El paper d'IT dins de Maldecap Medicaments S.A

Nom: Joan Borràs Llossas
Grau d'Enginyeria Informàtica

Consultor: Manuel Jesús Mendoza Florez

8/6/2016

FITXA DEL TREBALL FINAL

Títol del treball:	El paper d'IT dins de Maldecap Medicaments S.A
Nom de l'autor:	*Joan Borràs Llossas*
Nom del consultor:	*Manuel Jesús Mendoza Flores*
Data de lliurament (mm/aaaa):	*06/2016*
Àrea del Treball Final:	*Administració de Xarxes i S.O*
Titulació:	*Grau d'Enginyeria Informàtica*

Resum del Treball (màxim 250 paraules):

El present projecte pretén realitzar un anàlisi de la situació actual d'un departament d'IT dins d'una companyia i realitzar una proposta de millora.

El departament d'IT és molt petit i té un rol de proveïdor de serveis de tecnologia fonamentals, amb la majoria de serveis en mans de proveïdors i les seus treballant de manera independent.

L'objectiu del projecte és realitzar un anàlisi de la situació actual, que serveixi com a punt de partida per al CIO de la companyia de cara a la realització el pla estratègic dels Sistemes d'Informació de la companyia.

Aquest estudi es basarà en tres grans pilars:

1- Organitzatiu (replantejament del paper d'IT a la companyia)
2- Tècnic (re-definició tècnica a nivell de sistemes)
3- Econòmic

Cal esmentar que aquest no pretén ser un pla estratègic, sinó un estudi extern que servirà de base per al pla estratègic, necessari per a qualsevol companyia

Abstract (in English, 250 words or less):

This project aims to make an analysis of the current situation of an IT department within a company and to make a proposal for improvement.

The IT department is not well sized and most of their services are externalized and their offices are working independently.

The aim of the project is to perform an analysis of the current situation, to bring a tool to company's CIO in order to complete the strategic plan for information systems of the company.

This study is based on three pillars:

1- Organizational (rethinking of the role of IT in the company)

2. Technical (re-defining technical skills)

3- Budget

It should be mentioned that this is not a strategic plan, but an external study as a starting point for the strategic plan (needful for any company)

Paraules clau (entre 4 i 8):

Pla Estratègic de Sistemes d'Informació
Auditoria
Pla de millora
Anàlisi tècnic
Rol de les TI

Índex

1. Introducció 1
1.1 Context i justificació del Treball 1
1.2 Objectius del Treball 1
1.3 Enfocament i mètode seguit 1
1.4 Planificació del Treball 1
1.5 Breu sumari de productes obtinguts 3
1.6 Breu descripció dels altres capítols de la memòria 3
2. Anàlisi Organitzatiu 4
2.1 Breu Història de la companyia 4
2.2 El departament d'IT dins la companyia 5
3. Anàlisi Tècnic 8
3.1 Xarxa local 8
3.2 Xarxa Wi-Fi 13
3.3 Infraestructura de servidors 14
3.4 Còpies de Seguretat 15
3.5 Eines col·laboratives 16
3.6 Eines de suport d'IT 16
3.7 Altres consideracions 17
4. Anàlisi de Riscos 18
3.1 Xarxa Local 18
3.2 Xarxa Wi-Fi 19
3.3 Infraestructura de servidors. 19
3.4 Còpies de seguretat 20
5. Conclusions de l'estudi inicial 22
5.1 Aspectes organitzatius [5] 22
5.2 Xarxa Local 22
5.3 Xarxa Wi-Fi 23
5.4 Infraestructura de servidors 23
5.5 Còpies de seguretat 23
5.6 Eines Col·laboratives 23
5.7 Eines de Suport a IT 24
6. Proposta de Millora 25
6.1 Organitzatiu 25
6.2 Xarxa local 25
6.3 Xarxa WiFi 31
6.4 Còpies de seguretat 33
6.5 Eines Col·laboratives 35
6.6 Eines de suport a IT 37
7. Conclusions 40
8. Glossari 41
9. Bibliografia 43
10. Annex1: Metodologia Anàlisi de riscos 44
10.1 Metodologia 44
10.2 Avaluació de Riscos 44
10.3 Classes de Risc 44
10.4 Nivell de Risc 45
10.5 Matriu d'Anàlisi de riscos 45
11. Annex 2: Disseny de xarxes locals 47
11.1 Topologia 47
11.2 Divisió dels equips per grups (subxarxes) 47

11.3 VLANs 48
12. Annex 3: Estàndards Wi-Fi 49
13. Comparativa de fabricants 50
13.1 Xarxa local 50
13.2 Xarxa Wifi 51
13.3 Còpies de seguretat 54

Llista de taules

Taula 1: Evolució del personal 4
Taula 2: Sistema de backup 15
Taula 3: Vlans i adreçament de BCN 26
Taula 4: Vlans i adreçament de Toledo 27
Taula 5: Vlans i Adreçament de Madrid 27
Taula 6: Estàndars Wi-Fi 49
Taula 7: Comparativa fabricants de commutadors 51
Taula 8: Comparativa costos de commutadors 51
Taula 9: Comparativa fabricants WiFi 52
Taula 10: Comparativa costos de WiFi 53
Taula 11: Comparativa programari de Còpies de Seguretat 55

Llista de figures

Figura 1: Diagrama de Gantt 2
Figura 2: Evolució del personal 5
Figura 3: Rati usuaris per tècnic d'IT 6
Figura 4: Organigrama 7
Figura 5: Xarxa interna. Seu de Barcelona 9
Figura 6: Esquema de connexió intersite 13
Figura 7: Infraestructura ESX. Font: VmWare 14
Figura 8: Proposta xarxa interna. Seu de Barcelona 28
Figura 9: Proposta xarxa interna. Seu de Madrid 29
Figura 10: Proposta xarxa interna. Seu de Toledo 30
Figura 11: Tipologia de còpies de seguretat 34
Figura 12: Eines ITSM 38
Figura 13: Topologia de xarxa segons Cisco 47
Figura 14: Principals fabricants de commutadors 50
Figura 15: Quadrant de Gartner 2015 - Wireless 52
Figura 16: Quadrant de Gartner 2015 - Programari de Còpies de seguretat 55

1. Introducció

1.1 Context i justificació del Treball

El present document parteix d'una situació molt concreta d'un departament d'IT d'una companyia del sector farmacèutic.

Cal esmentar que aquest no pretén ser un pla estratègic, sinó un estudi extern que ha de servir al CIO de la companya com a punt de partida per al pla estratègic. Es per aquest motiu que no s'han incorporat al treball un anàlisi de processos ni objectius estratègics.

El resultat d'aquest estudi, serà la d'analitzar la situació global del departament d'IT dins la companyia i oferir possibles alternatives per tal d'optimitzar els recursos i els sistemes

1.2 Objectius del Treball

Els principals objectius d'aquest projecte son:

- Entendre el paper d'IT dins d'una organització concreta
- Analitzar la situació organitzativa i tècnica del departament
- Realitzar un proposta de millora dels sistemes d'Informació que serveixi de base al CIO de la companyia per a la realització del pla estratègic de Sistemes d'informació

1.3 Enfocament i mètode seguit

Aquest treball s'ha desenvolupat realitzant un estudi d'una situació inicial hipotètica del departament de sistemes d'informació d'una companyia.
L'objectiu és oferir un pla de millora tècnica i organitzativa que serveixi de punt de partida per a poder realitzar el pla estratègic de sistemes d'informació.

Per a poder realitzar aquest estudi, primer de tot calia fer un anàlisis exhaustiu del departament i la organització, tan a nivell tècnic com organitzatiu.

Un cop analitzats, es detecten aquells punts de millora o que suposen un risc per a la companyia. La millor manera per a detectar aquests punts clau és mitjançant l'anàlisi de riscos.

Basant-nos en l'anàlisi de riscos, es realitza la proposta de millora.

S'ha separat en diferents annexos, aquells punts que, tot i ser necessaris per al treball, no son el nucli del mateix

1.4 Planificació del Treball

Per a la realització d'aquest projecte seran necessaris els coneixements adquirits al llarg de tot el Grau, especialment les assignatures d'*Administració de xarxes i Sistemes Operatius, Administració i gestió d'organitzacions, Competència comunicativa per a professionals de les TIC, Fonaments de sistemes d'Informació, Planificació i ús estratègic de SI i Seguretat en xarxes de computadors*.

Les tasques a realitzar, a grans trets son les següents:

Tasca 1: Anàlisi de la situació actual
Aquesta tasca pretén estudiar la situació del departament d'IT dins de l'organització, realitzar un estudi tècnic dels sistemes actuals i un breu estudi sobre la situació econòmica actual.
Sens dubte, aquesta serà la tasca més important, donat que una bona presa de requeriments ens podrà dur a unes solucions adequades a les necessitats, mentre que una mala presa de decisions segur que ens durà al fracàs del projecte.
L'objectiu d'aquesta tasca és entendre la situació del departament, la seva història i tenir una fotografia el més complerta possible per tal de prendre les decisions més correctes

Tasca 2: Anàlisi de riscos
Aquesta tasca pretén detectar els riscos i les amenaces a partir de l'anàlisi de la situació actual. Aquest anàlisi ens permetrà avaluar el nivell de risc i extreure conclusions de cara al plantejament d'alternatives

Tasca 3: Conclusions de la situació actual
Durant aquesta tasca es desgranaran tots aquells punts d'ineficiència detectats durant l'anàlisi previ.
L'objectiu principal d'aquesta tasca és descriure tots aquells punts que seran la base de les següents tasques, i en definitiva, del projecte.

Tasca 4: Estudi d'alternatives
Durant aquesta tasca es realitzarà un estudi dels diferents punts trobats i descrits en la tasca anterior buscant diferents solucions a la problemàtica
L'objectiu d'aquesta tasca és documentar-se sobre les diferents opcions existents per a la problemàtica i oferir-ne un parell o tres indicant els pros i contres de cadascuna, així com el cost i les implicacions

Tasca 5: Pla de millora
Aquesta última tasca consisteix en plasmar les conclusions en forma de proposta formal.
L'objectiu d'aquesta tasca és realitzar un document formal en forma de proposta de millora per tal de presentar-lo a direcció.

La planificació es mostra en el següent diagrama de Gantt:

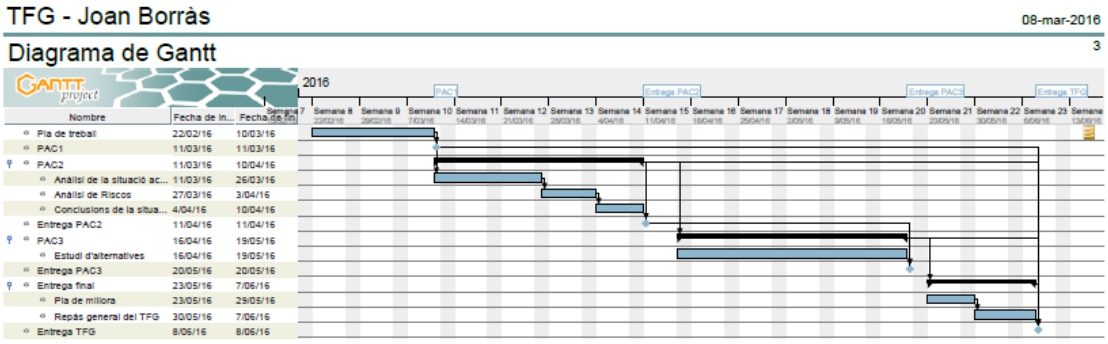


Figura 1: Diagrama de Gantt

1.5 Breu sumari de productes obtinguts

El resultat obtingut és un document amb dos grans blocs diferenciats:

1- Anàlisi objectiu de la situació departament dins la organització
2- Proposta de millora tècnica i organitzativa per al departament

Aquest document servirà per entendre les mancances i riscos de la situació actual, tant tècnica com organitzativa, conèixer els riscos actuals i serà un guia per al CIO per a establir les prioritats del departament i poder desenvolupar un pla estratègic dels sistemes d'informació dins la companyia

1.6 Breu descripció dels altres capítols de la memòria

Aquest treball està dividit en dos grans blocs lògics:

1- **Anàlisi de la situació actual**: a on es realitza un acurat anàlisi tant tècnic com organitzatiu de la situació del departament d'IT. Dins d'aquest bloc hi trobem els capítols 2, 3, 4 i 5

2- **Proposta de millora:** Aquest bloc, pretén ser una guia a on es proposen una sèrie d'alternatives tècniques i organitzatives per tal d'optimitzar el rendiment i el nivell de servei del departament

2. Anàlisi Organitzatiu

Per a poder realitzar un acurat anàlisi de la situació en la qual es troba la companyia, és necessari entendre la companyia i cóm ha arribat fins a la situació actual.

2.1 Breu Història de la companyia

L'empresa *Maldecap Medicaments S.A* és una empresa de capital principalment familiar fundada l'any 1930 .

Els inicis es van gestar a la rebotiga d'una petita farmàcia a un barri de Barcelona, realitzant fórmules magistrals.

Poc a poc, va anar creixent, principalment gràcies a la compra de laboratoris (fins a 7 durant els seus 85 anys d'història) fins arribar a l'any 2016 a ser una de les principals farmacèutiques del país amb una facturació que frega els 200 milions d'euros, més de 700 treballadors i 8 centres distribuïts per la geografia europea.

Però aquest creixement no ha estat igual per a tots els departaments, prioritzant la producció i destinant menys recursos a departaments de suport corporatius com poden ser IT.

La companyia disposa de 7 centres distribuïts per la geografia europea (entre centres de producció, logístics i oficines), sent les ciutats a on es troben aquests centres:

- Barcelona: Seu central i on resideixen els serveis corporatius com IT
- Toledo: On hi ha un centre logístic i un centre de producció
- Madrid: on hi tenen oficines per a la part de Màrqueting i vendes
- Dinamarca: hi ha un centre de producció
- Mònaco: oficines per a la gestió d'una part del port foli de productes

L'evolució del personal a la companyia els últims 8 anys ha estat constant i en ocasions s'ha incrementat molt notablement en molt poc espai de temps:

	BCN	Mónaco	Toledo	Madrid	Dinamarca	TOTAL
2008	167	0	67	11	0	**245**
2009	187	0	73	11	46	**317**
2010	193	0	73	14	46	**326**
2011	195	0	79	19	46	**339**
2012	216	0	106	74	60	**456**
2013	232	0	121	87	62	**502**
2014	242	0	126	102	74	**544**
2015	302	100	148	140	66	**756**

Taula 1: Evolució del personal

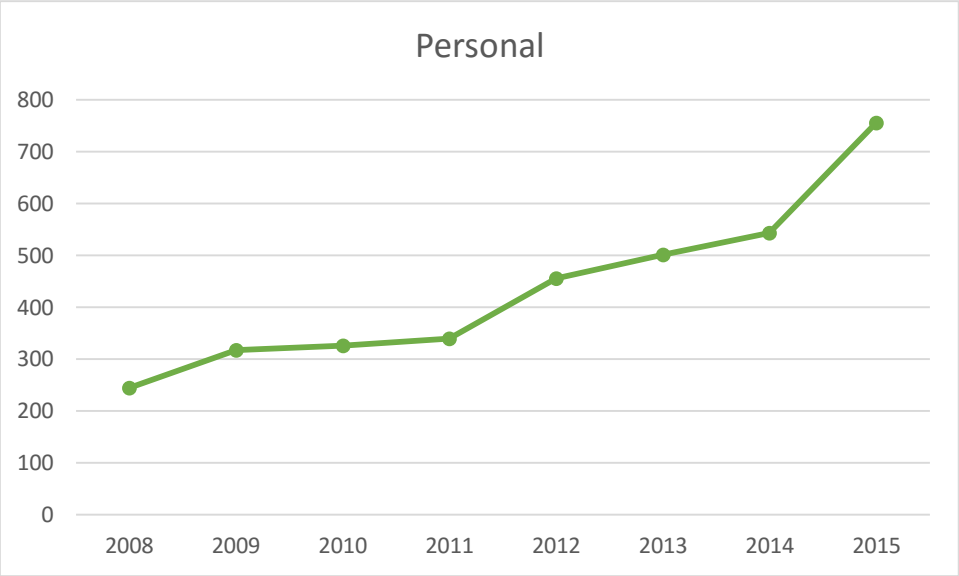


Figura 2: Evolució del personal

Tal i com es pot veure a la figura1, hi ha hagut dos grans salts en quant a incorporació de personal (any 2011-2012 i any 2014-2015) fruit de les adquisicions de dos laboratoris

Fruit del sector fortament regulat a on es troba la companyia (farmacèutic) ha ocasionat que s'hagi hagut de realitzar grans inversions els últims 5 anys per a l'adequació de les instal·lacions i els processos productius per tal de poder superar amb èxit les diferents auditories dels diferents països.

