

## CÒPIES DE SEGURETAT

Les còpies de seguretat és un dels reptes que la informàtica encara no ha pogut solucionar d'una forma fàcil, eficient, efectiva i ràpida. Es cert que amb els anys s'ha anat millorant molt i molt. Els que ja tenim una edat, encara recordem com una apagada de llum ens podia fer perdre més d'una tarda de feina, o el fet de no poder retornar un document a una versió escrita anteriorment.

En aquesta entrada del blog intentaré explicar, que són les còpies de seguretat, quins riscos te no fer-les o fer-les malament, quines són les millors opcions, quins costos tenen, etc.

D'entrada hem de tenir clar que la seguretat de les nostres dades mai serà del 100%. El que es mira d'aconseguir és que aquest percentatge s'atansí el màxim possible a aquest 100% amb el mínim cost possible. Però anem a pams:

### Què és una còpia?

Segons el Diccionari de l'Institut d'Estudis Catalans en l'accepció que ens afecta, una còpia és una informació que ha estat servada (guardada intacta) i que permet restituir l'original en cas necessari.

Vist amb aquesta definició sembla fàcil el tema de la còpia de seguretat, però si ens hi fixem be, ens apareixen dos conceptes molt importants: guardar intacta i restauració efectiva.



Això ens fa parar a pensar: molt be! fer una còpia amb els mitjans actuals és molt fàcil de fer, però és segura? A mi en aquest punt m'agrada sempre diferenciar dos conceptes: La còpia de seguretat i la còpia d'inseguretat.

## Factors que una còpia fan que sigui segura o insegura

Com hem dit abans una còpia mai serà segura al 100%, aleshores ens podem preguntar, quin és el límit que marca si una còpia es segura o no? Doncs molt senzill, el segon concepte de la definició de còpia: Poder-la conservar i restaurar efectivament en cas de necessitat.



## Factors que ens poden fer perdre la informació

El fet que la seguretat en les còpies no sigui mai al 100%, es per que mai podem definir tots els factors que ens poden fer perdre la informació. El que si que podem fer és agrupar-los en diferents categories:

- Errors humans: És una de les primers causes de pèrdues d'informació. Qui no ha esborrat mai una carpeta de l'ordinador per error?



- Avaries electròniques: La tecnologia electrònica també genera errors. Quants cops heu vist gent que ha perdut dades per una avaria al disc dur de l'ordinador o perdre les fotografies d'un dispositiu mòbil que ja no arranca? O us ha passat a vosaltres mateixos?



- Errors de programari. Els programes no són perfectes. Molts cops contenen error dels propis programadors de l'aplicació. Aquests errors ens poden arribar a causar la pèrdua de dades.



- Accidents i causes naturals. Encara que al llegir això ens posem les mans al cap, un servidor no seria el primer cop de veure dades d'empreses perdudes per un incendi o una fuga d'aigua d'una canonada.



- Altres causes: Són aquelles per les quals, segurament hi ha una de les explicacions anteriors, però no les hem pogut saber. Ningú a tocat res, els registres de l'ordinador diu que tot es correcte, i aparentment no ha passat res, però la informació ha desaparegut.

### Tipus d'informació a desar.

Un altre aspecte molt important al elegir el tipus de còpia de seguretat a utilitzar, és el tipus d'informació a desar, o millor dit la mida que pugui arribar a ocupar aquesta informació. No ocupa el mateix espai un document ofimàtic que un vídeo en alta resolució. Per això distingir de quina informació es necessària fer la còpia de seguretat i de quina informació no caldria, ens pot estalviar molt temps i diners.



Un exemple molt clar seria, si nosaltres tinguéssim una empresa d'edició de vídeo, no se'ns ocurreria pas fer les còpies dels nostres treballs al núvol. Ens sortiria molt car per la mida i a sobre tindríem constantment l'ample de banda de la nostra connexió ocupat enviant dades de la còpia.

## Tipus de mitjans per fer les còpies

Passarem a analitzar els 3 tipus principals de mitjans de còpies de seguretat, analitzant els seus pros i les seves contres:

**MITJANS ELECTRÒNICS:** Son aquells dispositius electrònics que ens permeten fer una còpia de les dades. Estem parlant d'altres ordinadors, memòries USB, discs externs, telèfons mòbils, etc. Els principals avantatges d'aquests sistemes són la facilitat de fer i recuperar les còpies, la gran capacitat d'emmagatzematge, i que econòmicament són molt assequibles. El seu gran taló d'Aquil·les: La seva inseguretat alhora d'emmagatzemar les dades. Normalment en aquests dispositius realitzem el que jo anomeno còpies d'inseguretat.



