PROYECTO DE FINAL DE CARRERA

ESTUDIO DE RECOMENDACIONES NECESARIAS PARA EL DESPLIEGUE DE LA SOLUCIÓN IT EN UN ENTORNO MULTINACIONAL

DESIGN OF REQUIRED RECOMMENDATIONS FOR IT SOLUTION DEPLOYMENT IN A MULTINATIONAL ENVIRONMENT

Estudios: Enginyeria de Telecomunicació
Autor: Juan Valladares Perales
Director: Ricardo Gilberto Hurtarte Carrillo
Ponente: Xavier Hesselbach-Serra
Año: 2010-2011

Índice

Índice de Ilustraciones

Índice de Tablas

1 Resum

El present projecte pretén donar una solució a una empresa multinacional que ha procedit a la adquisició de vàries fàbriques a diferents països arran d'Europa i el Nord d'Àfrica i es troba en un caos tecnològic degut a la variada naturalesa de components i proveïdors en matèria de telecomunicacions degut a les esmentades adquisicions. L'objectiu del projecte es la definició d'una sèrie de requisits que hauran de complir tots el elements involucrats per facilitar la feina de comparar entre diferents fabricants i escollir en cada cas el producte mes adient. Afegit a aquestes recomanacions per provar la bondat de les mateixes es duu a terme la posta en marxa d'una de les seus adquirides basant-se en els components escollits.

2 Resumen

El presente proyecto pretende dar solución a una empresa multinacional que tras la adquisición de varias fábricas en diferentes países en Europa y Norte de África se halla sumida en un caos tecnológico debido a la variada naturaleza de componentes y proveedores en materia de telecomunicaciones derivada de dichas adquisiciones. El objetivo del proyecto es la definición de una serie de requisitos que deberán cumplir todos los elementos involucrados para poder comparar entre diferentes fabricantes y escoger en cada caso el producto más adecuado. Como añadido a la definición de las recomendaciones y a modo de prueba de las mismas se lleva a cabo la puesta en marcha de una de las sedes adquiridas basándose en los componentes escogidos.

3 Abstract

The aim of current project is to give a solution to a multinational company that has recently acquired many factories around Europe and North Africa and it's currently in a technological chaos due to different nature of components and providers in telecommunications environment of recently acquired factories. The objective of the project is to define main requirements that should meet all involved components to be able to compare among manufacturers and to choose the right product in each field. Add to this recommendations definition and in order to verify the goodness of them, the implementation of one of them is carried out based on chosen components.

4 Contexto

Este proyecto se ha realizado en el marco de T2C – Technology to Client, una empresa de consultoría que proporciona soluciones de IT (Information Technology) para sus clientes.

El cliente es una multinacional catalana inmersa en un proceso de expansión y compra de nuevas empresas y factorías por toda Europa y Norte de África. Por motivos de confidencialidad en ningún momento se menciona dicho cliente durante la redacción del presente documento.

T2C colabora activamente con dicha empresa dándole soporte en Help Desk, comunicaciones y administración de servidores. En concreto en el presente proyecto la empresa acuerda con T2C definir las recomendaciones en el ámbito de comunicaciones para aplicarlo luego a todas las instalaciones actuales, en proceso de compra o futuras adquisiciones que plantee.

Dichas recomendaciones consisten en definir la estructura que ha de tener las instalaciones internas de cada una de las delegaciones, los componentes de los que han de disponer, la definición de un criterio para elegir cada uno de los componentes y la elección del producto recomendado en algunos de ellos. Por otro lado se define un criterio de dimensionamiento de las principales conexiones, dimensionamiento y cuantificación de determinados componentes, ya sea a través de criterios marcados desde dirección, ya sea con criterio propio.

La presente memoria de proyecto de fin de carrera tiene la misión de detallar la colaboración realizada por mi parte en la definición de dicho estándar y la presentación al cliente para su aprobación y la posterior puesta en marcha en una de las sedes. El proyecto incluirá las comparativas entre diferentes fabricantes para los diferentes entornos de actuación, diseño de la solución en función de las comparativas realizadas, pruebas de campo llevadas a cabo sobre la solución escogida y las conclusiones que de estas pruebas se derivan.

Es importante destacar que el proyecto no nació originariamente como un proyecto de final de carrera si no que fue en origen un proyecto puramente empresarial. A mediados del mismo se evalúa la posibilidad de realizarlo desde un marco más académico y se reconduce a tal fin. Ello implica que haya partes que se hayan tenido que adaptar a posteriori para darle una estructura acorde a lo esperado desde un punto de vista formativo y académico y no tan centrado en el origen empresarial con el que surgió.

El marco inicialmente empresarial del proyecto también implica que se haya optado en ocasiones por referenciar más de lo esperado, especialmente en el proceso de análisis de productos y comparativa, a documentación obtenida de Internet pues el esfuerzo básico del proyecto era el de la consecución de resultados finales buscando disponer de un producto operativo sin importar tanto el motivo de la selección de un producto u otro en concreto. En alguno de los puntos se ha preferido utilizar una comparativa extraída de internet que realizar dicha comparación dentro del proyecto, tanto por costes económicos de validación como por extensión y alcance del proyecto.

El proyecto de definición de recomendaciones se ha ido desarrollando a intervalos entre mediados del 2007 y finales del 2009, periodo que dura mi colaboración con el cliente en cuestión. El presente documento de memoria de proyecto de final de carrera se realiza desde principios de 2010 hasta la actualidad. Antes de comenzar este periodo de redacción de la memoria T2C finaliza la relación con el cliente con lo que se pierde el acceso a la instalación para tomar determinados datos y referencias para su uso en la presente memoria.

5 Objetivos

El proyecto que se lleva a cabo en el cliente y del que se da cuenta en la presente memoria tiene dos objetivos básicos. El primero es la definición de recomendaciones, reglas de cálculo, parámetros, y demás consideraciones que se han de tener en cuenta para la implantación de una solución de comunicaciones para las sedes locales en un entorno multinacional con unos servicios centrales que proporcionan toda una serie de servicios a las sedes.

El segundo objetivo del proyecto es verificar la bondad de las recomendaciones establecidas a través de la implantación de la solución en una de las sedes, que servirá como implantación piloto para el resto. Esta implantación piloto sin embargo no se puede considerar como un ensayo ya que está destinada a ser una instalación productiva sustituyendo la infraestructura de comunicaciones que utiliza la planta. Con lo cual lo que prima en el diseño de la estructura que se define es conseguir una plataforma que proporcione un funcionamiento apropiado por encima de conseguir el mejor diseño teórico posible.

Teniendo en cuenta el propósito empresarial del presente proyecto se puede entender que todo el mismo esté enfocado a un resultado práctico, que consiga a su vez alcanzar los objetivos que nos marca el cliente:

Máxima estabilidad: El proyecto ha de intentar minimizar las incidencias y los cortes de servicio asociados a la infraestructura de comunicaciones, durante su instalación y puesta en marcha y especialmente durante su funcionamiento una vez implantado. Prima por encima de todo que cualquier tipo de parada o interrupción del servicio sea programada con la máxima antelación posible. Por otro lado también se primará a la hora de elegir componentes el soporte ofrecido por los proveedores o fabricantes.

Seguridad: Tanto en la instalación como en el funcionamiento diario el proyecto ha de proporcionar un entorno completamente blindado a amenazas externas y a la fuga de información confidencial de la empresa.

Coste: Los objetivos en cuanto a coste quedan claros por parte del cliente, prefiere realizar una inversión inicial más elevada pero que proporcione una gran calidad y la instalación de componentes de larga amortización. Ello permite sobredimensionar el sistema para conseguir alargar al máximo la durabilidad teórica de los equipos.

Homogeneización: Se pide por parte del cliente realizar una homogeneización de proveedores y estructuras implantadas en las diferentes sedes para facilitar la implantación y el mantenimiento de todos los componentes, definir responsabilidades únicas por entornos siempre que se pueda y minimizar costes de compra y mantenimiento de componentes.

6 Problemática

La principal problemática que plantea el proyecto es la de intentar obtener unas recomendaciones válidas para todas las empresas del grupo para ahorrar costes de implantación, mantenimiento y soporte.

Dichas recomendaciones han de definir tecnologías, estructuras, capacidad y ubicación para todos los entornos de IT necesarios para comunicar la empresa con la central ubicada en Barcelona, así como para cubrir las necesidades intra-fábrica en materia de proveedores, comunicaciones, servidores, ubicación física de los componentes, alimentación eléctrica y cableado.

Incluye también la definición del proceso de instalación, seguimiento y control de la solución desde el análisis de estado de la instalación actual de la fábrica, evaluación de proveedores disponibles en el país, implantación de todos los componentes definidos, definición de indicadores para medir la calidad de la instalación y análisis de los resultados obtenidos en cada uno de los campos.

6.1 Requisitos de Infraestructura

En este apartado se evalúan los requisitos de infraestructura que ha de tener disponibles cada una de las fábricas, en cuanto han de tener un CPD (Centro de Procesado de Datos) y una sala acondicionada para audio y video conferencia.

En el análisis de elementos de infraestructura requeridos está basado en las necesidades físicas de las que ha de disponer toda fábrica para poder disponer de unas comunicaciones fiables. Ello implica disponer de toda una serie de elementos como un CPD acondicionado, un cableado que permita una velocidad apropiada de red y disponer de una sala para realizar videoconferencias con servicios centrales.

6.1.1 Estudio de requisitos del CPD

El Centro de Procesado de Datos debe cumplir toda una serie de requisitos en cuanto a refrigeración, tamaño, número de tomas de corriente, número de tomas de red, seguridad de acceso, seguridad anti incendio, potencia disponible, etc.

El estudio cuantitativo se ha de basar en la cantidad de servidores que ha de alojar y los requisitos de cada uno de ellos. Para ello se propone cumplimentar unas tablas que ayudarán en los cálculos de cada métrica para cada uno de los racks para poder determinar así el número de racks necesarios. Se adjunta un ejemplo de tabla para evaluar la capacidad de un rack.

RACK D			SAI A			SAI B			TOTAL		
Servidor / Dispositivo	Modelo	Us	Enchufes	Consumo Máximo (W)	Consumo Máximo (A)	Enchufes	Consumo Máximo (W)	Consumo Máximo (A)	Enchufes	Consumo Máximo (W)	Consumo Máximo (A)
Total		0	0	0,00	0,00	0	0,00	0,00	0	0,00	0,00
Máximo		40	16	7200,00	32,00	16	7200,00	32,00	32	14400,00	64,00
Diferencial		40	16	7200,00	32,00	16	7200,00	32,00	32	14400,00	64,00

Tabla 1: Dimensionamiento de RAC

A la hora de definir los requisitos cualitativos que ha de cumplir el CPD se tiene en cuenta las referencias del estándar TIA-942 [1]. En el estándar referenciado hay 4 niveles de disponibilidad y requisitos desde Tier I con un 99,671% de disponibilidad hasta el Tier IV con disponibilidad del 99,995%. Se escoge el nivel Tier II que implica un 99,749% de disponibilidad o lo que es lo mismo, 22 horas al año como máximo de parada. Además hay otra serie de consideraciones que se tendrán en cuenta:

- Sala dedicada: El CPD ha de estar alojado en una sala independiente, con la única función de CPD, no puede estar compartida para cualquier otra función de almacenaje, oficina, despacho u otra actividad que no sea la de alojar los servidores que ha de tener la fábrica. Además la ubicación de la misma ha de estar alejada de almacenes con materiales inflamables y se ha de evitar en la medida de lo posible la ubicación de la sala sobre aparcamientos cerrados de vehículos.

- Aire acondicionado: El CPD ha de tener una temperatura y humedad estables, acondicionadas para los requisitos de los servidores. Por ello ha de disponer de un sistema de aire acondicionado con la capacidad de mantener la temperatura independientemente de la temperatura exterior y suficiente para evacuar el calor desprendido por todos los servidores que estén ubicados en su interior.

- Alimentación ininterrumpida: La alimentación de la sala ha de ser ininterrumpida, para evitar caídas debido a falta de alimentación externa. Para ello además de la conexión a la red eléctrica externa, dispondrá de grupos electrógenos que se activarán automáticamente en caso de caída o bajada de tensión externa.

- Redundancia de alimentación: Los equipos de la red deberán tener como mínimo doble fuente de alimentación para poder conectarlos por un lado a la red eléctrica externa y por otro lado a la red particular dependiente de los generadores electrógenos.

- Piso elevado: La sala de servidores ha de tener un piso elevado como mínimo de 60cm para poder tener la conducción de aire acondicionado a través del suelo de manera que sea más eficiente la refrigeración de los servidores.

- Protección contra incendios: El CPD ha de disponer de un sistema antiincendios basado no en agua si no en gases como el FM-200 que consiguen apagar el fuego sin necesidad de utilizar agua que podría dañar los servidores ubicados en el CPD. Además del sistema de extinción se requiere un sistema de Detección que alerte al personal de monitorización por alertas detectadas en el interior del CPD

- Seguridad física 24x7x365: Se necesitará un sistema de vigilancia de manera que se impidan los accesos no autorizados. Entre estos sistemas se encuentra la videovigilancia a través de un circuito cerrado de televisión y cámaras de videovigilancia en la sala y los accesos, la vigilancia física de personal de vigilancia y el control de acceso a la sala a través de un sistema de tarjetas magnetizadas.

- Sistema de monitorización: Se implementará un sistema de monitorización del estado de los servidores en cuanto a alimentación, temperatura, humedad, fallo de una de las fuentes de suministro y conectividad, que será controlado de manera física in situ por el personal informático de la fábrica de 9 a 18 horas y desde central el resto de la jornada.

6.1.2 Sala de conferencias

Se necesitará para poder tener una correcta comunicación entre la sede central y las diferentes sedes europeas una sala adecuada para poder realizar conferencias, ya sean telefónicas o de videoconferencia.

Esta sala ha de cumplir una serie de requisitos para que las comunicaciones sean correctas y fluidas:

- Mobiliario: ha de disponer de una mesa y sillas suficientes según la cantidad de gente que se estime que deba participar en las conferencias.

- Tamaño: Ha de ser de un tamaño apropiado en función de la cantidad de gente que tenga que albergar.

- Dispositivos: ha de disponer de un teléfono con posibilidad de manos libres para poder realizar las audioconferencias. Las videoconferencias se realizaran con los portátiles de una o varias de las personas implicadas en la conferencia. Para ello se utilizará un software apropiado para tal fin. También se requerirá un proyector para poder realizar presentaciones.

- Comunicaciones: La sala ha de tener unas comunicaciones adecuadas. Ha de tener los suficientes puntos de red como para poder conectar todos los ordenadores portátiles de las personas que requieran de conexión incluyendo la conexión para el teléfono.

- Insonorización: La sala ha de estar correctamente insonorizada para evitar por un lado una comunicación incorrecta por ruidos externos de fábrica u oficina y por otro lado evitar la afectación del ruido propio de las conferencias en el resto de personas que trabajan en la oficina.

- Aire Acondicionado: debido a que las reuniones pueden ser prolongadas, es necesario que el aire esté acondicionado a una temperatura adecuada de trabajo. Interesará que sea independiente del aire del resto de la oficina al ser una sala que no estará permanentemente ocupada para así poder conectarlo y desconectarlo minimizando el consumo.

- Proximidad: dentro de las posibilidades de cada oficina, interesará que la sala esté próxima o dentro de las propias oficinas para ahorrar en tiempos de desplazamiento del personal implicado.

- Multiuso: Dependiendo de las posibilidades de las instalaciones se evaluará la posibilidad de darle más usos aparte de las conferencias. Estos usos pueden ser seminarios, cursos, reuniones, formación o recepción de visitas externas.

6.1.3 Cableado de red

La red de datos utilizará un cableado Ethernet, la tecnología más universal al respecto. Las prestaciones ofrecidas son muy elevadas y el coste reducido al ser una tecnología largamente implantada. El cableado ha de soportar velocidades de 1Gbps (*1000BASE-TX - Gigabit Ethernet*) y será de tipo cat6 (con el estándar ANSI/TIA/EIA-568-B.2-1).

6.2 Requisitos de Red

En este apartado se detallarán los requisitos de los elementos necesarios a disponer en la red interna de cada una de las fábricas. Se incluirán switches, routers, servidores de correo, FTP, DNS, etc. También se incluirá los requisitos de seguridad, firewalls, antivirus y por otro lado la red de pc's, dimensionamiento de los mismos etc.

6.2.1 Topología de la red

La topología de la red ha de incluir todos los elementos necesarios para el buen funcionamiento de la misma. Para poder llegar a una solución acorde con las necesidades del entorno lo principal es conocer dicho entorno, las consideraciones previas al desarrollo del presente proyecto y el alcance global del mismo.

En el presente proyecto se define toda una serie de servicios que serán proporcionados utilizando una arquitectura centralizada, es decir desde el CPD central de Barcelona y utilizando un portal Citrix de acceso a los mismos.

