

Memoria Final:

**Integración de solución de almacenamiento,
sincronización, compartición de ficheros y acceso a
aplicaciones web en la nube en el entorno empresarial.**

ÍNDICE DE CONTENIDO

ÍNDICE	2
ÍNDICE DE IMÁGENES	4
ÍNDICE DE TABLAS	4
1. INTRODUCCIÓN	5
1.1. Introducción y comentarios iniciales	5
1.2. Motivaciones	5
1.3. Objetivos	6
1.4. Estructura de la presente memoria	7
2. GESTIÓN DEL PROYECTO	8
2.1. Planificación inicial y cambios en la misma	8
2.2. Organización implicada	10
3. ANÁLISIS DE SITUACIÓN	11
3.1. Fundamentos para el trabajo colaborativo mediante aplicaciones web	11
3.2. Sistemas web conocidos para el trabajo colaborativo	11
3.2.1. DropBox	11
3.2.2. Google Apps	12
3.2.3. OwnCloud	12
3.3. Análisis de situación actual	13
3.3.1. Sistemas existentes involucrados en la integración	13
3.4. Definición de requerimientos	13
3.4.1. Requerimientos funcionales	13
3.4.2. Requerimientos no funcionales	14
4. DISEÑO DEL SISTEMA DE TRABAJO COLABORATIVO A INTEGRAR	19
4.1. Revisión de requerimientos	19
4.2. Proceso de planificación	20
4.3. Preparación de los sistemas	21
4.3.1. Adaptación de directorio de usuarios	21
4.3.2. Configuración de certificados digitales	23
4.3.3. Configuración de registros DNS	24
4.3.4. Configuración de sistema de correo electrónico	24
4.3.5. Adecuación de redes de comunicación	24
4.4. Visión esquemática global del sistema a integrar	26
5. IMPLANTACIÓN E INTEGRACIÓN DEL SISTEMA	30
5.1. Instalación y configuración de servidor dedicado	30
5.1.1. Instalación de OwnCloud en servidor dedicado	31
5.1.2. Configuración básica de OwnCloud en servidor dedicado	31
5.2. Integración de la solución con los sistemas existentes	33
5.2.1. Integración con el sistema de directorio de usuarios y de correo electrónico	33
5.2.2. Integración con la identidad digital de la empresa (certificados digitales)	36
5.3. Securitización del sistema de trabajo colaborativo	37
5.3.1. Securitización de accesos a nivel de red y de servicios	37
5.3.2. Securitización de datos	37
5.4. Configuraciones especiales	38
5.4.1. Adaptación de interfaz web	38
5.4.2. Adaptación de elementos de interacción con usuarios	40

6. PROCESO DE IMPLANTACIÓN E INTEGRACIÓN	42
7. PLAN DE PRUEBAS Y PILOTO INICIAL	46
8. DESPLIEGUE A USUARIOS	48
9. PLAN DE MANTENIMIENTO	49
10. ANÁLISIS ECONÓMICO: PRESUPUESTO Y ANÁLISIS DE COSTES	50
11. CONCLUSIONES	51
12. GLOSARIO	52
13. BIBLIOGRAFÍA	52

ÍNDICE DE IMÁGENES

<i>Imagen 1: Diagrama de Gantt</i>	9
<i>Imagen 2: Diagrama de infraestructura para acceso a Directorio de Usuarios</i>	22
<i>Imagen 3: Diagrama de actividad: acceso a Directorio de Usuarios</i>	22
<i>Imagen 4: Certificado Digital firmado por Verisign</i>	23
<i>Imagen 5: Esquema de nueva situación de redes de comunicación</i>	25
<i>Imagen 6: Esquema del sistema de accesos de usuarios a ClientBox</i>	26
<i>Imagen 7: Esquema del sistema de lectura de datos de usuarios desde ClientBox al ProxyLDAP</i>	27
<i>Imagen 8: Esquema del sistema de lectura de datos de usuarios desde el ProxyLDAP a OpenLDAP</i>	28
<i>Imagen 9: Esquema del sistema de envío de notificaciones por correo electrónico</i>	29
<i>Imagen 10: Configuración de VirtualHost de OwnCloud</i>	32
<i>Imagen 11: Configuración inicial de OwnCloud</i>	32
<i>Imagen 12: Configuración de conexión al ProxyLDAP</i>	33
<i>Imagen 13: Configuración de correlación de campo de objetos de tipo usuario</i>	34
<i>Imagen 14: Configuración de correlación de campo de objetos de tipo usuario</i>	34
<i>Imagen 15: Configuración de correlación de campo e-mail</i>	35
<i>Imagen 16: Configuración de conexión con el servidor de correo electrónico corporativo</i>	35
<i>Imagen 17: Configuración de Apache para utilización de certificado de ClientCorp</i>	37
<i>Imagen 18: Configuración de contraseña maestra de recuperación de ficheros encriptados</i>	38

ÍNDICE DE TABLAS

<i>Tabla 1: Cuestiones de integración</i>	20
<i>Tabla 2: Plan de pruebas – Piloto inicial</i>	47
<i>Tabla 3: Plan de mantenimiento</i>	49
<i>Tabla 4: Coste de implantación</i>	49
<i>Tabla 5: Coste de mantenimiento</i>	49

1. INTRODUCCIÓN

1.1. Introducción y comentarios iniciales

El presente documento refleja el análisis, diseño, implantación y final integración de un sistema de trabajo colaborativo por parte de una empresa de servicios informáticos que llamaremos “ConsultCorp, S.A.” (a partir de ahora ConsultCorp) en los sistemas e infraestructura de otra empresa, que denominaremos “ClientCorp, S.A.” (a partir de ahora ClientCorp).

La aplicación web para el trabajo colaborativo a integrar está basada en el software OpenSource denominado Owncloud y desarrollos propios y será accedida por empleados de todas las oficinas de ClientCorp (tienen presencia en varios países, teniendo la central administrativa y de infraestructuras de IT en Madrid, sumando un total de 200 trabajadores), empleados de ClientCorp con acceso desde Internet (redes no securizadas ni controladas por la compañía) y proveedores de la misma, que accederán desde redes securizadas por sus respectivas compañías y desde Internet en redes no seguras. Todos estos usuarios tendrán distintos tipos de permisos o acciones permitidas en el sistema, ya que cualquier usuario que no esté dado de alta en el sistema (bien sea la base de datos propia de Owncloud o en el directorio de usuarios LDAP de ClientCorp) únicamente podrá descargar ficheros que se compartan con ellos a través de URLs.

Como se verá más adelante ConsultCorp, además de hacer el análisis de la solución e integración, proveerá el propio sistema, soportado en infraestructura propia, por lo que para ClientCorp la solución se presenta en formato “SaaS” (“Software as a Service”), en el que ConsultCorp se hace cargo del mantenimiento del servidor donde se aloja el servicio.

Por todo lo comentado anteriormente, el éxito de la implantación e integración del sistema propuesto conlleva, además de formas nuevas y más eficientes de trabajar a sus usuarios, un ahorro de costes al externalizar tareas de mantenimiento del sistema, contratándolo como servicio y sin incurrir en costes de administración, mantenimiento y soporte del servidor donde se instalará la aplicación. En esta memoria se realizará un estudio del impacto económico de esta situación.

1.2. Motivaciones

La principal motivación de implantar un sistema de tipo “cloud” o en la nube para almacenar, sincronizar, compartir ficheros y acceder a ciertas aplicaciones web es permitir a los usuarios de ClientCorp, como se comentó anteriormente, trabajar de la forma más cómoda y eficaz posible, eliminando barreras que restricciones en los actuales sistemas de la compañía hacen complicadas ciertas tareas entre los distintos departamentos y con los proveedores de la empresa. Un sencillo y muy ilustrativo ejemplo de esta situación es el hecho de compartir un presupuesto o documentos de gran tamaño con empresas colaboradoras, siendo imposible el envío de e-mails de más de cierto tamaño, por lo que los usuarios tienen buscar soluciones creativas para efectuar la simple acción de compartir un documento (por ejemplo, enviarlo desde una cuenta personal de Gmail, compartirlo desde una cuenta no corporativa y no securizada de DropBox, o físicamente mediante un pendrive USB).

También se puede tener en cuenta que el panorama actual en cuanto a infraestructuras de TI se está centrando en cambiar de enfoque y hacer una pequeña revolución en lo que a la forma de trabajo se refiere. Según uno de los grandes fabricantes e impulsores de sistemas virtualizadores y generadores de sistemas “cloud”, estamos entrando en la denominada era post PC, en la que las estaciones de trabajo y soportes físicos para usuarios dejan de estar en el foco de los

departamentos de TI, para estar en los sistemas que generan máquinas virtuales y hacen flexible y escalable el despliegue de estaciones de trabajo y de aplicaciones individualizadas.

Esto tiene a día de hoy su reflejo en ciertos productos o aplicaciones relacionadas íntimamente con la temática que se desarrolla en este Trabajo Final de Carrera, como por ejemplo, vemos que sube la popularidad de programas como Dropbox o Google Drive, que hace unos 5 años poca gente usaba y que en la actualidad vemos que casi todos los usuarios de PC saben como utilizarlos y que de hecho los utilizan con frecuencia.

1.3. Objetivos

Los objetivos principales del presente Trabajo Final de Carrera son:

- Proponer e implementar un sistema que permita:
 - a. Almacenar datos de usuarios en sistemas fiables y redundados,
 - b. Compartir ficheros con usuarios tanto internos como externos.
 - c. Utilizar aplicaciones alojadas en la nube.
- Realizar la gestión del proyecto de implantación e integración.
- Integrar dicha solución en las infraestructuras existentes.
- Personalizar la apariencia a la imagen corporativa de la empresa y personalizar comportamientos de la aplicación para adecuarse a los requisitos definidos.

1.4. Estructura de la presente memoria

- **GESTIÓN DEL PROYECTO:** Se trata de la planificación de tareas dependencias de las mismas en el tiempo y la organización de recursos humanos implicados tanto por parte de ClientCorp como de ConsultCorp.
- **ANÁLISIS DE SITUACIÓN:** Se trata de la descripción y análisis de la solución a integrar. Además se realiza una descripción de otras aplicaciones de trabajo colaborativo que realizan funciones similares a la elegida para el desarrollo del proyecto, indicando los motivos que han decantado la elección por uno de ellos.
- **DISEÑO DEL SISTEMA DE TRABAJO COLABORATIVO A INTEGRAR:** Se trata de la descripción del diseño de la solución a integrar, teniendo en cuenta factores que hacen que la adaptación se realice de una determinada manera. Se indica también los sistema a tener en cuenta para realizar la integración y posibles cambios de configuración a realizar.
- **IMPLANTACIÓN E INTEGRACIÓN DEL SISTEMA:** Se trata de la descripción de elementos y técnicas utilizadas para adaptar adecuadamente las arquitecturas existentes en ClientCorp, además de indicar los elementos nuevos necesarios para la implantación de la solución diseñada.
- **PROCESO DE IMPLANTACIÓN E INTEGRACIÓN:** Se trata de la descripción esquematizada de los pasos a realizar para llevar a cabo la correcta integración del sistema, sin pretender ser un manual de instalación paso a paso, sino un esquema organizativo de la integración del nuevo sistema con la infraestructura de IT existente en ClientCorp.
- **PLAN DE PRUEBAS:** Se trata de la descripción de las pruebas necesarias para identificar posibles funcionamientos indeseados y validar que las funcionalidades del sistema cumplen con lo plasmado en los requisitos del sistema identificados y acordados entre ConsultCorp y ClientCorp.
- **PILOTO INICIAL:** Se trata de la descripción de la puesta en marcha en un entorno de test, con una cantidad de usuarios acotada, del nuevo sistema, antes de dar acceso y poner en producción el sistema para el total de los 200 empleados de ClientCorp, sin contar con los accesos de proveedores y externos en general.
- **DESPLIEGUE A USUARIOS:** Se trata de la descripción esquematizada de pasos a realizar para poner en marcha el sistema para todos los usuarios de ClientCorp.
- **PLAN DE MANTENIMIENTO:** Se trata de la descripción de la forma en que tanto ClientCorp como ConsultCorp realizarán el mantenimiento de los sistemas implicados en la solución implantada, en cuanto a recursos y tareas.
- **ANÁLISIS ECONÓMICO: PRESUPUESTO Y ANÁLISIS DE COSTES:** Se trata del presupuesto de la implantación e integración de la solución y el análisis de ahorros y costes que implica la misma.
- **CONCLUSIONES.**
- **GLOSARIO.**
- **BIBLIOGRAFÍA.**

2. GESTIÓN DEL PROYECTO

2.1. Planificación inicial y cambios en la misma

La planificación del proyecto queda de la forma que se muestra en el diagrama de Gantt (ver *Imagen 1*), teniendo en cuenta las fechas claves para la correcta gestión y control del proyecto.

Las fechas clave son las siguientes:

- **Inicio del proyecto:**
 - Inicio y fin el 28/02/2014.
 - Duración: 1 día laborable.
- **Toma inicial de datos:**
 - Inicio el 03/03/2014 y fin el 07/03/2014.
 - Duración: 5 días laborables.
- **Diseño Técnico:**
 - Inicio el 10/03/2014 y fin el 25/03/2014.
 - Duración: 12 días laborables.
- **Adecuación de la infraestructura existente:**
 - Inicio el 26/03/2014 y fin el 28/03/2014.
 - Duración: 3 días laborables.
- **Instalación y configuración del sistema a integrar:**
 - Inicio el 31/03/2014 y fin el 15/04/2014.
 - Duración: 12 días laborables.
- **Integración con sistemas de la empresa:**
 - Inicio el 16/04/2014 y fin el 21/04/2014.
 - Duración: 4 días laborables.
- **Piloto Inicial:**
 - Inicio el 22/04/2014 y fin el 30/04/2014.
 - Duración: 7 días laborables.
- **Despliegue a usuarios:**
 - Inicio el 01/05/2014 y fin el 07/05/2014.
 - Duración: 5 días laborables.
- **Entrega de documentación:**
 - Inicio y fin el 08/05/2014.
 - Duración: 1 día laborable.
- **Finalización del proyecto:**
 - Inicio y fin el 09/05/2014.
 - Duración: 1 día laborable.

