ESTUDI d' IMPLANTACIÓ D'UN SISTEMA
CLOUD STORAGE

Nom: Ivan López Garrido

Programa: Màster interuniversitari de Seguretat de les tecnologies de la informació i de les comunicacions (MISTIC)
Consultor: María Francisca Hinarejos Campos

Centre: Universitat Oberta de Catalunya, UOC

Tarragona, Gener de 2016

A) Copyright

© Ivan López Garrido
Reservats tots els drets. Està prohibit la reproducció total o parcial d'aquesta obra per qualsevol mitjà o procediment, compresos la impressió, la reprografia, el microfilm, el tractament informàtic o qualsevol altre sistema, així com la distribució d'exemplars mitjançant lloguer i préstec, sense l'autorització escrita de l'autor o dels límits que autoritzi la Llei de Propietat Intel.lectual.

Resum

En els últims anys, l'aparició dels sistemes Cloud Storage han obligat a canviar la visió de les empreses en quant a l'emmagatzemament de fitxers. Disposar d'un Cloud Storage per a que els usuaris puguin accedir a la informació des d'arreu on es requereixi, s'ha convertit en un objectiu prioritari i indispensable en la majoria de mitjanes i grans corporacions. La mobilitat i l'ús de múltiples i diferents dispositius per part dels seus empleats obliguen a les empreses a adaptar-se a aquestes noves necessitats.

El projecte descrit en aquest document és el resultat de l'anàlisi de diferents solucions de *Cloud Storage* existents al mercat. L'objectiu principal d'aquest projecte ha estat estudiar la viabilitat tècnica i econòmica d'implantar un sistema de *Cloud Storage* en una corporació mitjana que requereix d'un espai d'emmagatzemament al núvol per a que els seus usuaris pugin emmagatzemar fitxers i ser accessibles des de qualsevol ubicació i dispositiu, i alhora crear espais col.laboratius entre treballadors per l'intercanvi de documents.
L'anàlisi s'ha basat en estudiar les diferents solucions en base a les funcionalitats que ofereixen, la seguretat en els mecanismes d'autenticació, transmissió de dades, xifrat, etc.., així com la integració amb els serveis corporatius per a l'aprovisionament dels usuaris i l'accés al sistema.

Abstract

In recent years, the appearance of Cloud Storages has changed the view of the corporation in terms of the storage systems. Set up a Cloud Storage for corporate users to access the information from wherever required, has become an indispensable priority in most medium and large corporations. The mobility and the use of many different devices by their employees have forced companies to adapt to these new needs.

The project described in this document is the analysis result of different Cloud Storage solutions at the current market. The main target of this project have been study the technical and economical viability of implementing a Cloud Storage system in a medium corporation, which require a storage system in the Cloud, where the employers could upload, save and access files from wherever and from any device, besides, create collaborative spaces between employees to share documents and files.
This analysis has been performed in the study of different solutions, based on the features, the authentication security mechanisms, data transmissions security, encryption,.. and also, the corporate services integration for provisioning users and the final access to the system.

Índex

1. Introducció

La majoria de les actuals grans corporacions, amb un nombre de treballadors elevat, estan fragmentades, normalment, en diferents seccions, departaments, seus, etc.. Aquestes treballen conjuntament, amb la corresponent necessitat de comunicació entre el seu personal. Cada cop és més freqüent, entre els usuaris, compartir recursos i infraestructures tecnològiques com per exemple un sistema d'emmagatzematge de fitxers comú, al que els usuaris puguin accedir-hi des de qualsevol ubicació, mitjançant un ordinador, tauleta, mòbil o qualsevol altra dispositiu que disposi d'accés a Internet i suporti aquesta funcionalitat.

Des de fa uns anys és cada cop més comú que els usuaris de la corporació, utilitzin espais d'emmagatzematge de fitxers al núvol, on emmagatzemen fitxers i documents per després utilitzar-los fora de l'oficina, o fins i tot, per compartir-los amb altres usuaris. No totes les corporacions disposen d'aquests espais, pel que els usuaris opten per utilitzar els serveis de fitxers al núvol que ofereixen grans empreses tecnològiques com *Dropbox, Apple, Microsoft,* etc.. de forma gratuïta o de pagament (en cas de desitjar una capacitat major). Aquests espais per emmagatzemar fitxers personals són utilitzats des de qualsevol dispositiu amb accés a Internet, els quals només requereixen d'una autenticació prèvia de l'usuari per tenir-ne accés als fitxers.

Aquesta idea i/o activitat cada cop està més estesa entre els usuaris, i molt sovint, aquests utilitzen comptes personals per emmagatzemar fitxers i dades de la pròpia corporació amb la intenció d'utilitzar-lo en altres ubicacions, com per exemple, per treballar des de casa, per treballar mentre estan de viatge o en altres seus de la pròpia companyia, o simplement per poder tenir accés amb les seves tauletes o mòbils. Un altre gran ús d'aquests espais d'emmagatzemament en les corporacions, és el de compartició de fitxers entre diferents treballadors o departaments. Molt sovint, per poder treballar conjuntament sobre documents, fitxers, base de dades, etc.. entre diferents departaments que no tenen una connectivitat directa entre ells, s' utilitzen eines com aquestes per fer-ho, amb els perills o possibles incidents de seguretat que aquestes pràctiques poden comportar, per exemple, fuga d'informació, pèrdua de dades, accés no desitjat, etc..

Dins d'aquest marc, moltes d'aquestes corporacions, es veuen amb la obligació d'implantar una solució que doni resposta a aquestes necessitats d'emmagatzematge compartit i accessible des de qualsevol ubicació i dispositiu amb accés a Internet, és a dir, la necessitat d'implantar un sistema d'emmagatzematge al núvol on els seus treballadors disposin d'un espai personal, així com d'altres de compartits amb altres usuaris, i alhora, un espai comú per a tots els treballadors d'un mateix departament, seu o organització autònoma que ho requereixin.

En el cas propi de la corporació "OREV S.A." s'ha iniciat el projecte d'implantació d'un sistema d'emmagatzematge al núvol que doni resposta a la necessitat que els diferents departaments i els seus treballadors tenen de disposar d'un espai per emmagatzemar dades corporatives i que estiguin disponibles des d'una connexió a Internet.

L'accés al sistema haurà de poder realitzar-se des de qualsevol ubicació, mitjançant un client web, client d'escriptori o dispositiu mòbil, tot mitjançant una autenticació prèvia de l'usuari amb el sistema d'autenticació de la corporació "SingleSignOn", utilitzat per la majoria d'aplicacions corporatives.

1.1. Justificació

Aquest projecte s'ha iniciat per un motiu de necessitat, on ha prevalgut la tecnologia a utilitzar en el futur sistema, una tecnologia basada en el *Cloud Storage* i les mesures de seguretat que aquesta incorpora. Alhora s'ha intentat que aquest tingui el menor impacte d'implantació possible, respectant la situació econòmica que avui en dia afronten les corporacions, intentant no sortir dels límits pressupostaris establerts.

Actualment, la corporació disposa d'un sistema de fitxers corporatiu en el qual, els usuaris tenen els seus espais personals i comparteixen espais col.laboratius entre el personal de cada departament i entre departaments. Aquest sistema té grans limitacions d'escal.labilitat, flexibilitat i disponibilitat per raons d'obsolescència i el seu elevat cost econòmic tant d'expansió com de manteniment.
A més a més, aquest no permet accessibilitat des de fora de la xarxa interna de la corporació, i departaments que es troben en altres seus o ubicacions, no tenen accés directe. Aquest tampoc disposa de solucions per poder accedir-hi des de qualsevol dispositiu, és a dir, només és accessible des de ordinadors amb sistema operatiu *Windows* amb el client corresponent prèviament instal.lat. Per aquest motiu, es pretén que el nou sistema tingui accessibilitat directa des d'Internet per mitjà de qualsevol dispositiu amb connectivitat i que alhora, disposi d'una interfície amigable i intuïtiva.

Aquest projecte és un estudi previ d'una solució adient a les necessitats que s'han descrit, un anàlisi de les funcionalitats i mesures de seguretat que aquesta incorpora i de la infraestructura on residirà. A més s'hi incorpora el projecte d' implantació d'un entorn pilot del futur sistema per tal que aquest pugui ser testejat per un conjunt d'usuaris finals, una sèrie de responsables tècnics i directius de la corporació que validin i donin conformitat a la solució i aprovin la seva implantació final.

Per motius de confidencialitat en aquest projecte s'ha ocultat el nom de la corporació i s'ha substituït per un de fictici. Tanmateix, s'han ocultat altres dades, com són noms d'usuaris, noms de servidors, i altres dades de la corporació per evitar possibles conflictes amb la seva seguretat.

Així doncs, algunes dades que no alteren el resultat final, han sigut modificades o no incloses en aquest projecte, ja que podrien comprometre la seguretat de les infraestructures tecnològiques de la corporació, la confidencialitat de la informació interna, la seguretat dels propis treballadors, entre altres, per tal d'evitar possibles atacs en trobar-ne informació útil o vulnerabilitats en la solució instal·lada que s'ha descrit en aquest projecte.

1.2. Objectius

L'estudi d' implantació del nou sistema d'emmagatzematge de fitxers al *Cloud*, té com a finalitat la consolidació en un únic sistema d'emmagatzemament de fitxers corporatiu basat en el *Cloud Storage*. Aquest sistema ha de garantir, per sobre de tot, la confidencialitat, continuïtat, l'alta disponibilitat, la còpia i la restauració de les dades dels usuaris de la corporació, així com el compliment de les lleis de privacitat i protecció de dades.

Paral·lelament, és objectiu transversal, la integració amb el directori actiu d'usuaris de la corporació i el seu sistema d'autenticació unificat (Single Sign On), amb el qual es gestionaran els usuaris i grups. Aquesta solució tècnica ha d'estar ben dimensionada segons les condicions de la infraestructura actual de la corporació i per als requeriments actuals, i a més a més, tenir la capacitat de creixement i flexibilitat suficient pensant en el futur immediat.

En aquest marc, no només es valoren els beneficis del canvi, tant tecnològics com econòmics, sinó que també es valorarà el canvi a favor dels serveis que la corporació oferirà als diferents usuaris (treballadors) de la pròpia corporació, els diferents departaments i a la pròpia corporació.

Per tal de realitzar aquest estudi, escollir quina és la millor solució a implantar i posar en marxa el projecte pilot, s'han seguit els següents criteris:

- **Seguretat, confidencialitat i privacitat de les Dades**

El nou sistema ha de proporcionar uns mecanismes de seguretat sofisticats, per tal d'assegurar les dades que estiguin allotjades, protegint-les de qualsevol possible atac i garantir la confidencialitat i la privacitat d'aquestes. Sota cap circumstància les dades poden ser vulnerades ja que poden contenir informació molt sensible i confidencial de la corporació, i una possible fuga d'informació podria causar greus problemes pels interessos d'aquesta.

- **Continuïtat i Disponibilitat de les Dades**

Les dades de la corporació i dels seus usuaris han d'estar disponibles en tot moment, garantint l'accés les 24h al dia 365 dies l'any, sense limitacions, restriccions ni pèrdues de rendiment ni velocitat en l'accés. Tanmateix, aquestes dades han de ser accessibles des de diferents dispositius com poden ser ordinadors, tauletes, mòbils o altres dispositius que es consideri oportú i estiguin suportats pel sistema.

- **Compliment de les lleis sobre protecció i emmagatzematge de les Dades**

El sistema de *Cloud Storage* haurà de complir amb les obligacions estatals i internacionals sobre la llei de protecció de dades i l'emmagatzemament d'informació privada, així com donar resposta davant de qualsevol incident que es pugui ocasionar.

- **Backup, restauració i replicació, eficient i eficaç, de les Dades**

El sistema haurà de disposar d'un sistema de còpies de seguretat i recuperació que sigui adient a les polítiques de *Backup* que la corporació consideri oportunes.

- **Escalabilitat i flexibilitat del sistema**

El sistema haurà de suportar una escal.labilitat que garanteixi el creixement progressiu que la corporació requereixi segons les seves necessitats, així com una flexibilitat del sistema per adaptar-lo a possibles noves necessitats. Per aquest motiu, es valorarà altament, que el sistema disposi d'una API *(Application Programming Interface)* segura i robusta per a poder donar resposta a aquestes necessitats, i que la corporació pugui gestionar i fins i tot, desenvolupar-ne mòduls per a la integració amb el seus serveis interns.

- **Monitorització i gestió de la infraestructura**

El sistema de *Cloud Storage* haurà d'incloure una interfície de gestió dels serveis eficient, dinàmica i que faciliti la operativitat dels tècnics que el gestionin. Haurà de disposar d'eines de monitorització del serveis per controlar l'estat del sistema per part dels tècnics de la corporació en qualsevol moment que es requereixi, així com un sistema de notificacions en cas de fallada de qualsevol dels serveis o d'incidències que hi puguin sorgir.

- **Costos econòmics i de recursos humans d'implantació i manteniment del sistema**

Tant la implantació i posada en marxa, com el manteniment de la totalitat de la infraestructura haurà d'entrar dins els barems econòmics marcats per la corporació per a aquest projecte.
Els costos de recursos humans requerits per a la realització de la totalitat del projecte hauran de ser proporcionals a la magnitud del projecte.

- **Universalitat, accessibilitat i transparència tecnològica**

El sistema haurà de ser compatible amb la tecnologia actual, tant amb la que disposa la corporació com la que puguin disposar els usuaris amb els seus propis dispositius. Així mateix,

l'accés haurà de ser universal des de qualsevol dispositiu i en qualsevol ubicació d'Internet, sense limitacions ni restriccions.
En aquest punt, s'apostarà per utilitzar tecnologia *OpenSource* davant d'altres tecnologies privades que requereixen de compra directa del producte i de llicenciament. S'entén que la corporació haurà de fer front a un cost econòmic pel suport directe de part o de tota la infraestructura de *Cloud Storage*.
La corporació haurà de tenir un mínim control de la infraestructura, conèixer els detalls tècnics, el funcionament intern, les mesures de seguretat que incorpora, etc.. i poder instal.lar els productes o mòduls que aquesta consideri oportú per a poder portar un control i auditoria de la infraestructura.

- **Integració amb els sistemes corporatius**

El sistema d'emmagatzemament de fitxers al *Cloud*, especialment, haurà de poder integrar-se amb serveis propis de la corporació, com pot ser el directori actiu d'usuaris i el sistema d'autenticació "SingleSignOn", entre altres. A més, la infraestructura *Cloud Storage* podrà integrar-se amb serveis interns que es requereixin per tal de monitoritzar l'estat del sistema, notificacions, entre altres.

1.3. Planificació

Per tal de portar a terme el projecte, s'han marcat els següents objectius, els quals marcaran la planificació aproximada del projecte i els terminis que s'hauran de complir per tal finalitzar-lo en els terminis establerts.

1.3.1. Taula de fites

Objectiu	Durada en dies	Data Inici	Data Fi
Definició i planificació del projecte	14 dies	21/09/2015	05/10/2015
Establiment de la proposta i justificació	4	28/09/2015	30/09/2015
Definició dels Objectius	1	01/10/2015	01/10/2015
Planificació de les fases del projecte	2	02/10/2015	03/10/2015
Definició del diagrama de Gantt i anàlisi riscos	1	04/10/2015	04/10/2015
Revisió de la definició i planificació	1	05/10/2015	05/10/2015
Anàlisi del projecte	31 dies	05/10/2015	05/11/2015
Estudi situació actual i necessitats corporació	1	06/10/2015	06/10/2015
Anàlisi dels requisits tècnics i definició abast	2	07/10/2015	08/10/2015
Estudi de la tecnologia de Cloud Storage	10	09/10/2015	18/10/2015
Estudi i classificació diferents solucions existents	6	19/10/2015	24/10/2015
Estudi de les mesures de seguretat que incorporen	6	25/10/2015	30/10/2015
Anàlisi de viabilitat tècnica i econòmica	3	31/10/2015	02/11/2015
Anàlisi de la integració amb els serveis corporatius	3	03/10/2015	05/10/2015
Desenvolupament i Proves	36 dies	05/11/2015	11/12/2015
Elecció i Disseny de la solució a implantar	5	06/11/2015	10/11/2015
Elaboració diagrames i esquemes infraestructura	2	11/11/2015	12/11/2015

Objectiu	Durada en dies	Data Inici	Data Fi
Implementació solució Cloud Storage definitiva	10	13/11/2015	22/11/2015
Parametrització i tunning	2	23/11/2015	24/11/2015
Integració amb serveis corporatius	5	25/11/2015	29/11/2015
Posada en marxa i proves pilot	6	30/11/2015	05/12/2015
Millores i resolució d'incidències	6	06/12/2015	11/12/2015
Memòria	25 dies	11/12/2015	07/01/2015
Redacció, correcció i validació de la memòria final	24	11/12/2015	06/01/2015
Presentació de la documentació	1	06/01/2015	07/01/2015
Presentació del TFM	8 dies	07/01/2015	15/01/2015
Elaboració presentació disapositives	3	07/01/2015	10/01/2015
Realització vídeo defensa del TFM	4	10/01/2015	14/01/2015
Presentació final	1	14/01/2015	15/01/2015

Taula 1 - Taula de fites del projecte.

1.3.2. Diagrama de Gantt

Per a aquesta taula de fites s'ha elaborat un diagrama de Gantt que mostra el temps de dedicació previst per a cada una de les tasques al llarg de tot aquest projecte.

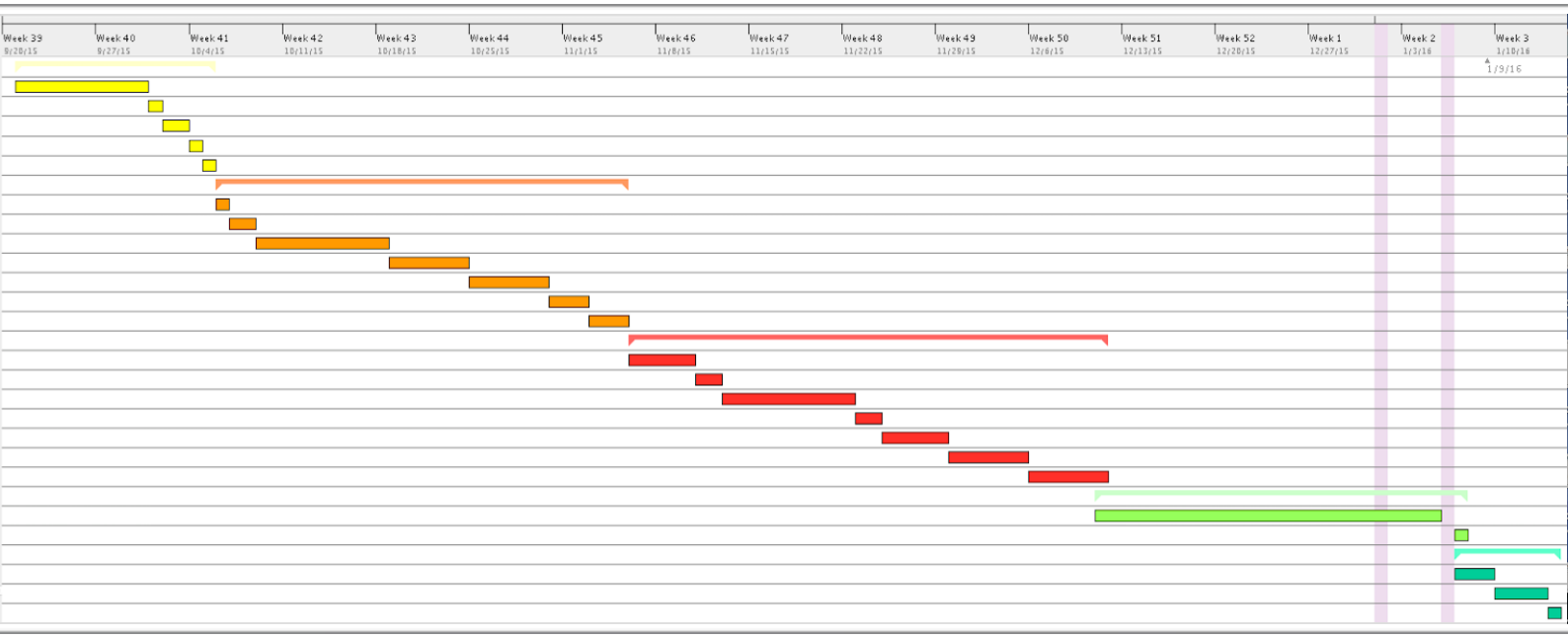

Fig. 1 - Diagrama de Gantt de la evolució del projecte.

1.4. Anàlisi de riscos

Dins d'aquesta planificació del projecte poden sorgir riscos associats al desenvolupament i finalització de les activitats programades, per tant, cal tenir en compte aquests i determinar quines poden ser les afectacions, la probabilitat que apareguin, les conseqüències que es derivin i l'impacte d'aquestes sobre la execució del projecte. A continuació es mostra una taula que descriu quins són els possibles riscos:

ID	Risc	Afectació	Conseqüències	Impacte	*Prob	Possible solució
R01	Errors de planificació	Planificació	Endarreriments	Marginal	Mitja	Augment dels recursos. Replanificació tasques.
R02	Desconeixement tecnologia a implantar	Planificació Execució Finalització	Endarreriments	Mig	Poc probable	Augment dels recursos. Replanificació tasques.
R03	Desacords en l'anàlisi requisits i abast	Planificació Finalització	Endarreriments Canvis execució	Insignificant	Mitja	Arribar a acords equip directiu
R04	Canvis en les polítiques corporatives	Planificació Finalització	Endarreriments Canvis execució	Marginal	Mitja	Debatir els canvis i analitzar repercussió. Replanificació tasques.
R06	Manca de solucions apropiades al projecte	Finalització	Endarreriments, pèrdues econòmiques Abortament projecte	Catasctrófic	Baixa	Reformulació requisits tècnics i polítiques. Sense solució.
R07	Mesures de seguretat ineficients	Finalització	Menor qualitat solució. Abortament projecte	Crític	Baixa	Buscar alternatives.
R08	Anàlisis inapropiats	Finalització	Pèrdues econòmiques, incompliment objectius, endarreriments.	Catastròfic	Mitja	Anàlisi resultats i buscar alternatives i solucions.
R09	Desconeixement dels tècnics en el procés d'implantació	Planificació Execució Finalització	Endarreriments, incompliment objectius.	Mig	Mitja	Augment dels recursos. Replanificació tasques.
R10	Dificultats integració serveis corporatius	Planificació Execució Finalització	Endarreriments, incompliment objectius.	Crític	Alta	Augment dels recursos. Buscar alternatives Replanificació tasques.
R11	Dificultats proves pilot	Planificació Finalització	Endarreriments	Mig	Alta	Buscar suport directe fabricant

Taula 2 - Llistat de riscos associats al projecte

*Prob = Probabilitat

2. Anàlisi de les necessitats

La corporació "OREV S.A." actualment està formada per un total de 18 departaments, amb un número de treballadors que segons les circumstàncies de càrrega de treball i època de l'any pot arribar fins a 100. Aquesta disposa d'un sistema de fitxers corporatiu centralitzat el qual dóna servei a tots els usuaris. Aquest sistema està basat en un sistema operatiu de xarxa *Novell-OpenSuse* sota Linux juntament amb un sistema d'emmagatzemam final basat en cabina de discos virtuals i ubicat en una xarxa SAN. Aquest sistema d'emmagatzemament final té una capacitat limitada, on actualment els usuaris disposen de fins a 2 TB d'espai disponible per emmagatzemar els seus fitxers sense possibilitat d'ampliació.