Se muestra a continuación un gráfico con la topología general de la red.

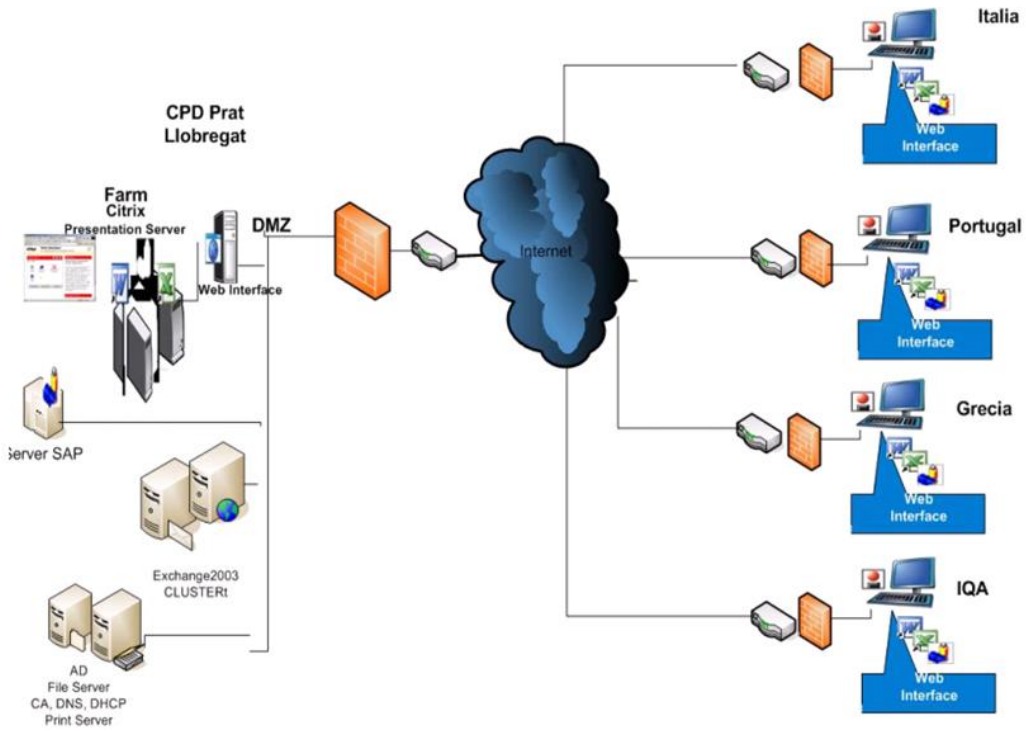

Ilustración 1: Topología general a implementar

La opción de arquitectura centralizada implica desde el punto de vista de la definición de la red, como principal inconveniente, que habrá un gran consumo de ancho de banda en la línea de comunicaciones con la sede central en Barcelona. Como principal ventaja de esta solución se considera que los requisitos Hardware y software del CPD y de las estaciones clientes serán mucho más reducidos que en una arquitectura distribuida. La solución de arquitectura centralizada no afecta a todos los servicios. En concreto afecta los servicios de:

- SAP – ERP
- SAP - Business
- Antivirus server
- Antispam Server
- Proxy
- Servidor de Correo
- Servidor de ficheros central
- Servidor de Portal

Sin embargo hay toda una serie de servicios y elementos que no conviene que los proporcione la arquitectura centralizada por temas de rendimiento y que han de ser proporcionados de manera local:

- Antivirus local
- Antispam local
- Cliente de portal
- Firewall
- Servidor DNS
- Servidor DHCP
- Servidor Active Directory
- Servidor de ftp
- Servidor de ficheros
- Gestor de ancho de banda
- Impresoras y servidores de impresión
- Routers
- Switches

Estos últimos elementos se deberán considerar en la topología y definir toda una serie de requisitos que han de cumplir para poder integrarlos sin problemas. Se define a continuación gráficamente lo detallado anteriormente.

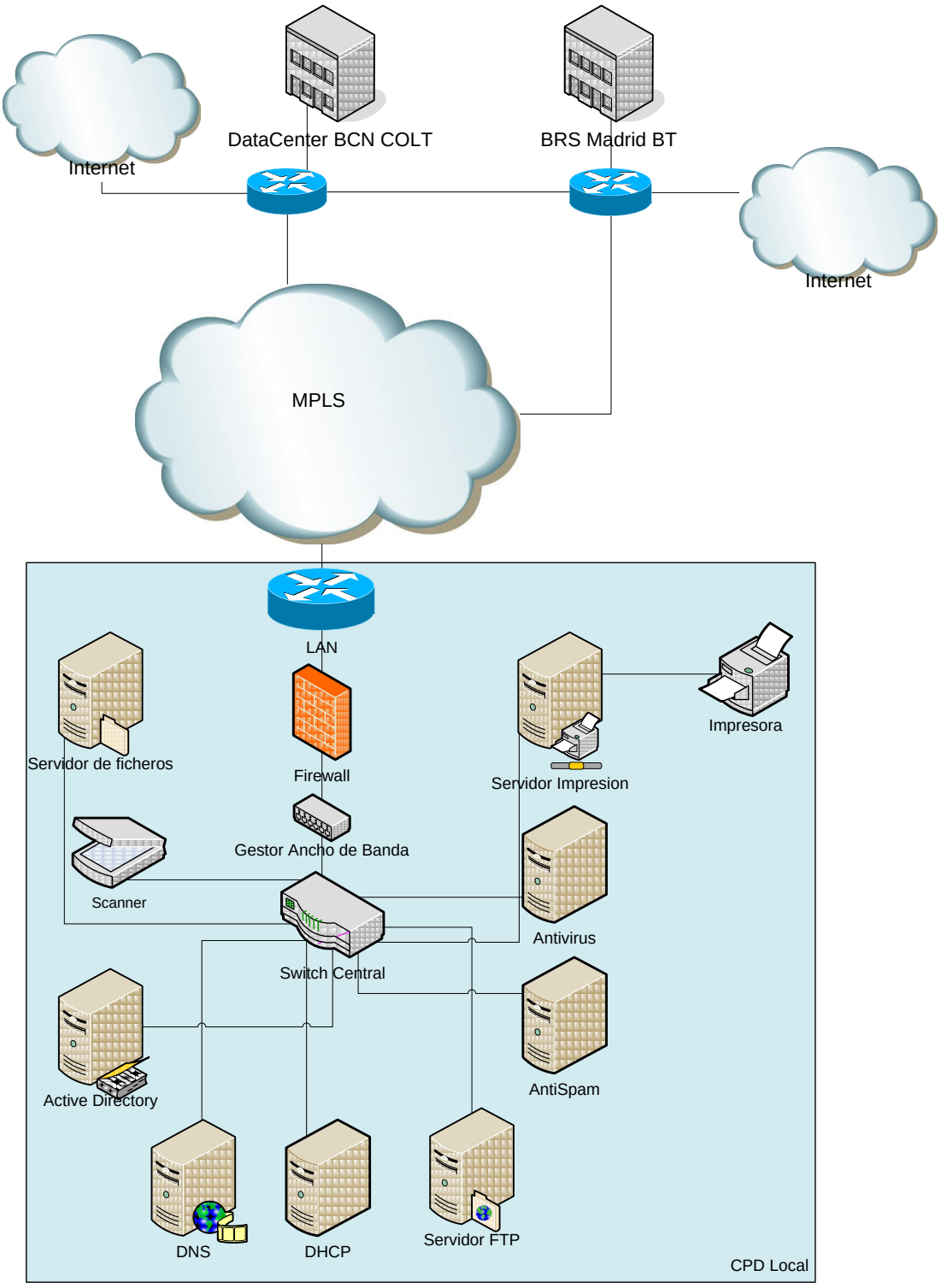

Ilustración 2: Topología de red local a implementar

Una vez definidos los elementos que van a integrar la red interna de cada una de las empresas se han de definir los requisitos necesarios para cada uno de los elementos así como algunas características que han de cumplir todos los elementos ya sea por separado o en conjunto.

Los requisitos que han de cumplir los diferentes dispositivos son:

- Compatibilidad: Se ha de verificar la compatibilidad entre los diferentes elementos. Para poder realizar dicha verificación se ha de realizar en primera instancia un análisis de las especificaciones técnicas de los elementos que tengan relación entre sí. Los elementos software soportan unos determinados dispositivos de hardware o unos determinados sistemas operativos.

- Interoperabilidad: A través de estudios publicados en diferentes medios se analiza el funcionamiento entre diferentes dispositivos de manera que se pueda escoger una opción en el que se maximice el rendimiento de los sistemas o en el peor de los casos una configuración que no estropee el rendimiento de ninguno de los elementos.

- Unicidad: Para optimizar el rendimiento de la red se buscará en la medida de lo posible que, en condiciones de funcionamiento normal, las funciones que realice cada dispositivo las realice únicamente él de manera que no se sobrecargue el sistema. Sirva como ejemplo un antivirus con funcionalidades de firewall o antispam. Si se define un firewall como elemento diferenciado de la red y a la vez el antivirus tiene las funcionalidades de firewall activado puede provocar comportamientos indeseados en el sistema.

- Multifunción en contingencia: A pesar de que en funcionamiento normal interesará que cada elemento realice su función de manera única, en caso de contingencia es interesante tener elementos que tengan la capacidad de realizar funciones asignadas a otro en caso de caída del elemento. De esta manera se puede tener redundancia de funciones sin tener que tener redundancia de elementos físicos para el caso de caídas. En el ejemplo anterior si el firewall cae sería conveniente que el antivirus fuera capaz de ejercer la funcionalidad de firewall de manera fácil.

- Escalabilidad: La solución escogida para cada uno de los elementos ha de ser escalable de manera que la inversión realizada no se pierda en el caso de necesitar un elemento de mayores prestaciones para incrementar la capacidad de un determinado punto.

- Soporte del producto: interesará tener un soporte adecuado para todos los componentes de la red, con lo que se evaluarán varios puntos asociados al soporte ofrecido por el fabricante.

    - Soporte on-site: interesará dado el ámbito europeo en el que se va a ubicar el proyecto que todos los elementos de la red dispongan si es

posible de soporte en el país en el cual se aloja la fábrica para llegado el momento el coste de dar el soporte sea menor.

  - Tipo de soporte: Se tendrá en cuenta para todos los componentes de la red el tipo de soporte que ofrecen, telefónico, e-mail o web, así como la descarga gratuita de actualizaciones, parches de software, firmware o controladores.

  - Tiempo de resolución de incidencias: Dependiendo de la criticidad del componente y de si afecta a la producción o no, se escogerá dentro de lo posible el producto que ofrezca una mejor respuesta para resolución de incidencias

  - Tiempo máximo de sustitución: En caso de problemas o roturas de parte o la totalidad del componente se evaluará el tiempo de respuesta para el cambio de piezas o del hardware al completo que ofrezca el fabricante.

  - Tiempo de soporte post-venta: En determinados componentes se escogerá no tener soporte contratado con lo que el tiempo de soporte gratuito post-venta se convierte en un punto a considerar.

- Coste: uno de los puntos más determinantes a la hora de decantarse por un dispositivo u otro será el coste del dispositivo. El coste se ha de tener en cuenta, no solo el de adquisición, sino también el coste de mantenimiento, el coste de soporte y el coste operacional.

- Canal de distribución: A la hora de decantarse por un fabricante u otro, es importante también la red de Partners y canales de distribución de los que disponga el fabricante, ya que facilita los procesos de compra y de obtención de soporte y licenciamiento.

- Tipo de licenciamiento: interesará, asociado con el coste, el tipo de licenciamiento que ofrecen los productos a comparar. Normalmente o van asociados a número de usuarios o van asociados a potencia del sistema.

En los siguientes subapartados se intenta determinar las características de cada uno de los elementos incluidos en la red.

6.2.2 Portal

Trabajar con portales es una filosofía de trabajo en la que se pretende liberar a los ordenadores cliente de la carga de trabajo de las aplicaciones de negocio y que dicha carga de trabajo sea realizada por una granja de servidores de manera que los ordenadores cliente solo tienen la misión de visualizar (salida) y servir como terminal para teclado y ratón (entrada) a las aplicaciones. También permite minimizar el tráfico de la red pues el único tráfico que transcurre entre el servidor y el cliente son los asociados a entrada y salida y por lo tanto mucho más fácil de controlar, ya que tiene un volumen máximo (pantalla solo hay una y el número de aplicaciones que visualiza el usuario es limitado) y de menor consumo de ancho de banda.

El portal a escoger es uno de los puntos más importantes en el sentido en que es el punto de entrada para el resto de aplicaciones. Si el portal no cumple con los requisitos que se definan provocará que el resto de aplicaciones no funcionen correctamente. Por ello y aunque el servidor del portal se halle ubicado fuera del entorno local de la fábrica, se decide incluirlo en el análisis porque el cliente del portal ha de estar instalado en todos los ordenadores y es el que permitirá un funcionamiento correcto del sistema.

Se busca una solución con la que se pueda ser capaz de instalar, publicar y gestionar aplicaciones y contenidos de manera centralizada. Los accesos a las aplicaciones y contenidos han de realizarse de forma segura, desde cualquier lugar y en cualquier momento. El único requisito para el usuario remoto es tener instalado el cliente del portal.

Se evaluarán a continuación las características que ha de tener el portal que se escoja:

Conectividad: El portal ha de garantizar la conectividad desde las oficinas locales contra el servidor central. La conectividad ha de ser para todas las aplicaciones disponibles en el portal, es decir, ha de poder conectarse a todas las aplicaciones desde un solo punto o interfaz de entrada.

Centralización: La gestión de las aplicaciones, accesos y permisos de los usuarios sobre las mismas ha de ser de manera centralizada y desde un solo punto. Además la información que se maneje ha de consolidarse dentro de los mismos sistemas de información. Esta centralización ha de permitir que la inclusión de nuevas sedes, nuevos usuarios o nuevas aplicaciones junto con el mantenimiento de las existentes para todos los usuarios sea sencilla y desde un único punto centralizado.

Movilidad de usuarios: El portal ha de permitir la movilidad de los usuarios del sistema que les permita acceder desde cualquier punto con acceso a internet. Este apartado es imprescindible para la fuerza de venta y es útil para el resto de personal, pues permite una mayor flexibilidad laboral al tener acceso a los datos desde cualquier punto sin necesidad de descargarlos.

Continuidad: Este sistema además ha de permitir el acceso ininterrumpido a los datos de negocio en caso de caída de la red principal, de desastres naturales o de mantenimientos. Al garantizarse el acceso desde cualquier punto se consigue esta continuidad de negocio deseada.

Reducción de costes de mantenimiento: El portal ha de permitir que la operativa diaria de copias de seguridad y mantenimiento se realice también desde un único punto centralizado de manera que sea más sencilla y menos costosa.

Volumen de usuarios: El portal ha de permitir la conexión en paralelo de todos los usuarios definidos en el sistema. Ha de ser eficiente gestionando los recursos de los servidores y ha de garantizar que el acceso a las aplicaciones críticas es suficientemente ágil para todos los usuarios del sistema.

Tipo de licenciamiento: Para dar soporte a un alto número de usuarios se deberá tener una licencia acorde. Dependiendo del tipo de licenciamiento que se permita para el producto puede ser que no interese un determinado portal.

A la hora de comparar entre portales se ha de tener en cuenta además otras funcionalidades y características:

- Protocolo utilizado: El protocolo utilizado en la comunicación puede hacer variar el rendimiento obtenido
- Balanceo de carga entre servidores: Un sistema de balanceo de carga permite reducir los costes de gestión pues implica que el sistema en global se autogestiona, redirigiendo peticiones a los componentes con una carga de trabajo menor
- Acceso a aplicaciones basado en Web: Si el acceso se realiza a través de un entorno web, lo único que se necesitará será un navegador web en el cliente.
- Gestión remota de impresoras: El portal ha de permitir que se configuren impresoras de manera remota y que se pueda imprimir desde el servidor ubicado en el CPD central contra las impresoras ubicadas en la sede.
- Control remoto de sesiones: Posibilidad de controlar los servidores o los ordenadores de manera remota, sin acceso a teclado o ratón local
- Instalación del cliente vía Web: La instalación para poder instalar el cliente del portal se puede realizar desde una página web

- Actualizaciones automáticas: El cliente se puede ir actualizando de manera automática cuando se realizan actualizaciones en los servidores de portal.
- Mapeo de discos locales: Desde el portal se pueden ver los discos externos ubicados en el ordenador
- Uso de portafolio remoto-local: Se puede utilizar el portafolio para copiar objetos y texto entre el entorno del portal y el entorno local
- Protocolos de seguridad: Se ha de verificar que el portal a utilizar permita protocolos seguros de comunicación.