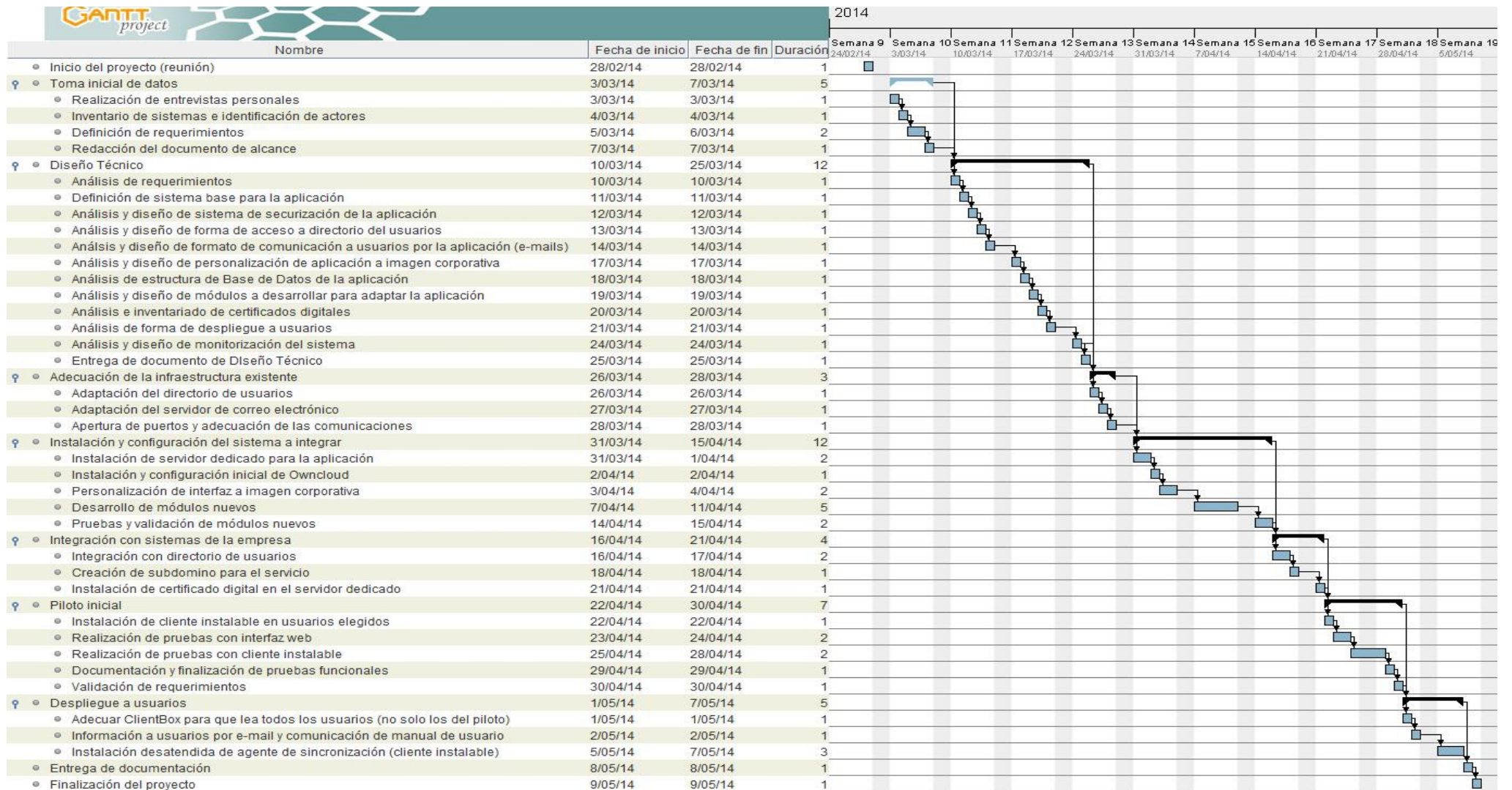


Imagen 1: Diagrama de Gantt.

2.2. Organización implicada

Para la realización del proyecto se han de tener en cuenta todos los suministradores y recursos humanos que se ven implicados en alguna, o todas, las fases del mismo.

El proyecto tiene una duración estimada, desde que se realiza la reunión de inicio del mismo hasta que se da por finalizado una vez se ha entregado y revisado la documentación, de 51 días, siendo el inicio del mismo el día 28/02/2014, con la reunión de arranque del proyecto y coordinación de primeras tareas a realizar.

En todo momento estará implicado el Jefe de Proyecto, que en este caso es Francisco Lievano Cos (trabajador de ConsultCorp) y que asumirá las responsabilidades y tareas de gestión y organización para llevar a buen término el proceso de instalación, personalización, implantación e integración de la aplicación web para el trabajo colaborativo en el cliente ClientCorp.

En las labores a llevar a cabo en el transcurso del proyecto, será necesaria también la participación de los recursos humanos siguientes (aportados tanto por ConsultCorp y por ClientCorp):

- Equipo de trabajo (personal de ConsultCorp y de ClientCorp):
 - Jefe de Proyecto:
 - Número de personas: 1.
 - Dedicación: jornada completa durante todo el proyecto.
 - Aportado por ConsultCorp.
 - Técnico de Sistemas - integrador:
 - Número de personas: 1.
 - Dedicación: jornada completa durante todo el proyecto.
 - Aportado por ConsultCorp.
 - Desarrollador PHP:
 - Número de personas: 1.
 - Dedicación: jornada completa hasta la entrega de módulos propios.
 - Aportado por ConsultCorp.
 - Técnico de Sistemas:
 - Número de personas: 1.
 - Dedicación: media jornada durante todo el proyecto.
 - Aportado por ClientCorp.
 - Técnico de comunicaciones:
 - Número de personas: 1.
 - Dedicación: media jornada durante todo el proyecto.
 - Aportado por ClientCorp.
- Recursos o proveedores externos a ConsultCorp y ClientCorp:
 - Proveedor de hosting y comunicaciones: “OVH Hispano S.L.U.” (desde ahora “OVH”).

3. ANÁLISIS DE SITUACIÓN

3.1. Fundamentos para el trabajo colaborativo mediante aplicaciones web

El trabajo colaborativo es visto por muchas empresas y organizaciones como una forma de aprovechar las nuevas tecnologías y mejorar la productividad entre distintos departamentos dentro de la misma o con organizaciones externas.

La ventaja de ofrecer un servicio de tipo web, en el que la aplicación no sea necesariamente accedida mediante clientes instalables o con la necesidad de cumplir unos requisitos en cuanto a software exigentes hace que dicha aplicación sea fácilmente accesible, mediante un navegador web sin necesidad de instalar software adicional.

Una de las tendencias en cuanto a tendencias en tecnología personal y empresarial, según la consultora Gartner, los “servicios personales en formato “cloud” ofrecidos a dispositivos” en el año 2013 fueron tendencia y en el futuro próximo cobrarán más fuerza. Esto quiere decir que la tendencia en el uso de servicios y dispositivos harán desaparecer gradualmente aplicaciones instaladas en dispositivos PC locales, a favor del acceso “ligero”, por ejemplo utilizando un navegador web, a todos los servicios necesarios por los usuarios, mediante casi cualquier tipo de naturaleza: móviles, tablets, portátiles o PCs obsoletos.

3.2. Sistemas web conocidos para el trabajo colaborativo

Los sistemas o aplicaciones ofrecidos como servicios más conocidos y que ofrecen una funcionalidad similar entre ellos son los indicados a continuación, teniendo en cuenta que hay diferencias conceptuales entre ellos que serán decisiva a la hora de tomar uno de ellos como solución a las necesidades de ClientCorp.

3.2.1. DropBox

La versión de este conocido software para empresas ofrece la funcionalidad de mantener ficheros en los servidores de dicho proveedor, con un control de versiones al realizar cambios en ficheros y la posibilidad de compartir con otros usuarios, mediante una interfaz web o con un cliente instalable.

En el marco del proyecto actual, esta solución no es del todo completa, ya que soluciona parcialmente la problemática de acceder a distintas aplicaciones de tipo web, enfocándose en el almacenamiento de ficheros y compartición de los mismos.

Más adelante, cuando se realice un análisis de requerimientos, se verá que esta solución no se adecuaría correctamente debido a que los datos de los usuarios estarían en almacenamiento de un proveedor cuyo control no puede ser verificado (no se controlaría dónde se están almacenando los datos).

3.2.2. Google Apps

La solución de Google para el uso de aplicaciones enfocadas a empresas ofrecidas como servicios web es la suite Google Apps, que engloba la solución de correo electrónico, mensajería instantánea y almacenamiento externo, entre otros.

Una de las fortalezas de estas aplicaciones web dentro de la empresa es que los usuarios ya están habituados a este tipo de herramientas, ya que la mayoría de ellos utilizan de forma personal aplicaciones como Gmail o Hangouts, que en el fondo son las mismas aplicaciones que se ofrece para el entorno empresarial.

Tal y como pasa con Dropbox, esta solución no se adecuaría correctamente debido a que los datos de los usuarios estarían en almacenamiento de un proveedor cuyo control no puede ser verificado (no se controlaría dónde se están almacenando los datos).

3.2.3. OwnCloud

La solución que ofrece OwnCloud se basa en el principio de sincronización y almacenamiento de ficheros, que mediante una interfaz web se puede subir, eliminar o acceder a ficheros almacenados en el sistema y mediante un agente instalable permite realizar sincronización de ficheros en tiempo real y con gestión de versiones.

Además de ofrecer almacenamiento y sincronización de ficheros, OwnCloud permite integrar en su interfaz web distintas aplicaciones, tales como reproductor de música y de imágenes, calendario, sistema de mensajería y sistema de gestión simple de tareas.

Una de las grandes ventajas que presenta este sistema respecto a otros es que puede ser instalado en servidores propios, o en un proveedor de hosting, y gestionar el almacenamiento donde serán guardados los ficheros y datos de los usuarios, que en los otros casos analizados no hay forma de controlar. Más adelante veremos la forma en que este software puede securizarse a nivel de redes y a nivel de datos.

El software elegido para formar parte de la solución a implantar en ClientCorp por parte de ConsultCorp es OwnCloud debido a que, como se ha comentado, es una solución integral de aplicaciones colaborativas accesibles vía web, además de dar solución a la sincronización y compartición de ficheros en una infraestructura que, aunque esté alojada en un proveedor de hosting, tenemos control del almacenamiento y los datos ubicados en él.

3.3. Análisis de situación actual

3.3.1. Sistemas existentes involucrados en la integración

La aplicación a implementar ha de estar integrada con los sistemas propios del cliente, ClientCorp, para que cumpla con los requisitos que se han acordado.

Los sistemas del cliente a integrar con la aplicación son los siguientes:

- Directorio de usuarios OpenLDAP corporativo: Sistema donde se almacenan los datos de los usuarios internos de la compañía, y contra el cual se realiza la autenticación, mediante credenciales de usuario/contraseña de los mismos.
- Sistema de correo electrónico corporativo: Sistema de correo electrónico, en el cual están configurados los dominios de ClientCorp y que funcionará como “relay” para que OwnCloud pueda enviar e-mails con una dirección corporativa.
- Servicio de nombres (DNS) corporativo: Servidor de nombres DNS, donde se añadirá un registro de tipo A para acceder a OwnCloud mediante nombre.
- Identidad digital de la empresa (certificados digitales): Se trata del certificado digital que ha de ser instalado en el servidor para que las conexiones remotas seguras (HTTPS) estén cifradas mediante un certificado propiedad de ClientCorp.
- Sistemas cortafuegos de la empresa: Los empleados de ClientCorp han de ser capaces de acceder a los servicios web de OwnCloud desde las redes de sus oficinas, por lo que es necesario permitir los accesos a nivel de cortafuegos.

3.4. Definición de requerimientos

3.4.1. Requerimientos funcionales

La identificación y análisis de requisitos funcionales se realiza también asignando un identificador al requisito y la descripción del mismo. Los requisitos funcionales han sido elaborados a partir de las impresiones de los integrantes del departamento de informática, pensando en la solución desde el punto de vista de los usuarios finales del sistema:

- **FR-1**: El sistema debería permitir login de usuarios con el mismo usuario y contraseña que en el resto de aplicaciones de la empresa.
- **FR-2**: El sistema debería reconocer a los usuarios por su nombre y apellidos (están en el directorio de usuarios).
- **FR-3**: El sistema debería reconocer la dirección de e-mail de cada usuario dado de alta en el sistema (están en el directorio de usuarios).

- **FR-4:** El sistema debería permitir la edición de ficheros de texto directamente desde el navegador.
- **FR-5:** El sistema debería mostrar directamente el contenido de documentos PDF directamente en el navegador si necesidad de descargarlos.
- **FR-6:** El sistema debería permitir la reproducción de ficheros de audio con un reproductor integrado.
- **FR-7:** El sistema debería mostrar imágenes embebidas en el navegador web, sin necesidad de descargarlas para ser visualizadas.
- **FR-8:** El sistema debería permitir recuperar ficheros y directorios eliminador, con una funcionalidad parecida a la de papelera de reciclaje.
- **FR-9:** El sistema debería tener un sistema de antivirus integrado que analice los datos almacenados en el servidor.
- **FR-10:** El sistema debería permitir a los usuarios personalizar un avatar.
- **FR-11:** El sistema debería permitir compartir ficheros mediante URLs o enlaces, protegidos con contraseña y fecha de caducidad.
- **FR-12:** El sistema debería permitir enviar mensajes instantáneos a otros usuarios del sistema.
- **FR-13:** El sistema debería permitir visualizar un calendario integrado, donde se puedan hacer anotaciones, citas y tareas.
- **FR-14:** El sistema debería permitir visualizar a cada usuario un histórico de actividades en cuanto a movimiento de ficheros y directorios.

3.4.2. Requerimientos no funcionales

La identificación y análisis de requerimientos no funcionales se agrupan en 4 apartados, según el tipo que sean: de rendimiento, de distribución, de seguridad y de usabilidad. A continuación se indican los requisitos no funcionales junto a un análisis de cada uno de ellos, y en apartados siguientes se analizará qué actores están implicados en dicho proceso:

- **Requisitos de rendimiento:**

Identificador:	NFR-1.1
Requisito:	El sistema ha de responder sin lentitud.
Descripción:	El sistema ha de responder rápidamente, tanto la interfaz web como el cliente instalable.
Stakeholders:	Responsable de Aplicaciones.
Criterio de aceptación:	El sistema ha de responder de forma fluida al acceder a la interfaz web y ha de sincronizar en el tiempo más rápido posible los datos añadidos a la carpeta que sincroniza el agente instalable.
Cuestiones pendientes:	Definir la autenticación de usuarios en la interfaz web contra el directorio de usuarios corporativo, que afectará al tiempo que tarda en responder la carga de los datos de los usuarios.

Identificador:	NFR-1.2
Requisito:	El sistema ha de estar disponible el mayor tiempo posible.
Descripción:	El sistema ha de estar accesible 24x7, la mayor cantidad de tiempo posible, teniendo en cuenta que hay pérdidas del servicio al realizar actualizaciones de software base de OwnCloud, de Apache y del Sistema Operativo.
Stakeholders:	Responsable de Aplicaciones.
Criterio de aceptación:	El sistema ha de estar disponible cada vez que un usuario de la compañía o externo a la misma intente acceder al mismo, dentro del horario normal de trabajo.
Cuestiones pendientes:	Definir la política de aplicación de actualizaciones.

Identificador:	NFR-1.3
Requisito:	El sistema ha de funcionar correctamente para todos los usuarios de la empresa (200 usuarios).
Descripción:	El sistema ha de funcionar correctamente para todos los usuarios de la empresa (200), teniendo en cuenta que prácticamente todos ellos tendrán el cliente instalado en sus PCs y estarán sincronizando ficheros continuamente.
Stakeholders:	Director del departamento de Informática.
Criterio de aceptación:	El sistema ha de funcionar con normalidad en horas pico de trabajo, teniendo todos los usuarios el cliente OwnCloud instalado.
Cuestiones pendientes:	Definir la política de aplicación de actualizaciones.

