PROYECTO DE RED INFORMATICA CORPORATIVA PARA EMPRESA COMERCIALIZADORA DE ELECTRICIDAD

JORGE GARCÍA MOLINERO
I.T. INFORMÁTICA DE SISTEMAS

jgarciamolin@uoc.edu

Consultor responsable
J.Ramón Esteban Grifoll

DEDICATORIA Y AGRADECIMIENTOS

A todas las personas que me han ayudado y a las que me desanimaron, ya que me dieron más fuerzas para continuar y llegar hasta este momento.

A mis consultores, profesores y tutores por sus conocimientos, paciencia y respuestas a mis dudas.

A mi familia y amigos.

A mis Valles.

RESUMEN

El presente TFC está enmarcado en el contexto de análisis y desarrollo de una infraestructura de red tipo. Tomando como modelo, la empresa ***DC Energía,*** empresa de nueva creación que se dedicará como tarea principal a la comercialización de energía eléctrica y productos derivados de ésta. El presente TFC estudiará la problemática actual de la empresa, analizando los requerimientos de la misma, partiendo de unos requerimientos iniciales, para la elaboración del TFC en base a éstos. Dichos requerimientos iniciales se detallarán convenientemente y contemplarán básicamente la siguiente información:

- Estructura física de las instalaciones de la empresa.
- Estructura departamental necesaria en la empresa. Estructura lógica.
- Servicios necesarios para la organización.
- Requerimientos de acceso por personal de la empresa que trabaja de forma descentralizada a la misma.
- Requerimientos de acceso interno a la red corporativa.
- Requerimientos VPN y WIFI.

Mediante el presente TFC se pretende dar una solución a la infraestructura de red necesaria para la empresa, ajustada en la medida de lo posible al presupuesto destinado para la misma. Así mismo, se ponen en práctica todos los conocimientos adquiridos en las asignaturas de redes de computadores, estructura de redes de computadores y seguridad de redes de computadores de la carrera de Ingeniería Técnica en Informática de Sistemas.

Este TFC planteará una posible solución detallada a los requerimientos de la empresa, tanto para la estructura física y lógica de la red. Se analizarán sistemas de virtualización actuales que puedan servir como solución a la infraestructura de servidores necesaria y mecanismos de copia de seguridad aplicables a esta infraestructura de red, además, se establecerán unas pautas de seguridad básicas a tener en cuenta a la hora de la implantación de la red.

La infraestructura de la red, afectará a todos los departamentos de la empresa, y el éxito de la misma puede depender de una forma directa de las decisiones que se tomen inicialmente en la planificación de esta estructura y del coste que suponga la implantación definitiva.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

1 INTRODUCCION.

Desde la liberación del mercado de la electricidad en el año 2007 (aunque finalmente se regula por la nueva ley del sector eléctrico 24/2013, aprobada en diciembre de 2013), el sector eléctrico está actualmente organizado en dos tipos de actividades:

- Actividades parcialmente liberalizadas (generación y comercialización)
- Actividades reguladas (transporte y distribución)

Las actividades liberalizadas, con el nuevo marco legal, pueden ser realizadas por cualquier agente libre, similar a cualquier otra actividad comercial, sin embargo las actividades reguladas resultan en la actualidad de la existencia de monopolios naturales (transporte y distribución), los cuales necesitan de una autorización y supervisión administrativa específica.

Centrándose en el tipo de actividades liberalizadas, a raíz de la liberalización del sector eléctrico, están surgiendo numerosas compañías comercializadoras de electricidad, con capacidad de suministrar energía eléctrica al cliente final.

Una de estas compañías comercializadora de electricidad es **DC Energía** (compañía ficticia, basada en una empresa real), la cual necesita una infraestructura de red, que le ayude a conseguir el máximo beneficio con el menor coste de inversión posible, y que cumpla con las mayores garantías en cuanto a seguridad, debido a la problemática actual, en cuanto al manejo de información y tránsito de la misma a través de internet.

Las empresas actuales, debido a la situación económica actual, buscan la optimización de sus propios recursos, infraestructuras tecnológicas, centralización de la información (si tienen centros dispersos), e integración del software.

Además la empresa para proporcionar una atención de calidad a sus clientes, necesitará del uso de un portal corporativo (o varios) con el máximo número de servicios web, aprovechando que hoy en día existe un porcentaje muy alto de acceso a internet con banda ancha. Por este motivo se deberá estudiar correctamente la implementación física de la red, para garantizar al máximo los requerimientos internos de la empresa, así como de cara a sus clientes.

En el estudio de la red se analizarán las posibilidades de virtualización de los servidores de la empresa, así como sistemas de copias de seguridad, escalabilidad de la información, y en definitiva todos aquellos aspectos que puedan ser adecuados para la infraestructura.

Por otro lado, se plantearán algunas pautas en cuanto a la seguridad de la red, tomados como base en la implantación inicial. Estos mecanismos podrán ser ampliados en un futuro.

Los costes de estas medidas deberán analizarse desde una perspectiva general, analizando las posibilidades desde el hardware físico, como analizando las posibilidades en software libre, para abaratar los posibles costes de la infraestructura necesaria.

1.1 JUSTIFICACION DEL TFC.

Hoy en día cualquier organización o empresa mediana requiere de una infraestructura de red corporativa acorde con los objetivos de la empresa. Esta infraestructura deberá estar optimizada correctamente, para obtener el máximo beneficio con el mínimo coste de inversión.

Mediante este proyecto se tomará como modelo los requerimientos de la empresa y se planteará una posible solución a los mismos.

La implantación de la red en cualquier empresa de nueva creación debería realizarse tras el estudio de un proyecto similar a este.

1.2 OBJETIVOS DEL TFC.

Los objetivos principales del presente TFC, son los siguientes:

- Garantizar la disponibilidad de servicios según el acuerdo de nivel establecido (LSA) con la empresa, y sin que ello represente ningún coste adicional de licencias asociado para los próximos 5 años.
- El coste de la infraestructura final de la red de la empresa no podrá superar el presupuesto destinado por la misma para este fin establecido en 30.000 €.
- Garantizar la escalabilidad de la información como mínimo a 5 años, prever el volumen de información a almacenar en los servidores durante este rango de tiempo, sin inversión adicional.
- Establecer un sistema de copias de seguridad que permita recuperar la mayor parte de la información sensible, ante posibles pérdidas.
- La infraestructura de red implementada deberá preservar la confidencialidad, integridad y disponibilidad de la información alojada en los servidores, protegiendo a éstos de accesos no deseados desde el interior o exterior de la red.

1.3 ENFOQUE Y METODOLOGIA SEGUIDA.

Como se ha comentado en los puntos anteriores el enfoque del proyecto se hará en base a la perspectiva del cliente, analizando los requerimientos y problemáticas de éste que desembocarán en una solución con posibles alternativas ajustadas al presupuesto de dicho cliente.

El método seguido para la elaboración del presente TFC en líneas generales se desglosa a continuación:

- Análisis de requerimientos.
    - Distribución física de las instalaciones.
    - Estructura departamental de la empresa.
    - Servicios necesarios en la organización.
    - Requerimientos de acceso a la red interna.
    - Requerimientos de acceso externo.
- Soluciones propuestas.
    - Estructura física de la red.
    - Estructura lógica.
    - Servidores necesarios.
    - Recomendación de virtualización y aplicación a la infraestructura.
    - Copias de seguridad.
    - Red Wi-fi.
    - Acceso remoto.
    - Seguridad de la red.
- Valoración económica de la solución.
- Conclusión.

1.4 PLANIFICACIÓN DEL PROYECTO.

El desglose temporal del TFC queda clarificado en el siguiente diagrama de Gantt, separado por tareas, y asignación de espacio temporal.

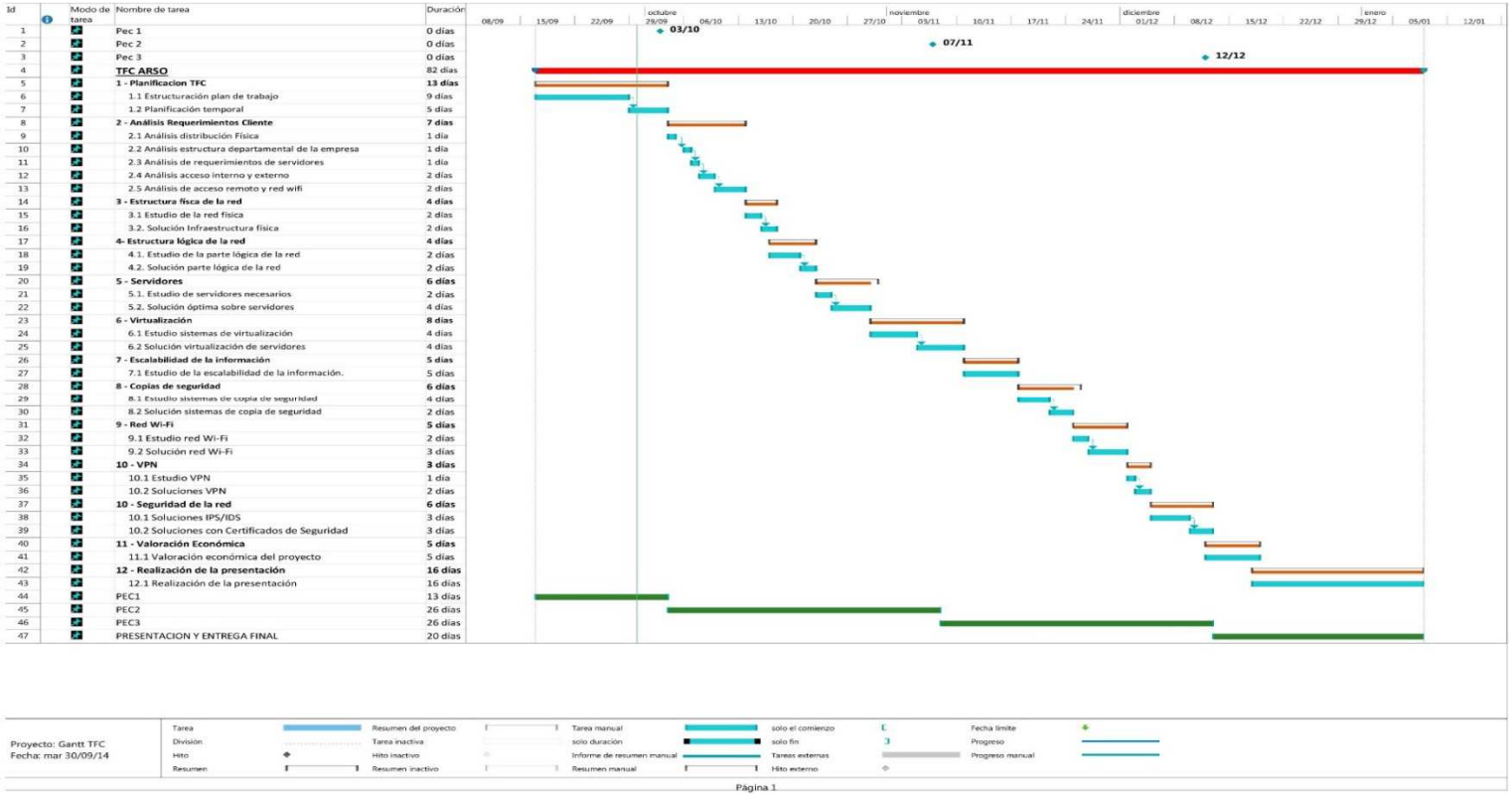

Figura 1-1 Diagrama de Gantt del Proyecto

2 REQUERIMIENTOS.

2.1 DISTRIBUCION FÍSICA DE LAS INSTALACIONES.

La empresa dispone de unas instalaciones físicas ubicadas en un polígono industrial de la ciudad. El edificio principal de la empresa está compuesto de 3 plantas de aproximadamente 120 m^2 cada una, además se dispone de un edificio anexo separado del edificio principal por unos 300 metros de distancia.

Este edificio anexo tiene 1 planta de unos 200 m^2 y se pretende utilizar como sala de reuniones, convenciones y formación, con capacidad para unas 50 personas.

Todas las plantas del edificio principal disponen de una altura de 3 metros, distribuidas en una estructura de tipo departamental, separadas por habitaciones.

Cada planta dispone de una zona de comunicaciones, donde se ubicarán todos los equipos necesarios por planta, y por donde se distribuirá el cableado correspondiente para comunicar cada una de ellas entre sí verticalmente. El cableado estructurado se distribuirá por el falso techo, a través de bandeja metálica, que ya se encuentra instalada.

En la planta inferior junto a la habitación de comunicaciones, estará ubicada la de servidores, junto al departamento de informática.

En los siguientes apartados se hará una descripción exacta de la estructura por departamentos de la empresa, junto con la distribución de los diferentes equipos, etc.

2.2 ESTRUCTURA DEPARTAMENTAL DE LA EMPRESA.

La estructura departamental de la empresa (por planta) sería la siguiente:

Primera planta:

- Recepción.
- Departamento de Informática.
- Departamento Comercial y atención al agente.

Figura 2-1 Edificio Principal - Planta Primera.

Segunda Planta

- Atención al cliente (Call-Center).
- Departamento de administración.
- Departamento de Operaciones.

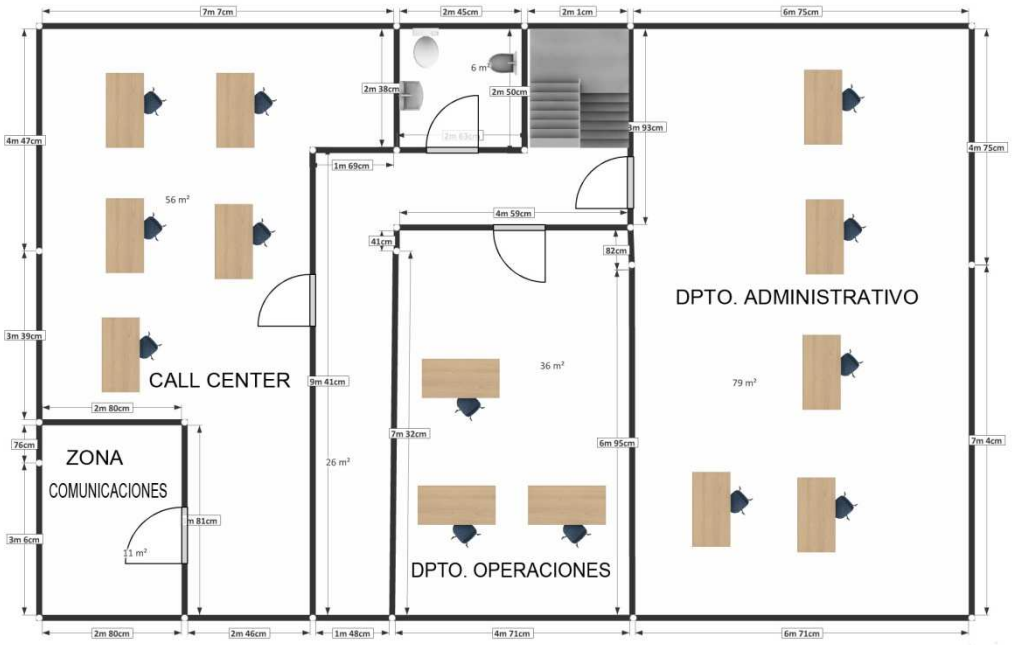

Figura 2-2 Edificio Principal - Planta Segunda.

Tercera Planta

- Dirección.
- Contabilidad.
- Marketing y publicidad.
- Formación.