2.2 El departament d'IT dins la companyia

Tal i com s'ha comentat a la breu història, la companyia va néixer l'any 1930 i a mida que anava creixent, cada departament confiava en el director de cada planta les necessitats en quant a sistemes *"computeritzats"* es tractava.

Aquest fet va perdurar molts anys , concretament 75 anys, confiant en els diferents proveïdors totes les necessitats d'IT de cada departament.

L'any 2000, la companyia contracta un tècnic de sistemes, que era l'encarregat de reparar tot allò que deixés de funcionar, sense massa veu ni vot a l'hora de millorar les infraestructures

L'any 2005, amb tota la gestió dels sistemes externalitzada i confiada a diverses empreses es crea el departament de sistemes d'informació, depenent del director financer i dins l'àrea de serveis corporatius.
Aquesta decisió no va ser fruit d'un anàlisi organitzatiu de la companyia sinó més aviat fruit d'una situació insostenible de fallides en els sistemes i la necessitat d'implantació d'un ERP corporatiu.

Per tal de dirigir el departament es va contractar en una persona experta en gestió de processos i gestió de l'ERP però poc coneixedora d'aspectes tècnics. Aquest departament inicialment va estar format pel CIO i el tècnic de sistemes que s'encarregava del suport, delegant els aspectes tècnics a tercers.

Els primers anys del departament van ser molt difícils donat que l'àrea de producció va voler seguir mantenint la gestió dels seus sistemes informàtics amb les empreses que els hi mantenia i gestionava.
Els recursos destinats a IT eren minsos i els coneixements tècnics pobres, fet que el suport que es donava era prou deficient. Aquest fet va ocasionar unes tensions molt grans entre ambdós àrees amb la resolució de seguir mantenint els sistemes separats.

Des del 2005 fins al 2011, es va anar incrementant el personal del departament de sistemes d'informació en l'àmbit de l'ERP, donat que encara existia la fractura entre les àrees de producció i serveis centrals.

De l'any 2011 al 2015, el nombre d'usuaris creix i la complexitat en la infraestructura també, arribant a tenir ratis d'usuari per tècnic d'IT molt alts (veure Figura 2).
La situació s'ha anat agreujant fins al punt de tenir un departament d'IT dedicat exclusivament a solucionar incidències, sense tenir temps d'analitzar les seves causes, ni poder dissenyar millores en els sistemes. Aquest fet ocasiona un descontentament general per part de la companyia amb el suport ofert per part d'IT a les diferents seus, cada cop més deficient, fet que s'intenta suplir contractant a un tècnic a cada seu (exceptuant Madrid, que donat el poc volum d'usuaris, es gestiona des de Barcelona).

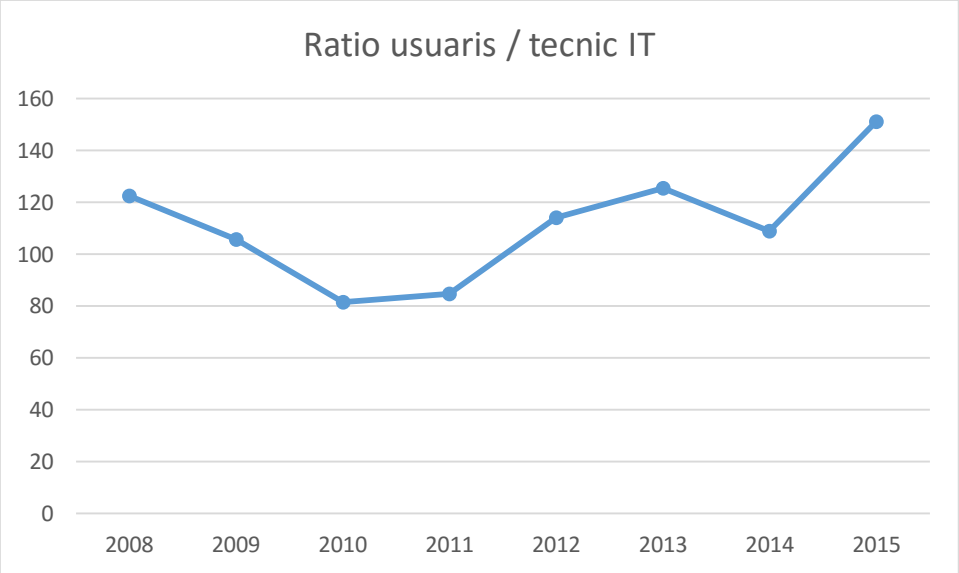


Figura 3: Rati usuaris per tècnic d'IT

Els recursos destinats a IT son molt minsos i s'ha convertit en el departament més mal valorat de la companyia.

Fruit d'aquesta mala reputació, l'any 2008 es va decidir des de Dinamarca, externalitzar tota la part d'IT de la seu escandinava a una empresa danesa. L'únic nexe d'unió entre les dues seus és l'ERP, situat a Barcelona.

La seu de Mònaco, de moment és independent i no es planteja la fusió d'IT fins que no s'hagi reestructurat la informàtica a totes les demés seus, prenent especial atenció a la seu central a Barcelona

A data d'avui, l'estructura del departament, és una estructura plana a on hi ha un únic responsable, CIO, i que correspon a les directrius de l'empresa en no jerarquitzar en excés l'organigrama:

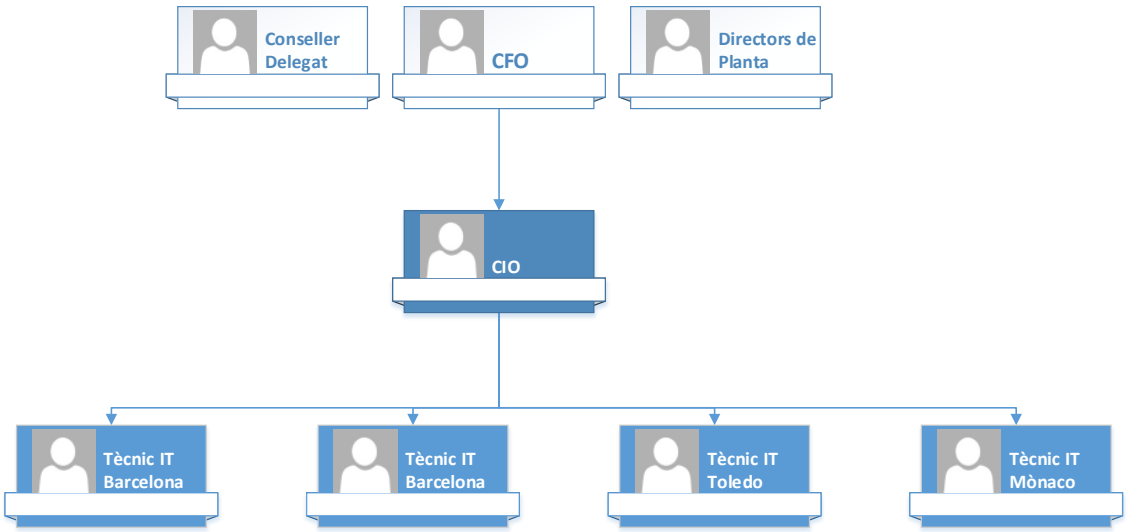


Figura 4: Organigrama

El departament d'IT el complerta dos consultors externs que gestionen tota la part de l'ERP corporatiu

Fruit d'aquesta situació, el CIO acorda amb direcció la contractació d'aquest estudi per tal de realitzar el pla estratègic dels sistemes d'Informació, amb el compromís ferm de la direcció d'assumir l'adopció de tots els canvis organitzatius i tècnics que facin falta per canviar la situació

3. Anàlisi Tècnic

3.1 Xarxa local

Maldecap Medicaments S.A disposa de 5 seus, dues de les quals són oficines i les altres 3 disposen de magatzems distribuïts en més d'un edifici.

El creixement de la infraestructura ha estat desigual en oficines (part gestionada per IT) i en la part de producció (on el departament de manteniment ha gestionat part del cablejat).
Per aquest motiu, les dues parts estan inconnexes i en la part de producció hi ha diferents subxarxes independents (cada cadena o màquina disposa de la seva pròpia xarxa).

L'estudi acurat per a les diferents seus és el següent:

Barcelona:
La seu de Barcelona (Seu central) disposa de tres edificis, un primer edifici on es situen les oficines, un segon edifici a on es troba el magatzem i un tercer edifici on es troben les cadenes de producció.

En el primer edifici es troba el CPD (Centre de procés de dades) on es troba l'armari de comunicacions. En aquest armari hi trobem 6 commutadors[1] (en anglès *switches*) de la marca *Cisco Systems* i model 1900.
Aquests commutadors tenen 24 ports a una velocitat de 10Mb/s i dos ports a 100Mb/s. En els ports a 10Mb/s estan connectats els equips clients i els servidors i en un dels ports a 100Mb/s hi ha un cable de xarxa UTP cat.5 connectat a l'armari de l'edifici 2.

En el segon edifici hi ha un magatzem amb un armari de comunicacions que comunica amb el CPD de l'Edifici 1 mitjançant un cable UTP Cat.5 per a donar serveis als equips connectats a la xarxa local.
Els 4 commutadors d'aquest armari son del mateix model que el de l'edifici 1.
Paral·lelament existeix una xarxa independent amb varis concentradors (en anglès *hubs*) encadenats per a la gestió d'una aplicació de lectura de codis de barres.

La situació en el tercer edifici és la més complexa, donat que cada model de màquina disposa de la seva pròpia xarxa (a part de la xarxa corporativa).
A grans trets ens trobem amb la xarxa corporativa que prové de l'armari de l'edifici 2 i dóna servei als clients amb 4 commutadors del mateix model que els dels demés armaris.
A més a més hi trobem 4 xarxes paral·leles amb petits commutadors i concentradors que no estan situats a cap armari totalment independents.

L'adreçament de xarxa de la seu és el següent:

- Xarxa: 192.168.0.0/22
- Màscara: 255.255.252.0
- Número de dispositius possibles: 1022
- Adreça de Broadcast: 192.168.3.254
- DHCP: Sí. Les adreces s'ofereixen dinàmicament

Les quatre xarxes independents tenen el mateix direccionalment de xarxa:

- Xarxa: 192.168.1.0/24
- Màscara: 255.255.255.0

- Número de dispositius possibles: 254
- Adreça de Broadcast: 192.168.1.254
- DHCP: No. Les adreces són estàtiques.

El següent esquema mostra l'estat de la xarxa interna de la seu:

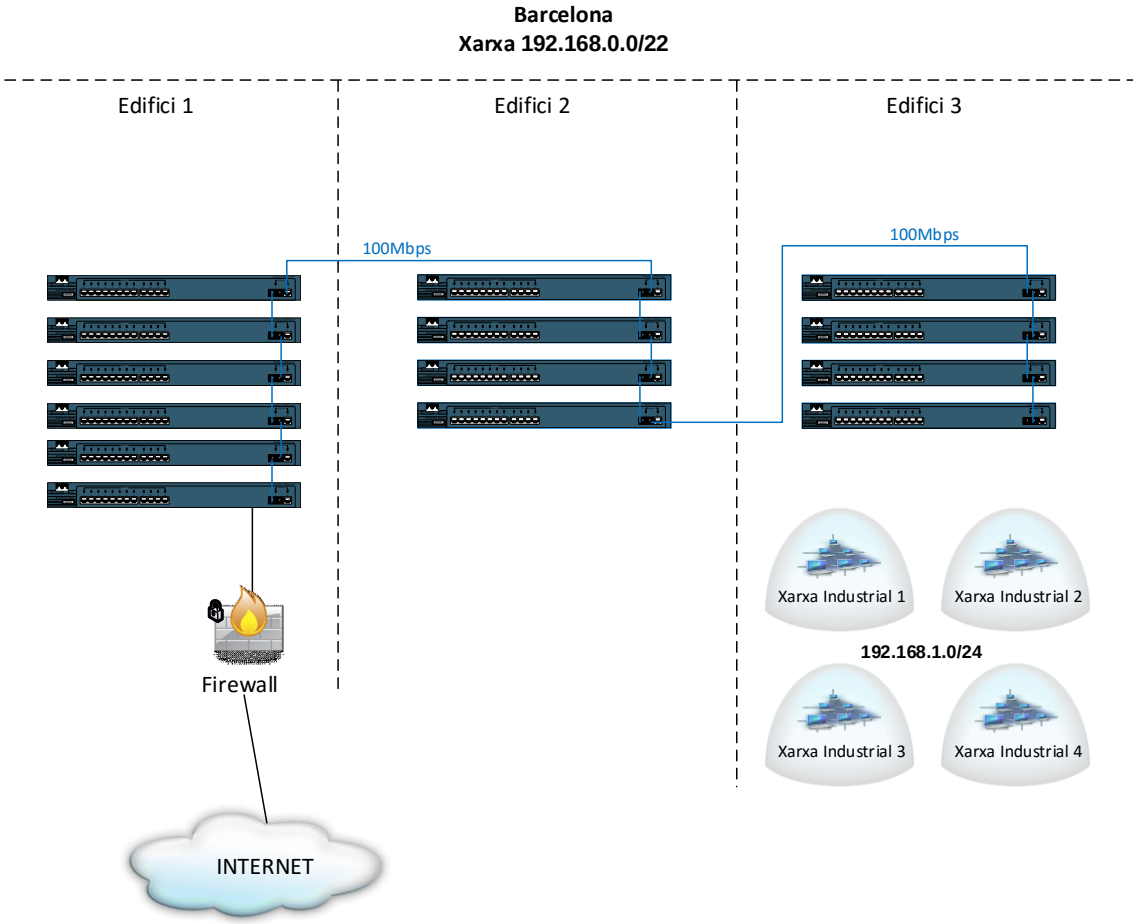


Figura 5: Xarxa interna. Seu de Barcelona

La infraestructura de la seu es complerta amb un tallafocs de la marca Cisco (model 5510) que separa la xarxa interna de la DMZ i la sortida a internet

NOTES ADDICIONALS:

- Hi ha queixes per part dels usuaris sobre la lentitud de les comunicacions i interrupcions del servei constants.
- L'aplicació que usa el personal de magatzem per a la lectura de codis de barres és molt antic i no està en manteniment. Els bloquejos i talls de comunicació són constants.
- El cablejat als tres edificis està estructurat
- No es disposa de cap certificació
- Existeix un únic rang d'Ips per a tota la seu i no existeixen commutadors de capa 3 capaços d'encaminar diferents adreçaments.
- Les portes dels armaris de comunicacions no estan tancades i els armaris no estan situats en habitacles restringits
- Els commutadors estan units en forma de cascada

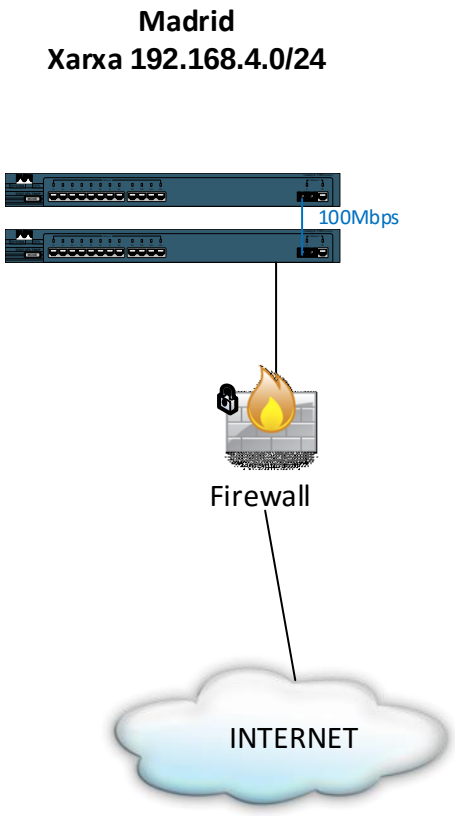
Madrid:
La seu de Madrid (Seu comercial) són unes oficines on hi treballen 30 persones fixes i hi sovintegen sovint alguns dels prop de cent visitadors mèdics distribuïts per la geografia espanyola.

El cablejat està estructurat i acaba a un armari situat en una habitació. Aquest armari conté dos commutadors de la marca *Cisco Systems* i model 1900.
Aquests commutadors tenen 24 ports a una velocitat de 10Mb/s i dos ports a 100Mb/s. En els ports a 10Mb/s estan connectats els equips clients i els servidors i en un dels ports a 100Mb/s estan interconnectat ambdós commutadors

L'adreçament de xarxa de la seu és el següent:

- Xarxa: 192.168.4.0/24
- Màscara: 255.255.255.0
- Número de dispositius possibles: 254
- Adreça de Broadcast: 192.168.4.254
- DHCP: Sí. Les adreces s'ofereixen dinàmicament

El següent esquema mostra l'estat de la xarxa:



La infraestructura de la seu es complerta amb un tallafocs de la marca Cisco (model 5505) que separa la xarxa interna de la DMZ i la sortida a internet

NOTES ADDICIONALS:

- No es disposa de cap certificació

- Existeix un únic rang d'IPs per a tota la seu i no existeixen commutadors de capa 3 capaços d'encaminar diferents adreçaments.
- Les portes dels armaris de comunicacions no estan tancades

Toledo:

La seu de Toledo (Fàbrica de producció) disposa de dos edificis, un primer edifici on es situa la fàbrica, i un segon edifici a on es troba el magatzem i centre de distribució.