- **Requisitos de distribución:**

Identificador:	NFR-2.1
Requisito:	El sistema ha de estar disponible para todos los usuarios de todas las delegaciones de la compañía.
Descripción:	El sistema ha de ser accesible por los usuarios de todas las delegaciones de la empresa, tanto por interfaz web como por cliente instalable.
Stakeholders:	Director del departamento de Informática.
Criterio de aceptación:	El sistema ha de funcionar con normalidad en horas pico de trabajo, teniendo todos los usuarios el cliente OwnCloud instalado.
Cuestiones pendientes:	Definir la política de aplicación de actualizaciones.

Identificador:	NFR-2.2
Requisito:	El sistema debe permitir compartir ficheros con usuarios de la compañía y externos a la misma.
Descripción:	El sistema debe permitir compartir ficheros mediante enlaces con usuarios externos a la compañía (sin usuario en OwnCloud o en el directorio LDAP) y permitir compartir con usuarios del sistema.
Stakeholders:	Director del departamento de Informática.
Criterio de aceptación:	Los usuarios externos e internos de la compañía deben poder abrir ficheros compartidos con ellos por otros usuarios internos del sistema.
Cuestiones pendientes:	Ninguna.

Identificador:	NFR-2.3
Requisito:	El sistema ha de permitir enviar notificaciones.
Descripción:	El sistema ha de permitir enviar notificaciones de compartición de ficheros a usuarios en ubicaciones distintas, de la compañía y externos a la misma.
Stakeholders:	Responsable de comunicaciones.
Criterio de aceptación:	El sistema envía un e-mail al usuario cuando otro comparte un fichero o directorio con él.
Cuestiones pendientes:	Ninguna.

- **Requisitos de seguridad:**

Identificador:	NFR-3.1
Requisito:	El sistema ha de autenticar a los usuarios.
Descripción:	El sistema ha de autenticar o validar a los usuarios con el directorio de usuarios (LDAP) de la empresa, al acceder a la interfaz web y al iniciar el agente instalable..
Stakeholders:	Responsable de aplicaciones.
Criterio de aceptación:	El sistema autentica a los usuarios contra el LDAP corporativo. Si no existe el usuario o introduce mal la contraseña no le permite acceder.
Cuestiones pendientes:	Identificar a qué rama del directorio de usuarios se incluye en el sistema.

Identificador:	NFR-3.2
Requisito:	El sistema debe permitir la encriptación de datos.
Descripción:	El sistema debe permitir la encriptación de todos los datos almacenados en el servidor.
Stakeholders:	Responsable de seguridad informática.
Criterio de aceptación:	Los datos de los usuarios no deben poder ser accedidos por otros usuarios en el servidor.
Cuestiones pendientes:	Decidir si se aplica la desencriptación con una contraseña maestra y evitar pérdida de datos de usuarios que pierden su contraseña.

Identificador:	NFR-3.3
Requisito:	El sistema debe integrar seguridad al compartir con personal externo.
Descripción:	El sistema debe obligar el uso de contraseña para acceder a ficheros compartidos con usuarios externos a la compañía.
Stakeholders:	Responsable de seguridad informática.
Criterio de aceptación:	El sistema debe pedir contraseña obligatoriamente contraseña cuando se intenta compartir un fichero por enlace.
Cuestiones pendientes:	Ninguna.

- **Requisitos de usabilidad:**

Identificador:	NFR-4.1
Requisito:	El sistema debe ser completo y vistoso.
Descripción:	El acceso a los ficheros con las opciones de compartición y permisos debe estar integrado en un mismo portal junto con el acceso a aplicaciones (como visor de imágenes o reproductor de música).
Stakeholders:	Responsable de aplicaciones.
Criterio de aceptación:	El sistema debe mostrar de forma sencilla el acceso a las distintas funcionalidades que ofrece.
Cuestiones pendientes:	Integración con la imagen corporativa (logos y colores).

Identificador:	NFR-4.2
Requisito:	El sistema debe ser fácil de configurar.
Descripción:	La configuración en cuanto a directorios a sincronizar, compartición de ficheros y directorios y configuración del agente instalable ha de ser sencilla para los usuarios.
Stakeholders:	Responsable de aplicaciones.
Criterio de aceptación:	El sistema debe mostrar de forma sencilla el acceso a las distintas configuraciones que ofrece.
Cuestiones pendientes:	Ninguna.

4. DISEÑO DEL SISTEMA DE TRABAJO COLABORATIVO A INTEGRAR

Como se ha comentado con anterioridad, la aplicación web para el trabajo colaborativo a integrar como solución para ClientCorp, estará alojado en un datacenter de un proveedor externo, OVH, contratado por ConsultCorp.

La solución propuesta conlleva la ejecución de unos pasos secuenciales, que a continuación son especificados y que surgen a raíz de la revisión de los requerimientos por parte del Jefe de Proyecto y el personal técnico implicado por parte de ClientCorp y ConsultCorp. Esta secuencia de pasos es la siguiente:

- Instalación de servidor dedicado para el servicio OwnCloud.
- Instalación de OwnCloud.
- Configuración inicial de OwnCloud.
- Personalización de la interfaz web.
- Configuración especial:
 - Integración con servidor de correo electrónico corporativo.
 - Integración con la identidad digital (certificados digitales).
 - Integración con dominio de la empresa (DNS).
- Desarrollo e implantación de módulos nuevos.

4.1. Revisión de requerimientos

Una vez realizado el análisis y revisión de los requerimientos obtenidos y conociendo la infraestructura del cliente, ConsultCorp es capaz de realizar el dimensionamiento y la adecuación de la infraestructura nueva necesaria para poder implantar la solución propuesta.

Las conclusiones a las que llega ConsultCorp como resultado del análisis de los requerimientos y que definen la forma en la que se abarca el proyecto son las siguientes:

- La aplicación web que forma parte de la solución estará alojada en un único servidor virtual.
- El servidor virtual estará dentro de un Datacenter virtual formado por dos servidores físicos.
- El Hypervisor utilizado es VMware , usando la versión Vsphere 5.1 y gestionado con Virtual Center.
- El Datacenter virtual dispondrá de alta disponibilidad (HA de VMware) en cuanto a Hardware y almacenamiento, y dispondrá de gestión automatizada de recursos (DRS de VMware) entre los nodos del cluster.

- El servidor virtual de ClientBox dispondrá de 1 única dirección IP pública.
- El dimensionamiento del servidor será el siguiente:
 - CPU: 4 vCPU a 2.3GHz.
 - Memoria: 4GB
 - Interfaces de red: 1 (dirección IP pública).
 - Almacenamiento:
 - Disco 1: 20GB (Sistema Operativo + instalación base).
 - Disco 2: 1TB (datos de usuarios).

Por otra parte, se decide que la aplicación se llamará, dentro del entorno de ClientCorp, con el nombre “**ClientBox**”, debido a que los usuarios podrán asociar su funcionalidad a la prestada por otro servicio comentado con anterioridad y que presta una funcionalidad similar a la de OwnCloud, como lo es Dropbox. Esto será decisivo a la hora de crear y configurar el servidor y la aplicación, ya que es conveniente dar el nombre correcto a la aplicación desde el primer momento y evitar reconfiguraciones que pueden evitarse.

4.2. Proceso de planificación

La correcta puesta en funcionamiento del sistema a integrar depende en gran medida, de como ya hemos comentado, de la correcta adecuación de los sistemas e infraestructura de TI en general. Ya hemos identificado los diferentes elementos que hay que adaptar y para ejecutarlos es necesario que ConsultCorp indique a ClientCorp los sistemas y parámetros a modificar antes de realizar la instalación e integración de ClientBox.

Para identificar de forma más ágil los elementos que ClientCorp ha de adaptar para el correcto funcionamiento de ClientBox, ConsultCorp confecciona una tabla con diversas cuestiones a tener en cuenta para que los técnicos de sistemas y de comunicaciones de ClientCorp completen (posteriormente analizaremos la información obtenida para detallar más adelante el proceso de adaptación de cada elemento).

La tabla resultante es la siguiente:

Cuestiones de integración	Sistemas de ClientCorp				
	OpenLDAP	MS Exchange 2007	Servidor DNS	Certificado digital	Firewall
Accesibilidad desde Internet	NO	NO	SI	SI	NO
Usuario de acceso	NO	NO	NO	NO	NO
Carga de trabajo de adaptación	25,00%	30,00%	5,00%	15,00%	25,00%
Usuarios dentro de sistemas	100,00%	100,00%	X	X	90,00%

Tabla 1: Cuestiones de integración.

Las conclusiones que podemos extraer de esta información son las siguientes:

- El servidor ClientBox no tiene acceso al directorio de usuarios OpenLDAP.
- El servidor ClientBox no tiene acceso al servidor de correo electrónico para hacer relay.
- No se dispone de un usuario de lectura del directorio de usuarios OpenLDAP.
- No se dispone de cuenta de correo electrónico para ser usada como remitente en las comunicaciones que se envíen a usuarios.
- No se dispone de usuario de gestión de nombres en servidor DNS para ConsultCorp.
- No se dispone de usuario para ConsultCorp para descryptar certificado digital a usar.
- El elemento que se estima que llevará más carga de trabajo por parte de los técnicos de sistemas y comunicaciones de ClientCorp es el correo electrónico, mientras que el que menos tiempo llevará, se estima que es el de DNS.
- Todos los usuarios de la compañía que han de acceder con usuario y contraseña en ClientBox están en el directorio de usuarios OpenLDAP, tienen cuenta de correo electrónico corporativa, pero el 10% acceden desde redes no controladas por la compañía.

4.3. Preparación de los sistemas

4.3.1. Adaptación de directorio de usuarios

El directorio de usuarios de la ClientCorp está basado en OpenLDAP, como ya hemos comentado anteriormente. De las consultas y entrevistas tenidas entre ConsultCorp y ClientCorp, se hace saber que dicho directorio no es accesible desde Internet, por lo que, si no se realiza ninguna labor de adaptación, el servicio de ClientBox no podrá leer datos de usuarios y no se integrará correctamente con su base de datos de usuarios.

La solución propuesta por ConsultCorp es la creación de un servidor en las instalaciones de ClientCorp que haga funciones de proxy LDAP. Dicho servidor proxy LDAP tendría acceso de sólo lectura (mediante usuario y contraseña y securizado con un Firewall) a los datos del servidor OpenLDAP de producción y sería accesible desde Internet, por lo que, con este modelo, no se exponen datos confidenciales y de máxima criticidad.

Los datos de los usuarios serían accedidos de esta forma por el servidor ClientBox por Internet, con una dirección IP fija y con un usuario de sólo lectura de datos de usuarios, mientras que internamente, dentro de la infraestructura de ClientBox, el servidor proxy LDAP sólo permitiría conexiones desde la dirección IP del servidor ClientBox y con el usuario de sólo lectura definido, mientras que en el directorio de usuarios de producción OpenLDAP sólo se daría acceso de lectura desde el servidor proxy LDAP.

El esquema de la infraestructura a modificar en ClientCorp quedaría como se muestra en la siguiente imagen:

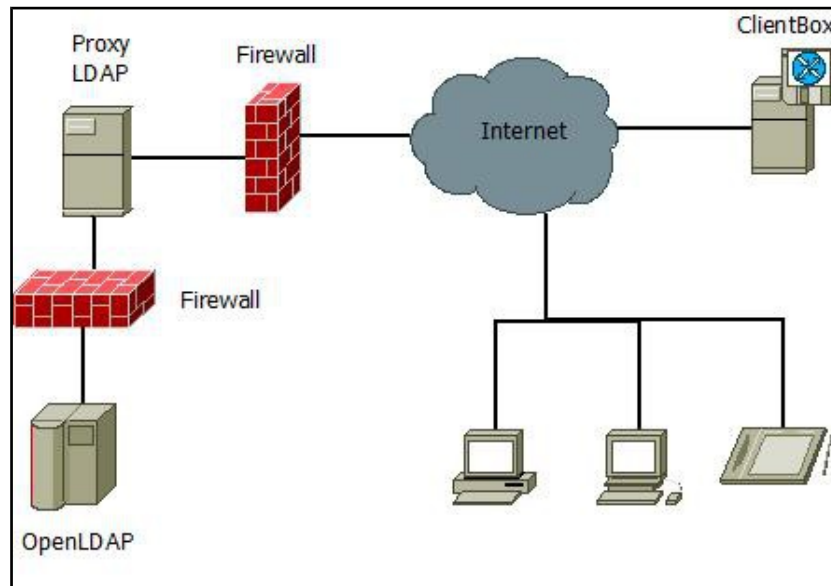


Imagen 2: Diagrama de infraestructura para acceso a Directorio de Usuarios.

Según el diagrama indicado, el flujo de trabajo cuando el sistema se encuentre funcionando en producción sería el siguiente:

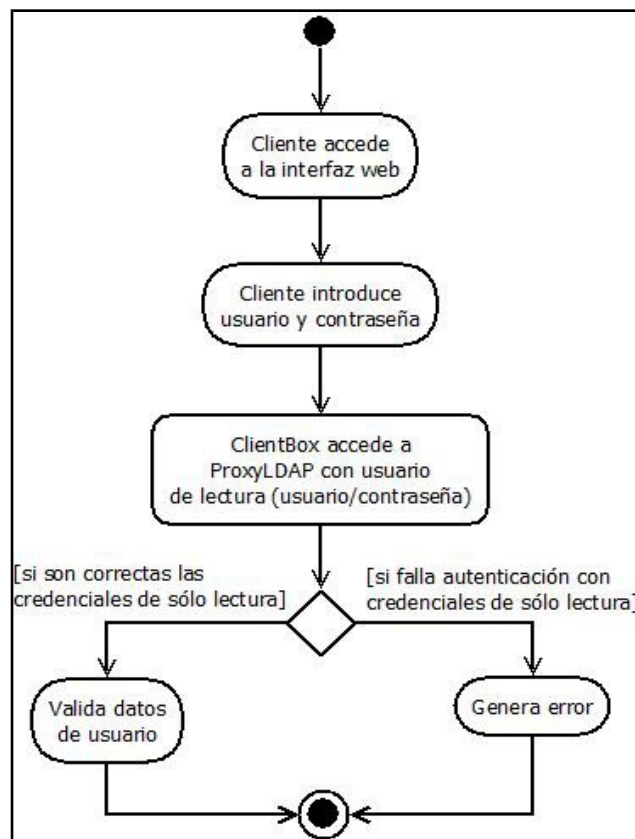


Imagen 3: Diagrama de actividad: acceso a Directorio de Usuarios.

4.3.2. Configuración de certificados digitales

La empresa ClientCorp posee un certificado digital de tipo “wildcard”, para el dominio clientcorp.com (el certificado es “*.clientcorp.com”).

Con este certificado ConsultCorp es capaz de configurar la aplicación para que los accesos a través de HTTPS, sean seguros ya que el certificado SSL está firmado por una autoridad certificadora válida (Verisign).

La aplicación web ClientBox es publicada por un servidor Apache sobre Linux. Específicamente es Apache 2.2.22 sobre la máquina virtual sobre la que se instalará ClientBox, basada en Linux.