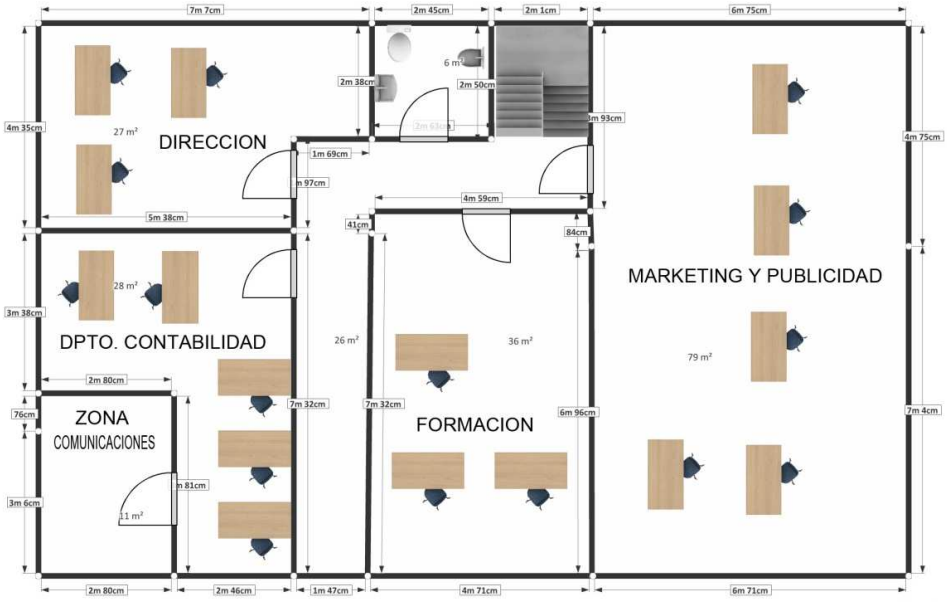

Figura 2-3 Edificio Principal - Planta Tercera

Edificio Anexo

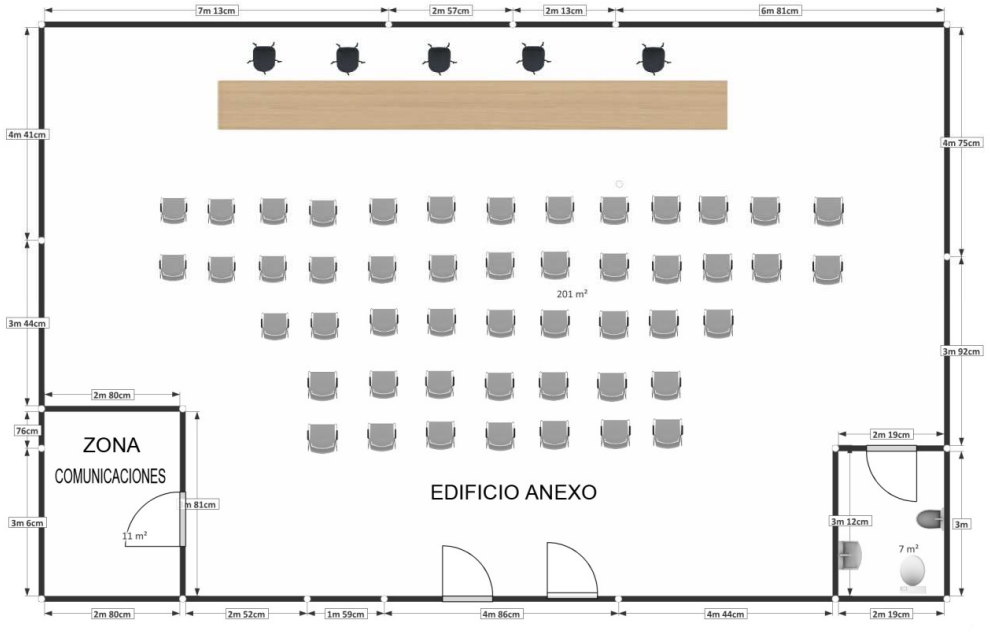

Figura 2-4 - Edifico Anexo

Departamentos

- Recepción: estará formado por una persona, será la encargada de recibir las visitas a la empresa.
- Departamento de Informática: estará formado por 5 personas, se encargarán de dar soporte a la red corporativa, y mantenimiento de servidores y aplicaciones.
- Departamento Comercial y atención al agente: estará formado por cinco personas, serán los encargados de resolver las incidencias de la red de agentes comerciales de la compañía.
- Departamento de atención al cliente (call center): estará formado por cinco personas, y serán los encargado de atender las incidencias del cliente final.
- Departamento de administración: estará formado por 5 personas, y serán los encargados de realizar la facturación al cliente final, y de la liquidación de comisiones a los agentes comerciales.
- Departamento de operaciones: estará formado por 3 personas, que serían las encargadas de resolver las incidencias con las diferentes distribuidoras de electricidad y de la compra en el mercado eléctrico de los Kilovatios necesarios para dar servicio a los clientes propios.

- Dirección: estará formado por 3 personas, serán los encargados de las relaciones a nivel de institución.
- Contabilidad: estará formado por 5 personas, serán los encargados de la contabilidad interna de la empresa.
- Marketing y publicidad: estará formado por 5 personas, serán los encargados del mantenimiento de la web corporativa, creación de nuevos productos y publicidad de la empresa.
- Formación: estará formado por 3 personas, las cuales serán las encargadas de dar la formación adecuada a los agentes comerciales. Aunque el personal de formación estará ubicado en las instalaciones del edificio principal, la formación física se realizará en el edificio anexo.

Resumen de puestos de trabajo.

DEPARTAMENTO	*Nº PUESTOS PREVISTOS (INICIALES)*
RECEPCION	*1 PUESTO*
DPTO. INFORMATICA	*5 PUESTOS*
DPTO. COMERCIAL	*5 PUESTOS*
DPTO. CALL CENTER	*5 PUESTOS*
DPTO. ADMINISTRACION	*5 PUESTOS*
DPTO. OPERACIONES	*3 PUESTOS*
DPTO. DIRECCION	*3 PUESTOS*
DPTO. CONTABILIDAD	*5 PUESTOS*
DPTO. MARKETING Y PUBLICIDAD	*5 PUESTOS*
DPTO. FORMACION	*3 PUESTOS*
TOTAL PUESTOS	*40 PUESTOS*

Tabla 1 - DESGLOSE PUESTOS DE TRABAJO

2.3 SERVICIOS NECESARIOS EN LA ORGANIZACIÓN.

Como se ha comentado anteriormente la empresa **D.C. Energía** se dedica principalmente a la comercialización de energía eléctrica. La empresa dispone de una red comercial externa, la cual nutre de clientes a la empresa, aunque también el cliente de forma directa puede contactar con la compañía para contratar los servicios proporcionados por ésta, ya sea a través de su portal en internet, o a través del teléfono. De esta manera la empresa deberá disponer de una estructura en internet muy sólida, ya que lo portales corporativos serán básicos para el correcto funcionamiento de la empresa.

Los agentes comerciales externos tendrán su propia cartera de clientes y tendrán su acceso propio para gestionarla a través del portal corporativo de la empresa. En este portal comercial, el agente podrá descargar los modelos de formularios, ofertas, etc. para poder ofertar los productos al cliente final. Una vez validado por el sistema, y por parte de la empresa, los nuevos contratos serán incorporados a la cartera de clientes del agente en cuestión. El agente además podrá gestionar los pagos de los clientes, consultar la facturación, reclamaciones, modificaciones contractuales, cambios de tarifa, etc. Dicho agente, además, obtendrá su comisión correspondiente en base a los clientes que haya aportado a la compañía.

Los clientes que contacten directamente a través del portal corporativo de la empresa, o a través del "call-center" serán asignados al agente más cercano por zona geográfica, y pasará a ser gestionado por éste.

El portal corporativo de la empresa también dispondrá de una zona para sus clientes, donde podrán acceder a su facturación electrónica y podrán realizar algunas gestiones a través del mismo portal, como por ejemplo cambiar datos de contacto, cuenta corriente de cargo, etc.

La empresa **D.C. Energía** contará con una intranet corporativa, que estará conectada con el resto de portales de la empresa. La citada intranet será principalmente la que usen los empleados para gestionar toda la información que se genere en la empresa, y estará comunicada tanto con el portal de clientes, como con el de agentes, así como con el software de gestión interna de la empresa.

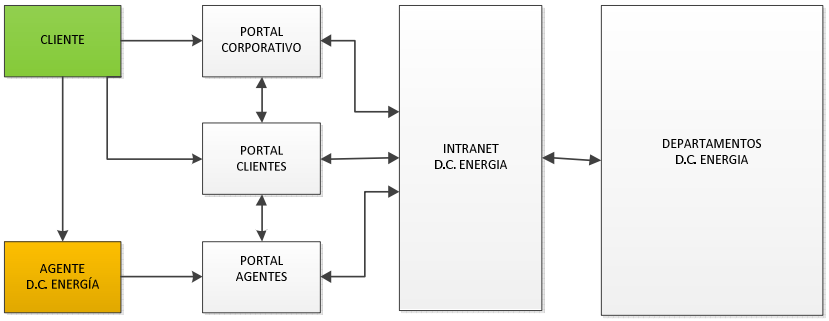

Figura 2-5 - ESQUEMA DE COMERCIALIZACIÓN DE LA COMPAÑIA.

La empresa **D.C Energía** pretende que la parte correspondiente a todos los servicios web así como la intranet, sean gestionadas desde la misma empresa sin necesidad de subcontratar servicios externos.

Los servicios web, así como la intranet corporativa, deberán estar protegidas convenientemente frente a posibles ataques desde el exterior, ya que una parte importante de los canales de comercialización de la empresa, será internet (como ya se ha comentado), por lo que parte de la estructura de la red corporativa estará expuesta a este tipo de ataques.

Los nombres de dominio de la empresa serán gestionados desde la propia empresa.

La empresa requerirá de un correo electrónico corporativo, para comunicaciones internas y hacia el exterior, así como de un correo electrónico vía web para la red de agentes comerciales, gestionado desde la propia empresa.

Para la parte de gestión y contabilidad la empresa ha encargado un software E.R.P. a medida a una empresa desarrolladora de software. Este software se ocupará de gestionar la parte de facturación y contabilidad de la compañía y funcionará bajo entorno Windows en una estructura del tipo cliente-servidor. El software funcionará en un sistema operativo Windows de tipo servidor (Windows 2012 server), dando servicio a los puestos correspondientes a los departamentos de administración, contabilidad y dirección de la empresa. El número de licencias que se deberán tener en cuenta para los sistemas operativos estarán limitadas a estos departamentos, ya que el resto no será necesario que tengan acceso al software de gestión de la empresa.

El resto de departamentos trabajará normalmente con la intranet corporativa de la empresa.

La base de datos del software de gestión y contabilidad estará comunicada con la base de datos de la intranet corporativa, que a su vez dará servicio a los servidores web.

2.4 REQUERIMIENTOS DE ACCESO A LA RED INTERNA.

Los trabajadores de **D.C. Energía** accederán a la información de los sistemas a través de aplicaciones de tipo cliente-servidor utilizando el protocolo TCP/IP.

Analizando el modelo de negocio, estructura departamental y servidores necesarios en la empresa, las restricciones de acceso a nivel de IP por parte de los miembros de la empresa será la siguiente:

- Todos los miembros de la organización deben tener acceso a internet y a los servidores de correo electrónico.
- El departamento de recepción deberá tener acceso a la intranet corporativa.
- El departamento de informática deberá tener acceso a todos los servidores y ordenadores personales de la empresa.
- El departamento comercial deberá tener acceso a la intranet corporativa.
- El departamento de *call-center* deberá tener acceso a la intranet corporativa.
- El departamento de administración deberá tener acceso a la intranet corporativa y al servidor de gestión empresarial.
- El departamento de operaciones deberá tener acceso a la intranet corporativa.
- El departamento de dirección deberá tener acceso a la intranet corporativa, servidor de gestión empresarial y al servidor de contabilidad.
- El departamento de Marketing y publicidad deberá tener acceso a la intranet corporativa y a los servidores web (para gestionar el diseño de los sitios web de la empresa).
- El departamento de formación deberá tener acceso a la intranet corporativa.

En el presente TFC no se analizará la estructura de los diferentes portales de la empresa ni la intranet de cliente. Esta parte entraría dentro del capítulo de análisis de software.

2.5 REQUERIMIENTOS DE ACCESO EXTERNO A LA RED CORPORATIVA.

Como se ha indicado en los apartados anteriores, internet es la forma de comercialización principal de la empresa, por lo que los servidores web de la compañía serán accesibles desde el exterior.

Todos los usuarios de internet podrán consultar la web pública de la empresa.

Los clientes que tengan contratados algún producto de la compañía tendrán acceso al portal de clientes.

Por otro lado los agentes comerciales al trabajar de forma descentralizada a la compañía principal dispondrán de una cuenta de correo IMAP de la empresa, así como del acceso correspondiente al portal de agentes de la compañía.

2.6 ACCESO VPN.

D.C. Energía en una segunda fase de implantación, pretende abrir diferentes sedes en algunas de las provincias más importantes de España. Por ello se deberán prever los mecanismos necesarios para comunicar las diferentes sedes con la sede principal.

En esta fase se debería comunicar cada una de las sedes con el servidor de gestión administrativa y la intranet de la empresa principal.

2.7 ACCESO WI-FI.

Dentro de las instalaciones de la sede principal no habrá acceso Wi-Fi, solo se ofrecerá en el edificio anexo. Entre estos dos edificios existe visión directa.

Analizando la situación geográfica entre los dos edificios se observa que pueden existir dificultades para la instalación de cableado físico entre éstos, ya que previsiblemente se necesitarán una serie de permisos a nivel de organismos que podrán resultar bastante costosos.

Se plantearán posibles soluciones para el caso de que no se pudiera establecer una conexión directa punto a punto entre los dos edificios mediante cableado físico, garantizando un ancho de banda mínimo para el caso del 100% de ocupación.

3 SOLUCIONES PROPUESTAS.

3.1 ESTRUCTURA FISICA DE LA RED CORPORATIVA.

Para adaptar la instalación de cableado a los requerimientos físicos de equipamientos de datos y voz se usará la normativa de cableado estructurado. Esta normativa regulará la problemática de hacer llegar el cableado necesario a cada uno de los puestos de trabajo.

Dentro de la normativa de cableado estructurado, se usará por un lado el cableado vertical para comunicar cada una de las plantas del edificio principal, y el cableado horizontal que determinará las conexiones entre el equipamiento de red de datos de la misma planta.

Para trazar las líneas del cableado vertical y comunicar las plantas entre sí, se optará por una canalización interior a través de las zonas comunes del edificio, y se utilizará el espacio etiquetado como “zona de comunicaciones”; ubicados en el mismo lugar, e intercomunicar cada una de las plantas. El hecho de que este espacio esté ubicado en el mismo lugar físico proporcionará un ahorro considerable en el costo de la instalación.

Para trazar las líneas de cableado horizontal por cada una de las plantas se realizará por el falso techo. En el interior del falso techo se utilizará bandeja metálica para la sujeción del cableado.

3.1.1 ESTRUCTURA FISICA EDIFICIO PRINCIPAL.

Como se ha indicado el edificio principal está formado por varias plantas, por lo tanto se distinguirá entre cableado horizontal y vertical.

- Cableado horizontal: mediante este cableado se interconectará cada uno de los host con los IDFs (*Intermediate Distribution Facility*). El cableado horizontal conectará cada una de las rosetas de los puestos de trabajo con los paneles de parcheo (*patch pannels*) de cada uno de los IDF por planta.

- Cableado vertical: el cableado vertical conectará los IDF situados en cada planta.

Un IDF (*Intermediate Distribution Facility*) es el habitáculo de comunicaciones donde residen los equipos de comunicación, así como los armarios de racks de comunicaciones. En este caso los IDF contendrán un armario rack que albergará los switch de cada planta.

Un MDF (*Main Distribution Facility*) también es un habitáculo de comunicaciones (armario o habitación), donde encontramos el POP (Punto de presencia del operador o ISP), junto con los routers, conmutadores, etc., principales de comunicaciones. Los servidores de la empresa como se observa, se encuentran ubicados junto al MDF.

Figura 3-1 - Vistas dispositivos de comunicaciones.

Los “patch-pannels” o cross-connectors, son los elementos pasivos, situados en los habitáculos de comunicaciones o armarios, que facilitan la conexión entre el cableado proveniente de las estaciones de trabajo y el cableado que cuelga de los equipos de comunicación (hubs, switches o routers).

Figura 3-2 - Vista Trasera Patch pannel

Los “patch-cords” son los cables que se utilizan para realizar las interconexiones entre los diferentes puertos del patch-pannel.

La principal función de los elementos pasivos es de protección de los equipos de los armarios. Los cables que provienen de las rosetas nunca se conectarán de forma directa a los puertos de los hubs, switches o routers que se encuentran en los IDF´s o MDF´s, ya que accidentalmente se podrían romper las entradas de los interfaces de los principales dispositivos activos.

3.1.2 ESTRUCTURA GENERAL DE LA RED.

El esquema del edificio principal a nivel de cableado horizontal, vertical y administrativo sería el siguiente:

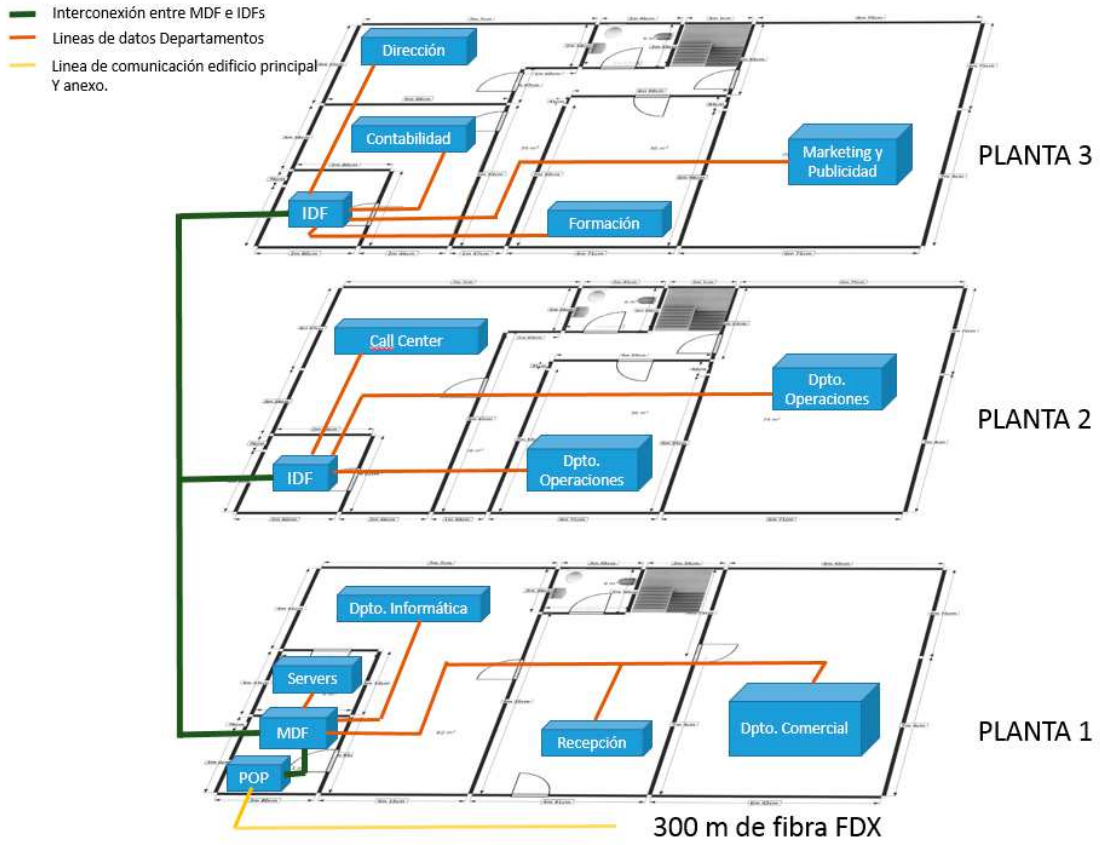

Figura 3-3 Estructura General de la Red

En las plantas dos y tres en el IDF de cada planta se colocarán los switches necesarios para dar conectividad a los puestos de los departamentos de cada planta.