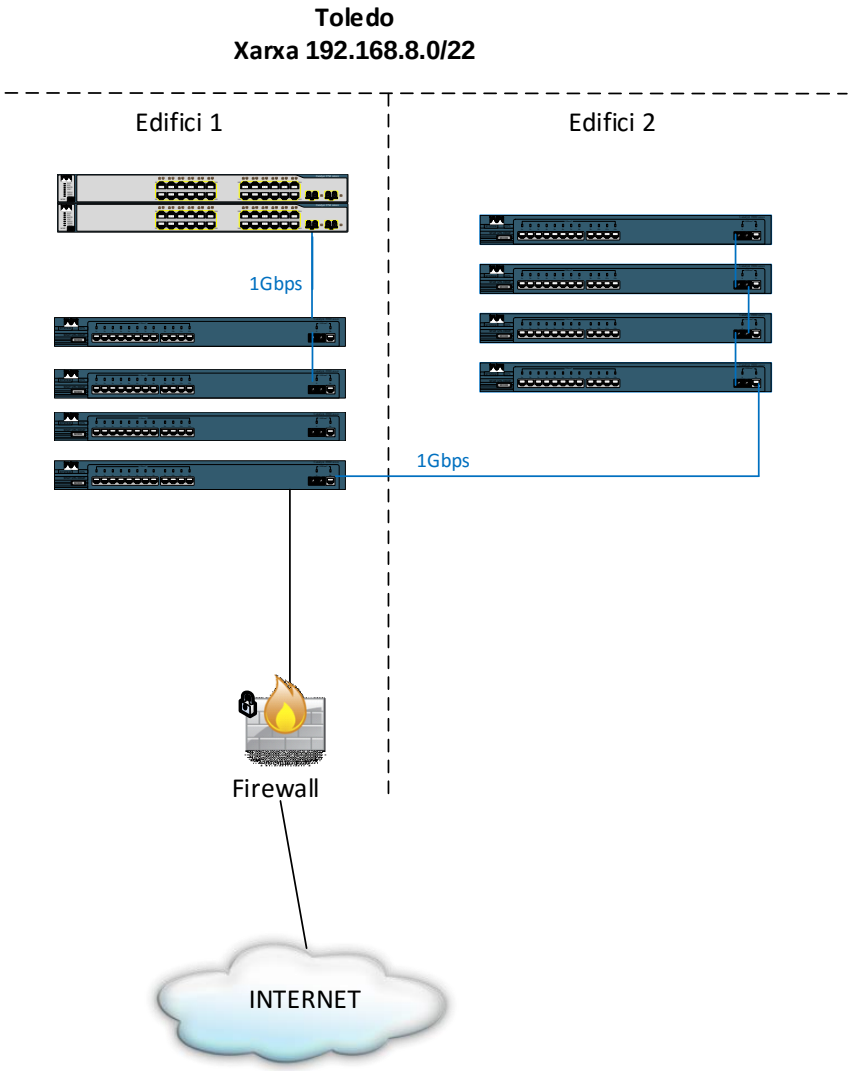
Aquestes instal·lacions van ser adquirides fa uns 12 anys a una multinacional farmacèutica alemanya i els equipaments no són els mateixos.
En aquesta seu es disposa de dos commutadors Cisco 3750 redundats capaços d'enrutar (capa 3) que actuen com a switxos de *nucli i distribució* (veure annex2: disseny de xarxes locals) que connecten amb els altres armaris. Aquests commutadors són capaços d'arribar a velocitats d'1Gps i hi estan connectats els servidors de la seu.

La seu disposa de dos armaris addicionals (un a cada edifici) a on es troben commutadors de capa2 de la marca Cisco i model 2960 (amb els ports a 100Mb per als clients i a 1Gbps per als enllaços)

L'adreçament de xarxa de la seu és el següent:

- Xarxa: 192.168.8.0/22
- Màscara: 255.255.252.0
- Número de dispositius possibles: 1022
- Adreça de Broadcast: 192.168.11.254
- DHCP: Sí. Les adreces s'ofereixen dinàmicament

El següent esquema mostra l'estat de la xarxa:



La infraestructura de la seu es complerta amb un tallafocs de la marca Cisco (model 5505) que separa la xarxa interna de la DMZ i la sortida a internet

NOTES ADDICIONALS:

- El cablejat als dels edificis està estructurat
- No es disposa de cap certificació
- Existeix un únic rang d'Ips per a tota la seu.
- Els commutadors estan units en forma de cascada

Dinamarca:

La seu Danesa (un centre de producció de pomades i aerosols), no està gestionada per IT.
Totes les decisions son preses per una empresa d'IT danesa que a través d'un contracte en vigor fins l'any 2016, gestiona tota la informàtica de la seu.

L'únic que comparteixen les dues seus és l'ERP situat a Barcelona, que a través d'una línia punt a punt redundada, s'hi connecten.

Mònaco:
L'empresa monegasca ha estat adquirida molt recentment i la direcció vol solucionar la problemàtica actual amb el departament d'IT abans de fer cap pas amb aquesta seu

Connexió entre Seus
La connexió entre seus es realitza a través d'un proveïdor de comunicacions (Colt). La tecnologia usada és MPLS entre les seus de Barcelona, Madrid i Toledo.

Les connexions entre les seus està redundada, ja sigui per anell de fibra (Barcelona, Madrid i Dinamarca) o bé per una línia de radiofreqüència secundària (Toledo).

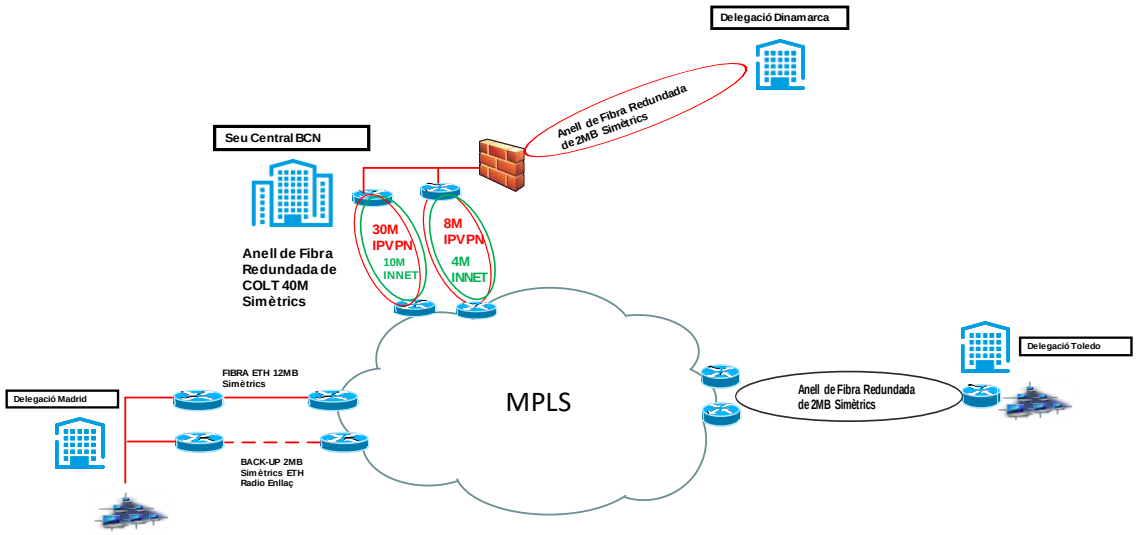


Figura 6: Esquema de connexió intersite

3.2 Xarxa Wi-Fi
Actualment, les seus de Barcelona, Madrid i Toledo disposen de punts d'accés de la marca Cisco (Aironet 1130 AG Series) situats a les sales de reunions.

Aquests punts d'accés ofereixen una velocitat teòrica (veure annex 3) de 54Mbps i els usuaris gairebé no la fan servir, degut a la saturació constant i la lentitud de la connexió.

Des de direcció s'ha demanat repetidament una revisió de la connexió inalàmbrica i que aquesta sigui extensible a tots els punts de la companyia, però els costos en hardware a nivell de controladores Wi-Fi ha fet caure financerament tots els projectes.

Ara, s'uneix un imperatiu al magatzem, donat que hi ha un projecte en marxa de lectura a traves de codi de barres per tal d'optimitzar els processos logístics i necessiten cobertura global.

Tècnicament, no hi ha una xarxa diferenciada per la Wifi (les IPs ofertes son del mateix rang de dades que els demés dispositius) ni una xarxa de convidats independent per a visites.
La validació a la xarxa es realitza a través d'una simple contrasenya, sabuda per tothom usant WPA2.

3.3 Infraestructura de servidors

L'empresa disposa d'un centre de procés de dades construït recentment i certificat amb la normativa *TIA-942*.

En tots els CPDs de les seus, disposen d'un SAI capaç d'alimentar els servidors durant un període de 2 hores.

A nivell de servidors hi trobem un clúster de 2 servidors amb VmWare, el qual permet la instal·lació de servidors virtuals i ofereix redundància en cas de caiguda d'un d'ells.
Tota la informació està emmagatzemada en una cabina de Discos SAN amb RAID6 connectada als servidors via fibra.

El mateix patró es repeteix en les seus de Madrid i Toledo, sent la capacitat dels servidors més reduïda (degut a la menor densitat de servidors virtuals que contenen).

Els servidors físics i els seus esquemes en cadascuna de les seus és el següent:

Barcelona:
A Barcelona hi ha 2 servidors IBM x3850 amb 4 processadors de 8 nuclis cadascun i 256GB de RAM.
La cabina de discos és una NetApp 2240 connectada per fibra amb dues safates de 24 discos de 900GB SAS i 4 SSD per a cache de dades.

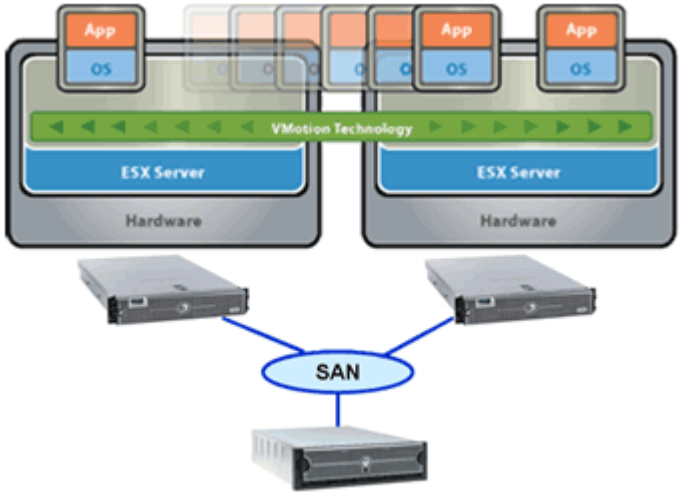


Figura 7: Infraestructura ESX. Font: VmWare

Els principals servidors virtuals que trobem a la seu de Barcelona serien:

- Controlador de domini
- Servidor de bases de dades (clusteritzat) suportant les dades de l'ERP corporatiu
- Servidor d'arxius
- Servidors de correu
- Gestió documental
- Granja d'escriptoris remots
- Servidors de Business Intelligence
- Servidor d'impressió
- Servidor de còpies de seguretat
- Altres servidors

Madrid:
A Madrid hi ha 2 servidors IBM x3500 M3 amb un processador de 4 nuclis, amb un NAS de 6 discos formant un RAID6 i obtenint una capacitat neta de 1TB

Els principals servidors virtuals que trobem a la seu de Madrid serien:

- Controlador de domini
- Servidor de còpies de seguretat
- Servidor d'arxius
- Servidor d'impressió

Toledo:
A Toledo hi ha 2 servidors IBM x3650 M3 amb un processador de 4 nuclis, amb una SAN de 8 discos formant un RAID6 i obtenint una capacitat neta de 1,4TB

Els principals servidors virtuals que trobem a la seu de Toledo serien:

- Controlador de domini
- Servidor de còpies de seguretat
- Servidor d'arxius
- Servidor d'impressió
- Altres servidors específics

Segons els requisits dels servidors virtuals i la infraestructura en aquest aspecte, el dimensionament és correcte i està dotat d'alta disponibilitat en cas de fallida a tots els nivells (fonts d'alimentació, discos, servidors, etc).

3.4 Còpies de Seguretat

Les còpies de seguretat a les seus de Barcelona, Madrid i Toledo es realitza mitjançant cintes magnètiques.
La següent taula mostra la tecnologia usada i informació sobre les capacitats i finestra de backup:

	BARCELONA	MADRID	TOLEDO
Tipus de capçal	LTO 4	VXA	LTO4
Número de capçals	1	1	1
Capacitat de cada cinta	745 GB nets	146 GB nets	186 GB
Espai ocupat	605	124	94
Espai lliure	140	22	92
Temps per a realitzar les còpies	8h 20m	10h 30min	3h

Taula 2: Sistema de backup

Algunes de les característiques de les còpies son:

- Es realitza una còpia diària de les dades
- Només hi ha un capçal a cada seu, pel que no es pot restaurar cap arxiu fins que no acabi la còpia de seguretat

La retenció és la següent:

- La cinta de la còpia diària, es duu a una localització remota (un armari ignífug situat a un altre edifici) i es sobreescriu cada setmana. La còpia diària es conserva una setmana
- Al final de la setmana es realitza una còpia anomenada “setmanal”. Hi ha dues cintes per a la còpia setmanal, es a dir, la còpia setmanal es guarda dues setmanes
- Al final de mes es realitza una còpia especial anomenada mensual. Hi ha dotze cintes per a còpies mensuals (una per a cada mes). Aquestes còpies anuals es mantenen un any a l’armari ignífug
- Al final d’any es realitza una còpia anual, la qual es manté cinc anys.

En total, a cada seu, es necessita un mínim de 21 cintes més les anuals.

No existeix un RPO (*Recovery Point Objective)* ni un RTO *(Recovery Time Objective)* definit dins del pla de continuïtat de l’empresa, com tampoc existeix cap BIA (*Business Impact Analysis*), pel que definirem l’actual punt objectiu de restauració i l’actual temps objectiu de restauració.

RPO: En el pitjor dels casos, en cas que el servei s’hagués de restaurar just abans de realitzar la còpia, hi haurien **24 hores de pèrdua de dades**.

RTO: segons la magnitud del desastre, el temps de restauració podria allargar-se dies, degut a que no es pot restaurar la informació en les altres seus (donat que els lectors de cintes son diferents).

3.5 Eines col·laboratives

Actualment les dues úniques eines que s’usen a l’empresa per a la comunicació i de treball en grup són el telèfon i el correu electrònic.

- **Telèfon**: La companyia disposa de telefonia IP a les tres seus i gestionada per una empresa de tercers en modalitat de pagament mensual. El sistema usat és una centraleta IP de la marca Cisco

- **Correu electrònic**: *Maldecap Medicaments S.A* disposa d’un servidor de correu allotjat al centre de procés de dades de Barcelona. Les característiques són:
  - Microsoft Exchange 2003
  - Bústies no replicades

3.6 Eines de suport d’IT

El departament de sistemes d’informació disposa d’un inventari realitzat amb el programa Microsoft Access, situat a un recurs compartit de la xarxa. Aquest inventari és omplert manualment pels tècnics d’IT però està molt des actualitzat

El procés de tramitació d’incidències consisteix en un enviament a una adreça de correu (suportIT@maldecapmedicaments.com) el qual es redirigeix a tots els membres d’IT o bé es truca a qualsevol dels tècnics per tal que resolguin la incidència.

3.7 Altres consideracions

Els controladors de domini estan actualitzats i hi ha certes directives de grup aplicades. La falta de coneixement i temps, fa que no se n'apliquin més per tal d'optimitzar la feina al departament.