El certificado digital válido, una vez instalado, debería poder verse como en la siguiente imagen al realizar un acceso a ClientBox mediante HTTPS:



Imagen 4: Certificado Digital firmado por Verisign.

Aunque el certificado digital a instalar en el servidor ClientBox y a ser configurado en su Apache esté firmado para cualquier subdominio de “clientcorp.com”, se configurará el “hostname” dentro de dicho servidor y su Apache para que responda al nombre de “box.clientcorp.com”, por lo que los accesos se realizarán a través de la URL <https://box.clientcorp.com>.

4.3.3. Configuración de registros DNS

Los cambios a realizar en el DNS público de ClientCorp están íntimamente relacionados con el punto anteriormente tratado (certificado digital). El nombre por el cual se va a acceder al servicio web es box.clientcorp.com.

Para que los accesos sean posibles a través de nombre, ClientCorp, propietario del dominio clientcorp.com, ha de añadir un registro de tipo “A” en su configuración para que además de poder acceder mediante dirección IP se pueda acceder con un nombre corporativo.

4.3.4. Configuración de sistema de correo electrónico

El servicio de ClientBox ha de ser capaz de enviar notificaciones por correo electrónico a usuarios internos y externos de la empresa, o lo que es lo mismo, a usuarios dentro del dominio configurado para el servicio de correo electrónico (clientcorp.com) y a usuarios que son externos a la compañía, por ejemplo proveedores, que tendrán cuentas de correo electrónico de otro dominio distinto al de ClientCorp.

El servidor de correo electrónico de ClientCorp está dentro de su infraestructura y dentro de su red corporativa, por lo que, como veremos en siguientes puntos, es necesario realizar modificaciones a nivel de comunicaciones (en firewalls) y en el propio servidor de correo electrónico, creando una cuenta para que se permita hacer relay desde el servidor virtual dedicado a ClientBox y alojado en un proveedor externo.

4.3.5. Adecuación de redes de comunicación

Las redes de comunicación internas de ClientCorp tendrán que ser adaptadas para dar servicio a la nueva infraestructura: nuevo servidor proxyLDAP, accesos salientes a ClientBox y accesos al servidor de correo electrónico desde el servidor de ClientBox.

A nivel de redes, hay que tener en cuenta todo el tráfico nuevo que se generará entre ClientBox y todos los sistemas internos, y entre el ProxyLDAP y el servidor OpenLDAP de producción.

Por parte de ConsultCorp, no será necesario realizar ningún tipo de adaptación especial, únicamente será necesario asignar una dirección IP pública libre, dentro del rango de IPs dadas por el proveedor del hosting, OVH.

Esquemáticamente, el tráfico nuevo generado a tener en cuenta sería mostrado en la siguiente figura (“imagen 5”):

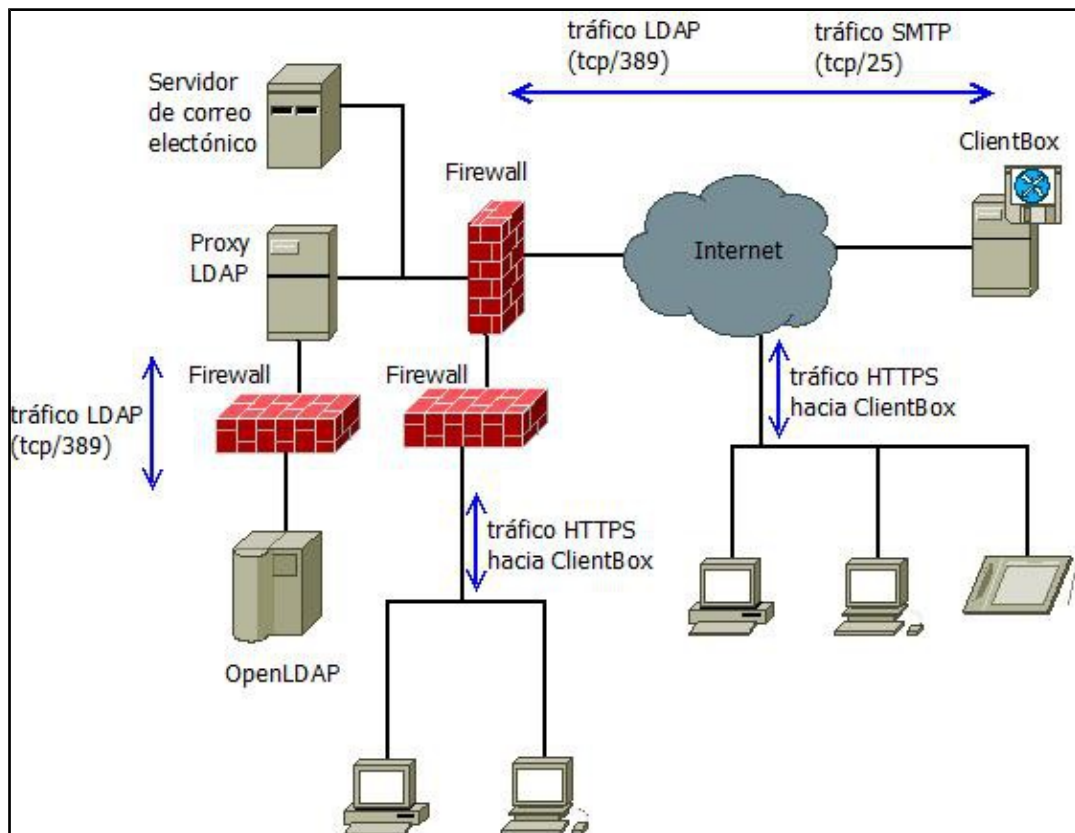


Imagen 5: Esquema de nueva situación de redes de comunicación.

En el esquema representado en la “imagen 5” se puede ver el flujo de datos que habrá que tener en cuenta en el proceso de integración de la solución propuesta:

- Tráfico de tipo HTTPS (puerto de destino tcp/443) entre los dispositivos de usuarios (origen) y el servidor ClientBox (destino). Los equipos de usuario pueden estar dentro de la red corporativa o fuera de la misma, accediendo desde Internet.
- Tráfico de tipo LDAP (puerto de destino tcp/389) entre el servidor ClientBox (origen) y el servidor ProxyLDAP (destino).
- Tráfico de tipo LDAP (puerto de destino tcp/389) entre el servidor ProxyLDAP (origen) y el servidor OpenLDAP (destino).
- Tráfico de tipo SMTP (tcp/25) entre el servidor ClientBox (origen) y el servidor de correo electrónico de ClientCorp (destino).

4.4. Visión esquemática global del sistema a integrar

El sistema se puede ver como un conjunto de subsistemas que interaccionan entre ellos y que tienen distintas formas de funcionar de forma individual. Por este motivo, y para que quede definido de forma más clara, se realizará un esquema por tipo de subsistema que realiza una función específica a integrar en el marco de la solución propuesta:

- Accesos de dispositivos de usuarios a ClientBox:

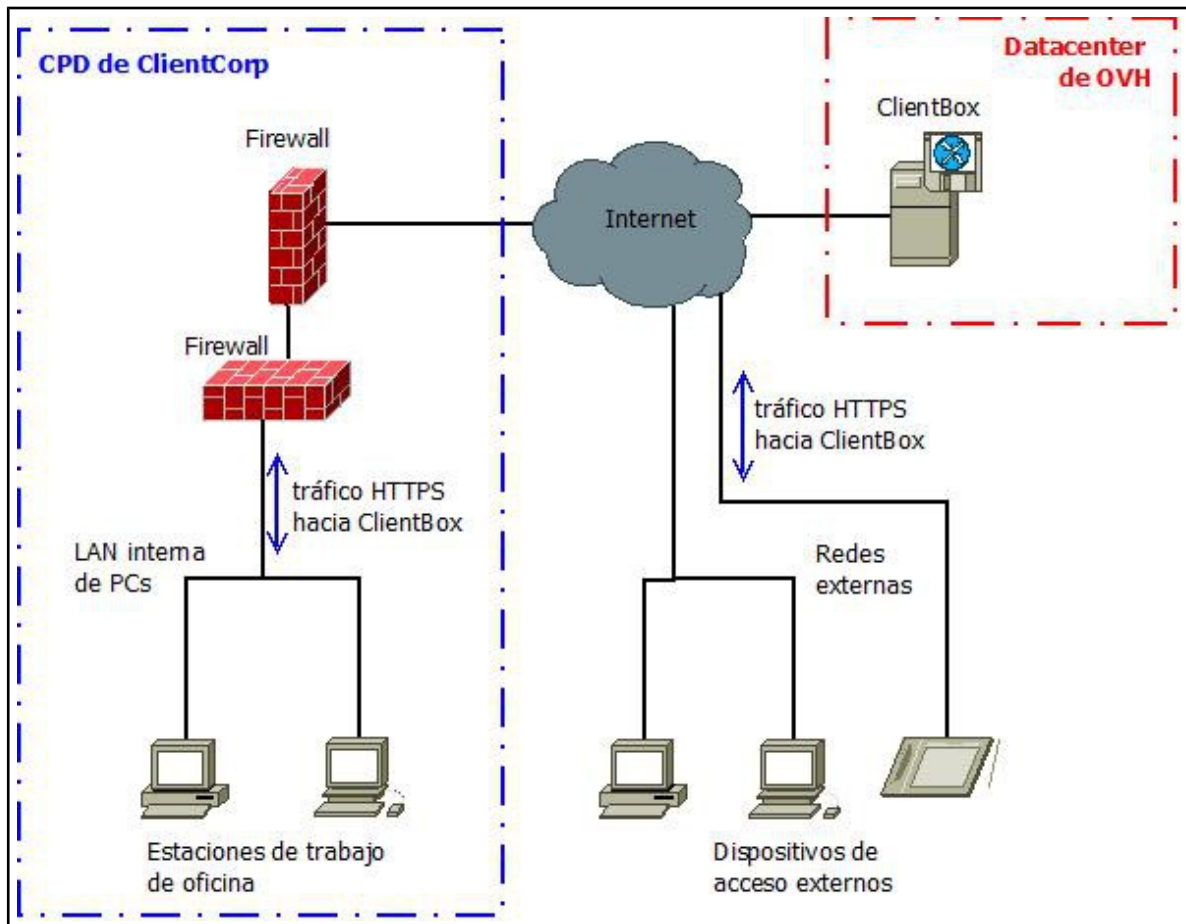


Imagen 6: Esquema del sistema de accesos de usuarios a ClientBox.

En el esquema representado en la “imagen 6” podemos ver que los dispositivos de usuarios desde los cuales se realizará uso de la aplicación a implantar están dentro de las redes de la empresa y fuera de la misma, en redes externas y que ni ClientCorp ni ConsultCorp pueden gestionar (son de proveedores o conexiones desde líneas ADSL domésticas).

- Lectura de datos de usuarios desde ClientBox al ProxyLDAP:

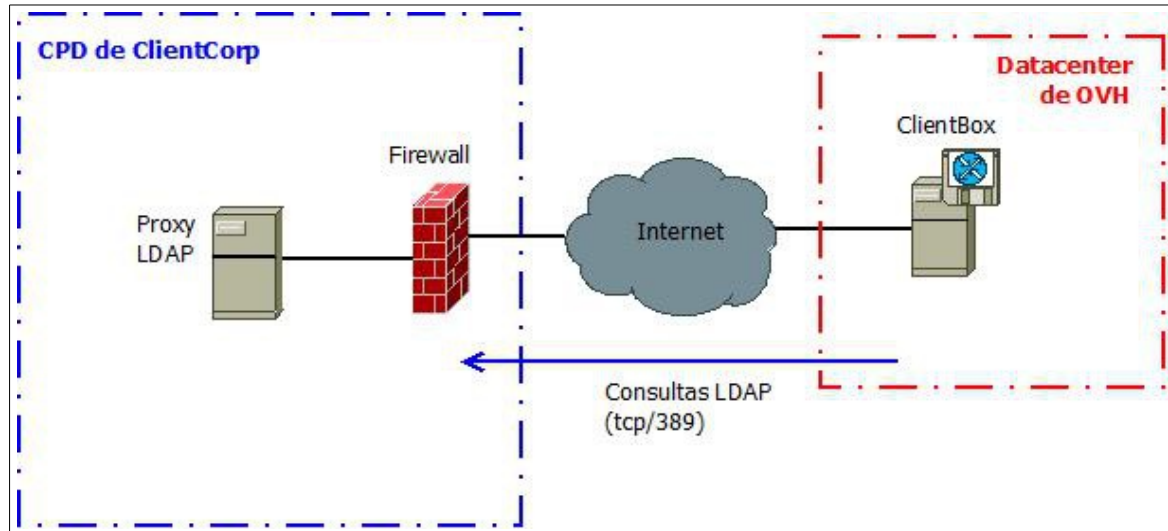


Imagen 7: Esquema del sistema de lectura de datos de usuarios desde ClientBox al ProxyLDAP.

En el esquema representado en la “imagen 7” podemos ver el servidor ClientBox realiza las consultas de tipo LDAP al ProxyLDAP mediante su dirección IP pública. Es necesario recordar y tener presente que el Firewall que protege al ProxyLDAP únicamente permite accesos al puerto tcp/389 del servidor ProxyLDAP desde la dirección IP pública del servidor ClientBox.

También es necesario tener en cuenta que los accesos que realiza el servidor ClientBox al ProxyLDAP mediante consultas LDAP al puerto tcp/389 de éste último se hacen autenticando un usuario y contraseña de sólo lectura, por lo que no hay riesgo de alteración de registros de datos de usuarios en el directorio OpenLDAP de producción.

Más adelante veremos también que, a su vez, el servidor ProxyLDAP accede con credenciales (usuario y contraseña) de sólo lectura al servidor OpenLDAP, por lo que esto también nos ofrece seguridad adicional (entre cada paso hay un dispositivo Firewall, donde se realizará la configuración de acceso único por dirección IP a servidores por puertos y protocolos específicos).

- Lectura de datos de usuarios desde ProxyLDAP a OpenLDAP (directorío en producción):

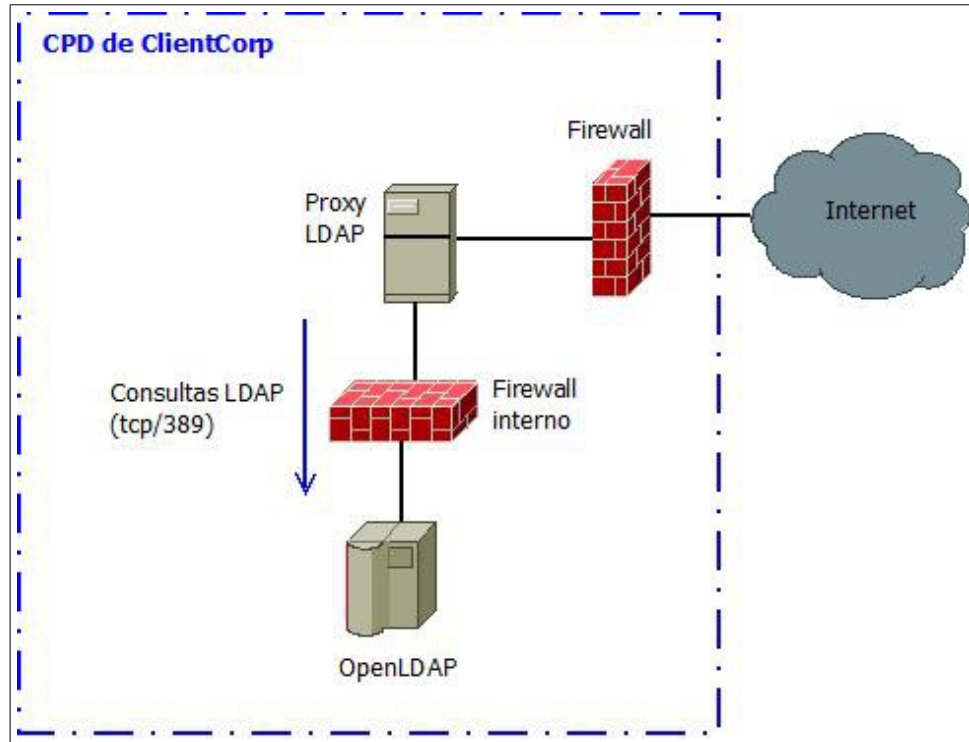


Imagen 8: Esquema del sistema de lectura de datos de usuarios desde el ProxyLDAP a OpenLDAP.

