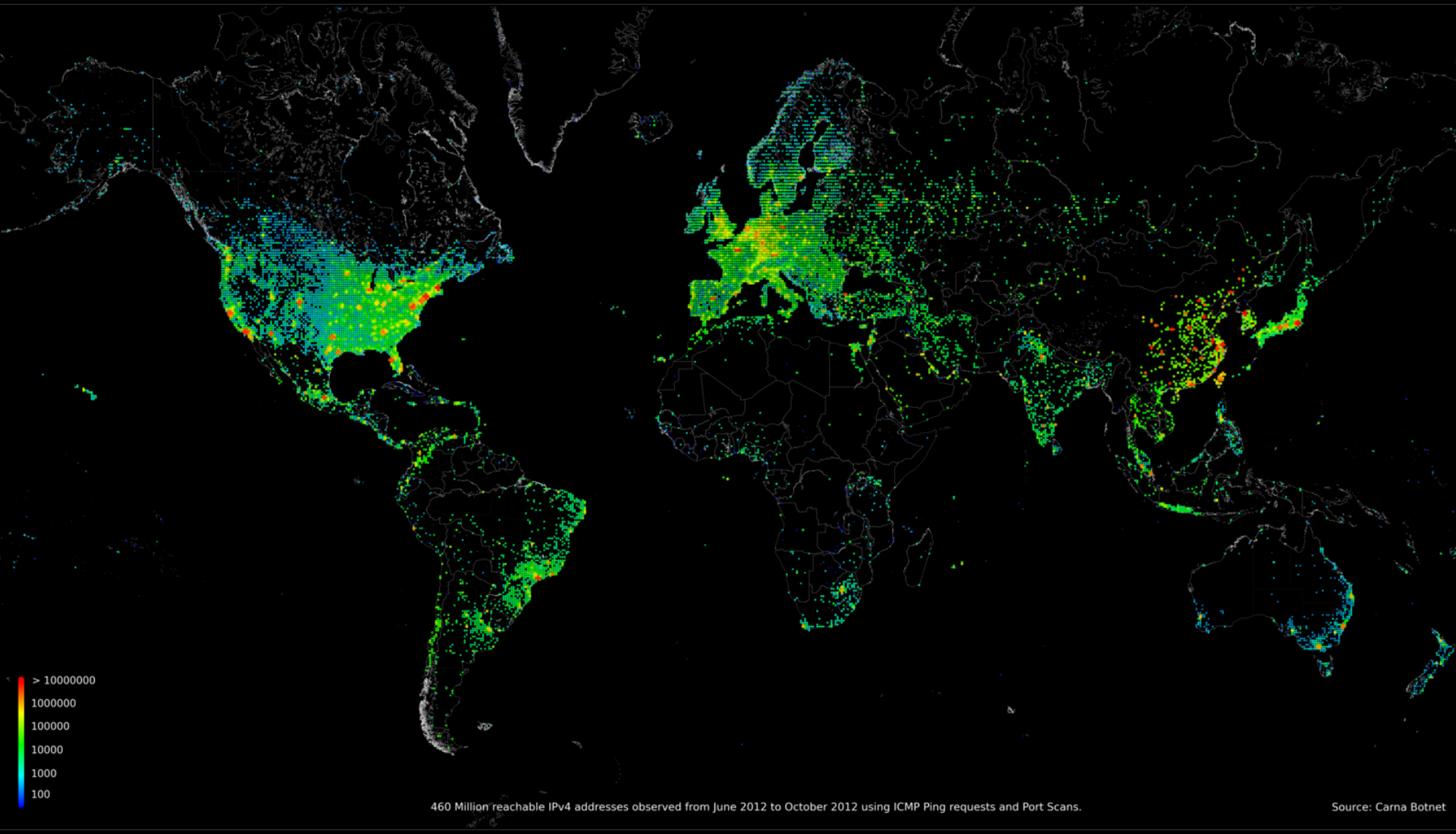
La seguretat TIC per a empreses que migren al núvol.