Per tal de gestionar l'accés a aquest sistema d'emmagatzemament, existeix un directori Corporatiu per administrar l'autenticació, autorització i els privilegis dels usuaris. Aquest treballa sota el protocol, a nivell d'aplicació, *LDAP (Lightweight Directory Access Protocol)*. Concretament es fa servir un servidor de directori actiu *OpenLDAP*, sota un servidor *Linux*, on s'emmagatzemen tots els usuaris, grups, i departaments de la companyia. Aquest servidor LDAP està integrat amb un sistema d'autenticació *Single Sign On* corporatiu, amb el que els usuaris s'autentiquen una única vegada per accedir a les diferents aplicacions corporatives.

Els usuaris disposen d'ordinadors personals amb el sistema operatiu *Windows 7* i tota una sèrie de programari per tal de desenvolupar les seves tasques. En aquest sistema es troba instal.lat un client de Novell per tal de connectar, autenticar i autoritzar els usuaris a la xarxa Corporativa. Cada usuari disposa del seu codi d'usuari, el qual es deriva i per tant, és exactament el mateix de que disposa al Directori Corporatiu.

2.1. Necessitats de la corporació

Pels motius descrits en la justificació d'aquest projecte, entre els que destaquem:

- la necessitat d'un sistema d'emmagatzemament de fitxers al núvol per donar solució a les necessitats dels usuaris i per tant, de la corporació,
- la impossibilitat d'ampliar el sistema d'emmagatzemament actual o la seva transformació en un entorn basat en el núvol,
- la limitació d'accés a aquest, únicament mitjançant el client d'escriptori actual i des de la xarxa interna corporativa,
- o bé, la necessitat d'accedir des de qualsevol ubicació amb accés a Internet, ja sigui des d'un client web, client d'escriptori o client mòbil.

La corporació ha decidit encomanar l'estudi d'una sèrie de solucions d'emmagatzemament al núvol, en base a les seves funcionalitats, característiques, la seguretat que incorpora cada una de les solucions, el cost econòmic de la implantació, i extreure conclusions de cada una de elles i escollir, finalment, la més adient per als seus interessos. Tanmateix, en aquest projecte es demana la implantació de la solució escollida en forma de prova pilot, per tal de que els usuaris i responsables tècnics i directius, puguin donar una valoració i, si s'escau, validar-la.

2.2. Funcionalitats Bàsiques

Aquest nou sistema haurà de garantir una sèrie de funcionalitat bàsiques com són l'emmagatzemament de fitxers, còpies de seguretat d'aquests, compartició de directoris i fitxers entre usuaris *[veure Fig.2]*, així com la sincronització del directori personal entre els diferents dispositius com ordinador personal, dispositiu mòbil i/o tauleta.

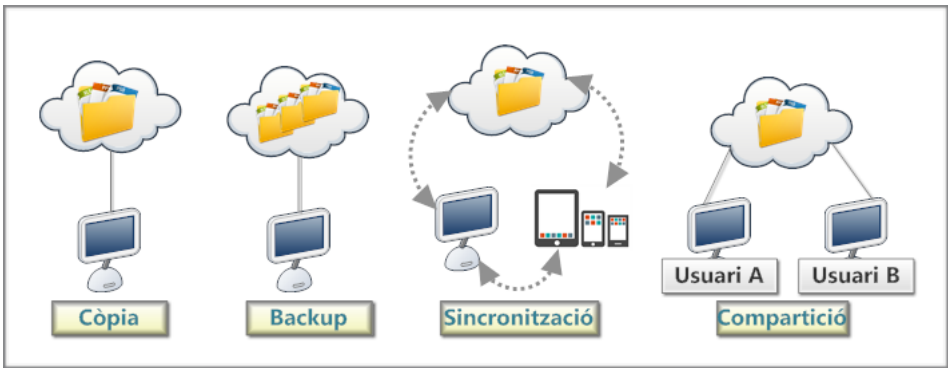

Fig. 2 - Còpia, Backup, Sincronització i compartició

2.2.1. Emmagatzemament de fitxers

Haurà de permetre a l'usuari crear còpies al núvol dels fitxers o directoris que emmagatzema en local. La finalitat es poder accedir a aquestes dades des de qualsevol ubicació o dispositiu que tingui una connexió a Internet.
Per a realitzar aquesta còpia, s'utilitzarà un client d'escriptori, aplicació mòbil o client web, que permeti copiar o moure fitxers fàcil i ràpidament, creant per exemple un directori en local, el qual serà copiat íntegrament i de forma automàtica al núvol. D'aquesta forma s'obté una estructura de directoris i fitxers al núvol idèntica a la que hi ha en local.
L'accés i còpia, també es podrà realitzar mitjançant una interfície web, amb la qual es gestionen tots els fitxers i directoris, pujar-ne de nous, modificar-los o esborrar-los.

2.2.2. Còpia de Seguretat o Backup

Aquests clients hauran de poder gestionar còpies de seguretat i posteriors recuperacions de fitxers emmagatzemats en local. Aquestes còpies seran emmagatzemades durant determinats períodes de temps, permetent a l'usuari recuperar en cas de pèrdua, robatori, etc.. Aquestes còpies de seguretat guardaran diferents versions d'un mateix fitxer o directori, on l'usuari pot escollir recuperar la versió que necessiti.
Les còpies de seguretat seran gestionades pel client, on es configuraran els directoris a copiar, les retencions al servidor i les programacions d'aquestes còpies. Aquestes es faran de forma automàtica i periòdicament, sense interacció i de forma transparent per a l'usuari.

2.2.3. Sincronització de dispositius

Els diferents clients permetran a l'usuari tenir les dades emmagatzemades al núvol disponibles en cada un dels dispositius que tingui vinculats al compte. Al existir diferents clients per a diferents plataformes, aquests poden ser instal.lats en ordinadors, tauletes, telèfons mòbils, etc.. i accedir a les dades de forma simultània i amb la seguretat de que aquestes estan actualitzades, sincronitzades i guarden la seva consistència.
Cada un dels clients ha de ser capaç de sincronitzar dades amb el núvol i poder detectar i resoldre possibles conflictes entre les dades pujades per cada un dels dispositius vinculats, permetent a l'usuari decidir que fer davant de conflictes com la duplicació de fitxers, sobre-escriptura, existència de diferents versions, etc..
Aquests dispositius, normalment, guarden les credencials d'accés al compte. Quan un d'aquests dispositius es vulnerat i aquestes credencials son interceptades, qualsevol atacant pot associar el seu propi dispositiu utilitzant el mateix mètode d'autenticació i accedir al compte i per tant, a les dades de l'usuari. Si aquesta acció no es notificada al propietari del compte, aquest desconeixerà que algú altre hi té accés i podrà manipular les seves dades.
Per tal de mitigar aquest risc, quan un nou dispositiu és associat al compte de l'usuari i en conseqüència, se li atorguen privilegis d'accés a les dades, l'usuari ha de poder aprovar aquesta nova associació abans de que l'accés es materialitzi. Aquesta confirmació ha de realitzar-se, per exemple, amb una notificació a un compte de correu electrònic indicant que un nou dispositiu ha demanat autorització per accedir al compte i a les dades. Si l'usuari no confirma aquest dispositiu, aquest no obtindrà accés.

Tanmateix, l'usuari ha de poder visualitzar el llistat de dispositius que té associats i poder administrar-ne l'accés. En el cas de pèrdua, robatori o simplement desig de revocar els privilegis d'un dispositiu, l'usuari podrà llistar-los, seleccionar el dispositiu a administrar i revocar-li els privilegis, eliminar les dades que contingui de forma remota o fins i tot i en alguns casos especials, bloquejar el dispositiu.

2.2.4. Compartició

La funcionalitat de compartició (*Sharing*) permetrà que un usuari publiqui contingut emmagatzemat al núvol i que altres usuaris tinguin accés. El tipus d'accés vindrà determinat per l'usuari que podrà atorgar privilegis de lectura, escriptura, esborrat, etc.. a un o diversos usuaris, ja siguin usuaris interns de la pròpia companyia o usuaris externs, sense vinculació directa.
Aquesta compartició es podrà realitzar tan per a fitxers únicament com per a directoris sencers, i la forma de publicitar-lo pot ser mitjançant directoris compartits dins del mateix compte o via creació de URLs per accedir-hi.

Existeixen fins a 3 formes diferents de compartir fitxers:

1) entre usuaris del mateix servei,
2) entre usuaris o grups d'usuaris aliens al sistema i que no disposen de compte,
3) de forma completament pública, és a dir, accessible per tothom.

Compartir fitxers amb usuaris concrets, és a dir, en els casos 1 i 2, l'usuari propietari i per tant administrador, crea una compartició, la qual pot administrar segons els seu criteri, atorgant permisos de lectura, escriptura, esborrat, etc.. diferenciant per usuaris o grups i revocant aquests quan així es consideri. El usuaris destinataris de la compartició, segons l'accés atorgat, podran visualitzar, modificar i esborrar els fitxers encara que no siguin propietaris. Aquest tipus de compartició de fitxers ha de complir amb els requisits següents:

- Els fitxers o directoris que es comparteixen han de ser, únicament i exclusivament, accessibles pels usuaris als quals se li ha donat els privilegis corresponents.
- Així mateix, aquests privilegis han de poder ser revocats per cada un dels usuaris i en el moment que es precisi.
- Els fitxers han de ser accessibles per totes les interfícies d'accés que hi hagi disponibles, per exemple, via web o via aplicació client.
- Quan els fitxers que es comparteixin estiguin xifrats per part del client, aquests no hauran de perdre el xifrat i per tant, no hauran de ser accessibles pel propi sistema, però si pels usuaris als quals es comparteixen.
- Quan un usuari que tenia accés a fitxers xifrats, se li revoquen aquest privilegis d'accés, aquest ha de deixar de tenir accés a la clau de desxifrat, i a més, els nous fitxers han de ser xifrats amb una nova clau.

Quan es comparteixen fitxers o directoris amb usuaris aliens, aquesta compartició normalment, s'ofereix mitjançant un accés web, és a dir, amb una URL d'accés. Els usuaris amb privilegis, accedeixen als fitxers, únicament, mitjançant aquesta URL, la qual es pública i per tant, qualsevol que conegui aquesta URL podrà accedir-hi. Per millorar la seguretat d'aquestes comparticions amb usuaris externs, existeix la possibilitat d'afegir una autenticació mitjançant credencials generades amb caràcter permanent o temporal.
En ambdós cassos, hi ha una sèrie de consideracions que el servei hauria de complir:

- La URL ha d'estar ofuscada, és a dir, s'ha d'amagar la URL real sota una de fictícia per tal que aquesta no contingui cap tipus d'informació relativa a l'usuari o al contingut de les dades que es comparteixen, i per tant, un possible atacant no pugui capturar informació valuosa.
- Si l'accés no requereix credencials, la URL hauria d'incorporar un identificador generat de forma aleatòria. Aquest identificador hauria de tenir una data de caducitat, si així ho precisa l'usuari que comparteix els fitxers.

2.2.5. Capacitat i Escal.labilitat

Per decisió consensuada entre la direcció de la corporació i els tècnics responsables de l'àrea de TI, el sistema haurà de suportar que cada usuari tingui un espai d'emmagatzemament de com a mínim 10 GB d'espai per compte. La totalitat del sistema tindrà una capacitat mínima de 5 TB. Aquest sistema haurà de garantir escal.labilitat per tal de fer front al possible creixement de la corporació, segons necessitats futures.

2.2.6. Integració directori corporatiu

El sistema haurà de disposar dels mecanismes per a sincronitzar-se amb el directori actiu de la corporació, per tal d'aprovisionar els usuaris al sistema i administrar-los. Aquesta sincronització es realitzarà de forma automatitzada, on es crearan els comptes d'usuari i la seva posterior eliminació quan ja no es trobin al directori actiu corporatiu.
Es valorarà també que aquest s'integri amb el sistema d'autenticació unificada de la corporació, Single Sign On (SSO).

2.2.7. Gestió centralitzada i monitorització

El sistema haurà d'incorporar una consola d'Administració per tal de gestionar els usuaris, grups i les dades d'aquests. Tanmateix, la consola haurà d'oferir una gestió i administració de les comparticions creades pels usuaris. Es podrà gestionar també els dispositius vinculats de cada usuari, permetent revocar els seus permisos, des d'aquesta consola quan així es consideri.
Al igual que succeeix en altres models d'emmagatzemament, en els sistemes basats en el núvol, s'ha d'incloure una auditoria de les dades. Conèixer qui, com, quan i des d'on ha creat, modificat o esborrat un fitxer o directori, permet fer un seguiment dels incidents que puguin sorgir i saber el cicle de vida sencer d'un fitxer dins el sistema. Aquestes polítiques d'auditoria, normalment, són de caràcter obligatori dins de les mesures de seguretat de moltes corporacions, sobretot quan aquestes compleixen amb els estàndards *ISO* [1] o similars.

2.3. Requeriments tècnics de seguretat

A més a més d'aquesta sèrie de funcionalitats, el sistema haurà de garantir que compleix amb els següents requisits tècnics en matèria de seguretat i que disposa de mecanismes de seguretat que els garanteixin.

2.3.1. Principis bàsics de seguretat de les dades

Com a norma base, hi ha tres principis que ha de complir qualsevol sistema d'emmagatzemament de dades per garantir la seva seguretat i la de les dades que hi formaran part. Aquests tres principis es coneixen com a "*The big three CIA: confidentiality, integrity and availability*" [2].

CONFIDENCIALITAT DE LES DADES

La confidencialitat és, possiblement, el requeriment més important en el que a seguretat de les dades es refereix. La confidencialitat garanteix que l'accés a les dades i a les comunicacions queda protegit contra la intercepció i/o lectura de persones o altres sistemes no autoritzats. Aquest principi es bàsic en qualsevol sistema, i sobretot, en els sistemes d'emmagatzematge de fitxers, ja sigui en el núvol o no, s'han de prendre les mesures necessàries per garantir, sota qualsevol circumstància, la confidencialitat de les dades que emmagatzema i a les que s'hi accedeix.
Per tal d'evitar que la confidencialitat sigui vulnerada, ja sigui de dades personals o de dades sensibles de companyies, totes les dades que circulen pel sistema d'emmagatzemament han de ser xifrades. Aquest xifratge s'ha de produir quan les dades s'estan transmeten, així com en el propi emmagatzemament final. Per tant, quan s'estableix una comunicació entre client i servidor,

aquest canal de comunicació ha de ser un canal segur, on les dades siguin xifrades, normalment, mitjançant un infraestructura de clau pública i privada.

INTEGRITAT DE LES DADES

Un altre requisit indispensable en la seguretat de les dades, és la integritat d'aquestes. La integritat garanteix que les dades no han sigut modificades ni alterades per un accés no autoritzat, tant en el procés de transmissió com durant el seu emmagatzematge i processament.
Dins el marc de l'emmagatzemament al núvol, la transmissió de dades entre servidor i diferents dispositius pot incrementar la possible pèrdua de la seva integritat. Per aquest motiu, tant en el procés de transmissió de les dades entre client (dispositiu) i el servidor, així com en el procés d'emmagatzemament final, el servidor haurà de garantir el principi d'integritat sota qualsevol circumstància.

DISPONIBILITAT DE LES DADES

El tercer principi bàsic, i no menys important, és el de la disponibilitat de les dades. El principi de disponibilitat indica que les dades han de ser accessibles sempre que aquestes siguin requerides i els serveis han d'estar operatius en tot moment.
Aquesta disponibilitat pot variar segons el nivell d'importància d'aquestes. Si les dades són altament crítiques i de vital importància, aquestes han d'estar redundades i ha d'existir un recolzament en forma de còpies de seguretat constants, per tal de garantir la seva disponibilitat sota qualsevol circumstància per crítica que sigui. Quan existeix una vulnerabilitat, aquesta normalment, ve determinada per problemes en la comunicació (client-servidor-dades). Per exemple, en el costat del client, poden aparèixer problemes tècnics en el seu dispositiu, a la xarxa, o fins i tot, atacs directes contra aquest, com el segrest de sessió i robatori de claus. En el pitjor dels casos, al costat del servidor, poden sorgir problemes de *hardware* que pugui patir el proveïdor de serveis, com problemes en la seva infraestructura de comunicació o d'emmagatzemament, o fins i tot, atacs de denegació de servei (DoS).

Tot sistema d'emmagatzemament al núvol haurà de garantir que aquestes 3 normes bàsiques (confidencialitat, integritat i disponibilitat) es compleixen mentre les dades resideixin als seus servidors, així com complir amb les normes reguladores i obligacions estatals i internacionals sobre la llei de protecció de dades, emmagatzemament, utilització i retenció d'informació personal i privada i donar resposta davant de qualsevol incident que es pugui ocasionar.
Dins del marc europeu, aquestes estan regulades sota la *Directiva 95/46 de la Unió Europea* [3] sobre el tractament de dades de caràcter personal, establint les bases reguladores en el '*Reglament General de Protecció de Dades'* i la *'Directiva de protecció de dades en matèria de cooperació policial i judicial'*. En el marc internacional, concretament en el marc de cooperació nord-americà i europeu (U.S-EU), existeix un reglament establert pel govern dels EUA, el qual garanteix el compliment de les normes reguladores europees per part de les companyies americanes sobre protecció de dades dels ciutadans europeus. Aquest marc normatiu de seguretat és conegut com a *'U.S.-EU Safe Harbor Framework' i 'U.S.-Swiss Safe Harbor Framework'* [4].
Per tant, serà requisit indispensable que els proveïdors de serveis d'emmagatzemament al núvol disposin de les corresponents certificacions, segons la ubicació i localització concreta dels seus sistemes d'emmagatzemament final.

A més, aquests sistemes han d'estar dotats de les mesures de seguretat físiques, com per exemple, control d'accés i identificació del personal, guàrdies de seguretat, circuits tancats de video-vigilància, control i gestió d'incidents, redundància dels components *hardware*, entre moltes altres.

2.3.2. Autenticació dels usuaris al servidor

L'accés als serveis al núvol són exposats públicament a Internet, normalment sota serveis web com HTTP. L'accés a aquests serveis, per tant, han de ser administrats de forma segura, aplicant

les mesures necessàries per no permetre un accés no autoritzat. Les dades són emmagatzemades i gestionades de forma remota, pel que l'usuari ha de conèixer la identitat i confiar en el proveïdor i en les mesures de seguretat que aquest aplica a les dades que gestiona.
Per a poder accedir a aquestes dades per part de l'usuari, el proveïdor ha de proveir d'un mitjà d'accés segur, per mitjà d'una identificació digital o credencials, que garanteixi que ningú sense identificació accedirà -*autenticació* - i que qui accedeixi, només tingui accés al contingut que li correspongui segons els seus privilegis - *autorització*.

AUTENTICACIÓ

En aquest procés d'identificació digital, el servidor haurà d'incorporar un sistema d'autenticació mitjançant usuari i contrasenya, el qual garanteix que l'usuari és qui diu ser. Tot usuari que no estigui autenticat, no tindrà accés sota cap circumstància. Aquesta autenticació s'haurà de realitzar sota canals de comunicació segurs HTTPS, basats en els protocols SSL i/o TLS.

Cal dir que aquesta forma d'abordar l'autenticació no està exempta de problemes de seguretat. Per exemple, les credencials emmagatzemades de forma permanent en un ordinador poden ser robades i utilitzades per un altre usuari, o bé obtenir les clau d'accés mitjançant un correu electrònic fraudulent. Per donar més seguretat a l'autenticació, existeixen mecanismes que donen un nivell més de seguretat i garanteixen que l'autenticació la realitza el propietari del compte, com és la verificació de la identitat en dos passos.
Es valorarà la inclusió del sistema d'autenticació basat en 2 passos (*Two-steps verification)*[5], com a capa extra de seguretat extra en la fase d'autenticació. L'usuari pot escollir entre rebre codis de seguretat via missatge de text o via aplicació TOTP (Time-Based One-Time Password)[6], on el codi es generat de forma temporal i vàlid durant un temps limitat, permetent així, validar l'inici de sessió al compte.

AUTORITZACIÓ

Una vegada l'usuari estigui correctament autenticat al sistema, aquest tindrà accés al seu contingut i altres que se li pugin atorgar privilegis. Per a gestionar aquest control hi ha d'haver un sistema que garanteixi que només tindrà accés a allò que li correspongui i que tingui el dret concedit.

2.3.3. Comunicació i transmissió de les dades entre clients i servidor

Els proveïdors de serveis d'emmagatzemament al núvol, normalment, ofereixen la possibilitat als clients d'utilitzar un *software* propietari el qual s'encarrega de la tasca de sincronització i la còpia de dades entre el dispositiu del client i el propi servidor. Altrament, aquests proveïdors, ofereixen la possibilitat també de gestionar les seves dades mitjançant entorns web. En ambdós casos, sempre existeixen riscos quan es sincronitzen les dades entre dispositius ja que poden aparèixer vulnerabilitats que permetin a un atacant capturar les dades que s'estan sincronitzant o inclús, manipular la informació abans que aquesta arribi al seu destí. Per evitar-ho, sempre ha d'existir una autenticació prèvia al servidor, i una vegada establerta, tota transferència que es realitzi ha d'estar correctament xifrada, assegurant així la confidencialitat i la integritat de les dades que s'hi intercanvien.

Per realitzar aquest xifratge, s'utilitzen normalment funcions criptogràfiques asimètriques, conegudes també com a funcions criptogràfiques de clau pública [7]. Aquest tipus de criptografia utilitza dues claus, una pública i una privada, que pertanyen a un únic propietari qui es qui envia el missatge. La clau pública, tal i com s'intueix, és pública i es pot enviar a qualsevol destinatari, amb la qual xifrarà el missatge de retorn. En canvi, la clau privada, sols serà coneguda pel propietari, que l'utilitzarà per desxifrar el missatge generat amb l'anterior clau. Aquesta clau serà l'única que podrà desxifrar-lo, garantint així la confidencialitat i integritat del missatge. Tanmateix s'utilitza, en menys ocasions, el xifrat per mitjà de funcions criptogràfiques simètriques [8], les quals utilitzen una única clau secreta per xifrar i desxifrar els missatges enviats. Amb aquest mètode, les dues parts s'han de comunicar prèviament per acordar quina clau utilitzaran, i per

tant, intercanviar-la. Una vegada s'han enviat les claus, el remitent xifra el missatge i l'envia al destinatari, el qual, amb la clau secreta prèviament intercanviada, desxifra el missatge. Ambdues funcions utilitzen algoritmes criptogràfics SHA-256 i SHA-512 (Secure Hash Algorithm)[9], els quals utilitzen generadors de claus aleatòries (CSPRNG o CPRNG).

2.3.4. Encriptació de les dades al servidor

Aquests sistemes basats en el núvol són, normalment, visibles a Internet i per tant, una gran font de possibles atacs. Per evitar aquests atacs i la pèrdua de la confidencialitat de les dades, la solució passa per xifrar totes les dades que s'emmagatzemen. Un dels algoritmes de xifrat més segur i utilitzat avui en dia, gairebé per tots els proveïdors, és l'estàndard de xifrat avançat AES (*Advanced Encryption Standard)*[10]. L'agència de Seguretat Nacional dels EUA (NSA) [11], el considera com un dels estàndards més recomanats per xifrar dades de caràcter confidencials, catalogades com a 'TOP SECRET'. A data d'avui, és l'estàndard de xifrat utilitzat pels governs, bancs i els sistemes d'alta seguretat de tot el món.

