KEEPWARE

(INSTAL·LACIó I EXPLOTACIó DE SISTEMES INFORMàTICS)

Jaume Viñas i Turné,
Enginyer de Telecomunicació,
Analista informàtic.

Març 1993

Premeu aquí per l'índex

TAULA DE CONTINGUTS

Jaume Viñas, "KEEPWARE", 1995

PREFACI

L'èxit d'una informatització no es basa només en omplir l'empresa de màquines i programes. Hi ha molts més factors. Aquests recursos han de ser ben usats. Cal formació, cal organització.

Però sens dubte el més fonamental del que cal és que els recursos siguin disponibles. Que els ordinadors funcionin i els programes i les dades hi siguin accessibles. Les millors màquines, els millors programes, la millor formació, etc. no serveixen de res front un tall de subministrament elèctric o un incendi.

El present informe pretén ser una eina general i genèrica perquè els responsables, a qualsevol nivell, de l'èxit d'una informatització, tinguin alguna cosa amb la qual abordar els aspectes que incideixen en l'esmentada disponibilitat.

Aquesta obra no pot ni vol tractar intensament els aspectes als quals fa referència, però sí que els tracta extensament en el sentit de no voler deixar-se'n cap.

Quan aquests responsables pensen en els dits aspectes, tenen dues solucions:

1. posar-se en mans de la/es empresa/es que subministra/en el hardware o/i el software,
2. demanar una informe / assessoria a una empresa de serveis o professional especialitzat/da i independent.

En el primer cas, les esmentades empreses o bé només procuraran que els seus productes satisfacin el client, sense donar-li cap suport o avís addicional, els quals casos encara existeixen, o bé proporcionaran en forma de servei addicional, amb factura addicional, un servei com el que contractariem en el segon cas, sense, estar clar, fer desaparèixer mai ombres de dubte quant a especialització i independència de les conclusions.

Cada vegada és més freqüent optar per la segona solució, per característica dels mercats informàtics, quant a obertura dels sistemes actuals i necessitat de l'especialització.

S'encarregui a uns o altres, aquesta assessoria sempre hauria de començar, i, segons com, acabar, amb un contingut equivalent al de l'obra que teniu a les mans. Que el responsable disposi d'aquests criteris "a priori" l'hi pot estalviar temps, diners i sorpreses.

Aquesta és la pretensió d'aquesta obra.

Jaume Viñas, "KEEPWARE", 1995

INTRODUCCIÓ

Quan una organització prèn la decisió d'informatitzar-se normalment ho fa amb un cert assessorament previ i en forma d'una transcendental decisió. La inversió acostuma a ser forta i s'espera de la introducció de la informàtica un fort impacte organitzatiu i en el compte de resultats. Aquesta esperança i/o temor arriba a vegades més enllà del que és lògicament previsible.

En definitiva, és clar que les empreses, les institucions, les administracions, s'ho miren molt abans d'adquirir un sistema informàtic.

Es considera acuradament l'elecció del hardware, el software de base i del software d'aplicació. Es consideren les possibilitats de creixement, la compatibilitat amb altres sistemes, el servei post-venda i, per supòsit, l'adaptació a les necessitats.

Això és comú en la totalitat dels futurs usuaris d'informàtica.

Hi ha encara una altre sèrie de temes també imprescindibles que solen ser menyspreats, tractats a corre-cuita o fins i tot oblidats per sempre més.

Són els que es refereixen a la seguretat, el manteniment i la correcta operació del sistema. En relacionem alguns:

- la correcta situació física dels equips,
- una adequada instal.lació elèctrica,
- una alimentació acurada,
- control ambiental,
- sistemes de vigilància i alarma,
- manual i pla d'explotació,
- contractes d'assistència i llicència,
- pla de seguretat,
- còpies de seguretat,
- pòlissa d'assegurança.

Fer en els noranta qualsevol tipus de treball sobre informàtica és quasi condemnar-lo d'origen a durar poc quant a la seva validesa. La velocitat amb què una realitat informàtica queda obsoleta per a donar una altra realitat informàtica és vertiginosa.

Les noves tecnologies hardware i software fan evolucionar el mercat d'una manera fins i tot difícil de seguir.

Hi ha però una característica fonamental que es conserva des de l'ENIAC de fa trenta anys fins els sistemes experts d'avui i que es mantindrà en tot el futur previsible: els ordinadors són bàsicament electrònics.

Funcionen amb energia elèctrica, dissipen calor, la

informació els arriba i en surt en cables. Tret que siguin especialment dissenyats són fràgils. Acostumen a tenir interruptors i polsadors perillosos.

De l'anàlisi d'aquestes característiques apareixen una sèrie de necessitats:

alimentació
ventilació i refrigeració
protecció i aïllament físic

Aquestes necessitats són sempre allò que el fabricant especifica amb major èmfasi en el moment de la instal.lació. Per desgràcia això arriba a l'usuari quan el temps en quant a la planificació de recursos i procediments és ja escàs si no és que ja s'ha esgotat.

El full de característiques tècniques de qualsevol equip hardware, i prenem per exemple una CPU (Unitat Central de Processament) en concret, inclou sempre elements com ara:

* tensió nominal d'alimentació,
* marge de tolerància de la tensió,
* potència de consum en diversos règims de treball,
* rang de temperatura i d'humitat relativa ambientals.

A més, la CPU de referència té un plafó central amb dos polsadors per inicialitzar el sistema i un interruptor general d'alimentació.

Aquesta CPU, com totes, consisteix en un elevat nombre de components electrònics sobre fràgils plaques de circuit imprès i tot ell muntat en rails dins d'un armari de fina xapa metàl.lica. Per darrera té un plafó de connexió de cables coaxials i de "flat cables" que constitueixen el nexe d'unió amb totes les màquines perifèriques

Característiques semblants trobarem en qualsevol element hardware i, en especial, en aquells que per raons operatives, i inclús de requeriments tècnics de senyal a vegades, han d'estar situats físicament a prop de la CPU: unitats de disc, unitats de cinta, consola, etc... Són els que podríem denominar "elements centrals".

Per suposat que una adequada protecció d'aquets elements centrals i el compliment dels seus condicionaments ambientals i d'alimentació no es poden garantir en l'entorn en què treballa habitualment el personal usuari del sistema, un entorn d'oficina en el millor del casos.

Es possible tenir tanta sort que totes aquestes precaucions resultin innecessàries.

Teòricament és possible que el clima natural sigui el perfecte per al funcionament de l'ordinador en tot moment, que

el subministrament elèctric sigui permanentment estable, etc. Però tot això és francament utòpic i literalment impossible de garantir.

Allò real, el que mostren les estadístiques (les poques estadístiques que hi ha al respecte, que no passen de ser la punta de l'iceberg, perquè empreses i responsables tendeixen a ocultar o maquillar els seus errors en vistes a no perdre credibilitat, prestigi o confiança dels clients) és que tard o d'hora apareixen aquests problemes en major o menor grau.

Tot equip té alguna vegada un fracàs i si no s'han près amb antelació les mesures oportunes acaben per prendre's quan ja s'ha produït un dany irreversible i probablement important.

Si s'ha cremat part del hardware o s'ha perdut el treball d'una setmana o, senzillament, queda inoperable el sistema durant un cert temps, el mal és certament irreversible perquè ja res no podrà impedir-lo i serà tant més important quan més gran sigui el sistema.

Per a qualsevol sistema "multi-lloc" és necessari de conjurar aquests riscos.

TERMINOLOGIA

Acabem de demostrar l'existència d'un conjunt de temes o aspectes amb importància a l'entorn de la informàtica. Tota aquesta obra està dedicada a analitzar aquest conjunt. Ens apareix la conveniència de "batejar-lo" d'alguna manera.

Com sempre que es "fabrica" un nom nou, s'ha de buscar que sigui assequible i que recordi el concepte el qual denomina.

Ja que es tracta d'una part del sistema informàtic, en la seva concepció més àmplia i completa, farem servir una norma que existeix "de facto" per a aquestes parts. Es tracta del sufix "ware".

Va començar a usar-se en la informàtica amb la paraula "hardware", ja existent en l'idioma anglès, i usat per comparació fonètica, donà lloc a "software" i "firmware", primer, i a tot un seguit de neologismes, molts d'ells enregistrats com a marques comercials, més recentment.

Totes aquestes paraules tenen l'inconvenient del seu origen anglosaxó, que les converteix en barbarismes per a les demés llengües. Però aquest és un mal que accepto.

Queda determinar el lexema prefix més adequat al nostre cas. Aquesta adequació consisteix en el fet de definir el conjunt. Així el problema queda reduït a determinar quina és la propietat característica que defineix per comprensió el nostre conjunt.

La característica fonamental del nostre conjunt és que els seus elements constitueixen un entorn, mig físic mig lògic, que envolta el sistema informàtic, en la concepció més restrictiva, tot mantenint-lo i guardant-lo per tal de possibilitar i protegir el seu funcionament normal, la disponibilitat del sistema informàtic per als seus usuaris.

Després de dissenyar i estudiar diverses opcions, com ara "periware" (d'envoltar) o "profilware" (de prevenir la malaltia), em quedo finalment amb "keepware" (de l'anglès "to keep": mantenir, guardar).

Registre Propietat Intel.lectual núm. 3609 de 31-3-93. Versió corregida

Jaume Viñas, "KEEPWARE", 1995

CONDICIONS DE FUNCIONAMENT

Els fabricants donen instruccions i recomanacions al respecte, com les que segueixen:

I EMPLAÇAMENT

* Amplada mínima d'un metre en passadissos i portes per al trasllat.
* Muntacàrregues amb suficient espai i capacitat (250 kg/m2).
* No situar l'equip en zones de trànsit i passadissos.
* Espai suficient per a la col·locació del sistema d'acord a les dimensions del mateix, incloses les zones de manteniment reservades per a cada perifèric.
* Disposar de l'espai lliure que permeti moure els equips (mínim 75 cm fins la paret i 50 cm entre si).
* Protecció de la radiació solar directa (equips i suports magnètics).
* Disposar de mètodes efectius de prevenció d'incendis.

II MEDI AMBIENT

- Temperatura funcionant 16-26ºC (òptima recomanada 21-23ºC).
- Temperatures extremes amb l'equip aturat: 16-32ºC.
- Màxima temperatura de bulb humit 24,5ºC.
- Màxima variació de temperatura 6,5ºC per hora.
- Humitat relativa funcionant 40-60% (no condensada).

III CONTAMINACIÓ AIRE

- L'aire procedent de calefacció, ventilació o condicionador haurà de ser filtrat, essent necessària la comprovació, neteja i canvi periòdic dels filtres.
- No es permetrà de fumar, beure o menjar prop dels discos i unitats de cinta.

IV ELECTRICITAT ESTàTICA

- S'ha de disposar de l'apropiada instal·lació elèctrica abans de la instal·lació de l'equip.
- La instal·lació disposarà d'una única i efectiva presa de terra (3 Ohm).
- L'escomesa des del comptador fins al quadre de distribució per a l'equip estarà protegida en tub metàl·lic, serà independent, estable i exempta de soroll elèctric. El quadre de distribució disposarà d'interruptor general i magnetotèrmics i diferencials per a cada branca de distribució. S'usaran diferencials de 300 mA o, millor per a la protecció de les persones, de 30mA. L'esmentada línia elèctrica serà per a ús exclusiu de l'equip. Els equips que utilitzen unitats de disc independents disposaran d'un magnetotèrmic per a cada unitat de disc.
- Llevat especificació contrària, els límits de xarxa permesos són 210-250 Volts. Cas d'excedir aquets límits

s'instal·larà un estabilitzador de tensió.

- Es recomana l'ús d'un sistema d'alimentació ininterrompuda (també denominats grups de continuïtat, SAI o UPS).
- L'alimentació constarà d'una fase, d'un neutre i d'una terra. Quan el neutre presenti més de 0,5 Volts respecte a terra, es disposarà de transformador separador connectat el neutre del secundari a terra (en cas de necessitar estabilitzador, aquest s'haurà d'incloure).
- Els equips remots estaran connectats a la mateixa fase que la unitat central, a ser possible.
- La freqüència de la xarxa haurà de ser 50 Hz +/-0,5 Hz.

VI CABLAT

Hauran de passar com a mínim a 1 metre de distància de qualsevol productor de soroll elèctric, com tubs fluorescents, motors, transformadors etc. En cas contrari hauran de ser protegits mitjançant tub metàl·lic connectat a terra.

Els cables d'interconnexió entre edificis hauran d'estar protegits en tub metàl·lic posat a terra.

Les interconnexions ocultes hauran de tenir fàcil accés.

En les proximitats dels equips, es deixarà un mínim d'1 metre de cable.

CONCLUSIONS PRELIMINARS

Si pensem per un moment en quina és la importància real del servei que dóna l'ordinador sens dubte ens mirarem tots aquests requeriments acuradament, de manera generosa, gens restrictiva.

Ja estem en condicions de fer-nos unes reflexions immediatament prèvies a l'establiment de solucions per a les correctes instal·lació i explotació del nostre sistema.

Podrien ser les següents:

1 Els elements centrals de l'ordinador són fràgils en si mateixos hauran de ser protegits de cops accidentals, pols excessiva, brutícia, llum solar directa, etc.

2 Entre els diferents elements centrals i des d'aquests fins tots els perifèrics hi ha cables també fràgils en si mateixos i quant a la seva connexió als aparells. Cal evitar que es moguin molt, que s'enredin i que siguin trepitjats o estirats.

3 Prop d'aquests elements centrals sol haver cert material com ara peces, recanvis, suports magnètics de treball i de backup que també demanden especial protecció.

4 Tot el mencionat fins aquí haurà de ser també protegit de males intencions: motins, sabotatges, etc.

5 Recapitulant els anteriors punts arribem a la conclusió que és convenient de tancar els elements centrals i algun material annex en un recinte segur, ben protegit del seu exterior, a ser possible amb una porta de seguretat. Convé que no tingui finestres que donin a l'exterior de l'edifici i que l'accés a aquest recinte sigui molt restringit i controlat, inclús amb una llista de persones autoritzades i amb un registre d'accessos. En aquest recinte no haurà d'haver conductes d'aigua, gas o qualsevol altre element que suposi un augment de risc.

6 Si tanquem totes aquestes màquines en una sala, la seva dissipació elevarà la temperatura d'aquesta sala fins treure-la dels marges donats pels fabricants. Cal pensar en ventilació i fins i tot en refrigeració.

7 Aquesta és una raó de més per restringir al màxim el número d'accessos a la sala de l'ordinador.

8 En un altre ordre de coses, l'alimentació defectuosa comporta un alt risc. Els equips estabilitzadors poden protegir el sistema contra oscil·lacions i transitoris de la tensió. El deixen desprotegit front microtalls. La protecció adequada només la pot proporcionar l'aïllament total a través d'un grup de continuïtat, amb emmagatzemament temporal d'energia.

9 Una vegada més s'incrementa la necessitat de refrigeració i

aquesta vegada és determinant. L'ús d'un equip d'aire condicionat és ja inqüestionable. Certs aparells tenen sobre els de consola partida ("split") l'avantatge de renovar l'aire de forma controlada. En qualsevol cas cal preveure per a ells les necessitats d'alimentació elèctrica i el desguàs de la humitat que poden condensar.

10 Una sala com la que estem configurant, amb bastants aparells funcionant sense presència humana i probablement (fins i tot de forma aconsellable) les 24 hores del dia i on l'energia en ús o emmagatzemada és un perill constant quant a que un malfuncionament acabi en incendi o, com a mínim, en les condicions ambientals fora de marge. Es fan necessari un sistema de detecció i alarma.