6.2.3 Antivirus

A la hora de escoger un antivirus apropiado se han de tener en cuenta, además de todos los elementos comunes, toda una serie de características:

- Estructura cliente-servidor-servidor central: Posibilidad de gestionar la instalación de manera centralizada, servidor ubicado en servicios centrales y sub-servidores en los CPD locales que gestionen a su vez los clientes en los PC's
- Características de seguridad: Se verificará que el antivirus cumple con los principales estándares de seguridad recomendados.
- Frecuencia de actualización: interesará tener la máxima frecuencia de actualización posible para poder estar protegidos cuanto antes de las nuevas amenazas que vayan surgiendo en la red
- Tipo de Actualización: Se verificará si es posible actualizar manual o automáticamente tanto el software como las bases de datos de virus.
- Rendimiento: Se intentará minimizar el impacto del antivirus en el sistema así como se buscará la mayor velocidad de escaneo posible para los archivos contenidos en los PC's
- Opciones de escaneo: Se evaluará si el software permite el escaneo al iniciar, el escaneo bajo demanda, el escaneo programado, escaneo de archivos comprimidos, limpieza automática al escanear, cuarentena de archivos infectados, protección de correo, protección de mensajería instantánea, protección P2P o la protección de registro de inicio de Windows.
- Opciones de soporte: Además del hecho de tener soporte on-site en los países a implantar, se evaluará si tiene soporte telefónico, si dispone de soporte por chat y/o e-mail, si dispone de foros de usuarios y si hay tutoriales y bases de conocimientos actualizadas.
- Compatibilidad: Se ha de verificar que será compatible con todos los sistemas operativos de los servidores y ordenadores de la empresa.

- Consola de gestión centralizada y distribuida: Se ha de poder realizar tareas de gestión y mantenimiento del antivirus desde el corporativo y también a nivel local.
- Delegación de derechos de administración a nivel local: Es necesario delegar en administradores locales las tareas de gestión y mantenimiento de cada sede local.

6.2.4 Antispam

El correo conocido como Spam es un tipo de correo con fines propagandísticos o maliciosos que se intenta transmitir por parte del creador del mismo al mayor número de personas posible, utilizando una metodología de broadcast que intenta autoreenviarse todas las veces posibles desde los servidores de correo a los que llega. Los efectos del mismo van desde la simple pérdida de tiempo y productividad en los trabajadores a daños en los ordenadores o pérdidas de información y de seguridad en los sistemas.

Para evitarlo se necesitará un elemento antispam en el sistema que evite a los usuarios la recepción de este correo basura para aumentar la productividad y la seguridad del sistema. A la hora de decantarse por un fabricante u otro se evaluará toda una serie de requisitos sobre rendimiento, capacidad, funcionalidad, etc.:

Puntos a evaluar:
Tipo: Un punto básico a tener en cuenta para decantarse por una opción u otra será saber si el dispositivo es físico, lógico o servicio externo. En la primera opción el coste es mayor y la escalabilidad depende del fabricante. En la segunda opción el coste es menor pero requerirá un equipo aparte para instalarlo. La tercera opción es la más económica pero provoca reticencias por temas de seguridad, ya que se ha de depender de alguien externo para que realice la limpieza de correo basura.

Motor Antivirus: Un antispam lleva un motor antivirus en el que se basa y con el que ha de ser compatible. Esto hace que la elección de antivirus y antispam vaya muy ligada.

Motor Antispam: En el caso de fabricantes de antispam que sea un dispositivo físico, el servicio de antispam puede proporcionarlo el fabricante o puede instalar un motor de otro desarrollador.

Opciones de filtrado: de todas las opciones existentes que puede tener un dispositivo, se estará interesado en determinadas acciones que haya de realizar,

con lo que el dispositivo que se escoja ha de poder dar respuesta a todas las necesidades definidas. Entre las posibles opciones se encuentran:

- Filtrado de salida: El dispositivo es capaz de evaluar el mail saliente para asegurar que no se está inyectando mails SPAM involuntariamente en la red.
- Blacklist: El dispositivo es capaz de utilizar una serie de listas negras publicadas en internet que contienen listados de spammers.
- Greylist: Similar a las listas negras, las listas grises no impiden recibir algún correo de dominios sospechosos de ser Spam pero limitan el número de mensajes recibidos de estos dominios
- Detección de programas "Zombie": El sistema es capaz de detectar una serie de programas denominados Zombie que se hayan inactivos para pasar desapercibidos pero una vez recibidos pueden activarse y generar Spam.
- RDNS lookup: El dispositivo es capaz de verificar contra internet que el correo recibido es auténtico. Se basa en el nombre DNS para verificar si los dominios que aparecen dentro de la dirección e-mail de origen existen o no.
- RPD: Las técnicas RPD (Detección de Patron Recurrente) son capaces de extraer el patrón de un mensaje para saber si es un correo Spam.
- Análisis Heurístico: Es similar al RPD pero con la capacidad de evaluar si un correo es spam de manera autónoma y sin basarse en un listado predefinido de patrones, sino autoevaluando si el patrón es susceptible de ser Spam. Marca los correos como sospechosos a la espera de que llegue una confirmación por parte de los administradores, locales o corporativos dependiendo de la configuración.
- Granularidad de políticas de seguridad: Evaluar los niveles a los que permite definir las políticas de seguridad. A nivel de usuario, de dominio, de sede, etc.
- Granularidad de cuarentena: Se ha de comprobar si el sistema permite definir diferentes niveles y zonas de cuarentena, ya sea por usuario, por dominio, por sede, etc.
- Capacidad de acción de usuario final: el usuario final ha de poder decidir sobre las listas negras de correo y sobre los correos a dejar en cuarentena.
- Reporting: El sistema es capaz de enviar un listado diario con los mails recibidos a cada usuario y al administrador del sistema.
- Monitorización: El sistema ha de ser monitorizable de manera externa. Evaluar también si es compatible con sistemas de monitorización estándares.

6.2.5 Firewall

Además del correo basura y los virus existen otros peligros en la red de los cuales se tiene que proteger adecuadamente. Entre ellos están los denominados hackers que pueden intentar acceder a los sistemas con diferente grado de mala intención, desde el simple reto de conseguir acceder hasta la obtención de información confidencial o la intención de causar daño en el sistema. El elemento que ayuda a defenderse del mismo es el firewall o cortafuegos.

Una vez definida su función se van a evaluar los puntos a comparar para decidir una solución u otra:

Ancho de banda firewall: Se ha de evaluar la capacidad del producto para verificar si se adecúa a las necesidades ya que todo el tráfico de la red ha de pasar por este elemento que actuará de filtro a todas las conexiones entrantes y salientes.

Ancho de banda VPN: Además de la capacidad general del firewall hay que verificar la capacidad de gestión de tráfico por VPN (Red Privada Virtual).

Modo de filtrado: Hay que verificar que el firewall sea capaz de filtrar a nivel de aplicación, a nivel de IP, a nivel de puertos y/o a nivel de conexiones.

Número máximo de sesiones simultáneas: Número de sesiones de usuario que puede soportar el firewall en paralelo.

Número máximo de túneles VPN: Otra manera de evaluar la capacidad del dispositivo, especialmente si se está interesados en trabajar con VPN, es el número máximo de túneles VPN que podrá atender en paralelo el firewall.

Número de interfaces Ethernet: Número de conectores Ethernet de entrada y salida de los que dispone el firewall.

Características opcionales: Además de las capacidades básicas se ha de evaluar si el firewall es capaz de satisfacer todas las opciones añadidas que se necesiten:

- Protección ante denegación de servicio: La DoS es uno de los ataques más comunes de los que ha de proteger un firewall. Es un ataque que a través del envío de un número masivo de peticiones bloquea la red.
- Protección ante Spoofing: Spoofing es la falsificación de la dirección IP por parte de las conexiones entrantes. El sistema ha de ser capaz de rechazar este tipo de ataque para verificar que las conexiones entrantes son fiables.

- Protección ante intrusos: Las tácticas denominadas IDS/IPS (sistema de detección de intrusos y sistema de prevención ante intrusos) son maneras de detectar y evitar el acceso indeseado de personas externas a la organización a la red. Es importante tanto la prevención para evitar que se produzcan ataques de estas características como la detección de intrusos si se llega a consumar un ataque.
- Antivirus Gateway integrado: El firewall es capaz de realizar las funciones de antivirus para los protocolos de mail, internet, ftp, streaming y terminal server.
- Verificación de antivirus en el cliente: El firewall verifica que el PC que intenta salir a internet tenga el antivirus corporativo instalado y actualizado. En el caso de no tenerlo instalado redirecciona directamente a la página del antivirus corporativo para su descarga y en el caso de estar desactualizado fuerza la actualización.
- Antispyware integrado: el firewall es capaz de filtrar y detectar a nivel de contenido la existencia de software maligno, poniendo en cuarentena los paquetes sospechosos o eliminando la parte de contenido que se detecte como peligrosa.
- Filtrado de mensajería: Capacidad de bloquear las conexiones asociadas a mensajería instantánea para algunos o para todos los usuarios de la red.
- Filtrado P2P: Capacidad de bloquear las conexiones Peer to Peer (usuario a usuario) mayoritariamente utilizadas para descargas ilegales o no permitidas por las empresas.
- Filtrado de contenidos: Capacidad de bloquear determinadas páginas web basándose en la categoría de las mismas, es decir, si son direcciones asociadas a pornografía, armas, drogas, búsqueda de trabajo, de viajes, juegos, apuestas, en definitiva consideradas o ilegales o como mínimo no productivas para la organización.
- Conectividad wireless: Capacidad para permitir la conexión directa desde los PC vía wi-fi.
- Asistente de instalación: el dispositivo dispone de un asistente para facilitar la instalación, especialmente útil si la persona que lo va a instalar no tiene el conocimiento suficiente de redes.
- Interfaz Gráfica: el firewall puede ser administrado de manera gráfica a través de una interfaz web. Facilita el uso del mismo respecto a los dispositivos que solo tienen interfaz de comandos.
- Balanceo de ISP: El firewall es capaz de tener conectados dos ISP (Internet Service Provider, o líneas de salida a Internet) y salir a internet por uno u otro en función de carga, o definir uno como principal y otro como backup.
- DHCP Relay: Al conectarse a una red lo primero que se necesita es conseguir una dirección IP que identifique para poder enviar y recibir tráfico. La característica de DHCP relay lo que permite es atravesar el

firewall hasta un servidor DHCP que esté en otra red y que sea éste el que proporcione la IP.

- Calidad de Servicio: La calidad de servicio asociada a un firewall es la capacidad de asignar prioridades diferentes a determinadas aplicaciones en función de si se definen como aplicaciones de negocio o no. Los estándares asociados a la gestión de calidad de servicio se estudiarán en el proceso de selección de proveedor de servicios de Internet.
- Voz sobre IP: Se verificará que el firewall permita la gestión de tráfico VoIP. VoIP es un protocolo que permite enrutar las conversaciones telefónicas a través de la línea de datos, como tráfico IP. Dicho protocolo viene definido en base al estándar de la IETF RFC 3261 [2] en el que se detallan sus consideraciones básicas de funcionamiento si bien se puede ampliar con otros RFC.
- Redes virtuales VLAN: Capacidad de gestionar diferentes redes virtuales dentro de la red física, asignando diferentes rangos de direcciones en función de si el elemento se considera perteneciente a una red o a otra. Las opciones de red virtual ha de cumplir con las recomendaciones IEEE 802.1Q.

6.2.6 Servidor DNS

El servidor DNS (Domain Name System) se utiliza en los sistemas de comunicaciones para determinar la relación entre los nombres asociados a un servidor y su dirección IP para poder enviar y recibir información a los servidores correctamente.

El requisito básico es de compatibilidad con los sistemas operativos Windows, Linux y las aplicaciones que se utilizan. Ha de estar adaptado al estándar RFC 1035 de la IETF [3].

Por otro lado se evaluará el tipo de DNS necesario, si se define como un dispositivo independiente o como un servicio de otro servidor que proporcione además otras funcionalidades.

6.2.7 Servidor DHCP

El servidor DHCP (Dynamic Host Configuration Protocol) es un servicio que proporciona la dirección IP y otros parámetros de configuración a cada uno de los elementos de la red de manera automática para reducir el coste administrativo que supondría hacerlo manualmente.

Las diferentes opciones de configuración son como dispositivo físico o como servicio dentro de otro servidor. Se elegirá uno u otro en función de las necesidades, coste y compatibilidades con el resto del sistema. El requisito básico que ha de cumplir es el de compatibilidad con el estándar de la RFC 2131 [4], para asegurarnos el correcto funcionamiento con la gran mayoría de componentes del mercado.

6.2.8 Servidor Active Directory

Active directory es un servicio de gestión centralizada de la seguridad de la red. Consiste en una base de datos que contiene usuarios, grupos, permisos y políticas de seguridad, todos pertenecientes a uno o varios dominios y subdominios. Permite la autentificación de usuarios y ordenadores dentro de una red determinada.

Las diferentes opciones a escoger en este caso es el fabricante, que en la mayoría de casos es Microsoft, pero también se debe evaluar otras alternativas como Samba, Novell o Java. Se buscará que cumpla con el estándar de la IETF RFC 2307 [5] para asegurar compatibilidad con todos los elementos de la red así como que cumpla con todos los estándares para ser compatible con LDAP [6]:

The Current State of LDAP

Developed by the Internet Engineering Task Force (IETF) in 1997, the current LDAPv3 implementation is a renovation of LDAPv2, which primarily tackles deployment limitations identified within the previous version. LDAPv3 also enriches compatibility with X.500 along with enhanced integration with non-X.500 directories. LDAPv3 encompasses LDAPv2 within a new set of RFCs.

LDAPv3 is a Proposed Standard currently defined by RFC 3377, which includes, the RFCs below in addition to support for the LDAPv2 RFCs listed above[1]:

- ***RFC 2251*** – Lightweight Directory Access Protocol (v3)
- ***RFC 2252*** – LDAP (v3): Attribute Syntax Definitions
- ***RFC 2253*** – LDAP (v3): UTF-8 String Representation of Distinguished Names
- ***RFC 2254*** – String Representation of LDAP Search Filters
- ***RFC 2255*** – The LDAP URL Format
- ***RFC 2256*** – A Summary of X.500(96) User Schema for use with LDAP (v3)
- ***RFC 2829*** – Authentication Methods for LDAP
- ***RFC 2830*** – LDAP (v3): Extensions for Transport Layer Security

Ilustración 3: Relación de RFC asociados a LDAP

Al ser en todos los casos en un elemento software, lo que se deberá escoger también es el servidor sobre el que se instala en base a la capacidad del mismo, el sistema operativo sobre el que va a correr y la versión del mismo.

6.2.9 Servidor de ftp

El servidor de ftp es necesario para poder disponer de la capacidad de guardar y descargar ficheros desde cualquier sitio del mundo con conexión a internet. Sirve especialmente para dar a los comerciales de la empresa la capacidad de disponer

de información cuando no están en las oficinas y no disponen de la posibilidad de acceder por VPN.

A la hora de elegir el servidor de ftp de entre los principales fabricantes del mercado, se han de evaluar una serie de características:

Tipo de servidor: Un servidor de ftp puede ser un dispositivo físico que disponga de un software propio destinado al servicio ftp o un software que se tenga que instalar en un servidor diferente.

Tipo de plataforma: Se evaluará si la plataforma sobre la que puede correr el servicio en caso de ser lógico o la que trae instalado el dispositivo en caso de ser físico se adecua a las necesidades del servicio.

Capacidad de almacenamiento: se evaluará la capacidad de almacenamiento requerida y en función de ello se escogerá un tipo de servidor u otro.

Complejidad de Administración: se evaluará las capacidades de administración en cuanto a seguridad y la facilidad de uso del producto.

Compatibilidad con SFTP: El servidor de ficheros ha de permitir el uso de Secure FTP que permite la comunicación fiable entre entornos. Ha de cumplir con el estándar RFC 2228 [7] para asegurarnos un correcto funcionamiento del servicio.

6.2.10 Servidor de ficheros

Similar al servidor de ftp pero con una orientación diferente, se implementará un servidor de ficheros.

El cambio respecto al servidor ftp es que este servidor está orientado a estar accesible solo desde dentro de la red de la empresa, de manera que los requisitos de seguridad no sean tan elevados.

En este caso las diferentes opciones a evaluar serán:

Tipo de servidor: puede ser un servidor físico, del estilo NAS, o un servidor cualquiera en el que se habilite la posibilidad de compartir ficheros y se permita el acceso remoto desde la red

Capacidad: Se ha de determinar la capacidad necesaria del servidor, en base a los requisitos de los usuarios del mismo.

Configuración de discos: Se ha de definir la configuración de discos del servidor en función del nivel a la tolerancia a fallos que se quiera implementar y el rendimiento que se quiera obtener del servidor. Una vez definida, el servidor que se escoja ha de permitir configurar este nivel de seguridad.