La companyia disposa d'antivíric corporatiu, llicenciat i actualitzat. Cada dia s'envia un informe a IT sobre possibles virus a la infraestructura

4. Anàlisi de Riscos

Les taules d'anàlisis de riscos estan explicades en l'Annex 1: Metodologia Anàlisi de riscos

3.1 Xarxa Local

Seguint la metodologia d'anàlisi de riscos descrita a l'Annex1, es descriuen els diferents riscos i el seu nivell de severitat, juntament amb el pla d'acció correctiu:

IDENTIFICACIÓ DEL RISC	ANÀLISIS DEL RISC				PLA D'ACCIÓ
POSSIBLES FALLIDES	**SEVERITAT**	**PROBABI-LITAT**	**DETECTA-BILITAT**	**NIVELL DE RISC**	**MESURES PER TAL DE REDUIR EL RISC**
Fallida: El sistema no està degudament dimensionat **Efecte:** Lentitud general a la xarxa	**Alta**	**Alta**	**Alta**	**Mitjà**	Adequació de la infraestructura a les necessitats actuals i futures de la organització Substitució pels commutadors 10/100 per 100/1000
Fallida: Col·lisions a la xarxa **Efecte**: Caigudes del servei i lentitud de la xarxa	**Alta**	**Mitja**	**Alta**	**Mitjà**	Substitució dels concentradors existents a la xarxa per commutadors
Fallida: Saturació dels enllaços entre els diferents armaris de comunicacions **Efecte:** Lentitud general a la xarxa en moments puntuals	**Alta**	**Mitja**	**Mitjà**	**Alt**	Substitució dels enllaços de coure per enllaços de fibra
Fallida: Saturació dels commutadors degut a una "tempesta de broadcast" produït per un bucle **Efecte:** Caiguda del servei de xarxa, lentitud, errors de crc, etc.	**Alta**	**Mitja**	**Baixa**	**Alt**	Divisió de la xarxa en diferents dominis de *Broadcast* (o domini de difusió)
Fallida (Seguretat): Connexió a la xarxa d'un equip no corporatiu **Efecte:** Possibles problemes de seguretat, introducció de virus, robatori d'informació	**Alta**	**Alta**	**Baixa**	**Alt**	Implantació de mesures de seguretat lògiques per tal de controlar els equips connectats a la xarxa
Fallida (Seguretat): Accés indegut als armaris de comunicacions **Efecte:** Possibles problemes de seguretat, robatori físic o desconnexió de punts	**Alta**	**Mitja**	**Alta**	**Mitjà**	Tancament dels armaris de comunicacions amb clau i aquesta ha de ser custodiada per IT
Fallida: Mal funcionament o parada de servei del commutador principal	**Alta**	**Mitja**	**Alta**	**Mitjà**	Redundància dels commutadors Disseny en forma d'anell en comptes de cascada

Efecte: Aturada de totes les comunicacions, al estar tots els commutadors en cascada					
Fallida: Mal funcionament o parada de servei del tallafocs **Efecte:** Impossibilitat d'accés a Internet. Tall de comunicacions amb les seus	**Alta**	**Mitja**	**Alta**	**Mitjà**	Redundància del tallafocs

3.2 Xarxa Wi-Fi

Seguint la metodologia d'anàlisi de riscos descrita a l'Annex1, es descriuen els diferents riscos i el seu nivell de severitat, juntament amb el pla d'acció correctiu:

IDENTIFICACIÓ DEL RISC	**ANÀLISIS DEL RISC**				**PLA D'ACCIÓ**
POSSIBLES FALLIDES	**SEVERITAT**	**PROBABI-LITAT**	**DETECTA-BILITAT**	**NIVELL DE RISC**	**MESURES PER TAL DE REDUIR EL RISC**
Fallida: El sistema no està degudament dimensionat **Efecte:** Lentitut general a la xarxa inalàmbrica	**Alta**	**Alta**	**Alta**	**Mitjà**	Adequació de la infraestructura a les necessitats actuals i futures de la organització Adequació de la xarxa WiFi a les noves necessitats empresarials
Fallida: Col·lisions a la xarxa **Efecte**: Caigudes del servei i lentitud de la xarxa	**Alta**	**Mitja**	**Alta**	**Mitjà**	Divisió de la xarxa en diferents dominis de Broadcast (o domini de difusió), creant una VLAN per a la xarxa inalàmbrica
Fallida (Seguretat): Connexió a la xarxa d'un equip no corporatiu **Efecte:** Possibles problemes de seguretat, introducció de virus, robatori d'informació	**Alta**	**Alta**	**Baixa**	**Alt**	Canviar el sistema d'autenticació de la xarxa inalàmbrica Crear una xarxa de convidats aïllada de la resta

3.3 Infraestructura de servidors.

Seguint la metodologia d'anàlisi de riscos descrita a l'Annex1, es descriuen els diferents riscos i el seu nivell de severitat, juntament amb el pla d'acció correctiu:

IDENTIFICACIÓ DEL RISC	**ANÀLISIS DEL RISC**				**PLA D'ACCIÓ**
POSSIBLES FALLIDES	**SEVERITAT**	**PROBABI-LITAT**	**DETECTA-BILITAT**	**NIVELL DE RISC**	**MESURES PER TAL DE REDUIR EL RISC**
Fallida: Mal funcionament o parada d'un dels servidors físics	**Baixa**	**Baixa**	**Alta**	**Baix**	El sistema ja disposa d'un sistema de redundància

Efecte: Les màquines virtuals dins d'aquest servidor automàticament es registrarien en el segon servidor					
Fallida: Fallida d'una font d'alimentació **Efecte**: Els servidors i les cabines de discos disposen de fonts d'alimentació redundades	**Baixa**	**Baixa**	**Alta**	**Baix**	En cas de caiguda d'una font d'alimentació, el sistema continuaria funcionant i enviaria una alerta als administradors
Fallida: Fallida d'un disc **Efecte:** Possibles problemes de seguretat, introducció de virus, robatori d'informació	**Baixa**	**Mitja**	**Alta**	**Baix**	El sistema continuaria funcionant gràcies al RAID de discos i enviaria una alerta als administradors del sistema
Fallida: Caiguda de la xarxa elèctrica **Efecte:** Es posa en marxa el SAI del CPD	**Alta**	**Baixa**	**Alta**	**Baix**	El SAI avisa als administradors per tal de realitzar un apagat controlat dels servidors en cas que l'avaria es perllongui

3.4 Còpies de seguretat

Seguint la metodologia d'anàlisi de riscos descrita a l'Annex1, es descriuen els diferents riscos i el seu nivell de severitat, juntament amb el pla d'acció correctiu:

IDENTIFICACIÓ DEL RISC	**ANÀLISIS DEL RISC**				**PLA D'ACCIÓ**
POSSIBLES FALLIDES	**SEVERITAT**	**PROBABI-LITAT**	**DETECTA-BILITAT**	**NIVELL DE RISC**	**MESURES PER TAL DE REDUIR EL RISC**
Fallida: Mal funcionament del lector de cintes **Efecte:** No es poden realitzar les còpies de seguretat ni restaurar-les	**Alta**	**Baixa**	**Alta**	**Baix**	S'hauria d'adquirir un altre capçal o reparar aquest. Durant aquest temps, el sistema deixaria de fer còpies
Fallida: Increment de les dades a copiar **Efecte**: modificacions a la finestra de còpies de seguretat i de restauració	**Baixa**	**Baixa**	**Alta**	**Baix**	En cas de caiguda d'una font d'alimentació, el sistema continuaria funcionant i enviaria una alerta als administradors
Fallida: No es realitza el canvi de cintes	**Mitja**	**Mitja**	**Alta**	**Baix**	El sistema continuaria funcionant gràcies al RAID de discos i enviaria

Efecte: Incompliment del SLA en quan a retencions de còpies de seguretat					una alerta als administradors del sistema
Fallida: Degradació de la cinta de backup **Efecte:** Errors al restaurar les dades inclús impossibilitat de restauració	**Alta**	**Mitja**	**Baixa**	**Alt**	El fet de no poder restaurar una dada pot tenir efectes molt greus per a la companyia. És molt difícil detectar la integritat d'un dispositiu físic fins que no s'intenta restaurar.
Fallida: **Efecte:** Errors al restaurar les dades inclús impossibilitat de restauració	**Alta**	**Mitja**	**Baixa**	**Alt**	El fet de no poder restaurar una dada pot tenir efectes molt greus per a la companyia. És molt difícil detectar la integritat d'un dispositiu físic fins que no s'intenta restaurar.

5. Conclusions de l'estudi inicial

5.1 Aspectes organitzatius [5]

La situació actual del departament d'IT dins la companyia, segons s'ha pogut veure en l'anàlisi organitzatiu, és força complexa i necessita una transformació a nivell corporatiu.

A nivell de personal, ens trobem amb un departament mal dimensionat amb uns ratis d'usuaris per personal d'IT molt elevat.

La complexitat dels sistemes ha anat incrementant en els darrers anys i no s'ha realitzat una inversió proporcional ni en personal ni en formació, convertint el departament en un departament reactiu que dedica una altíssima part del seu temps en resoldre incidències.

En quant a les relacions entre departaments, la situació entre Enginyeria i Informàtica és insostenible cal establir ponts efectius entre ambdós departaments i involucrar a direcció per tal de solucionar aquestes barreres i eliminar els SILOS entre els departaments.

No hi ha un pla estratègic de sistemes d'informació ni una estratègia definida mes enllà de la de sobreviure al dia a dia.

Objectius de la proposta:

- Plantejar una sèrie de mesures per tal de transformar el departament d'IT i situar-lo en una posició estratègica dins la companyia
- Dimensionar adequadament els recursos i reorientar els objectius del departament
- Establir un model capaç de mantenir el suport als sistemes tradicionals però que alhora pugui adaptar-se a les noves tendències.

5.2 Xarxa Local

Respecte a la xarxa local, observem una infraestructura amb dispositius obsolets que no cobreixen les necessitats del grup en termes de velocitat i disseny.

Segons podem observar en l'anàlisi tècnic i l'anàlisi de riscos, existeixen SILOS independents, problemes generalitzats deguts al transit i lentitud a la xarxa.

Cal destacar la falta de certificacions dels punts de xarxa i els riscos de seguretat associats a la manca de validació dels punts de xarxa

Objectius de la proposta:

- Redefinir l'estructura lògica de la xarxa per tal de complir amb les millors pràctiques del mercat
- Adequar la infraestructures a les necessitats actuals i futures de la companyia
- Establir un sistema robust, d'alta velocitat amb el menor impacte possible
- Definir un sistema de seguretat a nivell de capa 2 dins la companyia, el menys intrusiu possible
- Establir un pla de formació per a IT

5.3 Xarxa Wi-Fi

Cada cop més, la xarxa inalàmbrica és usada per més dispositius (ordinadors, portàtils, tauletes, mòbils, projectors, etc.) i l'actual infraestructura no està degudament dimensionada per donar resposta a les noves necessitats de la companyia.

El fet d'haver un projecte de Lectors de Codis de Barres, aguditza les mancances de l'actual infraestructura

L'actual xarxa inalàmbrica és un focus d'incidències i existeix un risc de seguretat, donat que la clau és coneguda per a tota la companyia (i fora d'ella).

Objectius de la proposta:

- Redefinir l'estructura lògica de la xarxa inalàmbrica per tal de complir amb les millors pràctiques del mercat
- Adequar la Wi-FI a les necessitats actuals i futures de la companyia
- Establir un sistema robust, d'alta velocitat amb el menor impacte possible
- Menor cost possible en actius
- Establir un sistema que permeti la separació de transit corporatiu dels convidats, garantint amples de banda, control i priorització
- Gestió senzilla (corba d'aprenentatge petita)
- Pla de formació

5.4 Infraestructura de servidors

De l'anàlisi tècnic es pot concloure que l'actual infraestructura de servidors està degudament dimensionada, responent a les necessitats actuals i futures del grup.

No es creu necessari una re definició en aquest àmbit en una primera fase.

5.5 Còpies de seguretat

De l'estudi inicial i l'anàlisi de riscos, s'extreuen les següents conclusions que seran el punt de partida per a l'estudi d'alternatives:

- Dependència del model de cintes magnètiques usades i del corresponent lector
- Temps de realització de còpies molt alt (finestra de restauració molt curta)
- Falta d'un RPO i RTO global
- Necessitat d'un operador per a canviar les cintes
- Falta d'un DRP (*Disaster Recovery Plan*)

Objectius de la proposta:

- Redissenyar el sistemes de còpies de seguretat, automatitzant al màxim les tasques de còpies i replicació
- Eliminar la dependència del maquinari per a la restauració (lectors de cintes magnètiques)
- Establir un sistema robust, que permeti la restauració deslocalitzada de manera ràpida, una major finestra de còpies i de restauració
- Establir un pla de formació per a IT

5.6 Eines Col·laboratives

No existeixen a la companyia eines col·laboratives, fora del correu electrònic, capaces d'optimitzar el temps del personal de la companyia.

Objectius de la proposta:

- Proposar eines que optimitzin el temps del personal de la companyia
- Eliminar SILOS i falta de comunicació entre departaments
- Augmentar la productivitat
- Millorar la imatge del departament, proposant solucions de baix cost econòmic però amb una visibilitat molt gran
- Establir plans de formació per a la companyia

5.7 Eines de Suport a IT

No existeix cap eina de gestió d'incidències per tal d'optimitzar el temps i recursos del departament d'IT, així com un programari d'inventari capaç de tenir documentats tots els actius d'IT de la companyia.

Tampoc existeix un punt d'entrada d'incidències o trucades únic, per tal d'evitar distraccions del personal d'IT

Objectius de la proposta:

- Optimitzar el temps i recursos del departament d'IT
- Millorar l'efectivitat del departament en la resolució d'incidències
- Augmentar la satisfacció dels usuaris

6. Proposta de Millora

6.1 Organitzatiu

En l'àmbit organitzatiu seria necessàries certes actuacions per tal que el departament d'IT pugui alinear-se amb els objectius estratègics de la companyia:

1- Alineació CIO-CFO. No entraré en el debat de si la posició del CIO dins l'organigrama de la companyia hauria de situar-se al mateix nivell que el CFO (crec que hi ha molts factors polítics i històrics que hi influeixen).
El que sí que és clar és que el CIO i el CFO han d'establir un mètode de treball conjunt, a on hi hagi total transparència de "dalt cap a baix" i de "baix cap a dalt" i una bona comunicació per tal que s'entenguin les necessitats i els objectius de la companyia.
També fóra bo que el CIO aprengués el llenguatge comptable per tal de poder transformar les oportunitats tecnològiques en beneficis i poder plasmar-los

2- Establir una estructura organitzativa clara dins del departament, separant la part de sistemes i la part de l'ERP, seleccionant dos líders per ambdós àrees. D'aquesta manera, aquests dos responsables reportarien directament al CIO, descarregant a aquest de tasques i decisions més tècniques per tal que es pugui centrar en tasques de més valor

3- Treball amb Recursos Humans per tal de trencar els SILOS establerts històricament amb el departament de producció. Cal definir les responsabilitats d'ambdós departaments i buscar les sinèrgies necessàries per tal de treballar conjuntament

4- Redimensionar adequadament el personal d'IT per tal de donar el servei que els usuaris esperen

5- Definir un pla estratègic de Sistemes d'Informació que permeti fer una anàlisi acurada del paper que ha de prendre IT dins la companyia

6.2 Xarxa local

Per tal de redimensionar la xarxa local es proposen les següents actuacions:

Topologia: a nivell lògic es proposa seguir el model de Cisco descrit a l'annex 2, amb una petita modificació i és que com la grandària de les seus no és excessivament gran, s'establiran dues capes: La capa de Nucli a on es situaran commutadors d'alta velocitat i redundats, i la capa d'accés a on es situaran els commutadors que donen accés als dispositius.

Disponibilitat: Per tal de garantir la disponibilitat del servei (a part dels commutadors de nucli que estaran redundats) es proposa activar el protocol STP a la infraestructura i crear anells lògics per si falla un commutador no fallin tots els demés de la cadena.

Rendiment: Per tal de millorar el rendiment es proposa el següent:

- Substituir els commutadors de nucli per commutadors a 10Gbps
- Substituir els commutadors d'accés per uns que funcionin a 1Gps amb possibilitat de fer enllaços a 10Gbps
- Establir enllaços de fibra duplicats des dels commutadors de nucli als demés edificis

- Certificar tots i cadascun dels punts de xarxa i mantenir un inventari de la situació del punt amb la seva corresponent certificació

Seguretat:

- Es proposa tancar tots els armaris i situar les claus corresponents a un clauer situat a IT.
- Establir un mètode d'autenticació per tal d'evitar la connexió de dispositius no autoritzats per la companyia. Per tal d'aconseguir aquest requisit s'implementaria un servidor RADIUS el qual validaria les MACs dels dispositius que es connectin. Segons les necessitats de la companyia, la implementació d'un sistema amb autenticació 802.1x seria molt invasiu, costós d'implementar i necessitaria molts recursos.