En resum, unes condicions idònies de funcionament del hardware ens obliguen, com s'encarrega de recordar-nos el fabricant, a una instal.lació idònia.

Jaume Viñas, "KEEPWARE", 1995

COM ENFOCAR EL DISSENY DE LA INSTAL·LACIÓ

Com a tota obra d'enginyeria, la instal·lació física, i en especial la dels elements centrals, ha de ser adequadament projectada i documentada, pensant en el manteniment posterior.

També hauria de preveure les ampliacions probables, especialment en tot allò més difícil de modificar mentre cal mantenir el sistema informàtic en servei: càrrega elèctrica, condicionament ambiental, mesures contra-incendis, etc.

La legislació vigent ha de ser tinguda en compte. Hi ha tot un seguit de normatives a complir. En mencionem algunes:

- Les normes sobre Instal·lacions Elèctriques en Baixa Tensió, dins les Normes Tecnològiques d'Edificació (NTE-IEB)
- Les Condicions de Protecció contra Incendis en els Edificis, dins les Normes Bàsiques d'Edificació (NBE-CPI) i les Instruccions de Protecció contra el Foc (IPF)
- Les relatives a la transformació i distribució d'energia elèctrica
- El Reglament Electrotècnic de Baixa Tensió i les instruccions MI-BT
- El Reglament de Seguretat per a Plantes i Instal·lacions Frigorífiques
- El Reglament d'Aparells a Pressió
- La Directiva 90/270/CEE relativa a l'ergonomia dels llocs de treball.

El disseny de la instal·lació d'un sistema informàtic apareix com una tasca bastant complexa i crítica. Se sol utilitzar un de dos sistemes: el procés "d'oferta i especificació" i el mètode "de claus en mà".

En el sistema d'oferta i especificació es contracta una empresa o equip de professionals per realitzar especificacions i l'esbós del projecte final. Aquesta empresa sol·licita llavors ofertes a contractistes, el quals per la seva part reuneixen ofertes de subcontractats. Aquests recullen a llur temps ofertes de distribuïdors de falsos terres, de sistemes SAI I equips d'energia, sistemes d'extinció d'incendis, etc.

Finalment, el client escollirà un projecte definitiu, a un preu predeterminat.

Per determinar les especificacions, els enginyers molt sovint busquen el catàleg d'un bon distribuïdor i copien l'especificació d'un producte concret paraula per paraula.

En un procés de tres nivells d'ofertes amb aquest, ni el contractiste principal ni ningú dels subcontractats necessiten preocupar-se de la qualitat de l'equip.

El que sol passar, és que el diner es converteix en l'únic criteri per a les ofertes i la pressió per ser el que realitzi l'oferta més baixa s'intensifica. A més a més, existeix un marge de benefici habitual a cada nivell.

Jaume Viñas, "KEEPWARE", 1995

El sistema denominat "de claus en mà", o també de "disseny i construcció", constitueix una via alternativa.

Amb aquest mètode, un contractista especialitzat en instal.lacions d'ordinador dirigeix i supervisa tot el treball directament. Normalment, aquests especialistes treballen amb subcontactats que aporten servei i destresa i en els quals el contractista confia.

Utilitzi la proposta de contractació que utilitzi, la companyia ha de considerar el sistema informàtic globalment. Les unitats d'aire condicionat són enllaçades al subministrament d'energia, i ambdues connectades al sistema d'extinció d'incendis: Totes les parts del sistema hauran de ser coordinades entre si.

Però, qui sap com construir adequadament un centre de processament de dades?

Cal comprovar que l'ajuda que es contracta està qualificada. Els arquitectes i certs enginyers no tenen perquè saber com evitar que els encreuaments en els cables de terra afectin les transmissions de dades.

També cal fer formació a un nombre suficient de persones perquè facin servir la maquinària de l'entorn. Els operadors hauran de saber com funciona el sistema d'extinció d'incendis, el SAI i tots els indicadors. En el cinc primers minuts d'una crisi poden fer-se errors d'un cost molt important.

Jaume Viñas, "KEEPWARE", 1995

COM ENFOCAR LES AMPLIACIONS

Les ampliacions d'un sistema informàtic en explotació han de fer reconsiderar tots els aspectes mencionats en aquest informe. Sovint això no es fa i una bona instal.lació-explotació queda degradada.

Cal tenir en compte tres tipus de possibles necessitats.

El primer tipus inclou:
- Més càrrega elèctrica en quadres de control i UPSs
- Més instruments en els quadres de control
- Nova presa de terra
- Nou cablat d'alimentació
- Nou cablat de dades
- Més refrigeració

El segon tipus inclou:
- Mès càrrega de treball per als operadors
- Execució d'obres i períodes transitoris i d'espera
- Interrupcions en el servei, a causa de les obres
- Increment del risc d'avaries en els equips existents

El tercer tipus inclou:
- Formació dels operadors
- Ampliació del Manual d'Explotació
- Nou disseny del Pla d'Explotació
- Nou disseny del Pla de Seguretat
- Nou disseny dels procediments de Còpies de Seguretat
- Adquisició de nous tipus de fungibles
- Ampliació de la pòlissa d'assegurança

TENDèNCIES

Cal assenyalar que els nous ordinadors tenen cada vegada menys condicionaments de funcionament dels aquí exposats (menor dissipació, menor consum, menor espai, menor manteniment) i que certes funcions són assumides directament pel hardware, disposant dins del propi armari de la CPU d'alguns elements del keepware (bateries per sostenir la memòria, detectors d'incendi).

Això no és, avui per avui, més que una tendència, però el cert és que es va cap a la supressió de la sala de l'ordinador sense cap detriment per al keepware, que segueix i seguirà existint.

Una mesura que facilita aquesta tendència, i que és aconsellable amb cautela en tot cas, es basa en guardar sistemàticament els suports magnètics en armari de seguretat ignífug, per compte de fer-lo en armaris o prestatges dins de la sala de l'ordinador.

Un altre tendència que es troba en les instal·lacions actuals consisteix en els denominats "centres de funcionament autònom", on els operadors han estat substituïts per keepware, hardware, software i pels propis usuaris.

La idea d'una sala d'ordinadors hermèticament tancada i sense ningú no és molt llunyana de la realitat a la qual s'encaminen actualment aquestes sales. El concepte de "funcionament autònom" s'està consolidant.

En la majoria dels casos els aparells només són manipulats pels tècnics de manteniment/reparació, o en cas d'incident imprevist, per exemple un tall de tensió.

El funcionament autònom de les sales d'ordinador comporta alguns avantatges que resulten obvis: les condicions de temperatura i d'humitat són optimitzades per al hardware; els riscos associats a contaminants com el pols disminueixen considerablement i la seguretat es veu simplificada quan els problemes d'accés no revesteixen ja tanta importància.

De totes maneres, no és possible prescindir totalment d'operadors. Fins on és possible preveure el futur, persistirà la necessitat de traslladar les dades més crucials a medis transportables a efectes d'arxiu o d'obtenció periòdica de còpies de seguretat.

Altra operació igualment necessària és la de guardar els arxius de dades de major volum i poc sol·licitats en suports off-line.

Jaume Viñas, "KEEPWARE", 1995

RECEPCIó I UBICACIó DELS EQUIPS

SELECCIó I PREPARACIó

Abans de la recepció de l'equip, els elements a considerar són:

* Accés i aparcament per als vehicles de transport, incloent, si és necessari, autoritzacions especials.
* La possibilitat d'entrada dels equips amb els seus embalatges en l'edifici, ja que en cap cas l'equip ha de ser desembalat a la intempèrie.
* La possibilitat d'entrada dels equips en l'emplaçament definitiu.
* La selecció de la ubicació apropiada i la disponibilitat d'espai suficient com per a permetre l'accés per a manteniment als equips, sense que sigui necessari el moviment dels mateixos. Es a dir, separació mínima entre els equips ("clearance") i les parets de l'habitació i una separació dels equips entre sí. També és necessària perquè hi circuli l'aire.
* El condicionament de la ubicació de forma que no es requereixin obres posteriors.
* La preparació de la instal·lació elèctrica, tenint la potència suficient i havent realitzat la instal·lació necessària.
* L'anàlisi de les condicions ambientals: temperatura, humitat, electricitat estàtica, etc. i la seva correcció.
* Els cables d'interconnexió
* La instal·lació de doble sòl (si es requereix).
* L'enllumenat ha de proporcionar 500 lux a 0,85 m d'altura, seguint la norma DIN 5035.

En la recepció cal:

- Comprovar la llista de material rebut i comparar-la amb el que esperàvem,
- Verificar que els equips i materials arriben en bones condicions,
- Guardar tot el material d'embalatge,
- Guardar les diverses instruccions de desembalatge, muntatge, instal·lació, etc.

CORRECTA SITUACIó FíSICA DELS EQUIPS

A distingir entre dues parts de l'equip: la formada pel processador central, discos i altres elements a centralitzar, i els terminals distribuïts tals com pantalles, impressores, etc.

L'emplaçament de la unitat central i dels discos és el que més atenció necessita, considerant que l'operativa de tot el sistema en depèn.

La millor distribució és aquella en què la unitat central (processador) i els discos es troben aïllats dels usuaris, recomanant que una pantalla, la consola, es trobi prop del processador.

S'els ha de donar protecció contra cops, pols, llum solar directa, sabotatges, brutícia, incendis, inundacions, etc.

En parlem en detall tot seguit.

Jaume Viñas, "KEEPWARE", 1995

CONSIDERACIONS PER ALS EQUIPS PERIFèRICS

Entendem aquí per equips perifèrics els no centralitzats, és a dir, els que no hem considerat "centrals" i que situem en la sala de l'ordinador i tampoc les impressores "especials", que també hem aïllat. Es tracta llavors, fonamentalment, de les terminals i de les impressores "normals".

Més en davant es mencionen les condicions d'instal.lació elèctrica i ambientals per als equips perifèrics.

Només subratllar aquí la importància, major de la que sembla, de l'entorn de treball d'aquests equips quant a la seva ergonomia.

- Mobiliari adequat. Hi ha en el mercat una bona varietat de cadires anatòmiques i taules dissenyades a l'efecte. La comoditat en el treball influeix directament en el rendiment i en la salut. També hi ha mobles especials per a PCs, impressores amb els seus volums de paper, alimentadors multi-formulari, faristols, etc.

  La taula ha de ser de color clar i no brillant. L'alçada entre 60 i 80 cm. Ha de tenir prou espai per a tots els instruments de treball i deixar lloc per a posar les cames còmodament.

  La cadira ha de tenir rodes, alçada i respatller regulables i seient flexible de teixit transpirable.

- Ergonomia dels terminals: teclat separat, pantalla molt orientable, filtre anti-reflexos o/i anti-estàtics connectat a terra, braç articulat, color verd o sèpia, orientació (soroll i flux del ventilador incorporat).

  La pantalla serà d'alçada regulable, giratòria i amb inclinació vertical ajustable. Contrast positiu: més clars els caràcters que el fons).

- Condicions de llum, ventilació, il.luminació, etc.

  Les fonts de llum estaran sobre la taula i tindran difusors. La pantalla estarà en posició perpendicular a les finestres.

  Temperatura mantinguda entre 19º i 24º. La humitat, entre 40 i 70% El soroll, per sota de 55 dB.

Per últim, recordar que el problema que apareix més sovint en la localització dels equips perifèrics està en el cables d'alimentació i dades a que estan connectats.

Aquets cables no han de constituir una barrera al pas de persones, amb el corresponent perill d'estirades accidentals, etc. sinó que han d'estar conduits en canals fixos al terra, o, molt millor, des de dalt, per un fals sostre.

Jaume Viñas, "KEEPWARE", 1995

EMPLAÇAMENT DEL PROCESSADOR I ELS DISCOS

Es requereix una ubicació neta, amb temperatura controlada i amb tràfic limitat de persones.

El control de la humitat relativa de l'aire pot en determinades ubicacions ser necessari i en tots els casos recomanable.

Es tindrà cura de no cobrir les ranures de ventilació dels equips.

Els petits animals paràsits, com ara insectes o rosegadors, són veritables perills per als equips electrònics i, encara més, per als cablats.

En la ubicació de l'equip s'ha preveure les possibles ampliacions de les unitats centralitzables.

Tenint en compte que des del processador és necessari estendre cables als perifèrics distribuïbles, ha de pensar-se en una ubicació que permeti fàcilment aquest treball.

L'alimentació de l'equip ha de ser una escomesa des del comptador i per l'ús exclusiu del mateix.

Els discos han d'estar lluny de les màquines de procés de paper (impressores, talladores, destructores, separadores) i fora de passadissos.

Es aconsellable disposar d'una connexió telefònica junt a la CPU i la consola.

SALA DE L'ORDINADOR

Convé situar els elements centrals de l'ordinador en una sala ad-hoc, acuradament escollida, preparada i vigilada.

Aquells elements que necessiten ser posats fora de servei amb certa freqüència per al seu manteniment, com ara, grups de continuïtat, condicionadors d'aire, extintors, etc., haurien d'estar duplicats.

Ja s'ha indicat quins són els elements "centrals" que han de ser situats en la sala de l'ordinador.

Hi ha dos aspectes de la sala de l'ordinador que seria bo emfasitzar.

En quant als accessos:

No hi ha d'haver altra cosa que sòlida paret donant a l'exterior de l'edifici.

Cap accés (porta, finestra, etc.) ha de poder-se obrir des de fora de la sala, tret que es faci servir clau.

Ha d'haver a la sala algun accés prou gran com per permetre el pas de les màquines. Aquest accés disposarà de rampa si hi ha desnivell entre la sala d'ordinador i el seu exterior o si en la sala hi ha instal·lat doble sòl.

Han de ser reduïts al mínim el número d'accessos físics, el número de vegades que s'obrin i el temps total en que romanen oberts. Si tot i així es poden produir problemes ambientals o si les diferències ambientals són grans entre la sala i el seu exterior haurà d'instal·lar-se una "resclosa d'aire" o doble porta.

En tot cas es disposarà d'una sortida d'emergència que no es pugui bloquejar. S'aconsella l'ús de barra anti-pànic per a aquesta sortida, que pot coincidir amb l'accés principal.

En quant a la configuració de la sala, a més a més dels elements hardware mencionats i de cert petit material, a la sala de l'ordinador hi ha d'haver:

Prestatges i/o armaris per a aquest petit material i per al material de neteja i armaris especials per a suports magnètics auxiliars i per a llistats en paper continu.

Espai adequat per als suports magnètics (cintes, discos, diskettes), tant pel que fa a les condicions per als suports (camps magnètics, pols, etc.) com pel que fa a l'operador (fàcil accés, etc.).

Termòmetre de màxima i mínima i higròmetre o psicròmetre, situats sobre la paret amb condicions ambientals més desfavorables per a l'equip. L'ús d'un psicròmetre en lloc d'un higròmetre té l'avantatge de major precisió i permet disposar de la interessant dada de temperatura de bulb humit, però l'inconvenient del seu major entreteniment (porta un petit dipòsit d'aigua que ha de ser ple) i haurà de ser bescanviat quan es dipositi cals en el camí del dipòsit al termòmetre humit.

Extintors per a focs tipus E.

Retolació àmplia quant a instruccions d'operació i manteniment i quant a indicacions de tot tipus, identificació

d'equips i materials i prohibicions (fumar, menjar, fer pols, etc.).