Normalment, la majoria de proveïdors implementa el seu propi sistema de xifrat basat en AES utilitzant una clau pròpia, coneguda com a '*corporate key*', només coneguda per la pròpia companyia. Aquest mètode mitiga les possibles pèrdues de dades i la seva confidencialitat quan el sistema es compromès, però no quan l'atac es produeix coneixent aquesta clau '*corporate key*' o quan l'atac es des de l'interior, executat pel propi personal que coneix aquesta clau.

2.3.5. Actualitzacions de seguretat

Un dels principis de seguretat de qualsevol *software* és la de mantenir-se actualitzat per prevenir possibles atacs. Mantenir un *software* no actualitzat pot comportar grans forats de seguretat en forma de vulnerabilitats que poden ser explotades per atacants. Per aquest motiu, és vital que el *software* client realitzi una comprovació constant i periòdica de noves actualitzacions. Si una nova versió del *software* està disponible, aquesta ha de ser desplegada el més aviat possible, sempre sota decisió de l'usuari final.
En l'àmbit corporatiu, aquesta política d'actualitzacions automàtiques o a decisió de l'usuari final pot ser motiu de debat segons les polítiques corporatives. Es recomanable que dins d'una organització, la política sigui la de actualitzar tant aviat com aparegui una actualització, ja sigui de forma massiva o dividida en grups, ja que utilitzar una versió antiga de la qual es coneixen vulnerabilitats que la nova versió soluciona, pot comportar greus problemes de seguretat i per tant, comprometre la confidencialitat i la integritat de les dades de la companyia.

3. Estudi de la tecnologia

3.1. Cloud Computing: Introducció

Avui en dia, la paraula *Cloud* és comunament utilitzada per tothom per a descriure qualsevol servei que es trobi a Internet. Normalment, aquest ús de la paraula *Cloud* s'identifica amb l'utilització d'espais d'emmagatzemament d'ús privat com són els famosos *Dropbox, Google Drive, iCloud,* etc.. Els sistemes d'emmagatzemament al núvol (privatius o no) són solament un petita part o porció dels serveis que ofereix el núvol. Aquí es on apareix la tecnologia de *Cloud Computing*. Així doncs, podem dir que el concepte de tecnologia *Cloud Computing* engloba tot el conjunt de serveis oferts i allotjats per mitjà de la xarxa Internet. Aquesta tecnologia es basa en oferir qualsevol recurs d'un sistema, *software* & *hardware*, servidors, emmagatzemament i *networking*, com un servei, negoci o fins i tot, com a tecnologia en si, sempre a través d' Internet.

El *NIST ("National Institute of Standards and Technology") [12]*, defineix el *Cloud Computing* com un model per poder habilitar l'accés convingut sota demanda a un conjunt compartit de

recursos computacionals, com per exemple, xarxes de comunicació, servidors, sistemes operatius, emmagatzemament, aplicacions i demés serveis, que poden ser ràpidament aprovisionats i alliberats amb un esforç mínim d'administració o d' interacció amb el proveïdor de serveis.

Aquest tipus de tecnologia es basa en 5 característiques essencials:

- Auto-servei sota demanda: l'aprovisionament de la infraestructura, és a dir, xarxa, emmagatzemament, capacitat de computació, etc.. que es requereixi es realitza des del costat del client, sense interacció directa amb el proveïdor. L'usuari, mitjançant la consola de gestió, s'auto-assigna aquells recursos que necessita i els allibera quan ja no els requereix.
- Accés des de la xarxa Internet: les funcionalitats estan accessibles a través de la xarxa Internet per mitjà de plataformes estàndards, com els PCs o Macs, ja siguin clients natius o els propis navegadors web, telèfons mòbils, tauletes, entre altres.
- Aprovisionament de recursos dinàmicament: els recursos computacionals s'habiliten per donar servei a diferents consumidors mitjançant el model *"multi-tenant"* on aquests recursos (tant físics com virtuals) són dinàmicament assignats i re-assignats segons necessitats. El consumidor normalment no té el control ni el coneixement dels recursos i infraestructura que se li assignen.
- Alta escal.labilitat i ràpida expansió: tant els recursos com les capacitats d'aquests poden ser ràpidament i elàsticament aprovisionats, i alliberats quan ja no siguin necessaris, en la majoria de casos, de forma automàtica des de la consola d'administració de la infraestructura.
- Servei mesurat: els sistemes *Cloud* controlen automàticament i optimitzen l'ús dels recursos mitjançant sistemes de gestió altament sofisticats segons el nivell d'abstracció del servei, com pot ser l'aprovisionament d'espai, ample de banda, usuaris, etc.. Aquest ús dels recursos poden ser monitoritzats, controlats i reportats, proporcionant total transparència entre el proveïdor i el client.

3.2. Cloud Storage Systems

Actualment, la popularitat dels serveis d'emmagatzemament al núvol, (a partir d'ara l'anomenarem "*Cloud Storage*") ha crescut de forma desmesurada fins arribar al punt que, gairebé, tot usuari d'Internet té creat i utilitza un compte personal d'alguna de les companyies que ofereixen aquest serveis gratuïtament, com per exemple, *Dropbox, Apple* amb el seu *iCloud, Google* amb el seu *Google Drive*, etc.. Aquests serveis ofereixen la possibilitat a l'usuari d'emmagatzemar tot tipus de contingut digital, ja sigui de caràcter personal o empresarial, com documents, fotografies, vídeos, música, llibres electrònics, etc.. en un directori al núvol i el qual és accessible des de qualsevol dispositiu (ordinador, mòbil, tauleta,..) amb accés a Internet.

Concretament, en el cas de *Dropbox*, diu en una de les seves últimes notes de premsa, que ja supera els 400 milions d'usuaris registrats, els quals pugen al núvol més d'un 1,5 milions d'arxius diàriament. Aquestes xifres són molt indicatives de cap a on es dirigeix el món de l'emmagatzemament digital [13].

El *Cloud Storage* és un sistema per emmagatzemar dades digitals al núvol més enllà d'una xarxa local. Aquest emmagatzemament, normalment, és proporcionat per un proveïdor de serveis de *Cloud Computing*, el qual permet accedir a les dades mitjançant la xarxa d'Internet. Més concretament, podria definir-se com una xarxa distribuïda de sistemes d'emmagatzemament que utilitza la tecnologia de *Cloud Computing*, la virtualització i tecnologies d'emmagatzemament estàndard com a base de la seva infraestructura. Aquests sistemes presenten una interfície, normalment estàndard i multi-plataforma, amb la que els usuaris emmagatzemen dades digitals permetent que aquestes estiguin disponibles i accessibles des de qualsevol dispositiu i des de qualsevol ubicació amb accés a Internet.

3.3. Classificació de la tecnologia Cloud

La tecnologia de *Cloud Storage* es pot dividir en fins a 4 tipus, segons la seva localització:

3.3.1. Public Cloud

La infraestructura d'aquest tipus de núvol és administrada i servida per tercers, és a dir, el proveïdor del servei. Els recursos de la infraestructura estan distribuïts en molts servidors, manegats per diferents nuclis virtualitzats i en clúster, per tal de garantir una alta disponibilitat i continuïtat dels serveis que ofereixen.
Aquest tipus de *Cloud* es caracteritza per compartir tots els seus recursos (sistemes, emmagatzemament, etc..) entre tots els clients de forma uniforme i transparent, sense que aquests coneguin la ubicació ni distribució dels mateixos. Gràcies a aquesta distribució, aquest sistema permet una gran escal.labilitat i flexibilitat segons les necessitats dels clients.
Les *Public Cloud* ofereixen disponibilitat immediata d'infraestructura via Internet, amb un sistema de pagament únic i per ús, pel que no es necessari cap tipus d'inversió en infraestructura. Per contra, tota la informació es allotjada en els servidors del proveïdor, pel que és una solució que presenta molt sobre la seguretat i privacitat de les dades.

3.3.2. Private Cloud

Aquest tipus de *Cloud* requereixen d'una infraestructura pròpia i on aquesta opera de forma interna. Són administrades i gestionades pel propi personal de la organització, i de la qual es té control i coneixement total. Aquestes, per tant, requereixen d'una inversió en forma de capital i infraestructura, com els servidors, dispositius de xarxa, emmagatzematge, protecció, etc.. La seva implantació i futur manteniment el proporcionarà la pròpia organització.
A diferència de les *Public Clouds*, aquestes estan més limitades en matèria escal.labilitat per dependre de la pròpia infraestructura, però per contra, ofereixen més garanties en matèria de seguretat i privadesa de les dades.

3.3.3. Hybrid Cloud

Aquest tipus de *Cloud* combina els dos models de núvol vist, públic i privat, és a dir, es tracta d'una solució intermitja entre aquestes dues. Normalment, els recursos principals, com són les els servidors d'accés (frontals), *proxies*, i aplicacions integrades, resideixen en la *Private Cloud*, mentre que la infraestructura d'emmagatzemament final i els recursos de caire més computacionals són delegats a altres *Public Cloud*, de forma distribuïda, per tal d'oferir una alta disponibilitat, flexibilitat, escal.labilitat o fins i tot, realitzar operacions amb aquestes dades que requereixin de nivells de processador més grans que la pròpia *Cloud* no disposa.
Aquests tipus de núvols presenten una complexitat alta, ja que requereixen d'una distribució dels recursos més eficient i per tant, una configuració més específica per part del personal de TI. Podríem dir que el seu ús no està molt estès, però es preveu que en els propers anys, aquestes adquireixin una importància major, proporcional a les futures necessitats de processament de dades per part de les companyies.

3.3.4. Community Cloud

Aquest tipus de *Cloud* esta basat en la infraestructura *'multi-tenant'*, on els recursos tecnològics i computacionals són compartits entre diverses organitzacions que tenen serveis, negoci, o objectius en comú. Aquesta coalició i compartició ve donada per les necessitats que aquestes companyies en matèria de seguretat, privacitat, disponibilitat.

3.4. Infraestructura dels Cloud Storage Systems

Les arquitectures dels sistemes de *Cloud Storage* estan dissenyades principalment per oferir serveis d'emmagatzemament sota demanda en infraestructures *'multi-tenant'* altament flexibles i de gran escal.labilitat mitjançant la virtualització dels seus servidors dedicats i la utilització de

Data-centers distribuïts. Generalment, les arquitectures *Cloud Storage* estan basades en un frontal - *Front-End* -, un servidor intermediari, conegut com a *middleware*, i un *Back-End*, que en aquest cas, és el propi sistema d'emmagatzematge.

El *Front-End* proporciona un conjunt d'APIs que permeten a l'usuari final accedir a l'emmagatzemament, com són els clients d'escriptori, aplicacions web, mòbils, etc.. A diferència dels tradicionals sistemes d'emmagatzemament que utilitzen protocols estàndards com l'SCSI/*FC*, NFS o CIFS per a accedir a les dades, els *Cloud Storage Systems*, utilitzen aquests mateixos protocols però en versions més evolucionades, normalment, sobre els protocols HTTP i HTTPS. Darrera aquests *Front-Ends* s'hi col·loca una capa lògica d'emmagatzemament o *middleware*, la qual implementa una sèrie de funcionalitats per tal d'optimitzar el rendiment alhora d'emmagatzemar les dades en el *Data-Center* o emmagatzemament final. La compressió, *deduplicació* o arxivat de les dades són algunes de les accions que pot realitzar-se en aquest *middleware*, així com la distribució de les dades en els diferents sistemes segons necessitats, ubicació i càrrega de treball.
Finalment, en la última capa, hi trobem el *Back-End* o emmagatzemament principal, on es guarden les dades finals. Aquests sistemes poden ser, des de sistemes NAS simples, fins a sistemes d'emmagatzemament de discos sobre una SAN, o fins i tot, *Data-Centers* més sofisticats. Aquests *Back-Ends* treballen sobre la majoria de protocols de xarxa com els protocols *NAS i SAN, FC, FCoE, iSCSI, NFS o fins i tot, SMB-CIFS*.

3.5. Avantatges de la tecnologia Cloud Storage

La tecnologia *Cloud Storage* pot oferir una sèrie d'avantatges molt interessants tant a curt com a llarg termini, però alhora presenta una sèrie d'inconvenients, sobretot a nivell de control i seguretat. Entre aquests avantatges tenim:

- *Reducció dels costos d'inversió i capital*: invertir en una infraestructura, xarxa, sistemes, emmagatzemament, *software*, etc.. requereix d'una inversió inicial molt elevada que normalment les empreses, sobretot les petites i mitjanes, no poden fer front. Amb l'ús de la tecnologia *Cloud* i el seu sistema de pagament per ús i servei, moltes d'aquestes poden oferir els serveis que pretenen sense necessitat d'un capital inicial i la respectiva inversió, ja que la infraestructura al complet, es proporcionada pel proveïdor.
- *Reducció dels costos de manteniment*: tota infraestructura, *Hardware & Software*, requereix d'un manteniment anual que doni resposta davant incidents. Normalment aquests contractes de suport i manteniment tenen un cost elevat que moltes empreses desestimen per no poder afrontar-lo.
- *Reducció dels costos de personal tècnic qualificat*: al no existir infraestructura *hardware* que gestionar, ni *software* base que la gestioni, no es requereix de personal qualificat. Les interfícies de gestió són molt intuïtives i amigables, pel que amb un mínim de coneixements, qualsevol tècnic pot encarregar-se de gestionar-la de forma eficient.
- *Escal.labilitat i flexibilitat*: la tecnologia *Cloud Storage* es basa en el pagament per ús. Com aquests són virtuals i depenen d'una macro-infraestructura que normalment ve gestionada i administrada de forma automàtica, l'escal.labilitat dels recursos que es necessiten es produeix de forma transparent i immediata, sense interacció per part del consumidor. I això no sols per als productes ja adquirits, sinó que quan es requereixen de nou, tan sols s'han de sol.licitar i en un breu espai de temps aquests es troben disponibles per ser utilitzats.
- *Mobilitat*: un dels grans avantatges d'aquesta tecnologia es que no requereix cap tipus d'infraestructura, ja que aquesta es troba en infraestructures de tercers, on amb un simple accés a Internet es pot tenir accés. A més, aquestes són estàndards, per a que des de qualsevol sistema o dispositiu amb connexió a Internet s'hi pugui accedir.

3.6. Possibles riscos associats al Cloud Storage

Pel que respecta als riscos i per tant, les desavantatges que apareixen amb l'ús de la tecnologia *Cloud* ens podem trobar amb els següents:

- *Seguretat*: es evident que externalitzar i delegar tota la infraestructura, perdent el control i part de la gestió, a una companyia aliena a la empresa comporta grans riscos i dubtes pel que a seguretat es refereix. Actualment totes les companyies que ofereixen serveis de *Cloud Storage* compten amb mesures de seguretat sofisticades, com la seguretat perimètrica, detectors d'intrusions, així com altres mesures que normalment fan que aquestes siguin més segures davant de possibles atacs.
- *Privacitat i confidencialitat*: la informació i les dades que es vulguin emmagatzemar han de ser tractades amb molta sensibilitat, on els proveïdors de serveis *Cloud Storage* han de garantir que aquestes estaran custodiades amb fermesa, garantint la seva privacitat i confidencialitat. S'ha d'avaluar que existeix la possibilitat que les dades sensibles i de gran valor d'una companyia, poden quedar exposades a un atacant, ja que no es té control sobre aquestes com es podria tenir, en cas de tenir una infraestructura pròpia.
- *Connectivitat*: utilitzar sistemes *Cloud Storage* requereix de connexions a Internet de gran velocitat i alta disponibilitat, ja que totes les dades es troben al núvol, i sense accés a aquestes es poden produir pèrdues econòmiques per part de la companyia.
- *Pèrdua de control*: com ja s'ha comentat, en els *Private Cloud* tota la infraestructura queda en mans de tercers, pel que es depèn completament de les mesures de contenció que el proveïdor incorpori. Les còpies de seguretat, replicació de dades, l'alta disponibilitat i continuïtat de la infraestructura, etc.. s'ha de deixar completament en mans del proveïdor amb el risc que això suposa per a la integritat de la companyia.

4. Estudi de solucions de Cloud Storage

En aquest apartat s'analitzaran fins a 5 solucions de *Cloud Storage*, de diferents proveïdors de serveis de Cloud existents actualment al mercat. Aquesta selecció s'ha realitzat, principalment, en base als objectius d'aquest projecte, és a dir, analitzant les funcionalitats que ofereixen, la capacitat i la escal.labilitat del sistema, la possibilitat d' integració amb els serveis corporatius, però sobretot, per les polítiques de seguretat que apliquen al tractament de les dades i el seu cost estimat d'implantació. A banda d'aquestes 5 solucions elegides, s'han estudiat d'altres solucions però que, per les seves característiques i funcionalitats, no s'adaptaven a les necessitats de la corporació, i per tant, s'han descartat.

Concretament s'han escollit 4 soluciones de *Cloud Storage* públic i una de *Cloud Storage* híbrid. La decisió d'analitzar 4 solucions de caràcter públic ha sorgit per la possibilitat de delegar tota la infraestructura al proveïdor per tal de reduir els costos que la posta en marxa del servei comportaria i evidentment, per les funcionalitats i característiques que aquestes ofereixen. Per un altre costat, s'ha decidit incloure una solució híbrida, que inclou la implantació d'un servei de Cloud Storage privat dins de la infraestructura interna i complementar-lo amb un emmagatzemament secundari utilitzant els serveis d'un proveïdor de serveis de *Cloud*, com és *Amazon AWS*. Aquesta solució híbrida pretén reduir costos d'implantació i manteniment alhora que proporcionar la escal.labilitat i major capacitat d'emmagatzematge que requereix la corporació, i alhora oferir un major control de la totalitat de la infraestructura, ja que part de la infraestructura és gestionada, íntegrament, per el servei de TI intern de la corporació.

4.1. Dropbox for Business

La més que coneguda *Dropbox*, una de les pioneres del *Public Cloud Storage* per a usuaris finals, ofereix com a *Cloud Storage* per a companyies una solució coneguda com a *Dropbox for Business* [14].

Estudi funcionalitats bàsiques

4.1.1. Emmagatzemament de fitxers

Dropbox disposa de client per a totes les plataformes conegudes, com *MacOSX*, *Windows*, *Linux*, etc.. Aquest client, crea un directori on s'emmagatzemaran tots els arxius que l'usuari vulgui pujar al núvol. Quan un fitxer es desat en aquest directori automàticament i de forma immediata és pujat al núvol en *background*. Per tant, tota la estructura de directoris i fitxers que hi hagi per sota aquest serà emmagatzemada al núvol amb el mateix esquema. Paral·lelament a l'ús del client, també existeix la opció d'utilitzar l'interfície web, amb la qual es poden gestionar tots els fitxers i directoris, pujar-ne de nous, modificar-los o esborrar-los.

4.1.2. Backup

Dropbox for business proporciona còpies de seguretat dels fitxers emmagatzemats, amb una alta granularitat, on des de la interfície web es poden recuperar totes les versions que hagin sigut pujades d'un fitxer o fins i tot, recuperar un fitxer que s'hagi esborrat. Aquesta funcionalitat està disponible amb una data màxima de 30 dies, encara que es pot contractar un suport de *Backup* amb més retenció.
Dropbox, de forma directa, no ofereix la possibilitat de realitzar *backups* de directoris o dispositius al complert, pel que si es requereix aquesta opció es pot realitzar copiant o movent contingut sota el directori principal.

4.1.3. Sincronització

Existeixen clients per a totes les plataformes conegudes, des de ordinadors personals amb *Windows* o *MacOSX*, com per a sistemes operatius de dispositius mòbils com *iOS*, *Android*, etc..
Dropbox, permet llistar els dispositius vinculats i revocar-li els permisos de sincronització si s'escau. En aquest llistat, es mostra informació com el nom del dispositiu, el país o ubicació des d'on es va connectar, la data i hora de la última connexió i la IP pública des d'on ho va fer, juntament amb la versió del client utilitzat.
Tanmateix, també permet visualitzar les sessions web actives de l'usuari i l'històric, mostrant la data i la última hora en la que es va connectar, i les aplicacions que hi ha vinculades. Alhora ofereix la possibilitat d'esborrar remotament les dades i les còpies locals de dispositius i ordinadors quan un empleat causi baixa o en el cas de pèrdua o robatori.

4.1.4. Compartició

Dropbox per defecte crea un directori anomenat "*Public*", el qual esta pensat per compartir els fitxers que s'inclouen de forma completament pública. Per compartir només cal, moure un fitxer en aquest directori, i crear-ne una URL pública amb la que accedir-hi. A més d'utilitzar aquest directori per compartir, es poden crear comparticions de tots els fitxers i directoris, ja sigui de forma pública o entre altres usuaris amb compte de *Dropbox*, de forma ràpida i senzilla. Mitjançant la funcionalitat "*Share*" es poden compartir directoris sencers entre usuaris, ja siguin usuaris amb compte o usuaris aliens. Per als usuaris amb comptes, aquests s'inclouen en el esquema de directoris sota el directori principal, mentre que per als usuaris aliens, aquesta

compartició es materialitza únicament mitjançant una URL pública.

Ara bé, referent a la compartició de dades amb usuaris no registrats o de forma totalment pública, aquesta presenta inconvenients de seguretat que cal comentar. Quan es comparteix un fitxer mitjançant una URL ***[veure Fig.3]***, aquesta es genera de forma semi-aleatòria amb un format similar a aquest:

https://www.dropbox.com/s/zpo....e1nsg/Subtitle%20Master%200.6.zip?dl=0

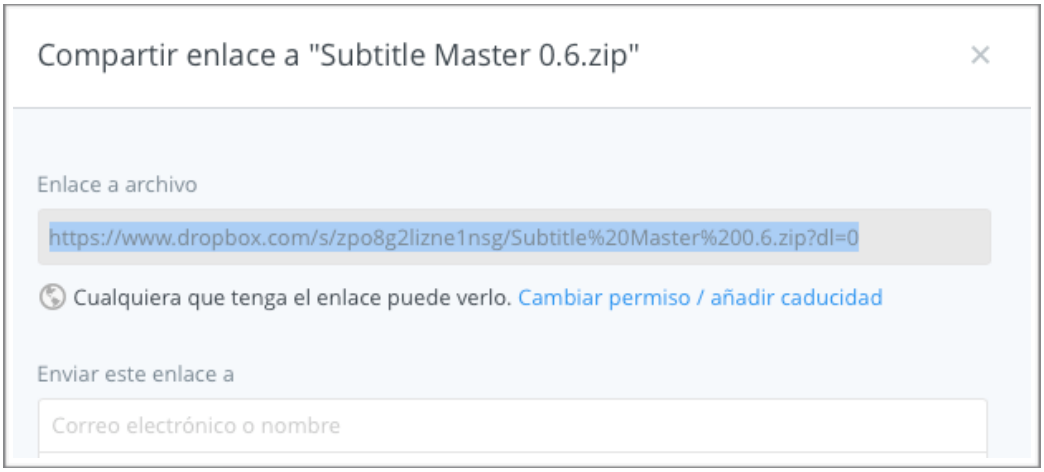

Fig. 3 - Creació enllaç de compartició - Dropbox

Com podem comprovar, la part final de la URL mostra clarament el nom del fitxer que es comparteix. Es cert que la primera part es generada aleatòriament amb un codi de 15 caràcters, però la segona mostra informació de l'usuari, i per tant, la URL no queda completament ofuscada. Aquest problema pot comportar que un atacant, amb un simple *script* que busqui diferents combinacions de URLs, trobi fitxers en directoris públics dels usuaris.