**MITJANS FÍSICS:** Són aquells que emmagatzemem les dades en un dispositiu físic no electrònic. Estem parlant de cintes, DVD, CD, etc. Tenen el gran avantatge que un cop feta la còpia és molt més difícil perdre les dades que hi han en ella, ja que acostumen a ser dispositius magnètics o òptics i la seva capacitat d'emmagatzematge pot ser molt alta. Són també molt fàcilment portables, el que ens permet separar les còpies en una distància suficient per evitar la pèrdua de dades a causa d'accidents o catàstrofes naturals. El seu principal inconvenient és la dificultat en fer i mantenir aquestes còpies. Hem de perdre un temps a

assegurar-nos que les còpies estan ben fetes i comprovar periòdicament que es poden restaurar correctament.



**MITJANS EN LÍNIA:** Ens permet fer còpies a través de la xarxa en servidors o espais habilitats a tal efecte. Es poden contractar serveis d'empreses dedicades especialment a això, o inclús algunes ens ofereixen un espai gratuït, o fins hi tot podem construir nosaltres el nostre propi sistema de còpies remotes en línia. Té l'avantatge de ser un sistema molt segur i fàcil de configurar, però per contra seva l'espai i la velocitat són limitades amb les tecnologies actuals. En el cas de fitxers d'una mida molt gran el sistema acostuma a ser inviàble o massa car.



## Seguretat de la informació

És important pensar amb el fet que com més còpies d'una informació hi hagin, menys possibilitats de pèrdua existeixen, però aleshores la seguretat de privacitat d'aquestes dades disminueix. I aquí el refranyer català és molt clar: Secret d'un és secret, secret de dos és difícil i secret de tres descobert és. Això ens indica que també hem de fer equilibris entre el nombre de còpies i la privacitat de les dades a copiar. En aquest punt hauríem de tenir en compte la necessitat o no d'encriptar la informació.



## I que fem?

Doncs com podeu veure per gustos, colors. El primer plantejament que cal fer sempre és mirar on estem situats dins de tota la informació que us acabo de donar, i elegir els millors sistema de còpies possible, analitzant els possibles factors de risc de pèrdua, la informació a desar i els mitjans que tenim disponibilitat, fent també un anàlisi costos-pèrdua d'informació. No podem tenir uns costos elevats de còpies per una informació que no ho val!!!!

## Casos pràctics:

Anem a veure un parell de casos pràctics per entendre i pair millor tot el que hem explicat.

*CAS 1: Sóc un estudiant de últim curs de carrera d'enginyeria, i estic fent el projecte de final de carrera. Les meves aficions són sortir els caps de setmana amb els amics a fer excursions i fem moltes fotografies de paisatges espectaculars. M'agrada molt el cinema i dispo de una col·lecció important de pel·lícules clàssiques.  
Dispo de un ordinador de sobretaula, d'un portàtil i telèfon mòbil.*

Sense analitzar més profundament, veiem que aquest xicot dispo de 3 tipus de dades diferents. Per una banda les dades dels seus estudis, fotografies seves i pel·lícules.

Disposant del que dispo, jo li aconsellaria que tota la seva informació hauria d'estar tant al ordinador de sobretaula, com al ordinador portàtil, o si no hi podés ser per raons d'espai de disc dur, que adquirís un disc extern de bona capacitat i que tota la informació TAMBÉ estigui al disc extern. Aleshores segmentant per tipus d'informació, li aconsellaria que amb això per les pel·lícules ja en tindria prou, ja que amb cas de pèrdua, les pel·lícules es podrien recuperar per altres mitjans (amb el seu cost en temps això sí!). Pel que fa a les fotografies, jo li aconsellaria que cada cop que faci una descàrrega de càmera de fotos fes una còpia en un DVD i emmagatzemés correctament aquesta còpia. Pel que fa a les dades dels seus estudis, li aconsellaria un programa de sincronització de dades en línia tipus

Dropbox, Microsoft One Drive, Google Drive, etc...

Amb aquest sistema plantejat, en cas de pèrdua tant de l'ordinador de sobretaula com del portàtil, aquesta persona amb més o menys feina podria recuperar les dades i ha tingut un cost raonablement baix. El telèfon mòbil per trucar si es perd anant d'excursió.

*CAS 2: Sóc metge, i tinc una consulta privada. A la consulta hi tinc 2 ordinadors, un amb la informació de gestió (factures, comptabilitat, horaris, etc.) i un altre on deso la informació dels historials mèdics dels pacients.*

El primer que li hauríem d'aconsellar amb aquest metge, és l'adquisició d'un servidor de dades amb la més alta seguretat possible. Les dades que gestiona són d'alt risc. El servidor a part de la seguretat ens els discs durs que pugui portar per naturalesa, hauria de tenir un sistema de còpies de seguretat amb cintes magnètiques que es realitzarien a diari, i s'emmagatzemarien en una caixa forta en la mateixa consulta. Periòdicament (setmanalment o quinzenalment) es faria una còpia que s'hauria d'emmagatzemar fora de la consulta, també en una caixa forta. Els ordinadors passarien a ser punts de treball, sense cap informació important emmagatzemada en ells.

Es un sistema costós, però en aquest cas ens asseguràrem tant la privacitat com la seguretat de les dades.