VLANs: L'hem mencionat apart degut a que un bon disseny de VLANs pot augmentar la disponibilitat, el rendiment i la seguretat. Els requisits per tal d'establir un sistema de Vlans adequat i fàcil de gestionar serien els següents:

- Definir les mateixes vlans a totes les seus per simplicitat i per agilitat
- Definir uns rangs que no siguin els que assignen els dispositius per defecte (192.168.x.x)
- Definir una Vlan de *management* per a tots els dispositius. L'objectiu d'aquesta vlan és disposar d'un rang per a gestionar els dispositius si hi ha saturació o bloqueig a la vlan per defecte (d'aquesta manera una tempesta de *broadcast* no impediria l'accés al dispositiu)
- Definir una vlan per a IT, diferenciada de la resta (per temes de divisió de transit)
- Separar el tràfic per grups lògics
- Definir una vlan a tots els commutadors que per defecte no sigui enrutable (si un equip es connecta a un commutador, necessàriament s'ha d'assignar una vlan a aquell port per motius de seguretat)
- Definir una Vlan de convidats (a on s'establiran polítiques específiques que bloquegin l'accés als recursos interns)
- Definir vlans per a aquell transit crític (sistemes de producció) o que generi un alt volum de dades (còpies de seguretat)

Les següents taules mostren la proposta de Vlans per a les seus de Barcelona Madrid i Toledo:

Vlan ID	Nom Vlan	Descripció	Xarxa	Màscara
1	Default	Vlan per defecte no enrutable	192.168.0.0	255.255.255.0
2	PCs	Vlan per als equips	172.20.0.0	255.255.252.0
3	VoIP	Vlan de veu per a la telefonia	172.20.8.0	255.255.255.0
4	Convidats	Vlan de convidats (WiFi)	172.20.9.0	255.255.255.0
5	Mgmt	Vlan de gestió d'equips	172.20.10.0	255.255.255.0
6	IT	Vlan per a l'àrea d'IT	172.20.11.0	255.255.255.0
7	Servers	Vlan per a servidors	172.20.12.0	255.255.255.0
8	Impresores	Vlan per a les impressores	172.20.13.0	255.255.255.0
9	Backups	Vlan per al tràfic de Backups	172.20.14.0	255.255.255.0
10	SistemesIndustrials	Vlan per als equips industrials	172.20.15.0	255.255.252.0

Taula 3: Vlans i adreçament de BCN

Vlan ID	Nom Vlan	Descripcio	Xarxa	Màscara
1	Default	Vlan per defecte no enrutable	192.168.100.0	255.255.255.0
2	PCs	Vlan per als equips	172.20.100.0	255.255.252.0
3	VoIP	Vlan de veu per a la telefonia	172.20.108.0	255.255.255.0
4	Convidats	Vlan de convidats (WiFi)	172.20.109.0	255.255.255.0
5	Mgmt	Vlan de gestió d'equips	172.20.110.0	255.255.255.0

6	IT	Vlan per a l'àrea d'IT	172.20.111.0	255.255.255.0
7	Servers	Vlan per a servidors	172.20.112.0	255.255.255.0
8	Impresores	Vlan per a les impressores	172.20.113.0	255.255.255.0
9	Backups	Vlan per al tràfic de Backups	172.20.114.0	255.255.255.0
10	SistemesIndustrials	Vlan per als equips industrials	172.20.115.0	255.255.252.0

Taula 4: Vlans i adreçament de Toledo

Vlan ID	Nom Vlan	Descripcio	Xarxa	Màscara
1	Default	Vlan per defecte no enrutable	192.168.200.0	255.255.255.0
2	PCs	Vlan per als equips	172.20.200.0	255.255.252.0
3	VoIP	Vlan de veu per a la telefonia	172.20.208.0	255.255.255.0
4	Convidats	Vlan de convidats (WiFi)	172.20.209.0	255.255.255.0
5	Mgmt	Vlan de gestió d'equips	172.20.210.0	255.255.255.0
6	IT	Vlan per a l'àrea d'IT	172.20.211.0	255.255.255.0
7	Servers	Vlan per a servidors	172.20.212.0	255.255.255.0
8	Impresores	Vlan per a les impressores	172.20.213.0	255.255.255.0
9	Backups	Vlan per al tràfic de Backups	172.20.214.0	255.255.255.0
10	SistemesIndustrials	Vlan per als equips industrials	172.20.215.0	255.255.252.0

Taula 5: Vlans i Adreçament de Madrid

La topologia final de la proposta seria la següent:

Barcelona: en aquesta seu hi hauria dos commutadors redundats de nucli el qual tindria tots els ports a una velocitat de 10Gbps.
D'aquest commutadors sortirien dues connexions de fibra cap a cadascun dels edificis on es connectaria amb el primer commutador d'accés i l'últim de la pila, creant un anell amb camins redundats (la informació pot arribar a cadascun dels commutadors per dos camins diferents). Si un camí es trenqués o un commutador s'apagués, el protocol STP bloquejaria aquest camí i activaria el que dóna continuïtat

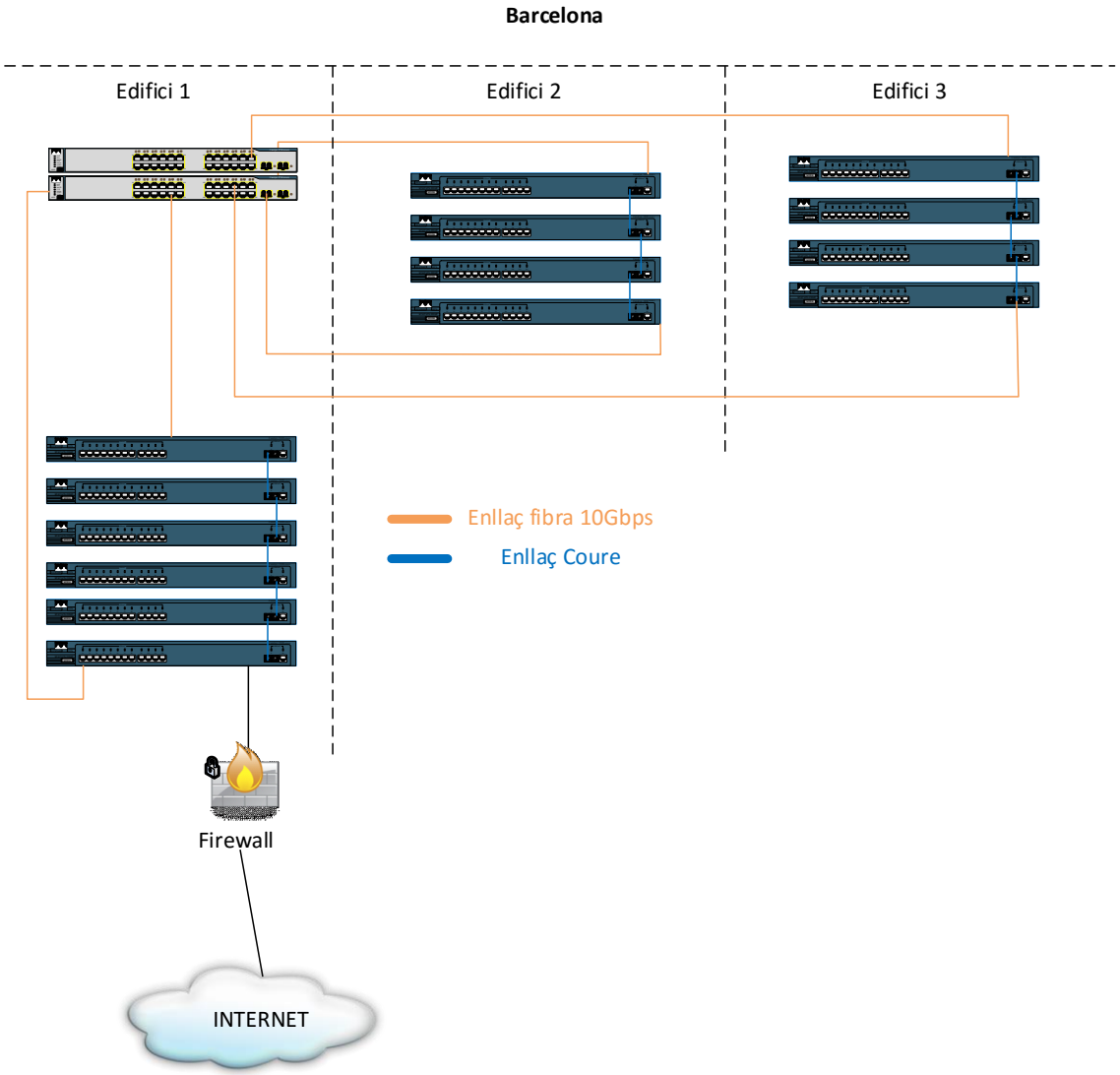


Figura 8: Proposta xarxa interna. Seu de Barcelona

Madrid: Aquesta seu és molt petita i no té sentit fer una gran despesa en crear una topologia de nucli i accés.
Al haver-hi tan pocs punts i l'absència d'enllaços amb d'altres armaris, es proposa la substitució dels dos commutadors actuals per dos commutadors a 1Gbps. D'aquesta manera es multiplicaria la velocitat d'accés dels dispositius:

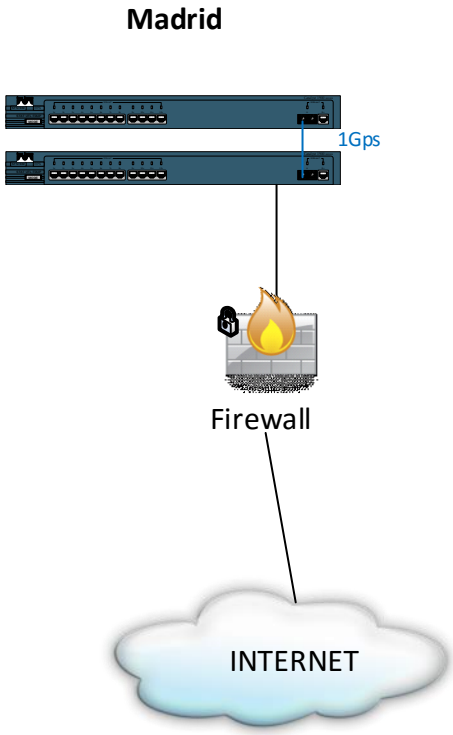


Figura 9: Proposta xarxa interna. Seu de Madrid

Toledo: en aquesta seu hi hauria dos commutadors redundats de nucli el qual tindria tots els ports a una velocitat de 10Gbps (s'haurien de substituir els actuals per dos de nous amb enllaços a 10Gps).
D'aquest commutadors sortirien dues connexions de fibra cap a cadascun dels edificis on es connectaria amb el primer commutador d'accés i l'últim de la pila, creant un anell amb camins redundats (la informació pot arribar a cadascun dels commutadors per dos camins diferents). Si un camí es trenqués o un commutador s'apagués, el protocol STP bloquejaria aquest camí i activaria el que dóna continuïtat

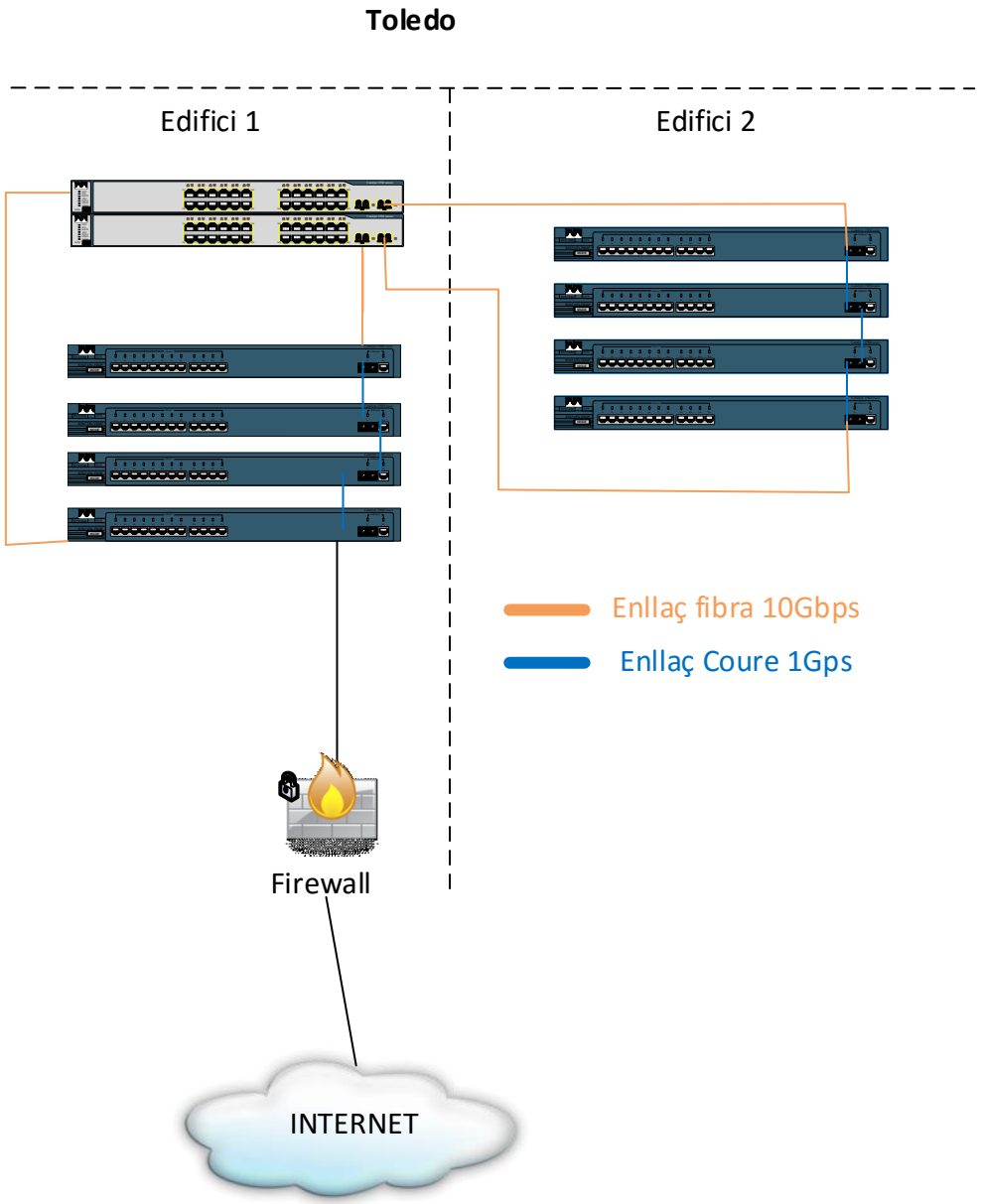


Figura 10: Proposta xarxa interna. Seu de Toledo

Cost de la solució

Segons es pot veure en l'Annex13 (comparativa de fabricants) podem observar que els costos dels commutadors poden variar molt depenent de la solució escollida.
Després d'analitzar les avantatges i els inconvenients dels diferents fabricants, descrits en el mateix annex recomanem l'adopció de dispositius Cisco per les següents raons:

1- La implementació es podria realitzar gradualment, disminuïnt el cost inicial de la inversió
2- L'impacte seria nul, donat que els dispositius existents són del mateix fabricant
3- El sistema de telefonia és de la mateixa marca i evitaria possibles efectes col·laterals en la telefonia
4- El cost de formació disminuiria, donat que el personal d'IT ja coneix com funciona la solució.

Per al projecte global es necessitaria 4 commutadors de nucli (dos per Barcelona i dos per Toledo) i 24 commutadors d'accés:

4x WS-C4928-10GE = 4 x 25000€ = 100.000€
24 x WS-C2960X-48TD-L = 24 x 1900€ = 45.600€

Sent el cost total en dispositius, seria 145000€, al qual s'hauria de sumar les hores de personal qualificat, que poden variar depenent del proveïdor escollit i el cost dels enllaços de fibra i les certificacions dels punts de xarxa

Planificació

Aquest projecte es podria planificar en quatre fases i el temps pot variar depenent de l'adopció del projecte (si es realitza globalment, o progressivament):

1- **Definició de la topologia**:
   a. Definició de les diferents Vlans
   b. modificacions als firewalls
   c. Configuració del servidor RADIUS
   d. Identificació de tots els dispositius autoritzats
   e. prova de la configuració en un simulador.

2- **Adequació del cablejat:**
   a. Realitzar les tirades de fibra pertinents per als enllaços
   b. certificació de tots els punts de xarxa

3- **Implementació dels commutadors de nucli:**
   a. Adquisició dels commutadors de nucli
   b. Càrrega de la configuració
   c. Substitució dels switches de nucli existents

4- **Implementació dels commutadors d'accés:**
   a. Adquisició dels switchos d'accés (tots o progressivament
   b. Càrrega de la configuració
   c. Substitució progressiva dels actuals commutadors

6.3 Xarxa WiFi

Per tal de poder definir una proposta, es definiran uns requisits, extrets de les conclusions de l'estudi inicial (apartat 5.3) i l'anàlisi de riscos.
Serà necessari dur a terme el projecte d'adequació de la xarxa local per tal de garantir una solució de qualitat sense colls d'ampolla.

Topologia: Es proposa la implementació de punts d'accés connectats als commutadors que tinguin ports a 1Gbps com a mínim.
Es prioritzaran aquelles solucions que no disposin d'equipaments complementaris i necessaris per tal que funcioni la solució com ara controladores addicionals o servidors.

Es proposa la contractació d'una sortida a internet complementària (de menys caudal que la que es disposa actualment) per donar sortida a la xarxa de convidats i evitar possibles saturacions a la línia d'internet corporativa.