Plànols-guia de les instal.lacions, esquemes dels quadres elèctrics i xarxes de cables de dades i alimentació.

Manual i pla d'explotació. Pla de seguretat.

Llum d'emergència.

Donem a continuació una relació de possibles petits materials convenients en un sistema informàtic i que, per tant, poden trobar-se fàcilment en una sala d'ordinador.

Allargadors elèctrics, aspiradora, ampolla per aigua/líquids (humidificador de presa de terra elèctrica, omplir psicròmetre), ventosa per al doble sòl, retoladors, llapis, substància deshumidificadora, materials de neteja "fina", drap de neteja, raspall, bates per als operadors, joc de tornavisos, caixa de transport de suports magnètics (disquets, cartridgos), adaptadors dels diversos tipus d'endolls, escombra, escala, recanvis de filtres per al condicionador, aparell humidificador o deshumidificador, eines per al tractament de cables i connectors, multímetre, soldador amb el seu suport i joc de puntes, alicates, pinces, joc de claus, etc.

Jaume Viñas, "KEEPWARE", 1995

EMPLAÇAMENT DELS TERMINALS

Es requereix:

* Disposar d'una xarxa d'alimentació que tingui el mateix origen que la que alimenta el processador.
* Disposar d'una bona presa de terra. La presa de terra ha de ser única per a un mateix ordinador (incloent perifèrics), excepte els terminals remots connectats via modem.
* No han d'existir diferències de potencial entre les fases, neutre i terra que alimenta els perifèrics i les que alimenten al processador.

Es aconsellable usar per als perifèrics un tipus d'endoll diferent de l'utilitzat per a la resta d'endolls de l'edifici, per garantir físicament l'exclusivitat de les línies d'alimentació.

Si perifèrics del mateix sistema informàtic (mateixa CPU) són sostinguts per diferents grups de continuïtat (casos d'edificis separats, per exemple) és convenient que aquest grups de continuïtat siguin sincronitzats en fase entre sí.

Si hi ha perifèrics no sostinguts per cap grup de continuïtat el/s grup/s que existeixin han d'estar sincronitzats en fase amb la xarxa.

En cap cas es posaran impressores a prop de les unitats de disc i cintes magnètiques, ja que generen partícules de paper altament abrasives.

Si els terminals són unitats d'arxiu en disquet, o unitats de cinta magnètica, la neteja ambiental és necessària.

En qualsevol cas i com que els terminals normalment es distribueixen per un medi d'oficina, és necessari que es minimitzin els efectes de l'electricitat estàtica.

Els equips perifèrics d'avui en dia no requereixen més condicions de les que es troben habitualment en qualsevol oficina i el que cal tenir en compte respecte d'ells és l'ergonomia.

ALTRES DEPENDèNCIES INFORMàTIQUES

L'única dependència exclusivament informàtica imprescindible és la sala de l'ordinador.

De totes maneres, i a mesura que el sistema és més gran, apareix la conveniència de disposar del següents espais dedicats:

Magatzem. Per als fungibles de tot tipus, especialment paper, per a material divers i inclús com a traster. El magatzem ha de ser ventilat, ser protegit contra sabotatges (imaginem que fàcil resulta provocar un incendi important en un magatzem de paper) i disposar d'alarma de foc amb sensors de fum i termo-velocimètric (de velocitat de canvi de la temperatura) per als materials que cremin sense fum (per exemple, certs tipus de paper).

Sala de la/es impressora/es principal/s o especial/s. Si el sistema disposa d'alguna impressora que, per les seves característiques (velocitat, tipus d'alimentació, "font", etc.), hagi de ser considerada des d'un punt de vista funcional com "especial", el seu ús haurà de restringir-se als operadors i ser "tancada" en alguna dependència ad-hoc.

Un altre bona raó per aïllar les impressores especials és el conjunt de condicions ambientals en que solen treballar: soroll considerable, necessitat de ventilació, conveniència d'alarmes de foc com en el magatzem de paper.

No s'ha de caure en l'error de situar-les en la sala de l'ordinador: recordem que un dels principals enemics dels elements centrals de l'ordinador, altres màquines i dels suports magnètics és la pols, en la qual producció i difusió les impressores són especialistes.

Tampoc s'aconsella situar impressores ni cap altra tipus de màquina en el magatzem, donat el risc d'incendi per l'elevació de temperatura i pels possibles malfuncionaments. Les impressores han de situar-se malgrat tot, a prop de magatzem i dels punts de consum final, independentment d'on estigui situada la sala de l'ordinador.

Com que, molt sovint, el compliment de tots aquests requeriments de situació pot ser complex i inclús anti-funcional (pensem que hem configurat el magatzem a prop dels punts de consum final, per exemple), es pot pensar en disposar d'un magatzem secundari o de consum immediat.

El control de les existències de fungibles i les previsions del seu consum, feines de l'operador, sempre necessàries, garanteixen que el pas del magatzem principal al secundari es farà a temps.

El local de la impressora fàcilment pot ser el millor per a: talladores, separadores, destructores, enquadernadores, guillotines, etc.

Sense ànim de parlar aquí d'altres possibles dependències com oficines, despatxos, sala de demostracions, cursets o

reunions i inclús sala "pool" de terminals (avui en desús), l'estudi de les quals escapa a l'objecte d'aquesta obra, si que cal emfasitzar certs temes respecte de la consola.

Encara que es tracti quasi sempre d'un terminal més, la consola té unes missions fonamentals que la fan especial: en les operacions més importants, en l'engegada i en l'aturada del sistema, en l'operació del sistema en condicions sense usuaris (manteniment o reparació d'avaries) i altres casos, la consola és el punt clau de control del sistema.

Per això, han de tenir-se en compte algunes precaucions en la seva localització:

* El més a prop possible de la sala de l'ordinador, o fins i tot dins si només serà utilitzat com a consola (la qual cosa és convenient). A vegades hi ha requeriments tècnics de distància màxima i mínima fins i tot.

* Llum d'emergència per a l'operació d'urgència en cas de falta de tensió en la xarxa.

* Manual d'explotació a la vista.

Jaume Viñas, "KEEPWARE", 1995

SòL I SOSTRE

SòL RECOMANABLE

El sòl ha de ser una superfície plana i estable.
Els requeriments de sòl estan relacionats amb l'estabilitat física i l'electricitat estàtica generada.

El sòl emprat no ha de produir vibracions, ha de ser fàcil de netejar i finalment no ha de ser productor d'electricitat estàtica.
Els sols encatifats o amb moqueta conserven la brutícia i són productors d'electricitat estàtica.
Si el sòl ja té moqueta, caldrà superposar-hi catifes anti-estàtiques connectades a la presa de terra. La superfície d'aquestes catifes ha de ser suficient, de forma que l'operador que accedeixi a l'equip descarregui la seva electricitat estàtica, mitjançant la catifa, abans de tocar l'equip.

El sòl i les parets han de ser de fàcil neteja. Es aconsellable no escombrar-los ja que s'aixeca pols. Millor fregar-los.
En la sala de l'ordinador hi ha d'haver un desguàs a nivell del sòl veritable.

DOBLE SòL I DOBLE SOSTRE

En algunes instal.lacions amb bastants equips centralitzats, el número de cables d'interconnexió i de connexió a xarxa pot ser tan alt que sigui aconsellable el disposar de doble sòl.
El doble sòl facilita, minimitza i protegeix l'estesa de cables i la refrigeració de l'equip a nivell de terra.
A vegades l'aire refrigerat entra pel fals sostre i surt per fals sòl o viceversa.

Cert tipus de doble sòl faciliten l'apantallament de l'equip. Són de fusta laminada recoberta per sota amb xapa conductora. Totes les llosetes es connecten elèctricament entre si i amb la presa de terra.

El doble sòl ha de tenir una resistència mínima i suportar certes càrregues puntuals.
No haurà de produir vibracions.
Normalment s'aixeca sobre el sòl veritable un màxim de 30 cm i un mínim de 11 cm.
Els materials per a dobles sòls i sostres ha de ser incombustible.
Cal tenir sovint una ventosa especial per poder aixecar les llosetes.

Jaume Viñas, "KEEPWARE", 1995

INSTAL·LACIó ELèCTRICA

ESCOMESA I DISTRIBUCIó D'ENERGIA

Abans de tot és necessari verificar que l'escomesa i el comptador de que es disposa suportaran la càrrega de l'equip a instal·lar, en cas contrari s'ha de contractar la potència necessària. No oblidem tenir present les futures ampliacions de l'actual equip.

Es aconsellable contractar a un electricista qualificat perquè revisi la instal·lació elèctrica abans de procedir a la instal·lació del sistema.

La majoria dels equips requereixen una tensió monofàsica de 230 Volts CA/50Hz. (fase, neutre i terra).

La instal·lació elèctrica haurà de ser exclusiva, estable i lliure de soroll elèctric.

El control de distribució (denominat sovint CGP per "Quadre General de Protecció" en castellà) haurà de ser de fàcil accés per a l'operador del sistema i estar ben senyalitzat. Ha de disposar d'un interruptor general i d'un interruptor automàtic (ICPM) per a cada branca de distribució. Els equips que utilitzin unitats de disc independents hauran de disposar d'un interruptor per a cada unitat de disc.

Els diferencials de protecció hauran de ser de 300 mA (0.3A). Per a la protecció de les persones són més interessants els de 30 mA i certs equips ho accepten. Perquè els magneto-tèrmics de les unitats de disc no es disparin durant l'engegada hauran de ser de corba lenta (G). En cas d'equips amb motors (discos) el consum d'engegada és unes quantes vegades (3 ó 4) superior al nominal durant una fracció de segon.

Les seccions de fil i el tipus d'endoll (Metropoli, CETAC, etc.) a utilitzar vindran determinats pels consums màxims especificats, corresponents a l'engegada de l'equip.

Per evitar interferències no es podran connectar altres aparells en la línia elèctrica utilitzada per l'equip.

La instal·lació elèctrica haurà de ser exclusiva, estable i lliure de soroll elèctric.

REQUERIMENTS ELÈCTRICS

La tensió entre fase i neutre (230 v ca) permet una tolerància de +/- 10%. Es recomana la utilització de grups d'alimentació ininterrompuda que asseguren la continuïtat del funcionament fins la desconnexió lògica dels elements vitals (processador, discos, consola). Aquests equips han de tenir commutador estàtic per evitar els temps de commutació, sincronització de fase amb la xarxa, i potència suficient per permetre la posada en marxa dels discos (o bé commutació de xarxa automàtica -"bypass"-).

Hi dediquem un capítol posteriorment en aquesta obra.

En cas de que sigui difícil suportar tots els equips amb UPS's, és convenient utilitzar per als discos (la CPU té preferència per l'UPS sobre qualsevol altre equip) un relé de rearmament manual, per evitar transitoris. Aquest relé manté la connexió mentre hi ha tensió en la xarxa, però la desconnecta a la primera interrupció de xarxa i ja no la torna a establir encara que la xarxa es restableixi.

En el cas d'equips instal.lats en edificis separats, amb diferents escomeses, no hauria d'haver diferència de tensió entre les fases R, S i T d'ambdues.

Jaume Viñas, "KEEPWARE", 1995

PRESA DE TERRA

La presa de terra és necessària per al bon funcionament de l'equip i està connectada a totes les parts metàl.liques (xassís) de les màquines. Es recomanable que sigui única per a tot el sistema informàtic i exclusiva per a ell.

Tots els elements d'un equip estan proveïts d'un cable per a la presa de terra. En el cas que existeixi un problema d'aïllament intern, aquesta connexió limitarà a un màxim la tensió al tacte en la superfície de la màquina.

Hauran de considerar-se el següent:

* S'utilitzarà presa de terra exclusiva per a l'ordinador (de l'ordre de 10 ohm). La presa de terra general d'un edifici no és recomanable per a cap ordinador.
* Utilitzar una única presa de terra. Si hi ha diverses piquetes, aquestes hauran d'unir-se entre si utilitzant cable de secció suficient.
* Utilitzar solament una connexió de presa de terra en cada perifèric, ja que del contrari, es poden produir bucles de corrent a través de les masses.
+ Les canalitzacions d'aigua no han de ser utilitzades com presa de terra.
* Les malles no poden tocar cap part metàl.lica de l'edifici.
* No desconnectar el cable de terra de les clavilles.
* Controlar sovint la presa de terra, i "regar-la" de forma periòdica. Un col.lector de pluvials fins el punt de presa de terra facilitarà aquesta labor.

Jaume Viñas, "KEEPWARE", 1995

ALIMENTACIó ELèCTRICA

SOROLL ELèCTRIC

La línia d'alimentació dels equips ha d'estar lliure d'interferències originades per equips externs. Aquestes interferències poder produir-se fins i tot estant connectat en línies elèctriques diferents. Són productors de soroll elèctric: transformadors, fotocopiadores, aspiradores, ascensors, tubs fluorescents, soldadors d'arc, etc.

Els equips solen disposar d'apantallament i filtres de xarxa, útils per a protegir-los de la destrucció de hardware, que només seran efectives si existeix una bona presa de terra. Aquestes proteccions seran insuficients en els casos de radiacions intenses d'alta freqüència.

Per a contraposar els efectes de les interferències externes existeixen diverses solucions:

* Actuació sobre la causa que l'origina. És a dir: filtrar, reparar, substituir o allunyar l'aparell causador del soroll.
* Instal.lar transformador separador i/o filtres de xarxa externs.
* Utilitzar estabilitzador de tensió.
* Utilitzar conductor elèctric de més secció.

Un UPS és la solució definitiva.
Totes aquestes solucions impliquen disposar d'una bona presa de terra.

Jaume Viñas, "KEEPWARE", 1995

QUALITAT EN EL SUBMINISTRAMENT

Les línies de distribució elèctrica estan subjectes, freqüentment, a una sèrie de pertorbacions, baixades, pics de tensió, microtalls, etc., que encara que poden no afectar al normal funcionament d'equips elèctrics, si que solen provocar greus anomalies, errors i alteracions en els discos, pèrdues d'informació...

Aquestes anomalies s'agreugen si es produeixen talls en el subministrament elèctric, ja que interrompen els processos en execució i llavors és necessari, normalment, realitzar una sèrie d'operacions de recuperació de dades.

La pèrdua de la disponibilitat del sistema és la nefasta conseqüència d'una energia no fiable.

L'energia elèctrica ha estat, des de sempre, la baula més dèbil de qualsevol sistema d'informació.

Els talls prolongats d'energia, les sobretensions sobtades o les caigudes de tensió han estat sempre presents de forma inevitable.

I el preu, en productivitat i integritat perdudes, sempre ha estat alt. Fins i tot una falla en el subministrament en només 15 milisegons pot inhabilitar un sistema.

En el que segueix s'ofereix una descripció de les alteracions que poden sufrir l'alimentació elèctrica de xarxa, amb les seves conseqüències i les possibles solucions a aquells problemes.

* Sorolls i impulsos en mode diferencial.

Es tracta de desviacions erràtiques de l'ona de tensió entre conductors actius.

Mal funcionament en càrregues amb circuits electrònics, especialment informàtics. Són aleatoris i poden passar inadvertits, cosa que fa més greu el problema. Els impulsos (sorolls alts i curts) elevats poden destruir els equips.

Pot ser solucionat amb transformador d'ultra-aïllament.

* Sorolls i impulsos en mode comú.

Es tracta de desviacions erràtiques de l'ona de tensió entre conductor actiu i terra.