Seguridad: A pesar de no tener los requisitos de seguridad tan elevados como un servidor de ftp, el servidor de ficheros también ha de permitir gestionar la seguridad tanto de lectura como de escritura para las diferentes carpetas que se considere necesario. Se valorará la integración para poder gestionar la seguridad con el servidor Active Directory previamente mencionado, así como una interfaz de gestión amigable.

6.2.11 Gestor de ancho de banda

El gestor de ancho de banda aporta una serie de características que mejoran de manera global el rendimiento de la red priorizando el diferente tráfico para que se adapte a los recursos disponibles. Sus principales objetivos son compresión del tráfico para que sea menor, aceleración de dicho tráfico, monitorización en tiempo real de todos los tipos de tráfico que pasan por la red y gestión los recursos de ancho de banda asignando cuotas que diferencian las aplicaciones de negocio del resto de aplicaciones que consumen ancho de banda.

Los puntos a evaluar entre los distintos fabricantes de gestores de ancho de banda son:

Rendimiento: Para evaluar el rendimiento de un gestor de ancho de banda el análisis se basará en los ratios de compresión o en el ratio de incremento de la velocidad.

Funcionalidades: Las diferentes funcionalidades que ofrezca el producto han de satisfacer cuanto menos las necesidades del cliente. Las funcionalidades que puede tener un gestor de ancho de banda son:

- Diferenciación de aplicaciones críticas: el aplicativo ha de permitir diferenciar entre tipos de tráfico para poder asignar cuotas en función de la criticidad.
- Asignación adaptativa de recursos en función del estado de la red. Para ello ha de ser capaz de autogestionarse y poder ir variando las asignaciones a las diferentes aplicaciones de manera dinámica.
- Monitorización: El sistema ha de ser capaz de monitorizar lo que está corriendo en la red y alertar cuando detecte comportamientos o tráfico no deseado.

- Control del tráfico: capacidad para limitar las aplicaciones que se consideren como maliciosas o de uso recreativo y que no están relacionadas con el negocio.

6.2.12 Impresoras y servidores de impresión

Para poder disponer de documentos impresos lógicamente se necesitará una o varias impresoras.

El criterio de evaluación para determinar el número de impresoras escogido es departamental. Cada departamento ha de tener como mínimo una impresora en blanco y negro. En caso de ser un departamento superior a 15 personas se instalarán 2 o más impresoras (este dimensionamiento es arbitrario y acordado con el cliente). Por otro lado, se encuesta a los departamentos para determinar cuáles de ellos necesitarán una impresora a color. En el caso de necesitarla el departamento pasaría a tener dos impresoras, una a color y otra en blanco y negro. La impresora en B/N se define siempre como predeterminada.

A la hora de definir la marca y modelo que se escogerá como corporativa se evaluarán diferentes puntos y características que se consideran de interés:

Capacidad de impresión: Se compara entre los diferentes modelos la capacidad de impresión que ofrecen para que no suponga un punto de retardo o pérdida de productividad de los empleados.

Posibilidad de impresión a color: Para aquellos departamentos que necesiten impresora a color, esta posibilidad la hace determinante a la hora de escoger un modelo u otro.

Capacidad multifunción: Para simplificar la topografía de red se buscará que el modelo de impresora en cuestión tenga capacidades multifunción:

- Impresora
- Fotocopiadora
- Escáner
- Fax
- Impresión de etiquetas
- Impresión de códigos de barras

Facilidad de mantenimiento: La intención desde el departamento de informática es que el mantenimiento de la impresora, el cambio de tóner y de consumibles se delegue desde el departamento de informática hasta el resto de departamentos.

Por ello interesará evaluar la facilidad de cambio de tóner, el número de pasos a realizar para ello y la simplicidad del modelo.

Monitorización remota: Para facilitar la gestión de las impresoras se buscará que la impresora permita la monitorización en remoto de diferentes parámetros y alertas:

- Falta de papel
- Atasco
- Desconexión
- Incidencias de Hardware o Software
- Nivel de tinta en tóner

Evolución de funcionalidades: Se evaluará si el fabricante es capaz de ofrecer adaptaciones futuras del software de impresión a posibles requisitos en cuanto a cambios de formato de etiquetas, códigos de barras o cualquier otra modificación o nueva funcionalidad que se requiera.

Servidor de impresión: El requisito básico del servidor de impresión entra dentro de los elementos comunes, es la compatibilidad con la impresora y con la red. El coste del servidor es el otro punto a tener en cuenta si bien también es uno de los puntos comunes de evaluación.

6.2.13 Routers

La función de los routers o enrutadores es la de dirigir el tráfico de la red hacia los diferentes destinos que se requieran, ya sean internos (dentro de la propia LAN) o externos (salida hacia WAN). El objetivo es conseguir dispositivos que sean capaces de realizar su función sin afectar al rendimiento del resto de sistemas. Por ello la principal característica que se tendrá en cuenta es el rendimiento que ofrecen los fabricantes de dicho elemento. Sin embargo también hay otros puntos a considerar. A continuación se explican todos los puntos que entran en juego para la elección del router adecuado.

Rendimiento: El rendimiento es el punto clave para la elección del router. Interesará aquel modelo que proporcione un rendimiento adecuado, pero además que mantenga este rendimiento en diferentes condiciones, como cuando se activa las opciones de calidad de servicio, firewall, voz sobre IP, videoconferencia o filtrado de accesos por IP.

Funcionalidades: El router ha de ser tener como servicios integrados la capacidad de manejar tráfico asociado a voz sobre IP o videoconferencia, dar la posibilidad

de usar calidad de servicio al tráfico enrutado o disponer de funcionalidades básicas como firewall en caso de caída del firewall principal.

Facilidad de gestión: Interesará que el router tenga una gestión simple para reducir el coste de administración.

Monitorización: Se necesitará para garantizar el correcto funcionamiento del sistema que el router sea monitorizable para detectar problemas de rendimiento, caídas o cualquier otro problema.

Número de interfaces: Un punto a evaluar también importante es la cantidad de interfaces que se podrán conectar al router. Cuanto mayor sea el número de interfaces del router menor será el número de routers necesarios.

Capacidad de redundancia en caso de caída: Interesa que el router en cuestión disponga de protocolos de redundancia, de manera que sea capaz de absorber el tráfico de otro router en caso de que este otro caiga.

6.2.14 Switches

Un switch o conmutador de paquetes es un elemento capaz de intercambiar datos dentro de redes LAN, entre diferentes segmentos de la misma red. Es un elemento similar al router pero sin la capacidad de redirigir información al mundo exterior.

Como en el resto de elementos, a continuación se definen los puntos que interesará evaluar para definir cuál es el modelo adecuado para las instalaciones:

Número de puertos: Al igual que en el caso del router, el número de puertos es significativo ya que el número de switches necesarios para la red dependerá del número de dispositivos que se pueda conectar a cada uno.

Gestión remota: Interesará que disponga de protocolos de gestión remota y que estos sean compatibles con los programas de monitorización y gestión del cliente. También interesará que esta gestión sea lo más amigable posible para el administrador.

Puertos auxiliares de red: También denominados puertos troncales, el switch ha de disponer de puertos auxiliares para interconectar switches entre ellos, preferiblemente que sean puertos de fibra óptica para garantizar un óptimo rendimiento, ya que por estos puertos auxiliares circulará un volumen mayor de tráfico que por el resto de puertos, puesto que son los puertos de concentración

de la mayoría de tráfico del resto de puertos (salvo aquel tráfico que circule entre elementos que estén en el mismo switch)

Velocidad de transferencia: se buscarán aquellos dispositivos que proporcionen una velocidad de transferencia suficiente para no provocar limitaciones a los elementos que estén conectados al switch. Como mínimo deberá disponer conexiones de 100BaseTX y Gigabit Ethernet para las conexiones con los dispositivos críticos.

Capacidad VLAN: Determinados switches disponen de la capacidad de manejar tráfico a través de VLAN (Virtual LAN). Esta funcionalidad es la capacidad de tratar diferentes redes lógicas o segmentos de red lógicos dentro de una sola red física y ser capaz de redirigir la información de todas estas redes lógicas hacia el router que tenga conectado.

Capas de switch soportadas: Existen principalmente 2 tipos de switches en función de las capas o rangos de actuación. Los switches que actúan en capa dos son aquellos que realizan puramente funciones de switch. Los switches de capa tres son aquellos que son capaces de realizar funciones de routing. En este caso interesará que disponga de funcionalidades de capa tres y que sea capaz de activar o desactivar dicha funcionalidad para por un lado no ser redundantes con los routers pero por otro lado ser capaces de funcionar como routers en caso de caída de alguno de ellos. Adicionalmente existen switches denominados de capa cuatro, que añaden funcionalidades de filtrado pero no hay un mercado suficiente para garantizar una correcta elección y se escoge la opción que la funcionalidad de filtrado la realice el firewall.

6.3 Requisitos de Comunicaciones

En el apartado referente a los requisitos de comunicaciones interesará fijar las necesidades asociadas a capacidad de comunicaciones para tener una correcta comunicación, en base a todas las aplicaciones que han de ejecutar los usuarios.

6.3.1 Conexión CPD Local - Proveedor

La interconexión entre el CPD local y el proveedor ha de poder garantizar el correcto funcionamiento de todas las aplicaciones que han de utilizar dicha conexión. Para dar un rendimiento adecuado, y teniendo en cuenta que todas las aplicaciones del sistema irán a través de un sistema Citrix que centraliza el ancho de banda consumido en un solo sitio, se definen una serie de parámetros que

influirán en la velocidad contratada con el proveedor de servicios escogido. Estos parámetros son:

- Consumo de conexión Citrix: Al ser un interfaz que centraliza la potencia de cálculo en los servidores y al cliente envía solo la interfaz gráfica, todas las aplicaciones abiertas consumen el mismo ancho de banda
- Número de conexiones Citrix en paralelo por usuario: se definirán un número estimado de las conexiones que tendrá abiertas el usuario en base a las aplicaciones que deberá utilizar
- Número de usuarios: Se establece el número de usuarios medio que ha de tener cada fábrica para evaluar la capacidad en conjunto requerida por el sistema
- Porcentaje de usuarios en paralelo: En base al número de usuarios anterior, se calcula que porcentaje de estos utilizarán el sistema en paralelo
- Ratio de compresión del gestor de ancho de banda: El gestor de ancho de banda permite dar una mayor velocidad de transmisión a la línea con lo que se optimiza el ancho de banda. Este ratio se ha de tener en cuenta también a la hora de calcular el ancho de banda necesario a contratar.
- Ancho de banda extra: Se define un porcentaje a aplicar hacia arriba para garantizar el servicio correcto y tener margen de operación en caso de incremento de la demanda de ancho de banda, ya sea por mayor número de usuarios o por mayor número de conexiones por usuario.

6.3.2 Conexión CPD Central - Proveedor

Para calcular el ancho de banda del CPD central con el proveedor tendremos en cuenta que para poder garantizar el tráfico del CPD central con los tráficos de todos los CPD locales, el enlace ha de ser mayor o igual que la suma de todos los enlaces entre CPD local y su proveedor calculados en el apartado anterior.

Este cálculo aplicará tanto para el cálculo de la conexión necesaria entre el CPD central con el proveedor como para el enlace entre CPD de BRS con el proveedor.

6.3.3 Requisitos para los proveedores de servicio

Las líneas deberán ser gestionadas por un operador de comunicaciones. A este operador se le han de exigir determinadas características que harán que se seleccione uno u otro en función de las mismas.

Red MPLS: El proveedor ha de permitir la implementación de redes con protocolo MPLS (Multi Protocol Layer Switching), que consiste en un tipo de red privada y segura pero con la flexibilidad que proporciona Internet. Permite aplicar

funciones de QoS (calidad de servicio), VPN (Virtual Private Network), políticas de enrutamiento y funciones de ingeniería de tráfico. Ha de permitir que las fábricas se vean entre sí, siempre pasando por el CPD central.

Presencia internacional: El operador ha de tener presencia en todos los países en los que haya fábricas de la empresa:

- España
- Grecia
- Italia
- Francia
- Alemania
- Bélgica
- Rumanía
- Turquía
- Reino Unido
- Portugal
- Luxemburgo
- Holanda
- Marruecos

Independencia: Ha de haber algún tipo de independencia entre la línea de producción y de backup, ya sea desde el punto de vista tecnológico (una línea MPLS y otra ADSL) o desde el punto de vista de operador (dos operadores diferentes).

Monitorización: Se requiere una monitorización de diferentes elementos:

- Dispositivos IP a través de los enlaces wan
- Uso del protocolo SNMP (Simple Network Management Protocol) para la monitorización de servicios TCP y UDP
- Plataforma de monitorización escalable que permita una arquitectura distribuida para permitir integrarse con cualquier tipo de red.
- Notificaciones por e-mail, móvil, etc., de alertas por pérdida de disponibilidad y por sobrepasar el 90% de ancho de banda.
- Informes configurables en formato WEB de disponibilidad, caudal utilizado y alertas.
- Sistema de aprendizaje automático preventivo para el control de los equipos.
- Acceso a la herramienta de monitorización por parte del cliente para gestionar alertas e informes.
- Estadísticas en tiempo real.
- Sistema automático de descubrimiento de red.
- Flexibilidad para permitir adecuar el servicio a las necesidades del cliente, añadiendo o eliminando dispositivos de las listas de monitorización.

Rendimiento: Las líneas de comunicaciones, al menos la principal, hacia la sede central tendrán que ser con caudal simétrico garantizado y dedicado al 100%.

Disponibilidad 99,99: Se requiere que el proveedor de servicio sea capaz de ofrecer una disponibilidad máxima para minimizar los posibles impactos que tendría una caída de la comunicación. Se han de exigir unos parámetros de SLA (Service Level Agreement) y compensaciones en caso de no cumplimiento de los mismos

Soporte: El proveedor de servicios ha de disponer de un servicio de Help Desk y procedimientos de escalado de incidencias. Debe disponer de varias criticidades de incidencia para poder priorizarlas y con diferentes grados de SLA. Dichos grados se definirán más adelante en el apartado de definición de las recomendaciones.

La atención de este equipo de Help Desk ha de ser 24x7x365 tanto telefónico como por internet y presencial en caso de ser necesario.

Los parámetros de SLA de dicho soporte han de ser para todas las criticidades como mínimo los siguientes:

- Tiempo máximo de sustitución de piezas o reparación de 24 horas
- Tiempo máximo de sustitución de equipos de 48 horas.
- Tiempo máximo de atención de incidencias de 4 horas.
- Latencia máxima de 50ms de respuesta para la línea principal.
- Latencia máxima de 90ms de respuesta para la línea de backup.

Equipo de enrutamiento: El equipo de enrutamiento en ocasiones lo ofrece el proveedor de servicios. En ese caso se han de tener en cuenta los requisitos especificados en el punto 3.2.13. Especialmente se requiere que los equipos que proporciona para enrutamiento el proveedor de comunicaciones soporten las funcionalidades de VoIP, Videoconferencia y calidad de servicio.

Tiempo de entrega de todas las líneas de comunicaciones: El tiempo máximo que transcurre desde que se solicita la línea hasta que se dispone de ella en para las nuevas fábricas y la unión a la red MPLS de las actuales fábricas será un punto importante a tomar en cuenta.

6.4 Requisitos de procedimiento

El procedimiento de implementación de todo el sistema ha de cumplir toda una serie de requisitos para minimizar el impacto en la fábrica de la implementación

de la solución escogida y para ser capaces de garantizar el éxito y la continuidad de la implantación. Siguiendo los pasos de las recomendaciones ITIL (Information Technology Infrastructure Library) se adopta un modelo de **mejora continua de servicio.**

Dicho modelo pretende que el modelo implementado de comunicaciones ofrezca cada vez un mejor servicio a los usuarios. Para ello propone un modelo que se retroalimenta evaluando la calidad del servicio en base a evaluar la calidad de los diferentes procesos que lo componen (midiendo indicadores clave como la disponibilidad de las comunicaciones, etc). Partiendo de los resultados obtenidos el modelo de mejora continua promueve la definición de iniciativas de mejora y por último una monitorización del resultado de la aplicación de estas iniciativas.

Ilustración 4: Diagrama de perfeccionamiento contínuo de ITIL

Esta filosofía se debe aplicar sobre todos los puntos referidos a procedimiento que se detallan a continuación.

6.4.1 Planificación

La planificación ha de realizarse con una antelación mínima de dos meses para poder disponer de todos los elementos necesarios, hardware, software, licencias y comunicaciones, evitando así demoras indeseadas de la puesta en producción.

Se ha de definir una planificación viable y con márgenes suficientes para evitar la acumulación de retrasos de cara a la fecha final de implantación.