En el esquema representado en la "imagen 8" podemos ver el servidor ProxyLDAP realiza las consultas de tipo LDAP al servidor de directorio de usuarios en producción OpenLDAP mediante su dirección IP/nombre de red interno. Es necesario recordar tener presente que el Firewall que protege al ProxyLDAP únicamente permite accesos al servidor OpenLDAP desde el puerto tcp/389 de la dirección IP interna del servidor ProxyLDAP.

Por otra parte, el servidor ProxyLDAP accede con credenciales (usuario y contraseña) de sólo lectura al servidor OpenLDAP, por lo que esto también nos ofrece seguridad adicional.

- Envío de notificaciones por correo electrónico:

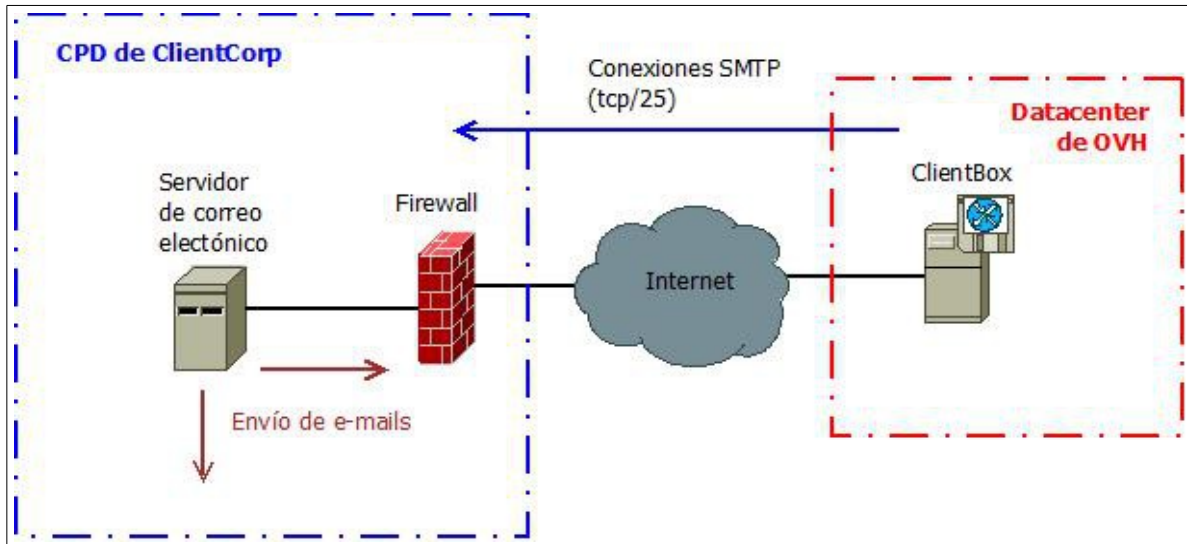


Imagen 9: Esquema del sistema de envío de notificaciones por correo electrónico.

En el esquema representado en la “*imagen 9*” podemos ver el servidor que el servidor ClientBox, cuando tiene que realizar un envío de notificaciones por correo electrónico realiza una conexión SMTP (Relay de correo electrónico) al servidor de correo de ClientCorp (conexión tcp/25). Esta conexión se asegura mediante el Firewall que han de atravesar los paquetes implicados, permitiendo el acceso al servidor de correo por el puerto 25 desde el servidor ClientBox.

Una vez se ha realizado la conexión entre ambos servidores, el sistema solicita credenciales para poder realizar el envío. La aplicación ClientBox introduce las credenciales dadas por el administrador del servidor de correo electrónico (usuario y contraseña de la cuenta box@clientcorp.com).

Por último, una vez realizada la conexión y efectuada la autenticación, la aplicación ClientBox es capaz de enviar correos electrónicos a cuentas internas del dominio clientcorp.com como a cuentas externas, con otros dominios, utilizando el servidor de correo corporativo.

5. IMPLANTACIÓN E INTEGRACIÓN DEL SISTEMA

El proceso de implantación e integración del sistema se lleva a cabo en varias fases, que han de realizarse de forma secuencial para asegurar la correcta integración de los sistemas y evitar reconfiguraciones que pueden inducir a errores.

Las tareas a realizar son las que se analizarán a continuación. Dichas tareas no se describirán en formato de manual de instalación, sino que pretenden ser una guía de elementos de configuración de parámetros y de sistemas imprescindibles a tener en cuenta para el correcto funcionamiento de la aplicación.

5.1. Instalación y configuración de servidor dedicado

El servidor ClientBox se aloja en una máquina virtual dedicada, alojada en un datacenter virtual gestionado por ConsultCorp y provisto por el proveedor OVH. Físicamente, los 2 servidores que forman el Cluster dentro del datacenter virtual están en el centro de datos de OVH en la localidad de Roubaix, al norte de Francia.

El software de virtualización utilizado, como se ha comentado en puntos anteriores es VMware VSphere 5.1, con un Virtual Center como servidor de gestión, con alta disponibilidad (HA) y gestión automatizada de recursos (DRS). El almacenamiento sobre el que residirá el servidor ClientBox está también configurado en alta disponibilidad, por lo que dicho proveedor ofrece un nivel de servicio (SLA) del 99,99% de disponibilidad en cuanto a host y un 100% en cuanto a almacenamiento. En cuanto a la disponibilidad de la red de comunicaciones, ofrecen un SLA de 100% de disponibilidad.

La instalación del servidor ClientBox la realiza ConsultCorp, y para ello se utiliza una imagen de disco de instalación del Sistema Operativo base que soportará OwnCloud.

El Sistema Operativo a instalar es Debian 7.3, Wheezy, para arquitecturas de tipo AMD64. Dicho sistema está basado en el Kernel Linux versión 3.2.0-4.

En cuanto a software distinto a OwnCloud (y dependencias básicas) a instalar en la máquina virtual, se instala un servidor SSH para la gestión remota de dicho servidor. Ya veremos en puntos más adelante que para el correcto funcionamiento de OwnCloud es necesario instalar MySQL Server, Apache y software adicional para la securización del propio servidor, como por ejemplo, un Firewall por software específico y SUDO (ejecución de comandos con permisos especiales a ciertos usuarios).

Por otra parte, para la correcta securización y adaptación del sistema con la identidad digital de ClientCorp, también se hace necesario instalar OpenSSL en el servidor donde se aloja ClientBox, además de ser necesario reconfigurar Apache para que sea capaz de trabajar sirviendo el sitio web protegiendo las comunicaciones mediante SSL a través del puerto TCP/443 (esto se verá en apartados más adelante).

5.1.1. Instalación de OwnCloud en servidor dedicado

La instalación de OwnCloud se puede realizar de varias formas: mediante la compilación y posterior instalación de fuentes o mediante gestores de paquetes. Para la instalación de OwnCloud en el servidor ClientBox se opta por realizarla mediante el gestor de paquetes de la distribución Debian, que es Aptitude, usando el comando “apt-get”. Esta forma de instalación facilita enormemente las tareas de mantenimiento que se comentarán más adelante, debido a que las actualizaciones se gestionan de forma más sencilla y resuelve dependencias entre software necesario para el funcionamiento de la aplicación que se desea instalar.

Como motor de base de datos se instala MySQL Server 5.5, también mediante el gestor de paquetes APT, por el mismo motivo por el cual se instala OwnCloud también con dicho gestor de paquetes. Para el correcto uso de MySQL por parte de OwnCloud, se crea un usuario llamado “owncloud” y un base de datos denominada “owncloud”, otorgando todos los permisos de gestión al usuario anteriormente creado a dicha base de datos.

El software mediante el cual se realiza la publicación web es Apache, en su versión 2.2.22, que se instala como dependencia de OwnCloud, y el intérprete usado para mostrar sus páginas web y ejecutar sus funcionalidades es PHP, en su versión 5.4.4, instalado también como dependencia del paquete OwnCloud.

5.1.2. Configuración básica de OwnCloud en servidor dedicado

Para el correcto funcionamiento de OwnCloud no es necesario realizar ningún tipo de modificación especial o cambio de la configuración por defecto de PHP, únicamente instalar manualmente el módulo *php5-ldap* para poder utilizar directorios de usuarios externos, mientras que para el caso de Apache sí es necesario crear un “virtual host” dedicado para OwnCloud. Este “virtual host” de Apache se configura para que el directorio base de contenido web sea el directorio “/var/www/owncloud”, que es el directorio donde la instalación de OwnCloud ubica todos los ficheros de la aplicación. Además de indicar la raíz del directorio se indica que es el directorio virtual raíz al acceder al nombre del host. Esto quiere decir que al acceder por dirección IP o nombre al servidor en caso de estar configurado el DNS, no haga falta introducir “/owncloud” al final de la URL.

Más adelante, en el apartado de “*Securización de accesos a nivel de red y de servicios*” veremos los cambios necesarios en la configuración de Apache para integrar la identidad digital (certificado digital de tipo wildcard) en el servidor ClientBox, así como los cambios de configuración a realizar en Apache.

El fichero de configuración de Apache, donde se indican los parámetros del virtual host de Apache queda de la forma que se muestra en la *Imagen 10*, teniendo en cuenta que no se ha realizado aún la integración con OpenSSL ni con el certificado digital de ClientCorp (el servicio OwnCloud se sirve a través del puerto tcp/80 del servidor):

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/owncloud
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    LogLevel warn
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Imagen 10: Configuración de VirtualHost de OwnCloud.

Hay que tener en cuenta que una vez se ha preconfigurado Apache, el servidor web va a estar publicando por el puerto tcp/80 la página de configuración de OwnCloud. En dicha página de configuración se introducen los datos de la base de datos a utilizar (motor MySQL, base de datos "owncloud"; usuario "owncloud" y contraseña la que se haya definido). Adicionalmente se introduce nombre y contraseña de la nueva cuenta de administración a usar por el servicio de OwnCloud (la crea el propio sistema y es una cuenta que se almacena en base de datos).

Los parámetros de la configuración inicial y básica de OwnCloud quedan como se muestra en la siguiente figura:

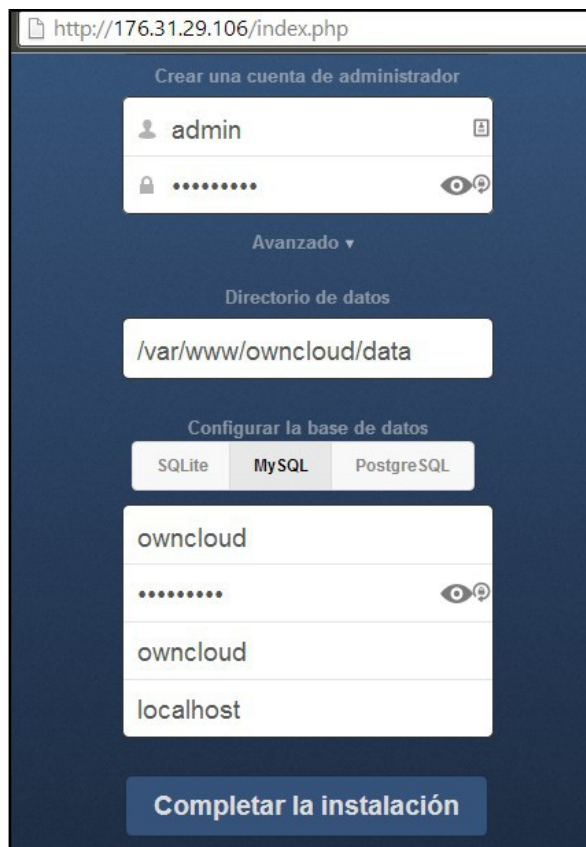


Imagen 11: Configuración inicial de OwnCloud.

5.2. Integración de la solución con los sistemas existentes

5.2.1. Integración con el sistema de directorio de usuarios y de correo electrónico

La integración del sistema de directorio de usuarios con OwnCloud tiene dos fases: la primera es habilitar el módulo de acceso a directorios de usuarios externos de OwnCloud y la segunda consta del proceso de configuración de dicho módulo:

- Para habilitar el módulo de acceso a directorios de usuarios externos (o distintos a los usuarios definidos internamente en OwnCloud), se accede al servicio mediante la consola web, y se habilita la aplicación denominada “LDAP user and group backend”. Este módulo permite utilizar datos de usuarios de directorios externos, bien sean OpenLDAP o de Directorio Activo de Windows. Como se ha comentado anteriormente, ha sido necesario instalar manualmente el módulo php5-ldap de forma manual, utilizando el gestor de paquetes APT.
- Una vez habilitado el módulo de acceso a directorios de usuarios externos, es necesario configurarlo para acceder a los datos de los usuarios de ClientCorp. Los datos necesarios para configurarlo correctamente, además de host,

La configuración necesaria a introducir en OwnCloud para la correcta integración con el directorio de usuarios es la mostrada en la siguiente secuencia de imágenes, teniendo en cuenta que se está conectando contra el servidor Proxy LDAP (no contra el directorio en OpenLDAP de producción):

- Configuración de la conexión contra ProxyLDAP, indicando puerto, usuario de conexión y base de lectura del directorio:

The screenshot shows the LDAP configuration interface in OwnCloud. It features a dark blue header with four tabs: 'Server', 'User Filter', 'Login Filter', and 'Group Filter'. The 'Server' tab is selected. Below the tabs, there is a dropdown menu showing '1. Server: 176.31.29.106' and a 'Delete Configuration' button. The main configuration area contains several input fields: a text field with '176.31.29.106' and a '38' icon, a text field with 'cn=admin,dc=clientcorp,dc=com', a password field with masked characters and a 'lock' icon, and a text field with 'dc=clientcorp,dc=com'. At the bottom right, there is a status indicator 'Configuración OK' with a green dot, a 'Continuar' button, and an 'Ayuda' link.