Idèntics problemes al cas diferencial. Els impulsos elevats poden ocasionar descàrregues als usuaris si es destrueixen els aïllants.

Pot ser solucionat amb transformador d'ultra-aïllament.

* Variacions lentes.

Canvis de tensió produïts entre conductors actius, en més de 10 s.

Perill de sobrepassar els límits de tensió d'alimentació.

Pot ser solucionat amb estabilitzador de preses.

* Variacions ràpides.

Canvis de tensió produïts entre conductors actius, en menys de 10 s.

Perill de sobrepassar els límits de tensió d'alimentació.

Pot ser solucionat amb estabilitzador de preses, excepte per a variacions de temps inferiors a 0,1 s.

* Microtalls.

Anul·lació de la tensió entre conductors actius, durant un temps inferior a 2 ms.

Errors en equips informàtics. Alguns ordinadors es desconnecten.

Pot ser solucionats amb estabilitzadors de resolució contínua.

* Talls llargs.

Anul·lació de la tensió entre conductors actius, durant un temps superior a 2 ms.

Errors en equips informàtics. Alguns ordinadors es desconnecten.

Pot ser solucionats només amb UPS.

* Distorsió.

Deformació permanent en l'ona de tensió entre conductors actius.

Normalment no hi ha problemes fins arribar al 5%.

Pot ser solucionat només amb UPS.

Hom afirma que, en la pràctica es venen a donar unes 150 d'aquestes pertorbacions cada any, de mitjana.

Tractant-se els ordinadors de màquines molt complexes,

totes aquestes pertorbacions poden tenir dos efectes simultanis la conjunció dels quals encara augmenta el problema:

1 d'una part, la pertorbació prou ser prou llarga com per afectar realment alguna cosa, el contingut de la memòria volàtil per exemple, però

2 alhora pot ser prou curta com per no ser advertida per la persona usuària, amb la qual cosa tenim un problema i ni tan sols ho sabem. Doble problema.

En conclusió, totes les pertorbacions i incidències en l'alimentació queden superades amb l'ús d'un UPS (Sistema d'Alimentació Ininterrompuda o Grup de Continuïtat Elèctrica).

Jaume Viñas, "KEEPWARE", 1995

GRUPS DE CONTINUïTAT ELèCTRICA

També denominats UPS (per "Uninterrupted Power System") o SAI (per Sistema d'Alimentació Ininterrompuda).

Com s'ha anunciat en un capítol anterior, són la millor, per no dir única, garantia d'una alimentació elèctrica de qualitat per als dispositius electrònics.

DESCRIPCIÓ I FUNCIONAMENT

Pel seu funcionament, podem classificar els UPS en dues classes:

* ON LINE: un rectificador (aparell electrònic que converteix Corrent Altern en Corrent Continu) alimenta unes bateries permanentment, les quals bateries (acumuladors normals, com les bateries de cotxe), també permanentment alimenten un ondulador (aparell electrònic que converteix Corrent Continu en Corrent Altern).

* OFF LINE: l'ondulador és alimentat normalment (en presència de tensió dins marges normals a la xarxa de subministrament) des del rectificador, mentre que les bateries romanen carregades sense intervenir fins que el rectificador no pot proporcionar alimentació en fallar el subministrament exterior. Llavors, automàticament, seran les bateries que alimentaran l'ondulador fins tornar a la normalitat (o final d'autonomia per esgotament de la càrrega de les bateries, està clar).

Els del segon tipus tenen, respecte dels del primer tipus, l'inconvenient que cal una commutació, que podria ser percebuda com un microtall pels equips alimentats a través de l'UPS.

Els avenços tecnològics en els UPS han estat importants i han afectat tots els seus components. El més afectat ha estat l'ondulador, que avui es basa en modulació d'amplada de polsos (Pulse Width Modulation).

Una altra característica de commutació dels UPSs és l'anomenat "by-pass". Quan s'activa el by-pass, l'UPS es comporta com un estabilitzador, amb els desavantatges que hem vist. Això succeeix en el cas de mal funcionament del propi UPS o de la càrrega elèctrica que aguanta (curt-circuit o sobrecàrrega).

Aquesta característica té un aspecte positiu o necessari: les unitats amb motors elèctrics (discos, per exemple) generen un pic de consum durant un molt breu període en la seva engegada. El by-pass permet que aquests equips puguin estar suportats per l'UPS sense danyar-lo en aquest període.

La freqüència de la línia de sortida de l'UPS es manté en fase amb la de la xarxa de subministrament, si aquesta està dins d'uns marges al voltant de la nominal.

Per a configuracions amb redundància, per a seguretat o en

cas de càrregues de gran consum, és possible de connectar diversos UPSs en paral.lel, sincronitzant-los entre si en fase.

AUTONOMIA

Cada model d'UPS disposa, entre la seva documentació tècnica, d'unes corbes que permeten determinar el temps d'autonomia en funció de la potència que l'equip ha de subministrar.

Hi ha també una fórmula aproximada que diu que el temps d'autonomia és, en hores, el 30% de la fracció:

(Cnb (Ah) * Vb (V))/(Pr (W) + 0.1 * Pn (W)),

on

Cnb és la capacitat nominal de les bateries,
Vb és la tensió nominal de les bateries,
Pr és la potència requerida a l'UPS, i
Pn és la potència nominal (màxima) de l'UPS.

COMANDAMENT

Els UPSs disposen d'un quadre de comandament, força senzill, que resulta sinòptic de l'estat del seu funcionament.

Un indicador de "sincronització" ens fa saber quan la sortida està sincronitzada en fase amb l'entrada.
Un indicador de "bloqueig" o "by-pass" ens fa saber quan s'ha activat aquesta commutació.
Un indicador de "càrrega" ens fa saber si des del rectificador s'està proporcionant energia a les bateries perquè aquestes no estan al 100% de la seva càrrega.
Un indicador "descàrrega" ens fa saber que no arriba energia a l'UPS (tall de subministrament a la xarxa), i, per tant, les bateries s'estan descarregant perquè proporcionen energia a l'ondulador.
Un indicador de "flotació" ens fa saber que les bateries estan al 100% de la seva capacitat nominal i, per tant, el rectificador només alimenta l'ondulador.

També hi pot haver indicadors del nivell de consum, o de la qualitat de l'entrada o/i de la sortida.
Aquest quadre de comandament pot ser remot.

Molts UPSs proporcionen sortida dels esmentats indicadors en interfície normalitzada d'informàtica, la qual cosa permet que els processadors alimentats per l'UPS o altres puguin tenir-ho en compte i auto-desconnectar-se o engegar còpies de seguretat automàtiques, etc.
Algun sistema operatiu de xarxa d'ordinadors porta, ja de base, el lligam amb tals indicadors d'UPSs, la qual cosa permet d'aprofitar aquests indicadors de forma molt segura i eficient.

Existeixen en el mercat bons sistemes "ad-hoc" de lligam del tipus esmentat i que també permeten fer anàlisis tant de les característiques de qualitat elèctrica de la xarxa com de les prestacions de l'UPS.

Alguns UPSs avançats porten aquestes facilitats incorporades i llavors també es possibiliten actuacions remotes sobre el propi UPS com ara servei de diagnòstic remot per línia telefònica. N'existeixen que monitoritzen permanentment la qualitat de la sortida i la situació d'entorn (consum, xarxa) i en donen una comunicació ja elaborada de forma programable.

INSTAL·LACIÓ I MANTENIMENT

No presenta cap dificultat, però, com en qualsevol màquina elèctrica, convé seguir les instruccions del fabricant.

Es recomana que la ubicació sigui espaiosa, airejada i de fàcil accés.

Per evitar caigudes de tensió i per facilitar la instal·lació convé que l'UPS quedi el més a prop possible de la càrrega elèctrica que ha d'aguantar.

Cada tres mesos aproximadament convé fer les següents operacions de comprovació:

1 Desconnectar la xarxa durant uns minuts i mirar si, un cop restablerta, el rectificador aconsegueix recarregar les bateries.

2 Comprovar, amb els instrument adequats, que la forma d'ona i els paràmetres de la tensió de sortida (ondulador) són els correctes.

3 Fer una descàrrega profunda tot vigilant la tensió de les bateries, per comprovar-ne el bon estat.

Si l'UPS roman una llarga temporada sense prestar servei cal guardar-lo amb les bateries ben carregades.

Normalment les bateries són considerades fora de garantia o de contracte de manteniment.

Jaume Viñas, "KEEPWARE", 1995

CONSIDERACIONS AMBIENTALS

Les consideracions ambientals (ventilació, climatització) han de ser avaluades i controlades abans de rebre el sistema.

Totes les consideracions ambientals requerides per l'equip, hauran de tenir-se presents també per a l'àrea d'emmagatzemament: respectar-se les consideracions referents a la temperatura, la humitat, l'electricitat estàtica i la netedat.

Hi ha cinc factors que determinen quin és l'ambient en un recinte:

1 Temperatura, que es mesura amb el termòmetre (de bulb sec) i per controlar la qual cal calefacció o refrigeració,
2 Humitat, que es mesura amb el termòmetre de bulb humit per diferència amb la lectura de la temperatura i per controlar la qual cal humidificació o deshumidificació,
3 Velocitat de l'aire, per controlar la qual cal incidir en la seva circulació,
4 Neteja, per controlar la qual l'aire es filtra, i
5 Ventilació, per controlar la qual s'introdueix aire de l'exterior.

La temperatura és el principal factor ambiental a tenir en compte. L'operació fora de marges és molt perillosa:

* En el marge inferior ocasiona la impossibilitat de càrrega del sistema operatiu fins que la temperatura interior de l'equip arriba als règims de treball.
* En el marge superior pot impedir la recuperació de la informació enregistrada en els discos, com també un increment en el número d'avaries.

El control de la temperatura l'obtindrem amb els condicionadors d'aire mitjançant els seus elements: centrals frigorífica i calorífica i sistema impulsor d'aire.

El treball en ambient molt humit és igualment perillós per als camps magnètics en el disc, com també per al funcionament de la tracció de paper en les impressores.

Si pel contrari treballem en un ambient massa sec, provocarem que un revestiment d'òxid es dipositi en els caps dels discos i cintes, cosa que originarà errors i pèrdues d'informació.

A més, haurem de tenir present que en ambients de baixa humitat s'incrementa el potencial de les descàrregues electrostàtiques. Les esmentades descàrregues poden destruir la informació continguda en memòria i en els suports magnètics. Una bona presa de terra disminueix aquest efecte, però no el suprimeix completament. Cal tenir en compte els materials usats: moquetes, etc.

En àrees molt seques pot ser necessària la instal·lació d'humidificadors, com també la utilització de deshumidificadors

en zones molt humides.

Existeix en el mercat gran varietat d'aquests dispositius, des de molt senzills fins a molt avançats. N'hi ha, fàcilment adquiribles que eliminen entre 10 i 20 litres diaris i poden mantenir la humitat com es desitgi, entre el 40% i el 90%.

Jaume Viñas, "KEEPWARE", 1995

CÀLCUL DE LA POTèNCIA DE CLIMATITZACIó

Les necessitats de refrigeració es poden calcular amb la fórmula següent:

T = H + W + (200 * P) + (0.86 * R)

on

T: dissipació total a eliminar amb la refrigeració, en kcal/hr,

H: kcal/hr necessàries per a mantenir la sala a la temperatura adequada, quan està desocupada però il.luminada,

W: dissipació total dels equips d'ordinador, en kcal/hr (si ve donada en Watt, multiplicar per 0.86; si ve donada en British Thermal Unit, multiplicar per 252),

P: nombre de persones que usualment estaran a la sala,

R: potència, en Watt, de la resta de màquines presents a la sala.

La magnitud resultant del càlcul (T) serà la principal dada per iniciar el disseny o tria del condicionador.

Les magnituds de W i R es poden obtenir dels fulls de característiques tècniques amb els manuals.

El valor de P dependrà de l'explotació planejada.

El valor de H és força difícil de calcular. Sovint es recorre a mètodes empírics, experimentals, de determinació. Es a dir que més aviat es mesura que no pas es calcula.

Si el volguéssim calcular el primer pas seria determinar quines esperem que siguin les condicions exteriors límit, tant a l'hivern com a l'estiu. Per a això fem servir informació meteorològica de la zona.

Haurem de tenir en compte l'orientació de la sala/edifici per veure com influeix la radiació solar directa. Està clar que, en calcular el cas més fred, a l'hivern, s'ha de fer considerant radiació solar nul.la.

Ens caldria, com a segon pas, conèixer com influeix la condició constructiva de l'edifici. Respecte d'això hi ha força literatura. Sempre es tractarà d'arribar a determinar la velocitat de pas del calor a través de parets, finestres, etc. és a dir el coeficient de transmissió característic.

A l'hora de buscar dades en la bibliografia és molt útil distingir entre dos tipus de calor present:

* Calor sensible: el guanyat per transmissió a través de parets, finestres, etc., el guanyat per radiació i l'aportat per les persones, i

* Calor latent: l'aportat per la humitat que introdueixen les persones. El calor latent depèn molt de l'activitat de les persones, al contrari del calor

sensible.

Jaume Viñas, "KEEPWARE", 1995

NETEJA I CONTAMINACIó

S'ha de procurar que no existeixi pols ni brutícia en les màquines. Tampoc no s'han d'instal·lar en zones polsoses o on hi pugui haver gasos corrosius o materials abrasius. A les zones sensibles ha d'estar prohibit fumar, menjar i beure.

Els ambients contaminats amb partícules de brutícia o pols, fins i tot el provocat pels fumadors, poden originar seriosos problemes en l'operació: desgast prematur en peces mecanitzades, curt-circuits en components electrònics, etc.

Les unitats d'emmagatzemament en suport magnètic (discos, cintes) són especialment sensibles perquè, a més, s'hi poden arribar a destruir els esmentats suports físics en danyar-se el material magnètic.

Normalment, les partícules de pols poden ser controlades amb l'ús de filtres que ja acostumen a anar acoblats als sistemes d'aire condicionat.

Si aquests filtres són insuficients, se n'hi poden afegir dels electrostàtics.

El sòl ha de ser netejat regularment amb les següents recomanacions:

* Abans de netejar la zona, cal retirar tots els suports magnètics i guardar-los en lloc sec, fresc i lliure de camps magnètics o radioactius. A aquest respecte cal recordar que els detectors iònics de fum són lleugerament radioactius.
* Per netejar el terra cal fer servir elements lleugerament humits.
* Les aspiradores no han de portar boca metàl·lica, perquè podrien provocar curt-circuits.
* No s'ha de donar lluentor al terra amb discos de llana, perquè creen electricitat estàtica.

Jaume Viñas, "KEEPWARE", 1995

ELECTRICITAT ESTàTICA

L'electricitat estàtica, a més de ser perillosa per a l'usuari, pot fer funcionar malament el sistema informàtic.

En els suports magnètics d'informació, aquesta informació pot desaparèixer, quan entren els suports en contacte amb algun element carregat, les mans de l'operador per exemple.

En els equips electrònics es poden interrompre o corrompre els processos i destruir-se components integrats.

Depenent del calçat i del sòl una persona pot arribar a portar a sobre milers de Volts. Amb bastant menys es poden provocar danys als equips i ni tan sols ser advertits per la persona en qüestió.

Es recomana de no fer servir catifes ni moquetes, especialment les acríliques. En tot cas, haurien de ser homologadament anti-estàtiques i evitar llavors l'ús d'accessoris de plàstic o nylon.

