrea (comunicacions, BD, etc.) atendrà el problema i cercarà una solució. Per tal de dur a terme les accions convenients a l'estació de treball afectada o, fins i tot, per tal de comprovar l'error *in situ*, utilitzarem eines de connexió remota que ens permetran accedir-hi ràpidament sense haver-nos de desplaçar.

Si la troba, actualitzarà la base de dades de coneixement i tancarà la incidència amb la conformitat de l'usuari. En cas contrari, la passarà al tercer nivell.

Glossari

antivirus *m* Programari que cerca virus al disc dur dels ordinadors.

base de dades de coneixement *f* Base de dades amb la informació necessària per resoldre incidències resoltes anteriorment. També permet extreure patrons i conductes de resolució.

CAU *m* Vegeu **centre d'atenció a l'usuari**.

centre d'atenció a l'usuari *m* Part del departament d'informàtica dedicat a atendre les incidències dels usuaris.
sigla: CAU

clonació *f* Operació de duplicar el contingut d'un disc dur en un altre disc dur, amb la qual cosa s'obté una còpia exacta impossible de distingir de l'original.
sin.: clonar

control remot *m* Control a distància d'una estació de treball o servidor mitjançant un programari client/servidor per a aquest efecte.

entorn d'usuari *m* El que troba l'usuari quan engega l'ordinador per treballar.

estació model *f* Ordinador patró que es prepara i s'utilitza com a base per configurar tots els altres ordinadors de l'organització. Es fa mitjançant programari, ja que d'aquesta manera la tasca és més senzilla.

FAQ *f pl* Vegeu **preguntes més freqüents**.

fitxer de signatures *m* Relació de marques que identifiquen els virus. Els utilitza l'antivirus per comparar i trobar virus.

imatge del disc *f* Còpia exacta del contingut d'un disc en un moment donat.

incidència *f* Demanda d'un usuari de solució d'un problema que l'impedeix treballar correctament.

perfil *m* Informació guardada de l'usuari, que amb la identificació configura l'estació de treball, de manera que ajusta els permisos, els accessos, la configuració de l'entorn gràfic, etc. (l'entorn de treball en general).

petició *f* Demanda d'un usuari per a l'actualització d'un programari, nova instal·lació o configuració.

PMF *f pl* Vegeu **preguntes més freqüents**.

preguntes més freqüents *f pl* Conjunt de dubtes sobre un tema concret que els internautes es plantegen repetidament i que es guarden en una pàgina web amb les solucions corresponents.
en.: *frequently asked questions*
sigla: PMF
sigla en.: FAQ

programari de base *m* Programari que es considera que han de tenir tots els ordinadors de l'organització que utilitzen els usuaris. Normalment comprèn, com a mínim, el sistema operatiu, el programari d'ofimàtica, un navegador i un programa de correu electrònic, i també aplicacions específiques de l'organització comunes a totes les estacions de treball.

programari d'ofimàtica *m* Programari que comprèn un programa de full de càlcul, un processador de textos, una base de dades petita, un programa de presentacions, una agenda i, actualment, també un programa client de correu electrònic.

taula d'aplicacions *f* Resum que conté la llista d'aplicacions amb la informació i els permisos que s'associen a cada grup de l'organització per a cada aplicació.

TI *f* Tecnologia de la informació.

TIC *f* Tecnologia de la informació i la comunicació.

tiquet *m* Número o identificador que identifica la petició o incidència oberta per l'usuari per tal que es pugui dur un control sobre aquesta.

Bibliografia

Barcelo García, M.; Pastor i Collado, J. (1999). *Gestió d'una organització informàtica*. Barcelona: Universitat Oberta de Catalunya.

CEP (2007). *Administración del Servicio de Atención al Usuario*. Madrid: CEP.

Diversos autors (2019). *Windows Server 2016 y Powershell: Utilice los Scripts Para Automatizar Sus Tareas Cotidianas de Administración* (2a. edició). Barcelona: ENI.

IT Governance Institute (2007). *COBIT Quickstart* (2a. edició). Estats Units: IT Governance Institute.

Jumes, J. G.; Coopper, N. F.; Chamoun, P.; Feinman, T. M. (1999). *Microsoft Windows NT 4.0 Seguridad, auditoría y control*. Madrid: MacGraw Hill.

Microsoft Corporation (1997). *Sourcebook for the help desk* (2a. edició). Estats Units: Microsoft Press.

Microsoft Corporation (1997). *Windows NT 4.0 Workstation Kit de Recursos*. Madrid: MacGraw Hill.

Office of Government Commerce (2007). *ITIL: Service Strategy*. Regne Unit: Office of Government Commerce.

Rohaut, S. (2017). *Linux: Dominar la Administración del Sistema*. Barcelona: ENI.