

## SEGURETAT DE LA XARXA INFORMÀTICA A L'EMPRESA

En aquest document s'explica quin és el maquinari (hardware) i el programari (software) bàsic i necessari per tenir en un bon nivell de seguretat el sistema informàtic, tant a nivell d'intrusions exteriors com de protecció de les dades.

**S.A.I. – Sistema d' Alimentació Ininterrompuda.** Protegeix als servidors i ordinadors (estacions de treball) de les caigudes i pujades de tensió en el subministrament d'electricitat. Es tracta d'un sistema amb bateria que es carrega (acumula) mentre hi ha corrent elèctric i es descarrega en el moment que n'hi falta, donant temps, entre 8 i 20 minuts, per fer una parada correcte dels equips.

De S.A.I. n'hi ha de dos tipus:

Els Off-line que només actuen en un tall de corrent i no detecten els "micro talls" o petites baixades de tensió. Mentre la tensió és correcte es limita a fer de "By-pass". El seu preu oscil·la entre els 70€ per una estació de treball de 600VA i els 600€ per un servidor de 2000VA o per un grup de fins a quatre ordinadors.



Els On-line que actuen sempre subministrant una tensió de sortida a 220V filtrada i estabilitzada encara que la d'entrada ja sigui correcte.

El seu preu oscil·la entre els 575€ de 1000VA apte per dues estacions de treball i els 1640€ de 3000VA per un Rack amb servidor o per un grup de sis ordinadors.



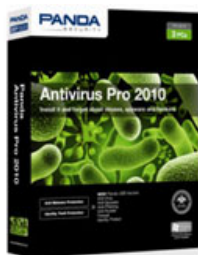
\* Cada ordinador / servidor junt amb el seu monitor han d'estar connectats a un S.A.I. i mai directament a l'endoll de corrent. També s'hi connectarà el router (encaminador) i el switch (distribuïdor) per tal de mantenir les connexions de la xarxa local actives i no provocar talls de comunicació que podrien afectar als programes de gestió / comptabilitat que treballen de forma distribuïda o centralitzada en l'equip que fa de servidor. Les impressores (sobretot les de tipus Làser) no s'hi connectaran mai degut al seu elevat consum al fer el secat del paper.

\* Cada dos anys s'ha de comprovar l'estat de la / les bateries internes, ja que amb el pas del temps van perdent capacitat de càrrega i ens podríem trobar que en el moment en que l'aparell hagi d'actuar no ho faci, o bé no proporcioni energia suficient per donar temps a parar els ordinadors.

\* La durada de subministrament d'energia d'un S.A.I. ve determinada per l'estat de les bateries, la seva potència nominal en VA i la càrrega que ha de suportar (els equips connectats), que mai ha de superar a la potència nominal de l'aparell.

**ANTIVIRUS** – Es un software que s'actualitza diàriament o com a molt setmanalment i que protegeix a l'ordinador dels arxius que són o contenen virus i que bàsicament entren en el sistema informàtic per 3 punts, el correu electrònic (conegut i no conegut), la navegació WEB per pàgines de dubtosa reputació i la descàrrega de programes / música / vídeos mitjançant programes P2P (tipus emule / Kazza).

El seu preu anual oscil·la entre els 45€ del Panda PRO 2010 per a 3 ordinadors i els 430€ del McAfee Active VirusScan Enterprise per a un mínim de 11 usuaris amb suport telefònic en català / castellà en horari laboral i en anglès les 24 hores els 365 dies de l'any.



\* Cada ordinador / servidor de la nostra xarxa ha de tenir instal·lat un Antivirus actualitzat almenys un cop per setmana, habitualment ja ho fan automàticament cada dia i en el cas de McAfee es pot planificar l'hora en que el volem actualitzar.

\* Tots els productes Antivirus s'han de renovar cada any, ja que en cas contrari deixen d'actualitzar-ne les noves definicions de virus i acaben sense protegir l'ordinador.

**ROUTER (Encaminador) ADSL**– És l'aparell que connecta la xarxa informàtica local amb l'exterior (INTERNET) per la línia telefònica. Normalment el subministra el proveïdor del servei ADSL i molts porten incorporat el sistema Wi-Fi (sense fils) que permet la connexió a la xarxa local i a Internet dels ordinadors sense el cable RJ-45. S'anomena router (encaminador) perquè encamina els paquets TCP/IP (correus, web, fitxers, etc...) que no porten el número de IP (interna) de la nostra xarxa cap a la xarxa exterior que és Internet, i els de la xarxa exterior que porten el nostre número de IP (externa) ens els deixa entrar a la xarxa local.