Una bona solució és la de superposar catifes conductores i connectades a la pressa de terra, on també estaran connectats els xassís de les màquines.

També ajudarà el mantenir un cert grau d'humitat.

Les cadires i taules haurien de tenir tapisseria anti-estàtics i rodes metàl.liques.

Jaume Viñas, "KEEPWARE", 1995

CONDICIONADORS D'AIRE

Hem dit que els condicionadors consten de: centrals frigorífica i calorífica i sistema impulsor d'aire.

La unitat frigorífica, per referir-me a la més complexa, consta de: compressor, evaporador (on la substància refrigerant s'evapora, prenent calor de l'ambient), condensador (on l'esmentada substància es liqua), sistema d'expansió i controls (relés, termostats).

Un cop regulat, el condicionador manté la temperatura fixada.

Però el condicionador d'aire pot fer molt més que refrigerar l'ambient. Influeix en la humitat, filtre el pols i el fum. Fa circular l'aire i fins i tot pot introduir-ne de frec.

CONSELLS

Cal recordar que cap obstacle no ha d'entorpir la circulació d'aire en les entrades i sortides del condicionador. A més de reduir-ne l'eficàcia es podria espatllar. Respecte d'aquest punt cal recordar les persianes i cortines.

Tampoc no pot funcionar l'aparell sense el filtre. L'entrada de partícules el podria fer mal bé i, en tot cas, està clar que l'aire no seria filtrat.

Els moments just posteriors a l'engegada del condicionador són els més durs per a l'aparell. Seria bo i més eficient mantenir obertures tancades, sala a fosques, etc.

La sala a condicionar hauria d'estar en condicions òptimes d'ambient abans d'engegar-hi les màquines llur dissipació haurem d'absorbir. És a dir, a la temperatura de treball abans d'engegar els ordinadors.

Com tot aparell de refrigeració, després d'una aturada s'hauria d'esperar un parell de minuts abans de tornar-lo a engegar.

MANTENIMENT

L'únic manteniment (entreteniment) per part de l'usuari és la neteja del filtre. Sigui rentant-lo o substituïnt-lo, depenent del tipus usat. Es bàsic que el filtre estigui net. El contrari pot, en primer terme, treure-li eficàcia al condicionador i, a la llarga, avariar-lo.

L'època òptima per al manteniment per part d'un servei tècnic especialitzat (una revisió anual) és la primavera (en l'hemisferi nord, és clar) i hauria d'incloure, si més no:

* Canvi de filtres, si cal,
* Comprovació de pressions en el circuit refrigerador,
* Comprovació de fugues. Càrrega de refrigerador, si cal.
* Comprovació dels controls, comprovació de la part elèctrica i revisió general.

Jaume Viñas, "KEEPWARE", 1995

SISTEMES DE VIGILàNCIA, ALARMA I SEGUIMENT

El sistema serà capaç de captar determinats paràmetres externs i provocar senyal d'alarma quan la situació o el canvi de qualsevol dels paràmetres impliqui la intervenció de l'operador.

Es tracta de tenir una informació el més completa possible sobre l'estat actual de la instal·lació i processar-la de forma "intel·ligent" per provocar alarma només quan convingui i fer seguiment en tot cas.

Els paràmetres a controlar poden ser els següents, capturats tots ells per sensors, els quals, per seguretat, haurien d'estar en redundància (duplicats):

1. Presència o falta de tensió en diferents punts de la xarxa d'alimentació elèctrica, per detectar la posició dels interruptors i proteccions elèctriques.

2. Consum o no d'energia per part d'algunes de les màquines, per detectar si estan treballant o no.

3. Estat d'obertura de portes o finestres.

4. Situació per sobre o sota llindars ambientals en:

   * temperatura mínima,
   * temperatura màxima,
   * humitat mínima,
   * humitat màxima,
   * velocitat d'increment de la temperatura,
   * presència de fum,
   * presència de gasos,
   * detectors d'inundació,
   * altres sensors ambientals: vibracions, moviment.

5. Situació de funcionament d'altres màquines (que ho comuniquin via un port electrònic), com ara condicionador d'aire o grup de continuïtat elèctrica.

Per al posterior seguiment, és molt convenient que inclogui registre sobre paper de l'estat de les variables controlades cada un període de temps prefixat en la configuració de l'equip, indicant data i hora del registre.

Cada canvi d'estat de qualsevol paràmetre o combinació de paràmetres provocarà també el registre immediat sobre paper del nou estat amb indicació de data i hora.

L'equip serà autònom (alimentació pròpia independent de la xarxa elèctrica i dels paràmetres controlats) i amb bateries que el puguin suportar en funcionament algunes hores sense alimentació de xarxa.

La situació de l'equip ha de considerar que l'alarma no

pugui ser esborrada per algú que no n'investigarà immediatament la causa i que el registre fornit per al seguiment de les incidències no podrà ser robat o manipulat.

Amb tot això es constitueix un element de seguretat i dissuasió contra males intervencions humanes i serveix per prevenir futures avaries.

Totes les alarmes han de ser comunicades a qui "estigui de guàrdia", allà on es trobi de forma el més comprensible possible.

Es necessari completar aquestes alarmes amb instruccions completes i molt clares sobre què fer en cada cas i amb un llibre de registre d'incidències, acuradament i rigorosament actualitzat.

En dissenyar i implantar aquest sistema d'alarma, específic per al sistema informàtic, cal no oblidar l'interessant paper que ha de jugar el sistema d'alarma general de l'edifici, per reforçar-se, complementar-se o fins i tot duplicar-se en alguna cosa.

FOC

En un capítol posterior parlarem més en general de la seguretat informàtica i de les mesures sistemàtiques que podem prendre al respecte, tot i que està clar que pràcticament tota la raó de ser d'aquesta obra gira al voltant de la seguretat, entesa com a garantia de la disponibilitat. Això s'haurà notat fins aquí i seguirà essent així.

Ara dediquem un capítol al més temut dels riscos amb que s'enfronta el centre de processament de dades: l'incendi, amb totes les seves possibles, probables i variades conseqüències directes i indirectes.

El risc d'incendi s'ha de tenir en compte tan a la sala de l'ordinador com a les altres dependències on hi hagi: magatzems de paper, biblioteques de cintes magnètiques, grups de continuïtat elèctrica, sub-estacions transformadores, condicionadors d'aire, tallers de reparació, etc.

Vegem breument les fases per abordar aquest risc que, com en tot risc, són, d'acord amb la seva cronologia respecte del sinistre:

* Abans -> supressió (precaucions) o prevenció (normes),

* Durant -> detecció (alarmes) i contenció (extinció i aïllament),

* Després -> restauració (còpies i contractes) i transferència (assegurances).

Ja hem mencionat les normes aplicables (a la protecció de les persones) quan parlàvem de com dissenyar la instal.lació. Hi ha altres normes per a la protecció dels suports magnètics, en especial, per als armaris ignífugs.

No farem aquí cap recull de normes. No cau dins els objectius de l'obra.

També hem parlat dels sistemes d'alarma.

Posteriorment, en d'altres capítols, parlarem de les còpies de seguretat, dels contractes i de les assegurances, tot plegat que ens pot ajudar a minimitzar el dany, a fer-lo més suportable.

Centrem-nos aquí en el que queda:

- cóm procurar que no es declari cap incendi ?,
- com procurar que un incendi ja declarat no afecti el nostre sistema informàtic ?,
- com extingir un incendi que ja ens afecta?

PRECAUCIONS I AïLLAMENT

Hi ha molts més incendis que comencen fora del centre de càlcul que no pas dintre.

Perquè hi hagi foc cal tres elements presents: combustible (alguna cosa que cremi), temperatura i comburent (oxigen, sempre present a l'aire). Alguns autors contemplen un quart element: la ignició.

La primera precaució es basa en limitar la quantitat i el tipus de materials presents.

L'ideal seria disposar d'un local separat de l'edifici general.

El sòtan representa perills d'inundació, aigua en general i enfonsament.

S'han d'evitar les zones amb més risc de l'empresa.

De res no serveixen les nostres precaucions si en la resta de l'edifici el tema està oblidat.

La facilitat per a l'accés de màquines, etc. sovint és contrària al lloc de més protecció.

En els conductes que entrin a la sala de l'ordinador, per exemple d'aire, caldrà instal·lar tancaments i extintors, automàtics.

El fum i els gasos procedents d'un incendi llunyà poden causar grans danys per corrosió.

Les parets, sòl i sostre, han de ser residents al foc, durant un mínim d'una hora, des del sostre veritable i fins al sostre veritable.

En les parets anti-incendi s'han d'evitar els finestrals panoràmics i tota mena d'obertures.

Les portes talla-foc sovint no són tall-fum i cal posar-ne una de cada mena.

La porta talla-foc podria tancar-se automàticament, si hi ha garanties que ningú no quedarà atrapat.

EXTINCIó

TIPUS DE FOCS

A On cremen sòlids,
B On cremen líquids,
C On cremen gasos,
D On cremen metalls,
E On hi ha tensió elèctrica

MèTODES D'EXTINCIó

1 BCF (bromo-clorodi-fuor-metà),
2 BTM (bromo-clorotri-fuor-metà), més conegut com Halon,
3 CO2 (diòxid de carboni) o neu carbònica,
4 pols polivalent,
5 aspersors ("sprinklers") d'aigua.

Característiques:

El BCF desplaça el comburent. Es tòxic.

El CO2 baixa la temperatura. Es asfixiant i lent. No és massa bo per a focs tipus A.

El pols crea una capa separadora entre el combustible i el comburent. Espatlla els elements mecànics. No és massa bo per a focs tipus A.

Els aspersors espatllen els equips electrònics si estan en funcionament. Si no, els equips només requeriran ser rentats i aixugats. Es inadequat per a focs tipus B, C i E.

Comentaris resultants:

No han de fer-se servir extintors de pols sec tret de cas de gran foc que amenaci l'exterior de la sala.

Es convenient disposar d'un poderós extintor de pols sec prop la porta de la sala de l'ordinador, preferentment fora d'aquesta, per si es dóna el cas mencionat.

Jaume Viñas, "KEEPWARE", 1995

CONSIDERACIONS RESPECTE DELS SISTEMES D'EXTINCIó AUTOMàTICA

S'aconsella una instal.lació d'extintor halon automàtica que no ha d'inhibir l'alarma de foc.

S'ha de sospesar aquesta solució "automàtica" perquè pot esdevenir "excusa" per a no intervenir amb profunditat o zel suficients en cas d'alarma, per la qual cosa, si s'adopta, ha de complementar-se amb instruccions suficientment coercitives.

En qualsevol cas, sigui l'engegada manual, automàtica o combinació de totes dues (segurament el més aconsellable), la distribució de l'agent extintor una vegada disparat, és més efectiva a través d'un sistema fix de conductors, a l'estil dels de ventilació, que la que s'obté amb els extintors mòbils.

Els sistemes automàtics tenen partidaris i detractors. En tot cas, s'haurien de disparar només amb doble detecció, de forma proporcionada al foc i en sales desateses per personal.

Jaume Viñas, "KEEPWARE", 1995

MANTENIMENT DELS EXTINTORS

Els extintors estan regulats pel "Reglamento de Aparatos y Recipientes a Presión". Han de sotmetre's a una revisió anual i a un retimbrat per part dels organismes públics cada cinc anys.

L'empresa que fa el manteniment té responsabilitat sobre l'eficàcia dels extintors i ha d'estar assegurada.

La revisió anual sempre contempla:

* revisió de l'extintor en general,
* revisió particular dels mecanismes i accessoris,
* verificació de l'estat de l'agent extintor,
* verificació de la quantitat de l'agent extintor,
* lliurament del certificat de revisió homologada.

Per als extintors de pols sec, a més:

* comprovació de la pressió, si l'extintor és de pressió incorporada,
* canvi de l'ampolla de pressió, si l'extintor és de pressió externa,
* neteja dels orificis, pistola, mànega, etc.

CòPIES DE SEGURETAT

S'establirà un pla per fer periòdicament còpia en suport extraïble de tota la informació continguda en el sistema perquè cap accident lògic ni físic pugui destruir-la.
En aquest pla haurà de quedar prefixat què és el que es copia.

Destinats a aquesta finalitat hi haurà un cert número de jocs de suports (normalment magnètics o òptics) cadascun dels quals contindrà una còpia feta en moments diferents i serà sempre el suport amb una de les còpies més antigues el que serà regravat quan correspongui fer nova una còpia de seguretat.
Hi ha diverses cadències típiques que segueixen aquesta norma.

Per exemple la que consisteix en tenir:

un suport per als dilluns,
un per als dimarts,
un per als dimecres,
un per als dijous,
tres per als divendres i
un per a l'últim divendres de mes.

També hi ha diversos criteris quant a què es copia en cada cas.
Per exemple, les còpies diàries moltes vegades només es fan de la part més variable, pot ser només de les dades (no dels programes) o és una còpia "diferencial" o "incremental", versus unes còpies setmanals completes.

El mateix procediment de còpia (en el "Job Control Language" corresponent) pot incloure operacions per assegurar la qualitat de l'enregistrament, com ara la lectura o verificació immediata del que s'ha copiat.
En qualsevol cas és important verificar periòdicament la bondat de les còpies de seguretat que s'estan realitzant.

Existeixen paquets de software específics per a fer còpies de seguretat en gran diversitat d'entorns, que permeten tota mena de sofisticacions, com ara fer en batch (desasistidament) les còpies en moments prefixats o quan es donen unes certes circumstàncies.

Convé que existeixin també còpies de seguretat en períodes diferents: si les normals són diàries poden existir també les setmanals i les trimestrals.
Com hem vist abans això pot quedar garantit per la pròpia cadència de còpia, però si no és així, les podem fer independentment, fora de cadència.

També es copiarà a termini relaxat i immediatament després d'un canvi de versió, el software de sistema i d'aplicació.

Per últim, és d'interès tenir còpies per a arxiu, en suports que no seran reutilitzats, tant del software, encara que ja no es faci servir, com de les dades en moments singulars (tancaments d'exercici, per exemple).

Aquests jocs de suports seran guardats físicament en algun lloc segur i amb riscos distints dels de l'ordinador (en un altre edifici, per exemple).

La caixa forta ignífuga és la millor protecció. En el mercat existeix diversitat de models i tamanys d'aquests armaris, amb interior especialment dissenyat per albergar tota mena de suports magnètics de dades.

Una solució parcial és la caixa forta de lloguer en una institució bancària.

Aquesta solució és interessant per a les còpies de seguretat a llarg termini però les més recents (diàries) han de ser utilitzades d'immediat en cas de necessitat i el seu accés no pot quedar restringit a l'horari comercial bancari.

Jaume Viñas, "KEEPWARE", 1995

CONTRACTES DE MANTENIMENT I ASSISTèNCIA

Per a hardware, software, grup de continuïtat, condicionadors d'aire, extintors, sistema d'alarma i demés elements subjectes a desgast, avaria o degradació, és a dir de fet, tots els elements, cal disposar de convenis amb empreses especialitzades que garanteixin d'alguna manera el suport que ens farà falta quan tinguem un dels esmentats entrebancs.

Les empreses subministradores acostumen a donar prioritat a les peticions dels clients amb qui tenen aquests contractes.

També són interessants des del punt de vista que els esdeveniments inesperats queden així previstos en el pressupost ordinari de despeses i no ens podem trobar amb la imperiosa necessitat de fer un dispendi puntual per a abordar una reparació o substitució.