Valls, 27 de març

cesicat
Centre de Seguretat de la Informació de Catalunya

idigital

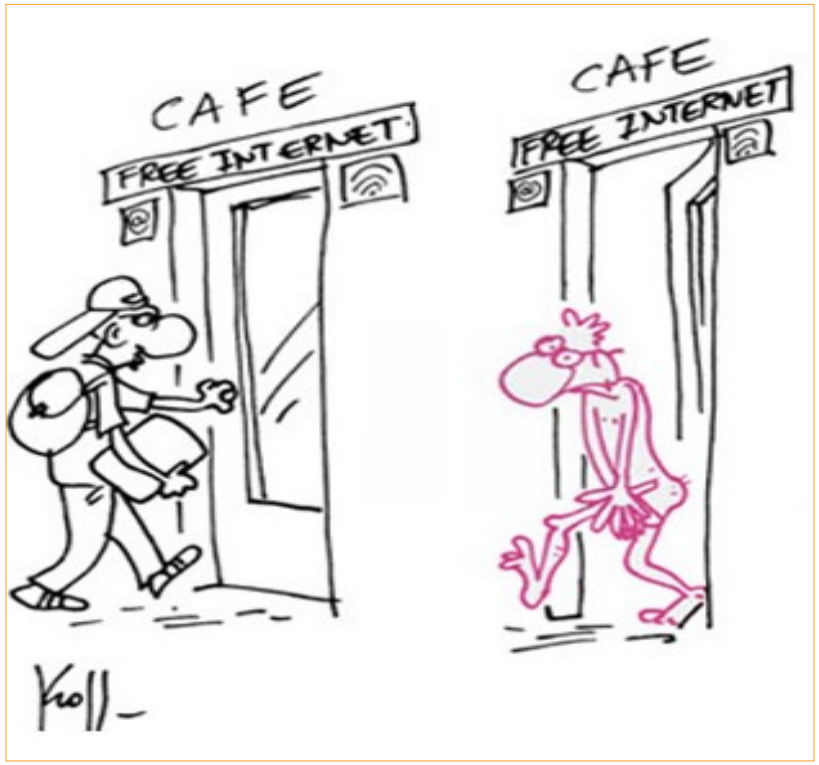
Generalitat de Catalunya



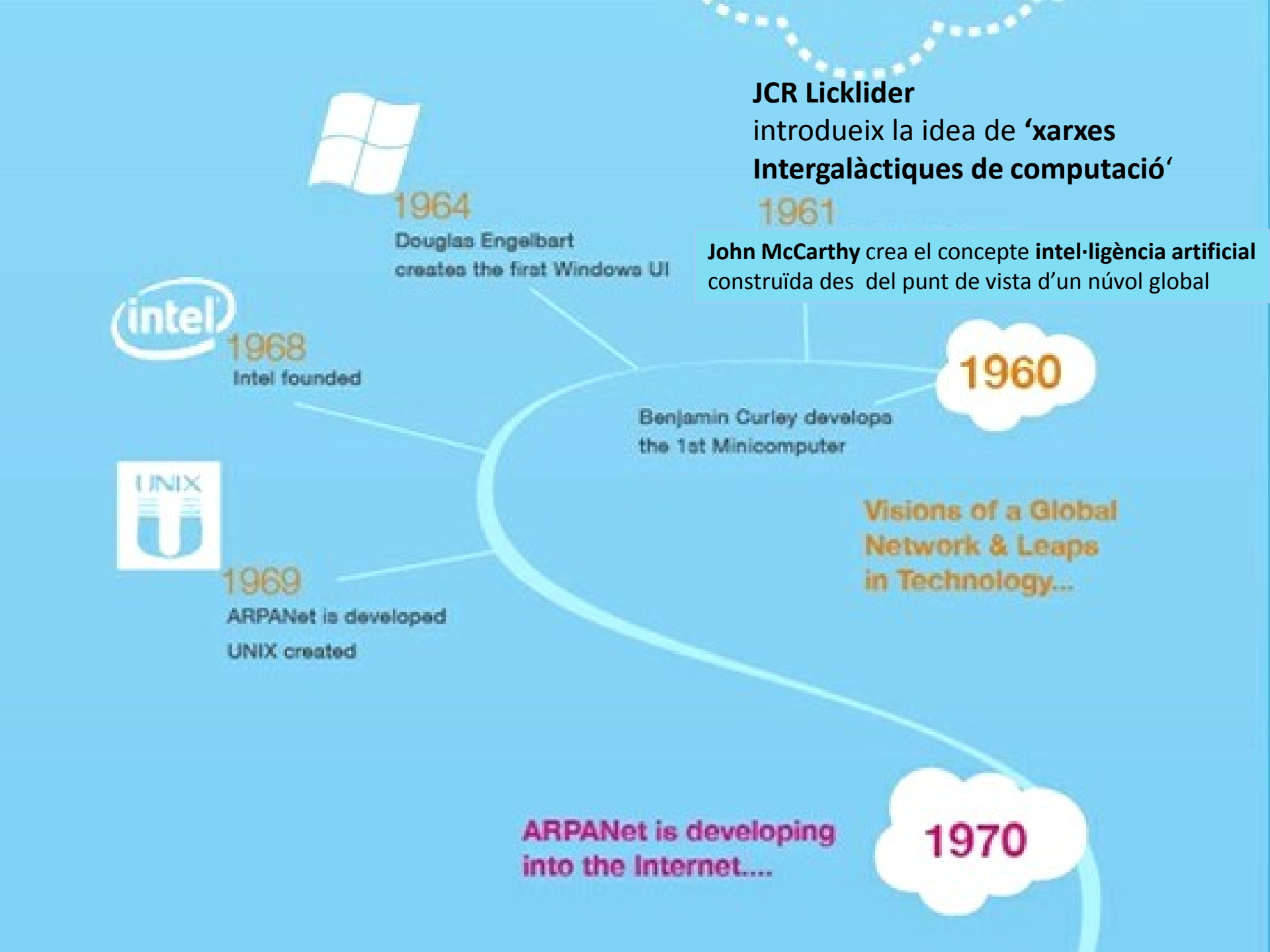
1.300 milions d'adreces IPs usades

http://internetcensus2012.bitbucket.org/paper.html (juny-octubre 2012)

Protecció de les dades personals: un dret fonamental



ec.europa.eu/justice/data-protection/


JCR Licklider
introdueix la idea de ‘xarxes Intergalàctiques de computació‘
1961
1964
Douglas Engelbart
creates the first Windows UI
John McCarthy crea el concepte intel·ligència artificial
construïda des del punt de vista d’un núvol global
intel
1968
Intel founded
1960
Benjamin Curley develops
the 1st Minicomputer
UNIX
1969
ARPANet is developed
UNIX created
Visions of a Global
Network & Leaps
in Technology...
ARPANet is developing
into the Internet....
1970

Microsoft 1974

Microsoft founded

ORACLE 1977

Oracle founded

1971

1st email sent

1976

Apple Computer founded

1980

Worldwide boom in computers...