6.4.2 Comunicación

Es muy importante definir una estrategia adecuada de comunicación para asegurar que todos los implicados en el proyecto son conscientes en todo momento de:

- Responsabilidades de cada uno de los implicados
- Fechas de entrega de todos los puntos
- Acuerdos alcanzados
- Reuniones
- Conclusiones y actas

6.4.3 Definición Hitos y Tareas

Se ha de definir un plan de acción para poder realizar un seguimiento adecuado, de manera que cada una de las tareas esté correctamente especificada y se tengan una serie de hitos a cumplir que permitan hacer un seguimiento adecuado del proyecto.

6.4.4 Definición de responsables

Cada una de las tareas de la planificación ha de estar perfectamente clara para todos los implicados en el proyecto y ha de tener un responsable claro, sin ningún tipo de ambigüedad que permita realizar un seguimiento de toda tarea a través de su responsable

6.4.5 Afectación a producción

La producción en todas las fábricas es 24x7 con lo que es imposible conseguir una nula afectación cuando un cambio obliga a detener un sistema. Sin embargo se debe intentar buscar la manera de minimizar el impacto buscando los periodos de calendario de menor producción. Si el cambio requerido implica también afectación a oficinas se procura realizar durante noches y fines de semana en los que el personal de oficinas no está presente, a pesar de que la afectación a producción sea la misma.

En el caso de requerir una parada de producción se avisará con una antelación superior a una semana para que los equipos de producción puedan planificar de manera ordenada la parada. Dependiendo del equipo afectado, la vuelta a la normalidad tras una parada puede costar hasta tres días, con lo que se ha de evitar en la medida de lo posible las paradas y realizar una correcta planificación de las mismas, intentando unir todas las acciones que requieran de parada en una sola.

6.4.6 Control de calidad

Una vez se ha puesto en marcha la infraestructura del modelo propuesto es necesario realizar un control de calidad de todos los puntos verificando que todo funciona según lo esperado. El control de calidad consta de diferentes puntos que deberán analizarse:

- Control físico: Una vez finalizada la instalación de todos los servidores y elementos de la red se ha de verificar que todos los elementos están correctamente fijados, que la interconexión de todos los sistemas es la definida y que la alimentación de todos los equipos es estable y adecuada.
- Operativa básica: Se ha de verificar que todos los equipos funcionan correctamente y responden a lo esperado en cada uno de ellos.
- Monitorización: se ha de comprobar que todos los dispositivos están correctamente monitorizados desde el CPD interno de la fábrica y desde el CPD central.
- Pruebas de estrés: Para cada uno de los dispositivos susceptibles a fallos por una sobrecarga de trabajo se ha de comprobar mediante pruebas de estrés que responden a las especificaciones definidas. Se ha de buscar en cada caso la herramienta más adecuada para cada componente.

6.4.7 Documentación

La documentación de todo el proceso es uno de los puntos de garantía de éxito y continuidad de cualquier proyecto. Por ello se ha de asegurar que durante todas las fases del proyecto se realiza una documentación apropiada para cada punto.

Dentro del apartado de documentación se definirán plantillas diferentes para cada tipo de documento:

- Acta de reunión
- Documento técnico
- Documento de usuario
- Análisis de capacidad
- Resultado de pruebas de validación
- Resultado de pruebas de estrés
- Presentaciones

Dependiendo de las fases se requerirá un tipo de documentación u otro. Todas las plantillas se adaptarán a las recomendaciones de calidad ISO-9001

6.4.8 Contingencia

Es necesario que la estrategia disponga de un plan de contingencia para la puesta en producción y posterior estabilización para poder disponer de una alternativa si hubiera que retroceder algún cambio aplicado en el sistema actualmente en producción. Hay que identificar, si los hay, los puntos de no retorno, es decir aquellos en los que una vez aplicado un cambio no es posible, no es recomendable o es demasiado costoso la marcha atrás.

6.4.9 Seguridad

Se necesita definir una serie de políticas de seguridad que aseguren que cada una de las personas implicadas en el proyecto disponga únicamente de los accesos necesarios e imprescindibles para el desarrollo de sus funciones. Se ha de evitar accesos indeseados por parte de personas ajenas al proyecto y dentro del grupo de personas involucradas en el proyecto se ha de garantizar que no se realizan accesos cruzados entre responsable y apartado.

Para conseguir alcanzar el nivel de seguridad deseado se consultarán diferentes estándares de seguridad y se buscará la mejor opción en lo referente a diferentes apartados:

- Seguridad física: El protocolo que se defina de seguridad ha de garantizar que los accesos que se realicen a los diferentes departamentos físicos (instalaciones, oficinas, salas, CPD, servidores) sean siempre de personas autorizadas para ello.
- Seguridad lógica de dispositivos: Dentro de los diferentes sistemas de información, se ha de garantizar que solo acceden a los diferentes servidores y dispositivos las personas que necesiten hacerlo
- Seguridad lógica de documentos: Los repositorios de documentación han de tener aplicada una correcta seguridad para que solo tengan acceso a documentos aquellas personas que lo necesiten. Se podrá definir accesos individuales, grupo o públicos. Lógicamente los denominados como públicos estarán restringidos a las personas de la organización que tengan acceso a los dispositivos (punto anterior).

7 Matriz de colaboración

Los requisitos del proyecto definidos en el punto anterior hacen referencia a las necesidades completas para la implantación de las recomendaciones que se pretenden obtener de este proyecto. A nivel global se ha colaborado en todos los puntos pero el análisis del estado de las tecnologías o la recomendación de un fabricante u otro no se ha realizado de manera global en todos los puntos. En algunos casos se ha realizado la comparativa, en otro caso se ha definido el componente y en otros casos se han realizado las pruebas del componente en cuestión. Por ello se define primero los roles de participación y para cada uno de los puntos anteriores el grado de colaboración:

- Colaborador: Cuando en un determinado punto se ha dedicado trabajo de consultoría, de colaboración, de participación en reuniones o en general la participación en la definición de los requisitos necesarios, se marca como colaborador en ese punto.
- Evaluador: Los puntos marcados con rol evaluador son aquellos en los que la función desempeñada ha sido la de realizar las comparativas entre los diferentes productos y tecnologías existentes.
- Ejecutor: Son aquellos puntos en los que en base a la evaluación previa se escoge una opción u otra.
- Verificador: Para las opciones escogidas, ya sea por nosotros o por otros se realizan las pruebas de funcionamiento, de capacidad, etc.

		ROL			
ETAPA	TAREA	COLABORADOR	EVALUADOR	EJECUTOR	VERIFICADOR
REQUISITOS DE INFRAESTRUCTURA	ESTUDIO DE REQUISITOS DEL CPD	X		X	X
	SALA DE CONFERENCIAS	X			
REQUISITOS DE RED	TOPOLOGÍA GLOBAL DE LA RED	X		X	
	TOPOLOGÍA INTERNA DE LA RED	X		X	
	PORTAL	X	X	X	X
	ANTIVIRUS	X	X	X	X
	ANTISPAM	X	X	X	X
	FIREWALL	X	X	X	X
	SERVIDOR DNS	X			
	SERVIDOR DHCP	X			
	SERVIDOR ACTIVE DIRECTORY	X			
	SERVIDOR DE FTP	X			
	SERVIDOR DE FICHEROS	X			
	GESTOR DE ANCHO DE BANDA	X			
	IMPRESORAS Y SERVIDORES DE IMPRESIÓN	X			
	ROUTERS	X			
	SWITCHES	X			
REQUISITOS DE COMUNICACIONES	ANCHO DE BANDA DE CONEXIÓN CON CPD CENTRAL	X		X	X
	ANCHO DE BANDA DE CONEXIÓN CON CPD BRS	X			
	REQUISITOS PARA LOS PROVEEDORES DE SERVICIO	X	X	X	X
REQUISITOS DE PROCEDIMIENTO	PLANIFICACIÓN	X		X	
	COMUNICACIÓN	X			
	DEFINICIÓN HITOS Y TAREAS	X		X	
	DEFINICIÓN DE RESPONSABLES	X			
	AFECTACIÓN A PRODUCCIÓN	X			
	CONTROL DE CALIDAD	X			
	DOCUMENTACIÓN	X		X	
	CONTINGENCIA	X			
	SEGURIDAD	X			

Tabla 2: Matriz de Colaboración en el proyecto

8 State of the art

Partiendo de la matriz de colaboración en el proyecto, se van a evaluar en este apartado todos aquellos puntos marcados en los que el papel jugado ha sido el de Evaluador. En todos ellos se han realizado comparativas de diferentes elementos marcando las fortalezas y debilidades de cada uno de ellos para la posterior decisión de una opción u otra en función de las mismas.

Varios de los análisis que se detallan a continuación están relacionados entre sí, ya que entre otras cosas se valora la compatibilidad entre diferentes puntos. Es decir, por ejemplo, el antivirus ha de funcionar bien con el firewall que se escoja para que no haya luego problemas de rendimiento o pérdida de información.

8.1 Procedimiento

A la hora de evaluar las tendencias, las novedades del mercado y elegir los productos que se incluirán en la comparativa se seguirán una serie de pasos. El primer paso es investigar cuáles son las mejores técnicas y las novedades que hay en el mercado. Para ello se realiza una labor de investigación a través de Internet basada en boletines de noticias on-line, publicaciones especializadas, recomendaciones o cualquier otro medio por el que se tenga conocimiento de nuevos protocolos, nuevas técnicas o avances referentes al componente a evaluar en cuestión.

El segundo paso es definir un criterio de selección por el cual se pre-seleccionará un número adecuado de productos, que dependerá del caso. Dicho criterio ha de quedar justificado en cada caso. El criterio más utilizado en este proyecto es el de escoger los productos mejor valorados en publicaciones con reputación y en concreto se recurrirá especialmente a los cuadrantes Gartner Magic Quadrant. En otros casos serán todos los productos que cumplan con unos requisitos mínimos (ISP o Internet Service Provider que puedan dar servicio en todos los países que se necesita).

El tercer paso es una vez escogidos los productos a comparar, plasmar las comparativas de la manera más gráfica posible, mediante tablas o gráficos, para facilitar la tarea de selección del producto a escoger.

Por último y basándose en las tablas anteriores se buscarán las fortalezas y debilidades de cada producto, destacando entre ellas las más importantes.

Cuadrantes Gartner

En este apartado se va a justificar por qué se escoge Gartner y sus Magic Quadrants para la preselección de productos que se van a evaluar.

Gartner es una compañía de consultoría e investigación dedicada a evaluar productos y componentes de las tecnologías de la información. Fue fundada en 1979 y tiene su sede ejecutiva en Stamford (EEUU). Es uno de los líderes mundiales en análisis de productos informáticos y una compañía de gran reputación en el mercado de consultoría informática y la investigación tecnológica.

Uno de sus productos de mayor éxito y más utilizados como punto de partida en la toma de decisiones respecto a productos informáticos son los Gartner Magic Quadrants. Estos cuadrantes clasifican de manera gráfica en cuatro segmentos los principales fabricantes del tipo de producto en cuestión.

Los dos ejes de análisis de los cuadrantes Gartner son en el eje horizontal la visión de mercado y la cobertura que realiza el fabricante a los diferentes requisitos que aparecen para ese producto, que es lo que Gartner llama completitud de visión. En el eje vertical el análisis se basa en la capacidad de ejecución, tanto por las características del producto como por la solvencia y la capacidad de la empresa para operar.

En el eje vertical de análisis se tienen en cuenta toda una serie de puntos con diferente valoración. Pese a que los criterios de evaluación son comunes para todos los cuadrantes de Gartner, el peso que tiene cada uno varía en función del producto que se vayan a analizar. A continuación se muestra un ejemplo del peso que tienen los criterios (el ejemplo es para la comparativa de firewalls):

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	standard
Sales Execution/Pricing	standard
Market Responsiveness and Track Record	standard
Marketing Execution	standard
Customer Experience	high
Operations	standard

Source: Gartner

Tabla 3: Criterio para valorar la capacidad de ejecución

A continuación se detalla una pequeña explicación para cada punto.

- Fortalezas del producto o servicio: El producto tiene buenas referencias por parte de clientes e instalaciones en las que funcione, buen resultado en encuestas y con alta fidelización. A nivel de producto están implantadas en instalaciones complejas que requieren de productos con alta flexibilidad.

- Viabilidad general: La empresa se encuentra en una situación financiera positiva que le permite afrontar las mejoras e innovación en sus productos. Los productos son fiables y se utilizan para aplicaciones críticas de negocio.

- Precio/ventas: El fabricante dispone de un extenso canal de distribución y de un soporte pre y post venta avanzado. No se evalúa un valor de precio global si no la relación calidad/precio y el TCO o Coste Total de Propiedad (Total Cost Ownership), que es el coste asociado al producto en toda su vida útil.

- Respuesta ante el mercado: La empresa y sus productos son dinámicos y fácilmente adaptables a las condiciones externas marcadas por los mercados.

- Presencia de mercado: Se valora la presencia en el mercado a nivel global.

- Experiencia del cliente: Incluye la percepción que los clientes tienen del producto en sí.

- Operaciones: El producto tiene una gran capacidad operativa para dar respuesta a grandes corporaciones.

En el otro eje de análisis, el eje horizontal, los apartados clave que se evalúan son, junto con su importancia a la hora de dar una clasificación. Al igual que en el caso de la capacidad de ejecución, los pesos asignados a cada criterio varían en función del producto.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	standard
Marketing Strategy	standard
Sales Strategy	low
Offering (Product) Strategy	high
Business Model	standard
Vertical/Industry Strategy	standard
Innovation	high
Geographic Strategy	standard

Source: Gartner

Tabla 4: Criterio para valorar la completitud de visión

- Comprensión del mercado: Son capaces de entender las necesidades del mercado y adaptarse al mismo

- Estrategia de Marketing: Tienen una estrategia definida a medio y largo plazo, no improvisan objetivos de una manera anual.

- Estrategia de Ventas: Disponen de servicio pre y post venta de manera que recomiendan la mejor opción antes de vender y una vez vendido dan un soporte adecuado.

- Estrategia de Oferta de producto: Disponen de un amplio catálogo de productos de manera que es fácil adaptarlo a las necesidades de cada cliente.

- Modelo de Negocio: En su modelo de negocio incluyen partidas para Investigación y Desarrollo (I+D), de manera que lo consideran parte fundamental de su negocio. Este presupuesto permite evolucionar los productos que luego ofrecen.

Estos son los criterios generales de análisis en un cuadrante de Gartner. Los criterios concretos que hacen que el producto se posicione en cada uno de los ejes dependen del producto que se está analizando y se irán detallando en los próximos apartados.

Basándose en estos dos ejes, Gartner define cuatro áreas donde ubicar los productos:

Leaders

Los Leaders o líderes son los productos que cubren todas las expectativas y funcionalidades del mercado, adelantándose a ellas, productos innovadores desarrollados por empresas con una amplia visión de mercado.

En el apartado de capacidad de ejecución son productos de alta potencia con experiencia en implantación en grandes corporaciones y con un soporte avanzado que minimiza las incidencias. Se trata de productos de alta calidad y con gran prestigio entre los clientes de Gartner que los han utilizado y que los tienen implantados. Además han de tener una gestión amigable y capacidad de generar informes de su actividad.

Challengers

Dentro del cuadrante de Challengers o retadores se encuentran aquellos fabricantes que están bien instaurados en el mercado pero cuya capacidad

evolutiva es limitada por lo que sus productos son estables, les cuesta desarrollar nuevas capacidades para adaptarse a las exigencias de mercado.

Por ello son generalmente productos que tienen un buen precio y es su manera de introducirse en los mercados.

A su vez son empresas muy focalizadas en el producto que ofertan, de manera que los productos son fiables a pesar de su lenta evolución.

Visionaries

Los Visionaries o visionarios son aquellas empresas que ofrecen productos en constante evolución, con amplias capacidades y con un amplio abanico de productos lo que implica que en muchos casos intentan disponer de productos multifunción, que integran diferentes capacidades dentro de un mismo dispositivo.

En el lado negativo son empresas con una mala estrategia de ventas y de posicionamiento en el mercado lo que implica que tienen una baja cuota del mismo.

Niche Players

Las empresas consideradas como Niche Players o de nicho de mercado, son generalmente pequeñas empresas que disponen de productos que cubren funcionalidades muy concretas y generalmente disponen de alguna característica especial que les permite mantener su pequeña cuota de mercado.

Al igual que los considerados visionarios, tienen una mala gestión de ventas y marketing lo que no les permite expandir su negocio más allá de su país o su zona geográfica.

8.2 Comparativa de portales

Una vez se define que se va a utilizar una arquitectura distribuida y con el acceso a todas las aplicaciones a través de un portal, es crítico definir el portal que se va a utilizar. Para poder escoger con facilidad una opción se requiere realizar una comparativa de los productos existentes en el mercado y definir para cada uno de ellos las fortalezas que ofrecen y las debilidades que tienen al compararlos entre sí.