4.1.5. Capacitat i Escal.labilitat

Dropbox ofereix una capacitat inicial de fins a 1 TB per usuari en la seva modalitat *Business*. No hi ha limitació en capacitat total, i ofereix una escal.labilitat il·limitada, sempre sota pagament per usuari i ús.

4.1.6. Integració directori corporatiu

Existeix integració amb Directoris Actius (AD) corporatius de *Microsoft*, però no per Directoris basats en LDAP[15]. Tanmateix, ofereix integració amb sistemes d'autenticació única (SingleSignOn), basats en l'estàndard "*Security Assertion Markup Language (SAML)*". Entre el llistat de proveïdors d'identitat que suporta hi ha:

- Ping Identity
- OneLogin
- Okta
- Centrify
- Symantec Identity
- Bitium
- Auth0
- Salesforce
- CA Siteminder

4.1.7. Gestió centralitzada i Monitorització

Dropbox incorpora un sistema de gestió centralitzada, la consola d'administració, des d'on es poden administrar els usuaris, grups, comparticions, dispositius. Entre les principals característiques i accions que es poden realitzar amb la consola hi ha [16]:

- Auditoria de l'activitat dels usuaris, fitxers, grups, etc.. Aquesta auditoria permet exportar dades d'usuaris concrets o grups de treball amb informació dels *logins* realitzats, comparticions, ús de dispositius, etc..
- Control de dispositius per comptes d'usuaris.

- Controls i administració dels permisos de compartició de fitxers dels diferents usuaris o grups d'usuari amb els altres usuaris de la corporació o usuaris externs.
- Control de les sessions web actives, on es pot fer un seguiment i finalitzar-les si es necessari.

Estudi requeriments tècnics de seguretat

4.1.8. Principis bàsics de seguretat de les dades

Dropbox compleix amb els estàndards de privacitat i protecció de dades ja que disposa de les certificacions següents [17]:

- *EU-U.S. and Swiss-U.S. Safe Harbor.*
- *Certificació ISO 27001.*
- *CSA STAR: Security Trust and Assurance Registry.*

Cal destacar per contra, que *Dropbox*, dins de les seves *Privacy Policies* comenta que podrà revelar informació d'usuaris a terceres parts en cas de sol·licitar-ne per via jurídica, o per evitar o ajudar a persones en perill o bé sota circumstàncies extraordinàries.

Dropbox utilitza els serveis d'*Amazon S3* com a proveïdor d'emmagatzemament final [18]. Concretament, utilitzen els *Data Centers* que *Amazon* té arreu el territori dels Estats Units, pel que totes les dades es troben físicament distribuïdes arreu del territori americà. Per contra, no proporciona cap informació de com tracta la seguretat física de la resta de la seva infraestructura.

4.1.9. Autenticació dels usuaris al servidor

L'autenticació, en tots els seus clients, requereix d'un usuari i contrasenya el qual es transmet sota canals de comunicació segurs, concretament sota els protocols SSL o TLS. Com a identificador d'usuari, s'utilitza l'adreça de correu amb la qual s'hagi donat d'alta l'usuari. Pel que respecta a la contrasenya, aquesta ha de ser de mínim 6 caràcters, encara que es permeten les contrasenyes febles. Per tal de minimitzar riscos en l'autenticació, *Dropbox* pot inhabilitar un compte quan aquest ha tingut un número elevats d'intents de *login* que hagin resultat fallits, evitant així els possibles atacs de força bruta.
Pel que respecta a la interfície web, aquesta sempre opera sota el protocol HTTPS, de manera que les comunicacions sempre estan protegides sota xifratge.
Dropbox ofereix l'autenticació en 2 passos, *Two-steps verification* [19].

4.1.10. Comunicació i transmissió de les dades entre clients i servidor

Per protegir totes les dades que han de ser tramesses entre els servidors *Front-End* i les aplicacions dels usuaris, *Dropbox* utilitza els protocols SSL i/o TLS, que creen canals de transmissió segurs basats en algoritmes AES-256 o superiors. A més, tant per a les solucions client d'escriptori i de dispositius mòbils com per als navegadors web, *Dropbox* utilitza algoritmes de negociació de clau autenticats mitjançant RSA, és a dir, la clau simètrica es genera utilitzant nous valors en cada una de les negociacions, aconseguint així *'Perfect Forward Secrecy'*[20]. El servidor utilitza la seva identitat digital per autenticar la negociació i així evitar possibles atacs 'M*an-in-the-Middle*'.

4.1.11. Encriptació de les dades al servidor

Les dades emmagatzemades als *Back-Ends* de *Dropbox* són sempre xifrades utilitzant algoritmes de xifrat AES-256. Les dades no són xifrades en el costat del client, pel que aquestes són tramesses i posteriorment xifrades en el costat del servidor utilitzant les pròpies claus de xifrat de *Dropbox* [21].

4.1.12. Actualitzacions de seguretat

Dropbox utilitza una política d'actualitzacions molt eficient la qual aplica quasi bé, cada setmana. Quan apareix una nova actualització, el client s'actualitza de forma automàtica, desatesa per part del client i, normalment, de forma transparent per a l'usuari final. D'aquesta forma, es garanteix que cap dels clients tinguin forats de seguretat que poden comprometre la confidencialitat de les dades.

4.2. SugarSync for Business

SugarSync for Business [22] és una de les solucions de *Cloud Storage* per a empreses que més està creixent en els últims temps. *SugarSync* va començar oferint servei de *Cloud Backup* exclusivament, però des de fa un temps ofereix les funcionalitats que el nostre sistema requereix.

Estudi funcionalitats bàsiques

4.2.1. Emmagatzemament de fitxers

SugarSync disposa de client per a les plataformes de *MacOSX* i *Windows*. Aquest client es mostra com una aplicació d'escriptori, en la qual es poden seleccionar aquells directoris que es pretenen copiar al *Cloud Storage*. Per tant, tots els directoris i fitxers que s'hagin seleccionat seran els que s'emmagatzemaran al *Cloud* i marcaran l'estructura de directoris a crear. Paral·lelament a l'ús del client, també existeix la opció d'utilitzar l'interfície web, amb la qual es poden gestionar tots els fitxers i directoris que s'hagin seleccionat per a copiar, permetent pujar-ne de nous, modificar o esborrar-los.

4.2.2. Backup

SugarSync inicialment era un producte que gestionava *Backups* de plataformes d'escriptori i de dispositius mòbils. Actualment encara disposa d'aquesta funcionalitat, encara que podríem dir que aquesta s'ha unificat amb l'emmagatzemament de dades al *Cloud Storage*. En aquest apartat cal destacar que *SugarSync* dins de les seves grans funcionalitats destaca la possibilitat de recuperar fitxers esborrats i/o aquells que han sigut modificats. Emmagatzema fins a 5 versions diferents d'un mateix arxiu. Aquests *backups* no són comptabilitzats dins la quota de l'usuari.

4.2.3. Sincronització

Com ja s'ha comentat existeixen clients per a *Windows* i *Mac*, i a més clients per a dispositius mòbils *iOS* i *Android*.
Sugarsync, permet gestionar els dispositius tal i com s'ha especificat en els requeriments. Permet llistar els vinculats i revocar-li els permisos de sincronització si s'escau. També ofereix la possibilitat d'esborrar remotament les dades de dispositius i ordinadors quan un empleat causi baixa o en el cas de pèrdua o robatori.

4.2.4. Compartició

SugarSync permet la compartició tant de fitxers com de directoris sencers. Aquesta compartició es pot realitzar entre usuaris registrats i amb usuaris externs, els quals accediran al fitxer o directori compartit mitjançant una URL d'accés. Per a usuaris del producte *business*, *SugarSync* incorpora una eina de compartició de directoris, on es poden crear comparticions de directoris entre grups privats de la mateixa companyia, on els usuaris poden crear, editar, esborrar i sincronitzar els fitxers.

Ara bé, la compartició mitjançant la creació d'un enllaç, presenta inconvenients de seguretat que cal remarcar. L'usuari crea una URL de forma aleatòria, la qual pot ser temporal o permanent. Qualsevol usuari que conegui aquesta URL i accedeixi, automàticament, es descarregarà el

fitxer. Aquesta no requereix d'autenticació prèvia per accedir-hi. Per una altra banda, quan es crea una compartició d'aquest tipus i permanent, qualsevol modificació del fitxer en local, es veu reflectit en el fitxer publicat. Aquest enllaç pot ser enviat de forma automàtica, via correu electrònic, a usuaris registrats i no registrats, els quals podran sincronitzar i descarregar el fitxer, respectivament. Ara bé, això pot ser un problema de seguretat si analitzem el format de la URL que es genera:

https://nom_usuari.sugarsync.com/getfiles/codi_aleatori

Com es pot veure aquí, la URL esta composada pel nom d'usuari i un codi aleatori. Qualsevol atacant que sàpiga el codi d'usuari d'una possible víctima, pot executar un *script* que contingui una iteració del codi aleatori en busca de fitxer públics d'aquest usuari. Quan un atacant trobi un enllaç públic, automàticament, podrà descarregar-se aquest fitxer, sense que l'usuari propietari se n'assabenti.

Aquesta mateixa compartició es pot realitzar per a directoris sencers, on el format de la URL és similar al següent: https://nom_usuari.sugarsync.com/nom_del_directori

Qualsevol atacant que sàpiga el codi d'usuari podrà realitzar intents de trobar directoris 'comuns' amb un simple atac de força bruta si no existeixen altres mesures per mitigar aquesta vulnerabilitat.

4.2.5. Capacitat i Escal.labilitat

SugarSync ofereix una capacitat total de fins 1 TB, sense limitació d'espai per usuari. No indica l'escal.labilitat que ofereix. El pagament es realitza per ús i per nombre total d'usuaris [23].

4.2.6. Integració directori corporatiu

SugarSync només ofereix integració amb Directoris Actius i sistemes SSO amb aplicacions de tercers com *OneLogin* o *miniOrange* [24]. No incorpora un sistema propi, pel que aquestes han de ser adquirides paral.lelament al sistema de *Cloud Storage*.

4.2.7. Gestió centralitzada i Monitorització

SugarSync incorpora un sistema de gestió centralitzada, *'Admin Dashboard'*, des d'on es poden administrar els usuaris, grups, comparticions, dispositius. Permet monitoritzar l'activitat constant de tots els usuaris, administrar l'emmagatzemament, administrar quotes, visualitzar els dispositius, eliminar dades remotament, etc.. Per contra, no existeix la possibilitat de generar informes d'estat.

Estudi requeriments tècnics de seguretat

4.2.8. Principis bàsics de seguretat de les dades

SugarSync compleix amb els estàndards de privacitat i protecció de dades segons les certificacions següents [25]:

- *EU-U.S.Safe Harbor framework and Swiss-U.S. Safe Harbor framework.*
- *TRUSTe Cerfified Privacy.*

Cal destacar, i al igual que *Dropbox*, dins de les seves *Privacy Policies* comenta que podrà revelar informació d'usuaris a terceres parts en cas de sol.licitar-ne per via jurídica, o en el cas de sol.licitar-ho explícitament per part de l'usuari.

SugarSync utilitza com a infraestructura de *Back-End* els serveis de *Cloud Computing Amazon AWS*, concretament l'*Amazon Simple Storage Service - S3*, com a un dels dos 'geo-redundants' Data-Centers de que disposa [26]. Per contra, *SugarSync* no proporciona cap informació de com tracta la seguretat física de la resta de la seva infraestructura.

4.2.9. Autenticació dels usuaris al servidor

SugarSync utilitza en tots els seus clients, ja sigui d'escriptori, dispositius mòbils com per a la interfície web, un mètode d'autenticació basat en usuari i contrasenya. Per norma general, per a aquest usuari s'utilitza l'adreça de correu electrònic, o bé en el cas del producte empresarial, l'usuari amb el qual s'hagi registrat. Per a la realització d'aquesta autenticació, s'utilitzen canals segurs de comunicació TLS. Pel que respecta a la interfície web, aquesta requereix d'una autenticació prèvia, sempre sota el protocol HTTPS, assegurant així que la informació que s'intercanvia sempre estarà xifrada.

SugarSync no incorpora la opció d'autenticació en dos passos, *'Two-Step Verification'*, que garanteix que cap dispositiu no autoritzat es vinculi al compte sense permís del propietari.

4.2.10. Comunicació i transmissió de les dades entre client i servidor

SugarSync utilitza canals segurs de comunicació, sempre sota el protocol TLS per a la sincronització de les dades de l'usuari i els seus servidors. Això vol dir, que prèvia transferència de dades entre usuari i servidor, existeix una negociació i establiment d'aquests canals segurs per on es transmeten les dades.

4.2.11. Encriptació de les dades al servidor

Una vegada les dades s'emmagatzemen en els *Back-Ends* de *SugarSync*, aquestes són xifrades mitjançant algoritmes AES-256. No s'ha pogut trobar més informació de com realitza aquest xifrat.

4.2.12. Actualitzacions

Els clients, tant d'escriptori com mòbils, requereixen de la interacció de l'usuari per a ser actualitzats, pel que aquest són els responsables de tenir-los en la última versió.

4.3. Box Business

Box Business [27] és una de les noves solucions de *Cloud Storage* per a empreses que s'està donant a conèixer en els últims anys i que va guanyant mercat poc a poc.

Estudi funcionalitats bàsiques

4.3.1. Emmagatzemament de fitxers

La principal funcionalitat de *Box* és la de emmagatzemar fitxers al *Cloud*. Disposa de client, en format d'aplicació per a escriptori, per a les plataformes de *MacOSX* i *Windows*. Quan s'instal.la el client, es crea un directori anomenat "*Box Sync*" en el que s'emmagatzemen totes les dades que es vulguin guardar al *Cloud*. Funciona igual que *Dropbox*, però en aquest cas, disposa d'una interfície per gestionar aquest directori, el qual pot ser modificat i escollir un de ja existent.
Al igual que amb les altres solucions estudiades, existeix la opció d'utilitzar l'interfície web, amb la qual es poden gestionar tots els fitxers i directoris que s'hagin copiat o mogut al directori establert al client d'escriptori, a més de poder crear-ne de nous, modificar o esborrar.

4.3.2. Backup

Box no disposa d'un sistema de *Backup* per a crear còpies de seguretat de directoris i fitxers, però tot el que s'emmagatzema sota el directori principal queda emmagatzemat al sistema, el qual ofereix la possibilitat de recuperar fitxers o directoris esborrats i de versions diferents. A més també permet recuperar les dades de dispositius vinculats a un compte.
Per contra, Box no informa de les retencions de temps aplicades a aquestes còpies de seguretat.

4.3.3. Sincronització

Existeixen clients per a *Windows* i *Mac*, i a més clients per a dispositius mòbils *iOS*, *Android*, *Windows Phones* i *Blackberry*. Tot usuari que tingui un compte Box, podrà vincular tots els dispositius que consideri i sincronitzar els seus fitxers entre tots aquests dispositius.

Box permet gestionar els dispositius tal i com s'ha especificat en els requeriments. Permet llistar els vinculats i revocar-li permisos de sincronització si s'escau. També ofereix la possibilitat d'esborrar remotament les dades i les còpies locals de dispositius i ordinadors quan un empleat causi baixa o en el cas de pèrdua o robatori per mitjà de la consola d'administració.

4.3.4. Compartició

Box, al igual que la resta, permet compartir tant fitxers com directoris sencers. Aquesta compartició es pot realitzar entre usuaris registrats, que veuran la compartició com un directori més, i/o amb usuaris externs, els quals accediran mitjançant una URL d'accés. Possiblement, en comparació amb la resta de solucions, aquesta presenta múltiples possibilitats i facilitats d'administració basada en nivells de privilegis sobre les comparticions de fitxers [28]. Entre les seves principals característiques trobem :

- Possibilitat de compartir fitxers mitjançant enllaços (URLs) protegides amb contrasenya. Aquestes contrasenyes poden tenir data d'expiració automàtica i restricció d'accés per descàrrega i usuari.
- Compartició de directoris entre usuaris registrats, aplicant privilegis de fins a 7 nivells: co-propietari, administrador, editor, accés de només lectura, etc..
- Creació de comparticions mitjançant URLs segures, compatibles amb totes les plataformes de dispositius mòbils. Aquestes comparticions poden tenir diferents criteris de seguretat segons cada un dels dispositius.
- Control de versions i disponibilitat dels fitxers compartits, amb la que es poden crear tasques programades per esborrar continguts i desactivar enllaços d'accés per usuari i dispositiu.
- Càrrega de fitxers via correu, amb notificacions dels canvis efectuats a cada compartició.
- Sistema de notificacions: es pot activar per directori o fitxer compartit, i permet enviar notificacions de les accions realitzades sobre una compartició com, per exemple, visualitzar, descarregar, pujar fitxers i esborrar-los.

Com es pot veure en la següent imatge ***[veure Fig.5],*** les URLs de cada una de les comparticions són generades mitjançant 32 caràcters semi aleatoris. El format de l'enllaç és el següent:

https://app.box.com/s/
3yzit755aiu2vf77b3bbaz7745cz4dsu

on els 32 caràcters ofereixen un rang de fins a 36^32 possibilitats. Si a més li sumem el 'salt' previ (caràcter posterior a la url) de app.box.com aquesta xifra incrementa notablement.

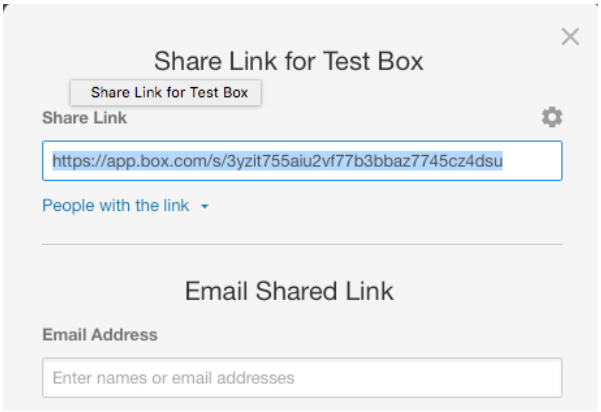

Fig. 5 - Creació enllaç de compartició - Box

Aquest format de URL, el qual no conté cap indici del nom d'usuari ni del nom de fitxer que es comparteix, redueix notablement la possibilitat de que un atacant pugui accedir al contingut mitjançant atacs de força bruta.

4.3.5. Capacitat i Escal.labilitat

Box ofereix una capacitat sense límits, és a dir, sense limitació d'espai per usuari, pel que l'escal.labilitat és il·limitada. Ara bé, restringeix la pujada de fitxers a com a màxim 5 GB per fitxer. El pagament es realitza per ús i per nombre total d'usuaris [29].

4.3.6. Integració directori corporatiu

Box ofereix integració amb Directoris Actius (AD i LDAP) per a l'aprovisionament d'usuaris i grups, i a més permet la integració amb sistemes SSO (*Open ID providers*) amb els quals es permet realitzar l'autenticació automàtica en el servei.

4.3.7. Gestió centralitzada i Monitorització

Box disposa d'un sistema de gestió centralitzada, '*Admin Console*', des d'on es poden administrar els usuaris, grups, comparticions, dispositius, integració amb el SSO. Entre les principals característiques trobem [30]:

- Control, administració i auditoria d'usuaris i grups d'usuaris, dels moviments de dades d'usuaris i entre usuaris, i qualsevol informació relativa a l'usuari i el seu compte. A més de la possibilitat d'extreure informació de les sessions establertes, històric de sessions, dispositius vinculats, etc.. Control i administració de les comparticions.
- Administració dels dispositius i aplicacions vinculades als comptes d'usuari.
- Generació d'informes d' estat del sistema i automatització de processos i *workflows* que poden ajudar als administradors de TI a facilitar les seves tasques.

Estudi requeriments tècnics de seguretat

4.3.8. Principis bàsics de seguretat de les dades

Box compleix amb els estàndards de privacitat i protecció de dades segons les certificacions següents [31]:

- *EU-U.S.Safe Harbor and Swiss-U.S. Safe Harbor.*
- *TRUSTe Cerfified Privacy.*
- *TRUSTe APEC Privacy.*
- *Certified ISO 27001.*
- *HIPAA Compliance: on garanteix que aplica les mesures de seguretat tant administrativa, tècnica com físiques dictades per la organització Health Insurance Portability and Accountability Act (HIPAA), referent en estàndards de transaccions electròniques als EUA.*

Box utilitza la tecnologia de proveïdors de *Cloud Computing* com *Equinix* (principalment) i *Amazon S3* [32]. Tenen 2 *Data-Centers* primaris situats al nord de Califòrnia (EUA) i un *Disaster Recovery Center* a Las Vegas. Tal i com detallen a la seva web [33], disposen de mecanismes de seguretat física, que inclouen polítiques estrictes d'accés controlades per mètodes d'autenticació biomètrics, circuits tancats de video-vigilància i monitorització, a més d'agents de seguretat armats per tal de protegir les dades que emmagatzemen.

4.3.9. Autenticació dels usuaris al servidor

Box utilitza en tots els seus clients, d'escriptori i dispositius mòbils, com per a la interfície web, un mètode d'autenticació basat en usuari i contrasenya. L'identificador d'usuari utilitza l'adreça de correu electrònic amb la qual s'ha registrat per a usuaris finals, mentre que per a usuaris del producte *Box for Business*, l'usuari ve donat per l'escollit com identificador de la companyia. L'autenticació es realitza mitjançant canals segurs de comunicació sota els protocols SSL i TLS, xifrats amb un algoritme AES-256.

Box, a diferència de la resta de solucions, incorpora una sèrie de mesures addicionals de seguretat [34] en l'autenticació dels usuaris corporatius, entre les que trobem:

- *Strong authentication*: on es pot personalitzar els requeriments per a la contrasenya aplicant, per exemple, longitud mínima i obligatorietat d'incloure caràcters especials en les contrasenyes, així com una política de caducitat, bloqueig en cas d'intents fallits de *login*, establiment de duració màxima d'una sessió, etc..
- *Two-Step Verification*: on es requereixi un permís del propietari per a poder autenticar-se o vincular nous dispositius, garantint així que usuaris no autoritzats puguin robar les credencials dels usuaris.
- *Granular Authoritzation*: on l'administrador pot definir fins a set nivells de privilegis per a l'accés, pre-visualització, edició i compartició de fitxers i directoris. D'aquesta forma, es garanteix que un usuari o grup d'usuaris només veuran allò al que tenen privilegis.
- *Flexibility access controls*: existeix la possibilitat de protegir mitjançant una contrasenya documents, presentacions i altres fitxers de major sensibilitat. Aquesta contrasenya pot ser permament o bé, tenir una data d'expiració automàtica.
- *Enterprise Mobility Management (EMM)*: Box ofereix la possibilitat d'integrar una tecnologia de control i configuració de dispositius mòbils externa. EMM permet manegar dispositius mòbils remotament, les aplicacions instal·lades i la informació que maneguen, controlant quins usuaris tenen accés a aplicacions concretes i quina informació poden veure, modificar, esborrar o fins i tot, transferir. Aquesta capa extra de seguretat, permet a l'administrador de TI tenir un control remotament sobre aquells dispositius que tracten amb informació de la companyia.