Els SSIDs que es creïn, seran els mateixos per a totes les seus per tal d'oferir mobilitat sense necessitat de realitzar canvis

Es proposarà una solució sense comptabilitzar la quantitat total de punts d'accés donat que no s'ha realitzat un estudi de cobertura exhaustiu

Disponibilitat: Per tal de garantir la disponibilitat del servei serà necessari que el sistema sigui tolerant a fallides.

Rendiment: Per tal de millorar el rendiment es proposa el següent:

- Realitzar un estudi acurat de cobertura a totes les seus per tal de definir la situació més òptima a on col·locar els punts d'accés
- Col·locació de punts d'accés amb tecnologia 802.11ac a les oficines per tal d'oferir la màxima velocitat
- Col·locació de punts d'accés amb tecnologia 802.11n als magatzems per al sistema de codi de barres. D'aquesta manera es reduiran els costos d'adquisició de la solució
- El sistema escollit haurà de ser capaç de gestionar l'ample de banda, garantint el trànsit corporatiu en front del de convidats des de l'equip fins el punt d'accés.

Seguretat:

- Es crearà un SSID corporatiu amb autenticació contra el directori actiu a on només els usuaris del domini que estiguin dins d'un grup de seguretat s'hi podran connectar.
  Aquest SSID es publicarà per directiva a tots els ordinadors de la companyia i serà necessària l'autenticació a través d'un RADIUS
- Es crearà un SSID per als convidats. Aquest tràfic serà totalment aïllat i només oferirà connexió a Internet
- Es proposa un sistema en que els propis punts d'accés disposin de tallafocs (desitjablement a nivell d'aplicació), per tal de bloquejar aquell tràfic no desitjat al propi punt d'accés

Cost de la solució

Segons es pot veure en l'Annex13 (comparativa de fabricants) podem observar que els costos dels punts d'accés poden variar molt depenent de la solució escollida.
Després d'analitzar les avantatges i els inconvenients dels diferents fabricants, descrits en el mateix annex recomanem l'adopció de dispositius Aerohive per les següents raons:

1- La implementació es podria realitzar gradualment, disminuint el cost inicial de la inversió
2- L'impacte seria molt baix dins la organització
3- La seva administració senzilla, evitaria una gran despesa en formació
4- Al ser una solució que no es basa en controladors, redueix costos i incrementa l'escalabilitat
5- La gestió unificada per a les diferents seus, incrementa l'agilitat en la gestió

No es pot definir un cost global de la solució, donat que es necessita un acurat estudi de cobertura a nivell global.

Planificació

Aquest projecte es podria planificar en tres fases ben diferenciades. Les fases d'implantació poden ser molt diferent, depenent dels recursos tècnics i econòmics que es destinin, i al ser una solució que es pot implantar gradualment, encara complica més definir una acurada planificació sense conèixer aquests recursos.

1- **Definició de la topologia (Temps aproximat; 15 dies):**
    a. Definició dels SSID i la seva seguretat
    b. Adequació de la infraestructura a on aniran connectats els punts d'accés

2- **Fase de Test (temps aproximat: 1 mes)**
    a. Durant aquesta fase es col·locaran dos o tres punts d'accés de proves a la organització per tal de veure si compleixen les expectatives i el departament es senti confortable amb la solució
    b. Es realitzarà la configuració inicial i es faran les proves pertinents.

3- **Estudi de cobertura**:
    a. Estudi de les necessitats per seu i departament (tipus d'AP a escollir, velocitat, densitat, etc.)
    b. Estudi de cobertura a la seu de Barcelona
    c. Estudi de cobertura a la seu de Madrid
    d. Estudi de cobertura a la seu de Toledo
    e. Identificació de tots els punts d'accés necessari

4- **Implementació dels punts d'accés per ordre de prioritat:**
    a. Implementar els punts d'accés per ordre de prioritat (recomanem la seva implantació per zones)

6.4 Còpies de seguretat

Després d'analitzar els sistema de còpies de seguretat amb les conclusions de l'estudi inicial (apartat 5.3) i l'anàlisi de riscos. Es realitzen una sèrie de propostes de millora:

Tipus de suport: Es proposa que el destí de les còpies de seguretat sigui sobre disc dur (per exemple un NAS amb RAID5). El sistema escollit haurà de deduplucar la informació per tal d'estalviar espai en disc de les còpies de seguretat. Les avantatges d'aquest mètode son les següents:

- No cal una forta inversió en lectors de cintes magnètiques a les tres seus ni la inversió inicial de les cintes
- La informació radica en disc i pot ser transportada per xarxa, en comptes d'extreure manualment les cintes
- L'escriptura a una biblioteca de discos no és seqüencial, pel que es poden realitzar múltiples treballs alhora, estalviant temps i permetent la restauració mentre s'estan realitzant backups
- Es poden afegir discos de diferents capacitats o canviar la biblioteca de discos, sense que quedi obsolet el lector
- No es requereix d'un lector específic per tal de realitzar la restauració (punt important en cas de Recuperació d'un desastre)
- Gràcies a la deduplicació de les còpies, s'evita el creixement insostenible de l'espai necessari a emmagatzemar, podent disposar de més còpies durant més temps i amb menys espai ocupat

Topologia: Es proposa un sistema totalment autònom de còpies de seguretat a on la intervenció del departament d'IT només ha de servir per a comprovar les còpies i realitzar backups.

El sistema es compon d'un servidor de còpies de seguretat a cada seu on realitzarà la còpia en discos locals (NAS).
Aprofitant la MPLS existent entre les seus i el nul tràfic que circula per la nit, es copiaran les còpies de seguretat diàries en una segona localització (aprofitant la deduplicació de la solució), sent la seu central la que tindrà sempre una còpia de totes les dades. D'aquesta manera, totes les còpies de seguretat es troben en dues localitzacions diferents i el més important, poden ser restaurades a la seu central en cas de necessitat:

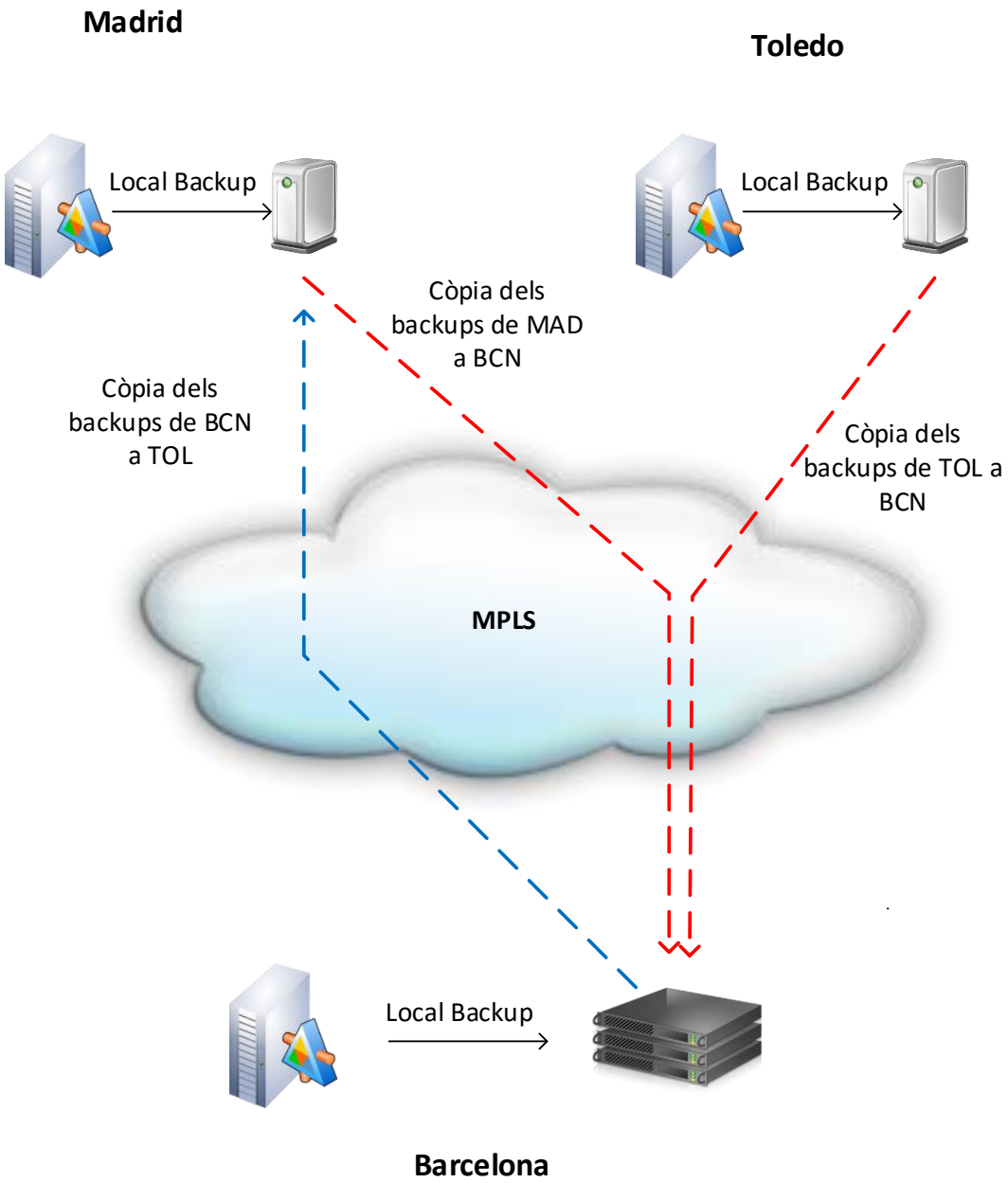


Figura 11: Tipologia de còpies de seguretat

Cost de la solució

Tal i com s'explica a l'Annex 13 (Apartat 13.3), no es pot realitzar un estudi econòmic faltant variables imprescindibles com ara la quantitat total de dades a copiar, sistemes, agents requerits etc.

L'objectiu d'aquest punt és conscienciar de la necessitat de realitzar un projecte de canvi de sistema de còpies de seguretat, partint com a punt de partida, quatre sistemes líders:

- Symantec NetBackup
- EMC NetWorker
- CommVault Simpana
- IBM Tivoli

Planificació

Aquest projecte implica la redefinició de la política de còpies de seguretat de la companyia i caldrà la implicació directa de Direcció per tal d'aprovar-la.

Les fases del projecte serien les següents:

1- **Definició de la política (temps aproximat: 1 mes)**
   b. Redacció de la política de còpies de seguretat i retenció general
   c. Redacció i acord amb direcció del RPO i RTO dels sistemes.
   d. Redacció d'un DRP (pla de recuperació de desastres)
   e. Redacció junt amb direcció del BCP (pla de continuïtat del negoci
   f. Signatura per part de direcció dels documents
   g. Publicació dels documents als usuaris

2- **Fase d'adquisició (temps aproximat: 1 mes)**
   a. Durant aquesta fase es comprarà la solució i tot el maquinari necessari per al seu funcionament (cabines de discos, servidors si s'escau, etc) així com l'adequació de la infraestructura

3- **Fase de configuració (temps aproximat: 1mes)**:
   a. Configuració de la solució
   b. Formació al personal d'IT

4- **Fase de proves (temps recomanat: de 2 a 3 mesos):**
   a. Durant aquesta fase es realitzaran les còpies paral·lelament amb els dos sistemes i es realitzaran les proves necessàries per a verificar el seu funcionament

5- **Implantació del sistema**
   a. Desconnexió de l'antic sistema de còpies de seguretat
   b. Salvaguarda de les antigues còpies en lloc segur, junt amb el seu lector

6.5 Eines Col·laboratives

Correu electrònic: Tal i com podem veure a l'apartat 5.3, la companyia disposa d'un servidor de correu electrònic que ja no està suportat pel fabricant (el final de manteniment de l'Exchange 2003 va ser a l'abril del 2014).

L'empresa no vol realitzar una gran inversió per a l'actualització del sistema de correu, havent d'evitar grans inversions en actius.

Els usuaris de la companyia i els seus directius estan molt acostumats al sistema client de Microsoft (Outlook) i no volen perdre funcionalitats.

Es proposa una migració del correu de la companyia al núvol amb un dels dos grans proveïdors de correu al Cloud: Google o Microsoft. Aquest sistema ofereix les següents avantatges:

- No requereix una inversió inicial en equips (servidors, discos...)
- No requereix una inversió inicial en llicenciament
- Conversió del CapEx en OpEx
- Disponibilitat de les últimes versions sense rellicenciament.
- Alliberament d'espai actualment ocupat per al correu

Respecte a la seguretat, cal esmentar que l'Agència Espanyola de Protecció de Dades ha declarat, després d'analitzar el servei i els models de contractes de l'Office 365, que aquests ofereixen als clients la solvència i les garanties adequades per exportar les seves dades personals a Microsoft a l'empara de la Llei Orgànica de Protecció de Dades (LOPD) confirmant a Microsoft com l'únic proveïdor Cloud que ofereix aquestes garanties, sent la primera companyia en complir la ISO27018.
Respecte a Google, des de juny de 2015 també adopta la ISO27018 com a estandard.

El preu de la solució pot variar entre dels 2€ als 8€ mensuals per usuari depenent de la capacitat de la bústia i el proveïdor escollit.

Caldria realitzar un estudi a fons sobre quina solució seria la més convenient, donat que tant Microsoft i Google tenen tot un ecosistema d'aplicacions interrelacionades i la decisió pot arribar a ser estratègica.

Missatgeria instantània / Videoconferència: Es recomana la implantació d'un sistema de missatgeria instantània i videoconferència de pagament per ús per tal d'evitar l'adquisició d'actius.
Els avantatges d'aquest tipus d'aplicacions son:

- Immediatesa en les comunicacions
- Estalvi de correus electrònics
- Videoconferències grupals sense necessitat d'anar a les sales habilitades per a tal efecte
- Col·laboració més eficaç entre els empleats
- Trucades i videotrucades sense cost des de l'extranger

Tant Google com Microsoft disposen de les seves solucions (Hangouts en cas de Google i Skype empresarial en el cas de Microsoft).

CAU (Centre d'Atenció a l'usuari): és important crear un Centre d'atenció a l'usuari amb un únic telèfon publicat el qual sempre serà contestat durant l'horari marcat.
Els objectius d'aquest CAU son els següents:

- Evitar les trucades directes als tècnics i evitar distraccions.
- Donar millor servei als usuaris evitant que situacions en que el tècnic no agafi el telèfon

És important definir uns indicadors clau per tal de monitoritzar el nivell servei del CAU. Algun dels indicadors poden ser:

- Trucades perdudes
- Usuaris amb més trucades
- Temps mitjà de trucada
- Departament amb més trucades

Gestió de projectes:
Actualment la companyia disposa de varis gestors de projectes instal·lats localment als ordinadors dels responsables dels projectes o caps de departament.

Es proposa l'adquisició d'un gestor de projectes online (SaaS) degut a que ofereixen grans avantatges en l'aspecte col·laboratiu com ara:

- tenir una visió global de tots els projectes de la companyia, l'activitat dels treballadors, planificacions futures, etc..
- estalvi de temps en comunicació via email, trucades, etc.
- Accessibilitat: Permetre la mobilitat gràcies al cloud.
- Cost: els gestors de projectes online ofereixen paquets de pagament per us molt assequibles
- Flexibilitat: el fet de ser pagament per us, es pot adaptar a les necessitats de cada empresa en cada moment
- Agilitat: en pocs minuts, tot l'equip pot estar treballant amb un nou projecte. Els temps d'implantació es redueixen dràsticament
- Facilitat d'ús: cada cop hi ha més competència i la facilitat d'ús de l'aplicatiu s'ha convertit en un cavall de batalla.

No analitzarem els diferents gestors de projectes online, degut a que cal fer un anàlisi de la tipologia de projectes, la quantitat d'usuaris que usin l'aplicació, la quantitat de projectes concurrents etc. Degut a que el llicenciament entre les diferents solucions varia molt (hi ha solucions que facturen per usuaris, d'altres per projectes actius, d'altres per espai, d'altres per tipus de metodologia, etc).

Cal que l'empresa prengui consciencia de les avantatges d'aquest tipus de solucions . A tall d'exemple en citem uns quants:

- ActiveCollab
- Assembla
- BaseCamp
- Confluence
- Producteev
- Teamwork
- Trello
- Wrikle
- ....

6.6 Eines de suport a IT

Com a punt i final de l'informe, cal establir una metodologia de treball a IT que asseguri:

- L'alineament de IT als objectius del negoci
- Arribar a la òptima efectivitat i eficiència de IT
- Controlar els costos en la provisió de serveis d'IT
- Aconseguir la satisfacció dels usuaris
- Facilitar l'ús de les TIC per tal d'aconseguir una avantatge competitiva
- Garantir, a través de processos ben definits, un cicle de millora continua per a l'entrega de serveis

Per tal d'aconseguir aquest canvi de filosofia es proposa seguir una pràctica basada en processos destinada a alinear l'estratègia dels serveis de tecnologia de la informació amb les necessitats de l'empresa: ITSM (*Information Technology Service Management*).