8.2.1 State of the art para portales

Se realiza una tarea de investigación para encontrar en el apartado de portales cuales son las funcionalidades más avanzadas que se encuentran en el mercado a través de Internet. Como resultado de dicha búsqueda se obtienen una serie de interesantes características que se buscará que disponga el producto:

Protocolos de comunicación: Se encuentran dos principales protocolos de comunicación destinados al tráfico de portales, que gestionan básicamente el tráfico de interacción usuario-aplicaciones. Dicho tráfico como se ha comentado en apartados anteriores está mayormente destinado a la visualización que devuelven las aplicaciones que corren en los servidores y la interacción de entrada y salida por parte del usuario. Estos dos protocolos son RDP e ICA.

RDP: Las siglas significan Remote Desktop Protocol (Protocolo de Escritorio Remoto). Es un protocolo desarrollado por Microsoft para terminal server y cuyas últimas novedades en el momento incluyen la posibilidad de utilizar ficheros ubicados en el cliente (archivos Office, base de datos de archivado de correo, etc...), mejoras en la presentación y soporte a nuevas aplicaciones y dispositivos.

ICA: Sus siglas en este caso son las de Independent Computing Architecture (Arquitectura de Computación Independiente). Es un protocolo desarrollado por Citrix. Como principales ventajas tiene que es multiplataforma, independiente del sistema operativo cliente, permite la gestión del ancho de banda e incluso permite ser configurado para que parte de la carga de procesado gráfico vaya sobre el ordenador cliente, liberando el servidor en caso de sobrecarga. Como otro elemento diferenciador, permite que el usuario disponga de sonido estéreo en el ordenador cliente.

A continuación se adjunta una tabla comparativa obtenida en base principalmente al documento de referencia [8] con las principales diferencias entre ambos protocolos de comunicación.

	Protocolo	
Característica	RDP 5.2	ICA
SO Clientes soportados	Win32, Win16, Win CE, Pocket PC	Win32, Win16, Win CE, Pocket PC, MS-DOS, Unix, MacOS, Linux, Java
Cliente basado en explorador	Require instalacion de Terminal Server Advanced	Soporta cualquier explorador web
Protocolo de transporte	TCP/IP	TCP/IP, IPX/SPX, NetBEUI, direct serial
Sonido	Sonido Beep	Estéreo
Compresión	SI	SI
Balanceo de Carga	Balanceo por servidor, se conecta el usuario a uno u otro	Balanceo en base a aplicación. El Servidor autobalancea

Detección automática de dispositivos cliente	Requiere un componente extra	SI
Mapeo de portafolios	SI	SI
Control remoto de sesiones de usuario	SI	SI
Detección de impresoras cliente	SI	SI
Visualización estilo Windows	NO	SI

Tabla 5: Comparativa de protocolos RDP vs ICA

Además según un estudio publicado en internet de referencia [9] en la bibliografía, el ancho de banda consumido por ICA es entre 4 y 20Kb mientras que el ancho de banda consumido por RDP es de 26Kb. Como se puede observar las principales diferencias dan ventaja al uso de ICA respecto del protocolo RDP.

Tecnologías utilizadas en Portales: En base a las consultas realizadas en la documentación de productos que permiten la publicación de aplicaciones en portales de manera remota, se encuentran una serie de técnicas interesantes que se tendrán en cuenta para valorar los productos a la hora de decantarse por uno u otro.

Priority Packet Tagging: Priority Packet Tagging cuya traducción sería la de Marcado de Prioridad de Paquetes es una táctica no demasiado novedosa desarrollada por Citrix (aparecen las primeras versiones de productos que la implementan en el 2001) pero implantada y funcionando con buen resultado desde su aparición y con mejoras en su funcionamiento en las últimas versiones. Consiste en el uso de canales virtuales para enviar la información para cada aplicativo con la posibilidad de asignar mayor o menor prioridad a cada canal, de manera que dan la funcionalidad de Calidad de Servicio (QoS) pudiendo definir aquellos tráficos que se consideran críticos para el negocio y darles prioridad sobre el resto para que tengan un óptimo rendimiento. Las prioridades de cada canal vienen configuradas por defecto pero se pueden modificar en función de las necesidades.

Application Isolation Environment: La traducción de este método es Entorno de Aplicación Aislado. Consiste en definir unas variables de entorno virtuales para la ejecución de aplicaciones de manera que cada aplicación corra de manera aislada. Esto conlleva que la aplicación no afectará ni se verá afectada por librerías ni configuración de registro de otras aplicaciones. La manera de funcionar de esta táctica es engañar a la aplicación para que crea que se ejecuta con una configuración mientras que en realidad está ejecutándose con otras opciones. Se crea una ruta de sistema y unas claves de registro ficticias y sobre este entorno se ejecutan los procesos de dicha aplicación.

Soporte de IP virtual: La posibilidad de uso de direcciones IP (Internet Protocol) virtuales para la gestión de servicios ofertados por el portal de aplicaciones permite que para las aplicaciones sea trasparente que servidor físico está dándoles realmente servicio de manera que minimiza la carga de gestión de los

servicios. Por otro lado permite asignar diferentes servidores que proporcionan el mismo servicio y que tienen una misma IP virtual asignada a un bloque de IPs físicas, con lo que permite el balanceo de carga entre dichos servidores.

Soporte de nuevos dispositivos: Con las últimas versiones de portales se introduce el soporte a nuevos dispositivos, tales como escáneres al soportar el protocolo de comunicación TWAIN o dispositivos PDA (Personal Digital Assistant) de manera que se puede acceder a los mismos teniéndolos conectados en local o en remoto indistintamente.

Workspace control and session reliability: El control del espacio de trabajo y la fiabilidad de sesión permiten a los usuarios conmutar de ordenador terminal sin perder lo que estuvieran ejecutando. Muy útil para garantizar a los usuarios movilidad tanto dentro de la oficina como en el exterior, ya que mantiene en funcionamiento los aplicativos del usuario y reduce considerablemente el tiempo de conexión.

Always-on SSL VPN Access: El acceso VPN siempre disponible a través de SSL (Secure Socket Layer) complementa a las características anteriores al mantener activas las sesiones en caso de caída de la conexión no deseada o imprevista.

Universal Printer Driver: El controlador de impresión universal unifica en un solo driver las funcionalidades de todas las impresoras con la posibilidad de gestionar el ancho de banda consumido para impresión y dando máxima resolución en impresión en blanco y negro y a color. En su versión más reciente (UPD3) da unas prestaciones hasta cuatro veces superiores en cuanto a velocidad de impresión, nuevas funcionalidades como la opción Proximity Printing que permite al usuario imprimir en las impresoras más cercanas a su puesto de trabajo sin necesidad de saber ni el nombre ni la configuración de las mismas.

Soporte al estándar AES (Advanced Encryption Standard): AES es un extendido estándar de encriptación utilizado por entre otros las agencias gubernamentales de los Estados Unidos. Incluir soporte a este y otros sistemas de encriptación permitirá tener comunicaciones seguras en las instalaciones. Hay que tener en cuenta que al fin y al cabo la comunicación entre instalaciones se va a realizar sobre Internet, con lo que a pesar de que sea a través de canales seguros, no está de más añadir una capa de encriptación a la comunicación que se visualiza desde el portal.

8.2.2 Selección de productos

Una vez analizadas cuales son las técnicas disponibles en el mercado, se van a comparar una serie de productos que proporcionen la ejecución de programas de

manera remota y el acceso a ellos a través de un portal. Lo primero que se hace al realizar una comparativa es buscar los productos a comparar. Se busca información de los cuadrantes Gartner asociados, pero en el momento en el que se empieza el proyecto no se dispone de ellos ya que en el mercado se encuentran como prácticamente únicos proveedores de portales las opciones de Citrix System de Citrix y Terminal Server de Windows. Por ello, a continuación se detalla la comparativa realizada sólo entre ambos.

Como primer punto se incluirá la comparativa estudiada en el caso anterior respecto a los protocolos de comunicación ya que Microsoft Terminal Server v2003 utiliza el protocolo RDP y Citrix Presentation Server v4 utiliza el protocolo ICA. Por este motivo, ya de manera previa a realizar la comparativa, Citrix parte con ventaja al utilizar un protocolo con más opciones.

8.2.3 Matriz de comparación

La siguiente matriz de comparación es un extracto del análisis realizado por el fabricante Propalms para comparar su producto con los ya existentes [10]. Se descarta el uso de Propalms por ser un producto de aparición muy reciente y no se quiere asumir el riesgo de realizar una implantación productiva con un producto de tan breve historia.

General Features	Windows 2003 Terminal Services	Citrix Presentation Server 4
Min. Terminal Server version required	n/a	2000
Protocol	RDP	ICA
License Type	Device/User	Concurrent
General Features	**Windows 2003**	**Citrix**
Application Publishing		•
Seamless Windows		•
Load Balancing		Advanced Edition
Web-Based Application Access		•
Content Publishing		•
File Association based application launch		•
Print driver mapping	•	•
Full Universal Printing solution for all client types[1]		
Session Shadowing	•	•
Client Features	**Windows 2003**	**Citrix**
Web-based client install	•	•
Auto client update		•
Client Drive Mapping	•	•
Client Printer Access	•	•
Local / Remote Clipboard Mapping	•	•
Client COM/LPT Port Access	•	•
Audio Redirection	•	•
Dynamic Shortcut creation		•
Application Favourites		
Disconnected session view		
24-bit colour	•	•
Client Platforms	**Windows 2003**	**Citrix**
32-bit Windows	•	•
16-bit Windows	•	•
DOS		•
Macintosh	•	•
Linux/Unix		•
Java		•
Windows CE / PocketPC	•	•
Security Features	**Windows 2003**	**Citrix**
SSL Encryption	•	•
Proxy Support	•	•
SSL Gateway		•
Pass-through authentication		•
Management Features	**Windows 2003**	**Citrix**
Delegated administration	•	•
Single Click Server install		
Client policies	•	•
Fully functional Web Management Console		
Clone Server		
System Monitoring	•	Enterprise Edition
Detailed Usage Reporting		Enterprise Edition
Publish to Organisational Unit		
View Published apps via OU / Group or User		

[1] UniPrint technology provides support for Linux, UNIX and Macintosh as well as Windows clients
[2] Currently in development

Tabla 6: Matriz de comparación entre portales

Además en la siguiente tabla se puede ver el coste de ambos productos en el segundo semestre de 2007:

	Portal	
Coste	Terminal Server	Citrix
Coste de Licenciamiento por usuario	61,53 €	187,99 €
Coste de Mantenimiento por usuario	8,00 €	24,44 €

Tabla 7: Comparativa de coste entre portales

8.2.4 Fortalezas y debilidades de portales

Se destaca a partir de esta matriz los elementos evaluados que presentan diferencias y que puedan ayudar a decantarse:

Fortalezas y debilidades de Microsoft Terminal Services

Fortalezas	Debilidades
El acceso al servidor se realiza desde la consola de Terminal Server que por defecto viene instalada en los sistemas operativos Windows.	La gestión de la plataforma es descentralizada. Si se tienen varios servidores el software se ha de instalar en todos
Para implementar el acceso por terminal server no es necesario configurar nada específico. Mientras el usuario tenga acceso al servidor puede hacer uso de él.	Tiene limitación de 40 usuarios concurrentes trabajando en un servidor.
El coste de licenciamiento es muy asequible	No tiene balanceo de carga, si no hay sesiones disponibles es el usuario el que manualmente ha de conectarse a otro servidor
Una plataforma de terminal services no necesita una especialización elevada. Los servidores han de tener instalado el software que se vaya a querer utilizar pero nada más.	El protocolo de conexión no tiene la posibilidad de limitar el ancho de banda, lo que limita la capacidad de gestión de las líneas de conexión
Dispone de herramientas de monitorización del sistema propias de Windows sin coste añadido.	No dispone de acceso web. Pese a la ventaja de tener el cliente de terminal server instalado, el acceso web está considerado como más seguro que el acceso por cliente.

Tabla 8: Comparativa de fortalezas y debilidades de Terminal Server

Fortalezas y debilidades de Citrix

Fortalezas	Debilidades
La plataforma se realiza de manera centralizada. Citrix dispone de un componente denominado Installation Manager que automáticamente replica las aplicaciones instaladas en un servidor al resto de servidores. Gracias al punto anterior, el coste de mantenimiento es muy bajo. Los cambios de versión de software son rápidos y eficientes. Permite hasta 120 usuarios concurrentes por servidor. Además añade balanceo de carga por lo que si hay varios servidores asociados redirige las conexiones a uno u otro en función de la carga y proporcionando así de una escalabilidad trasparente para el usuario. Utiliza un protocolo de conexión desarrollado por el fabricante que permite limitar y monitorizar el uso de las conexiones. El acceso se realiza vía web, lo que permite que los usuarios locales de los ordenadores cliente no necesiten tener ningún permiso especial.	La opción para monitorizar el sistema implica un coste adicional de licencias. Para utilizar el acceso web necesita un plug-in. Se descarga automáticamente en la primera conexión y no es necesario realizar ninguna acción añadida pero no viene por defecto instalado en el sistema. El coste de licenciamiento es muy elevado, aproximadamente el triple que Terminal Services La instalación inicial de la plataforma requiere de personal especializado.

Tabla 9: Análisis de fortalezas y debilidades de Citrix

8.3 Comparativa de Antivirus

Basándose en los requisitos estudiados en el apartado 2.2.3 en el que se evaluaron los diferentes elementos que debía cumplir el antivirus elegido, se ha procedido a realizar una comparativa entre los principales fabricantes de antivirus.

8.3.1 State of the art para Antivirus

En los tiempos que corren, en un mundo cada vez más globalizado, los avances en el mundo de la tecnología y en especial en la seguridad tecnológica van a un ritmo espectacular. El desarrollo de nuevos virus y nuevas tácticas de ataque por parte de hackers y demás personas con propósitos maliciosos así como la evolución y aparición de nuevos sistemas operativos y aplicaciones implica la apertura de nuevas posibilidades de ataque lo que implica esfuerzos por parte de las empresas de seguridad para desarrollar productos de antivirus completos y que cubran todas posibilidades de ataque que vayan surgiendo. Por ello además de hablar de últimas tendencias en antivirus es necesario hablar de últimas tendencias en amenazas y virus.

Cabe reseñar en este punto la definición de malware que no es más que todo aquel software diseñado con intenciones dañinas o maliciosas para obtener algún beneficio y/o causar daño en los ordenadores que se ven infectados. Los virus son considerados malware pero no son ni de lejos el único tipo de malware. Además de los clásicos virus, gusanos y troyanos, están apareciendo nuevas amenazas que pueden afectar al sistema:

Droppers: Es un programa malware auxiliar que permite la instalación del programa que realmente es perjudicial. Son más difíciles de detectar por los antivirus ya que ellos mismos en sí no realizan cambios sobre archivos ni otra acción destructiva.

Downloaders: De manera similar a los droppers, estos programas son un tipo de malware auxiliar que sirve para descargar desde internet y posteriormente instalar el programa que luego será utilizado para dañar al sistema.

Rootkit y stealthkit: Son programas que lo que buscan es permanecer ocultos en el sistema para no ser detectados y como principales elementos perjudiciales son una disminución del rendimiento del ordenador, la apertura de puertos, ocultando esta apertura al sistema, para permitir el acceso remoto al ordenador o cualquier otra acción que requiera ser ocultada para permitir la ejecución de otro programa malicioso. La diferencia entre ambos términos es básicamente que los programas stealthkit son una evolución de los rootkit. También se denominan rootkit de nueva generación.

Adware: Es un tipo de malware que una vez se instala en un ordenador muestra al usuario diferentes anuncios en forma de ventanas emergentes que se van abriendo sin que el usuario lo solicite.

Spyware: Son programas espía que buscan obtener información confidencial de los ordenadores donde son instalados. Puede ser información acerca de contraseñas, cuentas bancarias, navegación que realiza el usuario, etc. Además pueden abrir backdoors o puertas de atrás, es decir, dejan abierta, de alguna manera (a través de puertos tcp por ejemplo) la entrada al sistema para el desarrollador del software.

Keyloggers: Son un tipo de programa muy concreto que se utiliza para registrar claves de acceso varias. En combinación con los programas spyware permiten al desarrollador de malware obtener este tipo de información confidencial.

Targeted Threats: En este caso son programas destinados a un conjunto reducido de víctimas, como una empresa o sector en concreto, lo que provoca que tarden más en ser detectados e incluidos en las listas negras de los fabricantes de antivirus, puesto que la afectación es a un número menor de usuarios que las amenazas convencionales. De manera similar a los spyware suelen ser programas utilizados para obtener información confidencial. Se suelen enviar a través de e-mail, ataque de puertos, ataques Zero-day o mensajes de pishing (explicado a continuación).