Cal entendre bé el significat d'aquests contractes i no confondre'ls amb pòlices d'assegurances, les quals també calen i tractem posteriorment.

El personal del departament d'informàtica ha de conèixer bé els drets i les obligacions emanades dels contractes i la forma del seu ús. També ha de disposar de document que en demostri de forma fefaent la vigència.

En les clàusules d'aquests convenis o contractes s'ha d'especificar:

* la relació detallada dels serveis contractats,
* la data d'entrada en vigor,
* la durada,
* horari d'assistència,
* la forma de renovació (tàcita, normalment),
* la forma de revisió del preus (relacionada amb l'IPC, normalment),
* la relació detallada de tots i cadascun dels equips i/o elements objecte del contracte, amb el nom del constructor, el model o versió i el número de sèrie,
* un compromís de termini per a la reparació de les avaries.

MÀQUINES

El manteniment normal per a màquines consisteix en les revisions preventives periòdiques i la reparació de les avaries, material inclòs.

Pot contemplar també l'existència d'equip de background, sigui per substituir in situ l'avariat, sigui per a la realització remota de tasques afectades per l'avaria.

Alguns fabricants es comprometen a mantenir el hardware en funcionament durant una certa proporció del temps.

El client s'ha de comprometre a la conservació, la neteja i l'ús normal d'acord amb la documentació, i a facilitar, quant a accés i disponibilitat, les intervencions del tècnics de l'empresa mantenedora.

Els contractes exclouen:

* la intervenció en parts externes com ara climatitzacions i alimentació o comandaments elèctrics,
* l'ús en locals que no compleixen les especificacions tècniques o ambientals,
* el mal ús o l'ús excessiu (a definir),
* l'ús de fungibles no homologats,
* els fungibles i les peces subjectes a desgast,
* les intervencions tècniques no autoritzades,
* la modificació de les especificacions d'origen,
* els moviments o trasllats no supervisats, etc.

Per als extintors inclou una assegurança i cal recordar quant a les cadències que estan sotmesos al Reglament ja esmentat.

Jaume Viñas, "KEEPWARE", 1995

PROGRAMES

Per al software és bàsicament una llicència d'ús.

Una de les formes més avençades de definir el llicenciat és la d'aquell que posseeix legalment un original de la documentació completa i, si existeix, el dispositiu ("motxilla") o programa (encriptat) autoritzador.

La llicència sempre fa reserva absoluta de propietats per al constructor i prohibeix:

- fer còpies de la documentació,
- alterar de qualsevol manera els programes o la documentació, des de la seva versió venuda,
- permetre que altres usin l'autoritzador.

Per contra, es garanteix:

+ El dret d'ús en un únic processador del tipus i amb el sistema operatiu per als quals el software fou construït,
+ Que el software funcionarà com diu la documentació,
+ Durant un període inicial, els suports físics i la documentació escrita.

El contracte per al software pot incloure, més o menys discrecionalment, prestacions com ara:

* reparació o substitució de l'element físic autoritzador,
* disponibilitat de versions corregides de defectes o vicis ocults (no noves prestacions ni personalitzacions),
* documentació original completa i d'actualització o divulgació de novetats,
* dret a còpies de seguretat i dret a ús en sistemes secundaris,
* suport "hot-line" telefònic o remot via mòdem, etc.

Cal distingir molt bé entre tres menes de software:

1 Amb la màxima prioritat, el sistema operatiu,
2 Després, la resta de software de base, amb:
  sistemes gestors de bases de dades,
  compiladors,
  comunicacions,
  interfícies d'operació i administració,
  editors,
3 Per últim, els programes de les diferents aplicacions.

Molt sovint en microinformàtica, és la "compra" la que implica llicència d'ús i no hi ha cap més contracte que els documents d'adquisició. En aquests casos, el sol fet de treure el precinte al paquet que conté els suports amb els programes implica l'acceptació de les condicions, que equivalen als contractes de què hem parlat.

Registre Propietat Intel.lectual núm. 3609 de 31-3-93. Versió corregida

PÒLISSA D'ASSEGURANÇA

Tenint en compte l'elevada inversió de capital que la compra de l'equip informàtic representa, és oportú constituir una pòlissa d'assegurança per a alguna de les màquines, lògicament les més cares com a mínim.

El ja elevat marge de seguretat configurat en una instal.lació com la que aquí s'exposa no pot obviar, per suposat, els perills d'incendi, inundació, enfonsament, robatori, etc.

Cal assumir en tot moment que qualsevol pòlissa només afecta el valor de la maquinària. L'única possible assegurança per a la informació és el rigor en les còpies de seguretat. Per altra part la pòlissa tampoc no pot evitar, cas de sinistre, una interrupció més o menys prolongada en la disponibilitat del sistema informàtic.

Les companyies d'assegurances acostumen a disposar de diferents pòlices estandard per a diferents nivells de previsió i corresponents a diferents primes.

El cobriment de base es refereix als equips electrònics (hardware i altres màquines), relacionades en la pòlissa i llestos per a l'explotació normal.

Altres cobriments addicionals poden ser:

* la reconstrucció de la informació continguda en suports que hagin quedat destruïts, sempre que això sigui possible i la causa en sigui un fet indemnitzable,
* l'ús d'un sistema informàtic alternatiu durant la manca de disponibilitat del sistema assegurat a causa d'un fet indemnitzable, i
* les intervencions tècniques destinades a la conservació, prevenció i reparació (aquesta garantia quasi equival a un contracte de manteniment: n'és la part financera).

Jaume Viñas, "KEEPWARE", 1995

CONDICIONS d'UNA TíPICA ASSEGURANÇA D'ORDINADORS

Les condicions generals d'una pòlissa per al sistema informàtic són molt similars a les que ens podem trobar en qualsevol altra pòlissa. Tot seguit en fem un resum i n'emfasitzem les particularitats.

SíNTESI DE GARANTIES (INCLUSIONS)

Les garanties de la pòlissa s'estenen als danys i/o pèrdues materials que puguin succeïr-li a la maquinària objecte de l'assegurança a conseqüència de:

* AVARIA INTERNA

Aquesta garantia és més pròpiament coberta sota els contractes de manteniment existents sobre els equips assegurats.
No obstant, si l'avaria fos rebutjada per l'empresa que subministra el contracte de manteniment i el motiu del refús no fos un incompliment de les normes del contracte per part de l'assegurat, la pòlissa podria incloure el pagament del sinistre, amb dret de subrogació contra la subministradora del Contracte de Manteniment.

* AVARIA EXTERNA

- Imperícia, negligència i actes malintencionats del personal de l'Assegurat o d'estranys.
- Caiguda, impacte, col.lisió, obstrucció o entrada de cossos estranys.
- Tempesta, pedregada, gelada i desgel, incendi, llamp directe, explosió, inundació, huracà o cicló, aigua, robatori o intent de robatori.
- Vagues, lock-outs, boicots, sabotatges, motins i tumults populars.

EXCLUSIONS

- els riscos abans enumerats si tenen origen en hostilitats, guerra civil o internacional,
- sinistres coberts pel Consorci de Compensació d'Assegurances (Riscos Catastròfics), de conformitat amb l'establert en la Llei.
- el desgast, esgotament o vellesa pròpia de les peces, els danys estètics, aquells substituïbles o recanviables en els aparells, i en general avaries no seguides de dany en els equips, o que s'atenguin sota Contracte de Manteniment, com ara ajustaments, reemplaçaments de plaques, etc.

Jaume Viñas, "KEEPWARE", 1995

MANUAL D'EXPLOTACIó

Ocupa l'explotació diària. Ha de ser el fidel reflex i la màxima expressió d'una instal·lació informàtica acuradament calculada per a l'explotació sense problemes, amb cost i risc mínims, del sistema. El manual desenvolupa un pla d'explotació pensat per a una instal·lació dissenyada per al sistema.

Apareix per la necessitat de resoldre un problema que planteja l'explotació diària: que les operacions senzilles de funcionament rutinari no depenguin dels coneixements d'una sola persona.

INTRODUCCIÓ AL MANUAL

El present manual apareix per la necessitat de resoldre dos problemes que planteja l'explotació diària d'un sistema informàtic modern.

1) Que les operacions senzilles de funcionament rutinari no depenguin d'una sola persona (que té un horari de treball i unes vacances, que pot estar malalta i que té ocupacions físicament lluny del sistema informàtic), i

2) Que aquestes operacions podrien fàcilment arribar a col·lapsar el procés d'informatització.

Es fonamenta especialment el manual en dos aspectes de "deontologia professional administrativa":

1) L'èmfasi en assignar a persones concretes feines concretes, tot delimitant clarament responsabilitats d'actuació o d'omissió, i

2) La importància de la denominada "Llibreta d'Incidències", quadern de registre de totes les actuacions sobre el sistema: cada vegada que algú (no importa qui ni perquè) entra dins de la sala de l'ordinador, cada vegada que es dispara una alarma, el resultat de les revisions periòdiques, cada vegada que s'engega el sistema o s'atura, etc., això ha de ser anotat en la Llibreta d'incidències amb indicació de data, hora, succés, motiu i autor.

COMESES DE VIGILÀNCIA

Als efectes del sistema informàtic s'entén per vigilància dues coses simultànies:

1) Control permanent de l'accés a la sala de l'ordinador, incloent la custòdia de la Llibreta d'Incidències, i
2) Disposició constant per actuar en cas d'alarma, d'acord amb aquest manual.

Queda clar que aquestes funcions estan orientades a garantir la integritat del sistema i han de prestar-se PERMANENTMENT!.

Denominem "vigilant de guàrdia" o simplement "vigilant" a qui, en un moment donat, fa aquestes funcions. Ha d'estar sempre disposat a actuar i a fer-ho amb agilitat i sang freda.

CONTROL DE L'ACCéS A LA SALA DE L'ORDINADOR

* Garantir que ningú no autoritzat entri en ella.

* Fer complir la norma que qui entra en la sala de l'ordinador deixi anotat en la Llibreta d¡Incidències el moment i el motiu d'aquesta visita.

ACTUACIO EN CAS D'EMERGENCIA

Haurà d'acudir immediatament el vigilant de guàrdia, entrarà a la sala de l'ordinador i observarà acuradament la situació.

Un dels principals elements en la filosofia del disseny del sistema és la garantia de màxima disponibilitat. Per això en tota acció empresa en cas d'emergència ha de procurar-se evitar la interrupció del servei.

En tots els casos, si després de la pertinent actuació (l'explicació de les quals segueix en aquest text), s'ha aconseguit restablir totalment la situació de normalitat (anteriorment a presentar-se el problema), el servei informàtic ha de continuar. Per això, si haguéssim hagut d'aturar els ordinadors, després caldrà engegar-los.

Instruccions per a cada cas:

1 "Han saltat un o més dels interruptors d'algun CGP".

Una vegada identificats els interruptors que han saltat, segueixi el següent procediment:

Primer pas: Si ha saltat el diferencial de l'ordinador o el magneto-tèrmic general de l'ordinador, intentar per tres vegades, espaiades un minut entre si, re-posicionar el/s interruptor/s que hagi/n saltat i anotar el resultat en la Llibreta d'Incidències. Si no hi ha èxit en aquest intent, aturar l'ordinador en qüestió.

Si en el primer pas no ha estat necessari aturar l'ordinador en qüestió, procedir amb el segon pas:

Si ha saltat el diferencial o el magneto-tèrmic del condicionador, intentar per tres vegades, espaiades un minut entre si, reposicionar el/s interruptor/s que hagi/n saltat i anotar el resultat en la Llibreta d'Incidències.

2 "Foc en la sala".

El detector de fums és molt sensible i port haver notat la presència de fum que seria imperceptible a una persona. Cal no precipitar-se, doncs, suposant que es tracta d'una falsa alarma: després d'una estona podm tenir un important incendi.

Si no s'observa fum ni cap foc, cal sotmetre la sala a vigilància permanent durant uns minuts i després entrar a fer un cop d'ull cada 5 minuts si més no durant una hora.

Si s'observa fum cal tenir en compte que els aparells electrònics són considerablement incombustibles: normalment la cosa es quedarà en fum, per haver-se cremat algun dels seus components interiors.

Si s'observa foc o fum procedir segons quin sigui l'aparell font del problema: si el fum procedeix del condicionador caldrà aturar tots els sistemes de la sala de l'ordinador.

Si el fum procedeix de l'UPS, caldrà aturar tots els sistemes alimentats des d'ell.

En tot cas, val la pena de tallar l'alimentació dels equips aturats.

Seguidament evacuarem el fum o extingirem el foc de la manera menys aparatosa possible (sense extintor si es pot).

Si és necessari fer servir l'extintor, utilitzarem primer el de gas halon. Si aquest no és suficient, aturarem tots els sistemes de la sala de l'ordinador i utilitzarem un extintor de pols polivalent, elèctricament aïllant.

Després d'utilitzar l'extintor de pols no es poden engegar els ordinadors fins haver-los netejat per l'interior per part de les empreses de manteniment.

Com sempre, haurem de fer anotació completa en la Llibreta d'Incidències.

3 "Temperatura excessiva"

Engegar el condicionador d'aire si no ho està i després entrar a fer un cop d'ull cada 30 minuts fins que desaparagui el problema.

Cada vegada que s'entri, llegir el termòmetre. En qualsevol cas, es tracta de fer tornar la temperatura al seu marge òptim. Per a això, si es pot i es mantenen les garanties de control d'accés, poden utilitzat-se les condicions ambientals externes a la sala de l'ordinador (deixant la porta oberta).

Si la temperatura arriba els 27ºC, aturar d'immediat tots els sistemes de la sala de l'ordinador.

4 "Humitat excessiva"

Engegar el condicionador d'aire si no ho està i després entrar a fer un cop d'ull cada 30 minuts fins que desaparegui el problema.

Cada vegada que s'entri, llegir l'higròmetre o el psicròmetre. En qualsevol cas, es tracta de fer tornar la humitat al seu marge òptim. Per a això, si es pot i se mantenen les garanties de control d'accés, poden utilitzar-se les condicions ambientals externes a la sala de l'ordinador (deixant la porta oberta).

Amb humitat alta, revisar el bon estat dels dispositius deshumidificadors si són del tipus bola seca.

Si la humitat arriba al 80%, aturar d'immediat tots els sistemes de la sala de l'ordinador.

5 "No hi ha tensió en la xarxa"

Si en efecte no hi ha tensió, cal aturar tots els sistemes abans de 10 minuts, procurant esgotar aquest termini perquè si en aquest lapse es re-estableix la xarxa, serà innecessari aturar res.

6 "Fi de bateria de l'UPS"

Aturar IMMEDIATAMENT (EN MÀXIM D'UN MINUT) tots els sistemes. Si després d'un minut el sistema no ha estat correctament aturat es pot produir una PÈRDUA IRREVERSIBLE d'informació.

7 "Falla de l'UPS"

En el plafó de control de l'UPS la situació de normalitat és amb les llums Entrada (Input o Line), Sincronització (Syschronization), Flotació (Float) i Sortida (Ouput) enceses (colors verd o groc) i les demés apagades. Qualsevol altre situació ha de ser informada o/i anotada en la llibreta.

Si s'encén "By-pass" o "Bloqueig" (Fault) (vermella) o s'apaga "Sincronització" (verd), procedir:

1º- Aturar tots els sistemes alimentats per l'UPS
2º- Aturar l'UPS.
3º- Tallar l'alimentació UPS en el CGP.
4º- Restaurar l'alimentació UPS en el CGP.
5º- Engegar l'UPS.
6º- Engegar els sistemes alimentats per l'UPS.