1981

IBM launch the PC

IBM

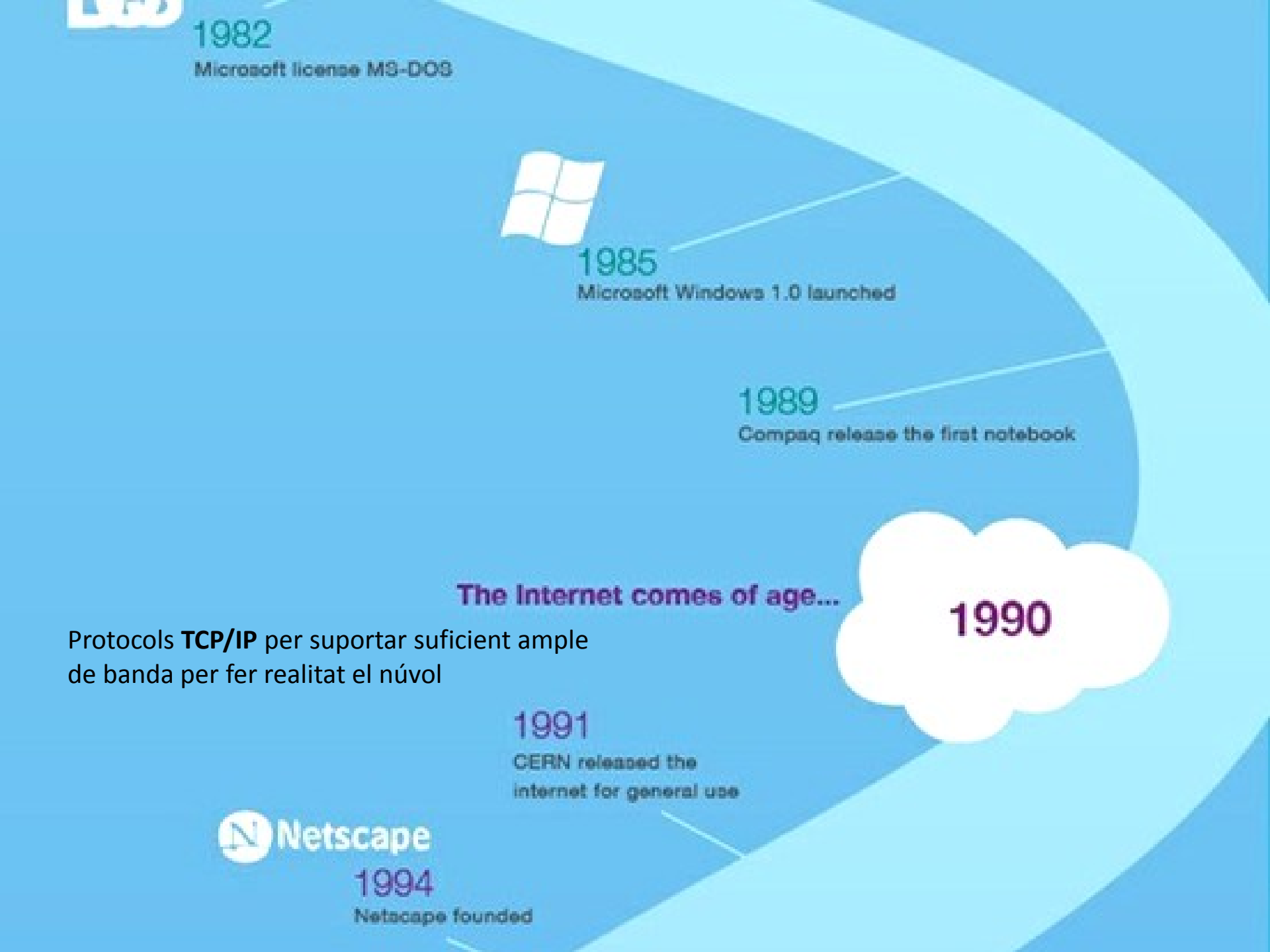
1984

Apple launch the Macintosh computer

Dell founded

The term 'Cyberspace' is coined by William Gibson

DELL



Protocols **TCP/IP** per suportar suficient ample de banda per fer realitat el núvol

Amazon comença amb els **Serveis Web** amb **AWS**, proveïnt un sistema avançat d'emmagatzemament

2004

Facebook founded

2006

Amazon launches S3 pay-as-you-go

Amazon introdueix el concepte **ELASTIC COMPUTE CLOUD EC2** (lloguer de servidors on fer córrer les aplicacions pròpies)

salesforce

2007

Salesforce launch force.com

Apple launch iPhone

2008

HTC launch the 1st Android phone

2009

Google Apps launch

2010

salesforce

Salesforce launch Database.com & Chatter

1 Million iPads sold within 28 days of launch

Samsung launch the 1st Android tablet

The Future

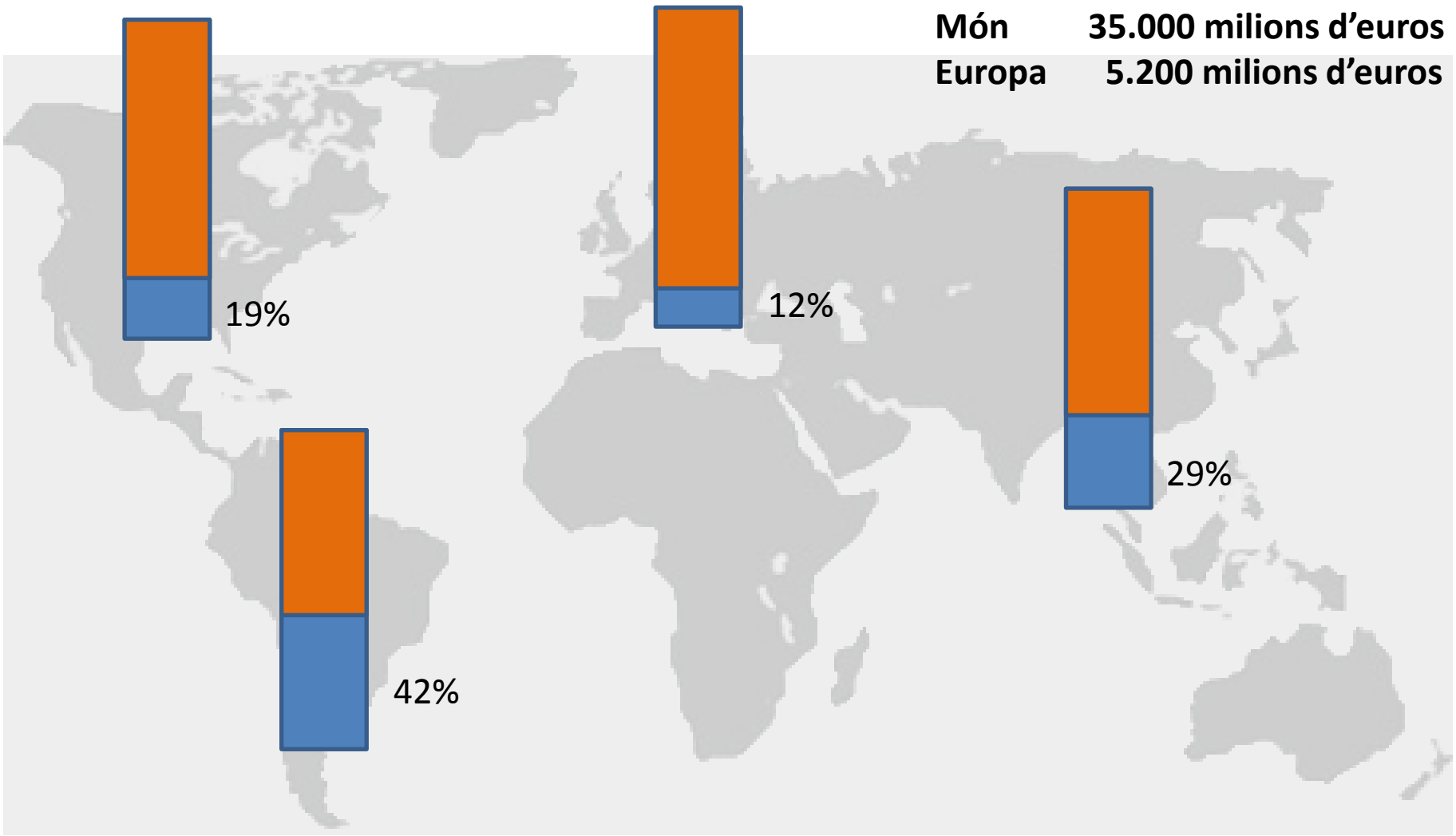
In 2013 1 billion* people will own smart phones