Pishing: El pishing consiste en la suplantación de identidad, es decir, enviar correos electrónicos o desarrollar páginas web iguales a las de entidades bancarias o cualquier otro sitio web del que se quieran obtener contraseñas para poder acceder de manera fraudulenta, de manera que se engaña al usuario que piensa que se está autentificando contra el servicio que desea y en realidad se está autentificando en un sitio diferente que guardará la clave introducida para acceder al sitio real. Las técnicas de pishing más habituales son las de modificar los links a páginas web de manera que parezca que accedes a una página cuando en realidad accedes a otra, la falsificación de sitios web de manera que a pesar de entrar a una página diferente el usuario crea que está accediendo a la que él cree (utilizando imágenes en lugar de texto que sobreponen al texto en sí, etc.) o la táctica MITM (Man In The Middle) en la que una persona interactúa entre la página fraudulenta y la real, reproduciendo los pasos del usuario y modificando por ejemplo la cuenta bancaria de destino de una transferencia.

Virus Polimórficos: Son un tipo de virus más difíciles de detectar al ser variables en la forma final. Son virus encriptados que se desencriptan, atacan y vuelven a encriptarse. En cada contaminación que realizan se encriptan de manera diferente con lo que no hay un patrón de bytes que los pueda identificar.

Teniendo en cuenta todas estas amenazas de la red se necesitará buscar la manera de estar protegidos ante todas ellas. Es necesario recalcar que debido a que en este proyecto se va a seleccionar tanto antivirus como antispam como firewall, el requisito principal es que entre todo el sistema de seguridad se esté

cubierto ante todas las amenazas, si bien se tiene la libertad de escoger en qué punto o puntos en el caso de querer redundancia de funciones se va a definir la protección ante cada una de ellas.

Como soluciones a todas estas amenazas de la red hay diferentes tácticas de actuación y evoluciones de los productos antivirus que resultan interesantes para tener en cuenta en la posterior evaluación que se realiza de los productos antivirus del mercado.

Análisis heurístico: El concepto de heurística en sí es el auto aprendizaje o descubrimiento por uno mismo. Aplicado a la programación antivirus, las tácticas de análisis heurístico son aquellas que no se basan en la detección de un virus o malware en concreto si no que a través de reglas deciden lo que puede ser un virus y lo que no. Esto permite que el sistema tenga cada vez mayor conocimiento de los diferentes virus y pueda estar preparado incluso para aquellos que ni siquiera se han desarrollado, siempre y cuando sigan alguna de las reglas de comportamiento definidas. Según el comportamiento del programa analizado, se le asigna una puntuación y cuando ésta supera un determinado umbral se marca como potencialmente peligroso y se introduce en área de cuarentena. Una evolución del análisis heurístico es el análisis heurístico negativo, consiste en aplicar técnicas de auto aprendizaje del modelo heurístico basadas en reglas y en las opciones que selecciona el usuario en aquellos aplicativos que se permite al usuario escoger si algún programa es virus o no y aplicarlas para que el programa sea capaz de detectar cuando se trata de un falso positivo y lo trate como tal.

SONAR (Symantec Online Network for Advanced Response): Es un protocolo propio de Symantec que utiliza tácticas heurísticas para determinar si un software puede ser malicioso o no en base a analizar diferentes atributos de los programas que están en ejecución. Entre ellos está el hecho de si una instalación deja accesos directos en el escritorio o entradas en el apartado de instalar/desinstalar programas. Se considera que si un programa tiene un comportamiento standard de instalación es porque seguramente sea un programa instalado por el usuario con su conocimiento.

Detección eficiente de variaciones de virus: Es una optimización del análisis heurístico tradicional que consiste en no recorrer los archivos al completo si no en base a la localización indicada en el fichero de reglas se dirige al punto en concreto del archivo para comprobar si tiene algún tipo de código que cumpla la regla heurística.

Generic Decryption Engine: Los sistemas de desencriptación genéricos son especialmente útiles para la detección de virus polimórficos. Estos sistemas son capaces de detectar el código de encriptación del virus, desencriptarlo y evaluar

si lo que hay dentro del fichero encriptado puede ser un virus o no, aplicando las técnicas que utilice el sistema antivirus para el resto de ficheros.

Personal firewall: En el viaje a la integración entre antivirus, antispam, antispyware, en definitiva en la unión de todos estos productos en uno solo, hay alguna característica más interesante que otras para que se aplique en los ordenadores cliente. Personal Firewall es la opción de trasladar o complementar las funciones del firewall de la red al ordenador cliente de manera que el usuario pueda filtrar algún tipo de acceso extra a su ordenador o bien estar protegido ante caída del firewall principal.

True Type File Filtering: Es una táctica de filtrado destinada al correo electrónico. Consiste en evaluar el fichero analizando el tipo de fichero que es sin tener en cuenta la extensión que tenga asociada en el nombre del mismo.

8.3.2 Selección de productos

A la hora de decidir qué antivirus entrarán en el análisis se partirá del cuadrante Gartner para Antivirus. Para ello se va a la última versión del cuadrante de Enterprise Antivirus, publicado a finales del 2006 (el análisis se realiza a finales del 2007 y este es el último publicado) y de allí se seleccionan los fabricantes mejor posicionados.

Los criterios para ser incluidos en el análisis Gartner en el caso de los antivirus son los siguientes:

- El fabricante ha de ofrecer Antivirus cliente, Antivirus para servidor de ficheros, Antivirus interno para los servidores de e-mail y antivirus para gateways.
- El fabricante ha de ser el desarrollador de al menos un motor de antivirus. Aquellos vendedores que no sean los desarrolladores y compren el motor a terceros quedan excluidos de este análisis.
- Los productos han de soportar entornos de más de 2500 usuarios con posibilidad de dispersión geográfica.
- Los fabricantes han de tener al menos 2000 clientes con el producto instalado y funcionando.
- Los fabricantes han de tener una facturación mínima de 20 millones de dólares.
- El producto tiene que haber estado disponible al menos durante 12 meses en el momento del análisis.

Con estos requisitos Gartner selecciona a los fabricantes de antivirus que cumplan con todos ellos y los clasifica en función de los criterios ya especificados en el apartado 4.1. Como se comentó en este apartado, hay toda una serie de criterios que permiten evaluar los productos en función de su capacidad de ejecución y la completitud de visión. Basándose en el peso de cada criterio y evaluándolos en función de los mismos, Gartner obtiene el cuadrante resultante que se muestran a continuación [11].

Como se puede observar los tres fabricantes calificados como líderes son Trend Micro, Symatec y McAfee, que son los que se incluirán en el análisis.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	Standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	High
Market Responsiveness and Track Record	High
Marketing Execution	Standard
Customer Experience	High
Operations	Low

Source: Gartner (August 2006)

Tabla 10: Capacidad de ejecución para Antivirus

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Low
Innovation	Standard
Geographic Strategy	Standard

Source: Gartner (August 2006)

Tabla 11: Visión de mercado de Antivirus

MAGIC QUADRANT
Figure 1. Magic Quadrant for Enterprise Antivirus, 2006

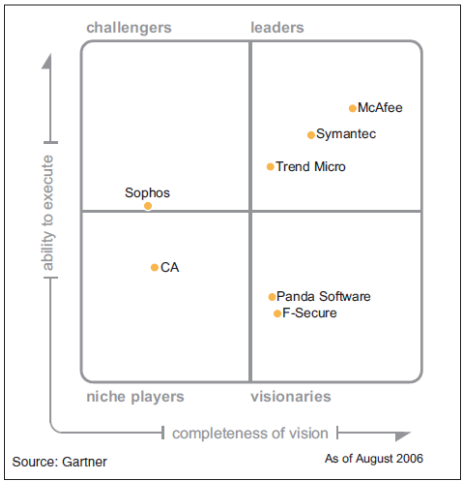

Ilustración 5: Cuadrante Gartner para Antivirus

Por otro lado, por razones históricas, ya que el cliente ya dispone de licencias para estos antivirus, se decide incluir en la comparativa dos productos conocidos por la empresa como son NOD-32 y Kaspersky.

Una vez decididos que fabricantes se van a evaluar, se busca en el mercado la última versión disponible de cada uno, con lo que los productos que se evalúan son:

- NOD32 Antivirus v2.7
- Norton Security 2007
- Trend Micro PC-Cillin 2007
- Kaspersky 2007
- McAfee Enterprise V7

8.3.3 Matriz de comparación

Para poder analizar de manera más sencilla y gráfica los antivirus que entran en el análisis, se realiza una matriz de comparación que permita ver con claridad cuáles son los puntos fuertes de cada uno.

Requisitos Comunes\Antivirus	NOD32 Antivirus v2.7	Norton Security 2007	McAfee enterprise V7	Trend Micro PC-Cillin 2007	Kaspersky 2007
Compatibilidad	NO	SI	SI	SI	SI
Interoperabilidad	SI	NO	SI	NO	SI
Unicidad	SI	SI	SI	SI	SI
Multifunción en contingencia	NO	NO	SI	NO	SI
Escalabilidad	SI	SI	SI	SI	SI
Soporte del producto					
On site	NO	NO	SI	NO	No
Email. Teléfono, web, parches, firmware	Si	SI	SI	SI	SI
Tiempo de resolución de incidencias	No lo cubre	8 horas	4 horas	8 horas	No lo cubre
Tiempo máximo de sustitución	N/A	N/A	N/A	N/A	N/A
Tiempo de soporte Post-Venta	1 año	1 año	1 año	1 año	1 año
Coste					
Coste del producto	20€ x unidad al año	28 € x unidad al año	22 € x unidad al año	26 € x unidad al año	20 € x unidad al año
Coste del mantenimiento anual	2 € x unidad al año	2,8€ x unidad al año	4 € x unidad al año	2,6 € x unidad al año	2 € x unidad al año
Requisitos Especificos para Antivirus					
Gestión centralizada por Consola	NO	NO	SI	SI	NO
Estándares de seguridad	SI	SI	SI	SI	SI
Frecuencia de actualización	4 horas	4 horas	4 horas	4 horas	4 horas
Delegación administración a nivel local	NO	NO	SI	NO	NO
Actualización Manual/Automática	SI/SI	SI/SI	SI/SI	SI/SI	SI/SI
Rendimiento					
Resultado de la exploración de archivos multimedia y documentos en Windows Server 2003	26,7 MB/s	20,5 MB/s	27 MB/s	22 MB/s	66,4 MB/s
Tiempo de acceso a los archivos	0,08 s	0,04 s	0,02 s	0,08 s	0,94 s
Recursos consumidos	120,63 MB	186,3 MB	117,93 MB	196,12 Mb	156,12 MB
Tiempo de inicio de aplicación	2,94 segundos	3,1 segundos	1,74 segundos	4,1 segundos	2,17 segundos
Tiempo de inicio del sistema	157 segundos	229 segundos	137 segundos	212 segundos	168 segundos
Opciones de Escaneo					
Escaneo al inicio	SI	SI	SI	SI	SI
Escaneo bajo demanda	SI	SI	SI	SI	SI
Escaneo programado	SI	SI	SI	SI	SI
Escaneo de archivos comprimidos	NO	NO	SI	NO	SI
Limpieza automática	SI	SI	SI	SI	SI
Cuarentena de archivos infectados	SI	SI	SI	SI	SI
Protección de correo	NO	NO	SI	NO	SI
Protección de mensajería instantanea	NO	NO	SI	NO	NO
Protección de P2P	NO	NO	NO	NO	NO
Protección de registro al inicio de windows	NO	NO	SI	NO	NO
Protección Exhuastiva					
Detección de virus In-the-Wild (activas en el mundo real) , sin generar ni un falso positivo	53	47	37	16	43
Virus In-the-Wild detectados					
- En Acceso	26	29	64	70	34
- Bajo Demanda	1	2	71	68	16
Protección en tiempo real contra 16 amenazas zero-day (Virustotal.com)	57%	14%	62%	29%	21%
Evaluación Proactiva	68%	26%	80%	27%	24%

Tabla 12: Matriz de comparación para Antivirus

Esta matriz está basada en los requisitos analizados en el apartado 2.2.3. Hay toda una serie de puntos que deben aclararse para poder tener una referencia de cómo han sido obtenidos. Por un lado el coste evaluado, son precios ofertados al cliente entre septiembre y diciembre de 2007.

Por otro lado se analizan las métricas de rendimiento que se utilizan para valorar los productos. Téngase en cuenta que se instalan y evalúan todos los productos para realizar una verificación del rendimiento ofrecido teniendo en cuenta el hardware de los ordenadores cliente y la maqueta software que se instala para

todos ellos. De esa manera además se verifican problemas de incompatibilidad con cualquiera de los productos instalados en los ordenadores. El apartado de Protección Exhaustiva está extraído de la publicación Virus Butlletin.

A continuación se observa una tabla en la que se definen los criterios de medición de cada una de las métricas obtenidas.

Rendimiento	
Resultado de la exploración de archivos multimedia y documentos en Windows Server 2003	Ratio entre el tamaño ocupado de disco y tiempo que tarda en escanearlo. Se obtiene tomando la ocupación de disco de windows y el tiempo de análisis que todos los antivirus proporcionan
Tiempo de acceso a los archivos	Media de tiempo en acceder a los archivos que entran en nuestra red para escanearlos. Se obtiene utilizando un sniffer antes del antivirus y otro después y restando los tiempos obtenidos. Se hace una media de 10 archivos
Recursos consumidos	La memoria consumida se evalúa con una utilidad denominada ProcDump que nos permite saber la memoria máxima y media ocupada por un proceso
Tiempo de inicio de aplicación	Es el tiempo que tarda en arrancar el cliente de antivirus. Se obtiene con la utilidad ProcDump
Tiempo de inicio del sistema	Es el tiempo transcurrido entre que se le da a botón de inicio del ordenador y se considera totalmente arrancado. Para medirlo se utiliza una utilidad de descarga gratuita denominada Boot Tracer

Tabla 13: Método de cálculo de indicadores

8.3.4 Análisis individualizado

Partiendo de la matriz de comparación del apartado anterior se pasa a detallar las fortalezas y debilidades de cada uno de los productos que entran en el análisis.

NOD 32 Antivirus 2.7

NOD 32 es un programa de antivirus desarrollado por la empresa ESET, de origen eslovaco. Es un producto robusto compuesto de elementos modularizados, en el que cada uno de los módulos cumple con unas funciones determinadas. La interfaz de acceso es una interfaz de comandos lo que hace que no sea muy amigable de cara a usuario.

Las principales fortalezas que presenta este producto son un rendimiento bastante aceptable, un coste unitario y de mantenimiento bajo, cumple con todas las funcionalidades mínimas de escaneo y un ratio de actualización y detección de virus zero-day (aquellos que aparecen el mismo día) muy bueno.

Las debilidades que presenta dicho antivirus son problemas de compatibilidad con la plataforma de firewalls que se pretende implementar, soporte deficiente en algunos de los aspectos que se evalúan y no dispone de algunas de las funcionalidades no requeridas pero deseadas para el software de antivirus.

En un análisis más pormenorizado de las características del producto se puede ver el detalle de las conclusiones mencionadas anteriormente:

- Rendimiento: El rendimiento observado en las pruebas realizadas es bastante bueno, sin ser el mejor de los productos probados ni tener los mejores indicadores para ninguno de los aspectos, en media da un resultado correcto:

    - Ratio de exploración de documentos: En base al tamaño ocupado en el disco duro y el tiempo de exploración empleado, el ratio resultante es de 26,7Mb/s.
    - Tiempo de acceso a los archivos: Utilizando herramientas que permiten medir el tiempo de acceso a los archivos, la media resultante es de 0,08 segundos.
    - Memoria RAM utilizada: Uno de los límites básicos en un ordenador es la memoria RAM. Por ello es importante que saber cuál es el nivel de uso de RAM por parte del proceso. El nivel medio de memoria ocupada por este producto es de 120,63Mb.
    - Tiempo de inicio de aplicación: Es el tiempo que tarda en arrancar el programa antivirus en el ordenador. En este caso 2,94 segundos.
    - Tiempo de inicio del PC: Con este antivirus instalado el ordenador tarda en arrancar 157 segundos.

- Coste: Para evaluar el coste del antivirus se utilizará el coste unitario, es decir, el coste de licencia para instalar el programa para cada usuario nominal, y el coste de mantenimiento unitario anual, es decir, el coste de renovar las licencias cada año.

    - Coste unitario: El coste de este software es de 20 euros por usuario
    - Coste de mantenimiento: El coste en este caso es de 2 euros por año.

- Funcionalidades básicas de escaneo: Este antivirus cumple con las funcionalidades básicas que se esperan de un antivirus, como son el escaneo al inicio, bajo demanda o programado, limpieza automática y cuarentena para archivos infectados o la posibilidad de actualización manual o automática.

- Protección exhaustiva:
    - Ratio de detección zeroday: se destaca este ratio porque en comparación con los demás está bastante por encima de la media. Es de un 57%. Este ratio es ofrecido por el fabricante.

- Compatibilidad: los fabricantes de firewalls detallan que antivirus son compatibles para poder integrar la consola de administración de ambos

productos y con la plataforma escogida de firewalls este producto no tiene compatibilidad.