Los switches de las plantas dos y tres estarán unidos a un switch troncal en la planta primera. Este switch estará comunicado con el router encargado de dar servicio de internet y al router que gestiona los accesos desde el exterior, y a la centralita de VoIP.

En la planta primera, se dispondrá de los switches apilables necesarios para dar conectividad tanto a los servidores, como a los equipos de los departamentos ubicados en dicha planta, así como al resto de equipos de comunicaciones.

3.1.3 DISPOSITIVOS DE COMUNICACIONES.

Switches

Seguidamente se indicarán las características que deben tener los switches propuestos para llevar a cabo la instalación.

- Ser apilables y modulares.
- Ser gestionables.
- Deberán tener funcionalidades VLAN en base a Access Control List.
- Velocidad de puertos seleccionables 10/100/1000 Mbs
- Capacidad de conexión por fibra
- Se deberán colocar los switch del mismo tipo, y se debería disponer de al menos uno de reserva para el caso de avería.

Los modelos de switch seleccionados para la red, debido a sus prestaciones y precio son de la marca **HP serie 2610** [1]en sus versiones de 48 y 24 puertos.

El importe aproximado de este modelo rondará los 400 y 700 euros, dependiendo del número de puertos.

Figura 3-4 - Switch HP 2610 Series

Routers

Los routers se elegirán de arquitectura modular para adaptarlos a nuestros requerimientos. Se necesitarán dos conexiones Ethernet Giga y una conexión de cara a Internet en cada uno de ellos. Los routers estarán equipados con sus correspondientes unidades de proceso y tarjetas FIC para la conectividad.

El modelo de router seleccionado será el HP MSR2000 Router Series [2] cuyo precio aproximado de mercado ronda los 800 euros.

[1] Para más información sobre el switch HP 2610 Series se puede acceder al siguiente vínculo http://pro-networking-h17007.external.hp.com/us/en/products/switches/HP_2610_Switch_Series/index.aspx
[2] Para más información sobre el router HP MSR2000 se puede acceder al siguiente vínculo http://h17007.www1.hp.com/us/en/networking/products/routers/HP_MSR2000_Router_Series/index.aspx#.VHej-me9bgU

Figura 3-5 - Router HP MSR2000 Series

Rosetas

Las rosetas serán de superficie y dobles. Cada puesto de trabajo dará servicio a un ordenador y a un teléfono IP.

Figura 3-6 - Rosetas (Puestos de trabajo)

Cableado

Se utilizarán dos tipos de cableado. Por un lado el que une las estaciones de trabajo a su switch correspondiente que será del tipo UTP cat 5e con sus correspondientes conexiones RJ45, para conectar los terminales a las rosetas.

El cableado vertical será de fibra óptica. Para conectar los IDF´s con el MDF, se utilizará fibra óptica monomodo.

Los estándares que se acostumbran a utilizar en el cableado vertical son 100 BASE-FX (FastEthernet con fibra óptica) y 1000 BASE-FX (Gigabit Ethernet con fibra óptica). Por lo tanto todos los racks deberán tener conectores en el panel de conexión tanto de fibra óptica como de cable RJ-45 para cubrir todas las necesidades de todo el edificio.

Los enlaces entre las diferentes plantas se realizarán con fibra óptica de 1 Gbps (Gigabit Ethernet), que permitirá suplir todas las necesidades de tráfico del sistema a largo plazo.

Racks

Los racks necesarios para los IDF´s y MDF serán de 22 u, para colocación de switches y paneles de parcheo. Se debe tener en cuenta la reserva de espacio para posibles ampliaciones, así como para cada switch la reserva de una unidad para su panel de parcheo correspondiente.

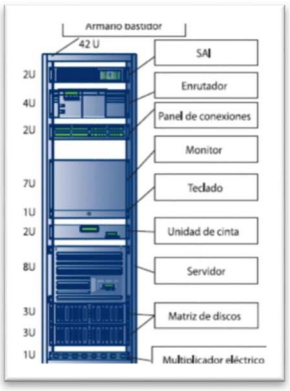

Figura 3-7 - Vista Rack Servidores – 42 U

El rack principal de servidores será de 42 u, y tendrá una vista similar a la de la imagen.

Figura 3-8 - Rack 22 u

3.1.4 CÁLCULO REQUERIMIENTOS DE CABLEADO.

El cableado partirá del armario de comunicaciones hasta el techo y será distribuido por el falso techo. Se supone una altura aproximada de 2 m. La caída desde el falso techo hasta cada uno de los puestos será también de 2 m, (desde el techo hasta el puesto de trabajo).

Planta 1

- Líneas desde zona de comunicaciones (MDF) hasta servidores (30 metros).
- Líneas desde zona de comunicaciones (MDF) hasta Dpto. Informática:
    - 14 m + 2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) * 5 puestos = 90 metros cable UTP datos y 90 metros UTP teléfonos.
- Líneas desde zona de comunicaciones (MDF) hasta Recepción:
    - 17 m +2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) * 1 puesto = 21 metros de cable UTP datos y 21 metros UTP teléfonos.
- Líneas desde zona de comunicaciones (MDF) hasta Dpto. Comercial y agentes:
    - 25 m + 2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) *5 puestos = 145 metros de cable UTP datos y 145 metros UTP teléfonos.

Planta 2

- Líneas desde zona de comunicaciones (IDF) hasta Dpto. Call Center:
    - 15 m + 2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) * 5 puestos = 95 metros cable UTP datos y 95 metros UTP teléfonos.
- Líneas desde zona de comunicaciones (IDF) hasta Dpto. Operaciones:
    - 18 m +2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) * 3 puestos = 66 metros de cable UTP datos y 66 metros UTP teléfonos.
- Líneas desde zona de comunicaciones (IDF) hasta Dpto. Administrativo:
    - 25 m + 2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) *5 puestos = 145 metros de cable UTP datos y 145 metros UTP teléfonos.

Planta 3

- Líneas desde zona de comunicaciones (IDF) hasta Dpto. Contabilidad:
  - 8 m + 2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) * 5 puestos = 60 metros cable UTP datos y 60 metros UTP teléfonos.
- Líneas desde zona de comunicaciones (IDF) hasta Dpto. Dirección:
  - 12 m + 2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) * 3 puestos = 48 metros cable UTP datos y 48 metros UTP teléfonos.
- Líneas desde zona de comunicaciones (IDF) hasta Dpto. Formación:
  - 18 m +2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) * 3 puestos = 66 metros de cable UTP datos y 66 metros UTP teléfonos.
- Líneas desde zona de comunicaciones (IDF) hasta Dpto. Marketing y publicidad:
  - 25 m + 2 m de caída (armario) + 2 m de caída (por puesto) aproximadamente (por línea de datos) *5 puestos = 145 metros de cable UTP datos y 145 metros UTP teléfonos.

Como previsión de un posible aumento de plantilla en cada uno de los departamentos de la planta, se instalará por cada puesto previsto, uno adicional con cableado UTP para voz y datos. Por lo que habrá que duplicar el cableado estimado para los puestos de trabajo.

Cableado fibra óptica.

Fibra óptica necesaria para comunicar MDF con IDFs de cada planta, 40 metros.

Patch cords necesarios.

Los patch cords necesarios para conectar cada puesto desde su patch panel correspondiente a cada switch serán los siguientes:

41 para equipos + 41 para equipos adicionales (escalabilidad horizontal).

41 para teléfonos, 1 teléfono para cada dos puestos (escalabilidad horizontal).

3.1.5 COMUNICACIÓN DE EDIFICIOS.

Para comunicar los edificios se plantearán dos opciones.

OPCION 1 - Punto a Punto mediante fibra óptica.

Se establecerá una tirada de cableado de fibra óptica de unos 300 metros aproximadamente entre el edificio principal y el edificio anexo. Se requerirán dos conectores SC de fibra multimodo. La tirada máxima de este tipo de fibra alcanza unos 550 metros de distancia (fibra MMF 50/100 µm).

OPCION 2 – Punto a Punto mediante antenas Wi-Fi.

Otra forma de comunicar los dos edificios sería mediante antenas de radio frecuencia. Hoy en día este tipo de antenas son económicas y tienen grandes prestaciones, garantizando la conectividad hasta 30-40 km de distancia.

El establecimiento de la conexión "punto a punto" se realizará mediante un "puente de red", configurando las antenas en modo "bridge", mediante la MAC de los dispositivos de comunicación (antenas). La marca seleccionada para este tipo de antenas es Ubiquiti. Y el modelo de enlace seleccionado es el Air Fiber 5[3].

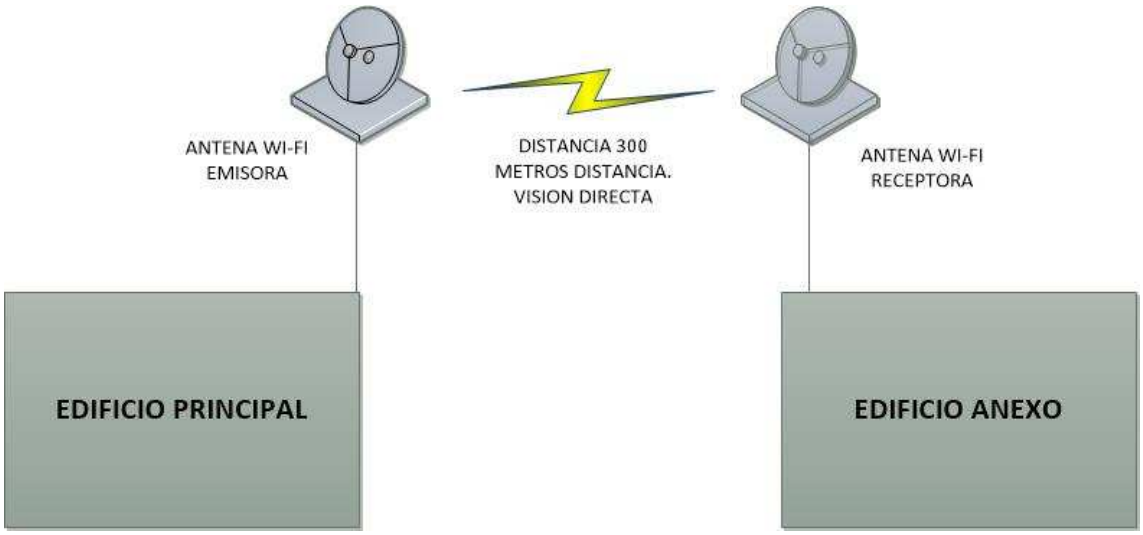

Figura 3-9 - Enlace punto a punto con antenas Wi-Fi

El precio aproximado de este tipo de antenas es de unos 700 euros.

En el capítulo correspondiente a la valoración económica se hará una propuesta económica de las dos opciones planteadas en este capítulo.

[3] Para ver más características sobre el dispositivo Air Fiber 5 de Ubiquiti, visitar el enlace http://landashop.com/catalog/ubiquiti-airfiber-5458-gbps-gigabit-p-3076.html

3.2 ESTRUCTURA LOGICA DE LA RED CORPORATIVA.

El esquema de VLANs y enlaces trunk quedaría como sigue:

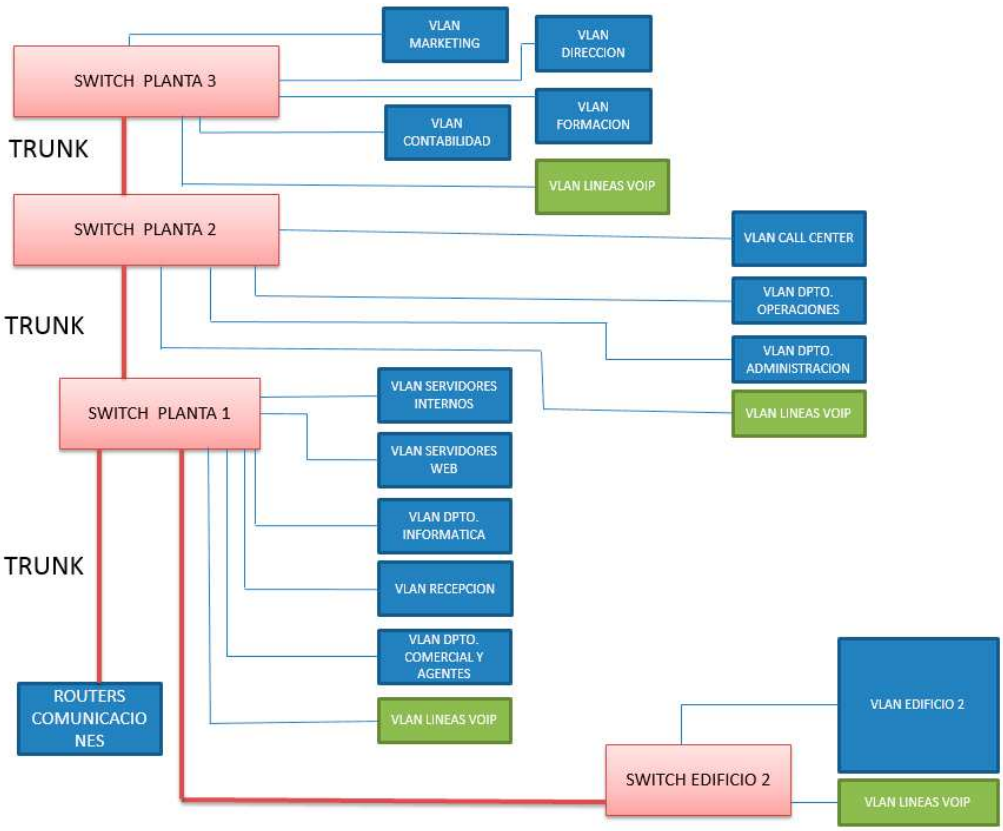

Figura 3-10 - Esquema VLANs y enlaces TRUNK.

En cada planta, como se ha comentado, se colocará un switch donde se gestionarán las VLANS correspondientes. Los switch se conectarán a otro switch principal, situado en la primera planta. Dicho switch estará conectado a los otros switches secundarios con enlaces trunk (troncales), ya que estos enlaces establecen una comunicación punto a punto entre dos dispositivos de red, que a su vez transportan más de una VLAN, por si en algún momento se necesitase agrupar a los usuarios de la misma VLAN que se encuentran ubicados en diferentes zonas. Entre el switch principal y los routers de comunicaciones también se definirá un enlace troncal.

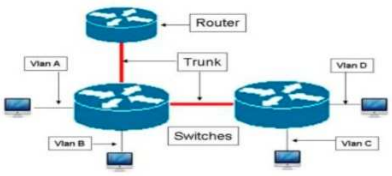

Figura 3-11 - Ejemplos de enlaces Trunk.

3.2.1 ESQUEMA DE RED DMZ y MZ.

El esquema general de la red, diferenciando la zona Militarizada (MZ) y la desmilitarizada (DMZ), sería el siguiente:

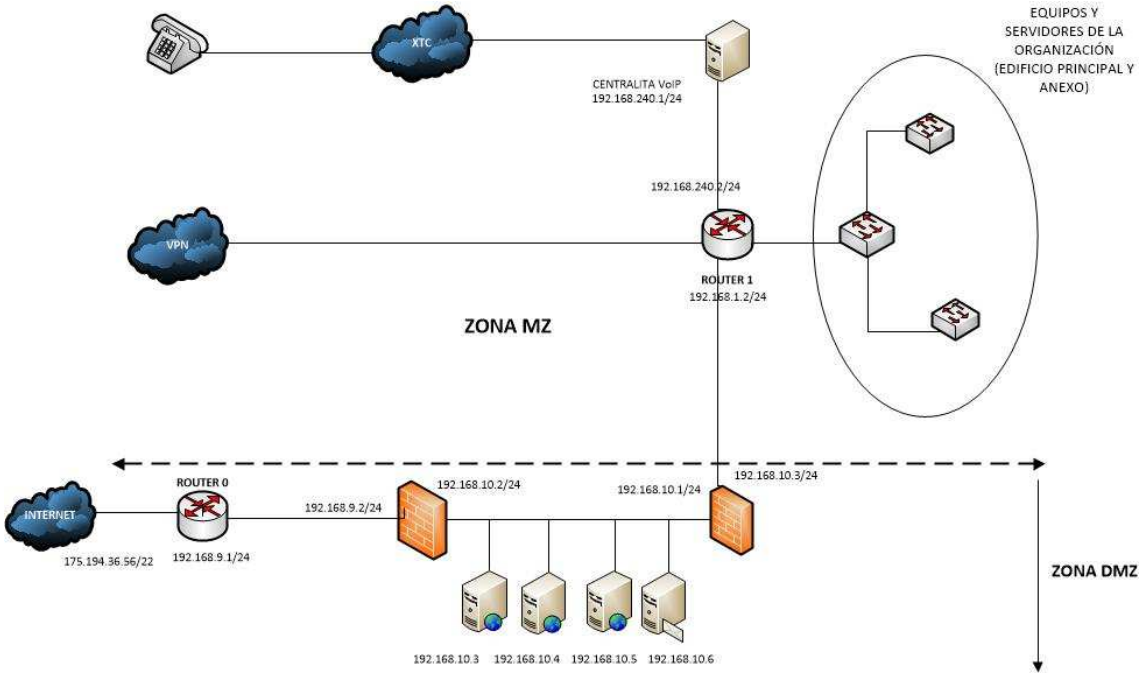

Figura 3-12 - Esquema completo de la red Corporativa.

3.2.2 DISTRIBUCION IP PRIVADAS SUBREDES ZONA MZ.

Distribución de IP privadas de las subredes de la zona MZ (o red interna).