El *cloud* al món

Previsió any 2013

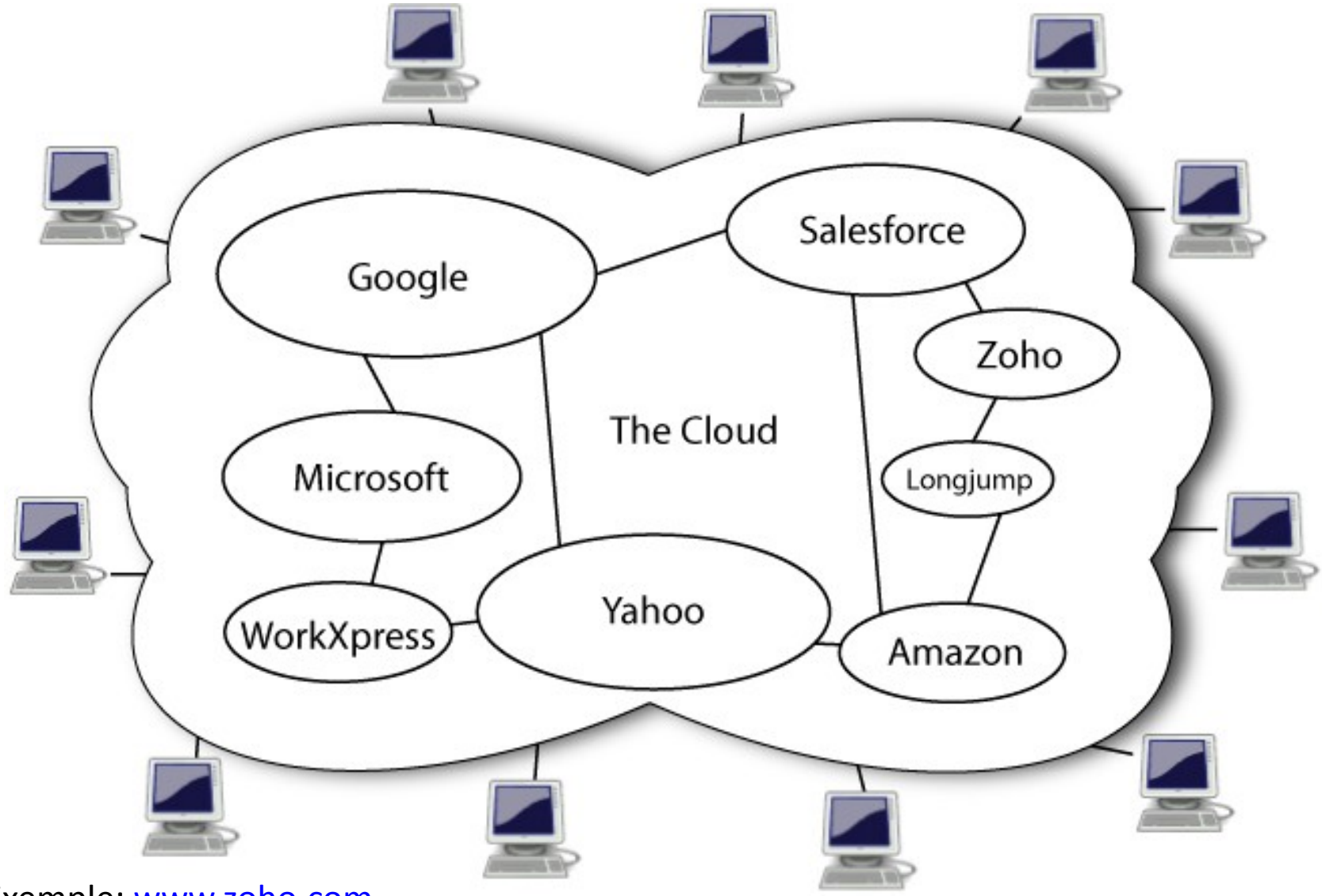
Món **35.000 milions d'euros**

Europa **5.200 milions d'euros**



FONT: [Tata Consultancy Services]

El present i el futur: aplicacions basades en web



Exemple: www.zoho.com

(diferents eines de forma gratuïta per emprenedors o miniempreses)

“Cloud computing”

Moltes empreses que han començat en els últims vint anys ho van fer en el núvol ... tan bon punt es va incorporar a Internet i de correu electrònic. L'ús comú de l'expressió, però, es refereix a desenvolupaments relativament nous:

1. **Les aplicacions o els programes com a servei (SaaS)**

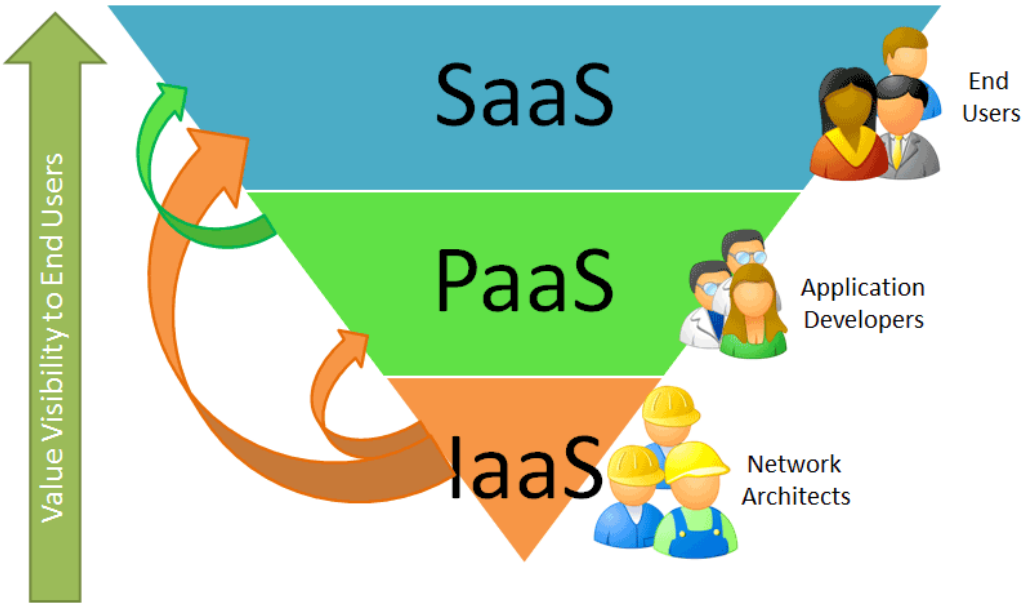
el programari que normalment s'instal·len als equips d'oficina a través d’un navegador d'Internet. “Programari allotjat" o "aplicacions allotjades. – Salesforce CRM, SugarCRM, Google Docs –