4.3.10. Comunicació i transmissió de dades entre client i servidor

Box garanteix que les dades que manega compleixen amb els requisits de confidencialitat i integritat, ja sigui quan aquesta es transfereix des dels clients cap als servidors de *Box*, com una vegada s'emmagatzemen en aquests ***[veure Fig.4]***. *Box* utilitza canals segurs de comunicació, sota els protocols SSL v3.3 i/o TLS per a la transmissió de les dades de l'usuari.

A més, per a la solució for *Business*, ofereix l'*"Enterprise Key Management (EKM)"* [35]. Aquesta solució permet utilitzar claus de xifrat administrades pel client (corporació) per protegir les dades pròpies. Amb l'ús d'aquesta EKM, les corporacions tenen un control de les claus de xifrat utilitzades assegurant així que les dades no podran ser accessibles quan aquestes s'emmagatzemin als servidors de *Box*, alhora que s'audita tot xifrat i ús de les claus corporatives [36]. L'ús d'aquesta solució garanteix el tractament i emmagatzemament segur de les dades sensibles i confidencials d'una companyia, així com controlar i oferir transparència en l'accés i modificació.

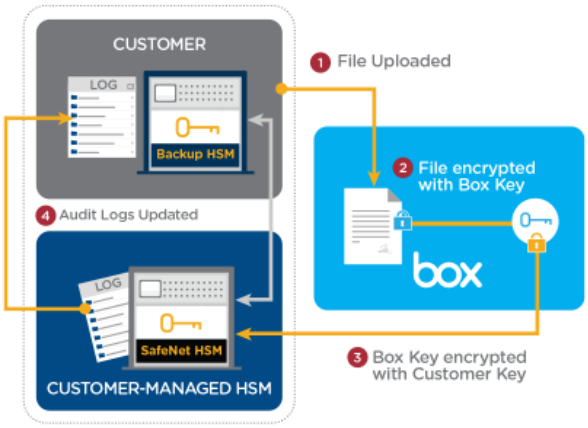

Fig. 4 - Comunicació xifrada entre client i servidor - Box

4.3.11. Encriptació de les dades al servidor

Una vegada les dades s'emmagatzemen en els *Back-end* de *Box*, aquestes són xifrades utilitzant mètodes de xifrat multi-capa amb algoritmes AES-256. Les claus de xifrat utilitzades, a diferència de les demés solucions, són emmagatzemades de forma segura en diferents localitzacions.

4.3.12. Actualitzacions

Les actualitzacions de les aplicacions d'escriptori es realitzen de forma automàtica, desatesa i transparent per a l'usuari. D'aquesta forma s'evita que l'usuari final treballi amb clients obsolets i que poden tenir problemes de seguretat que comprometin la seguretat de les dades. Els clients de

dispositius mòbils s'actualitzen sota petició de l'usuari.
La consola d'Administració no requereix d'actualització ja que aquesta es gestiona via web, pel que les actualitzacions les realitzen des del costat del proveïdor.

4.4. SpiderOAK Enterprise

SpiderOak Enterprise [37] és una solució de *Cloud Storage* per a empreses que més prestigi té en quan a seguretat es tracta. Tal i com diuen en la seva presentació, són la solució de *Cloud Storage* que ofereix *'Zero-Knowledge privacy'* [38], on tots els fitxers que són emmagatzemats són 100% privats i només visibles pel seu propietari.

Estudi funcionalitats bàsiques

4.4.1. Emmagatzemament de fitxers

SipderOak disposa de client d'escriptori, per a les plataformes de Mac OSX, Windows i Linux, així com versions per a Android i iOS. Alhora d'instal.lar el client, crea un directori sota la '*home*' d'usuari local, anomenat *"SpiderOak Hive"* en el qual l'usuari podrà emmagatzemar totes les dades que vulgui guardar al *Cloud*. Aquest client, treballa com un servei en local i en *background*, actualitzant les dades constantment.
També existeix la opció d'utilitzar l'interfície web, però a diferència de la resta, en aquesta gestió web no es permet pujar ni manegar els fitxers emmagatzemats. Tan sols, permet descarregar els fitxers guardats al *Cloud*, ordenats pels dispositius que s'hagin vinculat.

4.4.2. Backup

SipderOak ofereix la possibilitat de realitzar còpies de seguretat de les dades que es consideri oportú, seleccionant per directoris complets o per fitxers. Quan s'instal.la el client, dins de l'apartat *Backup*, es seleccionen aquells directoris a copiar i automàticament, aquests són copiats al *Cloud*. A més de realitzar *backups*, *SpiderOak* emmagatzema fins a 20 versions diferents d'un mateix fitxer, i permet recuperar la versió que l'usuari desitgi.

4.4.3. Sincronització

SipderOak permet vincular dispositius amb *Android* OS i iOS, tants com es consideri, i sincronitzar els seus fitxers entre tots aquests dispositius. La sincronització entre dispositius de *SpiderOak* podríem dir que es completament automàtica, però incorpora una funcionalitat extra que permet crear "*SharedFolders*", on es poden seleccionar 2 directoris de diferents dispositius per a que siguin sincronitzats entre sí ***[veure Fig.7]*.**
Dins de la gestió web, només permet descarregar fitxers d'aquests dispositius vinculats i no podent realitzar cap altra acció. En aquesta gestió si que permet, si es necessari, desvincular-los i suspendre la sincronització dels dispositius que es consideri.

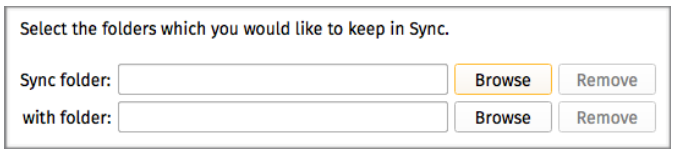

Fig. 7 - Sincronització de directoris - SpiderOak

4.4.4. Compartició

SpiderOak permet crear "*SharedRooms*", tal i com ells anomenen. Aquests són simples comparticions de fitxers i directoris entre usuaris registrats i/o amb usuaris externs, els quals accediran al fitxer o directori compartit mitjançant una URL d'accés. En aquest cas, no es generen automàticament URLs per compartir ràpidament fitxers i directoris, sinó que cal realitzar un procés previ, on es creen *SharedRooms*, les quals contindran els directoris a compartir.

Per començar a compartir es requereix crear un '*SharedID*' ***[veure Fig.8]***, el qual serà utilitzat per a crear la URL d'accés. Posteriorment, es crea el del *SharedRoom* assignant-li un nom i un directori al qual accediran els convidats. Finalment, es pot crear una contrasenya d'accés per a limitar i assegurar que només qui realment té privilegis d'accés pot accedir-hi.

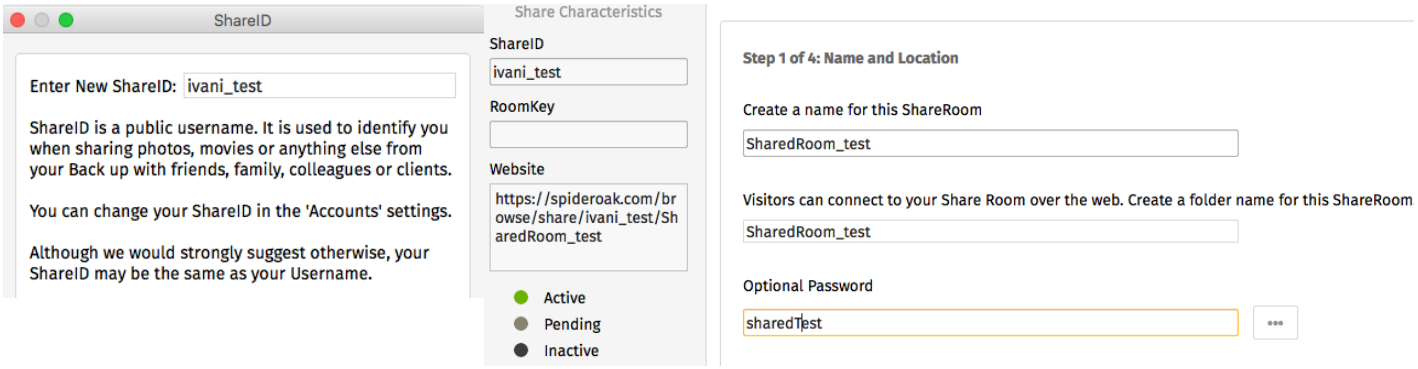

Fig. 8 - Creació compartició, SharedID i SharedRoom - SpiderOak

Un cop creada aquesta *SharedRoom*, tan sols s'ha de seleccionar el directori que es vol realment compartir. Un cop seleccionat es genera la URL amb la que s'accedirà amb un format similar a aquest: https://spideroak.com/browse/share/ivani_test/SharedRoom_test

Com es pot veure en aquesta URL d'exemple, no conté cap informació 'real' del directori o fitxer a compartir. La URL es construeix a partir de dos noms escollits pel propi usuari (identificador i nom del *SharedRoom*). Aquesta no identifica quin usuari l'utilitza o comparteix, quin es el nom del fitxer o directori o el possible contingut d'aquest, pel que no pot ser utilitzat per un atacant. Com aquesta és generada a partir de noms semi-aleatoris, els atacants tindran més dificultats per utilitzar atacs de força bruta per endevinar possibles comparticions d'usuaris.

4.4.5. Capacitat i Escal.labilitat

SipderOak ofereix espai il.limitat per al producte *Enterprise* sense cap limitació per usuari. El pagament es realitza per mes i nombre d'usuaris totals.

4.4.6. Integració directori corporatiu

SpiderOak només ofereix integració amb Directoris Actius i sistemes SSO amb aplicacions de tercers com *OneLogin* [39]. No incorpora un sistema propi, pel que aquestes han de ser adquirides paral·lelament al sistema de *Cloud Storage*.

4.4.7. Gestió centralitzada i Monitorització

SipderOak disposa d'un sistema de gestió centralitzada, des d'on es poden administrar els usuaris, grups, *SharedRooms* i dispositius vinculats. Entre les seves principals funcionalitats trobem:

- Gestió d'usuaris i grups, on es poden editar les configuracions d'aquests, deshabilitar o eliminar comptes, navegar pels seus directoris de fitxers, recuperar fitxers esborrats, etc..
- Administració de les *SharedRooms*, deshabilitar, eliminar, etc..
- Visualització senzilla de l'estat del sistema, amb el llistat de dispositius vinculats, espai utilitzats, *SharedRooms* creades, i la possibilitat de veure els *logs* dels sistema.

Estudi requeriments tècnics de seguretat

4.4.8. Principis bàsics de seguretat de les dades

SipderOak compleix amb els estàndards de privacitat i protecció de dades segons les certificacions de que disposa [40]:

- *EU-U.S.Safe Harbor and Swiss-U.S. Safe Harbor.*
- *HIPAA Compliance.*

SpiderOak utilitza únicament el seus propis *Data-centers*. Les dades són emmagatzemades utilitzant sistemes de fitxers clusteritzats amb una tolerància a fallades molt elevada i marge d'error de 0,000099%, que garanteixen la continuïtat i disponibilitat de les dades encara que la major part de la seva infraestructura estigui afectada. Tots els *Data-Centers* de *SpiderOak* estan securitzats, administrats i monitoritzats en mode 24x7, i estan ubicats a Kansas City (EUA) [41].

4.4.9. Autenticació dels usuaris amb el servidor

SipderOak utilitza un mètode d'autenticació basat en usuari i contrasenya per a totes les seves interfícies, ja sigui d'escriptori, web o dispositiu mòbil. Com a identificador d'usuari utilitza l'adreça de correu electrònic amb la qual s'ha registrat. L'autenticació es realitza mitjançant canals segurs de comunicació xifrats amb un algoritme de AES-256, sota els protocols SSL i/o TLS.
SipderOak centra la seva aposta per la seguretat sota el lema de "*Zero Knowlegde*"[42]. En la seva pàgina web, asseguren que són la única solució que garanteix la total privacitat de les dades que s'emmagatzemen al *Cloud [43]*. "*Zero Knowlegde*" significa que ells no coneixen res de les dades que es guarden al seus servidors. Garanteixen que el sistema de xifrat és únic, i que les dades són xifrades als ordinadors dels client, només transferides quan aquestes han finalitzat el procés de xifrat i mai desxifrades fins que aquestes tornen al dispositiu, mitjançant la pròpia contrasenya ***[veure Fig.9]***. Per tant, la contrasenya de l'usuari és, en si mateixa, la clau de xifrat i desxifrat de les dades.

It's not just "end to end encryption;" it's a Zero Knowledge System [38].

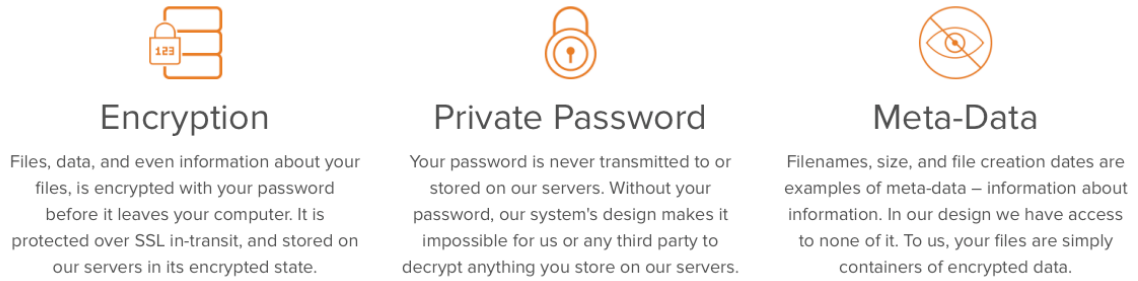

Fig. 9 - Ús de la contrasenya de l'usuari en el xifrat SpiderOak - Zero Knowlegde

En conseqüència d'aquest ús de la contrasenya, és de vital importància que l'usuari utilitzi una contrasenya forta i que mai l'oblidi. Per garantir això, recomanen utilitzar un "Password Hint" que ajudi a recordar aquesta contrasenya, ja que si aquesta es oblidada no es podran desxifrar les dades [42].

Però ara bé, aquesta tècnica comporta cert risc. Per desxifrar les dades, la contrasenya ha de ser emmagatzemada en alguna ubicació del dispositiu i ser utilitzada quan l'aplicació la requereixi. Això pot ajudar a que qualsevol atacant pugui capturar-la si té les eines suficients. Com eviten aquesta situació? Quan s'accedeix a les dades mitjançant un dispositiu mòbil o la interfície web, la contrasenya és emmagatzemada al servidor de *SpiderOak*, però només durant la duració de la sessió o fins que l'usuari tanqui el navegador. Per aquest període de temps, la contrasenya es guarda en un espai de memòria xifrat, on aquesta mai és copiada o moguda a un espai de memòria sense xifrar. Quan la sessió finalitza, la contrasenya és completament esborrada.

SpiderOak, disposa del sistema d'autenticació basat en 2 passos, *'Two Factor Authentication'*.

4.4.10. Comunicació i transmissió de les dades entre client i servidor

Com ja s'ha comentat, *SpiderOak*, xifra completament els fitxers de l'usuari al seu propi ordinador o dispositiu, evitant així, que aquests siguin enviats sense xifrar. Fins que el procés no acaba, cap dada surt dels dispositiu. Les dades són xifrades amb un algoritme de AES-256 i una clau de xifrat derivada a partir de la contrasenya de l'usuari (mitjançant PBKDF2-SHA256) més un 'salt' aleatori de 32 bytes. Cada fitxer i cada directori s'xifra amb una nova clau generada d'aquesta forma. Aquestes claus, mai són emmagatzemades en text pla als servidors de *SpiderOak*. L'ús d'aquesta tècnica minimitza la possibilitat d'atacs de força bruta o altres atacs realitzats utilitzant la clau de xifrat.

Tanmateix, totes les connexions entre client i servidor són securitzades mitjançant el protocol HTTPS sota TLS, xifrades amb algoritmes AES-256.

4.4.11. Encriptació de les dades al servidor

El procés de xifrat es realitza completament en el costat del client, és a dir, les dades són xifrades pel client abans de ser tramesses. Quan aquestes arriben al costat del servidor, ja estan protegides per la clau generada a partir de la contrasenya de l'usuari i per tant, ja xifrades.

4.4.12. Actualitzacions

Les actualitzacions dels clients, tant d'escriptori com dels dispositius mòbils han de ser executades manualment pels usuaris finals o desplegades a través de la consola de gestió, fet que pot suposar que mentre s'utilitzin versions antigues i aquests continguin vulnerabilitats conegudes, la seguretat de les dades pot ser compromesa.

Cloud Storages Privats

4.5. OwnCloud

Dins del *Private Cloud Storages*, *OwnCloud* [44] possiblement, ocupa un dels primers llocs del '*ranking*' de solucions més implementades per les companyies. *Owncloud* és una aplicació de codi obert que ofereix serveis d'emmagatzemament de fitxers al núvol, i que a diferència de la resta de solucions de *Cloud Storage* vistes fins ara, aquesta es troba dins la infraestructura de la companyia, utilitzant el propis servidors, *xarxes* i emmagatzemament. Per tant, les dades dels usuaris són emmagatzemades i administrades per la companyia i els seus tècnics de TI, els quals seran responsables de la seguretat d'aquestes.

OwnCloud ofereix accés universal als fitxers per mitjà d'un *Front-End*, normalment situat a la xarxa DMZ, amb el qual els usuaris s'hi connecten per poder accedir a les dades emmagatzemades en el B*ack-End*, des de qualsevol dispositiu, ja sigui mòbil, ordinador personal o per mitjà d'una interfície web, des de qualsevol ubicació i en qualsevol moment.

OwnCloud és una solució *OpenSource*, de la qual existeixen dues versions: *OwnCloud Server (Community Version),* reduïda en funcionalitats, i *OwnCloud Enterprise*, per a petites i grans companyies que requereixen de funcionalitats extres, així com un suport avançat garantit.

Estudi funcionalitats bàsiques

4.5.1. Emmagatzemament de fitxers

Com tota solució de *Cloud Storage*, la funcionalitat principal és la de emmagatzemar fitxers al *Cloud*, en aquest cas, al núvol híbrid. Existeixen clients d'escriptori per a *Windows*, *MacOSX* i *Linux*. Al igual que amb les altres solucions estudiades, existeix la opció d'utilitzar l'interfície

web que requereix d'una autenticació per part de l'usuari i amb la que es poden gestionar, pràcticament, totes les funcionalitats que incorpora.

4.5.2. Backup

OwnCloud no incorpora la opció de backup de directoris ni fitxers concrets, però si que implementa còpies de seguretat de tots els fitxers esborrats per un usuari. Aquests fitxers poden ser restaurats amb una antiguitat màxima de 30 dies i obtenir les diferents versions de cada un dels fitxers esborrats. Per activar aquesta funcionalitat, s'ha d'habilitar el mòdul pertinent.

4.5.3. Sincronització

Els usuaris podran vincular tots els dispositius que considerin i sincronitzar els seus fitxers entre tots aquests. Disposa de client web, client d'escriptori i clients per a dispositius mòbils, *iOS* i *Android*. Quan existeixen conflictes de sincronització, ja sigui per la modificació simultània d'un fitxer o el moviment d'aquest entre dos dispositius diferents, *OwnCloud* no esborra ni modifica cap fitxer, sempre crea una segona versió i deixa a l'usuari que decideixi quina de les dues es la versió correcta.

4.5.4. Compartició

La compartició dins d'*OwnCloud* és una funcionalitat que pot ser desactivada a gust de l'administrador. *OwnCloud* permet compartir dades tant amb usuaris registrats al sistema com amb usuaris externs. En el primer cas, l'usuari pot crear directoris o fitxers compartits amb altres usuaris amb visibilitat directa dins de la seva estructura de directoris per part de l'usuari destí. A aquesta compartició se li poden assignar diferents nivells de privilegis, edició, esborrar o compartir de nou. També permet crear-ne enllaços i donar una data d'expiració concreta.
Quan l'usuari no es un usuari del sistema, la forma de crear-la es mitjançant una URL. A aquesta també se li permet atorgar privilegis, així com crear-ne una contrasenya d'accés i afegir una data d'expiració. En ambdós casos, existeix la possibilitat d'enviar una notificació al destinatari.

4.5.5. Capacitat i Escal.labilitat

La capacitat del nostre *Cloud Storage* vindrà determinada tant pel sistema d'emmagatzemament intern, el qual té una capacitat limitada.

4.5.6. Integració directori corporatiu

OwnCloud es pot integrar amb serveis de directori LDAP o *Active Directory* corporatius, amb els que gestionar els usuaris d'una forma integrada i centralitzada. També incorpora la opció d'integrar-se amb sistemes d'autenticació única (SSO), mitjançant mòduls dissenyats específicament per a realitzar aquesta tasca.

4.5.7. Gestió centralitzada i Monitorització

OwnCloud disposa d'una consola d'Administració centralitzada molt potent, versàtil i amb múltiples funcionalitats, des d'on es poden administrar els usuaris, grups, *comparticions, calendaris*, etc.. Per contra, no disposa d'un control dels dispositius vinculats a un compte, i per tant, la possibilitat d'administrar-los. Aquesta consola permet monitoritzar l'activitat dels usuaris, els grups, les comparticions creades, enllaços públics actius, entre altres.

Estudi requeriments tècnics de seguretat

4.5.8. Principis bàsics de seguretat de les dades

En aquest cas, les dades són manegades pel frontal i emmagatzemades finalment en el sistema d'emmagatzemament intern de la corporació. Així doncs, la infraestructura de la corporació serà l'encarregada de garantir la seguretat de les dades. S'entén doncs, que aquesta gaudeix dels mitjans necessaris i esta dotada dels mecanismes de seguretat requerits en aquest projecte.

4.5.9. Autenticació dels usuaris al servidor

OwnCloud, també utilitza un mètode d'autenticació basat en usuari i contrasenya per a totes les seves interfícies, ja sigui d'escriptori, web o dispositiu mòbil. Aquest suporta tant els protocols HTTP, com canals segurs de comunicació sobre HTTPS xifrats amb un algoritme AES-256, sempre sota els protocol TLS.
OwnCloud, suporta el sistema d'autenticació basat en 2 pasos, *'Two Factor Authentication'*.

4.5.10. Comunicació i transmissió de les dades entre clients i servidor

Owcloud utilitza el protocol TLS, per defecte, per protegir les comunicacions entre clients i servidor. Tots els clients, web, d'escriptori i dispositius mòbils, utilitzen el protocol HTTPS, sota TLS, per a transmetre les dades i sincronitzar els fitxers.

4.5.11. Encriptació de les dades al servidor

Owcloud utilitza un mòdul anomenat *"OwnCloud's Encryption 2.0"*, per al xifratge de les dades emmagatzemades al *Backend*. Aquest utilitza una infraestructura de xifrat asimètrica, que genera un parell de claus, pública i privada, de fins a 4096-bits per a cada usuari ***[veure Fig.10]***.
Aquestes claus privades dels usuaris són generades quan l'usuari s'autentica per primer cop al sistema, i posteriorment xifrades mitjançant un algoritme de xifratge AES-256, utilitzant la pròpia contrasenya de l'usuari executada fins a 100.000 vegades en una funció de derivació de claus PBKDF2[53]. Per cada login de l'usuari, la clau privada és desxifrada i emmagatzemada en la pròpia sessió web PHP de l'usuari, utilitzada posteriorment per desxifrar tots els fitxers de l'usuari. Quan la sessió finalitza aquesta clau és completament eliminada.