VLAN SERVIDORES INTERNOS	192.168.100.0/24
VLAN RECEPCION	192.168.50.0/24
VLAN DPTO INFORMATICA	192.168.51.0/24
VLAN DPTO. COMERCIAL	192.168.52.0/24
VLAN DPTO. CALL CENTER	192.168.53.0/24
VLAN DPTO. ADMINISTRACION	192.168.54.0/24
VLAN DPTO. OPERACIONES	192.168.55.0/24
VLAN DPTO. DIRECCION	192.168.56.0/24
VLAN DPTO. CONTABILIDAD	192.168.57.0/24
VLAN DPTO. MARKETING Y PUBLICIDAD	192.168.58.0/24
VLAN DPTO. FORMACION	192.168.59.0/24

Tabla 2 - Distribución IP Privadas subredes zona MZ

En la zona MZ, también se encuentra el servidor VOIP, y los routers configurados para VPN.

3.2.3 DISTRIBUCION IP PRIVADAS SUBREDES ZONA DMZ.

La zona DMZ (o red perimetral), estará ubicada entre la red interna, y la red externa (internet). El objetivo de esta red es que las conexiones desde la red interna y externa a la DMZ estén permitidas, sin embargo las conexiones desde la red DMZ, sólo se permitirán hacia el exterior.

En este caso los servidores web pertenecientes a la organización, así como el servidor de correo IMAP, estarán ubicados en esta DMZ.

La zona DMZ estará protegida por dos firewalls físicos o por software a través de servidores Linux que actúen como Firewall, el análisis de estas dos opciones se realizará en el capítulo de seguridad de la red.

Los dos firewalls dispondrán de herramientas de filtrado de tráfico, así como herramientas IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) configurables por el usuario.

FIREWALL 0	192.168.10.1
FIREWALL 1	192.168.10.2
SERVIDOR WEB 1(PUBLICO)	192.168.10.3
SERVIDOR WEB 2(AGENTES)	192.168.10.4
SERVIDOR WEB 3 (CLIENTES)	192.168.10.5
SERVIDOR DE CORREO IMAP	192.168.10.6

Tabla 3 - Distribución IP zona DMZ

3.3 HARDWARE DE SERVIDOR Y VIRTUALIZACION DE SERVIDORES (JUSTIFICACIÓN).

Atendiendo a los servicios necesarios por la empresa, se necesitarán de varios servidores para cubrir todos los servicios requeridos, ya que como se indica en los requerimientos se necesitarán de sistemas operativos diferentes, con diferentes aplicaciones, aunque en una misma máquina del mismo tipo de sistema operativo se podrían ejecutar varios servicios de forma simultánea, por ejemplo, en la misma máquina donde se ubicase el servidor web se podría ubicar el servidor DNS, e incluso los servidores de correo electrónico POP y vía web (IMAP).

Según los requerimientos necesarios por la empresa, por un lado se necesitaría cubrir la infraestructura web (portal corporativo, clientes y agentes), para ello, se podría utilizar software libre para evitar gasto adicional en licencias. La intranet corporativa, también funcionará bajo entorno web y también podría estar montada bajo plataforma de software libre, alojados en los servidores de la empresa (aunque los servidores web puedan estar replicados en la nube).

Los servidores de correo tanto POP, para el correo interno, como IMAP para el correo de agentes comerciales, así como los servidores de nombres también se podrían montar usando software libre.

Como se ha comentado anteriormente, los dos firewalls que servirán para proteger la parte DMZ de la red, serían montados con dos máquinas Linux, con mecanismos IPS/IDS, para proteger a esta, de esta manera se evitaría un coste adicional en máquinas físicas.

La parte correspondiente a gestión y contabilidad, sería necesario montarla en un entorno Windows. Se utilizaría Windows 2012 SERVER, para montar la ERP de gestión y contabilidad, así como las licencias adicionales para los equipos cliente de los departamentos de gestión, contabilidad y dirección.

La centralita de Voip, se podría montar sobre un servidor Asterisk[4] (software libre), por lo que se necesitaría otra máquina adicional.

Para poder implementar todos estos servicios, en principio, se necesitarían de varias máquinas físicas, con sus correspondientes sistemas operativos, aunque en algunas de ellas, como ya se ha indicado, se podrán ejecutar varios servicios de forma simultánea. Aunque se intentase minimizar el número de máquinas físicas incluyendo el máximo número de servicios en la misma máquina, se podría tener el problema de que una máquina en concreto tuviese excesiva carga de trabajo y otra todo lo contrario, dependiendo de los servicios que se ejecutasen en ésta, por lo que se podrían desperdiciar recursos, provocando desequilibrios en la estructura general de la red. Otros problemas adicionales si se plantease la estructura de servidores con máquinas independientes, sería el siguiente, si en un futuro se quisiera ampliar

[4] Visitar http://www.asterisk.org/ para más información.

el sistema, se debería realizar una inversión adicional con el consiguiente coste económico, así como costes añadidos en cuanto a mantenimiento, tanto a nivel físico como lógico y eléctrico.

De esta manera, ***se propone como solución adecuada para una empresa como la planteada en el presente TFC el uso de la virtualización de servidores***, no sólo por el ahorro económico en cuanto a máquinas físicas independientes, sino por las posibilidades que ofrecen este tipo de sistemas, como por ejemplo: escalabilidad, seguridad de la información, reducción de costos de mantenimiento, centralización, simplicidad, etc. En los apartados siguientes se recogen las características más importantes de este tipo de sistemas indicando una posible solución aplicada a la red de la empresa, determinando además las ventajas que este tipo de sistemas pueden proporcionar para una estructura como la planteada en el presente TFC.

3.3.1 CONCEPTO DE VIRTUALIZACIÓN

Básicamente la virtualización es la abstracción del sistema operativo respecto a los recursos de una máquina física o host, de esta manera se podrían ejecutar diferentes máquinas virtuales con sistemas operativos diferentes en la misma máquina física de forma concurrente.

En un entorno profesional, cuando se hace referencia a virtualización, a lo que se está refiriendo referencia en sí es a la virtualización de servidores, lo que significa particionar un servidor físico en varios servidores virtuales. De esta manera cada máquina virtual puede interactuar de forma independiente con otros dispositivos, aplicaciones, datos y usuarios, como si se tratara de un recurso físico independiente.

Dado que las diversas máquinas virtuales están aisladas unas de las otras, en caso de ocurrir un bloqueo en una de ellas, este no afectaría a las demás máquinas virtuales.

3.3.2 VENTAJAS DE LA VIRTUALIZACIÓN.

Existen muchos beneficios para la consolidación de servidores Linux o Windows mediante el aprovechamiento de los diferentes productos de virtualización de servidores existentes en el mercado. A continuación se enumeran algunos beneficios que brinda esta tecnología:

1. Disminuye el número de servidores físicos. Esto trae como consecuencia una reducción directa de los costos de mantenimiento de hardware.
2. Mediante la implementación de una estrategia de consolidación de servidores, el cliente podría aumentar la eficiencia de la utilización del espacio disponible de almacenamiento.
3. Al tener cada aplicación dentro de su propio “servidor virtual” se podría evitar que una aplicación impacte a otras aplicaciones en el momento de realizar mejoras o cambios.
4. Se pueden desarrollar normas de construcción de servidor virtual que puedan duplicarse fácilmente lo que aceleraría la implementación del servidor.
5. Se pueden desplegar múltiples tecnologías de sistemas operativos en una sola plataforma de hardware (es decir, Windows Server, Linux, etc.)

3.3.3 OPCIONES DE SOFTWARE DE VIRTUALIZACIÓN DISPONIBLES EN EL MERCADO.

Actualmente existen numerosos tipos de software de virtualización, en la siguiente tabla, se muestran algunos de estos sistemas con sus características más importantes:

Nombre	Fabricante	HOST CPU	GUEST CPU	HosOS(s)	Guest (OS)	Tipo Licencia
Hyper-V	Microsoft	X64 + hardware-assisted virtualization (Intel VT or AMD-VT)	X64,x86	Windows 2008/Hyper-V, Windows Hyper-V Server	Drivers soportados para Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, etc. Linux (SUSE10, etc)	Propietaria (Sin cargo con Windows Server 2008)
Oracle VM	Oracle Corp.	Intel x86, x86-64, Intel VT-x	Intel x86, x86-64, Intel Vt-x	Sistema Operativo propio	Microsoft Windows, Oracle Enterprise, Linux, Red Hat Enterprise Linux	Libre
Sun xVM VirtualBox	Sun Microsystems	X86-64, SPARC	X86, (x86-64 only on VirtualBox 2 with hardware virtualization)	Windows, Linux, Mac OS X (Intel), Solaris, eComStation	Dos, Windows Linux, OS/2, FreeBSD, Solaris	Libre para uso personal y educacional y evaluación.
VMWare ESXi	VMWare	X86, x86-64	X86, x86-64	Sistema Operativo Propio	Windows, Linux Netware, Solaris, FreeBSD,...	Propietaria
VMWare Server	VMWare	X86, x86-64	X86, x86-64	Windows, Linux	DOS, Windows, Linux, FreeBSD, Netware, Solaris, Virtual appliances	Propietaria
Xen	Citrix Systems	X86, AMD64	Mismo que el Host	NetBSD, Linux, Solaris	FreeBSD, NetBSD, Linux, Solaris, Windows XP & 2003	GPL

Figura 3-13 Software de Virtualización en el mercado

3.3.4 ELECCIÓN DEL SOFTWARE DE VIRTUALIZACION.

Actualmente el producto estrella en virtualización de servidores es VSphere de VMWare, este sistema proporcionaría los recursos necesarios para la instalación y administración de una infraestructura de servidores virtualizada de alto rendimiento y alta disponibilidad.

Sus competidores inmediatos y que también se podrían aplicar como solución al presente TFC son Citrix SenServer y Microsoft Hyper-V 2012.

- Citrix SenServer: tiene como ventaja principal el tipo de licencia (GNU) y dispone de funcionalidades similares a las de VSphere, tales como migración en caliente, balanceo de carga, etc. Esta opción es altamente recomendable para pymes, ya que la licencia sólo tendría coste si se contratase el soporte oficial del producto. Como deficiencia de este sistema, se podría indicar que este sistema necesita de un sistema operativo huésped para su instalación y posterior ejecución.
- Microsoft Hyper-V 2012: Es la opción actual de Microsoft. Como los anteriores productos tiene funcionalidades similares, pero se necesitaría contratar la licencia de Windows Server 2008/2012 oficial.

Para el presente proyecto se recomendará la opción VSphere[5] por los siguientes motivos:

- VSphere dispone de ESXi, capa de virtualización que hace que no se requiera Sistema Operativo huésped, y por lo tanto se pueda aprovechar de forma directa los recursos de la máquina física.
- VSphere es el sistema de virtualización más completo, ya que dispone de numerosas aplicaciones adyacentes para la gestión del sistema de virtualización (Ver apartado 3.3.6.).
- El ahorro económico que supondría la virtualización en cuanto a costos de servidores físicos independientes, proporcionaría los recursos necesarios para invertir en un producto contrastado y de garantías.
- La facilidad de manejo e instalación del sistema y la gestión de los recursos disponibles.

En los anexos del presente TFC se incluyen una serie de enlaces que describen el proceso de instalación paso a paso de VSphere ESXi, así como de alguna de las aplicaciones más importantes de este sistema.

[5] Para más información http://www.vmware.com/es/products/esxi-and-esx/overview

3.3.5 CARACTERISITICAS PRINCIPALES VSPHERE V5.

HIPERVISOR ESXi.

ESXi es una capa de virtualización que se instala directamente sobre el servidor físico y almacenará las diferentes máquinas virtuales.

Figura 3-14 - Hipervisor ESXi

La tarea del ESXi es la de proporcionar a cada máquina virtual (VM) el acceso a los recursos físicos subyacentes, de tal forma que varias máquinas virtuales pueden tener acceso al mismo hardware sin estar relacionadas unas con otras.

VMWare ESXi puede ser montado sobre un sistema de virtualización, pero este sistema no sería aconsejable para producción, ya que para sacar el máximo partido a los recursos del servidor sería conveniente que estuviese montado directamente sobre el hardware físico.

ALMACENAMIENTO COMPARTIDO.

Una de las grandes ventajas de VSphere es la de poder compartir el almacenamiento de las máquinas virtuales, por lo que se puede añadir cualquier VM a cualquiera de los host ESXi que tengan como almacenamiento compartido el mismo Datastore.

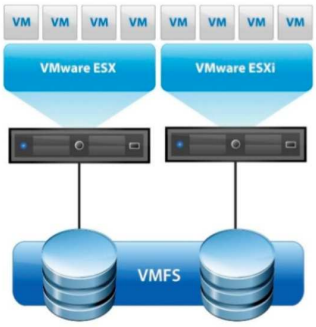

Figura 3-15 - Almacenamiento Compartido en VSphere

Algunas de las posibilidades para añadir los Datastores para el almacenamiento compartido son las siguientes:

- iSCSI (Internet SCSI)
- NFS (Network File System)
- FC (Fibre Channel)
- FCoE (Fibre Channel over Ethernet)

VMWARE VCENTER SERVER (GESTION DE INFRAESTRUCTURA).

VMWare vCenter Server es considerado el componente más importante de una infraestructura virtual en VMware vSphere 5.5. Es el punto central que permite gestionar múltiples servidores VMware vSphere ESXi y máquinas virtuales.

Este componente añade funcionalidades en áreas como el balanceo de carga (VMWare DRS), alta disponibilidad (VMWare HA), Fault Tolerance (FT), actualización de componentes (Update Manager), y conversores de servidores físicos a servidores virtuales (VMWare Converter).

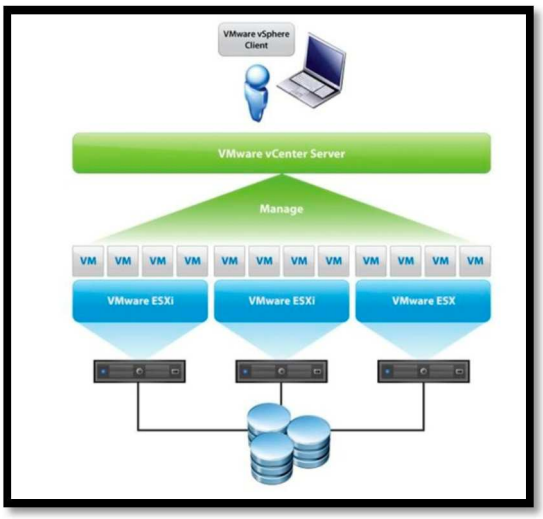

Figura 3-16 - VMWare Vcenter

VMOTION.

VMWare Vmotion permite la migración en caliente de máquinas virtuales desde un servidor ESXi a otro con tiempo de inactividad “cero”, y la disponibilidad del servicio de forma constante.

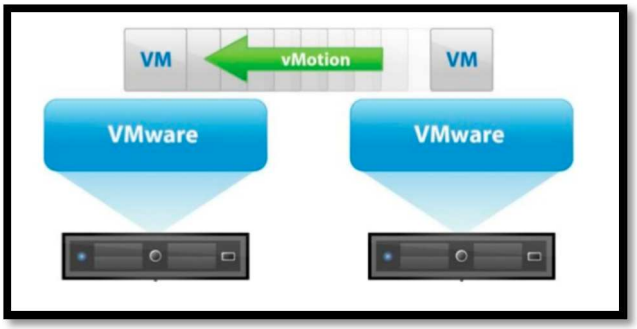

Figura 3-17 - VMotion

HIGH AVAILABILITY (HA).

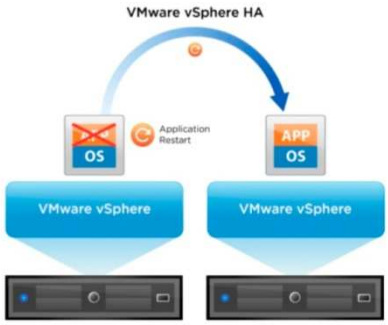

Figura 3-18 - High Availability (HA)

VSphere HA es una característica que proporciona alta estabilidad a las máquinas virtuales. Este sistema supervisa todos los host ESXi dentro de un cluster, para detectar fallos o errores de estos.

Si un host ESXi fallase, VSphere HA reiniciaría las máquinas virtuales de ese host y las movería a otro host ESXi con recursos disponibles.

VSPHERE DISTRIBUTED RESOURCE SCHEDULER (DRS).

La función de VSphere DRS es ayudar a administrar un conjunto de Host ESXi calculando los recursos disponibles. DRS utiliza VMotion para migrar máquinas virtuales a Host diferentes para que la carga general de la infraestructura esté equilibrada.

La configuración de este sistema puede ser de dos tipos:

- **Manual:** VMware DRS mostrará los consejos y recomendaciones para mantener el entorno equilibrado. El administrador sería el responsable de decidir si se realiza o no la migración de las VM.
- **Automático:** Cuando el entorno es muy grande y se disponen de muchas VM, sería aconsejable elegir esta opción. De esta forma se migrarían automáticamente las máquinas virtuales entre ESXi.

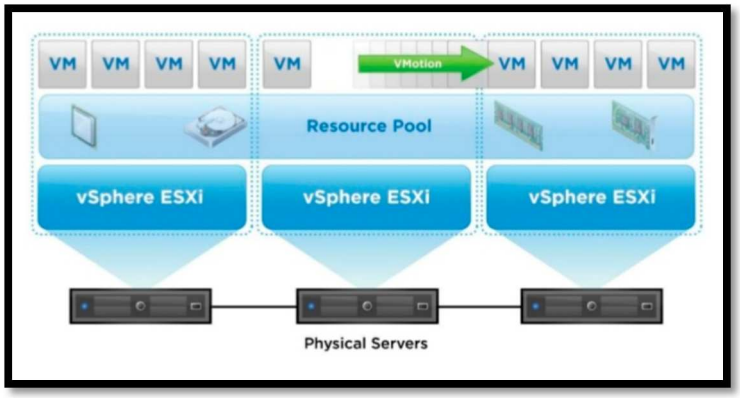

Figura 3-19 - VSPHERE (DRS)

FAULT TOLERANCE (FT).

Si esta opción está habilitada se crearía una copia secundaria de la original en un Host ESXi diferente.