2.**Plataformes com a servei (PaaS)**

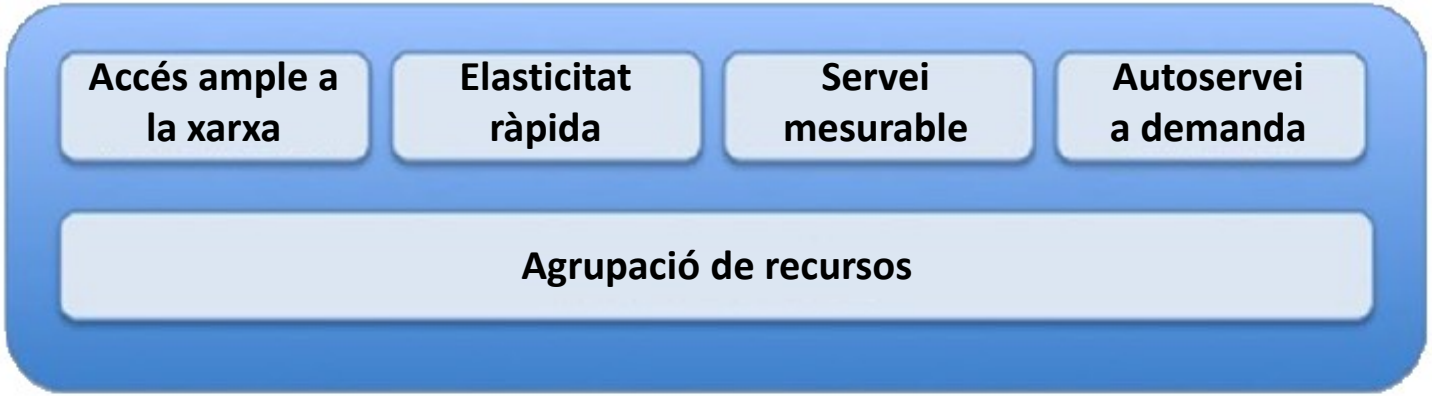
Es focalitza en poder fer-hi córrer les diferents aplicacions i llenguatges de programació que han d’interactuar (*application framework* i *runtime-system*).
– Microsoft Azure, Force i App Engine de Google –

3. **La infraestructura com a servei (IaaS)**

llogar espai en un centre de dades i l'ús dels seus servidors en lloc de comprar un nou maquinari per gestionar dins de l’empresa.
– Amazon EC2 i S3, Enterprise Cloud, Windows Live Skydrive, hosting –



Característiques principals



Models de servei

Models de desplegament

Els serveis disponibles

IaaS	PaaS	SaaS
✓ Emmagatzematge ✓ Xarxes de subministrament de continguts ✓ Còpia de seguretat i recuperació ✓ Gestió de serveis ✓ Plataforma d'allotjament ✓ Computació ✓ altres serveis	✓ Bases de dades ✓ *Business Intelligence* ✓ Desenvolupament i proves ✓ Integració ✓ Desplegament d'aplicacions ✓ altres serveis	✓ ERP ✓ Recursos humans ✓ Facturació ✓ Vendes ✓ CRM ✓ Gestió de continguts ✓ altres serveis

Cas pràctic FCB

FCBARCELONA
més que un club

Els reptes

Un dels principals productes gnuine és **Ubiquo Sports,** especialitzat en gestió de continguts (CMS) SaaS centrat en la solució de les necessitats específiques per a organitzacions esportives que s'executa per complet a la plataforma Amazon Web Services (AWS).

Per què Amazon Web Services

Lluís Alsina *FCBarcelona Manager Online*, diu que va decidir utilitzar AWS basat en l'elasticitat i el model de pagament per ús. **Ramon Salvadó, director de tecnologia de gnuine**, es va mostrar satisfet amb aquesta decisió. Ell comenta: "Ja teníem un munt d'experiència amb AWS de diversos projectes anteriors, tots amb bons resultats." I afegeix: "L'expansió, l'aprovisionament i la seguretat són molt importants per a nosaltres i per als nostres clients. AWS és un pas natural, ja que ens permet disposar d'una capacitat pràcticament il·limitada, mentre que només paga pel que fem servir sense inversions inicials. AWS també fa que sigui fàcil per fer front als pics de trànsit, que són comuns a esports, gràcies a les seves capacitats elàstiques. "

The Business Benefits

The Gnuine solution for FCBarcelona uses a number of AWS products:
***Amazon Route 53** for name resolution.*
***Amazon CloudFront** as a content delivery network (CDN) for fast media and assets delivery.*
***Amazon Simple Storage Service** (Amazon S3) for scalable assets and media documents storage.*
***Amazon Elastic Compute Cloud** (Amazon EC2) with **Amazon Elastic Load Balancing** (Amazon ELB) and Auto Scaling for dynamic generated HTML and XML pages.*
***Amazon CloudWatch** for alarms and service monitoring.*
***Amazon Simple Notification Service** (Amazon SNS) for several platform notifications.*
***Amazon Relational Database Service** (Amazon RDS) as a database service (MySQL).*
***Amazon CloudFormation** for automation and provisioning.*

http://aws.amazon.com/es/solutions/case-studies/futbol-club-barcelona/

El canvi cultural

Com canvia la forma de subministrar els serveis i els productes?

Un canvi d'enfocament

Un canvi de mentalitat, dirigida per un fort desig de tots nosaltres per tenir accés a la informació que volem quan més ho necessitem, en qualsevol moment i en qualsevol lloc.

1.Des del punt de vista del client

La demanda de consum de tecnologia és com una *utility*, mantenint un avantatge competitiu i maximitzant el retorn de les inversions.

El canvi a Cloud modifica les expectatives del client. Els clients volen resultats més ràpids.

Ser capaços de contractar un servei i començar a utilitzar-lo.

2. Des del punt de vista empreses TIC

L'impacte s'estén des de les eines de productivitat fins les aplicacions empresarials.

El programari es transforma en una despesa operativa mensual i no en una costosa inversió amb un procés d'implementació complex.

La forma en què pensem i fem servir el programari ha canviat per sempre.

Transforma la manera que aportem valor als nostres clients.
Ajusta les nostres percepcions i la forma d'operar.
Per augmentar els beneficis, es requereix desenvolupar un millor model empresarial que aposti per créixer i ser sostenible a llarg termini.

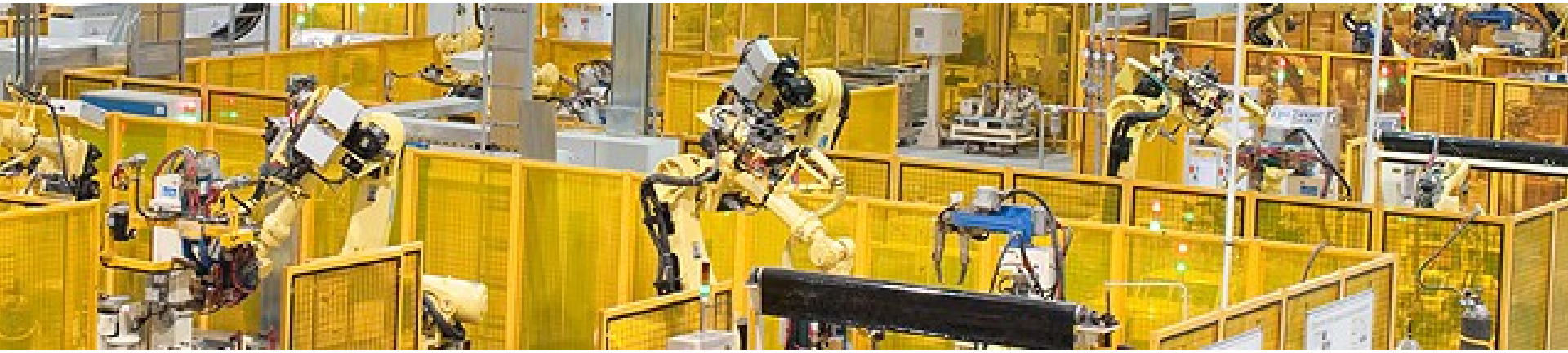
Beneficis que aporta:

- **mobilitat en el treball (46%)**
- **la productivitat (41%)**
- **l'estandardització (35%)**
- **noves oportunitats de negoci (33%)**
- **nous mercats (32%)**

Confidencialitat, integritat i disponibilitat

Com sortiria perjudicada l'empresa si ...

1. l'actiu estigués públicament accessible i disponible?
2. un treballador del proveïdor de *Cloud* accedís a l'actiu?
3. el procés fos alterat per algú extern?
4. el procés o funció no proporciona els resultats esperats?
5. la informació o les dades s'alteren de manera inesperada?
6. l'actiu no està disponible durant un temps?



Els riscos

1. **Accés dels usuaris amb privilegis**

   Mantenir la informació confidencial amb els tercers té riscos inherents, ja que es pot passar per alt la infraestructura TI d'aquesta empresa i el seu equip de suport.

2. **Compliment de normatives**

   Els clients són responsables de la seva pròpia seguretat i de la integritat de les dades.

3. **La localització de les dades**

   No sabeu on es troba emmagatzemada físicament la informació, pot ser a qualsevol lloc del món.

4. **Segregació de dades**

   Les dades es guarden juntament amb les dades d'altres empreses i una errada de programes podria fer que les dades quedessin completament inservibles.

5. **Recuperació**

   Què succeeix en cas de desastre? Les dades estan replicades?

6. **Suport a la investigació**

   Les activitats inapropiades o il·legals poden ser difícils o impossible d'investigar.

7. **Viabilitat a llarg termini**

   Què passa si el proveïdor es ven o entra en fallida?

Analyst firm Gartner identifica set riscos percebuts en el *cloud computing*:

L'elecció d'un proveïdor al núvol

Podem triar per allotjar aplicacions i infraestructura de manera selectiva en el núvol o optar per un proveïdor que ofereix una oferta de núvol global

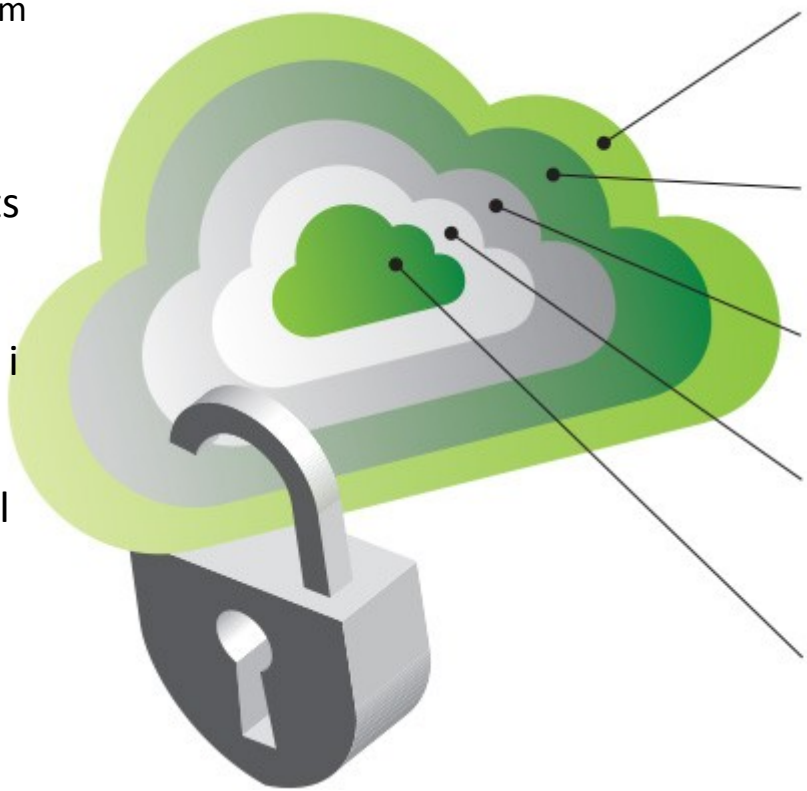
- **Preguntar abans a coneguts, proveïdors, organitzacions professionals i altres empreses què utilitzen.**
- **Realitzar una recerca/comparació dels diferents "serveis en el núvol"**. Cal cercar:
  - Evidències de l'experiència que tenen.
  - Algú que pugui ajudar a tant si creixem com si canvien les necessitats.
  - La confiança que són gent que entenen els requeriments i el tipus de negoci.
  - Tenim referències.
  - Que aborden els problemes de manera que els poden entendre.
  - Les empreses tenen recursos suficients per satisfer totes les necessitats.
- **Contractes de *Cloud*** *"take-it-or-leave-it" standard contracts*
  Necessitem contractes per escrit amb clàusules que defineixin de forma clara:
  - Què és exactament el que faran per nosaltres (i què esperen que fem nosaltres).
  - Un calendari per a qualsevol projecte de treball que es durà a terme (per exemple, quant de temps es triga a instal·lar un servidor nou).
  - Un acord de nivell de servei (SLA o ANS)- quant de ràpid respondran i com es resoldran els problemes. Quina disponibilitat necessitem? (24x7? Són negociables?)
  - Qui i com assumeix responsabilitats en matèria de seguretat.
  - Una estructura de tarifes clares.

http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

Bones pràctiques de seguretat al *cloud*

Els proveïdors de serveis al núvol han d'adoptar pràctiques integrals de seguretat i procediments, que incloguin com a principis:

- ❑ Criteris de seguretat reconeguts, transparents i verificables.
- ❑ Robustesa en la identitat, d'autenticació i mecanismes de control d'accés adaptats o que es corresponguin amb el nivell de sensibilitat de les dades.
- ❑ Proves completes i permanents de les mesures de seguretat abans i després de la implementació.



D-DOS Prevention

Monitors and controls specific network patterns related to D-DOS attacks and allows source IP to be deactivated without impacting site.

Web Application Firewall

Firewall specifically designed to control and monitor web site traffic.

Intrusion Detection (IDS)

Monitors all network traffic within savvisdirect DMZ for malicious patterns of activity.