Paral.lelament, per a cada un dels fitxers de l'usuari, es crea una clau generada aleatòriament de fins a 256 bits. Quan un fitxer es creat, es genera una d'aquestes claus i s'associa al fitxer, amb la que s'xifra el fitxer. Cada fitxer contindrà una única clau de xifrat.
Però com poden accedir els usuaris amb comparticions a aquests fitxers xifrats? Doncs, per resoldre aquest "conflicte", *OwnCloud* crea per cada un d'aquests fitxers, una clau 'compartida' anomenada *Share-Key*, utilitzant la clau pública de l'usuari amb accés al fitxer ***[veure Fig.10]*.**

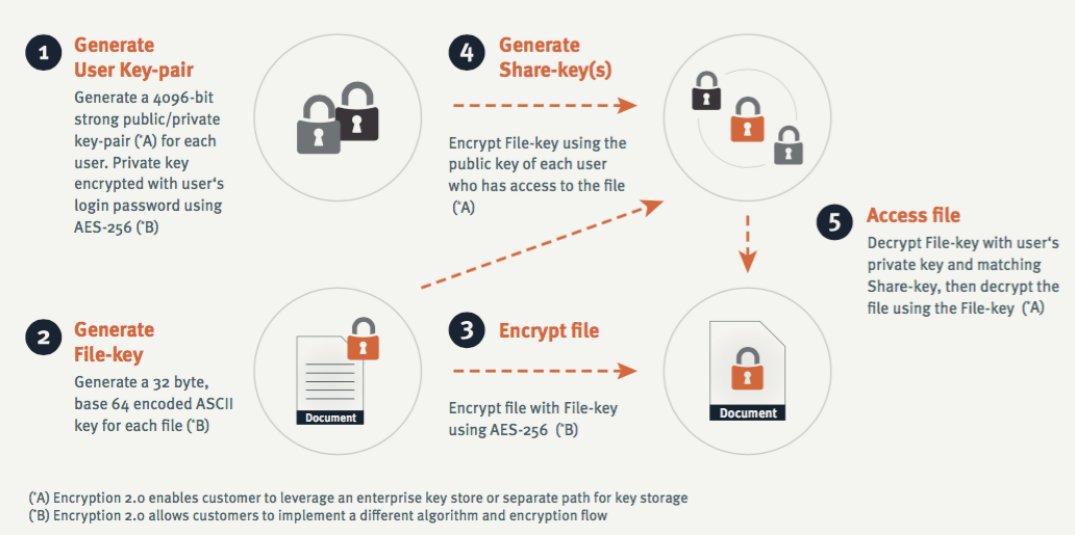

Fig. 10 - Infraestructura d'enciptació 2.0 - *OwnCloud*

4.5.12. Actualitzacions

OwnCloud disposa d'un sistema d'actualitzacions automàtiques dels clients. Aquesta ha de ser activada o desactivada des del propi client, el qual realitza les actualitzacions disponibles de forma automàtica i desatesa per part del client. D'aquesta forma es garanteix que el client està lliure de possibles vulnerabilitats i conté les últimes funcionalitats. En el cas del client per a *Linux*, aquesta ha de ser executada de forma manual i a petició de l'usuari administrador.

4.6. Resum comparatiu de les funcionalitats i característiques

A continuació es mostra una taula comparativa de totes les funcionalitats disponibles en cada una de les solucions i dels mecanismes de seguretat emprats:

	DROPBOX	SUGARSYNC	BOX	SPIDEROAK	OWNCLOUD
Còpia de Fitxers	Utilització directori concret "Dropbox"	• Copia i Backup unificada. • Selecció de directoris locals a copiar al núvol • Recuperació Fins a 5 versions fitxer	Utilització directori concret "Box Sync"	Utilització directori concret "SpiderOak Hive"	Utilització directori concret o possibilitat d'utilitzar el directori "*home*" local.
Backup	• Fins a 30 dies • Recuperació versions fitxer		• Recuperació de fitxers i versions • No informació retenció	• Selecció directoris per a Backups • Programació • Recuperació de fitxers de fins a 20 versions diferents	• Fins a 30 dies • Recuperació versions fitxer
Sincronització	• Llistat dispositius • Revocació permisos • Esborrat dades remotament	• Llistat dispositius • Revocació permisos • Esborrat dades remotament	• Llistat dispositius • Revocació permisos • Esborrat dades remotament	• Shared Folders: sincronització directoris concrets • Llistat dispositius • Revocació permisos	No disposa d'un control dels dispositius.
Compartició	• Directori públic • Creació URLs i directoris compartits • Granularitat Permisos • Presenta deficiències seguretat • Ofuscació parcial URLs generades aleatòriament	• Creació URLs i directoris compartits • Granularitat Permisos • Presenta deficiències seguretat • Ofuscació parcial URLs generades aleatòriament • Vulnerable atacs força bruta	• Creació URLs segures i protegides amb contrasenya • Granularitat Permisos • Upload fitxer via mail • Desactivació automatizada • Sistema notificacions	• SharedRooms • Creació directoris compartits via SharedID i nom_dir • Creació URLs protegides contrasenya	• Creació URLs segures i protegides amb contrasenya i data venciment • Desactivació automatitzada • Granularitat Permisos • Sistema notificacions
Tractament i Privacitat Dades	• *EU-U.S. and Swiss-U.S. Safe Harbor.* • *ISO 27001* • *CSA STAR: Security Trust and Assurance Registry*	• *EU-U.S. and Swiss-U.S. Safe Harbor.* • *TRUSTe Certified*	• *EU-U.S. and Swiss-U.S. Safe Harbor.* • *ISO 27001* • *HIPAA compliance* • *TRUSTe Certified* • *TRUSTe APEC*	• *EU-U.S. and Swiss-U.S. Safe Harbor.* • *HIPPA Compliance*	*Garantit per la pròpia infraestructura*
Localització	Amazon S3 (Estats Units)	Amazon S3 (Estats Units)	Equinix i Amazon S3 (Estats Units)	Infraestructura pròpia (Kansas - Estats Units)	Infraestructura pròpia
Capacitat	1 TB / Il.limitat	1 TB total	Il.limitada	Il.limitada	Limitada
Integració LDAP/SSO	Active Directory SSO (basat en SAML)	Aplicacions de tercers	Active Directory OpenLDAP SSO	Aplicacions de tercers	Active Directory OpenLDAP SSO
Gestió centralitzada	• Activitat usuaris • Moviment fitxers • Sessions actives • Dispositius i aplicacions vinculades • Administració comparticions	• Activitat usuaris • Moviment fitxers • Dispositius vinculats	• Activitat usuaris • Auditoria moviment fitxers i comparticions • Administració dispositius • Generació informes d'estat sistema	• Gestió usuaris • Administració dispositius • Generació informes d'estat sistema	• Activitat usuaris • Auditoria moviment fitxers • Activitat i administració de comparticions

	DROPBOX	SUGARSYNC	BOX	SPIDEROAK	OWNCLOUD
Mètodes Autenticació	SSL / TLS •HTTPS Login • Two Steps verification • Inhabilitació compte	SSL / TLS •HTTPS Login	SSL / TLS •HTTPS Login • Two Steps verification • Strong Auth. • Granular Auth. • Flexibility acces control •Enterprise Mobility Manag. (EMM)	SSL / TLS •HTTPS Login • Two Steps verification	SSL / TLS •HTTPS Login • Two Steps verification
Seguretat Comunicació	SSL/TLS Encriptació AES-256	TLS Encriptació AES-256	SSL/TLS Encriptació AES-256	SSL/TLS Encriptació AES-256 CFB/HMAC-SHA256	SSL/TLS Encriptació AES-256
Tipus Encriptació	256-bits AES Server- Side	256-bits AES	256-bits AES EKM (Enterprise Key Management)	*'ZeroKnowlegde'* 256-bits AES + Clau xifrat basada en contrasenya	Infraestructura clau pública/privada per usuari (4096-bits) Clau corporativa de recovery
Actualització	Automàtiques	Manuals	Automàtiques	Manuals	Automàtiques

Taula 3 - Taula comparativa de les solucions estudiades

4.7. Cost econòmic de cada solució

Per cada una de les solucions, s'ha realitzat una valoració econòmica basada principalment en el número d'usuaris que utilitzaran el servei, exactament uns 100 usuaris, així com la capacitat mínima d'espai que s'ha establert anteriorment per a cada un d'aquests usuaris i la global del sistema. Paral·lelament, també s'ha tingut en compte el tipus de suport tècnic que obtindríem en cada cas.

Els costos econòmics mostrats a continuació han sigut extrets de les planes web corporatives, així com a través de consultes via correu electrònic amb els comercials de les companyies. Algunes solucions ofereixen paquets per número d'usuaris, és a dir, a partir de 50, 100, 500 usuaris. En aquest cas s'ha dividit el preu total pel nombre total d'usuaris, obtenint el cost per unitat.

	Preu Usuari	Espai GB/ usuari	Tipus suport	Total mensual 100 usuaris	Total anual
DROPBOX	€12	1 TB	No especificat	€1200	**Total= 14400 €**
SUGARSYNC	€18	1 TB	12×5 Suport telefònic	€1800	**Total= 21600 €**
BOX	€18	Il.limitat	24x7 Suport telefònic especialitzat	€1800	**Total= 21600 €**
SPIDEROAK	€9 + 299 € Management Console	Il.limitat	No especificat	€1199	**Total= 14388 €**
OWNCLOUD	€9,6	Limitat per la infraestructura	12×5 Suport telefònic i correu electrònic	€960	**Total= 11.520€**

Taula 4 - Taula comparativa del cost econòmic de cada solució

4.8. Conclusions

Després de l'anàlisi efectuat de les diferents solucions i de provar cada una d'aquestes en entorns de test, podem veure que únicament dos de les solucions compleixen, gairebé al 100%, amb els requisits i les necessitats establertes en aquest projecte i per la pròpia corporació. Aquestes dues solucions són *Box*, com a *Public Cloud* i *OwnCloud* com a *Private Cloud,* les quals incorporen els mecanismes necessaris per a la correcta integració amb els serveis corporatius.

Per un costat Box, és una solució que ofereix totes les funcionalitats que necessita la corporació, a més d'implementar unes mesures de seguretat molt eficients, on destaquen, la forma d'abordar l'autenticació incorporant mecanismes addicionals, la metodologia de xifratge de les dades, així com el tractament d'aquestes, aportant tota una sèrie de certificacions que garanteixen que aquestes són tractades sota grans mesures de seguretat. Per contra, aquestes dades sempre són emmagatzemades en ubicacions concretes dels EUA, i per tant, sotmeses sota la legislació vigent en aquest país.
Ara bé, encara que sembla la solució més adient, el seu cost d'implantació i manteniment és el més elevat, i gairebé duplica el cost d'implantar la solució *d'OwnCloud*.

En l'altre costat es troba *OwnCloud*, solució que també proporciona totes les funcionalitats necessàries, destacant per sobre de totes, la gestió centralitzada mitjançant la consola d'administració i la infinitat de possibilitats extres que aquesta ofereix. A més, aquesta incorpora les mesures de seguretat adients, destacant, la metodologia de xifratge de les dades. Per contra, aquesta solució manca de l'escal.labilitat que requereix el sistema ja que depèn de la infraestructura existent, dins de la pròpia corporació.

Analitzant tots els factors podem dir que, com acostuma a succeir, el factor econòmic fa decantar la decisió per un costat o per un altre. Finalment, per la diferencia econòmica (gairebé més de 10.000€) s'ha optat per la solució de *Cloud* privat, *OwnCloud*.

La corporació disposa de la suficient infraestructura per tal d'implementar aquesta solució *OpenSource*, però per tal de garantir l'escal.labilitat i la flexibilitat del sistema necessària i requerida dins els objectius d'aquest projecte, s'ha optat per complementar aquesta solució amb un sistema d'emmagatzemament secundari subministrat per un proveïdor de *Cloud*, el qual estarà ubicat en les dependències d'aquest i garantirà així el possible creixement que la corporació requereixi.

5. Implementació solució *OwnCloud*

En aquest apartat es pretén mostrar tres dels factors clau i més importants de l'implementació de la solució escollida. Primerament es detallarà el sistema d'emmagatzemament secundari escollit per tal de donar l'escal.labilitat necessària al sistema. Seguidament es mostrarà com integrar el sistema de *Cloud Storage* amb els serveis corporatius, LDAP i servei d'autenticació unificada, per a l'aprovisionament d'usuaris i per a la delegació de l'autenticació, respectivament.

5.1. Integració sistema emmagatzemament secundari

La solució més adient, segons les conclusions extretes anteriorment, manca d'un requisit: l'escal.labilitat del sistema. Per tal de resoldre aquest inconvenient, i cobrir completament les necessitats de la corporació, s'ha decidit implementar una solució híbrida, és a dir, unir la solució *OwnCloud*, implementada en la infraestructura pròpia de la corporació, amb dos emmagatzemament finals, un de principal de caràcter privat i ubicat a la pròpia infraestructura i un de secundari, allotjat al servei de *Cloud Computing d'Amazon AWS* [47] - *Amazon S3*.
L'emmagatzemament privat i primari, es centrarà en emmagatzemar aquelles dades que es considerin de caràcter privat i/o sensible, com documents interns i estratègics de la companyia, llistat de clients, proveïdors i personal, documents amb informació sobre nòmines, compres i ventes, etc.. Aquest tipus de dades són considerades de vital i extrema importància per qualsevol companyia, pel que requereixen ser emmagatzemades amb les majors garanties de seguretat, confidencialitat, integritat i disponibilitat. Per aquest motiu, emmagatzemar-les a les pròpies dependències de la companyia, gestionades i controlades en tot moment pel personal qualificat d'aquesta, pot ser la solució més adient.
Pel que respecta a l'emmagatzemament secundari, es pretén que aquest doni solució a les carències que la pròpia companyia té en matèria de capacitat i escal.labilitat dels seus sistemes d'emmagatzemament actuals. D'aquesta forma, els usuaris podran emmagatzemar aquells documents o fitxers que no siguin de naturalesa privada, com poden ser documents estàndards, documents a compartir entre usuaris, imatges, vídeos, MP3, entre altres, disposant així d'una gran capacitat per emmagatzemar tot tipus de dades sense afectar l'emmagatzemament principal, el qual contindrà les dades realment importants de la companyia.
D'aquesta forma, la companyia gaudirà d'una sèrie d'avantatges com:

- Major control de la infraestructura, degut a que el sistema encarregat de donar accés als usuaris serà gestionat íntegrament pel personal de TI de la companyia.
- Reducció de costos d'emmagatzematge, tant a nivell de inversió inicial en infraestructura d'emmagatzematge final com en l'adquisició de llicències d'usuaris per a solucions privades.
- Escal.labilitat il·limitada i possibilitat d'integració amb altres productes d'*Amazon*.
- Possibilitat de migració de les dades cap a la infraestructura pròpia en qualsevol moment.

5.1.1. Que és Amazon S3?

Amazon Web Services (AWS)[45] proporciona serveis de computació i d'emmagatzemament sota demanda, d'alta escal.labilitat i elasticitat, per a una tot un ventall de possibilitats de negoci que van des de serveis de servidor, emmagatzemament, base de dades i infinitat de serveis d'aplicació a través d'Internet. Tots aquest serveis s'ofereixen des de diverses localitzacions, on *Amazon* disposa dels seus *Data-Center*s que treballen conjuntament i de forma distribuïda per donar serveis a més de 190 països.

Pel que respecta a l'emmagatzemament *Cloud*, *Amazon* dins de la seva cartera de serveis ofereix el que anomenen *Amazon S3* (*Amazon Simple Storage Service*)[48]. Aquest tipus d'emmagatzemament, també conegut com emmagatzemament com a servei (*Storage as a Service - SaaS)* [47], no és més que un emmagatzemament d'objectes al núvol, segur i amb una alta

escal.labilitat, gestionat a través d'una interfície web senzilla accessible per mitjà de *Web Services* per emmagatzemar i recuperar qualsevol tipus de dades des de qualsevol ubicació d'Internet. Aquesta modalitat d'emmagatzemament que ofereix *Amazon*, és de pagament per ús, és a dir, pagament per la quantitat de dades (GB) emmagatzemades.

5.1.2. Per què Amazon S3?

Amazon S3 és possiblement un dels sistemes d'emmagatzemament més transparents, més segurs, més versàtils i amb major capacitat d'emmagatzemament de totes les solucions existents al mercat. Entre les seves principals característiques destaquen [48]:

- Alta disponibilitat de les dades de fins a 99,99%.
- Seguretat en les comunicacions, ja que les dades que es transfereixen són xifrades mitjançant el protocol SSL, i un cop emmagatzemades poden ser xifrades de forma automàtica, escollint diferents tipus de xifrat.
- Il.limitada escal.labilitat, ja que no existeix cap tipus de restricció en la capacitat màxima que es pot emmagatzemar.
- Alt rendiment gràcies a càrrega de dades de forma distribuïda en diverses parts per tal de maximitzar el rendiment i la agilitat de la xarxa de comunicacions, minimitzant la latència d'aquesta.
- Baix cost, gràcies al pagament per quantitat de dades emmagatzemades, sense limitació ni restriccions de càrrega o descàrrega.
- Integració amb altres serveis de *Amazon AWS* com *Amazon Glacier* (còpies de seguretat), *Amazon CrossRegion Replication*, etc..

5.1.3. Anàlisi d'Amazon S3

A continuació farem un breu anàlisi de les funcionalitats i dels requisits tècnics, descrits en els objectius d'aquest projecte, en referència a l'inclusió de l'emmagatzemament secundari dins del sistema *OwnCloud*. En aquest apartat no s'analitzaran tots els punts en concret, sinó que es donarà una valoració global ja que moltes d'aquests depenen exclusivament del propi sistema *OwnCloud*, ja analitzat anteriorment.

5.1.3.1. Funcionalitats bàsiques

OwnCloud incorpora un mòdul específic encarregat de gestionar l'emmagatzematge secundari. Aquest realitza un muntatge de l'objecte d'emmagatzemament en qüestió, on per cada usuari crea un directori per sota aquest i el qual es muntat sobre cada compte d'usuari. Els usuaris veuen aquest directori com un directori més, sota l'arrel de directoris del compte, amb un nom específic ("*AmazonS3Bucket*").
La còpia de fitxers es realitza de la mateixa forma que amb qualsevol altre directori. Aquest directori és sincronitzat com un directori més de l'usuari, i les comparticions, tant dels fitxers com dels directoris existents, poden ser compartits com qualsevol altre, heretant totes les funcionalitats ja descrites.
OwnCloud manté la política de *backups* descrita anteriorment, com si d'un directori local es tractés, pel que es poden recuperar tots els fitxers esborrats fins a 30 dies i en diferents versions.

Amazon S3 ofereix espai il.limitat sense cap tipus de limitació. El pagament es realitza per quantitat de dades emmagatzemades en GB. El cost de cada GB emmagatzemat és de 0.0125€.
Si fem un càlcul aproximat sobre uns 5TB d'ocupació, el cost mensual d'aquest emmagatzemament ascendeix a 62,5€, i per tant, uns 750€ anuals. Cost més que assumible per a la corporació.

5.1.3.2. Requeriments tècnics de seguretat

Aquest emmagatzemament secundari està delegat al serveis d'*Amazon AWS [47]*, i per tant, aquest serà l'encarregat de complir amb la regulació vigent. Concretament, *Amazon AWS*, així

com tots els serveis que ofereix, compleix amb els estàndards de privacitat i protecció de dades segons les certificacions següents [50]:

- *EU-U.S.Safe Harbor and Swiss-U.S. Safe Harbor.*

A diferència de la resta de emmagatzemaments al núvol, *Amazon AWS* permet establir la ubicació física de les dades, és a dir, permet escollir en quin *Data-Center* s'ubicaran les dades. Aquests poden estar en països europeus com Irlanda, Alemanya, etc.. En el nostre cas, s'ha establert que les dades seran emmagatzemades en el *Data-Center* ubicat a Irlanda.

Les connexions entre el sistema *OwnCloud* i *Amazon S3* sempre són realitzades sota canals segurs de comunicació HTTPS, concretament utilitzant els protocols SSLv3 i/o TLSv1.0. *Amazon S3* no es compatible amb versions anteriors d'aquests protocols.

Amazon AWS permet dues opcions pel que a la protecció de dades es refereix. Permet el xifrat 'server-side' on les dades són xifrades pel propi sistema, o bé, xifrat 'client-side', on les dades són xifrades per part del sistema que les manega (origen). En aquest cas, s'ha decidit utilitzar el xifratge des del costat del client. D'aquesta forma, les claus de xifratge s'emmagatzemaran en els servidors propis de la companyia.

Per tal de poder connectar amb l'emmagatzemament *Amazon S3* es requereix d'unes credencials d'accés al sistema. *Amazon AWS* utilitza un sistema d'autenticació mitjançant una clau d'accés (*Access Key ID*) i una contrasenya (*Secret Access Key*). Aquestes poden ser descarregades des de la consola d'administració, tal i com es mostra en l'annex a aquesta memòria.

5.1.4. Creació de l'emmagatzematge secundari - Amazon S3

Per tal d'implementar l'emmagatzemament secundari, és necessari crear un objecte "*bucket*"[51] dins d'*Amazon Storage S3*. Per crear aquest servei, dins la consola de gestió en l'apartat d' "Storage & Content Delivery", cliquem sobre S3, i ens apareix la opció de crear un nou "*Bucket*". Si accedim i cliquem sobre el botó de crear "bucket", aquest ens demana donar-li un nom i escollir en quina regió volem crear-lo ***[veure Fig.11]***. En el nostre cas, s'ha decidit crear-lo en la regió *Ireland*, per tal de que les nostres dades estiguin en territori europeu i per tant, es regeixin per les lleis de la comunitat europea.

El nom escollit finalment és: *uoc_cloudstorage*.

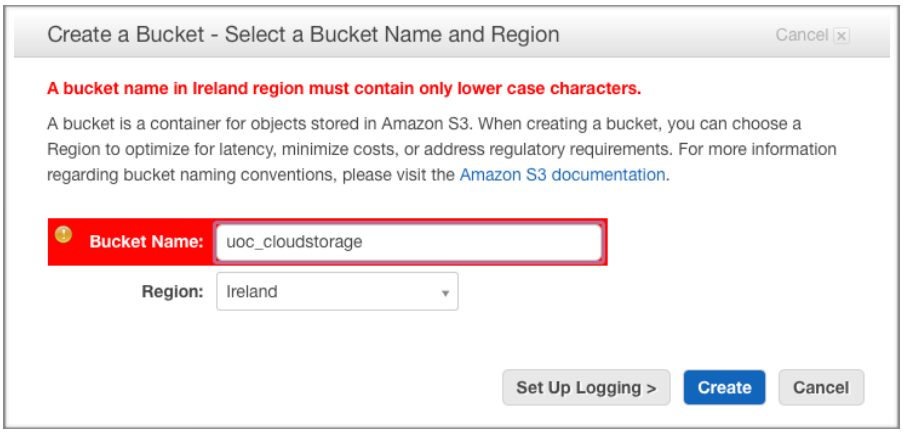

Fig. 11 - Creació del bucket, emmagatzemament S3.