Todas las acciones realizadas en la VM primaria también se aplicarían a la VM secundaria, de esta manera si un host ESXi falla o la VM primaria no está disponible, FT activaría de forma inmediata la máquina virtual secundaria, convirtiéndola en primaria, proporcionando disponibilidad continua en el servidor elegido.

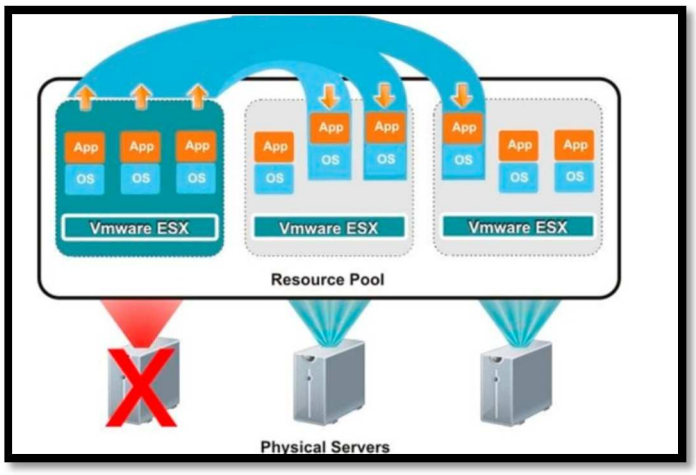

Figura 3-20 - FAULT TOLERANCE (FT)

3.3.6 APLICACIÓN DE LA VIRTUALIZACIÓN A LA INFRAESTRUCTURA DE LA EMPRESA OBJETO DE ESTUDIO.

Una vez estudiados los requerimientos a nivel de servicios de la organización, seguidamente se indica una posible solución incorporando los elementos hardware y software necesarios.

Se propone la utilización de dos máquinas físicas HP Proliant (ver apartado 3.3.7). En cada una de estas máquinas físicas se montaría un servidor ESXi, que daría soporte a las máquinas virtuales con la siguiente distribución:

SERVIDOR FÍSICO Nº1

SERVIDOR ESXi (Software de virtualización vSphere) – Máquinas virtuales: Servidores Web, correo electrónico, DNS, servicios FTP, firewalls (software) para zona DMZ.

En este primer servidor se montarían todos los servidores web, dns y correo electrónico, y los dos firewalls en sistema operativo LINUX bajo distribución DEBIAN.

SERVIDOR FÍSICO Nº 2

SERVIDOR ESXi – Máquinas virtuales: Servidores de bases de datos y aplicaciones, centralita Asterisk VoIP.

En este servidor se montarían los servidores de bases de datos, e intranet de la empresa, en sistema operativo LINUX (DEBIAN), así como el servidor de aplicaciones de administración y gestión en WINDOWS SERVER 2012.

El hecho de utilizar el máximo número de máquinas virtuales LINUX, proporcionará un gran ahorro en cuanto a licencias.

La licencia de vSphere que se recomienda para cubrir la infraestructura de la red del presente TFC será la siguiente:

Tabla 4 - vSphere Essential Plus

PRECIO BUNDLE CON SOPORTE BÁSICO 1 AÑO(12X5)	4895 €
ADMINISTRACION CENTRALIZADA	vCenter Essentials
Licencia Incluida	3 Servidores Físicos con 1 o 2 Procesadores Físicos
Licencia vRAM	32GB por servidor (192 GB)
Thin Provisioning	SI
Update Manager	SI
vStorage API para Backups	SI
vCenter Data protection	SI
Alta Disponibilidad (HA)	SI
vMotion	SI

Con esta versión se cubrirá la incorporación de licencias prevista en los requerimientos iniciales, e incluso se tendría la posibilidad de incrementar, en un futuro, un servidor físico adicional, ya que la licencia comentada nos permite hasta 3 servidores físicos.

Las máquinas físicas (servidores HP Proliant), contarán con 4 TB de almacenamiento local, para instalar las máquinas virtuales (ver características específicas del hardware de servidor en el Anexo número 2).

Los servicios se distribuirán en la medida de lo posible en máquinas virtuales independientes, para evitar conflictos entre servicios, y aprovechar al máximo los beneficios que la virtualización ofrece.

El hecho de montar dos servidores ESXi en máquinas físicas independientes servirá para poder utilizar las capacidades que proporciona vSphere para aprovechar al máximo los recursos disponibles (ver apartado 3.3.5.), al disponer de dos servidores ESXi se podrán utilizar las opciones VMOTION, High availability (HA), y DRS, entre otras.

En el siguiente esquema se muestra una propuesta de servicios distribuidos en máquinas virtuales, por servidor físico.

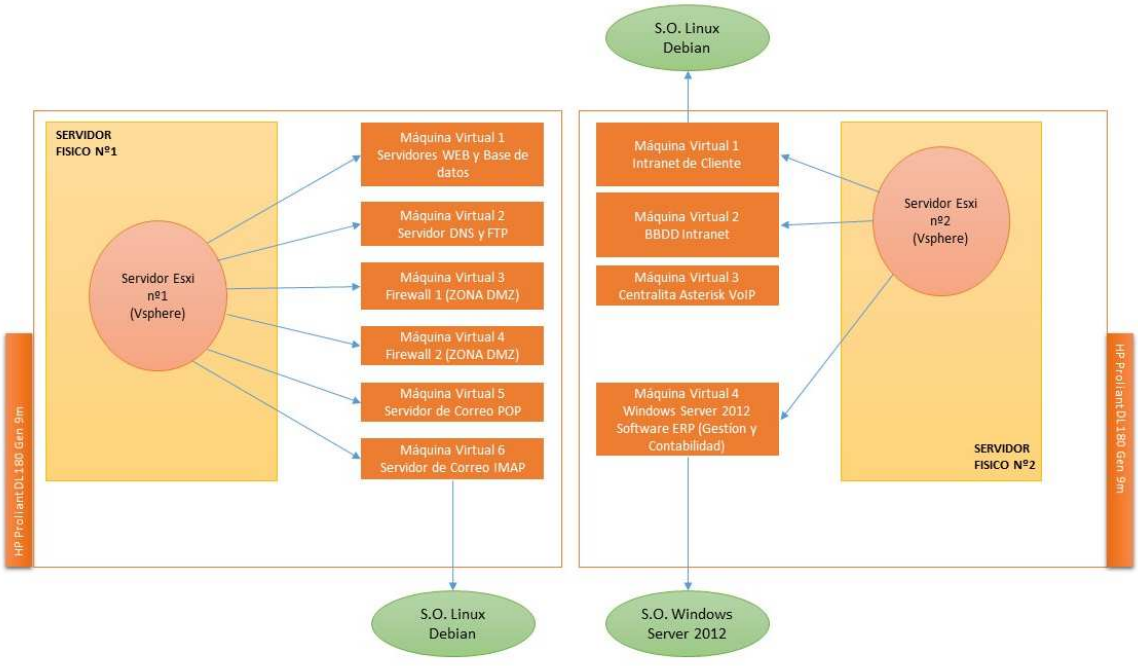

Figura 3-21 Distribución máquinas virtuales en Servidores Físicos

3.3.7 ELECCIÓN DEL HARDWARE PARA SERVIDORES.

Las características mínimas que deben cumplir los modelos de servidor que se seleccionarán para cubrir las expectativas de la empresa son las siguientes:

- Servidor apilable.
- Capacidad de ampliación, rendimiento, fiabilidad y gestionabilidad.
- Menor costo posible.

Atendiendo a estos requisitos una buena elección en cuanto a hardware de servidor sería la gama de servidores ***HP Proliant DL 180 Gen 9m***, por los siguientes motivos:

1. Escalabilidad: proporciona amplia capacidad de almacenamiento bajo demanda con configuraciones de 4 a 12 unidades con factor de forma grande (LFF) y de 8 a 16 unidades con factor de forma reducido (SFF).
2. Admite hasta dos procesadores Intel Xeon E5-2600 v3 con un máximo de 12 núcleos.
3. Admite hasta 16 ranuras DIMM de memoria DDR4.
4. Dispone hasta 6 ranuras PCIe 3.0 para admisión de una amplia gama de GPU, y tarjetas de Red.
5. Disponibilidad de datos con tecnología SAS de 12 Gb/s.
6. Alta disponibilidad y eficiencia para aplicaciones de almacenamiento denso.
7. Dispone de tecnología HP SmartDrive, para mejora de mantenimiento y pérdida de datos.
8. Dispone de HP SmartMemory, para evitar la pérdida de datos y el tiempo de inactividad.
9. Ahorro de hasta un 94% de eficiencia, reduciendo el consumo y la capacidad de refrigeración del sistema de servidores.
10. Gestión ágil de la infraestructura: ofrece una gestión convergente para simplificar la automatización a través de servidores, almacenamiento y red.
11. Paneles personalizados de gestión en línea, para visualizar el estado de la infraestructura.
12. Gestión integrada para implementar, supervisar y dar soporte al servidor de forma remota.
13. Actualizaciones de firmware y controladores, reduciendo el tiempo de inactividad.

La gama de servidores proliant son adaptables al presupuesto que la empresa disponga, ya que existen diferentes familias del mismo producto y diferentes modelos configurables y adaptables a los requerimientos de cualquier tipo de cliente.

3.4 ESCALABILIDAD DE LA INFORMACIÓN.

El sistema informático planteado en el presente TFC, corresponde a la arquitectura de un sistema distribuido, debido a que no deja de ser una colección de computadores autónomos enlazados mediante una red computacional y además estará equipada con un software de sistema distribuido. El software de sistema distribuido habilita a los computadores para coordinar sus actividades y para compartir los recursos del sistema, tanto hardware como software y datos.

Un sistema distribuido opera de manera efectiva y eficiente a muchas escalas diferentes. La escala más pequeña desde el punto de vista de un sistema distribuido correspondería a dos estaciones de trabajo conectadas a un servidor de ficheros. Un sistema distribuido construido alrededor de una red de área local simple podría contener cientos de estaciones de trabajo, varios servidores de ficheros, y otros servidores de propósito específico. Está red simple, podría comunicarse con otras redes de área local, o definir varias subredes dentro de la misma red local, conformado entre todas ellas un único sistema distribuido, permitiendo que los recursos sean compartidos entre todas ellas, como es el caso de la red de nuestro TFC.

Uno de los objetivos de la implantación de la red del presente TFC es la de garantizar la escalabilidad del sistema a cinco años vista, esto significa que tanto el software de sistema como el de aplicación no deberían cambiar aunque la escala del sistema aumente. La demanda de escalabilidad en las organizaciones actuales y en sus sistemas distribuidos ha conducido a una filosofía de diseño en la que cualquier recurso simple –hardware o software- puede extenderse para proporcionar servicio a tantos usuarios como se quiera, de tal forma que si la demanda de un recurso crece, debería ser posible extender el sistema para darle servicio.

3.4.1 ESCALABILIDAD HORIZONTAL DEL SISTEMA.

La escalabilidad horizontal será la capacidad del sistema de poder soportar o añadir nuevos equipos conectados al sistema distribuido, sin costo adicional en modificaciones de la estructura de la red.

La empresa actualmente tiene previsión de que pueda haber un incremento de personal a cinco años entre el 20 y el 25%. La red como está planteada en el presente TFC, estará diseñada para soportar un aumento de host conectados al sistema distribuido sin ningún coste adicional en cuanto a infraestructura, ya que está suficientemente dimensionado para este objetivo (Ver apartado 3.1.4.). Si se produjese un aumento mayor a este porcentaje, se podría necesitar adquirir algún dispositivo adicional de comunicaciones tales como Switches, e incorporarlos a su correspondiente zona con el mínimo gasto en implementación, debido a que el sistema está perfectamente modularizado.

Si hubiese modificaciones en cuanto a la reubicación de personal en los departamentos de la empresa, simplemente se deberían tocar temas de configuraciones a nivel de VLAN y permisos, sin necesidad de cambiar instalaciones físicas.

3.4.2 ESCALABILIDAD VERTICAL DEL SISTEMA.

La escalabilidad vertical o la capacidad de agregar recursos a un solo nodo del sistema (cpu, memorias, discos duros), estará calculada para no hacer desembolso adicional en el plazo marcado, incluso aunque se produjese el crecimiento de personal del 20-25% visto anteriormente.

Con los recursos presupuestados, quedará cubierto este hecho aunque a priori no sabremos el crecimiento del volumen de información almacenada en el sistema.

El sistema se diseñará estimando un aumento de la información almacenada del 30% anual. Los servidores recomendados en el presente TFC están calculados, para que no exista ningún problema de almacenamiento de la información con el costo de inversión previsto inicialmente.

En las características de los servidores vistas anteriormente, se observó que los servidores aconsejados para este TFC, son modulables, y pueden ser ampliados en cuanto a recursos físicos tales como memoria RAM, procesadores, y almacenamiento. La inversión inicial planteada cubrirá las expectativas en cuanto a almacenamiento durante los próximos cinco años.

Si se requiriese almacenamiento adicional futuro, se podrá aumentar la capacidad en los servidores, y en el servidor NAS de almacenamiento (Ver capítulo 3.5.).

3.5 SOLUCION DE ALMACENAMIENTO Y COPIAS DE SEGURIDAD.

3.5.1 SISTEMA NAS.

El almacenamiento conectado en red (NAS) es un dispositivo de almacenamiento compartido que proporciona servicios de almacenamiento y sistema de archivos consolidados para servidores de sistemas abiertos. En nuestra red las aplicaciones y los usuarios obtendrían el acceso a los datos a través de la red utilizando el protocolo (IP). Cada dispositivo NAS utilizaría su propia IP exclusiva.

Puede ser difícil administrar y respaldar grandes cantidades y distintos tipos de niveles de versiones de almacenamiento conectado directamente (DAS) o de almacenamiento interno, además de costoso debido a las tasas muy bajas de utilización total. NAS proporciona ahorros de costos y la simplicidad de consolidar almacenamiento mediante la red IP existente sin necesitar del costo y la complejidad de crear y mantener una red secundaria como con la red de área de almacenamiento (SAN).

En el siguiente esquema se muestra dónde estaría ubicado el sistema de almacenamiento NAS en una estructura de red similar a la planteada en el presente TFC.

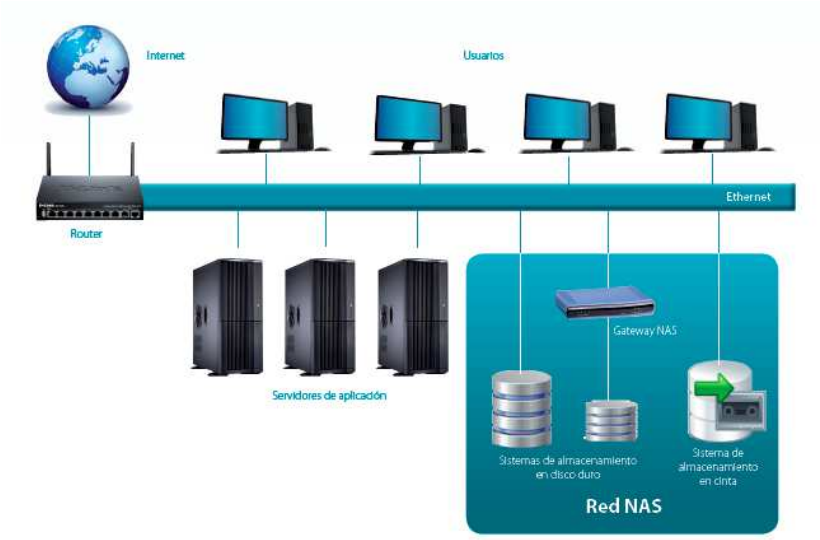

Figura 3-22 - Esquema conceptual NAS

Como se ha comentado en el apartado anterior dedicado a los servidores y virtualización, los servidores físicos disponen de almacenamiento propio para alojar el servidor Esxi, así como las máquinas virtuales.

En el servidor de almacenamiento NAS, se alojarán los datos de usuario de la red corporativa (documentos de trabajo, imágenes, hojas de cálculo, etc). La centralización de los datos en un único sistema de almacenamiento, permite centralizar la información y facilita el acceso a la misma al resto de usuarios de la red corporativa.

El dispositivo de almacenamiento NAS, en la infraestructura de nuestra red también se utilizará para volcar las copias de seguridad de los servidores virtuales, para una eventual recuperación de uno de ellos (aunque también se requerirá que estas copias de seguridad se almacenen externamente, como se verá posteriormente).

Una solución económica de este tipo de dispositivo es la gama de servidores NAS de EMC, en concreto el modelo Lenovo EMC px4-400r Network Storage Array 70CL - 70CL9000WW[6].

El esquema integrando el servidor NAS dentro de la red quedaría tal como se indica en la siguiente figura.