Continual Vulnerability Scans

Internal and External penetration and vulnerability scans to proactively identify unprotected areas of the system.

Continual Source Code Scans

Developed source code is continually scanned to assure best practice coding structures. Immediate feedback is given to developers.

Seguretat física, inherent a les característiques del propi centre de dades 24x7 biomètrica, i seguretat lògica al quedar integrada en la plataforma de seguretat integral (p.e. PCI CyberSource de procés targetes de crèdit)

Avaluar el ROI i el ROSI del *cloud*

Les empreses determinen el benefici d'una inversió en funció del **retorn de la inversió (ROI)** que reben. En general es calcula que hi ha reduccions de cost d'entre 10-20% respecte model tradicional. No obstant això, aplicar criteris purament monetaris a la inversió en seguretat de la informació és poc pràctic, ja que els beneficis associats a la inversió en seguretat no tenen una traducció comptable directa.

Una inversió en seguretat és rendible si l'efecte de mitigació del risc és més gran que els costos estimats.

Els beneficis de la implantació de seguretat en una empresa cal mesurar-los més en funció de la reducció de les pèrdues que produeixen en evitar o mitigar els incidents de seguretat, més que dels beneficis econòmics que generen. Per poder quantificar aquest benefici, es defineix el **retorn sobre la inversió en seguretat (ROSI)**.

El ROSI permet d'identificar quant s'estalviaria o deixaria de perdre una empresa gràcies a la implantació d'un sistema de seguretat que mitigués els efectes dels incidents de seguretat.

VALOR DE LES MESURES DE PROTECCIÓ (V) =
PÈRDUES CAUSADES PELS INCIDENTS SENSE TRACTAR (PST) -
PÈRDUES CAUSADES PELS INCIDENTS MITIGATS O EVITATS (PSM)

COST DE LES MESURES DE PROTECCIÓ (C) =
INVERSIÓ INICIAL EN MESURES (IM) +
INVERSIÓ PERIÒDICA (IP)

$$\textbf{ROSI} = \frac{\textbf{(VALOR - COST)}}{\textbf{COST}}$$

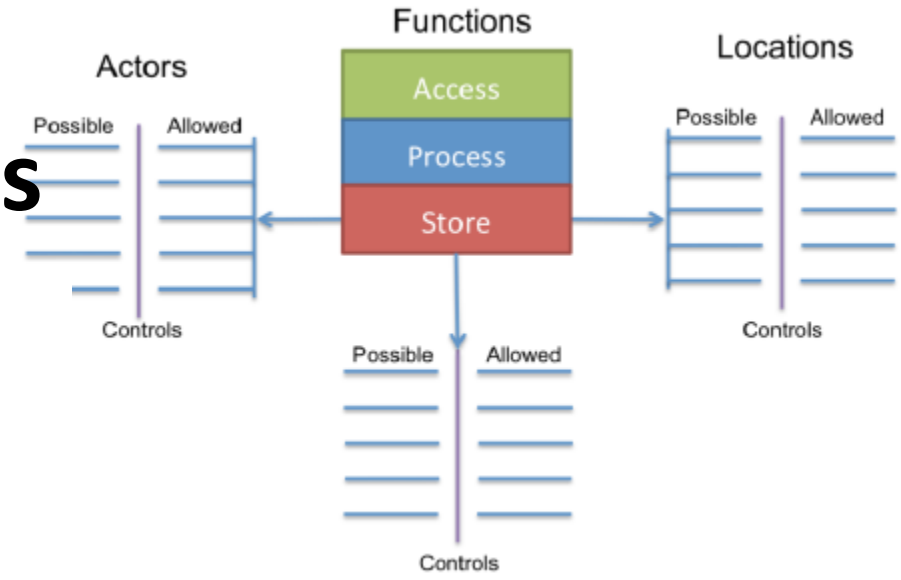
Si el VALOR és superior al COST (ROSI > 0)
el ROSI és acceptable.

Annualized Lost Expectancy (ALE)

http://www.iso27001standard.com/es/rosi/return-on-security-investment

cesicat Centre de Seguretat de la Informació de Catalunya
idigital Generalitat de Catalunya

Cicle de vida de la seguretat de les dades



Govern de la informació

Classificat informació **> P**olítiques de gestió **>** de **L**ocalització i legalitat **> A**utoritzacions i permisos **> P**ropietat **> C**ustòdia

Gestió de les dades

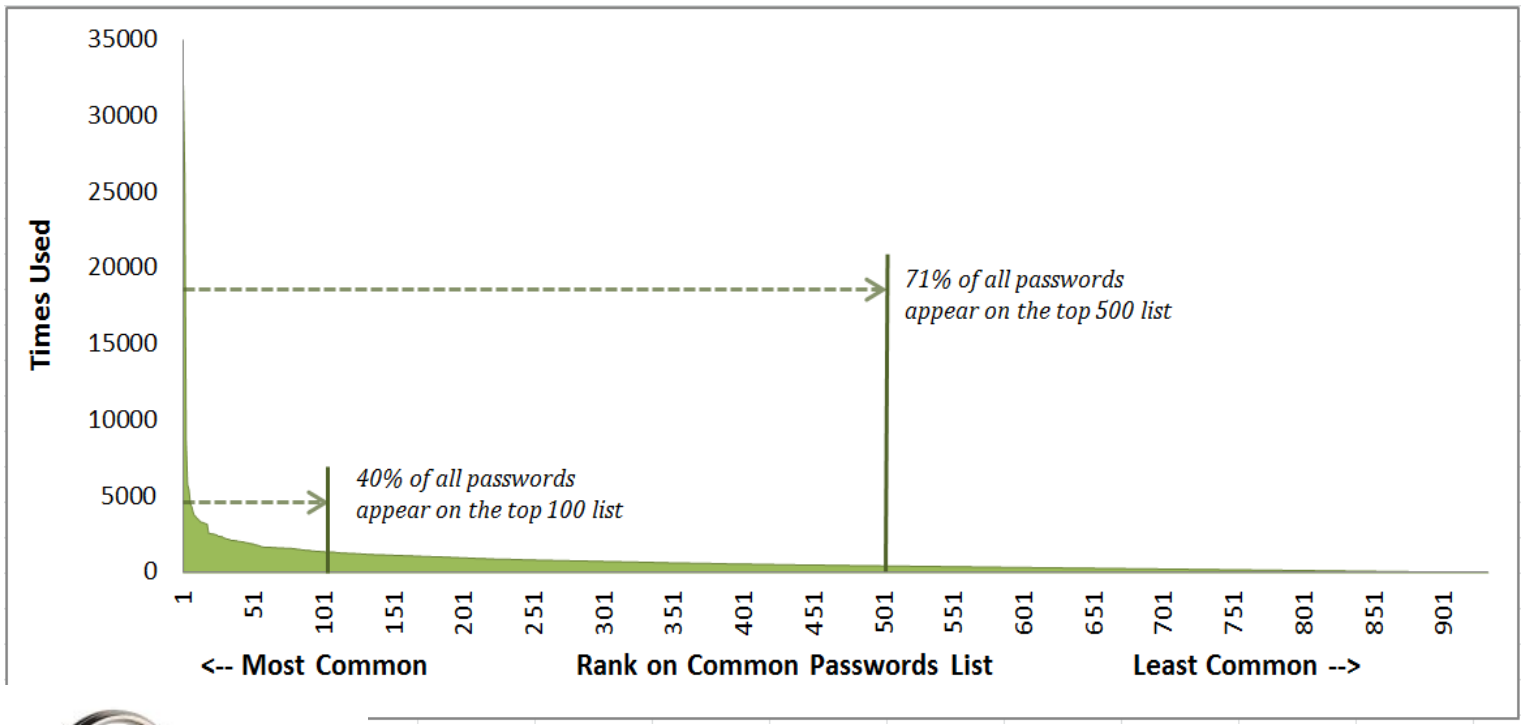
-Monitorar l'existència de moviments interns de dades amb eines de monitoratge d'activitat de bases de dades **(DAM)** i d'activitat d'arxius **(FAM)**