Els beneficis de ITSM son:

- Reducció i control de riscos en el compliment dels objectius de negoci
- Reducció de costos a llarg termini
- Demostrar el valor de IT a la organització
- Millora en la relació entre IT i els usuaris i proveïdors
- Capacitat de gestionar un major nombre de canvis
- Establiment i operació de processos sota les millors pràctiques auditables

La implementació de les eines de suport s'haurien de realitzar en tres fases ben diferenciades:

1. Eines de suport a l'usuari (Help Desk)
    a. Gestió d'incidències
    b. Gestió de problemes
    c. Administració d'inventari
    d. Gestió del coneixement

2. Eines de servei al client (Service Desk)
    a. Gestió del canvi
    b. Provisió de serveis interns
    c. Gestió de SLA per a incidències
    d. Petició de serveis

3. Eines d'administració de suport als serveis (IT Service Support Management Tools)
    a. Mobilitat
    b. Anàlisis i reporting
    c. ...

El següent gràfic de Gartner, mostra l'ecosistema d'aplicatius ITSM:

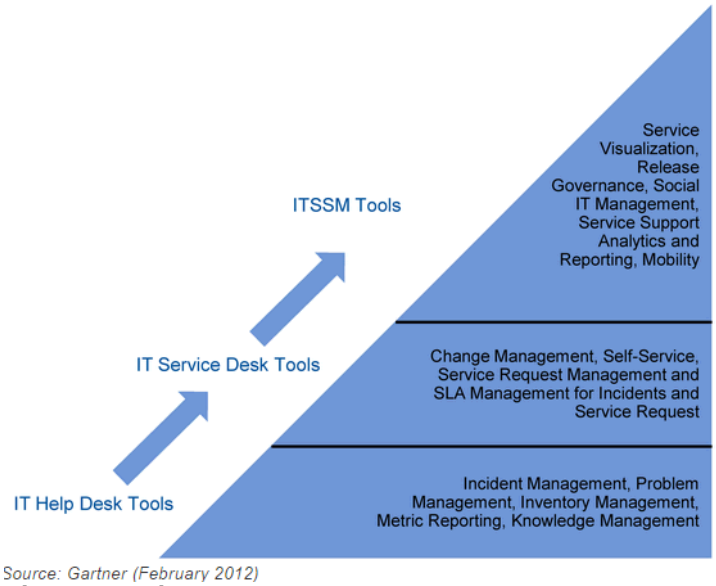


Figura 12: Eines ITSM

Queda fora de l'abast d'aquest estudi l'anàlisi acurat de les diferents opcions del mercat, donat que existeixen multitud d'opcions amb un cost econòmic molt variable.
Caldria realitzar un estudi sobre les necessitats, el pressupost assignat i la metodologia d'implantació de cadascuna de les solucions per tal d'oferir les alternatives adequades

7. Conclusions

Els principals objectius d'aquest projecte, eren:

- Entendre el paper d'IT dins d'una organització concreta
- Analitzar la situació organitzativa i tècnica del departament
- Realitzar un proposta de millora dels sistemes d'Informació que serveixi de base al CIO de la companyia per a la realització del pla estratègic de Sistemes d'informació

Ha estat un treball on l'anàlisi inicial de la situació tècnica i organitzativa del departament d'IT ha estat la part fonamental.
Un bon estudi inicial, entendre la situació i sobretot, a on es vol arribar es clau per tal de realitzar una proposta coherent.

Partint de la situació base, s'ha vist que el projecte anava agafant grans dimensions i s'ha hagut de escurçar. L'apartat menys desenvolupat és la proposta de millora en alguns aspectes, degut a que intervenien moltes variables i l'extensió del projecte podria haver-se allargat massa

S'ha seguit la planificació inicial i s'ha hagut de realitzar algun ajust respecte a la proposta inicial, sobretot en l'apartat de la proposta de millora (hagués volgut realitzar una proposta més acurada però ha faltat temps)

Aquest treball és un bon punt de partida per tal de realitzar un pla estratègic de sistemes d'informació i, coneixent el pressupost i les prioritats, desenvolupar una millor proposta de millora.

Com a conclusió final, he d'admetre que la idea del projecte era molt extensa i abstracta. Aquesta falta d'acotació ha fet que m'hagi costat molt encarar i desenvolupar el treball.

8. Glossari

Commutador[1]: aparell de xarxes que permet agrupar un conjunt d'ordinadors i fer que passin pel mateix cable.

Concentrador[2]: és un dispositiu de xarxa que permet agrupar un conjunt de dispositius Ethernet en un mateix segment de xarxa. Actua al 1r nivell o nivell físic, sense entrar per tant a analitzar les adreces MAC de destí

CPD: Centre de procés de dades. Instal·lació on hi resideixen els sistemes informàtics com ara commutadors, encaminadors i servidors.

Broadcast: Es un missatge des d'un dispositiu connectat a una xarxa a tots els demés dispositius de la xarxa. Els broadcasts son una eina necessària i útil usada per molts protocols per a permetre la comunicació de dades a les xarxes.

Domini de Broadcast: Els broadcasts estan continguts dins d'una xarxa. Es per aquest motiu que una xarxa també es coneix com *domini de Broadcast.* L'administració de la mida dels dominis de broadcast dividint una xarxa en diferents subxarxes assegura que el rendiment de la xarxa i dels dispositius no es degradin.

DMZ: *Zona desmilitaritzada.* és una subxarxa d'àrea local (LAN) situada entre la xarxa privada d'una organització i la xarxa externa, normalment Internet.
Amb l'ajuda d'un Tallafocs les connexions cap a la xarxa DMZ són permeses tant des de la xarxa exterior com des de la xarxa privada, però no són permeses en canvi, les connexions des de la DMZ cap a la xarxa privada de l'organització.

MPLS: Xarxa privada IP que combina la flexibilitat de les comunicacions punt a punt i la fiabilitat i seguretat dels serveis Frame Relay o ATM. Ofereix alts nivells de rendiment i priorització de tràfic, així com aplicacions de veu i multimèdia.

TIA 942: és un estàndard publicat per la *Telecomunications Industry Association (TIA)* a l'abril del 2005, y es divideix en 8 punts y 9 annexes. El propòsit d'aquesta norma és recopilar una sèrie de guies y pautes per al el disseny y construcció de Centre de Proces de dades

RPO (*Recobery Point Objective)***:** és el temps màxim establert des de la última còpia de seguretat o la quantitat de dades (en temps) que es pot permetre l'empresa de perdre en cas de desastre

RTO (*Recobery Time Objective)***:** és el temps objectiu per a la reanudació del servei en cas de desastre. Quan més petit sigui aquest valor, major haurà de ser la inversió en la infraestructura

BIA (*Business Imact Analysis)***:** és usat per estimar l'afectació que podria patir una organització com a resultat d'un incident o desastre.

STP *(Spanning Tree Protocol)*: Protocol de xarxa de capa 2 de la OSI que analitza i evita els possibles bucles que es puguin presentar

RADIUS (Remote Authentication Dial-In User Server). És un protocol d'autenticació i autorització per a aplicacions d'accés a la xarxa o mobilitat IP. Utilitza el port 1813 UDP per establir les seves connexions

SSID: *(Service Set Identifier)* és una seqüència de caràcters que identifica de manera única una xarxa sense fils d'àrea local

CapEx: Inversions de capital. Usualment son compres de béns amb una vida útil major d'un any, amb un tipus de comptabilització de propietat

OpEx: Despeses Operatives. Són costos necessaris per a mantenir un negoci funcionant. El pagament acostuma a ser mensual

9. Bibliografia

[1]: *Commutador (Xarxa), (s.f). A Wikipedia.* Recuperat el 20 de Març de 2016 de https://ca.wikipedia.org/wiki/Commutador_(xarxa)

[2]: *Concentrador, (s.f)*. A *Wikipedia*. Recuperat el 20 de Març de 2016 de https://ca.wikipedia.org/wiki/Concentrador

[3]: *DMZ, (s.f)*. A *Wikipedia*. Recuperat el 27 de Març de 2016 de https://ca.wikipedia.org/wiki/DMZ

[4]: *RPO, (s.f)*. A *TrendsInycom*. Recuperat el 5 d'Abril de 2016 de http://trends.inycom.es/diferencia-rto-vs-rpo/

[4]: *RTO, (s.f)*. A *TrendsInycom*. Recuperat el 5 d'Abril de 2016 de http://trends.inycom.es/diferencia-rto-vs-rpo/

[5] DOWNES, LARRY. *La màquina estratègica*. Ed. HarperBusiness, 2002.

[5] FERNÁNDEZ, JOSÉ ANTONIO. *La tecnología de la información, factor estratégico en la segunda mitad de los 90*. Harvard Deusto Business Review, núm 64, novembre-desembre, Ed. Deusto, Bilbao, 1994.

[5] LIENDO AREVALO, MILNER DAVID. *Les tecnologies de la informació dins de la estrategia competitiva de les PYMES*. Mèxic. Ed. Alay Ediciones S.L., 2002.

[5] SYNNOT, W. y GRUBER, W.H. *Information Resource Management- Opportunities and strategics for the 1980´s*. John Wiley, New York, 1981.

[A1_1]: Directive 2003/94/CE (EU GXP), Principles and guidelines of good manufacturing practices for medicinal products for human use

[A1_2]: GMP-UE: ANNEX 11: Sistemes informatitzats i ANNEX 15: Qualificació i Validació.

[A1_3]: GAMP Guide. Validation of Automated Systems in Pharmaceutical Manufacture. Version: V5.0.

[A1_4]: PIC/S: Good Practices for Computerized Systems in Regulated "GxP" Environment. September 2003.

10. Annex1: Metodologia Anàlisi de riscos

10.1 Metodologia

S'aplica la metodologia d'anàlisis de riscos descrita a la guia GAMP (*Good Automated Manufacturing Practices*) editada per la ISPE (*International Society for Pharmaceutical Engineering*).

S'ha optat per aquesta metodologia perquè està específicament enfocada a sistemes informatitzats i té una amplia difusió en un sector altament regulat, com és el farmacèutic-sanitari (sector al qual pertany l'empresa *Maldecap Medicaments S.A*)

L'elaboració d'aquesta metodologia es basa en un conjunt de normatives i guies de referència descrites a la bibliografia com [A1_1] fins [A1_4]

10.2 Avaluació de Riscos

L'Apèndix M3, punt 5.4 de la GAMP5, estableix una metodologia d'anàlisi de riscos basada en tres paràmetres: *Severitat*, *Probabilitat* i *detectabilitat*.

Severitat: de manera genèrica, és l'impacte que tindria una eventual fallida en la salut del pacient, la qualitat del producte o la integritat de les dades. Amb la finalitat de concretar més, en aquests anàlisis s'entendrà severitat l'impacte que pugui tenir una fallida en el sistema informàtic analitzat en el compliment de les normes GAMP

Probabilitat: fa referència a la probabilitat que es produeixi una fallida en el sistema

Detectabilitat: és la probabilitat que una fallida sigui detectada per als usuaris del sistema

Per a cada funcionalitat o aspecte dels sistemes analitzats, s'identifiquen les seves possibles fallides i es puntuen els tres paràmetres en una escala relativa. En funció de la puntuació assignada, es calcula el nivell de risc de cadascuna de les funcionalitats. Les funcionalitats amb un nivell de risc alt, seran l'objectiu prioritari de l'estudi

10.3 Classes de Risc

El primer pas per tal d'avaluar el risc associat a una funcionalitat del sistema és determinar la seva severitat i la seva probabilitat. A partir dels valors d'aquests paràmetres s'obté la classe de risc analitzat

Severitat: Nivell d'impacte que el sistema analitzat té sobre les dades o sobre el treball diari dels usuaris

Alta:	Impacte negatiu major
Media:	Impacte negatiu moderat
Baja:	Impacte negatiu menor

Probabilitat de fallida: Probabilitat que la fallida es produeixi.

Alta:	La fallida pot produir-se sovint
Media:	La fallida pot produir-se amb certa freqüència
Baja:	La fallida pot produir-se en rares ocasions

La següent taula mostra com s'estableix la classe de risc analitzat, en funció de la severitat i la probabilitat:

Severtat \ Probabilitat	Baixa	Mitja	Alta
Alta	Risc de **Classe 2**	Risc de **Classe 1**	Risc de **Classe 1**
Mitja	Risc de **Classe 3**	Risc de **Classe 2**	Risc de **Classe 1**
Baixa	Risc de **Classe 3**	Risc de **Classe 3**	Risc de **Classe 2**

10.4 Nivell de Risc

Segon pas és puntuar el Nivell de risc analitzat, a partir de la seva classe i de la seva detectabilitat.

Detectabilitat (probabilitat de detecció de l'error): determina la facilitat de detecció de l'efecte/fallida en cas que ocorregués:

Alta:	Detecció segura
Mitja:	Detecció raonable
Baixa:	Detecció difícil

La següent taula mostra com es puntua el nivell de risc analitzat:

Classe de Risc \ Detectabilitat	Alta	Mitja	Baixa
1	**Nivell Mitjà**	**Nivell Alt**	**Nivell Alt**
2	**Nivell Baix**	**Nivel Mitjà**	**Nivell Alt**
3	**Nivell Baix**	**Nivell Baix**	**Nivell Mitjà**

10.5 Matriu d'Anàlisi de riscos

L'Anàlisi de riscos es complerta identificant en una matriu totes les funcions o processos que afecten al sistema. Per a cada funcionalitat s'indiquen les possibles fallides i es seves conseqüències (FMEA, *Failure Mode Effects Analysis*). A partir de les possibles identificades per a cada funció o procés, es puntuen els factors de severitat, probabilitat i detectabilitat i es calcula el Nivell de risc resultant.

A la última columna de la matriu es recullen les verificacions i canvis a realitzar al sistema.

11. Annex 2: Disseny de xarxes locals

11.1 Topologia

En el disseny de la topologia de les xarxes, seguiré el model proposat per *Cisco Systems, Inc*. La qual distingeix 3 capes lògiques amb un model jeràrquic:

Capa d'accés: La capa d'accés a la xarxa és el punt a on es connecten els dispositius finals. En aquesta capa es controla als usuaris i l'accés de grups de treball o els recursos de xarxa.
En aquesta capa és on es produeix la connexió amb els elements de xarxa, com ara equips, impressores, etc.

Capa de distribució: Les funcions d'aquesta capa és proveir d'enrutament, filtratge, accés a la xarxa WAN i determinar els paquets que han d'arribar a la següent capa (nucli). A més a més, és la responsable de la segmentació de la xarxa en múltiples dominis de difusió (*broadcast)*

Capa de Nucli (core): La seva única funció és commutar el tràfic tan ràpid com sigui possible d'una manera eficaç i veloç (la latència i la velocitat son els principals factors d'aquesta capa).
El tràfic és derivat a la capa de nucli des de la capa de distribució tan sols si és necessari i una caiguda afectaria a tots els usuaris, pel que la tolerància a fallides és molt important

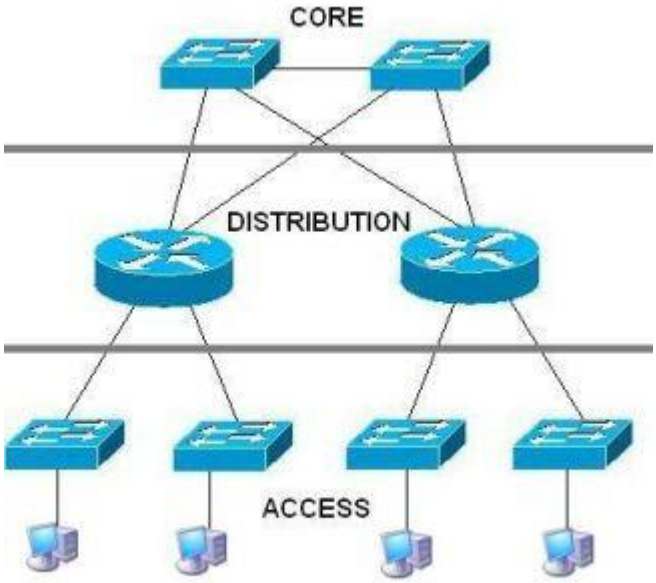


Figura 13: Topologia de xarxa segons Cisco

11.2 Divisió dels equips per grups (subxarxes)

Els principals motius per a separar els dispositius en grups lògics son els següents:

Rendiment: Un gran nombre d'equips connectats a una sola xarxa poden produir un gran volum de transit que podrien fer minvar (si no els saturen) els recursos de xarxa com ara l'ample de banda i enrutament.
L'administració de la xarxa i el transit de control (sobrecàrrega) també augmenten amb la quantitat de dispositius.

Un dels factors que contribueixen de manera significativa a produir aquesta sobrecàrrega poden ser els *broadcasts*.