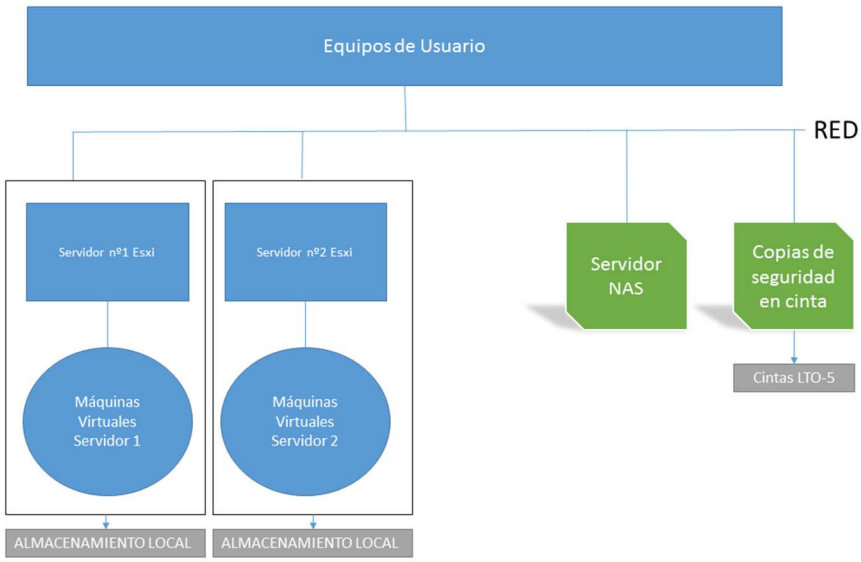

Figura 0-1 - Integración del NAS en la infraestructura de la red

[6] Para más información sobre este producto http://www.tiendalenovo.es/lenovoemc-px4-400r-network-storage-array-70cl-70cl9000ww.html?gclid=CJDKoJKR-8ECFS3HtAod2XUAiQ

3.5.2 COPIAS DE SEGURIDAD.

En informática una copia de seguridad o backup, es una copia de los datos originales que servirá para disponer de un medio para volver a recuperarlos en caso de pérdida. Las copias de seguridad son de vital importancia en la gestión de la estructura de un sistema informático debido a que serán necesarias ante este tipo de eventualidades:

- Recuperar los sistemas informáticos y los datos ante una posible catástrofe informática, natural o ataque.
- Restaurar una pequeña cantidad de ficheros por posible eliminación accidental, por corrupción de ficheros, por infección de virus u otras causas.
- Almacenar información histórica.

Las copias de seguridad pueden ser de dos tipos: del sistema o de datos. Dichas copias tienen como objetivo dotar de una herramienta que permita recuperar el sistema ante un incidente determinado, por lo tanto realizan una copia del propio sistema operativo y del software instalado. Las copias de seguridad de datos tienen el objetivo de almacenar solamente información de ficheros y bases de datos.

Las copias de seguridad del sistema en la empresa objeto de estudio pueden ser menos sensibles en cuanto a criticidad de la misma, ya que en un momento dado siempre se puede partir del software de instalación original para recomponer el sistema, ahora bien una buena planificación de la misma hará que se ahorre un tiempo considerable para conseguir el mismo fin. Sin embargo las copias de ficheros y datos son bastante más sensibles, ya que una pérdida de este tipo de datos puede ser definitiva e irrecuperable, además este tipo de copias de seguridad deberían depositarse externamente al propio sistema en un tipo de soporte tales como CD-ROMS, DVD-ROMS, cintas mágneticas (DDS), incluso ser almacenadas por los responsables de seguridad informática de la empresa en un recinto seguro ante una catástrofe de la empresa (incendio, etc).

Tener una buena planificación de este tipo de copias de seguridad es una parte crítica de la planificación informática de las empresas y de su política de seguridad. Este tipo de medidas serán vitales para el correcto funcionamiento de la empresa, e incluso de su viabilidad, debido a que ante una eventual pérdida de información sin la correcta planificación de este tipo de medidas puede poner en riesgo la continuidad de la empresa.

Para decidir qué tecnología sería la adecuada habría que tener en cuenta lo siguiente:

- Volumen de datos a copiar.
- El coste económico del sistema de copia.
- La operatividad de la solución escogida tanto para el tiempo de copia como para el tiempo de recuperación.

Para la correcta planificación de las copias de seguridad, algunas de las decisiones que se tendrían que tomar serían las siguientes:

- La periodicidad de las copias. Cuanto más periódicamente se realicen este tipo de copias, mayor capacidad de recuperación se obtendrá.
- El número de copias. Si se hacen más de una copia y como se ha indicado anteriormente se depositan en ubicaciones separadas, se aumentará la seguridad.
- Compresión de los datos. Para aprovechar la capacidad de almacenamiento disponible aumenta el volumen de datos a copiar, pero incrementa el tiempo de copia.
- Tipo de modelo de copia: completa, diferencial o incremental. Dependiendo de si el tipo de datos para realizar la copia de seguridad es de sistema o de datos.

3.5.3 SOLUCIÓN ELEGIDA PARA COPIAS DE SEGURIDAD DE LOS SERVIDORES.

Para realizar las copias de seguridad de los servidores virtuales se utilizará vSphere Data Protection. Este software es la solución de Backup de VMware en la actualidad.

El producto vSphere Data Protection está incluido en todas las versiones de vSphere con la excepción de vSphere Essentials. Es decir que tanto vSphere Essentials Plus, Standard, Enterprise y Enterprise Plus incluyen este Appliance.

La solución de copias de seguridad de VMware está orientada a copias a disco y se integra totalmente con vCenter. De hecho la única forma de gestionar este Appliance es mediante el vSphere Web Client.

Las principales características de VMware vSphere Data Protection son las siguientes:

- Almacenamiento de duplicado de las Copias de Seguridad.
- Solución de Backup sin agentes en las Máquinas Virtuales.
- Soporte FLR que permite recuperación a nivel de fichero (Windows y Linux).
- Utiliza la tecnología de Snapshots en segundo plano para copias en caliente.
- Soporte de CBT (Change Block Tracking) que permite copias diferenciales optimizadas.
- Copia de un máximo de 100 Máquinas Virtuales por Appliance
- Cada servidor de vCenter puede gestionar un máximo de 10 Appliance de VDP (vSphere Data Protection).
- Gestión únicamente a través de vSphere Web Client (requiere Adobe Flash).

FORMA DE ALMACENAMIENTO Y CÁLCULOS NECESARIOS.

El Appliance es una Máquina Virtual con Sistema Operativo Linux SUSE Enterprise que está aprovisionada con 4 vCPUs y 4 GB de Memoria RAM.

Existen tres tipos de Appliance predefinidos, cada uno con un tamaño: 500GB, 1TB y 2TB.

Los discos pueden ser configurados tanto en formato Thin Provisioning como también en Thick.

Los tamaños de consumo real de cada disco son de 850GB, 1,3TB y 3,1TB respectivamente.

Se deberán realizar algunos cálculos para determinar el número Appliances a desplegar considerando el total de Máquinas Virtuales a copiar, su tamaño, su tasa de crecimiento y la política de retención a utilizar para conocer la relación de VM/VDP Appliance y el tamaño preconfigurado del disco del vSphere Data Protection que se utilicen. Este cálculo se explicará seguidamente.

Se debe tener en cuenta que, una vez desplegado el VDP, no es posible modificar el tamaño del disco. En caso de necesitar más espacio se tendrá simplemente que desplegar un VDP adicional.

Según se ha indicado anteriormente como característica del sistema, se pueden almacenar hasta 100 Máquinas Virtuales, por appliance, pero naturalmente que esto dependerá de varios factores como el tamaño de la VM, tasa de crecimiento, política de retención, etc.

Para el caso del presente proyecto se deberá comprobar el tamaño de ocupación de cada una de las máquinas virtuales, una vez instaladas y en funcionamiento, para determinar el número de VDP.

vSphere Data Protection realiza una única copia completa de cada Máquina Virtual y a partir de esa primera copia todos los backups de esa VM son diferenciales a nivel de bloque, y se irá incrementando su tamaño dependiendo de la política de retención y la tasa de crecimiento de la propia Máquina Virtual.

De esta forma el espacio real en disco que consumirán las copias estará extremadamente optimizado.

Para el caso de los dos servidores Esxi, el dimensionamiento de capacidad aproximado, teniendo en cuenta el número de máquinas virtuales a instalar sería el siguiente:

SERVIDOR ESXI Nº1	**TAMAÑO DE INSTALACION APROX**	**ESTIMACIÓN DE CARGA DE DATOS**	**TAMAÑO TOTAL APROX**
Servidores Web	20 (Gb) Linux Debian	200 Gb	220 Gb
Servidor DNS y FTP	20 (Gb) Linux Debian	40 Gb	60 Gb
Firewall Nº 1	20 (Gb) Linux Debian	20 Gb	40 Gb
Firewall Nº 2	20 (Gb) Linux Debian	20 Gb	40 Gb
Servidor de Correo POP	20 (Gb) Linux Debian	100 Gb	120 Gb
Servidor de Correo IMAP	20 (Gb) Linux Debian	100 Gb	120 Gb
TOTAL	***120 GB***	***480 GB***	***600 GB***
ESPACIO COPIAS SEG			***600 GB***
ALMACENAMIENTO EXTRA			***500 GB***
DIMENSIONAMIENTO APROXIMADO			**1.7 - 2 TB**

Tabla 5 - Dimensionamiento de capacidad Servidor Esxi número 1

SERVIDOR ESXI Nº2	**TAMAÑO DE INSTALACION APROX**	**ESTIMACIÓN DE CARGA DE DATOS**	**TAMAÑO TOTAL APROX**
INTRANET	20 (Gb) Linux Debian	80 Gb	100 Gb
BBDD	20 (Gb) Linux Debian	80 Gb	100 Gb
ASTERISK	20 (Gb) Linux Debian	20 Gb	40 Gb
WINDOWS SERVER 2012 (y aplicación ERP)	40 (Gb) Linux Debian	100 Gb	140 Gb
TOTAL	***100 GB***	***280 GB***	***380 GB***
ESPACIO COPIAS SEG			***380 GB***
ALMACENAMIENTO EXTRA			***500 GB***
DIMENSIONAMIENTO APROXIMADO			**1.5 TB**

Tabla 6 - Dimensionamiento de capacidad Servidor Esxi número 2

En principio se necesitarían dos appliances predefinidos de un tamaño aproximado de 1.5 TB - 2TB.

LICENCIA DE Vsphere Data Protection.

VMware VDP se licencia junto con los Host y el vCenter y el precio está embebido en la propia licencia del Host y vCenter.

Por cada servidor de vCenter es posible desplegar hasta un máximo de 10 Appliances de vSphere Data Protection, a la vez que cada Appliance es capaz de gestionar la copia de hasta 100 Máquinas Virtuales.

Tanto si se tiene un único Host de vSphere con un servidor de vCenter, se podrá desplegar el máximo de 10 Appliances.

La licencia que se usará para dar todo el servicio al sistema del presente TFC como se ha comentado en el punto (3.3.6) será la Essentials Plus, que cubre todas las funcionalidades vistas en el presente TFC, e incluye la nueva versión de vCenter Data protection comentada.

3.5.4 SISTEMA DE COPIA DE SEGURIDAD EXTERNA Y PLANIFICACIÓN.

Para la realización de copias de seguridad en un dispositivo externo que puedan ser almacenadas de forma segura por el responsable de seguridad de la empresa, y cumplir con las garantías de la Ley de protección de datos, se recomienda un sistema de cintas LTO-5, debido a su constante evolución y las prestaciones que ofrece este sistema.

Existirían posibilidades más económicas que la escogida en el presente TFC, si bien también existen opciones mucho más costosas, por ejemplo las de almacenamiento en disco, pero el hecho de escoger esta opción inicialmente queda determinada por los siguientes motivos:

- Capacidad de almacenamiento elevada por cinta extraíble.
- Seguridad en los datos almacenados.
- Control de acceso a los datos almacenados mediante cifrado AES, evitando accesos no autorizados.
- Alta velocidad de transferencia.
- Alta fiabilidad.
- Relación calidad/precio.

Para determinar el número de medios extraíbles (cintas LTO) que se requerirían para garantizar la correcta utilización de los distintos tipos de copias de seguridad (completa, diferencial o incremental), se tomará como referencia el dimensionamiento aproximado de los dos servidores Esxi, al que habrá que añadir el tamaño del volumen de ficheros de trabajo del resto de los equipos de la red. Esta información de trabajo (documentos de texto, pdf, hojas de cálculo, imágenes, etc.) estaría almacenada en el servidor NAS.

Teniendo en cuenta que el número de usuarios de la empresa es de unas 50 personas aproximadamente, si se reservase un espacio aproximado de unos 200 GB de información por usuario, se necesitaría un espacio adicional de 1 a 1,5 TB (TeraBytes) de información.

El tamaño aproximado de almacenamiento de una cinta es de 1.5 a 3 TB (como se verá más adelante), por lo que se necesitarían 2 cintas para hacer una copia de seguridad de toda la infraestructura de datos de la red.

Teniendo en cuenta los requisitos de capacidad planteados, la planificación de copias de seguridad podría ser como la siguiente:

SÁBADOS 11:00 PM: COPIA COMPLETA. MEDIOS: S1, S2, S3, S4, S5(*)

- LUNES 11:00 PM: COPIA DIFERENCIAL. MEDIO: L
- MARTES 11:00 PM: COPIA DIFERENCIAL. MEDIO: M
- MIERCOLES 11:00 PM: COPIA DIFERENCIAL. MEDIO:X
- JUEVES 11:00 PM: COPIA DIFERENCIAL. MEDIO:J
- VIERNES 11:00 PM: COPIA DIFERENCIAL. MEDIO: V

(*) S5 solo se utilizaría en el caso que coincidan 5 sábados.

Cada medio de copia completa S(n), en función del volumen de datos, estará formado por dos o más cintas LTO, por ejemplo, aunque debido a su alta capacidad, podría ser también de una sola cinta LTO. Sin embargo, lo más normal será que los medios diferenciales e incrementales sí que tengan suficiente con una única cinta LTO, ya que normalmente ocupan poco volumen. En tal caso, se necesitarían un total de 10 cintas LTO, para empezar, ya que de esta forma se podrá tener un plan de copias de seguridad que podría permitir restaurar todo el contenido hasta un mes de antelación.

En principio, con lo indicado anteriormente no sería suficiente, por lo que se deberá recurrir al archivado de medios por más tiempo, de forma que si se sustituye el Medio S1 por uno que lleve el nombre del mes, se estará guardando el contenido del primer sábado de cada mes durante un año:

ENE, FEB, MAR, ABR, MAY, JUN, JUL, AGO, SEP, OCT, NOV, DIC.

Con esta modificación, se restauraría toda la información hasta un año hacia atrás, pero si además se sustituye el medio ENE (enero) por cinco nuevos medios de rotación que se sobrescriban anualmente, se podrá recurrir a un backup de la información hasta 5 años hacia atrás. Con este último cambio, el conjunto de medios resultante sería el siguiente:

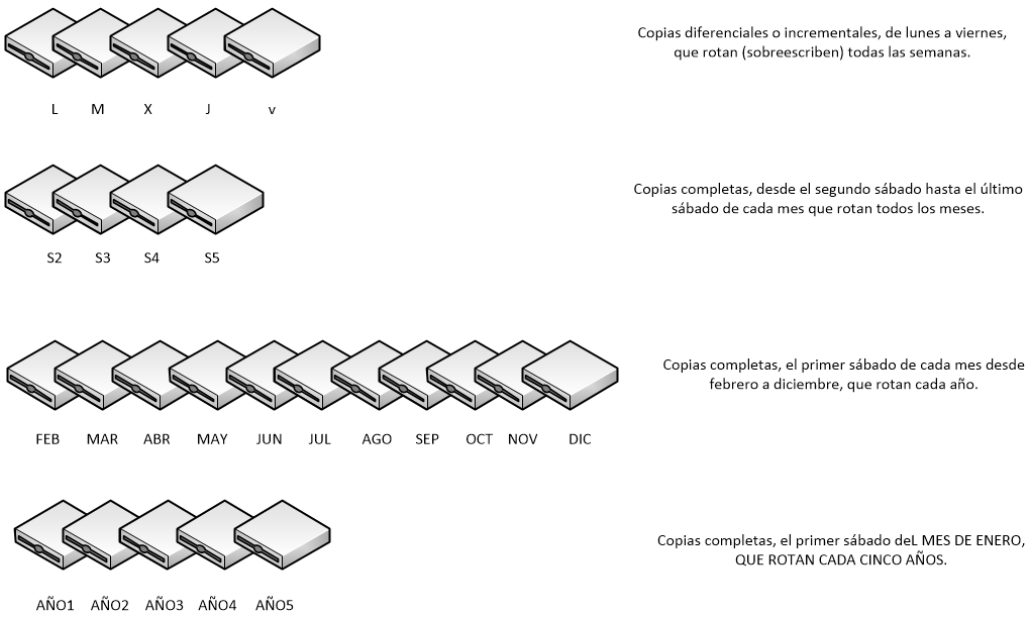

Figura 0-2 Distribución temporal de copias de seguridad en cinta LTO

En resumen, con un conjunto de medios finito (25 cintas LTO), se definirá un plan de copias de seguridad que permitiese recuperar la siguiente información de esta manera:

- Datos perdidos cualquier día de la semana anterior.
- En caso de necesitar datos más antiguos de una semana, se podrán recuperar de sábado en sábado, ya que los medios diarios habrán sido sobrescritos.
- En caso de necesitar datos más antiguos de un mes, se podrán recuperar de mes en mes (primer sábado de cada mes, que corresponde a las cintas etiquetadas con el nombre de cada mes).
- En caso de necesitar datos más antiguos de un año, se podrá recurrir a las cintas LTO etiquetadas como AÑO(n), que contendrán un backup completo del primer sábado de cada año.

En función de las necesidades de la empresa, se modificará el número de cintas, el calendario de backup y los horarios, esto se traducirá en un cambio en el ámbito de restauración, permitiendo el ajuste personalizado del plan de copias de seguridad. De esta forma se obtendría un plan de copias de seguridad bastante completo, con un número de medios moderadamente reducido.

SISTEMA CINTAS LTO-5 SELECCIONADO.

El sistema de cintas recomendado para el presente TFC es el HP LTO-5 Ultrium 3000 SAS Internal Tape Drive [7]con unidad de cinta del tipo LTO Ultrium (1.5 TB / 3 TB).

Las unidades de cinta HP LTO Ultrium, disponen de una tecnología que les permite almacenar hasta 3TB por cartucho. Este sistema se recomienda por los siguientes motivos:

- Capacidad y rendimiento con sistema de supervisión/gestión y cifrando hardware.
- Fiable y compatible: permite ajustar de forma dinámica y continua la velocidad de la unidad, para mantener el flujo de datos de las unidades y optimizar el rendimiento, a la vez que se reducen las paradas y reinicios para mejorar la fiabilidad de las unidades y cintas HP.
- Solución completa: proporciona soportes HP LTO, cartucho de limpieza, copia gratuita del software básico HP Data Protector Express, que incluye soporte para cifrado de datos de hardware y OBDR, cables y documentación.
- El tipo de interface es Serial Attached SCSI 2.