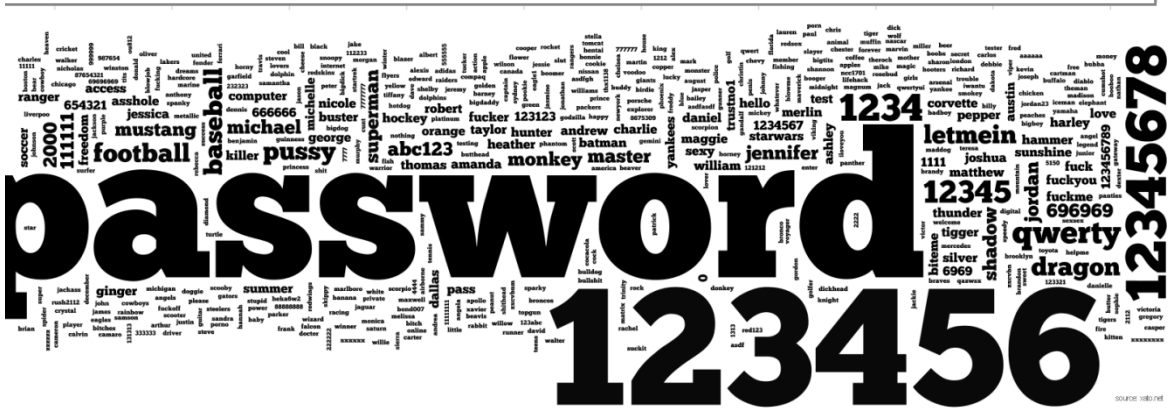
-Monitoratge de migració de dades a Cloud amb filtres URL i eines *Data Loss Prevention*

Polítiques de credencials dels usuaris i adm.

TOP25 WORST >20%casos

password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball
football
letmein
monkey
696969
abc123
mustang
michael
shadow
master
je
11
2(
jo
su
ha
12





cesICAT
Centre de Seguretat de la Informació de Catalunya

idigital

Generalitat de Catalunya

Protegir la migració de dades cap el (o dins el) *Cloud*

En les implementacions de *Cloud públiques i privades, i a través dels diferents models de servei, és important protegir les dades en trànsit.*

Això inclou:

- Les dades que es mouen des de la Infraestructura tradicional als Proveïdors Cloud, incloent Públic / Privat, interior / exterior.
- Les dades migrant entre els proveïdors de Cloud.
- Les dades que es mouen entre instàncies.

Hi ha tres opcions:

1. Xifrat client/aplicació

Les dades són xifrades en l'extrem o en el servidor abans d'enviar-se per la xarxa o ja emmagatzemats en un format de xifrat adequat. Això inclou el xifrat en el client local, per exemple per a arxius emmagatzemats, o el xifrat integrat en aplicacions.

2. Xifrat enllaç/xarxa

Tècniques de xifrat de xarxa estàndard incloent SSL21, VPNs22, i SSH23. Pot ser maquinari o programari. És preferible extrem a extrem però pot no ser viable en totes les arquitectures.

3. Xifrat basat en Proxy

Les dades són transmeses a un servidor dedicat o servidor proxy, en xifra les dades abans de ser enviades per la xarxa. És l'opció escollida freqüentment per a la integració amb aplicacions *legacy però no es generalment recomanable.*

http://www.ismsforum.es/ficheros/descargas/guia-csa1354629608.pdf

98 controls del Cloud Controls Matrix (seguiment de l'ENS en entorn cloud i RLOPD)
http://www.ismsforum.es/ficheros/descargas/version-espanola-del-cloud-control.xlsx

GUÍAS DE SEGURIDAD DE ÁREAS CRÍTICAS EN CLOUD COMPUTING V3.0

ISACA®
Serving IT Governance Professionals

- **Per què interessa el *cloud* a les empreses?**
- ***Due diligence* prèvia a la contractació de serveis en el núvol**
- **Efectes del *cloud* sobre el marc de control de TI**
- **Implicacions del *cloud* sobre la seguretat**
- **Guia per avaluar els serveis en el núvol**
- **Visió global de normes i estàndards aplicables al *cloud computing***

FORMACIÓ VIRTUAL ISAKA (8 hores)
Abril 2013 http://isacamadrid.stagehq.com/events/2082

Com desenvolupar el model de negoci en cloud computing i la transició de les empreses

- ✓**Reduir els temps d'activació**
- ✓**Optimitzar les inversions**
- ✓**Obtenir estalvis dels costos**

Autor: Nimboesfera

http://www.nimbosfera.com/ver-noticia/como-desarrollar-el-modelo-de-negocio-en-cloud-computing-guia-para-empresas-tics

cesicat Centre de Seguretat de la Informació de Catalunya
idigital
Generalitat de Catalunya

L'empresa i la seguretat de la informació

- Cultura empresarial
- Planificar abans d'actuar
- Analitzar els riscos
- Continuïtat del negoci
- Política de seguretat
- Infraestructura tècnica
- Suport tècnic qualificat
- Còpies de seguretat

http://www.idigital.cat/documents/10501/34386/guia_seguretat-cambra-idigital.pdf

Gràcies per la vostra atenció!

Servei d'orientació per pimes digital

Correu electrònic per a consultes

info@cesicat.cat

Telèfon d'informació

977 010 893

Telèfon d'emergència

902 112 444

www.cesicat.cat

www.idigital.cat/web/seguretat

@cesicat

cesicat Centre de Seguretat de la Informació de Catalunya

idigital

Generalitat de Catalunya