Si es repeteix, realitzat la mateixa operació un màxim de tres cops, i si continua la mateixa situació de "By-pass" o "Bloqueix" (Fault), aturar tots els sistemes i l'UPS.

COMESES D'OPERACIó

ENGEGADA DEL SISTEMA

Consultar la Llibreta d'Incidències per cerciorar-se de que no hi ha cap inconvenient per a l'operació, especialment si el sistema va ser aturat a causa d'una alarma.

Procedir a la revisió de l'estat de la instal.lació, excepte en quant al seu informe detallat.

Verificar que la consola estigui connectada, tant per l'interruptor que porta incorporat com pel de paret. Entrar en la sala de l'ordinador i procedir a la connexió de les màquines (annex) en ordre.

En el plafó de la CPU, prémer el polsador d'inicialització i cerciorar-se de que no dóna cap indicació d'error.

Si aquest indicador dóna error, repetir el procés des que es va pulsar la inicialització. Repetir l'operació un màxim de tres vegades, si en la primera no hi ha hagut èxit i tampoc en la segona.

Si ha estat necessari pulsar la inicialització més d'una vegada, tot el procés serà anotat amb precisió en la Llibreta d'Incidències, indicant especialment quin és el contingut de l'indicador d'error que a la llarga no desapareix, si això succeeix.

Des de la consola, fer IPL del sistema.

Anotar l'èxit o fracàs en la Llibreta d'Incidències.

OPERACIÓ DE LA/ES IMPRESSORA/ES

1 Control de la cua d'impressió

Aquesta cua és el conjunt, ordenat per ordre d'arribada, de totes les ordres (fitxers) d'impressió que els usuaris han donat i que no han estat encara satisfetes.

Quan l'operador faci sortir tots els fitxers d'impressió el primer pas ha de ser el d'entrar a controlar aquesta cua per garantir màxima eficàcia en no permetre que s'usi l'ordinador com fotocopiadora i procurar minimitzar el número de canvis de paper.

2 Control de la/es impressora/es, canvi del tipus de paper i control de les existències de fungibles.

Es tracta de respondre els requeriments que en faci el sistema sobre l'ús de les impressores.

Aprofitant cada canvi de tipus de paper, ha de ser controlat l'estoc, i igualment si es canvia la cinta entintada.

Si la impressió en curs està interrompuda per alguna raó:

* Raons fortuïtes, com fi del paper, mal funcionament etc.
* Raons de màquina, com que la tapa estigui oberta, etc.
* Perquè hagi estat aturada.

El tractament ha de ser el de corregir la causa de la interrupció: anar la impressora, veure que li passa i adobar-ho allà mateix.

3 Neteja de les impressores.

Especialment important per causa de la gran quantitat de pols que produeix el paper. Han de ser mogudes totes les caixes de paper més properes. La impressora ha de ser netejada per dins (amb la tapa oberta), ha ser possible amb una aspiradora.

COPIES DE SEGURETAT

El procediment per fer la còpia de seguretat és la següent:

En certs sistemes és necessari que l'ordinador quedi dedicat en exclusiva a aquest procés per raons d'incompatibilitat d'accessos.

Posar en marxa el procediment (JCL) de còpies de seguretat.
Al principi el programa ens indicarà que joc de cintes usar i tindrem que obtenir-les d'on estiguin guardades. Després seguir amb el procés, posant en la unitat de cinta les cintes que ens indiqui en cada moment el programa.

Si durant el procés apareix un problema sense solució específica que impedeixi continuar-lo fins al seu final, procedir a fer IPL com està explicat en aquest manual.

Obtenir en la impressora els llistats originats (automàticament) pel procés i arxivar-los en la carpeta corresponent.

Anotar el fet, amb indicació de qualsevol problema sorgit o de normalitat, en la Llibreta d'Incidències.

ATURADA DEL SISTEMA

Verificar que ningú estigui treballant.

Entrar en la sala de l'ordinador i procedir a la desconnexió de les màquines, a excepció del sistema d'alarmes.
Haurà de deixar-se funcionant el/algun condicionador per refrigerar, si cal, i l'UPS si alimenta altres equips.

Anotar el fet, amb indicació de qualsevol problema sorgit o de normalitat, en la Llibreta d'Incidències.

Només s'ha de procedir a l'aturada d'emergència del sistema quant, per raons d'urgència, no sigui possible procedir a l'aturada normal.
Difícilment una alarma justificarà una aturada d'emergència.

COMESES DE MANTENIMENT

El manteniment preventiu de la instal·lació informàtica és la millor assegurança contra avaries.

La revisió de l'estat de la instal·lació serà comesa varies vegades per setmana.
La neteja de l'estat de la sala de l'ordinador serà comesa al menys una vegada al mes.
La humidificació de la terra elèctrica serà comesa setmanalment.
La descripció detallada d'aquestes tres comeses segueix en els paràgrafs següents.

També hauran de ser netejades periòdicament a fons les dependències amb paper: magatzem i impressora.
Pot ser siguin aquestes les feines més ingrates de les contingudes en aquest manual però, a llarg termini, són les més importants i les instal·lacions informàtiques solen fallar a causa de que aquestes no han estat suficientment fetes.
Convé, doncs, que l'encarregat de manteniment sigui un "manetes" i, a ser possible, un "apassionat" de l'electricitat - electrònica - informàtica.

REVISIÓ DE L'ESTAT DE LA INSTAL·LACIÓ

Constitueix la inspecció detallada de l'estat de tota la instal·lació del sistema informàtic i el seu informe precís.
Si l'estat d'algun aspecte o part de la instal·lació no fos el correcte, a més a més de fer-ho constar en l'informe, serà retornat a la normalitat.

Haurà de donar-se especial atenció a la sala de l'ordinador, en quant els següents aspectes:

Nivell del detector de temperatura: ha de marcar aproximadament 22.
Nivell del detector d'humitat: ha de marcar aproximadament 80.
Lectura dels plafons de la CPU i d'altres unitats de l'ordinador.
Lectura dels instruments de l'UPS i del sistema d'alarma.
Comandaments del condicionador d'aire.
Temperatura màxima, mínima i actual i re-posicionament dels indicadors per posició de màxima i mínima. Els marges de temperatura tolerats són, funcionant l'ordinador, de 16ºC a 26ºC i, sense funcionar, de 5ºC a 45ºC. Fer constar expressament si s'ha sortit d'aquests marges.

Lectura dels termòmetres de l'higròmetre del psicròmetre (mesurador d'humitat que es tingui): termòmetre sec i termòmetre humit i càlcul de la humitat relativa que es dedueix d'aquestes lectures. Els marges d'humitat són, en funcionament de

l'ordinador, de 20% a 80% i, sense funcionar, de 10% a 90%. Fer constar expressament si s'ha sortit d'aquests marges.

Manòmetres dels extintors.
Dipòsit d'aigua del psicròmetre. Ha d'estar ben ple.
Il.luminació: general i llum d'emergència.

Nivell de neteja i estat general de porta, sostre i terra.
Suports i estat general de la part dels condicionadors d'aire que queda en l'exterior de l'edifici, donat al carrer, i en el seu entorn.

L'encarregat del manteniment farà, personalment, cada sis mesos, prova només per verificar que segueixen funcionant (SENSE OBRIR CAP APARELL) del sistema d'alarma, del CGP i de l'UPS.

NETEJA DE LA SALA DE L'ORDINADOR

La sala de l'ordinador s'ha de mantenir neta de pols i de tot element de rebut. En aquest sentit, s'haurà d'escombrar incloent sostres i parets, i traient la pols que s'hagi acumulat sobre els aparells, caixes i prestatges.
Aquesta neteja es farà amb l'ordinador aturat totalment i amb fundes protectores per la CPU, unitats de disc i unitat de cinta posades. La neteja sempre s'efectuarà en sec, mai amb líquids ni aerossols.

HUMIDIFICACIO DE LA TERRA ELèCTRICA

Serà vessada aigua (uns quants litres) en la reixa de la presa de terra. Es pot tenir en compte la pluja recent com a eximent, en tot o en part, d'aqueta feina.

Jaume Viñas, "KEEPWARE", 1995

PLA D'EXPLOTACIó

El pla d'explotació és el conjunt de disposicions, horaris i ordres internes a l'organització sobre ocupacions relacionades amb el sistema informàtic i previstes i reglamentades en el Manual d'Explotació i altres regles d'ús del sistema. El Pla de Simulacres també en podria formar part.

Es fonamenta especialment el pla en l'èmfasi en assignar a persones concretes tasques concretes delimitant clarament responsabilitats d'actuació i omissió, i en fer un seguiment estricte.

És molt variable segons l'organització i la instal.lació concretes però sempre ha d'incloure instruccions molt clares sobre com actuar en cas d'emergència i com fer les operacions més rutinàries i imprescindibles: engegada, aturada, còpies de seguretat.

És aconsellable de fer supervisions de l'explotació de dues menes:

* les unes exhaustives, periòdiques, de tràmit,
* les altres selectives, aleatòries, per sorpresa.

Aquestes supervisions han de ser sempre seguides de les correccions oportunes, tant per a restaurar l'eficàcia de l'explotació com per mantenir la motivació del personal implicat.

Jaume Viñas, "KEEPWARE", 1995

PLA DE SEGURETAT

Les raons per a una seguretat estricta es fonamenten en la necessitat de disminuir el risc, necessari i inevitable, de la dependència, necessària i inevitable, organització - informació - informàtica.

A ningú no escapa el risc de que incidents fortuïts o intencionats causin danys en el patrimoni material (màquines informàtiques, condicionadors d'aire, grups de continuïtat elèctrica, etc.) o/i en el patrimoni lògic (documentació escrita, programes i dades).

No és tan conegut però sí tan real i important, més difícil d'avaluar i complex de prevenir el risc de paralització de les activitats per falta de disponibilitat del sistema informàtic.

El pla de seguretat és el conjunt d'actuacions i normes encaminades a prevenir aquests riscos.

El pla de seguretat ha de basar-se en la consciència de que no existeix la seguretat total i que cal arribar a un compromís entre risc i cost de la prevenció i ha de ser recolzat per la Direcció i responsabilitzat al més alt nivell, molt difós, contínuament auditat i adaptat a la situació real de l'organització en cada moment.

No és aconsellable portar la seguretat fins més enllà del que és convenient. A part dels elevats costos econòmics, comportaria uns procediments i normes d'operació realment tediosos i lents en la pràctica, que es ferien inoperants.

La complexitat del sistema de seguretat dependrà finalment d'una avaluació i valoració dels riscos i del diner disponible.

Les estadístiques poden ajudar a determinar quines han de ser les prioritats. La valoració dels riscos ha d'incloure un factor de probabilitat que succeeixin.

D'altra banda, i com ja hem dit en parlar dels sistemes d'alarma, ls seguretat específica del sistema informàtic ha de coordinar-se amb la seguretat més general de tot l'edifici o de l'empresa com a organització completa.

En tot cas, la seguretat sempre es dissenya per guanyar temps.

Riscos I EL SEU CONTROL

En aquesta obra no pretenc fer un estudi dels riscos, que és una cosa molt peculiar de cada sistema, sinó només parlar-ne genèricament i incidir en el més lligats al que hem anomenat keepware, el motiu de l'obra.

En un estudi detallat, sempre referit ja a un cas concret, caldria tenir en compte els següents aspectes que també apareixen en tots els sistemes informàtics:

A La confidencialitat, la inviolabilitat, i la integritat de dades i programes,

B Les especials circumstàncies dels microordinadors personals o departamentals, amb especial èmfasi en els "virus" i les xarxes d'aquests microordinadors,

C Les paraules de pas, els drets d'accés, el xifratge.

El control dels riscos significa passar per quatre fases:

1 Acceptació de l'existència d'un risc, com a possibilitat que alguna cosa vagi malament i això representi un cost.

2 Eliminació si el risc no és realment necessari. Això ho podem aconseguir potser amb alguna alternativa.

3 Reducció del risc mitjançant, si més no, un complet coneixement d'aquest risc des de tots els angles possibles.

4 Transferència del risc a tercers: assegurança. Val a dir que la prima serà menor quantes més i millors mesures prenguem per evitar-lo i que mai no podrem incloure el cost de la pèrdua d'oportunitat causada per la no disponibilitat temporal.

Els riscos canvien amb el temps. Canvia l'entorn legal. Canvia la situació econòmica. Apareixen noves activitats delictives.

Per tot això cal mantenir-se al corrent i realitzar constantment proves tot intentant trencar els propis sistemes de seguretat per trobar-ne els punts dèbils, que són canviants.

Perills "naturals", no producte de mala intenció, que amenacen la informació:

* Inadequada configuració o desconeixement del hardware, del sistema operatiu o d'altra software de base (compiladors, etc.),
* Errors d'anàlisi, de programació o d'operació.

Molt més gran és la varietat de causes per les quals alguna persona (intern o extern) pot fer mal intencionadament. Hi dedicarem un subcapitol expressament.

Jaume Viñas, "KEEPWARE", 1995

CONSIDERACIONS ENTORN DE LES ACTUACIONS PERSONALS

Pel que fa al propi personal, partim del fet que sense la conformitat i aprovació dels treballadors, no funcionarà cap sistema de seguretat.

El propi personal té l'oportunitat i, part d'ell la capacitat, per cometre un delicte. Només l'hi falta el motiu, i a vegades també el té. Les situacions familiars, econòmiques, socials i altres, poden afectar el comportament de la gent, fins i tot de forma subconscient.

Cal prendre precaucions en contractar la gent, quant a la selecció i quant a la redacció jurídica de les clàusules del contracte, i en controlar-la després. La millor sinó única solució és tenir la gent contenta o acomiadar-la quirúrgicament d'immediat.

De personal extern podem patir espionatge industrial o sabotatge des de la competència. La més eficaç de les solucions automatitzables estriba en sofisticats sistemes de control d'accessos, amb suport organitzatiu i informàtic.

Però aquestes solucions automatitzables no ho són tot: algú dels nostres pot ser amenaçat, extorsionat o segrestar.

Hi ha tres tipus de mesures d'identificació d'un usuari autoritzat per a un ordinador i que podem fer servir tant per a personal propi, en el decurs de la seva activitat normal, com aliè, en el decurs de les seves visites:

* les que es refereixen a codis secrets que només coneix la persona autoritzada,
* les que es refereixen a mitjans físics, com ara targetes amb banda magnètica, que només posseeix la persona autoritzada,
* les que es refereixen a característiques físiques de la persona autoritzada: petges digitals, retina, veu.

De tota mena d'individus ens podem esperar accions violentes diverses. No són aquestes actuacions les que ens ocupen aquí, ja que són fàcils d'identificar i tenen el seu tractament en la seguretat física de l'edifici i, en última instància, en les assegurances.

La tendència és a l'augment en quantitat i en transcendència d'aquests delictes "informàtics".

Diguem, per finalitzar, que cal saber distingir entre una acte deliverat i un acte accidental o involuntari.

Com a criteri de discriminació, val a dir que, en general, els actes intencionats, respecte dels involuntaris són més complexos, estan ocults, s'han usat les millors habilitats, és possible una confabulació de diverses persones i se'n destrueixen les proves.

Jaume Viñas, "KEEPWARE", 1995

RESPONSABILITATS PER TRACTAMENT DE DADES PERSONALS

Cal fer esment de les obligacions emanades de la Llei Orgànica de Regulació del Tractament Automatitzat de Dades (LORTAD) de caràcter personal.