Imagen 12: Configuración de conexión al ProxyLDAP

- Configuración de los tipos de objetos de LDAP que serán considerados por OwnCloud como usuarios válidos:



Server User Filter Login Filter Group Filter

Limitar el acceso a ownCloud a los usuarios que cumplan el siguiente criterio:

solamente de estas clases de objeto:

solamente de estos grupos:

↓ Editar el filtro en bruto en su lugar

Usuarios 7 encontrados

Configuración OK ●

Imagen 13: Configuración de correlación de campo de objetos de tipo usuario

- Configuración de los tipos de objetos de LDAP que serán considerados por OwnCloud como grupos válidos:



Server User Filter Login Filter Group Filter

Limitar el acceso a ownCloud a los grupos que cumplan este criterio:

solamente de estas clases de objeto:

solamente de estos grupos:

↓ Editar el filtro en bruto en su lugar

Grupos 2 encontrados

Configuración OK ●

Imagen 14: Configuración de correlación de campo de objetos de tipo usuario

- Configuración del campo de LDAP que será considerado o “mapeado” al campo E-mail dentro de OwnCloud:

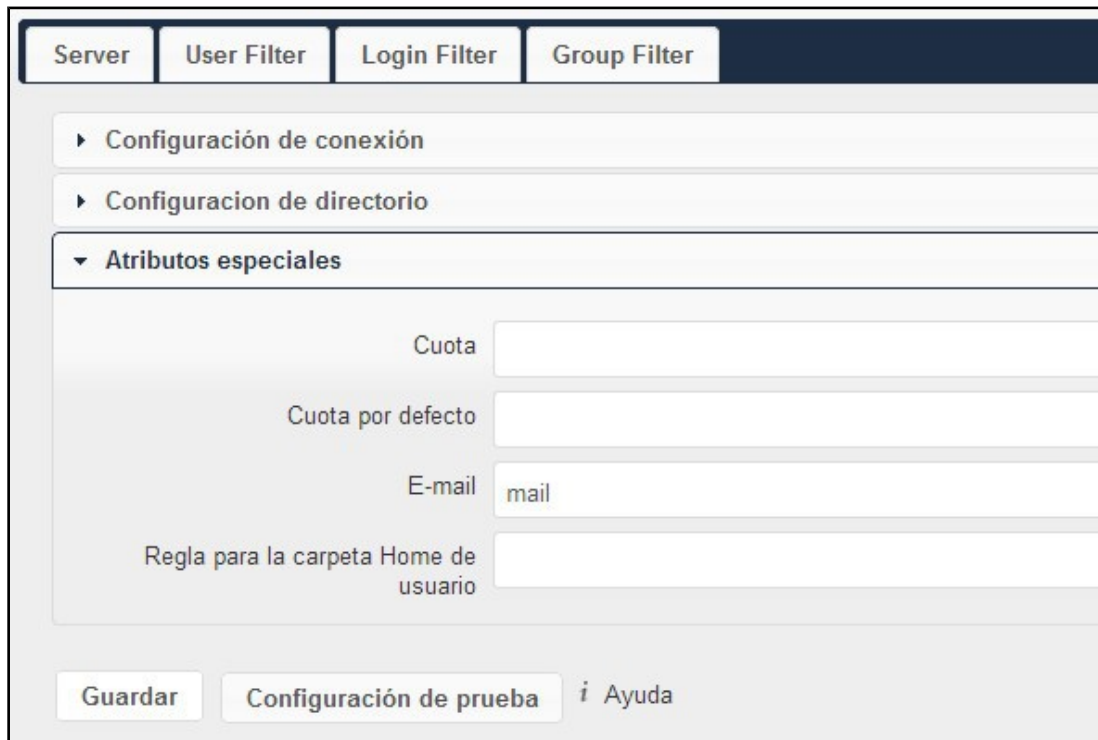


Imagen 15: Configuración de correlación de campo e-mail.

Adicionalmente, es necesario tener en cuenta que las cuentas de usuario también pueden ser externas al directorio corporativo de usuarios, es decir, se pueden definir cuentas de usuario de OwnCloud que se almacenarán en su base de datos, cuya gestión realiza el usuario administrador a través del panel de gestión web de la aplicación: pertenencia a grupos, administración de grupos, cuota, nombre de usuario y contraseña.

Para la integración con el sistema de correo electrónico de ClientCorp, únicamente es necesario modificar el fichero `/var/www/owncloud/config/config.php` e indicar los datos de conexión con el servidor corporativo de correo electrónico de ClientCorp, como se puede ver en la Imagen 16:

```
'mail_smtpdebug' => true,
'mail_smtpmode' => 'smtp',
'mail_smtp host' => 'correo.clientcorp.com',
'mail_smtpport' => 25,
'mail_smtp timeout' => 10,
'mail_smtpsecure' => 'tls',
'mail_smtpauth' => true,
'mail_smtpauth type' => 'LOGIN',
'mail_smtpname' => 'clientbox',
'mail_smtppassword' => 'p@ssw0rd',
```

Imagen 16: Configuración de conexión con el servidor de correo electrónico corporativo.

5.2.2. Integración con la identidad digital de la empresa (certificados digitales)

La integración con la identidad digital de la empresa pasa por la correcta configuración del certificado digital de la ClientCorp en el servidor web Apache de ClientBox.

La instalación de OpenSSL es necesaria para que Apache pueda servir páginas web a través del puerto seguro SSL, que es justo lo que se desea.

Como se puede ver a continuación, la única configuración necesaria a realizar es indicar al servidor web Apache dónde están los certificados digitales dentro de la configuración del VirtualHost que sirve por el puerto 443:

```
<VirtualHost *:443>
  ServerName box.clientbox.com
  SSLEngine on
  SSLCertificateFile /etc/ssl/crt/cliencorp_comt.crt
  SSLCertificateKeyFile /etc/ssl/key/clientcorp_com.key
  SSLCertificateChainFile /etc/ssl/crt/clientcorp_com_CA.crt
  DocumentRoot /var/www/owncloud
  CustomLog /var/www/logs/ssl-access_log combined
  ErrorLog /var/www/logs/ssl-error_log
</VirtualHost>
```

Imagen 17: Configuración de Apache para utilización de certificado de ClientCorp.

De esta forma veremos que las conexiones realizadas con el servidor ClientBox a través del puerto seguro SSL estarán cifradas y correctamente verificadas por VeriSign (CA que firma el certificado digital de ClientCorp).

5.3. Securización del sistema de trabajo colaborativo

El sistema ClientBox puede securizarse a varios niveles: se puede proteger el sistema y el acceso indebido a datos (con posible fuga o corrupción de datos), y se puede proteger los datos como tal, para que otro usuario que no sea su propietario no pueda ver su contenido, mediante técnicas de encriptación,

A continuación analizamos los dos niveles de protección de la información a implementar en ClientBox;

5.3.1. Securización de accesos a nivel de red y de servicios

El servidor trabaja con un Sistema Operativo Linux, específicamente una distribución Debian 7 de 64 bits. Aunque estos sistemas son difícilmente afectados por software intruso, como gusanos, troyanos o virus, es siempre muy recomendable la instalación de protección antivirus en el mismo.

En el caso de ClientBox, se opta por la instalación del software ClamAV, en modo demonio y con actualizaciones periódicas de las firmas de virus. Dicho software se instala mediante el gestor de paquetes Aptitude, como el resto de software instalado en el servidor ClientBox.

5.3.2. Securización de datos

El servidor ClientBox contiene datos confidenciales de los usuarios de dicho sistema, y es una situación que ha de controlarse para evitar que los datos de cualquier usuario puedan ser robados y utilizados.

La solución a la problemática indicada pasa por encriptar los datos que los usuarios sincronizan, mediante el agente de sincronización o la interfaz web, con el servidor ClientBox.

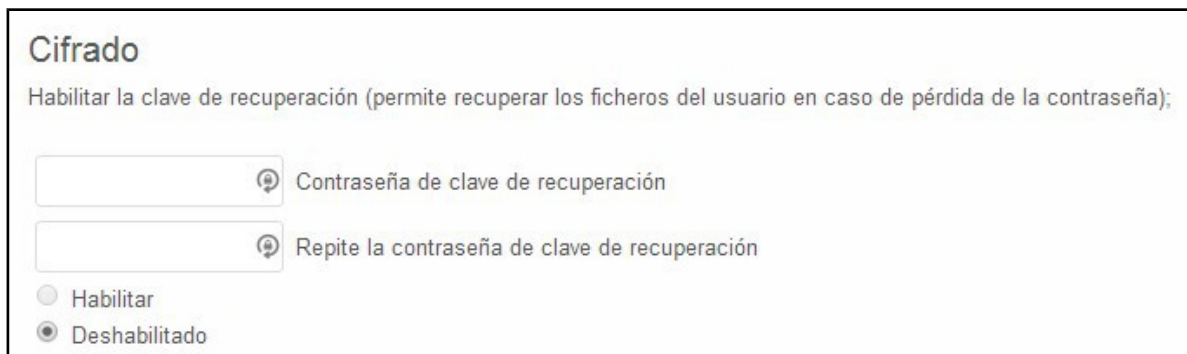
La aplicación OwnCloud viene con una aplicación o módulo de encriptación, que para ser activado simplemente hace falta ser administrador del sistema y habilitar dicho módulo o aplicación, como se puede ver a continuación:




Imagen 17: Activación de módulo de encriptación.


La encriptación permite que únicamente el usuario propietario del fichero pueda abrirlo. Para ello, necesita la clave privada del usuario y la contraseña del mismo. Sin dicha contraseña no se puede acceder al fichero, excepto cuando se comparte el fichero con otro usuario, en cuyo caso se permite que la clave del usuario con el que se comparte dicho fichero permita descriptarlo, para que el usuario tenga acceso a él.

Además, OwnCloud permite que se configure una contraseña de recuperación maestra de ficheros de usuarios, para el caso en el que algún usuario pierde su contraseña y necesite acceder a sus ficheros. Dicha configuración sólo se le permite al administrador del sistema:



Cifrado
Habilitar la clave de recuperación (permite recuperar los ficheros del usuario en caso de pérdida de la contraseña);

 Contraseña de clave de recuperación

 Repite la contraseña de clave de recuperación

Habilitar

Deshabilitado

Imagen 18: Configuración de contraseña maestra de recuperación de ficheros encriptados.

5.4. Configuraciones especiales

Hay dos tipos de configuraciones a realizar en la aplicación para adaptarla a los requisitos puestos por el cliente. Dichas configuraciones son propias de la interfaz web, y otras configuraciones que modifican comportamientos de interacción con usuarios (configuraciones distintas al comportamiento de la web al presentar datos).

5.4.1. Adaptación de interfaz web

La adaptación de la interfaz web de OwnCloud a la imagen corporativa de ClientCorp se basa en adaptar a las distintas pantallas los logos y colores corporativos de la misma.

Vemos punto a punto las configuraciones que se han de modificar para llevar a cabo la adaptación de la interfaz web a la necesaria por ClientCorp:

- **Paso previo:** copiar los logos en tamaño mediano y tamaño pequeño en el directorio siguiente del servidor:
 - Directorio de imágenes: `/var/www/owncloud/core/img`
- **Adaptar logo de la pantalla de login:**
 - Fichero: `/var/www/owncloud/core/templates/layout.guest.php`

- Código fuente adaptado:

```
<body id="body-login">
  <div class="wrapper"><!-- for sticky footer -->
    <header><div id="header">
      getName()); ?>" />
```

- **Adaptar logo en las pantallas de navegación:**

- Fichero: /var/www/owncloud/core/templates/layout.user.php
- Código fuente adaptado:

```
<header><div id="header">
  <a href="<?php print_unescaped(link_to('',
'index.php')); ?>" title="" id="owncloud">getName()); ?>" /></a>
```

- **Adaptar logo en la pantalla de acceso a ficheros compartidos por enlace:**

- Fichero: /var/www/owncloud/apps/files_sharing/templates/public.php
- Código fuente adaptado:

```
<header><div id="header" class="icon icon-noise <?php
p((isset($_['folder']) ? 'share-folder' : 'share-file')) ?>">
  <a href="<?php print_unescaped(link_to('', 'index.php')); ?>"
title="" id="owncloud">getName()); ?>" /></a>
```

- **Adaptar colores en la pantalla de login (por tipo de navegador):**

- Fichero: /var/www/owncloud/core/css/styles.css
- Código fuente adaptado:

```
/* HEADERS */
#body-user #header, #body-settings #header {
  position:fixed; top:0; left:0; right:0; z-index:100; height:45px;
line-height:2.5em;
  background:#1d2d44 url('../img/noise.png') repeat;
}
#body-login {
  text-align: center;
  background: #ffffff; /* Old browsers */
  background: url('../img/noise.png'), -moz-linear-gradient(top,
#ffffff 40%, #1d2d44 100%); /* FF3.6+ */
  background: url('../img/noise.png'), -webkit-gradient(linear, left
top, left bottom, color-stop(40%,#ffffff), color-stop(100%,#1
d2d44)); /* Chrome,Safari4+ */
  background: url('../img/noise.png'), -webkit-linear-gradient(top,
#ffffff 40%,#1d2d44 100%); /* Chrome10+,Safari5.1+ */
  background: url('../img/noise.png'), -o-linear-gradient(top,
#ffffff 40%,#1d2d44 100%); /* Opera11.10+ */
  background: url('../img/noise.png'), -ms-linear-gradient(top,
#ffffff 40%,#1d2d44 100%); /* IE10+ */
  background: url('../img/noise.png'), linear-gradient(top, #ffffff
40%,#1d2d44 100%); /* W3C */
  filter:
progid:DXImageTransform.Microsoft.gradient( startColorstr='#ffffff',
endColorstr='#1d2d44',GradientType=0 ); /* IE6-9 */
}
```

- **Adaptar llamadas a instancia para el Footer, Título y Disclaimers:**

- Fichero: /var/www/owncloud/lib/private/defaults.php
- Código fuente adaptado:

```
function __construct() {
    $this->l = OC_L10N::get('core');

    $this->defaultEntity = "ClientCorp"; /* e.g. company name, used
for footers and copyright notices */
    $this->defaultName = "ClientBox"; /* short name, used when
referring to the software */
    $this->defaultTitle = "ClientBox"; /* can be a longer name, for
titles */
    $this->defaultBaseUrl = "http://clientcorp.com";
    $this->defaultSyncClientUrl = " http://owncloud.org/sync-clients/";
    $this->defaultDocBaseUrl = "http://doc.owncloud.org";
    $this->defaultSlogan = $this->l->t("Servicio web");
    $this->defaultLogoClaim = "";

    if (class_exists("OC_Theme")) {
        $this->theme = new OC_Theme();
    }
}
```

5.4.2. Adaptación de elementos de interacción con usuarios

La adaptación de elementos de ClientCorp que interaccionan con los usuarios son variados: van desde el comportamiento del envío de notificaciones personalizadas a los usuarios hasta el comportamiento de la aplicación al intentar compartir un fichero.