La connexió Wi-Fi, en cas de voler tenir-la activada, sempre ha d'estar codificada i mai l'hem de deixar oberta (sense clau) ja que des de qualsevol ordinador, habitualment portàtil, situat a menys de 70 metres del router (encaminador), es pot entrar a la xarxa local i veure, copiar o esborrar els arxius i carpetes que hi han compartides en el servidor o en els ordinadors que s'utilitzen com estacions de treball.

Bàsicament existeixen dos tipus de codificació de la connexió Wi-Fi:

WEP és la codificació que normalment deixen configurada els proveïdors del servei ADSL i que és vulnerable en pocs minuts per un "hacker" sense excessius coneixements, ja que la clau "viatja" per ones entre els ordinadors i el router.

WAP o WAP-PSK és la codificació òptima, ja que la clau únicament es troba en el router o punt d'accés inalàmbic i en l'ordinador que es connecta, la clau no "viatja" per les ones, no la pot saber ningú que no tingui accés a un dels dos aparells.

Xarxa local (rang)

IP: 192.168.1.XXX

Xarxa externa

IP: 80.35.214.36



**N.A.S. – Network Attached Storage** – És un aparell de xarxa que fa la funció de servidor de fitxers, similar a un ordinador però amb un gran avantatge, no precisa de sistema operatiu, i un cop configurat no necessita de cap manteniment ni actualitzacions. No pot actuar com a servidor d'aplicacions.

Els que porten incorporats dos discs durs en el seu interior són els recomanables per a l'àmbit empresarial, ja que es poden configurar com a RAID1, sistema que permet que un dels discs sigui el "mirall" de l'altre, aportant una doble seguretat, ja que en cas de fallada d'un disc, l'altre continua treballant.



D-Link DNS-323 500 Gb x 2 discs  
El preu és de 350 €  
IOMEGA IX2 500 Gb x 2 discs  
El preu és de 335 €



\* És un sistema vàlid, ràpid i econòmic per centralitzar les còpies de seguretat locals en un entorn empresarial petit o mitjà.

\* El DNS-323 permet configurar una adreça de correu electrònic per enviar-hi una notificació en cas de fallada de un dels discs o d'excés de temperatura.

**FIREWALL (TALLAFOCS)** – L'objectiu d'un tallafocs és impedir o limitar l'accés de persones no autoritzades als ordinadors de la xarxa des de l'exterior, és a dir des de Internet.

De tallafocs n'han de dos tipus :

**Per software.** És un programa que bloqueja els ports d'entrada TCP/IP en l'ordinador, no els de sortida, ja que si ho fes no podríem navegar ni enviar correus. El propi Windows XP a partir de la versió SP2 ja n'incorpora un.

Es pot configurar des de el propi sistema per obrir els ports d'entrada que utilitzen els programes que necessitem (connexions remotes, Emule, servidor Web, etc ...), això vol dir que un virus o troià que tinguem dins l'ordinador també ho pot fer.

**Per hardware.** És un aparell que es connecta entre el router (encaminador) i el Switch (distribuïdor), és transparent per els usuaris de la xarxa local però que convenientment configurat filtra tots els paquets TCP/IP que n'entren i en surten, detectant i bloquejant virus, pàgines WEB perilloses o poc recomanables i accessos no autoritzats.

Els que porten antivirus incorporat s'actualitzen diàriament i s'ha de pagar la llicència anual. Igualment passa amb el filtrat de continguts (pàgines web).



ZyXel Zywall USG100.  
Per xarxes de fins a 25 usuaris.  
Filtre antivirus Kaspersky.  
Filtre continguts Blue Coat.  
Connexions VPN IPsec.  
El preu és de 490€

\* En l'actualitat molts routers (encaminadors) porten incorporat un firewall (tallafocs) simple a nivell de gestió de ports TCP/IP, el que no inclouen són els filtres de continguts i d'antivirus ni les connexions VPN segures.

**CÒPIES DE SEGURETAT EXTERNES** – La llei de protecció de dades obliga, i el sentit comú ho confirma, que s'han de tenir unes còpies de seguretat dels fitxers importants per el funcionament de l'empresa fora del lloc de treball per el cas que hi hagués un robatori o incendi. Les assegurances cobreixen el maquinari, en algun cas el programari, però mai les dades.

Hi ha dos sistemes vàlids per realitzar les còpies externes:

- 1) Un disc dur USB que es connectarà, com a mínim un cop per setmana, al servidor i on es copiaran els fitxers de documents d'ofimàtica com fulls de càlcul, textos, plànols, etc., i els arxius de les aplicacions de comptabilitat i gestió comercial o facturació.
- 2) Contractar un espai en un servidor extern (Data Center) on cada cop que s'hagi programat, s'hi enviaran els fitxers mitjançant la connexió ADSL. Normalment és un procés que es realitza de nit en hores que no es treballa a les oficines.



Tant un com l'altre tenen avantatges i inconvenients.