Una vegada creat, aquest ens retorna a la plana de configuració del "*Bucket*" i ens mostra el llistat dels que ja tenim creats. Si cliquem sobre les propietats ***[veure Fig.12]***, podem modificar els valors d'aquestes, com per exemple, els permisos sobre l'emmagatzemament, el nivell de monitorització que volem aplicar-li, la gestió dels events, entre una sèrie d'altres accions. En

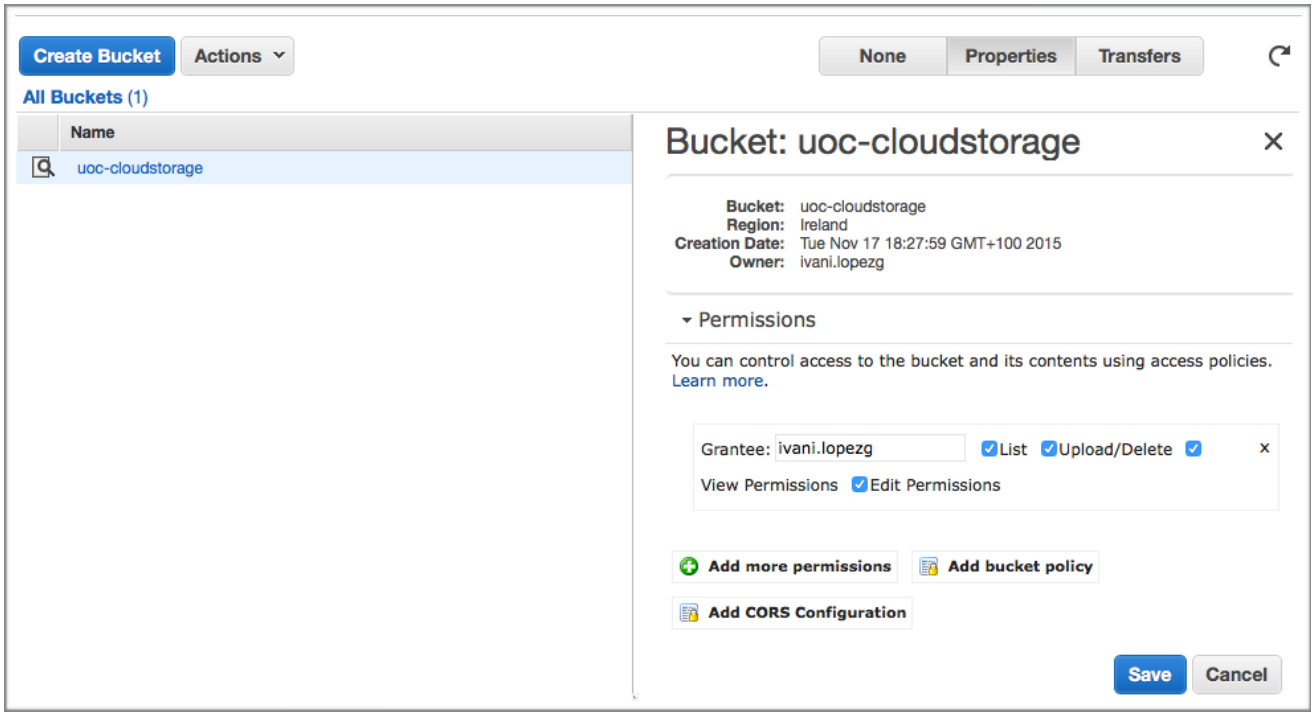

Fig. 12 - Propietats del *bucket* creat per a l'emmagatzemament extern.

aquest cas, tan sols s'ha comprovat que el sistema de fitxers del "*bucket*" pot ser modificat pels serveis que hi accedeixin.

Fig. 13 - Mòdul OwnCloud per l'emmagatzemament secundari extern.

5.1.5. Configuració de l'emmagatzemament extern al servidor OwnCloud

Per tal de poder configurar l'emmagatzemament secundari "Bucket S3" creat, es requereix habilitar l'aplicació interna del servidor *OwnCloud* que s'encarregarà de gestionar-lo, anomenat *"External storage support"* ***[veure Fig.13]***. El procediment d'habilitar el mòdul s'ha descrit en l'Annex a aquest document, pel què obviarem aquest pas i continuarem amb la configuració.

Un cop habilitat, sota la plana d'administració, es mostra el mòdul habilitat i les opcions de configuració disponibles. Del desplegable, seleccionem *"External Storage"* com a *"Amazon S3"* i ens apareix un formulari ***[veure Fig.14].*** Les dades de configuració a emplenar són:

- ***Bucket Name***: uoc-cloudstorage
- ***Hostname***: en el cas d'utilitzar un Virtual Host, hauríem d'afegir el nom del host. No s'utilitzarà.

- ***Port***: el port pel qual accediríem al Virtual Host. No s'utilitzarà.
- ***Region***: Ireland.
- ***Enable SSL / Enable Path SSL***: si volem que les comunicacions siguin xifrades mitjançant SSL Layers.
- ***Acces Key***: la clau d'accés obtinguda anteriorment.
- ***Secret Key***: la contrasenya d'aquesta clau d'accés.

Després d'afegir la configuració correcta, es pot comprovar que aquest realitza la connexió de forma satisfactòria ***[veure Fig.14]***. En conseqüència, s'afegeix al fitxer de configuració del sistema *OwnCloud*, la configuració relativa al sistema d'emmagatzemament secundari *Amazon S3*. Aquest, a partir d'ara, podrà ser visible per a tots els usuaris com un directori més dins la seva estructura de directoris. L'administrador té la potestat de poder escollir quins usuaris o grups tindran accés a aquest emmagatzemament addicional, tan sols afegint el nom d'usuari o grup en el bloc de text destinat a tal finalitat.

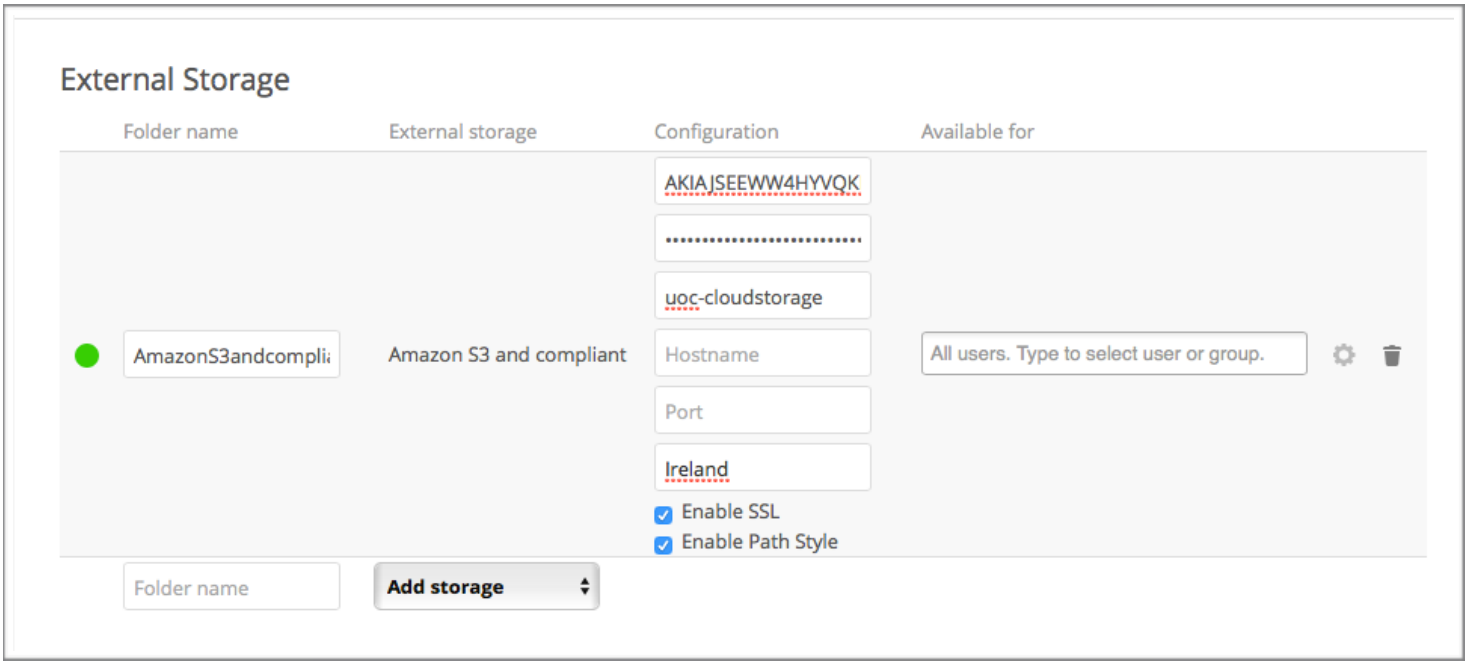

Fig. 14 - Configuració realitzada per connectar a l'emmagatzemament extern "bucket - Amazon S3" creat.

Tal i com es pot veure a continuació, aquesta mòdul ha modificat el nostre fitxer de configuració, afegint la configuració corresponent a l'emmagatzemament extern:

```
'objectstore' => array(
  'class' => 'OCA\ObjectStore\S3',
      'arguments' => array(
        'key' => 'AKI******BQ4A',
        'secret' => 'ZYUg*********0JzC8',
        'bucket' => 'uoc-cloudstorage',
      ),
),
```

5.2. Integració servei de directori LDAP

En aquest apartat es pretén mostrar, de forma resumida, com la solució privada *OwnCloud* s'integra amb els dos serveis interns de la corporació. Concretament, es mostrarà la integració, mitjançant la API corresponent, amb el servei de directori actiu corporatiu LDAP, per tal d'aprovisionar els usuaris dins del sistema de *Cloud Storage*.

Moltes corporacions utilitzen un servidor de directori actiu per a l'administració centralitzada dels usuaris. En el nostre cas, aquest directori actiu és un directori lliure i de codi obert, *OpenLDAP* (*Open Lightweight Directory Access Protocol*) *[52]*. *OpenLDAP* és una base de dades dissenyada per emmagatzemar objectes de forma centralitzada en un únic repositori. Aquest facilita l'administració, creació, modificació i eliminació de comptes d'usuaris, i a més a més realitzar la funció de servidor d'autenticació i autorització per a aplicacions.

5.2.1. Aprovisionament usuaris

OwnCloud incorpora una aplicació o mòdul per tal d'integrar-se amb servidors LDAP amb la finalitat d'importar usuaris i realitzar l'autenticació a través d'aquests. D'aquesta forma, la gestió dels usuaris i grups és centralitzada i delegada completament al servidor de directori, sense necessitat de crear usuaris ni administrar-los des de la consola *d'OwnCloud*. Aquesta delegació no obliga necessàriament que els usuaris només puguin ser creats des del costat del servidor *OpenLDAP*, ja que permet crear usuaris locals.

Aquest mòdul s'anomena "*LDAP user and group backend*" ***[veure Fig.15]*** i el trobem dins el llistat de mòduls sota suport *d'OwnCloud*. Abans de procedir amb la configuració, aquest ha de ser habilitat. El procediment d'habilitar el mòdul s'ha descrit en l'Annex a aquest document, pel què obviarem aquest pas i continuarem amb la configuració.

Fig. 15 - Mòdul "LDAP user and group backend".

5.2.2. Configuració integració LDAP

Un cop habilitat, aquest és visible i configurable des de la consola central d'administració. Es poden configurar tants servidors com es requereixi. Entre les dades del servidor LDAP requerides tenim:

- ***Servidor***: IP o domini del servidor LDAP al qual ens connectarem.
- ***Port***: port a través del qual es realitza la connexió cap al servidor LDAP. Les connexions es poden fer a través de dos ports, el port 389 i el 636. Si es realitza la connexió a través del 389 les dades que es transmeten no estaran protegides, mentre que si la connexió es realitza a través de port TCP 636 (LDAPS), les dades estaran protegides i xifrades sota el protocol SSL. Es recomana, sempre utilitzar connexions protegides mitjançant LDAPS.
- ***Usuari***: usuari del directori actiu amb el que accedirem per tal de llegir i importar tots els usuaris. El format d'aquest usuari s'ha de correspondre amb l'objecte LDAP al qual es fa referència.
- ***Contrasenya***: contrasenya de l'usuari en qüestió.
- ***Base DN***: cadena o arrel principal del servidor LDAP on es troben els usuaris a importar. Normalment, aquesta cadena es configura a partir d'una unitat organitzativa (OU), en la qual es troben els usuaris a importar.

En la següent captura de pantalla es pot veure la plana principal de configuració del mòdul d'integració amb LDAP ***[veure. Fig.16]*** :

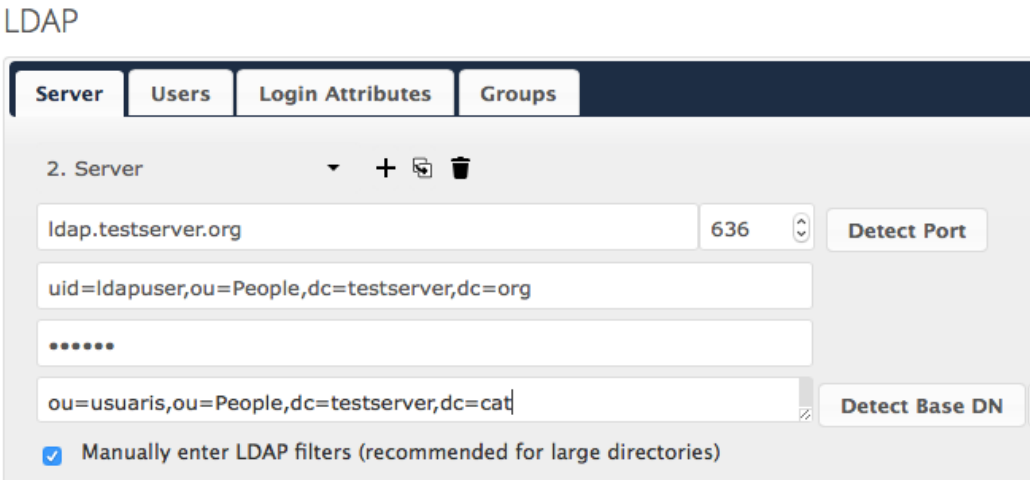

Fig. 16 - Configuració paràmetres LDAP. Mòdul "LDAP user and group backend".

Posteriorment, s'han de configurar els filtres que ens determinaran quins tipus d'objectes de l'LDAP volem importar. En la pestanya "USERS" es configuren els objectes, normalment tipus "PERSON", "USER" o "INETORGPERSON", que han de cercar-se al directori ***[veure. Fig.17]***.
En la següent pestanya, configurem l'atribut dels usuaris ha utilitzar per a realitzar l'autenticació al sistema. Normalment, l'autenticació es realitza amb l'atribut "UID" (identificador d'usuari) o bé l'atribut "MAIL" (adreça de correu de l'usuari) ***[veure. Fig.17]***.

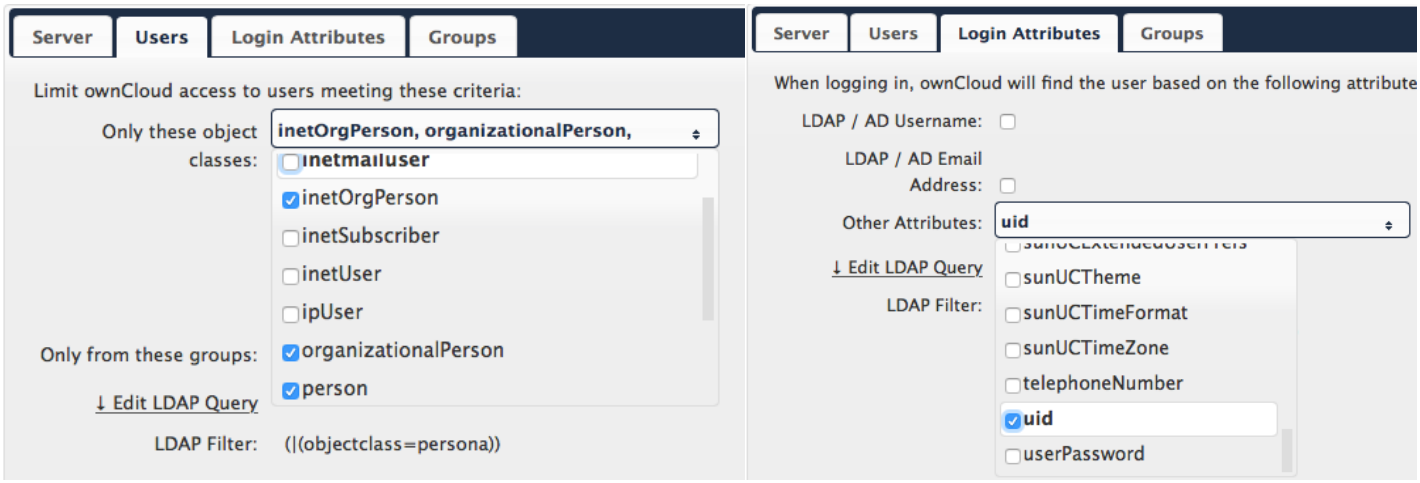

Fig. 17 - Configuració filtres LDAP. Mòdul "LDAP user and group backend".

Finalment, l'última pestanya s'utilitza per seleccionar i importar els grups del directori que es vulguin afegir al servidor *OwnCloud*. En aquest cas, les dades a seleccionar variaran molt en funció de cada un dels directoris, és a dir, si tenen grups basats en unitat organitzatives (OU), basat ens grups d'usuari, etc..

Si la configuració ha donat com a resultat una connexió satisfactòria, els usuaris i les seves corresponents credencials d'accés s'hauran importat sobre el servidor *OwnCloud* i per tant, tot usuari existent podrà autenticar-se al sistema.

5.3. Integració i delegació del sistema d'autenticació - SSO

En aquest apartat, un cop els usuaris s'han importat correctament, es mostra el procediment a seguir per tal d'integrar i securitzar el sistema mitjançant el servei d'autenticació única corporatiu, *Single Sign-On* (SSO). D'aquesta forma l'autenticació al sistema per part dels usuaris quedarà delegada al servei d'autenticació corporatiu, qui gestionarà les sessions i els privilegis d'accés.

5.3.1. Single Sign On / CAS Server

Un sistema Single Sing-On (SSO) permet als usuaris autenticar-se una única vegada i mantenir la sessió establerta amb èxit per a la resta d'aplicacions que facin ús del SSO. Aquests sistemes SSO realitzen les autenticacions, normalment mitjançant, usuari i contrasenya, encara que també permet utilitzar altres mètodes com els certificats digitals, identificadors biomètrics, etc..

Per l'altra banda, CAS (*Central Authentication Service*) o també conegut com a CAS-Jasig *[53]*, podem dir que és una aplicació web que ens permet implementar el sistema d'autenticació unificada SSO. El seu funcionament és bàsic, quan un usuari es connecta a una de les aplicacions integrades, el sistema el re-dirigeix al servidor CAS, el qual comprova si l'usuari esta autenticat. Si no ho esta, li retorna el valor *Null* i el re-envia cap a la plana de *Login*. Si ja esta autenticat per CAS, aquest retorna un valor amb el que el sistema sabrà que l'usuari té accés i per tant valida l'autenticació. CAS, s'encarrega única i exclusivament de l'autenticació, és a dir, de comprovar si l'usuari i contrasenya són correctes. L'autorització vindrà determinada pel propi sistema origen.

A continuació es mostra com *OwnCloud* s'integra amb un servidor *CAS-Jasig*, servidor de SSO utilitzat actualment per la corporació. A diferència del mòdul d'LDAP, el mòdul d'integració no es troba ja instal.lat sobre el sistema i es requereix instal.lar-lo des de la pròpia web *d'OwnCloud*, concretament des del repositori d'aplicacions. El procediment d'instal.lació s'ha descrit en l'Annex a aquest document, pel què obviarem aquest pas i continuarem amb la configuració.

El mòdul encarregat de gestionar la connexió amb el servidor CAS es diu *"CAS Authentication Backend"*, i un cop habilitat el trobarem sota la mateixa plana principal de la consola d'administració *d'OwnCloud*.

5.3.2. Configuració integració CAS-Jasig

Per configurar i delegar l'autenticació mitjançant el servidor SSO CAS-Jasig, primer s'han de conèixer els paràmetres del servidor, nom DNS o IP el servidor, port per on es presenta (normalment i per seguretat, sempre sota el protocol HTTPS) i el context on es troba dins de servidor web on es allotjat. Aquests paràmetres dins el mòdul CAS, són els següents:

- ***CAS Server Version***: actualment la versió més recent es la versió 3.X. Aquest mòdul només permet configurar la versió 2.0, versió completament compatible amb l'actual.
- ***Cas Server Hostname***: nom del servidor on es troba el servidor CAS. Aquest pot ser configurat per nom DNS o bé per IP, segons convingui.
- ***CAS Server Port***: port per on esta escoltant el servidor CAS. En la majoria de casos, aquest escolta pel port per defecte pel protocol HTTP, el 443. Segons la configuració del servidor destí, aquest pot variar.
- ***Cas Server Path:*** el servidor CAS, normalment, es troba sota context dins del servidor web on és hostatjat. Aquest sol implementar-se sota el context "/cas" en la majoria d'instal.lacions.
- ***Certification file path:*** quan en el costat del servidor web hi ha un certificat que requereix ser reconegut pel sistema s'ha d'incloure el *path* d'on es troba. En la majoria de casos, aquest no requereix ser validat, pel que aquest apartat es pot considerar com a opcional.

- ***Disable CAS Logout:*** quan es realitza un *logout* de l'aplicació *OwnCloud*, aquest pot ser vàlid per només el sistema actual o bé realitzar un *logout* de la pròpia autenticació al servidor CAS. Aquesta elecció es deixa com a opcional segons criteri de cada corporació.

A continuació és pot veure un exemple de com quedaria aquesta configuració inicial del mòdul de *"CAS Authentication backend"* ***[veure. Fig.18]***.

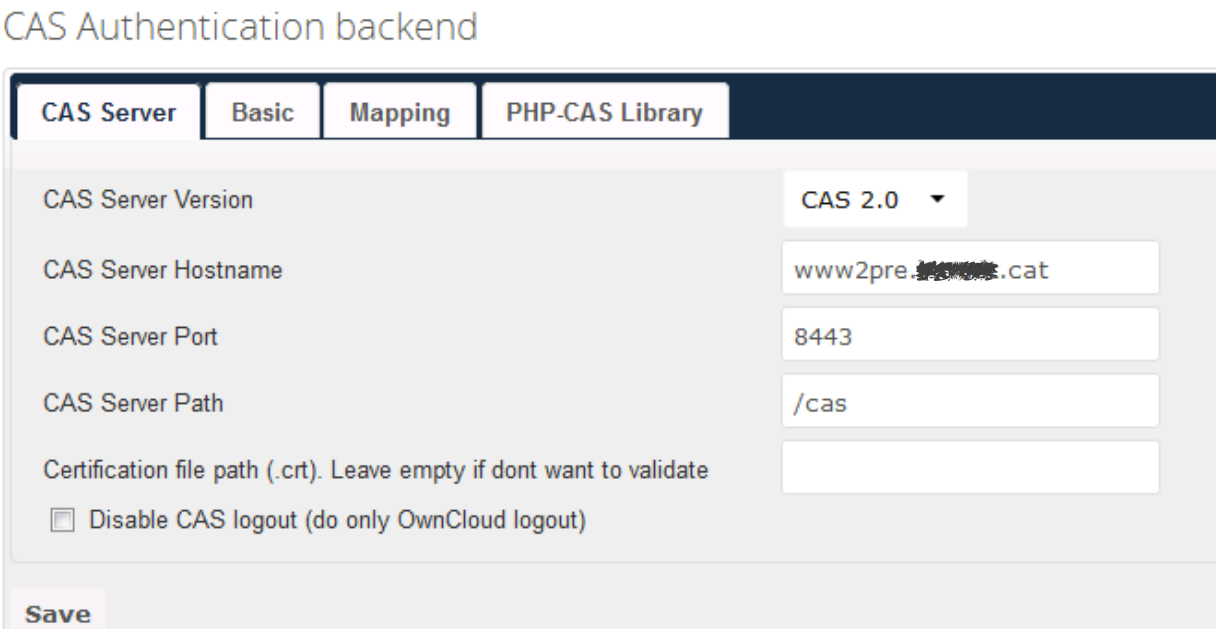

Fig. 18 - Configuració dels paràmetres d'accés al servidor CAS-Jasig.