Vemos punto a punto las configuraciones que se han de modificar para llevar a cabo la adaptación de elementos de interacción con usuarios:

- **Adaptar remitente de los correos electrónicos:**

- Fichero: /var/www/owncloud/lib/public/util.php
- Código fuente adaptado:

```
public static function getDefaultEmailAddress($user_part) {
    return 'clientbox@clientcorp.com';
}
```

- **Adaptar mensaje de e-mail al compartir ficheros:**

- Fichero: /var/www/owncloud/core/templates/mail.php
- Código fuente adaptado:

```
<?php
print_unescaped($l->t('Hey there,<br><br>just letting you know that %s
shared »s« with you.<br><a href="%s">View it!</a><br><br>',
array($_['user_displayname'], $_['filename'], $_['link']));
if ( isset($_['expiration']) ) {
    p($l->t("The share will expire on %s.", array($_['expiration'])));
    print_unescaped('<br><br>');
}
p($l->t('Cheers!'));
?>
```


- **Adaptar comportamiento para evitar que usuarios puedan modificar información personal protegida:**

- Fichero: /var/www/owncloud/settings/personal.php
- Código fuente adaptado:

```
$tmpl = new OC_Template( 'settings', 'personal', 'user');
$tpl->assign('usage', OC_Helper::humanFileSize($storageInfo['used']));
$tpl->assign('total_space',
OC_Helper::humanFileSize($storageInfo['total']));
$tpl->assign('usage_relative', $storageInfo['relative']);
$tpl->assign('clients', $clients);
$tpl->assign('email', $email);
$tpl->assign('languages', $languages);
$tpl->assign('commonlanguages', $commonlanguages);
$tpl->assign('activelanguage', $userLang);
$tpl->assign('enableDecryptAll', $enableDecryptAll);
$tpl->assign('enableAvatars', \OC_Config::getValue('enable_avatars',
true));
$tpl->assign('avatarChangeSupported',
OC_User::canUserChangeAvatar(OC_User::getUser()));
$tpl->printPage();
```

- **Adaptar comportamiento para evitar que se puedan compartir ficheros mediante enlaces sin contraseña:**

- Fichero: /var/www/owncloud/core/js/share.js
- Código fuente adaptado:

```
html += '<input type="checkbox" disabled="disabled" name="showPassword"
id="showPassword" value="1" style="display:none;" /><label
for="showPassword" style="display:none;">'+t('core', 'Password protect')
+</label>';
html += '<div id="linkPass">';
html += '<input id="linkPassText" type="password" placeholder="'+t('core',
'Password')+'"/>';
html += '</div>';
```

#Además, quitar condicional IF en:

```
$('#linkPass').show('blind');
$('#showPassword').attr('checked', true);
$('#linkPassText').attr('placeholder', '**OBLIGATORIO**');
```

- **Adaptar texto de bienvenida y de descarga de agente de sincronización:**

- Fichero: /var/www/owncloud/apps/firstrunwizard/templates/wizard.php
- Código fuente adaptado:

```
<h1><?php p($l->t('Welcome to ClientBox'));?></h1>
<?php if (OC_Util::getEditionString() === ''): ?>
<p><?php p($l->t('Personal Cloud of CLIENTCORP.'));?></p>
<?php else: ?>
<p><?php p($theme->getSlogan()); ?></p>
<?php endif; ?>
```

- **Adaptar traducción del mensaje de bienvenida:**

- Fichero: /var/www/owncloud/apps/firstrunwizard/l10n/es.php
- Código fuente adaptado:

```
<?php $TRANSLATIONS = array(
```

```
"Welcome to ClientBox" => "Bienvenido a ClientBox",
"Your personal Cloud of CLIENTCORP." => "Su nube personal de CLIENTCORP.",
"Get the apps to sync your files" => "Obtenga las apps para sincronizar sus
archivos",
"Connect your desktop apps to ownCloud" => "Conecte sus aplicaciones de
escritorio a ownCloud",
"Connect your Calendar" => "Conecte su Calendario",
"Connect your Contacts" => "Conecte sus Contactos",
"Access files via WebDAV" => "Acceda a sus archivos vía WebDAV",
```

6. PROCESO DE IMPLANTACIÓN E INTEGRACIÓN

A continuación se realiza un detalle técnico de las tareas enumeradas en la planificación del proyecto (representada en el gráfico de Gantt), desde la adecuación básica del entorno hasta la puesta en marcha del sistema y ejecución de pruebas sobre el mismo.

Las tareas definidas son las siguientes (las dependencias entre ellas se pueden comprobar gráficamente en la *Imagen 1: Gráfico de Gantt*, siendo las subtareas de las tareas “Adecuación de la infraestructura existente”, “Instalación y configuración del sistema a integrar” e “Integración con sistemas de la empresa”:

TAREA 1	Adaptación del directorio de usuarios
Descripción:	<ul style="list-style-type: none"> Preparación de OU's o ramas del directorio que ha de leer ClientBox Creación de usuario de lectura del directorio de usuarios. Creación y configuración del servidor ProxylDAP al que accederá ClientBox en modo sólo lectura desde Internet.
Responsable:	Técnico de Sistemas de ClientCorp.
Recursos necesarios:	Técnico de Sistemas de ClientCorp.
Duración:	1 día.
Resultados:	<ul style="list-style-type: none"> Se ha de tener claro qué ramas del directorio de usuarios se va a integrar. El usuario de sólo lectura del directorio de usuarios conecta en local y no puede modificar ni añadir ni eliminar datos. El usuario de lectura también puede conectarse a otro servidor, al ProxylDAP y puede leer la misma información de forma transparente (cambia la cadena de conexión al ser un host distinto).
Dependencias:	Realización del diseño técnico del proyecto.

TAREA 2	Adaptación del servidor de correo electrónico
Descripción:	<ul style="list-style-type: none"> Creación de cuenta para envío de notificaciones. Creación de conector SMTP para relay de envío.
Responsable:	Técnico de Sistemas de ClientCorp.
Recursos necesarios:	Técnico de Sistemas de ClientCorp.
Duración:	1 día.
Resultados:	<ul style="list-style-type: none"> Conexión local a servidor de correo electrónico con cuenta de usuario creada y posibilidad de envíos al dominio clientcorp.com y a cualquier dominio externo.
Dependencias:	Adaptación del directorio de usuarios.

TAREA 3	Apertura de puertos y adecuación de las comunicaciones
Descripción:	<ul style="list-style-type: none"> ● Apertura de puertos para la correcta comunicación entre: <ul style="list-style-type: none"> ◦ ProxyLDAP y OpenLDAP de producción (tcp/389). ◦ Internet y ProxyLDAP (tcp/389). ◦ Internet y servidor de correo electrónico (tcp/25). ◦ Oficinas y ClientBox (tcp/443).
Responsable:	Técnico de Comunicaciones de ClientCorp.
Recursos necesarios:	Técnico de Comunicaciones de ClientCorp.
Duración:	1 día.
Resultados:	<ul style="list-style-type: none"> ● Acceso a datos de LDAP desde Internet (apuntando a ProxyLDAP). ● Correcto envío de e-mails desde servidor externo (haciendo relay en servidor de correo electrónico corporativo).
Dependencias:	Adaptación del servidor de correo electrónico.

TAREA 4	Instalación de servidor dedicado para la aplicación
Descripción:	<ul style="list-style-type: none"> ● Instalación de sistema base (sistema operativo y aplicaciones base).
Responsable:	Técnico de Sistemas de ConsultCorp.
Recursos necesarios:	Técnico de Sistemas de ConsultCorp.
Duración:	2 días.
Resultados:	<ul style="list-style-type: none"> ● Acceso por SSH a servidor ClientBox con usuarios definidos.
Dependencias:	Adecuación de la infraestructura existente.

TAREA 5	Instalación y personalización inicial de OwnCloud
Descripción:	<ul style="list-style-type: none"> ● Instalación de OwnCloud en servidor virtual dedicado y de sus dependencias. ● Configuración de entorno de base de datos para OwnCloud. ● Creación de usuario administrador.
Responsable:	Técnico de Sistemas de ConsultCorp.
Recursos necesarios:	Técnico de Sistemas de ConsultCorp.
Duración:	1 día.
Resultados:	<ul style="list-style-type: none"> ● Acceso a ClientBox mediante interfaz web con usuario administrador (almacenado en base de datos).
Dependencias:	Instalación de servidor dedicado para la aplicación.

TAREA 6	Personalización de interfaz a imagen corporativa
Descripción:	<ul style="list-style-type: none"> ● Cambio de logos de OwnCloud por logos corporativos. ● Cambio de combinación de colores de la interfaz por colores corporativos. ● Cambio de plantilla de correos electrónicos.
Responsable:	Técnico de Sistemas de ConsultCorp.
Recursos necesarios:	Técnico de Sistemas de ConsultCorp.
Duración:	2 días.
Resultados:	<ul style="list-style-type: none"> ● Se muestran los colores y logos corporativos. ● Los e-mails aparecen con la nueva plantilla.
Dependencias:	Instalación y configuración inicial de OwnCloud.

TAREA 7	Desarrollo de módulos nuevos
Descripción:	<ul style="list-style-type: none"> ● Comportamiento al compartir ficheros mediante enlace. ● Integración de módulos de mensajería, calendario y reproductores multimedia. ● Comportamiento al realizar primer acceso mediante interfaz web.
Responsable:	Desarrollador PHP de ConsultCorp.
Recursos necesarios:	Desarrollador PHP de ConsultCorp.
Duración:	5 días.
Resultados:	<ul style="list-style-type: none"> ● Código PHP a integrar en OwnCloud.
Dependencias:	Personalización de interfaz a imagen corporativa.

TAREA 8	Pruebas y validación de módulos nuevos
Descripción:	<ul style="list-style-type: none"> ● Subida de código nuevo a servidor dedicado. ● Pruebas de los módulos modificados/creados.
Responsable:	Desarrollador PHP de ConsultCorp. Técnico de Sistemas de ConsultCorp..
Recursos necesarios:	Desarrollador PHP de ConsultCorp. Técnico de Sistemas de ConsultCorp..
Duración:	2 días.
Resultados:	<ul style="list-style-type: none"> ● Solicitud de contraseña de forma obligatoria al intentar compartir un fichero mediante enlaces, esté o no encriptado el fichero a compartir. ● Aparición de módulos externos en el panel de aplicaciones de ClientBox.
Dependencias:	Desarrollo de módulos nuevos.

TAREA 9	Integración con directorio de usuarios
Descripción:	<ul style="list-style-type: none"> Configurar ClientBox para que lea la rama base de OpenLDAP de producción a través de ProxyLDAP, con usuario y contraseña de lectura.
Responsable:	Técnico de Sistemas de ConsultCorp. Técnico de Sistemas de ClientCorp.
Recursos necesarios:	Técnico de Sistemas de ConsultCorp. Técnico de Sistemas de ClientCorp.
Duración:	2 día.
Resultados:	<ul style="list-style-type: none"> Visibilidad de usuarios que están dentro de la rama de usuarios en el apartado de Usuarios mediante una cuenta administradora de ClientBox (tener en cuenta que, para la fase piloto, no hay que dar acceso a todos los usuarios, sino a usuarios específicos seleccionados para dicha prueba piloto). Acceso mediante cuenta de dominio mediante la interfaz web.
Dependencias:	Instalación y configuración del sistema a integrar.

TAREA 10	Creación de subdominio para el servicio
Descripción:	<ul style="list-style-type: none"> Añadir registro "box.clientcorp.com" de tipo A en la configuración de DNS del dominio "clientcorp.com".
Responsable:	Técnico de Sistemas de ClientCorp.
Recursos necesarios:	Técnico de Sistemas de ClientCorp.
Duración:	1 día.
Resultados:	<ul style="list-style-type: none"> Acceso desde las redes de la compañía así como desde Internet al servicio ClientBox mediante el FQDN: box.clientcorp.com.
Dependencias:	Integración con directorio de usuarios.

TAREA 11	Instalación de certificado digital en el servidor dedicado
Descripción:	<ul style="list-style-type: none"> Copiar certificado digital y clave pública en el servidor ClientBox. Reconfigurar Apache para que escuche únicamente por través del puerto seguro SSL tcp/443,
Responsable:	Técnico de Sistemas de ConsultCorp.
Recursos necesarios:	Técnico de Sistemas de ConsultCorp.
Duración:	1 día.
Resultados:	<ul style="list-style-type: none"> Se accede correctamente a ClientBox a través de la URL: https://box.clientcorp.com, y la verificación del certificado digital es correcta (no aparece advertencia de seguridad en el navegador con el cual se ha accedido al servicio).
Dependencias:	Creación de subdominio para el servicio.

7. PLAN DE PRUEBAS Y PILOTO INICIAL

Antes de poner en producción el sistema ClientBox integrado con los sistemas de la empresa, es necesario realizar una serie de pruebas y verificar que el comportamiento del sistema como conjunto es el esperado. Para ello es necesario ejecutar la batería de pruebas que se indica en la *Tabla 2*.

Para la realización del piloto inicial, se seleccionaría un grupo de unos 5 usuarios controlados para que utilizaran el servicio ClientBox operando sobre el mismo tal y como lo haría cualquier usuario de los aproximadamente 200 que utilizarán el sistema cuando se haya puesto en producción.

El objeto de realizar un plan de pruebas que valide el sistema y un piloto inicial es poder reflejar de forma fehaciente qué funcionalidades se asegura que funcionan antes del inicio de la producción del servicio y, sobre todo, intentar descubrir fallos funcionales no detectados durante los procesos de instalación, integración e implantación antes de que sean descubiertos y notificados por usuarios del sistema una vez puesto en funcionamiento.