[7] Para más información sobre el producto
https://h10057.www1.hp.com/ecomcat/hpcatalog/specs/provisioner/99/EH957A.htm

3.6 RED WI-FI.

Para proporcionar RED Wi-Fi al edificio anexo, se necesitaría como mínimo dos puntos de acceso del tipo Access-Point (cisco aironet 1602i[8]), para suministrar señal a unos 60 equipos.

Estos dos puntos de acceso se colocarían en dos de las esquinas del recinto en diagonal, en suma estos dos puntos de acceso proporcionarán aproximadamente unos 600 Mbps, garantizando al menos 10 Mbps a cada uno de los equipos en máxima ocupación, aproximadamente.

Estos Access-Point utilizan los estándares 802.11b y 802.11g los cuales funcionan en la banda de 2.4 – 2.5 GHz de la ISM. Son los más utilizados en la actualidad.

En esta banda se definieron 14 canales utilizables para equipos Wi-Fi, que pueden configurarse para las necesidades particulares. Sin embargo los 14 canales no son completamente independientes ya que se reparten 83,5 Mhz de franja radioeléctrica disponible. El ancho de banda de la señal 22 Mhz es superior a la separación entre canales consecutivos (5Mhz), por este motivo se hace necesaria una separación de al menos 5 canales con el objetivo de evitar interferencias entre canales adyacentes.

Como máximo se utilizarán 3 canales dentro de un área determinada, por ejemplo, el 1 el 6 y el 9.

En este caso se utilizarán los canales 1 y 5 para dar servicio a cada uno de los Access-Point para dar conectividad a los equipos de la zona.

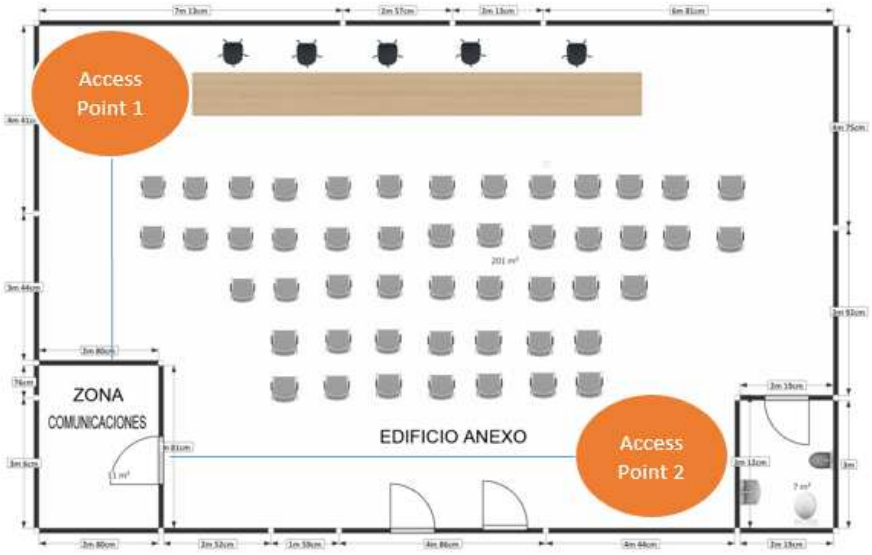

Figura 0-3 - Esquema Puntos de Acceso Wi-Fi

[8] Para más información sobre el producto
http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1600-series/data_sheet_c78-715702.html

3.7 ACCESO REMOTO VPN.

Uno de los objetivos a medio plazo, como queda reflejado en los requerimientos del cliente, será la de la creación de diversas sedes de la empresa en otras ciudades, para ello se necesita que el sistema esté preparado para comunicar las diversas sedes a la sede principal, de forma remota.

Para realizar este cometido, se plantea como solución el uso de las redes virtuales o VPN. Una red privada virtual VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública como internet. Los paquetes de datos de la red privada viajarán por un túnel definido en la red pública. De esta forma se permitirá que la computadora de nuestra red envíe y reciba datos sobre redes públicas como si fuera una red privada con toda funcionalidad, seguridad y políticas de gestión de este tipo de redes.

3.7.1 REQUERIMIENTOS BASICOS DE UNA VPN.

Cuando se plantea la utilización de un sistema VPN, se debe asegurar que el mismo garantiza las siguientes características:

- Identificación de usuario: La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados, además deberá crear registros de conectividad, estadísticos, y uso del sistema.
- Administración de direcciones: la VPN deberá establecer una dirección del cliente a la red privada.
- Codificación de datos: los datos que se vayan a transmitir a través de la red pública, deberán viajar de forma encriptada, para que no puedan ser leídos por usuarios que no tengan acceso a la red privada.
- Administración de claves: la VPN ha de generar y renovar las claves de codificación para el cliente y el servidor.
- Soporte de múltiples protocolos de comunicaciones: la VPN debe poder soportar los protocolos más comunes que se utilizan en la red pública, tales como el protocolo de internet (IP), intercambio de paquetes a través de internet (IPX), etc.

3.7.2 VENTAJAS DE UNA VPN.

Entre las ventajas más significativas de la utilización de una VPN, son la integridad, confidencialidad y seguridad de los datos, así como:

- Reducción de costos.
- Facilidad de uso.
- Control de acceso basado en políticas de la organización.
- Los algoritmos de compresión optimizan el tránsito de la información del cliente.
- Facilidad de instalación en el cliente, en cualquier PC.

3.7.3 APLICACIÓN DE LA VPN A LA RED CORPORATIVA OBJETO DE ESTUDIO.

Para conectar la sede principal con las futuras sedes mediante VPN, se utilizará un router/firewall con capacidad de gestión y creación de túneles VPN, que facilitará la tarea de conexión y enlace.

En la sede principal, se utilizará un router/firewall, de más alta gama que en las sedes secundarias, por ejemplo el sonicwall TZ215 de la casa DELL. Este Router/firewall es capaz de soportar un máximo de 25 conexiones VPN de forma simultánea.

En el resto de sedes se podrá utilizar un router/firewall de menor gama, como por ejemplo el sonicwall TZ160, que serviría para crear la conexión túnel entre sedes.

Para la creación de las VPN, este tipo de dispositivos disponen de asistentes bastante sencillos para la realización de la configuración necesaria para el establecimiento de la conexión.

El esquema resultante será como el que se muestra en la figura:

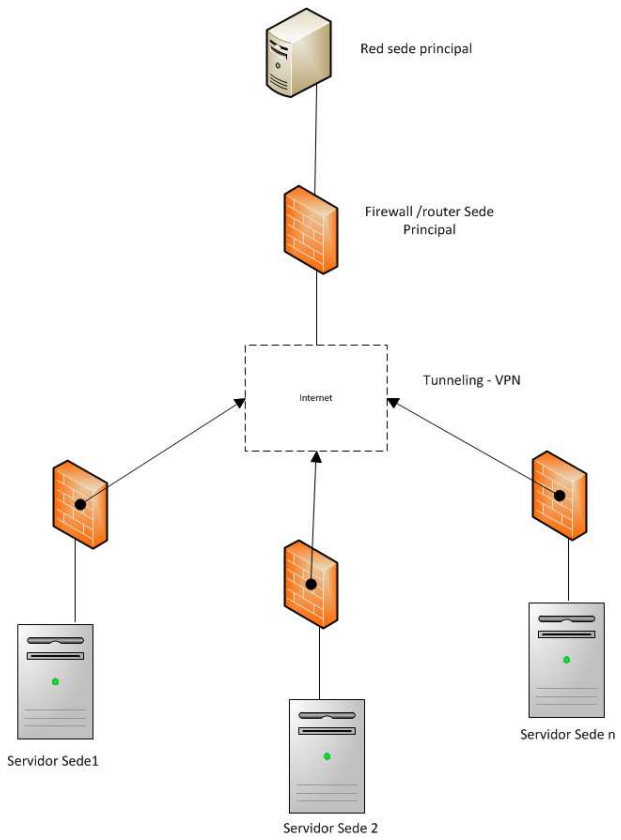

Figura 0-4 Esquema VPN entre sede principal y secundarias

3.8 SEGURIDAD DE LA RED CORPORATIVA.

En este último apartado se hará referencia a aspectos relativos a la seguridad informática de la red corporativa.

Hoy en día las redes de ordenadores son más esenciales para la vida diaria y empresarial, incrementándose en igual medida los ataques e intrusiones a través de las redes públicas y privadas, y pueden causar daños irreparables.

Existen multitud de tipos de amenazas y ataques que puede sufrir nuestra red, como por ejemplo: ataques de denegación de servicio, sniffing, man in the middle, spoofing, pharming, etc.

Para combatir estos tipos de ataques, existen numerosas herramientas en la actualidad, que se pueden utilizar para realizar una auditoría a nuestra red tales como wireshark, nmap, etc.

Las amenazas de seguridad causadas por intrusos en redes corporativas tales como las del presente TFC, pueden ser de dos tipos principalmente:

- Amenaza externa: los atacantes son externos a la red privada y logran introducirse desde redes públicas.
- Amenaza interna: los atacantes acceden sin autorización o pertenecen a la red privada de la organización, comprometiendo así la seguridad, información y servicios de organización

Como propuesta para la protección ante posibles amenazas internas, se plantean las siguientes acciones:

- Realizar un buen diseño de subredes dentro de la red corporativa.
- Crear políticas de administración de direccionamiento estático para servidores y routers.
- Monitorización del tráfico en la red.
- Realizar modificaciones de configuraciones de seguridad, de forma periódica.
- Establecer un nivel alto de seguridad en redes inalámbricas.

Como se ha indicado en el apartado de estructura lógica de la red (apartado 3.2), ésta dispondrá de una zona DMZ que se deberá proteger mediante dos firewalls. Un firewall es un dispositivo que filtra el tráfico entre redes (como mínimo dos). El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general un firewall se debe interpretar como una caja con dos o más interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no.

Hoy en día un firewall es un hardware específico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red.

En el presente TFC, para la protección de la DMZ se propone el uso de dos máquinas montadas en Linux con IPTABLES como se explica seguidamente, para evitar adquirir hardware adicional para cumplir la misma función.

3.8.1 IPTABLES.

IPtables es un sistema de firewall vinculado al kernel de Linux. Mediante iptables que estará instalado en el sistema operativo se ejecutarán una serie de reglas, mediante las cuales se decidirá qué se hace con un paquete en concreto, en función de cómo estén definidas estas reglas.

Existen 3 tipos de reglas de filtrado INPUT, OUTPUT, O FORWARD. Además de reglas de filtrado, mediante IPtables se pueden aplicar reglas de tipo MANGLE, destinadas a modificar los paquetes, y reglas NAT, encargadas de redireccionar puertos y realizar cambios en las IPs de origen y destino.

Las reglas de filtrado INPUT y OUTPUT se aplican a los paquetes que van a la misma máquina, mientras que las reglas de filtrado FORWARD, filtran paquetes que van dirigidos a otras redes o máquinas.

Las reglas PREROUTING Y POSTROUNTING, son reglas de filtrado NAT.

Los firewalls de protección de la DMZ del presente TFC ejecutarán scripts con este tipo de reglas, los cuales tendrán el siguiente aspecto:

Ejemplo de protección de la misma máquina:

```
#!/bin/sh
## Ejemplo de script para proteger la propia máquina
## FLUSH de reglas

iptables –F
iptables –X
iptables –Z
iptables -t nat -F

## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

## Empezamos a filtrar

# El localhost se deja (por ejemplo conexiones locales a mysql)

iptables -A INPUT -i lo -j ACCEPT

# A nuestra IP le dejamos total acceso
iptables –A INPUT –s 195.65.34.234 –j ACCEPT
```

```
# Al administrador de base de datos le dejamos entrar al mysql para que mantenga la BBDD
iptables –A INPUT –s 231.45.134.23 –p tcp –-dport 3306 –j ACCEPT

# A un diseñador le dejamos usar el FTP
iptables –A INPUT –s 80.37.45.194 –p tcp –dport 20:21 –j ACCEPT

# El puerto 80 de www debe estar abierto, es un servidor web.
iptables –A INPUT –p tcp -–dport 80 –j ACCEPT

# Y el resto, lo cerramos
iptables –A INPUT –p tcp -–dport 20:21 –j DROP
iptables –A INPUT –p tcp –-dport 3306 –j DROP
iptables –A INPUT –p tcp –-dport 22 –j DROP
iptables –A INPUT –p tcp –-dport 10000 –j DROP

# Fin del script
```

Como se puede comprobar en el ejemplo anterior sobre el uso de Iptables, se ve que existen diferentes tipos de cadenas para definir el comportamiento de los paquetes según las reglas que se definan en cada una de éstas, si es que se define alguna. Básicamente, el significado de las palabras principales que se encuentran en el ejemplo son las siguientes:

INPUT: Tráfico de entrada al sistema.
OUTPUT: Tráfico de salida del sistema.
FORWARD: Tráfico de redirección de cadenas de NAT.
PREROUTING: Acciones previas de enrutamiento de los paquetes.
POSTROUTING: Acciones posteriores al enrutamiento de los paquetes.
MASQUERADE: El objetivo especificado enmascara una dirección IP privada con una dirección IP externa del firewall / gateway.
DROP: Esta opción se pone al final de la sentencia para indicar que el paquete se ignore.
REJECT: Esta opción devuelve un paquete indicando que el paquete no está al alcance.
LOG: Identifica el paquete y sigue con las reglas establecidas.
ACCEPT: Acepta los paquetes de la regla determinada.

3.8.2 SISTEMAS IPS/IDS.

Como herramienta de detección de intrusiones en un entorno empresarial como el planteado en el presente TFC, se propone el uso de ***SNORT*** como sistema de detección de intrusiones.

El esquema básico que compone la arquitectura de este sistema es el siguiente:

- Módulo de captura de tráfico: es el encargado de capturar todos los paquetes de la red.
- Decodificador: es el encargado de formar las estructuras de datos con los paquetes capturados e identifica los protocolos de enlace, de red, etc.
- Preprocesador: permiten extender las funcionalidades preparando los datos para la detección. Existen diferentes preprocesadores dependiendo del tráfico que queremos analizar (por ejemplo: http, telnet…)
- Motor de detección: analiza los paquetes en base a las reglas definidas para detectar los ataques.
- Archivo de reglas: definen el conjunto de reglas que rigen los análisis de los paquetes detectados.
- Plugins de detección: partes del software que son compilados con Snort usados para modificar el motor de detección.
- Plugins de salida: permiten definir qué, cómo y dónde se guardan las alertas y los correspondientes paquetes de red que las generan. Pueden ser archivos de texto, bases de datos, etc.

Para poder llevar a cabo una buena configuración, no sólo hay que tener un detector de intrusiones activado en el sistema, sino que necesitaremos también herramientas de prevención de intrusiones tipo antivirus, etc. Snort se utilizará como herramienta adicional para facilitar el trabajo del administrador del sistema y tener controlado los puntos más débiles del sistema en cuestión, por ejemplo la exposición de ciertos servicios a internet.

Snort podrá ser instalado en los Firewalls Linux que disponen de Iptables, para controlar el tráfico desde o hacia la red interna. La configuración de reglas se realizará en base a las políticas de seguridad de la empresa, y serán gestionadas por el administrador del sistema. La creación de las políticas de seguridad y la configuración de snort para el uso concreto asociado a estas políticas serían analizadas con posterioridad a la implantación de la red.

3.8.3 SSH y CERTIFICADOS DIGITALES.

Los usuarios “maliciosos” tienen a su disposición herramientas que les permiten interceptar y redirigir el tráfico de la red para ganar acceso al sistema. En términos generales este tipo de amenazas se pueden clasificar de la siguiente manera:

- Intercepción de la comunicación entre dos sistemas: en este escenario, existe un tercero en algún lugar de la red entre entidades en comunicación que hace una copia de la información que pasa entre ellas. La parte interceptora puede capturar y conservar la información, o puede modificarla y luego enviarla al recipiente al cual estaba destinada. Este ataque se puede realizar a través del uso de un software de tipo sniffer, una utilidad de red muy común.
- Personalización de un determinado host: con esta estrategia, un sistema interceptor finge ser el recipiente a quien está destinado un mensaje. Si la estrategia funciona, el sistema del usuario no se da cuenta del engaño y continúa la comunicación con el host incorrecto. Esto se produce con técnicas como el envenenamiento del DNS o spoofing de IP.

Ambas técnicas interceptan información potencialmente confidencial y si esta interceptación se realiza con propósitos hostiles, el resultado puede ser catastrófico.

Utilización de SSH para mejorar la seguridad en la Red.

SSH™ (o *S*ecure *SH*ell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host de forma remota. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

Para el caso de este TFC, el uso de SSH se aplicaría para proteger a los servidores web, y a las conexiones VPN.

Si se utiliza SSH para inicios de sesión de shell remota y para copiar archivos, se pueden disminuir las amenazas de seguridad vistas anteriormente notablemente. Esto es porque el cliente SSH y el servidor usan firmas digitales para verificar su identidad. Adicionalmente, toda la comunicación entre los sistemas cliente y servidor es encriptada. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una llave conocida sólo por el sistema local y el remoto.