\* El primer cas es tracta d'un sistema econòmic (100€ és el que costa un disc USB de 250 Gb) i ràpid, ja que la transferència de dades es fa localment connectat al servidor, però amb un greu problema de seguretat que és el transport, on es pot espatllar, es pot perdre, i terceres persones podrien obtenir les dades.

\* El segon cas es tracta d'un sistema més segur, ja que la informació està guardada de forma redundant (en més d'un servidor) i codificada, per tal que ningú que no conegui la clau no hi tindrà accés, però és més car ja que es paga per la capacitat d'emmagatzemament contractada (uns 30€/mes per 10Gb) i és més lent, la informació "viatja" per la línia ADSL, que de pujada sol funcionar a una velocitat de 300Kb/s (0,3Mb).

**DOCUMENT DE RECURSOS INFORMÀTICS** – Es tracta d'un dossier on es detallen i es descriuen les característiques i configuracions de tots els actius informàtics que té l'empresa: ordinadors, servidors, impressores, escàners, etc ..

El document ha de contenir tota la informació necessària perquè en el cas d'haver de substituir un o varis equips per manteniment o renovació es puguin tornar a deixar amb les mateixes funcionalitats anteriors.

A cada equip se li assignarà un codi i se li obrirà un full on es detallarà la següent informació :

En un ordinador / servidor s'indicarà:

- 1) Les característiques del maquinari: processador, memòria RAM, disc dur, placa de xarxa i/o vídeo, etc.. i la data d'adquisició, deixant un espai per descriure-hi possibles ampliacions i/o reparacions.
- 2) Les característiques del programari: sistema operatiu, programes instal·lats amb la seva versió i les dates en que s'han instal·lat, així com l'empresa responsable del manteniment de les aplicacions de facturació, comptabilitat o altres específiques que hi estiguin instal·lades.

- 3) Les característiques de configuració: la ubicació física de l'aparell, les carpetes compartides (si n'hi ha), les impressores que té configurades, el o els noms d'usuaris així com les contrasenyes que tenen adjudicades, la direcció IP (en cas que sigui estàtica), el nom de la màquina i el seu grup de treball o domini.

En una impressora s'indicarà:

- 1) Quin tipus de connexió la uneix a la xarxa. Si és per Ethernet s'ha d'indicar la direcció IP (en cas que sigui estàtica) i si està connectada a un ordinador si és per USB o Paralel, el nom del recurs compartit (si ho està) i nom d'ordinador.
- 2) Els ordinadors que tenen accés a imprimir-hi (en cas d'estar compartida).
- 3) La data de compra i d'instal·lació.
- 4) Detall i vida útil dels consumibles que requereix per el seu funcionament.
- 5) Quin és el nom d'usuari i la contrasenya per accedir a la seva configuració per web (en cas que sigui possible configurar-la per navegador WEB).

En un altre dispositiu de xarxa (encaminador, tallafocs, N.A.S., etc...) s'indicarà:

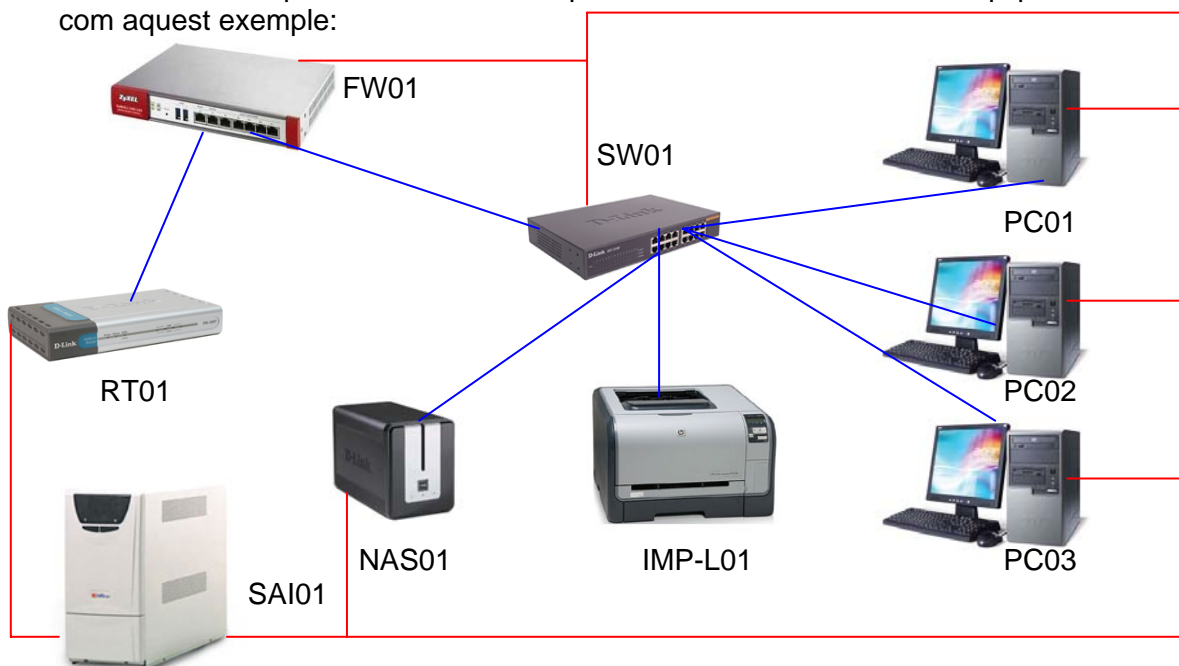
- 1) Quina és la seva funcionalitat i les seves característiques.
- 2) La data de compra i d'instal·lació.
- 3) Indicar la direcció IP (en cas que sigui estàtica).
- 4) Quins ordinadors / usuaris hi tenen accés.
- 5) Quin és el nom d'usuari i la contrasenya per accedir a la seva configuració per web i/o telnet (en cas que sigui possible).
- 6) Descripció detallada de la configuració actual.