Las acciones que pueden llevar a cabo dichos usuarios son las también reflejadas en la misma *Tabla 2*:

Tipo de prueba	Id	Descripción de la prueba	Responsable de ejecución	Resultado de la prueba
Pruebas de instalación y configuración:	1	Acceder a https://box.clientcorp.com	Técnico de Sistemas de ConsultCorp	Se accede correctamente
	2	Hacer login con usuario local de ClientBox	Técnico de Sistemas de ConsultCorp	Login OK
	3	Hacer login con usuario de dominio	Técnico de Sistemas de ClientCorp	Login OK
	4	Verificar certificado digital en el navegador web	Técnico de Sistemas de ConsultCorp	Identidad verificada por VeriSign
	5	Comprobar login en servidor de correo electrónico con usuario dedicado a ClientBox	Técnico de Sistemas de ClientCorp	Login OK
	6	Envío de correo electrónico a dominio interno clientcorp.com con cuenta de ClientBox	Técnico de Sistemas de ClientCorp	Envío correcto
	7	Envío de correo electrónico a dominio externo con cuenta de ClientBox	Técnico de Sistemas de ClientCorp	Envío correcto
Pruebas de conectividad:	1	Acceder a https://box.clientcorp.com	Técnico de Sistemas de ConsultCorp	Se accede correctamente
	8	Acceder a interfaz web desde la red corporativa de ClientCorp	Técnico de Sistemas de ClientCorp	Se accede correctamente
	9	Acceder a interfaz web desde red distinta a la de ClientCorp	Técnico de Sistemas de ConsultCorp	Se accede correctamente
	10	Comprobar listado de usuarios leídos de ProxyLDAP en apartado de "usuarios", con usuario administrador de ClientBox	Técnico de Sistemas de ConsultCorp	Se muestran usuarios del dominio correctamente
	11	Comprobar conexión a servidor de correo electrónico desde ClientBox (telnet a su puerto 25, con login de usuario)	Técnico de Sistemas de ConsultCorp	Acceso correcto, login correcto y envío de correo correcto
	12	Comprobar conexión a servidor de correo electrónico otro servidor distinto a ClientBox (telnet a su puerto 25, con login de usuario)	Técnico de Sistemas de ConsultCorp	Acceso denegado
	6	Envío de correo electrónico a dominio interno clientcorp.com con cuenta de ClientBox	Técnico de Sistemas de ClientCorp	Envío correcto
	13	Acceso por SSH a servidor ClientCorp desde red de ConsultCorp	Técnico de Sistemas de ConsultCorp	Acceso correcto
	14	Acceso por SSH a servidor ClientCorp desde red de ClientCorp	Técnico de Sistemas de ClientCorp	Acceso correcto
	15	Acceso por SSH a servidor ClientCorp desde red distinta de ClientCorp y de ConsultCorp	Técnico de Sistemas de ConsultCorp	Acceso denegado
	1	Acceder a https://box.clientcorp.com	Técnico de Sistemas de ConsultCorp	Se accede correctamente
	3	Hacer login con usuario de dominio	Técnico de Sistemas de ClientCorp	Login OK
	16	Subir un fichero mediante la interfaz web	Técnico de Sistemas de ConsultCorp	Subida de fichero OK
	17	Crear directorio mediante la interfaz web	Técnico de Sistemas de ConsultCorp	Creación de directorio OK
	18	Creación de fichero de texto mediante la interfaz web	Técnico de Sistemas de ConsultCorp	Creación de fichero OK
19	Edición de fichero de texto a través de la interfaz web	Técnico de Sistemas de ConsultCorp	Edición de fichero OK	
20	Eliminar fichero o directorio mediante la interfaz web	Técnico de Sistemas de ConsultCorp	Eliminación OK	
Pruebas funcionales del sistema:	21	Recuperación de ficheros individuales de la papelera de reciclaje	Técnico de Sistemas de ConsultCorp	Recuperación OK
	22	Borrado de todos los elementos de la papelera de reciclaje	Técnico de Sistemas de ConsultCorp	Eliminación OK
	23	Recuperación de versión anterior de documento	Técnico de Sistemas de ConsultCorp	Recuperación OK
	24	Visualización correcta de imágenes	Técnico de Sistemas de ConsultCorp	Visualización OK
	25	Reproducción correcta de multimedia (audio y vídeos)	Técnico de Sistemas de ConsultCorp	Reproducción OK
	26	Compartición de ficheros con otros usuarios y grupos del sistema	Técnico de Sistemas de ConsultCorp	Compartición OK
	27	Compartición de ficheros a través de enlace	Técnico de Sistemas de ConsultCorp	Compartición OK
	28	Notificación por e-mail a usuario con el que se comparte un fichero	Técnico de Sistemas de ConsultCorp	Notificación OK
	29	Cambio de permisos a usuario al que se le ha compartido un fichero	Técnico de Sistemas de ConsultCorp	Cambio OK
	30	Creación de eventos en calendario	Técnico de Sistemas de ConsultCorp	Creación OK
	31	Modificación y eliminación de eventos en calendario	Técnico de Sistemas de ConsultCorp	Cambios OK
	32	Creación de contactos	Técnico de Sistemas de ConsultCorp	Creación OK
	33	Modificación y eliminación de contactos	Técnico de Sistemas de ConsultCorp	Cambios OK
	34	Visualización de actividad registrada	Técnico de Sistemas de ConsultCorp	Visualización OK
	35	Instalación de agente de sincronización	Técnico de Sistemas de ConsultCorp	Instalación OK
	35	Configuración de cuenta de usuario en agente de sincronización	Técnico de Sistemas de ConsultCorp	Configuración OK
36	Sincronización de carpetas y ficheros	Técnico de Sistemas de ConsultCorp	Sincronización OK	

Tabla 2: Plan de pruebas – Piloto inicial

8. DESPLIEGUE A USUARIOS

El despliegue de la aplicación a todos los usuarios de la compañía consta de 3 fases, que pueden describirse como tareas. Han de realizarse necesariamente de forma secuencial. Dichas tareas son las siguientes:

TAREA 12	Adecuar ClientBox para que lea todos los usuarios (no solo los del piloto)
Descripción:	<ul style="list-style-type: none"> ● Modificar la configuración de ClientBox para que lea toda la rama del directorio de usuarios de ClientCorp, no solo los de la prueba piloto.
Responsable:	Técnico de Sistemas de ClientCorp.
Recursos necesarios:	Técnico de Sistemas de ClientCorp.
Duración:	1 día.
Resultados:	<ul style="list-style-type: none"> ● Se accede correctamente a ClientBox con cuentas de usuarios que no estaban dentro del grupo de usuarios de la prueba piloto.
Dependencias:	Piloto inicial.

TAREA 13	Información a usuarios por e-mail y comunicación de manual de usuario
Descripción:	<ul style="list-style-type: none"> ● Notificar a los usuarios de la disponibilidad del nuevo servicio. ● Publicar en Intranet corporativa manual de usuarios.
Responsable:	Técnico de Sistemas de ClientCorp / Responsable de TI.
Recursos necesarios:	Técnico de Sistemas de ClientCorp / Responsable de TI.
Duración:	1 día.
Resultados:	<ul style="list-style-type: none"> ● Los usuarios reciben e-mail comunicando el nuevo servicio y pueden acceder al manual de usuario de ClientBox en la Intranet.
Dependencias:	Adecuar ClientBox para que lea todos los usuarios.

TAREA 14	Instalación desatendida de agente de sincronización (agente instalable)
Descripción:	<ul style="list-style-type: none"> ● Al acceder a la consola web, los usuarios se pueden descargar el cliente instalable para sobremesas. ● Asegurar que instalador se puede acceder desde las redes de ClientCorp.
Responsable:	Técnico de sistemas de ClientCorp / Usuarios
Recursos necesarios:	Técnico de sistemas de ClientCorp / Usuarios
Duración:	3 días.
Resultados:	<ul style="list-style-type: none"> ● Los usuarios pueden acceder, descargar el instalador e instalarlo.
Dependencias:	Información a usuarios por e-mail y comunicación de manual de usuario.

9. PLAN DE MANTENIMIENTO

El sistema ClientBox requiere de un mantenimiento continuado, ya que es un sistema de producción vivo que requiere de una alta disponibilidad y ha de tener el mayor rendimiento posible. Este mantenimiento continuado ha de llevarse a cabo de forma estricta, debido a que su función es mantener el sistema estable y evitar tener que incurrir en costes correctivos en caso de producirse fallos graves.

El plan de mantenimiento presentado por ConsultCorp para el sistema ClientBox es el que se representa en la *Tabla 3*, que consta de varias tareas de mantenimiento, llevadas a cabo por un responsable con cierta periodicidad.

Las tareas de mantenimiento del sistema son las siguientes:

Tipo de mantenimiento	Id	Tarea de mantenimiento	Responsable de ejecución	Periodicidad
Hardware	1	Mantener Hardware virtual acorde a la versión de Hypervisor Vsphere	Técnico de Sistemas de ConsultCorp	Mensual
	2	Mantener Cluster donde reside la máquina virtual correctamente balanceado	Técnico de Sistemas de ConsultCorp	Diaria
	3	Comprobar alarmas a nivel de hosts provistos por OVH y que conforman el Cluster	Técnico de Sistemas de ConsultCorp	Diaria
	4	Comprobar y solicitar actualización de sistema Hypervisor o de hosts físicos en caso de proceder	Técnico de Sistemas de ConsultCorp	Mensual
	5	Comprobación de correcta ejecución de backups de máquina virtual	Técnico de Sistemas de ConsultCorp	Diaria
Sistema Operativo	6	Revisar parámetros de monitorización de recursos (uso de CPU, de memoria, uso de discos, IOPS, estado de interfaz de red, consumo de red)	Técnico de Sistemas de ConsultCorp	Diaria
	7	Actualizar paquetes y parchear sistema operativo en caso de haber actualizaciones o parches	Técnico de Sistemas de ConsultCorp	Semanal
	8	Revisión de logs del sistema para detectar anomalías en cuanto a hardware o actividad que implique riesgo	Técnico de Sistemas de ConsultCorp	Semanal
	9	Acceso por SSH a servidor ClientCorp desde red distinta de ClientCorp y de ConsultCorp	Técnico de Sistemas de ConsultCorp	Acceso denegado
OwnCloud	10	Comprobar existencia de actualizaciones	Técnico de Sistemas de ConsultCorp	Semanal
	11	Aplicar actualizaciones de OwnCloud en entorno de test con una VM distinta	Técnico de Sistemas de ConsultCorp	Mensual
	12	Realización de cambios en personalización a imagen corporativa (logos, colores, textos)	Técnico de Sistemas de ConsultCorp / Desarrollador PHP	Bajo petición
	13	Revisión de logs de la aplicación para detectar comportamientos anómalos	Técnico de Sistemas de ConsultCorp	Semanal

Tabla 3: Plan de mantenimiento

10. ANÁLISIS ECONÓMICO: PRESUPUESTO Y ANÁLISIS DE COSTES

La implantación de la aplicación de compartición y trabajo colaborativo en ClientCorp requiere un trabajo de jefatura de proyecto, de adaptación técnica y de desarrollo.

ConsultCorp elabora dos presupuestos: uno de ellos es una única cuota, e incluye los trabajos de análisis, diseño técnico, implantación y desarrollo del sistema adaptado al entorno de ClientCorp. El segundo es una cuota mensual, renovable año a año, que incluye los trabajos contenidos en la “*Tabla 3: Plan de mantenimiento*”.

Los presupuestos emitidos por ConsultCorp son los siguientes:

	Cantidad	Precio Unitario (€)	Precio Total (€)
DIRECCIÓN Y DISEÑO			
Jefatura y dirección del proyecto	1	500	500
Realización de Diseño Técnico	1	500	500
INSTALACIÓN Y CONFIGURACIÓN			
Jefe de Proyecto (jornada)	17	150	2550
Técnico de Sistemas (jornada)	22	120	2640
Desarrollador PHP (jornadas)	5	120	600
PRECIO TOTAL (única cuota):			6790

Tabla 4: Coste de implantación

	Cantidad	Precio Unitario (€)	Precio Total (€)
MANTENIMIENTO MENSUAL			
Servidor virtual con HA y backups	1	250	250
Almacenamiento (1TB)	1	150	150
Gestión y monitorización del servicio	1	200	200
PRECIO TOTAL (cuota mensual):			600

Tabla 5: Coste de mantenimiento

Además de los costes de implantación y mantenimiento de la aplicación, ClientCorp ha de tener en cuenta que tendrá que dedicar recursos propios al proyecto. Dichos recursos se traducen en dedicación diaria de un Técnico de Sistemas y de un Técnico de Comunicaciones de la misma. Se estima que la dedicación de ambos recursos es:

- Técnico de Sistemas: 10 días.
- Técnico de Comunicaciones: 1 día.

11. CONCLUSIONES

La implantación de la solución de aplicación web para el trabajo colaborativo ha requerido de distintas fases, que como hemos venido estudiando ha implicado a personal técnico de la empresa donde se ha implantado, ClientCorp, y de la empresa integradora de servicios de IT ConsultCorp.

La aplicación ClientBox ofrece a la compañía un entorno y una forma nueva de trabajar, en la que se tiene un control centralizado sobre los datos que los usuarios consideran de importancia y sobre aplicaciones adicionales que la empresa considera que los usuarios pueden requerir, dentro del marco de la misma aplicación. El hecho de ser una solución de almacenamiento y sincronización de ficheros de los empleados de ClientCorp ofrece a los responsables del departamento de TI garantizar un nuevo nivel de control y de seguridad de dichos datos, ya que la empresa no dispone de un sistema de backup de equipos de usuarios y ClientBox, en cierta medida, puede verse también como una solución de backup “autogestionado”, en el que los usuarios deciden qué carpetas sincronizar con la aplicación y qué fichero se desea excluir de la misma, mediante reglas de excepciones (configurables a nivel de agente de sincronización).

Al final de la implantación, ClientCorp tiene en funcionamiento un sistema que facilita el trabajo entre sus empleados y entre los mismos con personas externas a la misma, con un sistema dinámico en el cual se puede modificar de forma sencilla el comportamiento de la misma para todos los usuarios, añadiendo o quitando aplicaciones disponibles. Por ejemplo, si la empresa decide potenciar el uso de su Intranet Corporativa, puede desarrollar una “app” que se integre con el resto de aplicaciones en ClientBox (panel izquierdo de aplicaciones) donde al acceder a ella puede navegar dentro de la Intranet (a través de la misma pantalla de ClientBox).

Este proyecto de implantación objeto de este Trabajo Final de Carrera evidencia que cada día más las empresas a nivel mundial están optando por una externalización de servicios, que motivada por un cambio de paradigma más que de costes, pone el punto de mira en facilitar el acceso al trabajo a los empleados y en centralizar los datos de los mismos. Esto mismo también se está viviendo en otro tipo de software, como por ejemplo los cada día más fuertes softwares de virtualización de puestos de trabajo, en el que se centraliza el entorno de trabajo y los datos que los usuarios manejan en una única plataforma central, donde los responsables de TI tienen el control de los datos, cambiando de esta forma la forma de trabajar habitual, en el que los usuarios ejercen control sobre sus datos.

12. GLOSARIO

- **CA:** Certification Authority (Entidad Certificadora). Organismo responsable de emitir y revocar certificados digitales.
- **Cloud:** Computación en la nube. Paradigma que permite ofrecer servicios informáticos de computación a través de Internet.
- **DNS:** Domain Name System (Sistema de Nombres de Dominio). Sistema donde se almacena información IP a nombres de dominios (o subdominios). Un registro de tipo A es un registro de dirección.
- **FQDN:** Fully Qualified Domain Name (Nombre Completo de Dominio). Nombre de host/computador y su nombre de dominio asociado.
- **HA:** High Availability (Alta Disponibilidad). Se refiere a la capacidad de un sistema de mantenerse en funcionamiento mediante distintos mecanismos, ante cualquier eventualidad.
- **Hipervisor:** Sistema que permite la gestión de sistemas de virtualización.
- **PHP:** Hypertext Preprocessor. Lenguaje de programación de código abierto orientado al desarrollo web.

13. BIBLIOGRAFÍA

- **Fuente:** Wikipedia. “*Computación en la nube*” (2014).
http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube
- **Fuente:** Gartner. “*MarketScope for Enterprise File Synchronization and Sharing*” (2013).
<http://www.satisnet.co.uk/pdfs/Gartner-MarketScope-EFSS-Feb2013.pdf>
- **Fuente:** Gartner. “*Gartner Identifies the Top 10 Strategic Technology Trends for 2013*” (2012).
<http://www.gartner.com/newsroom/id/2209615>
- **Fuente:** OVH. “*Dedicated Cloud*” (2014).
<http://www.ovh.es/dedicated-cloud/>
- **Fuente:** OwnCloud (2014).
<http://owncloud.org>
- **Fuente:** GitHub. Repositorio de código de OwnCloud (2014).
<https://github.com/owncloud>
- **Fuente:** PHP. “*PHP Manual*” (2014).
<https://www.php.net/manual/en/>