Un cop realitzada la configuració bàsica, existeixen altres paràmetres de configuració en la pestanya "BASIC", tots ells opcionals segons criteri de l'administrador ***[veure. Fig.19]***.

- *Force user login using CAS?*: paràmetre per forçar l'autenticació mitjançant el servidor SSO.
- *Autocreate user after CAS login?*: paràmetre que permet crear l'usuari dins el sistema (de forma local) si aquest encara no existeix.
- *Link CAS authentication with LDAP users and groups backend:* si prèviament s'ha configurat l'aprovisionament d'usuaris via LDAP, l'activació d'aquesta opció obliga que els usuaris estiguin registrats sobre el directori, no permeten que s'autentiquin usuaris no vinculats.
- *Update user data after login?:* aquesta opció permet actualitzar la informació de l'usuari en local després d'autenticar-se. Quan s'ha configurat l'aprovisionament mitjançant el servidor LDAP, aquest paràmetre no té validesa, ja que la informació del directori es la que preval.

Existeixen dos pestanyes més, però a diferencia de les altres, aquestes són merament informatives, i només caldria modificar-les en cas de tenir un servidor CAS molt específic.

Amb aquests paràmetres, si les connexions entre servidors són satisfactòries, és a dir, el possible *Firewall* o IDS permeten aquestes, l'autenticació queda delegada al servidor CAS, el qual autoritzaria l'accés dels usuaris al sistema si les credencials són correctes i es corresponen amb les credencials existents en el directori corporatiu LDAP.

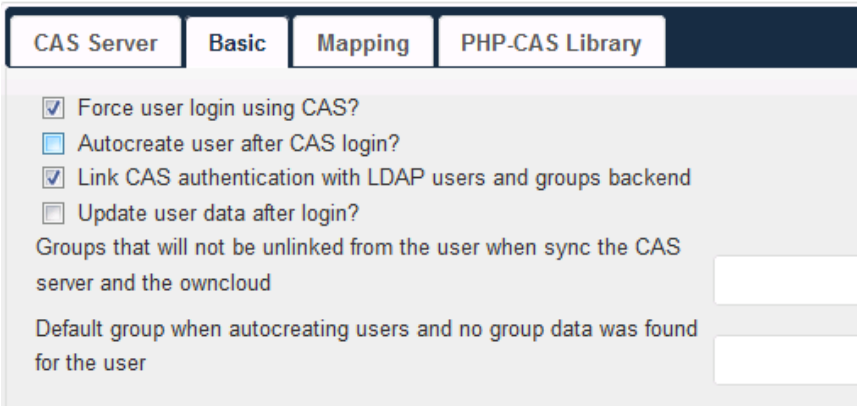

Fig. 19 - Configuració paràmetres opcionals mòdul CAS-Jasig.

5.3.3. Esquema de la infraestructura resultant

En la següent imatge ***[veure Fig.20]*** es mostra l'esquema de la infraestructura resultant després d'afegir l'emmagatzemament secundari, així com la integració del sistema d'autenticació centralitzat i el servidor LDAP per a l'aprovisionament dels usuaris.

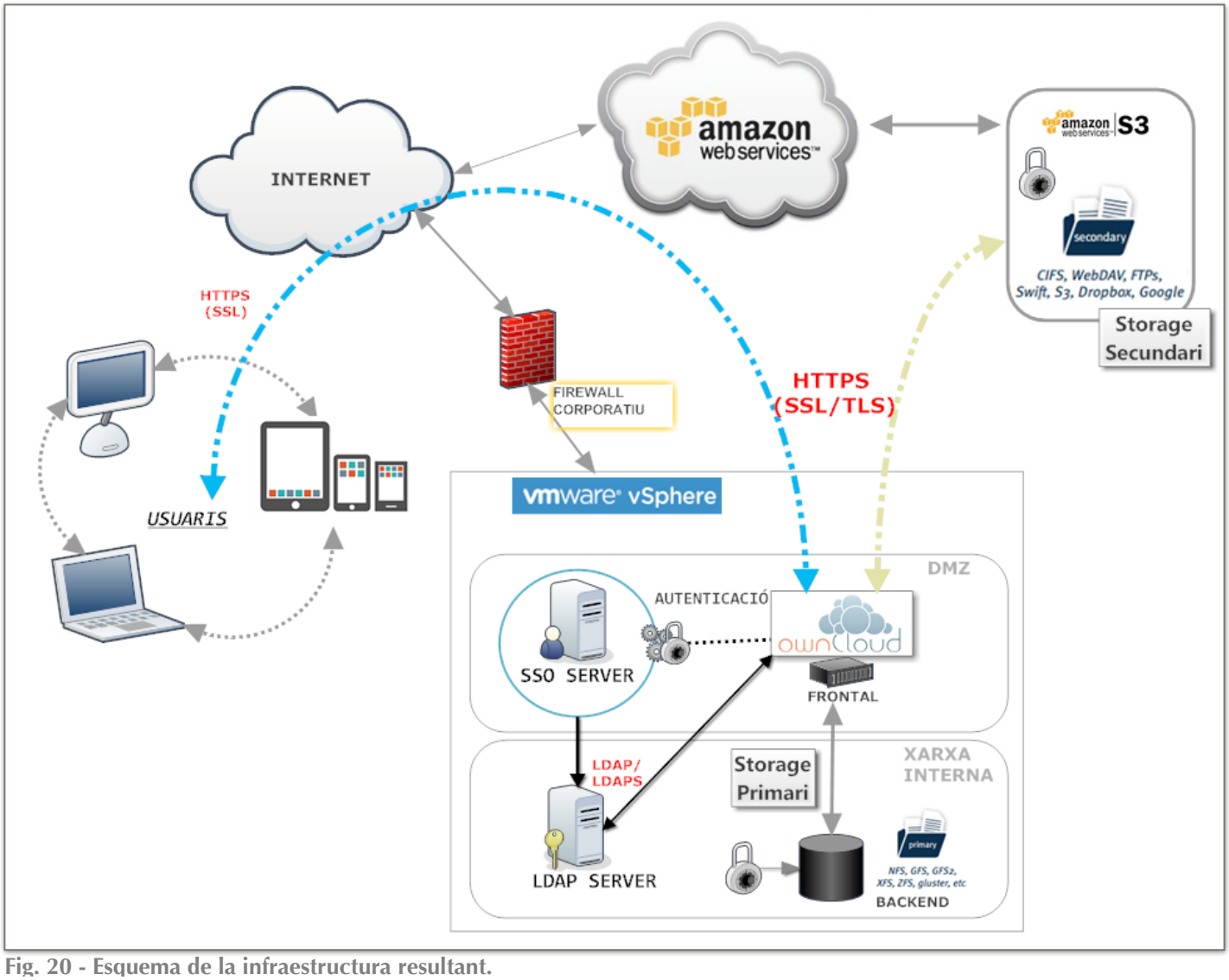

Fig. 20 - Esquema de la infraestructura resultant.

6. Conclusions

Un cop realitzat l'anàlisi de les 5 solucions, una de les primeres conclusions que podem extreure és que totes elles presenten una sèrie de funcionalitats molt pròximes i similars entre elles, que compleixen amb els requisits bàsics de còpia de fitxers, *backup*, sincronització i compartició de fitxers entre usuaris amb diferències mínimes en aquest últim punt, on cadascuna de les solucions aporta la seva pròpia visió de la compartició. Per contra, tant *Dropbox* com *SugarSync* presenten deficiències de seguretat en la generació d'enllaços de compartició que cal tenir en compte.

Totes les solucions presenten una consola de gestió centralitzada que compleix amb els requisits, a excepció de la solució *SugarSync* que presenta una consola molt bàsica i amb reduïdes funcionalitats i monitorització del sistema. *Box*, en canvi, presenta una consola molt potent i versàtil, al igual que *OwnCloud* que recolzada per la possibilitat d'instal.lar infinitat de mòduls, permet tenir un control molt exhaustiu del sistema, l'activitat dels usuaris, les comparticions i a més, tenir per darrera una constant evolució i noves característiques gràcies a la pròpia comunitat.

Pel que respecta a la seguretat en les transmissions de dades entre clients i servidor, totes elles treballen sota protocols segurs de comunicació, essent HTTPS sota TLS el protocol utilitzat per unanimitat. Analitzant el xifrat de les dades un cop les dades són finalment emmagatzemades, totes elles realitzen aquest xifrat en base a algoritmes AES-256 que garanteixen la completa integritat i confidencialitat d'aquestes. Ara bé, cal destacar els mètodes utilitzats tant per *OwnCloud* com *SpiderOak* que basen el seus mecanismes en xifrar els fitxer amb funcions derivades de les pròpies contrasenyes d'usuari, garantint que les dades són únicament desxifrables pel propi usuari propietari.

Seguint amb la protecció de les dades, en l'apartat corresponent al tractament de la privacitat, és cert que totes les solucions públiques, posseïxen les certificacions corresponents, però totes elles treballen amb *Data-Centers* ubicats a territori americà i per tant, aquestes estan subjectes a la legislació vigent americana. Si a aquest fet afegim que, a excepció de *SpiderOak*, totes elles declaren que podran revelar informació d'usuaris a terceres parts, la confidencialitat i privacitat de les dades de la companyia podria veure's afectada.

En l'aspecte possiblement més important, l'econòmic, existeixen dues solucions que es desmarquen de la resta pel seu elevat cost d'implantació, com són *SugarSync* i *Box*. Per una altra banda, les dues solucions públiques més econòmiques, no especifiquen quin tipus de suport tècnic ofereixen, mesura imprescindible per a la implantació de qualsevol solució. *OwnCloud*, és la opció més econòmica amb diferència, però per contra, manca de l'escal.labilitat que es demana.

Finalment, un dels factors claus a l'hora de prendre una decisió final és la integració amb els serveis corporatius. Tres de les solucions, *Dropbox*, *SugarSync* i *SpiderOak*, no compleixen els requisits ja que requereixen d'aplicacions de tercers per a realitzar la integració amb SSO, fet que complicaria i encariria el cost d'implantació.

Si tenim en compte tots aquests factors, però sobretot, els factors claus de la seguretat en el tractament de les dades, l'econòmic i la integració, *OwnCloud i Box* són les opcions més adients per a aquesta corporació. Les dues solucions compleixen gairebé amb el 100% dels requisits, però existeix una gran diferència en l'aspecte econòmic. La implantació de la solució *Box* té un cost molt elevat, exactament el doble de despesa que implantar la solució *OwnCloud*.

És cert que *OwnCloud* no cobreix totes les necessitats, concretament, no cobreix el requisit de l'escal.labilitat per al futur creixement, però amb la solució addicional implementada *Amazon* S3, aquesta queda coberta. En l'aspecte econòmic, aquest servei extra només incrementa en uns

750€ anuals el preu final, pel que es considera que és un preu assumible per part de la companyia.
També és cert que implantar *OwnCloud* comporta un sobre-esforç per part dels tècnics de TI, però a favor, podem dir que amb aquesta solució s'obté un major control i seguretat de les dades, minimitzant les possibles pèrdues i fuites d'informació sensible. La diferència econòmica pot compensar aquest sobre-esforç.

Finalment, un cop desplegada la prova pilot amb l'emmagatzemament secundari d'*Amazon S3* afegit, la integració amb el directori corporatiu i la integració amb el servei d'autenticació unificada, juntament amb un joc de proves exhaustiu, una comprovació de la versatilitat de la consola de gestió, una verificació del funcionament dels mecanismes de seguretat incorporats, entre d'altres accions realitzades, podem confirmar que la solució compleix i garanteix les necessitats i requisits establerts en aquest projecte.

La integració i el cost econòmic d'implantació final, així com la viabilitat tècnica del projecte, com ja s'ha comentat, ha sigut factor clau i determinant per donar un veredicte final. En el nostre cas, *OwnCloud* és la solució més adient.

Índex d'il.lustracions

Índex de taules

Bibliografia

[1] - International Organization Standards - http://www.iso.org/iso/home.html
Últim accés: 24 Desembre de 2015
[2] - Perrin, Chad. "The CIA Triad". http://www.techrepublic.com/blog/it-security/the-cia-triad/
Últim accés: 05 Novembre 2015
[3] - Directiva 95/46/CE del Parlamento Europeo y del consejo. "Diario Oficial de las Comunidades Europeas"
http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES
Últim accés: 10 Novembre 2015.
[4] - U.S.Department of Commerce - Welcome to The U.S.-EU & U.S.-Swiss Safe Harbor Frameworks
http://export.gov/safeharbor/swiss/index.asp
Últim accés: 11 Novembre 2015
[5] - Wikipedia - Two-factor authentication https://en.wikipedia.org/wiki/Two-factor_authentication
Últim accés: 15 Desembre 2015
[6] - Wikipedia - Time-based One-time Password Algorithm
https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm
Últim accés: 15 Desembre de 2015
[7] - Wikipedia: Criptografia asimètrica - https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asimétrica

Últim accés: 27 Desembre 2015
[8] - Wikipedia: Criptografia simètrica - https://es.wikipedia.org/wiki/Criptograf%C3%ADa_simétrica
Últim accés: 27 Desembre 2015
[9] - Secure Hash Algorithm - https://en.wikipedia.org/wiki/Secure_Hash_Algorithm
Últim accés: 30 Desembre 2015
[10] - Wikipedia: AES, Advanced Encryption Standard - https://es.wikipedia.org/wiki/Advanced_Encryption_Standard
Últim accés: 27 Desembre 2015
[11] - NSA, National Security Agency - EUA. Cryptography standards. https://www.nsa.gov/ia/programs/suiteb_cryptography/
Últim accés: 27 Desembre 2015
[12] - NIST, «The NIST Definition of Cloud Computing,» Recommendations of the National Institute of Standards and Technology, no 800-145, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
Últim accés: 12 Novembre de 215
[13] - Dropbox news - Techcrunch - Dropbox Now Has More Than 400 Million Registered Users
http://techcrunch.com/2015/06/24/dropbox-hits-400-million-registered-users/
Últim accés: 15 de Novembre de 2015
[14] - Solució Cloud Storage Dropbox for Business - https://www.dropbox.com/business
Últim accés: 21 Desembre 2015
[15] - LDAP & SSO Integration - Dropbox - https://www.dropbox.com/business/trust/security/control-visibility
Últim accés: 21 Desembre 2015
[16] - Dropbox for Business Admin Console features - https://www.dropbox.com/business/tour/cloud-security-control
Últim accés: 21 Desembre 2015
[17] - Compliment de normes i estàndards - Dropbox for Business - https://www.dropbox.com/es/help/238
Últim accés: 21 Desembre 2015
[18] - Dropbox Amazon S3 store data - https://www.quora.com/Why-does-Dropbox-still-use-Amazon-S3-to-store-data-instead-of-building-its-own-data-center
Últim accés: 22 Desembre 2015
[19] - Two-steps verification in Dropbox - https://www.dropbox.com/es/help/363
Últim accés: 21 Desembre 2015
[20] - Perfect Forward Secrecy - https://en.wikipedia.org/wiki/Forward_secrecy
Últim accés 21 Desembre 2015
[21] - Encriptació fitxers en Dropbox - https://www.dropbox.com/help/27
Últim accés: 21 Desembre 2015
[22] - SugarSync for Business - https://www.sugarsync.com
Últim accés: 22 Desembre 2015
[23] - Modalitat pagament SugarSync for Business - https://www.sugarsync.com/business/index.html#customForm
Últim accés: 22 Desembre 2015
[24] - LDAP & SSO Integration partners - https://www.sugarsync.com/partners/
Últim accés: 22 Desembre 2015
[25] - Polítiques de privacitat i protecció de dades SugarSync for Business - https://www.sugarsync.com/privacy
Últim accés: 22 Desembre 2015
[26] - Comparativa entre Dropbox i SugarSync - http://www.groovypost.com/howto/reviews/sugarsync-vs-dropbox-alternative-you-never-asked-for/
Últim accés: 22 Desembre 2015
[27] - Box for Business - https://www.box.com/business/
Últim accés: 22 Desembre 2015
[28] - Box Enterprise Security: Collaboration - https://www.box.com/business/online-collaboration/
Últim accés: 22 Desembre 2015
[29] - Llistat de preus i capactitats Box Business & Enterprise - https://www.box.com/pricing/
Últim accés: 22 Desembre 2015
[30] - Box IT admin Controls: Admin Console https://www.box.com/business/it-admin-controls/
Últim accés: 22 Desembre 2015
[31] - Polítiques de privacitat i protecció de dades Box - https://www.box.com/legal/privacypolicy/
Últim accés: 22 Desembre 2015
[32] - TechWorld, Box to operate from Equinix data centres worldwide - http://www.techworld.com/news/big-data/box-deliver-cloud-collaboration-from-equinix-data-centres-worldwide-3410435/

Últim accés: 22 Desembre 2015
[33] - Box Enterprise Security: Data Center Security and Availability - https://www.box.com/business/enterprise-security/
Últim accés: 22 Desembre 2015
[34] - Box Enterprise Security: Control Access, Authentication and Authorization - https://www.box.com/business/enterprise-security/
Últim accés: 22 Desembre 2015
[35] - Box Enterprise Security: Box Enterprise Key Management - https://www.box.com/business/enterprise-key-management/
Últim accés: 22 Desembre 2015
[36] - Jon Brodkin. Box aims for NSA-resistant cloud security with customers holding the keys - http://arstechnica.com/information-technology/2013/09/box-aims-for-nsa-resistant-cloud-security-with-customers-holding-the-keys/
Últim accés: 22 Desembre 2015
[37] - SpiderOak Enterprise - https://spideroak.com/solutions/spideroak-enterprise
Últim accés: 23 Desembre 2015
[38] - SpiderOak Zero Knowledge - https://spideroak.com/features/zero-knowledge
Últim accés: 23 Desembre 2015
[39] - Integració de SpiderOak amb aplicacions de tercers - https://www.onelogin.com/connector/spideroak-single-sign-on
Últim accés: 23 Desembre 2015
[40] - Polítiques de privacitat i protecció de dades SpiderOak - https://spideroak.com/about/hipaa
Últim accés: 23 Desembre 2015
[41] - Localització data-center SpiderOak & equip tècnic - https://spideroak.com/about/team-&-leadership
Últim accés: 28 Desembre 2015
[42] - Privacy by Design - SpiderOak - https://spideroak.com/features/private-by-design
Últim accés: 23 Desembre 2015
[43] - Security & Access - SpiderOak - https://spideroak.com/manual/security--access
Últim accés: 23 Desembre 2015
[44] - Owncloud Home Page - https://owncloud.org
Últim accés: 25 Desembre 2015
[45] - Funció de derivació de claus - PBKDF2 (Password-Based Key Derivation Function 2) - https://en.wikipedia.org/wiki/PBKDF2
Últim accés: 29 Desembre 2015
[46] - OwnCloud Security and Encryption 2.0; A Technical Overview - https://owncloud.com/wp-content/uploads/2015/09/Whitepaper_ownCloud-Security-and-Encryption-Technical-Overview_ENG_151101.pdf
Últim accés: 29 Desembre 2015
[47] - Amazon Web Services AWS - https://aws.amazon.com/es/
Últim accés: 25 Desembre 2015
[48] - Amazon S3 - Amazon Simple Storage Service - https://aws.amazon.com/s3/
Últim accés: 25 Desembre 2015
[49] - SaaS - Software as a service - https://es.wikipedia.org/wiki/Software_como_servicio
Últim accés: 25 Desembre 2015
[50] - Polítiques de privacitat i protecció de dades Amazon Web Services - AWS - https://aws.amazon.com/privacy/
Últim accés: 25 Desembre 2015
[51] - Bucket, emmagatzemaments Amazon S3 - http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html
Últim accés: 30 Desembre 2015
[52] - *OpenLDAP (Open Lightweight Directory Access Protocol)* - http://www.openldap.org/project/
Últim accés: 10 Gener 2016
[53] - Cas-Jasig, Enterprise Single Sign-On - http://jasig.github.io/cas/4.1.x/index.html
Últim accés: 10 Gener 2016

[54] - Aaron Wheeler & Michael Winburn - Cloud Storage Security (A practical guide) - Ed. Elsevier
Format Llibre e-Pub. Últim accés: 26 Desembre 2015
[55] - Jesús Díaz Vico - Seguridad en servicios de Almacenamiento - Instituto Nacional de Ciberseguridad (INCIBE)

https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/estudio_seguridad_almacenamiento_nube
Últim accés: 21 Desembre 2015
[56] - Anthony T.Velte, Toby J.Velte, Robert Elsenpeter - Cloud Computing - A practical Approach
http://ftp.sustech.edu/cloud/Toby_Velte,_Anthony_Velte,_Robert_Elsenpeter_Cloud_Computing,_A_Practical_Approach__2009.pdf
Últim accés: 21 Desembre 2015
[57] - Ronald L.Krutz and Russel Dean Vines - Cloud Security (A comprenshive guide to secure cloud computing)
http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470589876.html
Últim accés: 21 Desembre 2015
[58] - Linda Xu, Miklos Sandorfi, Tanya Loughlin - Cloud Storage for Dummies. Hitachi Data Systems Edition
https://community.hds.com/servlet/JiveServlet/previewBody/1003762-102-1-275946/Cloud_Storage_for_Dummies.pdf
Últim accés: 21 Desembre 2015
[59] - Kan Yang, Siaouhua Jia, Security for Cloud Storage Systems. Springer
http://www.asecib.ase.ro/cc/carti/Security%20for%20Cloud%20Storage%20Systems%20[2013].pdf
Últim accés: 21 Desembre 2015
[60] - Fraunhofer Institute for secure information technology - SIT Technical reports - On the security of Cloud Storage Services - March 2012
https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf
Últim accés: 21 Desembre 2015
[61] - Gehana Booth, Andrew Socknacki, Anil Somayaji. Cloud Security: Attacks and current defenses
http://www.albany.edu/iasymposium/proceedings/2013/16-BoothSoknackiSomayaji.pdf
[62] - OwnCloud Architecture Overview - https://owncloud.com/owncloud-architecture-overview/
Últim accés: 25 Desembre 2015
[63] - OwnCloud 8.0 Server Administration Manual - https://doc.owncloud.org/server/8.0/admin_manual/
Últim accés: 27 Desembre 2015