Seguretat: Dividir una xarxa és un mitjà per a assegurar les comunicacions i les dades de l'accés no autoritzat, ja sigui per a usuaris dins de l'organització o fora d'ella. La seguretat entre xarxes s'implementa mitjançant un dispositiu intermedi (router o Firewall) al perímetre de la xarxa.

Administració d'adreces: Internet esta format per milions de dispositius i cadascun d'ells s'identifica per la seva adreça única de xarxa (adreça Ip). Si cadascun dels dispositius ha de conèixer l'adreça de cadascun dels demés dispositius, seria imposar una càrrega de processament que degradaria el rendiment.
Dividir grans xarxes per tal que estiguin agrupats els dispositius que necessiten comunicar-se, redueix la càrrega innecessària de tots els dispositius per tal de conèixer totes les adreces.

11.3 VLANs

Una VLAN permet que un administrador de xarxa creï grups de dispositius connectats a la xarxa d'una manera lògica que actuen com si estiguessin a la seva pròpia xarxa independent, inclús si comparteixen una infraestructura comú amb d'altres VLAN.

Una VLAN és una subxarxa IP separada de manera lògica. Les VLAN permeten que xarxes d'IP i subxarxes múltiples existeixin dins la mateixa xarxa commutada.
Per tal que els dispositius es comuniquin dins la mateixa VLAN, cadascun ha de tenir una adreça IP i una màscara de subxarxa que pertanyi dins la VLAN.
Als commutadors s'ha de donar d'alta les VLANs i a cada port assignar-li la VLAN corresponent (d'aquesta manera, dos equips connectats físicament al mateix commutador no significa que es puguin comunicar)

Els dispositius connectats a dos VLANs diferents necessiten un enrutador (Capa 3) o un switch de capa 3.

Les avantatges de les VLAN son les següents:

Seguretat: Els grups que disposen de dades sensibles es poden separar de la resta de la xarxa, disminuint les possibilitats que es produeixin robatoris d'informació confidencial.

Reducció de costos: l'estalvi en el cost ve donat per la manca d'actualitzacions de maquinari i un us més eficient dels enllaços i ample de banda existents

Millor rendiment: La divisió de les xarxes planes de capa 2 en múltiples grups lògics de treball (dominis de Broadcast) redueix el transit innecessari a la xarxa i potencia el rendiment

Mitigació de la tempesta de broadcast: La divisió d'una xarxa en VLANs redueix la quantitat de dispositius que poden participar en una tempesta de broadcast.

Major eficiència del personal d'IT: Les VLAN faciliten l'administració de la xarxa donat que els usuaris amb requeriments similars comparteixen la mateixa VLAN. Quan s'instal·la un commutador nou, totes les polítiques i procediments que es van configurar per la VLAN particular s'implementen quan s'assignen els ports.

12. Annex 3: Estàndards Wi-Fi

Les xarxes Wi-Fi permeten la connectivitat d'equips mitjançant ones de ràdio. Existeixen diferents estàndards que parteixen de l'inicial 802.11
Les característiques de cadascun varia (freqüència, ample de banda, velocitat i abast).

Els estàndards més usats actualment son els següents:

Protocol	Freqüència	Senyal	Ample de Banda	Velocitat teòrica màxima
802.11	2,4 GHz	FHSS o DSSS	22 MHz	2 Mbps
802. 11a	5 GHz	OFDM	20MHz	54 Mbps
802. 11b	2,4 GHz	HR-DSSS	22MHz	11 Mbps
802.11g	2,4 GHz	OFDM	20MHz	54 Mbps
802. 11n	2.4 o 5 GHz	OFDM	20/40 MHz	600 Mbps
802. 11ac	5 GHz	256 QAM	80/160 MHz	1.3 Gbps

Taula 6: Estàndars Wi-Fi

13. Comparativa de fabricants

13.1 Xarxa local

Basant-nos en els documents d'IDC (http://www.idc.com/) trobem 5 grans fabricants mundials de commutadors que dominen el mercat mundial: Cisco, Juniper, HP, Arista i Huawei:

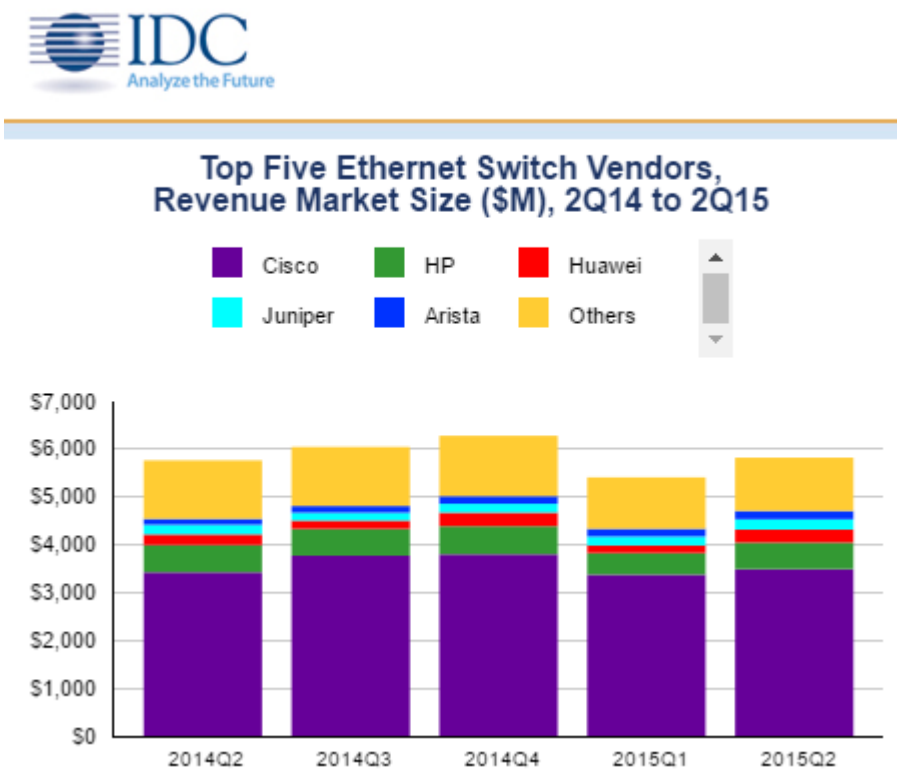


Figura 14: Principals fabricants de commutadors

Per al projecte d'adequació de la xarxa local es necessitaran bàsicament dos tipus de commutadors:

- Commutadors de nucli: commutadors de capa 3 a velocitat 10Gps i opcions de fibra
- Commutadors d'accés: commutadors de capa 2 a velocitat 1Gps i enllaços a 10Gps

A continuació descrivim les avantatges i desavantatges de cada fabricant:

Fabricant	Fortaleses	Debilitats
Cisco	Líder del Mercat Facilitat en trobar proveïdors Pla de formació molt consolidat Possibilitat d'una migració progressiva Qualitat del producte	Preu elevat Protocols propietaris
HP	Preu Facilitat en trobar proveïdors	Cost de formació (el sistema és totalment diferent a l'actual) Dificultat per a realitzar una migració progressiva
Huawei	Rendiment econòmic elevat (velocitat/preu)	Poca implantació a Espanya

	Qualitat del producte Gran increment de vendes en els últims anys	Possible dificultat en trobar personal qualificat Alt cost en formació Dificultat en realitzar una migració progressiva
Juniper	Qualitat del producte elevada Competència directa de Cisco Bona relació qualitat/preu Gran increment de vendes en els últims anys a nivell mundial	Possible dificultat en trobar personal qualificat Alt cost en formació Dificultat en realitzar una migració progressiva
Arista	Qualitat del producte elevada	Possible dificultat en trobar personal qualificat Alt cost en formació Dificultat en realitzar una migració progressiva

Taula 7: Comparativa fabricants de commutadors

A continuació es detallen els preus orientatius dels dos models tipus de commutadors necessaris per al projecte. Per a la comparativa hem escollit els tres principals fabricants:

Marca	Model Switch Nucli	Preu unitat	Model Switch accés	Preu unitat
Cisco	WS-C4928-10GE	25.000€	WS-C2960X-48TD-L	1.900€
HP	HPE5900AF-48XG-4QSFP+	17.000€	HP2530-48G	1.500€
Huawei	S6720	13.000€	S5720	1.000€

Taula 8: Comparativa costos de commutadors

13.2 Xarxa Wifi

Per tal de realitzar una selecció de les companyies a analitzar, ens basarem en el quadrant màgic de Gartner® on anualment analitza els fabricants en quatre quadrants: Empreses líder, retadores, empreses nínxol i visionaries.
Per a l'estudi escollirem dues empreses líder i dues de visionaries.

Segons es pot veure en la figura 12, trobem dues empreses líders al mercat: Cisco i Hewlett Packard (gràcies a l'adquisició d'Aruba Networks).
Com a empreses visionaries hem triat Extreme Networks i Aerohive (que repeteix quadrant per segon any consecutiu).

Figura 15: Quadrant de Gartner 2015 - Wireless

Fabricant	Fortaleses	Debilitats
Cisco / Meraki	Líder del Mercat Facilitat en trobar proveïdors Meraki ofereix un sistema de controladors basat en Cloud Firewall integrat en el cas de Meraki	Preu elevat Protocols propietaris Dificultat de gestió en cas de Cisco En el cas de Meraki aconsellen adquirir els seus commutadors
HP / Aruba	Facilitat en trobar proveïdors Solidesa contrastada Firewall integrat	Disposa de la tecnologia sense controlador, però realment és un punt d'accés que exerceix el rol de controlador
Extreme Networks	Rendiment molt alt dels dispositius	Necessitat de controladors Dificultat en trobar suport a Espanya
Aerohive	Únic fabricant que ofereix una solució sense controladors (totalment autònoms). Segon any consecutiu al quadrant de visionaris Gran relació qualitat/preu Facilitat de gestió	Poca implementació a l'Estat espanyol És l'empresa més petita de les analitzades (era una Startup al 2009)

Taula 9: Comparativa fabricants WiFi

A continuació es detallen els preus orientatius dels dos models tipus de commutadors necessaris per al projecte. Per a la comparativa hem escollit els tres principals fabricants:

Marca	Model punt d'accés	Preu unitat	Model Controlador	Preu unitat
Meraki	Meraki MR34 802.11ac + 3 anys mant.	1500€	----	
HP/Aruba	Aruba 320 series 802.11ac + 3 anys mant	1500€	----	
Extreme Networks	AP3825 802.11ac	650€	C25 (up to 100 APs)	5.995€
Aerohive	AP 230 802.11ac + 3 anys mant	950€	----	

Taula 10: Comparativa costos de WiFi

Per tal de valorar la solució, es valoraran els pros i els contres i es realitzarà una puntuació basada en els següents requisits (depenent del seu grau de compliment):

Requisit 1: Punts d'accés amb tecnologia 802.11ac – màxim **20 punts**
Requisit 2: Gestió unificada de tot el parc de punts d'accés – màxim **8 punts**
Requisit 3: Senzillesa i agilitat alhora de desplegar la solució i nous punts d'accés – màxim **9 punts**
Requisit 4: Control d'accés a nivell d'aplicació (tallafocs), gestió d'ample de banda i priorització de transit – màxim **6 punts**
Requisit 5: Punts d'accés autònoms sense necessitat de controladores – màxim **8 punts**
Requisit 6: Preu de la solució – màxim **10 punts**
Requisit 7: Altres característiques no descrites: màxim **5 punts**

A continuació es detalla la puntuació assignada a cadascuna de les solucions i un petit comentari:

Cisco/Meraki
Requisit 1: **20 punts**. La companyia disposa de punts d'accés amb tecnologia 802.11ac
Requisit 2: **8 punts.** Tots els punts d'accés es poden gestionar via web de manera centralitzada
Requisit 3: **6 punts.** Meraki recomana la instal·lació de commutadors de la mateixa casa per tal que el rendiment sigui òptim
Requisit 4: **6 punts**. El sistema disposa de tallafocs i gestió d'ample de banda
Requisit 5: **6 punts.** Tot i que està basat en cloud, el sistema continua usant controladors, però aquests estan redundats i al Cloud.
Requisit 6: **8 punts**.
Requisit 7: **1 punts.** Suport del principal fabricant a nivell mundial

Puntuació total de la solució Meraki/Cisco: 55 punts

HP/Aruba
Requisit 1: **20 punts**. La companyia disposa de punts d'accés amb tecnologia 802.11ac
Requisit 2: **8 punts.** Tots els punts d'accés es poden gestionar via web de manera centralitzada
Requisit 3: **5 punts.** El desplegament d'aquesta solució és més complexa que Meraki o Aerohive
Requisit 4: **6 punts**. El sistema disposa de tallafocs i gestió d'ample de banda
Requisit 5: **5 punts.** El sistema no és sense controlador natiu. Usa un dels punts d'accés com a Controlador virtual.
Requisit 6: **8 punts**.
Requisit 7: **0 punts.**

Puntuació total de la solució Aruba/HP: 52 punts

Extreme Networks
Requisit 1: **20 punts**. La companyia disposa de punts d'accés amb tecnologia 802.11ac
Requisit 2: **4 punts.** La gestió es realitza per controladora
Requisit 3: **5 punts.** El desplegament d'aquesta solució és més complexa que les altres donat que requereixen controladores addicionals
Requisit 4: **6 punts**. El sistema disposa de tallafocs i gestió d'ample de banda
Requisit 5: **0 punts.** Es necessiten controladores addicionals.
Requisit 6: **2 punts**.
Requisit 7: **0 punts.**

Puntuació total de la solució Extreme Networks: 37 punts

Aerohive Networks
Requisit 1: **20 punts**. La companyia disposa de punts d'accés amb tecnologia 802.11ac
Requisit 2: **8 punts.** Tots els punts d'accés es poden gestionar via web de manera centralitzada
Requisit 3: **9 punts.** De les quatre solucions és la mes senzilla d'administrar i implementar
Requisit 4: **6 punts**. El sistema disposa de tallafocs i gestió d'ample de banda
Requisit 5: **8 punts.** És la única solució lliure de controladores gràcies a la tecnologia de panell d'abella a on cada punt d'accés actua de manera independent
Requisit 6: **10 punts**.
Requisit 7: **1 punts.** Destaca la seva senzillesa i la rapidesa en la seva implantació

Puntuació total de la solució Aerohive: 62 punts

13.3 Còpies de seguretat

És impossible realitzar un estudi econòmic de les diferents solucions de còpies de seguretat i molt menys seleccionar una guanyadora, degut a que es desconeix per complert la capacitat d'informació a la qual s'ha de realitzar còpies de seguretat.
El preu de la solució pot variar molt depenent de la informació a copiar, la quantitat d'agents necessaris, etc.

Con a guia, prendrem els següents requisits:

1- El programari ha de permetre la còpia a disc
2- La còpia en disc ha de ser deduplicada, millor si la dedupliació es realitza a l'origen
3- S'ha de poder realitzar còpies a localitzacions remotes, permeten control d'ample de banda
4- La solució ha de ser agnòstica al maquinari (no ha de dependre del model o marca de cabines de discos, servidors o lectors magnètics)
5- El sistema ha de permetre la còpia de seguretat de sistemes antics i heterogenis (degut a la gran quantitat de sistemes industrials existents)

Basant-nos amb aquests requisits (sobretot en el punt número 5), es descarta solucions de backups en sistemes virtualitzats i solucions propietàries de cabines de discos (snapshots) per no ser agnòstiques al maquinari.

De nou ens fixarem en el quadrant de Gartner® sobre sistemes de backup:

Figura 16: Quadrant de Gartner 2015 - Programari de Còpies de seguretat

Segons es pot veure en la figura 14, trobem quatre empreses líders al mercat: EMC, IBM, CommVault i Symantec. Com a empreses visionaries hem triat Veeam Backup

Mostrarem a continuació les fortaleses i debilitats de cadascuna de les principals solucions:

Fabricant	Fortaleses	Debilitats
EMC	Líder del Mercat Aquisició de múltiples solucions de backup els darrers anys	Poca integració entre els seus propis productes Dificultat en realitzar els upgrades de versions
IBM Tivoli	Escalable per a grans volums de dades Suport de snapshots de múltiples fabricants	La interfície de TSM és molt poc amigable El preu pot ser molt elevat
CommVault Simpana	Suport de snapshots de múltiples fabricants Única consola per a gestionar totes les tasques Alta integració amb multitud de fabricants de cabines de discos	El preu del manteniment pot arribar a ser molt elevat
Symantec NetBackup	Escalable a grans volums de dades Venda d'apliances (maquinari amb tot el sistema integrat, disc i programari)	Existeixen moltes queixes sobre l'atenció al client El cost global pot ser molt elevat
Veeam	Gran senzillesa en realitzar les còpies	Només protegeix entorns virtualitzats (Es descarta la solució)

Taula 11: Comparativa programari de Còpies de Seguretat