En un S.A.I. s'indicarà:

- 1) Quin és el model i la potència nominal que pot suportar.
- 2) La data de compra i d'instal·lació.
- 3) A quins aparells està connectat i dona el servei.
- 4) Les dates dels canvis de bateria que s'han fet.

En un apartat del document s'especificarà on es guarden els CD's originals dels "Drivers" del maquinari, sistemes operatius i programes adquirits que estaran etiquetats amb el codi assignat a cada equip on estan instal·lats.

S'inclourà un esquema bàsic de la disposició i les connexions dels equips a la xarxa com aquest exemple:





El cablejat de color **blau** pertany a connexions de **xarxa** i el de color **vermell** pertany a connexions d'**electricitat** dels equips connectats al S.A.I.

Es mantindrà un registre de les dates que s'han fet les còpies de seguretat, tant locals com externes.

\*La documentació dels recursos informàtics proporciona una resposta més immediata i fiable al tècnic a l'hora de fer una intervenció o de la resolució d'un problema de configuració d'un equip de la xarxa.

\*Les hores dedicades a la seva confecció (entre 6 i 12) es recuperen ràpidament i el responsable de l'empresa té documentada la seva infraestructura informàtica a l'hora de prendre decisions sobre l'actualització, manteniment o compra de nou equipament..

#### **EN RESUM:**

- El S.A.I. evitarà parades incorrectes, per falta de tensió elèctrica, dels ordinadors i servidors de la xarxa, que poden alterar o corrompre els fitxers de les aplicacions amb les que es treballa.
- Els antivirus evitaran que programes d'origen desconegut i dubtós puguin instal·lar-se en l'ordinador i provocar-ne un mal funcionament o capturar-ne les dades.
- El router (encaminador) ha d'estar ben configurat, amb els ports TCP/IP d'entrada no necessaris tancats i amb la Wi-Fi desactivada o codificada amb WPA-PSK.
- El N.A.S és un dispositiu segur, econòmic i amb una gran capacitat d'emmagatzemament per utilitzar-lo de servidor de fitxers o per centralitzar les còpies de seguretat locals.
- EL firewall (tallafocs) és necessari en cas de voler realitzar connexions VPN permanents i segures des de una altra sucursal de l'empresa o filtrar els continguts o serveis als que accedeixen els ordinadors.
- Tenir unes còpies de seguretat dels fitxers fora del lloc de treball és una obligació segons la llei de protecció de dades, es poden fer amb un disc dur extern, dispositiu de cinta DAT o bé enviar-les a un servidor extern (Data Center) de forma comprimida i codificada.
- Tenir confeccionat el document de recursos informàtics facilita la feina de manteniment, reparació o renovació de l'equipament informàtic a l'hora d'instal·lar-lo i configurar-lo o d'identificar i solucionar possibles problemes de connexió a la xarxa.

#### **OBJECTIU:**

L'objectiu d'aquest document ha estat explicar i orientar d'una forma senzilla, visual i didàctica als responsables de les petites i mitjanes empreses que no disposen de departament d'informàtica propi, i que en moltes ocasions no se'ls dona una visió global de la seguretat de la xarxa i de la funció que realitza cada aparell, la importància de tenir els seus arxius protegits, complir la llei de protecció de dades i tenir documentada la seva estructura informàtica.

#### **NOTA:**

Els logos i les imatges incloses en aquest document són propietat de les seves marques. Acer, Banckup, D-Link, Hewlett Packard, Iomega, McAfee, Panda, Riello i Zyxel.

Els preus dels aparells exposats són orientatius, abans d'incloure impostos i a data de la confecció.