4 VALORACION ECONÓMICA.

CANTIDAD	CONCEPTO	PRECIO UNITARIO	TOTALES
2	**IDF FORMADO POR**		
1	Rack 22U con panel de alimentación incorporado.	256,00 €	
1	Panel de parcheo 48 puertos	45,00 €	
1	Switch HP serie 2610 48 puertos	600,00 €	
	Subtotal	901,00 €	
	TOTAL APARTADO		**1.802,00 €**
1	**MDF FORMADO POR**		
1	Rack 42U, con panel de alimentación incorporado	400,00 €	
1	Panel de parcheo 48 puertos	45,00 €	
1	Switch HP serie 2610 48 puertos	600,00 €	
1	ROUTER HP MSR2000	800,00 €	
1	ROUTER/FIREWALL DELL sonicwall TZ215	900,00 €	
	Subtotal	2.745,00 €	
	TOTAL APARTADO		**2.745,00 €**
	CABLEADO ESTRUCTURADO		
1.200	METROS CABLE UTP CAT 5E	0,65 €	780,00 €
40	METROS CABLE FIBRA OPTICA COMUNICACIÓN IDF´S CN MDF	1,2	48,00 €
50	PUESTOS DE TRABAJO(ROSETAS) DOBLES CON TOMAS DE ALIMENTACIÓN	25,00 €	1.250,00 €
150	PATCH CORDS (1M)	0,75 €	112,50 €
	TOTAL APARTADO		**2.190,50 €**
	COMUNICACIÓN EDIFICIOS OPCIÓN 1		
300	METROS CABLE FIBRA OPTICA EXTERIOR PARA COMUNICACIÓN EDIF. PRINCIPAL Y EDIF. SECUNDARIO	1,20 €	360,00 €
1	PERMISOS + INSTALACION	1.500 € APROX.	1.500,00 €
	TOTAL APARTADO		**1.860,00 €**
	COMUNICACIÓN EDIFICIOS OPCIÓN 2		
2	ANTENAS AIR FIBER 5 (UBITIQUI)	700,00 €	1.400,00 €
	TOTAL APARTADO		**1.400,00 €**
	RACK COMUNICACIONES EDIFICIO SECUNDARIO		
1	RACK 9U CON TOMAS DE ALIMENTACION INCORPORADAS	100,00 €	
1	SWITCH HP SERIES 2610 22 PUERTOS	400,00 €	
1	PANEL DE PARCHEO 22 PUERTOS	24,00 €	
	SUBTOTAL	**524,00 €**	
	TOTAL APARTADO		**524,00 €**

	HARDWARE DE SERVIDOR		
2	SERVIDORES HP PROLIANT DL180 GEN 9m (CARACTERÍSTICAS ESPECIFICADAS EN ANEXO NÚMERO 2)	2.400,00 €	
	SUBTOTAL	**4.800,00 €**	
	TOTAL APARTADO		**4.800,00 €**
	SOFTWARE DE VIRTUALIZACIÓN		
1	Licencia Vcenter Essentials	4.895,00 €	
	SUBTOTAL	**4.895,00 €**	
	TOTAL APARTADO		**4.895,00 €**
	SISTEMA DE ALMACENAMIENTO NAS		
1	LENOVO EMC PX4-400r NETWORK STORAGE ARRAY 70CL	1.600,00 €	
	SUBTOTAL	**1.600,00 €**	
	TOTAL APARTADO		**1.600,00€**
	COPIAS DE SEGURIDAD EN CINTA		
1	HP LTO5-ULTRIUM 2000 SAS INTERNAL TAPE	1.500,00 €	1.500,00 €
25	CINTAS LTO-5	35,00 €	875,00 €
	SUBTOTAL	**2.375,00 €**	
	TOTAL APARTADO		**2.375,00 €**
	RED WI-FI (EDIFICIO ANEXO)		
2	ACCESS POINT CISCO AIRONET 1602I	450,00 €	
	SUBTOTAL	**900,00 €**	
	TOTAL APARTADO		**900,00 €**
	LICENCIA WINDOWS 2012 SERVER		
1	WINDOWS 2012 SERVER R2	1.069,00 €	1.069,00 €
3	PACK 5 LICENCIAS CAL WINDOWS 2012	616,00 €	1.848,00 €
	SUBTOTAL	**2.917,00 €**	
	TOTAL APARTADO		**2.917,00 €**
	TOTAL PRESUPUESTO INSTALACIONES DE RED		26.148,50 €
	En el precio está incluido el I.V.A. La opción de comunicación entre edificios incluida es la de las antenas Air Fiber, ya que en principio desconoceríamos el importe de los permisos que habría que solicitar para la tirada de un cable físico entre edificios.		
	Los precios están obtenidos de la web, y no directamente con el fabricante, por lo que podríamos obtener mejores descuentos.		

CONCLUSIONES.

La intención del presente TFC es aportar una posible solución a la infraestructura de red para una empresa con unas características determinadas, planteando diferentes alternativas en ciertas partes de la infraestructura, para dar opciones al cliente a la hora de la ejecución final del trabajo y ajustándose en la medida de lo posible a los objetivos planteados.

Las problemáticas que se pueden encontrar al planificar un proyecto de nueva ejecución (desde cero), como el planteado en este TFC, es que no se tendrá el 100% de la información desde el principio, al ser una empresa de nueva creación. A priori no se sabrá el volumen de información con la que la empresa va a trabajar, por lo que se deberá realizar un dimensionamiento de la infraestructura con un margen de tolerancia amplio. Esto puede implicar que se puedan dimensionar de forma no ajustada a la realidad final, parte del equipamiento de red. Tampoco se dispondrá de toda la información sobre el software de gestión de la empresa, el cual podría repercutir a la hora de elegir cierto tipo de equipamiento físico y de software de sistema.

Otra de las problemáticas que se pueden encontrar a la hora de presupuestar el equipamiento final (dispositivos físicos y software) es la variedad de productos que existen en el mercado. En el TFC se ha intentado plasmar una solución real ajustada en la medida de lo posible al presupuesto de partida, comprobando que las características de los equipos físicos puedan realizar las funcionalidades necesarias por el sistema, pero no es descartable que existan otros productos de marcas diferentes, que cumplan las mismas funcionalidades y puedan ser incluso más económicos.

A la hora de valorar el presupuesto del proyecto definitivo sería necesario realizar un sondeo más exhaustivo, de los productos existentes en ese momento concreto en el mercado, versiones de modelos similares, etc. Contrastando las características de cada uno de ellos en diferentes marcas.

Como medidas de mejora futuras, se puede plantear la incorporación de un servidor adicional (físico), de respaldo frente a posibles paradas de los servicios web, este servidor actuaría como espejo del servidor virtual número 1, y entraría en funcionamiento cuando se produjese algún fallo del servidor en funcionamiento.

Otra medida a plantear en un futuro sería la realización de una auditoria de la red, para verificar posibles deficiencias de seguridad, una vez el sistema esté en funcionamiento, para la mejora de la infraestructura en cuanto a seguridad de la misma.

Este proyecto contempla de forma general todos los aspectos necesarios para el análisis y posterior ejecución de una infraestructura de red tipo para una empresa mediana, analizando diferentes casuísticas y aportando soluciones concretas.

Cada uno de los apartados del presente TFC puede constituir en sí mismo un proyecto concreto.

GLOSARIO DE TERMINOS.

- DNS: Sistema de Nombres de Dominio, asigna los nombres de dominio a las direcciones IP y la localización de los servidores de correo electrónico.
- CORREO POP: protocolo de correo que permite que el mismo sea descargable en el ordenador del cliente.
- CORREO IMAP: protocolo que hace que el correo se almacene en el Host/Servidor remoto.
- IDF: Intermediate Distribution Facility, habitáculo intermedio de distribución de cableado. Permite comunicar el cableado horizontal de la planta, con el MDF (Main Distribution Facility).
- MDF: (Main Distribution Facility), habitáculo principal de comunicaciones. Centralización de conexionado horizontal, vertical y comunicaciones.
- UTP cat 5e: Cables para la trasmisión de datos y señales analógicas y digitales. Cable de uso interior, avanzada tecnología para trasmitir datos a alta velocidad. Proporcionan unas excelentes características que superan los requerimientos de la Cat 5, obteniendo unos valores de rendimiento muy superiores a los cables existentes en el mercado para esta categoría.Cubierta de PVC, LH o PE.
- Fibra óptica multimodo. Una fibra multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 2 km, es simple de diseñar y económico.
- MAC: en inglés control de acceso al medio, identificador de 48 bits que identifica ed forma única cada dispositivo de la red.
- VLAN: red de área local virtual, método para crear redes virtuales independientes dentro de la misma red local.
- TRUNK: conexión troncal entre conmutadores, la cual está compuesta por diferentes redes virtuales o VLAN.
- DMZ: Demilitarized Zone. Zona desmilitarizada. Segmento de red configurado de tal forma que se tenga acceso a él desde una red pública como internet.
- MZ: Militarized Zona. Red interna.
- IDS: Intrusion Detection System. Software utilizado para detectar accesos no autorizados a la red.
- IPS: Intrusion Prevention System. Software utilizado para prevenir accesos no autorizados a la red.
- NAS: Network Attached Storage. Dispositivo de almacenamiento que ofrece sus servicios de archivos a la red local.

- SAN: Storage Area Network. Red de área de almacenamiento. Red dedicada exclusivamente al almacenamiento.
- LTO: Linear Tape Open. Tecnología de cinta magnética de almacenamiento de datos.

- WAP, AP: Access Point, Wireless Access Point: punto de acceso, o punto de acceso inalámbrico. Permite distribuir la conectividad de la red, entre puntos físicos y dispositivos inalámbricos.
- VPN: Virtual Private Network, tecnología de red que permite la extensión de la red local.
- LAN: Local Area Network, red de área local.
- Firewall: Cortafuegos. Dispositivo de red diseñado, para cortar los accesos no autorizados a una red.
- IPTABLES: Herramienta de cortafuegos que permite el filtrado y la redirección de paquetes de datos.
- NAT: Network Address Translator. Traducción de dirección de red. Mecanismo utilizado por routers para el intercambio de paquetes entre dos redes.
- SNORT: Software “sniffer” de paquetes y detector de intrusiones basados en red.
- SSH: Secure Shell. Intérprete de órdenes seguras.
- FTP: File Transfer Protocol. Protocolo de transferencia de ficheros.

BIBLIOGRAFIA.

Redes

Halsall, F. (1998). Comunicaciones de datos, redes de computadoras y sistemas abiertos (4.ª ed.). Addison-Wesley.

Tanenbaum, Andrew S. (2003). Redes de computadores (4.ª ed.). Pearson

Virtualización

Gillet, Philippe (2010). Virtualización de sistemas de Información con VMWare. ENI.

VMWare	www.vmware.com	
Sitiio web del fabricante de software de Virtualización		

Software Libre

Debian	www.debian.org	
Sitio web de la distribución de Linux.		

Software Propietario

Armelin Asimine (2014). Windows Server 2012 R2. Configuración de servicios avanzados.

Microsoft	www.microsoft.org	
Sitio web del fabricante de software.		

Seguridad de redes.

Cheswik, W.R.; Bellovin, S.M. (2003) Firewalls and Internet Security. Addison-Wesley Professional Computing.

Snort	www.snort.org	
Sitio web oficial de snort		

ANEXOS.

Anexo número 1 - Equipos de Red

SWITCH HP SERIES 2610 (Versiones 24 y 48 puertos)

Número de puertos.	(IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX), tipo de soporte: MDIX automático, dúplex: semi o completo.
	1 puerto serie RJ-45 para consola
	2 puertos 10/100/1000 de detección automática (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T), dúplex: 10BASE-T/100BASE-TX: semi o completo 1000BASE-T: solo completo
Memoria y procesador	Procesador: MIPS a 300 MHz, 16 MB de memoria Flash, tamaño de búfer de paquetes: 1 MB, 128 MB de SDRAM
Latencia	Latencia de 100 Mb: < 4,1 µs Latencia de 1000 Mb: < 2,9 µs
Capa 2 switching	Soporte VLAN, soporta IEEE 802.1Q (4.094 VLAN IDs) y 256 VLANs simultáneas. GARP VLAN Registration protocol. Permite asignación dinámica de VLANs
Capa 3 routing	Basic Ip routing: activa de forma automática el routeo a las VLans conectadas, y permite hasta 16 reglas estáticas.
Seguridad	Permite multitud de métodos de autentificación.
Características completas: http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=c04111724&doctype=quickspecs&doclang=EN_US&searchquery=&cc=es&lc=es	

ROUTER HP MSR2000

I/O puertos y slots	3 SIC slots, or 1 DSIC slot, and 1 SIC slot 2 RJ-45 1000BASE-T ports
Características AP	3G, 4G LTE
Rendimiento	1 Mpps (64-byte packets)
Tamaño de la tabla de enroutamiento	200000 entries (IPv4), 200000 entries (IPv6)
Características completas: http://h17007.www1.hp.com/us/en/networking/products/routers/HP_MSR2000_Router_Series/index.aspx#tab=TAB3	

ANTENAS WIFI UBITIQUI AIR FIBER 5

Frecuencia de operación	Frecuencia de operación: 5,470 a 5,6 , 5,650-5,850 GHz
Dimensiones y características Físicas	Dimensiones: 938,4 x 468,4 x 281,4 mm Peso: 16 kg (montaje incluido) Max . Consumo de energía: 40W Fuente de alimentación: 50V, 1.2A Adaptador GigE PoE (incluido) Método de alimentación: Passive Power over Ethernet (42- 58V) Kit de montaje en poste (incluido) Temperatura de funcionamiento : -40 a 55 ° C (-40 a 131 ° F) Puerto de datos : 1x Puerto Ethernet 10/100/1000 Puerto de configuración : 1x 10/100 Puerto Ethernet Puerto auxiliar: 1x RJ -12, puerto de alineación Tone.
Información del sistema	Caudal máximo: 1,0 + Gbps Alcance máximo : 100 + km (dependiendo de la región reguladora) Paquetes por Segundo : Más de 1 Millón Cifrado: AES de 128 bits FEC : 164/205 Relación de enlace ascendente / descendente : 50 % fijo Sincronización de cuadros Radio : GPS Ancho de banda del canal: 50 MHz TX / RX Ganancia: 23 dBi Ancho de haz : 6 ° Polaridad : Dual Slant Polarización

ROUTER VPN DELL SONICWALL TZ215

Interfaces	5 Ethernet 10/100/1000 1 Interface de consola 2 puertos USB
Clientes VPN	Max. 25
SSL VPN clientes	Máx. 10
Nº máximo de conexiones	48.000
Nuevas conexiones/seg	1.800

Anexo número 2 – Servidores

HP Proliant DL180 Gen9 E5-2603v3 1.6GHz 6-core

Procesador	HP DL180 Gen9 Intel Xeon E5-2603v3 (1.6 GHz/ 6 Core/ 15 MB/85W) FIO Processor Kit
Memoria RAM	HP 8GB Single Rank x4 DDR4-2133
Controladora de almacenamiento	HP Embedded B140i Controller HP DL180 Gen9 4LFF
Riser Card	HP DL180 Gen9 3 Slot x8 PCI-E Riser Kit
Factor de forma	2U Small Form Factor
Fuente de alimentación	HP 550W FIO Power Supply Kit
Disco Duro	HP 1TB 6G SATA 7.2K rpm LFF (x4)
Red	HP Ethernet 1 GB 2-port 332T Adapter
Gráfica	NVIDIA Quadro K2200

Anexo número 3 – Sistema NAS

LenovoEMC px4-400r Network Sorage Array. 70CL-70CL9000WW

CPU	Intel Atom D2701 (dual core) 2.13 GHz
RAM	2GB DDR3
Disco Duro	4TB (4HD x 1TB), eSATA (ampliable a 16TB)
RAID	0,1,5,10
USB 3.0	1 Frontal
USB 2.0	4 traseros
Salida Video	1HDMI
RED	2x Ethernet 1GbE RJ45
Factor de Forma	RACK 1U

Anexo número 4 – Sistema de cintas LTO

HP LTO-5 Ultrium 3000 SAS Internal Tape Drive - Unidad de cinta - LTO Ultrium (1.5 TB / 3 TB) - Ultrium 5 - SAS-2 - interna - 5.25" - cifrado

Tipo	Unidad de cinta - LTO Ultrium
Norma de grabación	LTO Ultrium 5
Tipo de Interfaz	Serial Attached SCSI 2
Capacidad de almacenamiento	1.5 TB (nativo) / 3 TB (comprimido)
Cartuchos soportados	Ultrium 4, Ultrium 5
Velocidad de transferencia de datos (nativo)	140 MBps (504 GBph)
Velocidad de transferencia de datos (comprimido)	280 MBps (1008 GBph)

Anexo número 5 – Red Wi-Fi

CISCO AIRONET 1600 SERIES ACCESS POINT

Características del dispositivo: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1600-series/data_sheet_c78-715702.html

Anexo número 6 – Vsphere (Virtualización)

En los siguientes enlaces de video se muestra los aspectos más importantes de instalación y configuración de VSphere en su versión 5. Los enlaces de video muestran todos los aspectos tratados en el (apartado 3.3.) sobre el sistema de virtualización recomendado para este proyecto.

Instalación y Configuración ESXi	https://www.youtube.com/watch?v=x59MsL-A-Ck&list=PL3DCA00BE8652EBBE&index=1
Cómo crear máquinas virtuales	https://www.youtube.com/watch?v=SpF9XAWkXcg&index=2&list=PL3DCA00BE8652EBBE
Instalar y configurar vCenter	https://www.youtube.com/watch?v=qqDlWgGW3w0&index=3&list=PL3DCA00BE8652EBBE
Configuración de las redes virtuales	https://www.youtube.com/watch?v=fkmRZUYpKLE&list=PL3DCA00BE8652EBBE&index=4
Configuración del almacenamiento	https://www.youtube.com/watch?v=IyJQzdDqkpY&index=5&list=PL3DCA00BE8652EBBE
Gestión de las máquinas virtuales	https://www.youtube.com/watch?v=hQKZ1ShJAiM&index=6&list=PL3DCA00BE8652EBBE
Alta disponibilidad y DRS	https://www.youtube.com/watch?v=9EvbSoT1Bw0&list=PL3DCA00BE8652EBBE&index=7
Monitorización y gestión de recursos.	https://www.youtube.com/watch?v=S6LoPDNYi0E&index=8&list=PL3DCA00BE8652EBBE

En documento adjunto, se acompaña manual de instalación de Vsphere V5 Esxi en un entorno de pruebas.