Aquesta llei consagra els drets d'autodeterminació, amparament, rectificació i cancelació de les dades personals, que defineix com "Qualsevol informació concernent a persones físiques identificades o identificables".

Com a paràgraf significatiu n'extrec el següent: "El responsable del fitxer haurà d'adoptar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat, vist l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, bé provinguin de l'acció humana bé del medi físic o natural."

Jaume Viñas, "KEEPWARE", 1995

MESURES ENCAMINADES A AUGMENTAR LA SEGURETAT

Tipologia de mesures pràctiques a adoptar, en el pla de seguretat, per protegir la informació:

1 Mesures dirigides a evitar la destrucció de software de base, del software d'aplicació i de les dades.
2 Mesures dirigides a supervisar la bondat de les aplicacions i la racional utilització que es fa de programes, dades i altres recursos.
3 Mesures dirigides a assegurar la utilització reservada de programes i dades.

Relació de mesures pràctiques, cronològicament ordenades pel que fa a quan cal començar a prendre-les:

1 selecció del personal,
2 modularitat en el disseny de tot el sistema,
3 distribució de comeses del personal,
4 documentació de qualitat, en detall i actualitzada,
5 ús de xifratge, paraules de pas i nivells d'accés,
6 ús de dígits de control en les transcripcions,
7 rigor en les còpies de seguretat,
8 fer proves completes amb jocs d'assaig adequats,
9 implicar l'usuari en les proves globals d'acceptació,
10 identificar els punts crítics en els procediments,
11 normar els trasllats de programes de proves a explotació,
12 normar la modificació de programes, incloses les urgents,
13 utilitzar les prestacions d'automatització,
14 controlar l'entrada i sortida d'informació,
15 usar màquines destructores per a tot allò confidencial,
16 tenir "log's" el més complets possible,
17 editar i actualitzar normes d'operació i actuació,
18 neteja regular de les dades no necessàries,
19 auditoria permanent per fer comprovacions i verificacions,
20 tenir medis redundants,
21 preveure que es pugui funcionar en part malgrat falles,
22 tenir establerts procediments de recuperació.

COMPONENTS DEL PLA DE SEGURETAT

Un pla de seguretat complet hauria de tenir en compte el següents aspectes:

* requisits de les assegurances,
* efectes dels canvis d'organització,
* seguretat física,
* seguretat contra incendis,
* normativa d'operacions,
* normativa de programació,
* normativa de la gestió dels sistemes,
* normativa per a la integritat de les dades,
* contractació del personal,
* relacions amb els treballadors,
* auditoria periòdica,
* aspectes econòmics.

Dos dels elements fonamentals en el Pla de Seguretat són el Pla de Simulacres d'Emergència i el Pla de Recuperació des d'un Desastre o Pla de Contingència.

Els simulacres d'emergència haurien de contemplar totes les possibles emergències i afectar a totes les possibles persones que hi haguessin de respondre. Com a relació de les emergències a considerar ha de servir la prevista en el Manual d'Explotació.

El pla de recuperació defineix de forma detallada els processos a endegar en cas de desastre per garantir la continuïtat de l'activitat informàtica mentre es restaura l'activitat del sistema original.

Existeixen diverses opcions a l'hora d'elegir una solució. Des de la simple i barata duplicació de suports amb la informació fins a la molt cara duplicació total del departament d'informàtica.

Una solució intermèdia, que no requereix inversions sinó que pot ser perfectament pressupostable, és l'accés ràpid per contracte a un sistema alternatiu compatible del tot amb el nostre. Són els denominats centres de "backup" o en "stand-by".

La disponibilitat d'un tal centre en stand-by es pot aconseguir:

* contractant el servei a una empresa informàtica (constructor o centre de càlcul), o,
* pactant la prestació mútua amb entitats que tenen el mateix problema i sistemes compatibles amb el nostre, o,
* mantenint de forma compartida, entre aquestes entitats, un centre ad-hoc sempre disponible.

Jaume Viñas, "KEEPWARE", 1995

CONTROL DE L'EXPLOTACIÓ

Que l'explotació del sistema informàtic sigui correcta, en el sentit que s'ajusti al Pla d'Explotació i els seus procediments segueixin el Manual d'Explotació, és quelcom en el qual hom no pot confiar cegament. La confecció de l'esmentat Manual i la implantació de l'esmentat Pla no garanteixen, per si soles, que l'explotació sigui correcta sinó que només en posen les bases.

Com sempre, els procediments periòdics tendeixen a degradar-se o a oblidar-se si no són contínuament controlats, si no s'en fa un seguiment exhaustiu.

Per altra part el treball quotidià d'un centre de processament de dades exigeix portar un bon control sobre certs aspectes que no poden dependre simplement de la memòria humana: Què hi ha gravat en tal cinta ?, Quantes caixes tenim de tal tipus de paper ?

Per últim, és molt aconsellable portar un complet seguiment de les incidències que es produeixin en el sistema: avaries, manteniments, canvis de release, etc.

Tots aquests elements es constitueixen en el Control de l'Explotació, que ha de ser rigorosament mantingut al dia.

Per concretar elements d'interessant control citarem:

- garanties, contractes i pòlisses,
- còpies de seguretat,
- inventari de recursos i la seva disponibilitat,
- configuració del sistema,
- suports extraïbles no volàtils,
- fungibles,
- documentació (escrita o en altre suport),
- seguiment d'incidències.

Si el control de l'explotació es fa amb suport informàtic es possibiliten:

* llistats operatius,
* historial,
* estadístiques,
* validacions automàtiques.

Comencen a aparèixer en el mercat potents paquets de software que proporcionen aquest control de forma molt eficaç i eficient. Però encara no poden cobrir, si més no amb totes les seves prestacions, les necessitats actuals, per dues raons:

* els estandards (siguin "de facto" o siguin "de iude") són indispensables, de cara a contemplar sistemes oberts multi-venedor (cal anunciar, al respecte, la norma Distributed Management Environment confeccionada per l'Open Software Foundation),
* encara sobreviuen i sobreviuran durant molt de temps sistemes propietaris (no oberts).

Es poden fer, però, solucions actuals, senzilles però suficients i immediates en aquesta direcció.

Jaume Viñas, "KEEPWARE", 1995

A nivell d'exemple, el que segueix és el disseny d'una aplicació software per facilitar el suport informàtic al control de l'explotació.

He escollit una implantació senzilla, sense massa rigideses, sobre un Sistema Gestor de Bases de Dades Relacionals, amb procediments en el llenguatge estructurat de consultes estandard (SQL).

La precisió d'evitar rigideses es basa en que, a vegades, seria possible un grau d'automatització superior, però a la pràctica seria difícil de complir i l'experiència demostra que això acaba degradant l'ús de l'aplicació i la qualitat de la informació manegada. He procurat un compromís.

La informació relativa a l'explotació s'organitza en mitja dotzena de taules. L'accés a aquestes és públic quant a consultes i llistats. Quant a modificació i inserció, l'accés es delimita amb "views" d'aquestes taules.

Molt rarament, altres procediments més complexos faciliten la navegació i automatitzen treballs addicionals.

Una estructura d'usuaris completa el disseny de l'aplicació:

* "administrador", és el propietari de l'aplicació, amb tots els drets,
* "operador", és l'usuari habitual per al manteniment, amb els drets limitats pels views,
* "assessor", és per a l'staf directiu, amb drets de només consulta.

Jaume Viñas, "KEEPWARE", 1995

ESQUEMA DE L'ESTRUCTURA DE LA INFORMACIó

Tota la informació de l'aplicació es concentra en les següents taules:

- "ware" reuneix la informació inherent a cadascun dels elements del sistema.
- "microordinadors" resumeix les característiques tècniques dels microordinadors.
- "fungibles" fa de cens dels diferents tipus de fungibles que es fan servir i facilita la seva gestió d'estocs.
- "suports" conté les dades bàsiques sobre el contingut i la localització del suports (magnètics), per al seu cens i control d'ús.
- "documentació" és la relació de tota la documentació (manuals, llibres, etc.) de que es disposa en el sistema, permetent el seu registre i el control de la seva localització.
- "incidències" registre i seguiment dels esdeveniments en el sistema, per a posteriors historials i estadístiques.

Les taules més importants en el control de l'explotació són la "ware" i la "incidències". La taula "ware", a més de ser probablement la més important de totes, és sens dubte la més complexa. Per aquesta raó en fem una descripció extensa tot seguit.

Jaume Viñas, "KEEPWARE", 1995

TAULA "WARE" D'ELEMENTS DEL SISTEMA

OBJECTIU

L'objectiu de la taula és reunir tota la informació d'interès per al control de tots i cadascun dels elements del sistema.

ESTRUCTURA

Nemònic Clau d'accés a la taula. Obligatòria i unica. Columna de 12 caràcters alfanumèrics. És el codi biunívoc amb el qual s'identifica un element concret, diferenciant-lo dels altres, dins l'organització usuària del sistema. Fa de clau principal d'accés en tota estructura de dades relativa a l'element.

Descripció Breu explicació de la funció de l'element. Lloc físic on es troba: edifici, local i estància. Persona física usuari habitual. Interlocutor principal o divulgador. Obligatori. Columna de 48 caràcters alfanumèrics.

Tipus_ware Tipologia de l'element. Fa de classificador a l'hora d'interpretar correctament el contingut de certes columnes d'aquesta taula. Obligatori. Un sol caràcter, que representa: (h)ardware / (k)eepware / (s)oftware / (t)elecomunicacions.

Constructor Marca, en cas d'aparell. Propietari - llicenciador, en cas de procediment. Obligatori. Columna de 24 caràcters.

Model_release Model, en cas d'aparell. Versió, en cas de procediment. Columna de 24 caràcters.

Núm_sèrie Número de sèrie, fabricació o llicència, que identifiqui biunívocament l'element sabut el seu fabricant o llicenciador. Columna de 24 caràcters.

Documentació Tipus de documentació (i codi intern, si és possible) de referència tècnica (no comercial) que tenim a l'abast, relativa al funcionament de l'element: manual, etc. Columna de 24 caràcters alfanumèrics.

Data_estrena Data de posada en servei de l'element. D'interès per a la finalització de la/es garantia/es i inici del seu seguiment. Columna tipus data.

Inserció_sistema Informació molt depenent de la tipologia. Resumeix de quina manera l'element s'integra en el sistema global, tot relacionant-se amb altres elements o de forma aïllada. S'implementa amb dues columnes de 12 caràcters alfanumèrics cadascuna:

* inserció_subsistema (per a classificació en subsistemes dels elements del sistema global),
* inserció_terminal (per a identificar el node terminal que ocupa l'element, dins el subsistema al qual pertany).

Emp_manteniment Empresa que fa el manteniment, o atorga la garantia, de l'element. Columna de 24 caràcters alfanumèrics.

Tip_manteniment Tipus d'assistència pactada amb l'empresa mencionada: contracte de manteniment, garantia, etc. Columna de 12 caràcters alfanumèrics.

Data_manteniment Data de finalització de l'actual vigència d'aquesta assistència. Columna tipus data.

Transferència_suport Informació relativa a la capacitat de recuperació en cas de desastres. Per a aparells, pòlissa d'assegurança en vigor. Per a procediments / programes, suport no volàtil on hi ha la còpia més recent. Columna de 24 caràcters alfanumèrics.

Transferència_data Per a aparells, data de finalització de l'actual vigència de la pòlissa. Per a procediments / programes, data de la còpia. Columna tipus data.

Situació Switch intern de l'aplicació per a distingir els elements que estan en servei actiu (1) dels que han estat retirats (0) i dels que estan encara en algun nivell de projecte (>1). Un dígit decimal. Obligatori.

UTILITATS

Per la seva estructura, la taula ware té les següents utilitats simultànies:

1ra Fa d'inventari actualitzat. Dóna una idea precisa dels recursos disponibles i de la inversió efectuada al llarg del temps.

2na Informa de la distribució actual dels recursos, com una fotografia instantània de la configuració.

3ra Resumeix dades importants dels elements, que cal guardar en algun lloc perquè són de fàcil pèrdua, de forma coherent i unificada.

4ta Tipifica les fonts d'incidència, en identificar biunívocament els elements. Això és imprescindible per poder fer un seguiment correcte de les incidències.

5na Facilita la confecció automàtica o semiautomàtica d'informes.

Proporciona una plataforma única de control per als següents aspectes, per als quals caldria algun control ad-hoc:

6na Darreres còpies de software o documentació electrònica.

7na Cobriment per garanties.

8na Cobriment per contractes de manteniment.

9na Cobriment per pòlices d'assegurança.

UTILITZACIó

Les següents columnes:

nemonic,

tipus_ware,
constructor,
model_release,
núm_sèrie,
data_estrena, i
documentació

s'han d'omplir en registrar l'element (inserir la fila) i NO tornar-les a tocar.

La correcció de les dades d'aquestes columnes, així com la inserció de files, la supressió de files (això només té sentit per causa d'error) i la modificació de la columna Situació, són reservades a l'administrador del sistema.

Les següents columnes:

descripció,
emp_manteniment,
tip_manteniment,
data_manteniment,
inserció_subsistema,
inserció_terminal,
tranferencia_suport, i
transferencia_data

es poden modificar (actualitzar) per l'operador del sistema, a través de "views" de la taula.

Jaume Viñas, "KEEPWARE", 1995

ESTRUCTURA DE LES ALTRES TAULES

Microordinadors

Placa base: processador, arquitectura, RAM, velocitat de rellotge,
Capacitat fixa d'emmagatzemament (disc dur),
Mitjans d'entrada i sortida (disquets, streamer),
Ports d'entrada i sortida (sèrie, paral.lel, de jocs)
Monitor (tamany, norma de definició, color/monòcrom),
Teclat (norma d'arquitectura, nombre tecles, idioma, norma de clavilla),
Altres dispositius interns (plaques d'expansió),
Altres dispositius externs (mouse, joysticks, etc., sense incloure màquines "independents" amb prou entitat en si mateixes com ara impressores, taules digitalitzadores, scanners o dispositius d'autorització).

Fungibles

Codi intern del tipus de fungible (nemònic),
Tipologia (diferents tipus de paper, cinta entintada, toner, etc.),
Quantitat mínima que cal tenir en estoc,
Quantitat que s'usa simultàniament,
Quantitat realment en estoc,
Quantitat demanada al subministrador,
Data d'aquesta petició,
Dades del subministrador.

Suports

Codi intern del suport individual,
Tipologia (cinta, cartridge, disquet, etc.),
Informació relativa al seu contingut, suficient com per poder-lo llegir (què hi ha enregistrat,
Data d'enregistrament, mètode, etc.),
Propietari,
Localització actual,
Disponibilitat (a guardar per a arxiu, a guardar com a original, lliure per a l'ús discrecional, per guardar provisionalment, per a còpies de seguretat, etc.),
Relació amb altres suports (si forma part d'un enregistrament multi-volum).

Documentació

Codi intern del volum individual,
Títol,
Autor,
Editorial,
Any de l'edició,
Referència (ISBN o altra),
Element del sistema al qual documenta,
Localització actual.

Incidències

Font de la incidència: un element del sistema, tipus

de fungible, suport magnètic o volum de documentació (el qual ha d'estar donat d'alta com a tal en la taula corresponent),

Data en què es produí la incidència,

Persona física més coneixedora de les circumstàncies de la incidència,

Breu explicació de la incidència,

Estat actual del tractament (tipificat i codificat),

Data des de la qual l'estat és l'indicat.