- Soporte: Este fabricante no dispone de soporte on-site en todas las delegaciones a cubrir y por otro lado tampoco ofrece un tiempo máximo de resolución de incidencias.
- Funcionalidades faltantes: El producto no dispone entre otras funcionalidades de la posibilidad de gestión centralizada por consola, delegación de administración a nivel local ni multifunción para poder actuar como otro elemento en caso de contingencia.

Norton Security 2007

Norton Security 2007 es un producto desarrollado por la empresa americana de software Symantec Corporation. La versión 2007 (versión técnica 13.0) tiene una interfaz de usuario bastante amigable y el software se proporciona en un único interfaz de acceso.

En cuanto a la relación de fortalezas y debilidades, el análisis realizado aporta que no destaca en ninguno de los ámbitos. En cuanto a rendimiento es un producto bastante deficiente salvo en alguno de los indicadores, en referencia a funcionalidades, aporta las funcionalidades básicas pero tampoco ofrece funcionalidades extra, en referencia al coste es el más caro de los analizados y desde el punto de vista de soporte si ofrece un soporte adecuado pero tampoco ofrece soporte on-site en todos los países que se necesita. Por si fuera poco también presenta algún problema de interoperabilidad.

Detalle de elementos evaluados:

- Rendimiento:
  - Ratio de exploración de documentos: En este caso, y con el mismo criterio de obtención del ratio, el ratio resultante es de 20,5Mb/s.
  - Tiempo de acceso a los archivos: Este producto tarda una media en acceder a los archivos a explorar de 0,04 segundos. Sin ser el mejor dato obtenido, es uno de los pocos puntos en los que destaca respecto a la media del resto de antivirus.
  - Memoria RAM utilizada: El nivel medio de memoria ocupada por este producto en tiempo de escaneo es de 186,3Mb. Como se puede observar superior al anterior.
  - Tiempo de inicio de aplicación: Este producto tarda en abrir la interfaz de usuario 3,1 segundos.
  - Tiempo de inicio del PC: Con este antivirus instalado el ordenador el tiempo de inicio se retrasa hasta los 229 segundos.
- Coste: Este producto tiene un coste unitario de 28 euros y un coste de mantenimiento de 2,8 euros.

- Funcionalidades extra: al igual que en el caso del NOD 32, no dispone entre otras funcionalidades de la posibilidad de gestión centralizada por consola, delegación de administración a nivel local ni multifunción para poder actuar como otro elemento en caso de contingencia
- Soporte: En este caso, Norton si que ofrece un nivel de respuesta ante incidencias de 8 horas. Sin embargo, uno de los puntos críticos que es el de soporte on-site no lo ofrece.
- Interoperabilidad: El producto no está soportado por el servidor de correo Microsoft Exchange que es el utilizado.

Trend Micro PC-Cillin 2007

Trend Micro PC-Cillin 2007 (versión técnica v15) es un software desarrollado por la empresa americana Trend Micro. Es una plataforma que integra todos los componentes de antivirus en una única consola de usuario. Aunque a principios de 2007 sale en los análisis con baja puntuación en detección de virus según diferentes estudios, durante el 2007 evoluciona posicionándose como un software a tener en cuenta para la evaluación.

En la comparativa para detectar sus fortalezas y debilidades se observa a nivel global que a pesar de tener alguna característica que mejora respecto al anterior análisis de Norton, sigue sin ser de los mejores productos en su categoría.

Los elementos a destacar en el análisis es un rendimiento bajo, coste por encima de la media, soporte adecuado pero sin ser on-site y alguna característica de las deseadas que en el caso anterior no estaba disponible como la gestión centralizada por consola. Como en el caso anterior no está certificado para funcionar con Exchange como servidor de correo.

En el detalle de dicho análisis se encuentra:

- Rendimiento:
  - Ratio de exploración de documentos: el ratio de exploración de documentos para este producto es de 22Mb/s.
  - Tiempo de acceso a los archivos: El tiempo de acceso a archivos para este producto es en media de 0,08 segundos.
  - Memoria RAM utilizada: El nivel medio de memoria ocupada por este producto en tiempo de escaneo es de 196,12Mb. De todos los antivirus examinados este es el que ofrece un peor dato en este aspecto.
  - Tiempo de inicio de aplicación: Este producto tarda en abrir la interfaz de usuario 4,1 segundos.

  - Tiempo de inicio del PC: Una vez se procede a la instalación del producto y se mide el tiempo de arranque, el resultado es de 212 segundos.
- Coste: En este caso el coste unitario es de 26 euros y como en el resto de casos, el de mantenimiento es de un 10%, 2,6 euros al año.
- Funcionalidades extra: En este caso dispone de gestión centralizada por consola que es uno de los requisitos extra que interesa. El resto de puntos los comparte con los productos anteriores, no permite la multifunción para sustituir a elementos como el firewall en caso de caída de éste ni de la posibilidad de delegación para una administración local.
- Soporte: De manera similar al producto de Norton, dispone de Tiempo máximo de respuesta ante incidencias, pero tampoco dispone de soporte en todos los países que interesan.
- Interoperabilidad: En este caso tampoco está certificado por Exchange para funcionar como antivirus de correo.

Kaspersky 2007

Kaspersky 2007 es un producto desarrollado por Kaspersky Lab, una empresa rusa productora de diferentes tipos de software relacionados con seguridad. Es un software que a través de una interfaz de usuario permite acceder a toda la funcionalidad, al igual que los dos anteriores.

El análisis de debilidades y fortalezas revela una serie de puntos que hacen que resulte más interesante que los anteriores. En cuanto a compatibilidad e interoperabilidad funciona correctamente con todos los elementos del sistema. En lo referente al coste también es de los más económicos. Algunos de los puntos de rendimiento analizados son los mejores de todos los evaluados y además ofrece algunas funcionalidades de escaneo que el resto de los programas evaluados no ofrece o los ofrece con un coste añadido. Una de sus debilidades es el soporte, que no ofrece un tiempo mínimo de resolución de incidencias ni tiene soporte on-site.

En el análisis detallado se observa:

- Rendimiento:
  - Ratio de exploración de documentos: De todos los productos analizados es el que ofrece un mejor ratio de exploración 66,4Mb/s.
  - Tiempo de acceso a los archivos: Este punto sin embargo devuelve el peor dato de acceso: 0,94 segundos.

  - Memoria RAM utilizada: En este parámetro se observa que el resultado que ofrece es un punto medio entre los demás productos, 156,12Mb de uso de memoria.
  - Tiempo de inicio de aplicación: En este apartado el producto también arroja un resultado bastante satisfactorio, 2,17 segundos.
  - Tiempo de inicio del PC: En el arranque del sistema con el antivirus instalado el resultado es de 168 segundos, con lo que el dato está ligeramente por debajo de la media, pero tampoco es el mejor de los datos obtenidos.
- Coste: En este caso el coste unitario es de 20 euros y el de mantenimiento es de 2 euros al año.
- Funcionalidades extra: No dispone de consola de gestión centralizada ni permite la multifunción para sustituir a elementos como el firewall en caso de caída de éste ni de la posibilidad de delegación para una administración local. Sin embargo, si dispone de la posibilidad de escaneo de archivos comprimidos y de escaneo de correo electrónico.
- Soporte: En este caso el soporte ofrecido no ofrece un tiempo máximo de resolución de incidencias, algo crítico en una implementación como la que se busca. Tampoco dispone de soporte on-site.

McAfee Enterprise V7

McAfee Enterprise V7 es un producto de la empresa norteamericana McAfee Network Associates. Es una consola de administración que integra todos los componentes del antivirus en una única interfaz.

Una vez se realiza el análisis de fortalezas y debilidades, se observa entre otras cosas que ofrece un mayor número de funcionalidades que el resto de competidores, que el soporte cumple con todas los requisitos, incluyendo el soporte on-site y que el rendimiento es el mejor en casi todos los ratios. En referencia al coste es intermedio, ligeramente por debajo de la media.

En un mayor detalle de los parámetros a comparar se observa:

- Rendimiento:
  - Ratio de exploración de documentos: El ratio de exploración de documentos es el segundo para este producto, sin embargo muy alejado del primero: 27Mb/s.
  - Tiempo de acceso a los archivos: En este apartado este producto devuelve el mejor resultado, 0,02 segundos.
  - Memoria RAM utilizada: También en este apartado el resultado es el mejor de todos los productos analizados: 117,93Mb.
  - Tiempo de inicio de aplicación: Este producto es el que menos tarda en arrancar la consola de administración, 1,74 segundos.

  - Tiempo de inicio del PC: En referencia al tiempo de arranque del PC con este producto instalado, también es el que ofrece un mejor dato, 137 segundos.
- Coste: El coste unitario es de 22 euros por usuario. El coste de mantenimiento anual de 2,2 euros.
- Funcionalidades extra: Este producto ofrece toda una serie de funcionalidades extra, como serían la gestión centralizada por consola, la posibilidad de delegar la administración a un nivel local, servicios multifunción que pueden ser activados en caso de contingencia (firewall o antispam), protección del correo electrónico, protección del servicio de mensajería instantánea y el escaneo de archivos comprimidos.
- Soporte: Se dispone en este caso de soporte on-site y un tiempo máximo de respuesta ante incidencias de 4 horas, elementos diferenciadores respecto al resto de productos.
- Compatibilidad e interoperabilidad: Es compatible con todos los productos de la plataforma.
- Protección exhaustiva: En el apartado de detección de virus recién salidos o zeroday también ofrece los mejores números.

8.4 Comparativa de Anti-Spam

En este punto se va a proceder a analizar en base a los criterios establecidos en el apartado 2.2.4 diferentes productos que ofrecen Antispam para determinar cuál es la mejor opción.

Para realizar esta comparativa, primero, como en los otros apartados se va a evaluar lo que hay en el mercado disponible, en cuanto a que técnicas hay en relación al componente antispam.

8.4.1 State of the art para Antispam

Las técnicas antispam se pueden agrupar por niveles en función de la capa de actuación sobre la que actúen. A continuación se muestra un diagrama de funcionamiento de una solución antispam:

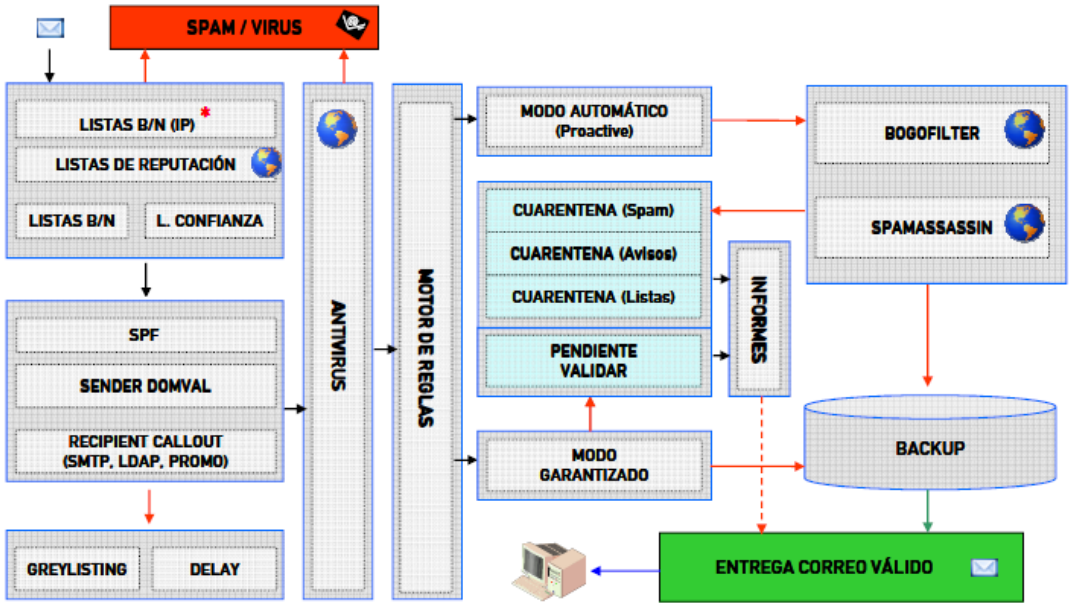

Ilustración 6: Método de análisis antispam

Se dividen básicamente en técnicas de protección aplicadas al nivel de conexión, técnicas de protección aplicadas al nivel de protocolo de comunicaciones y técnicas de protección aplicadas en el nivel de aplicación.

Las primeras actúan desde el nivel más primario de filtrado de IP's, listas negras, etc. Un ejemplo de táctica de este nivel sería el Realtime Black Lists. Tanto las listas negras como las listas blancas de dominios origen ya existían como tal. Se trata básicamente de recopilaciones de dominios desde los que se prohíbe enviar e-mails (listas negras) como de recopilaciones de dominios desde los que se asegura que los correos no serán Spam (listas blancas). La novedad es que estas listas se actualizan dinámicamente, de manera que son capaces de detectar Spam aunque el remitente cambie de dirección IP o utilice a un mail relay (transmisor de correo) externo para remitir sus correos spam.

Otro ejemplo sería la funcionalidad IP Connection Filtering, que consiste en el filtrado de direcciones IP. El problema de este protocolo es que es de mantenimiento manual lo que implica un bajo nivel de actualización.

Actuando desde el filtrado a nivel de protocolo se pueden encontrar otras técnicas como por ejemplo:

Advanced Reputation Management (ARM): Este protocolo desarrollado por sonicwall consiste en una técnica en la que el servidor antispam aprende a determinar que mensajes son fiables y cuáles no en base a diferentes factores, como la estructura del mensaje, el contenido, las direcciones URL incluidas, los ficheros adjuntos, etc.

Sender ID Framework (SIDF): Este protocolo, diseñado por Microsoft y adoptado como standard por parte de la IETF (Internet Engineering Task Force) con el estándar de referencia RFC-4406 detallado en la referencia [12], consiste en asegurar que el remitente es quien dice ser y no es una dirección falsificada. Para ello el dispositivo antispam pregunta al dispositivo DNS si la dirección que le envía el correo corresponde con la que el servidor DNS tiene almacenada para ese dominio.

En la imagen de la derecha se puede observar un ejemplo de funcionamiento del protocolo SIDF. Cuando el remitente envía un mensaje, un servidor de recepción (Inbound) comprueba el identificador del remitente, verifica a través de un DNS que el dominio es el correcto y dependiendo de si lo es o no lo envía al destinatario o lo deja en cuarentena

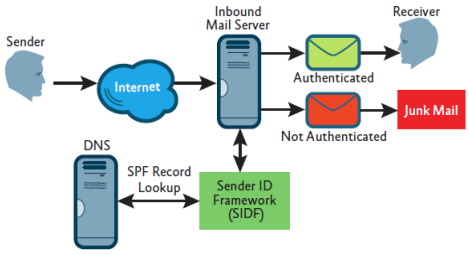

Figure 1 Checking SPF records for incoming messages

Ilustración 7: Funcionamiento de SIDF

El protocolo SIDF se basa en el estándar abierto SPF (Sender Policy Framework) publicado en el documento de referencia RFC-4408, disponible en la referencia [13].

Como técnicas de actuación a nivel de aplicación se encuentran entre otras:

Signature Networks: Es una técnica que consiste en detectar a un determinado mensaje de spam a través de un patrón que lo identifique. El problema que presenta esta táctica es que hasta que no recibe el mensaje unas cuantas veces no puede establecer el patrón, con lo que las primeras veces puede pasar por un mensaje deseado.

Bayesian analysis: El análisis bayesiano consiste en realizar un análisis de probabilidades de Spam en base a palabras que contenga el mensaje. El problema que presenta este tipo de filtrados es que la gente que quiere enviar correo spam evoluciona sus mensajes y para las palabras clave puede modificar la escritura de las mismas para que pasen sin ser detectadas, por ejemplo sustituyendo letras por números (o por 0) o separando con espacios las palabras susceptibles de ser identificadas, con lo que requiere un alto nivel de actualización. Los filtros bayesianos más avanzados son capaces de identificar mensajes de spam por proximidad de palabras, analizar el contenido de los mensajes HTML, etc.

Intelligent Message Filter (IMF): El filtrado de mensaje inteligente es una táctica desarrollada por Microsoft que permite reconocer mensajes Spam utilizando protocolos heurísticos basados en millones de ejemplos que contiene su base de datos. Este tipo de programas van instalados en los gateways de manera que realizan el filtrado en el primer punto de entrada de la red tras el firewall,

minimizando el ancho de banda consumido por los mensajes spam. El método de funcionamiento es el siguiente, cuando llega un mensaje externo a la red, el sistema IMF evalúa el contenido del mismo en base a las muestras de correos de las que dispone y le asigna un ratio en función de la probabilidad de que el mensaje sea Spam. Este ratio es almacenado en una propiedad de los mensajes llamada Spam Confidence Level (SCL). Los administradores del sistema deciden qué ratios entrarán y cuáles no. En la figura se puede observar el punto de filtrado donde se ubica este tipo de protocolos.

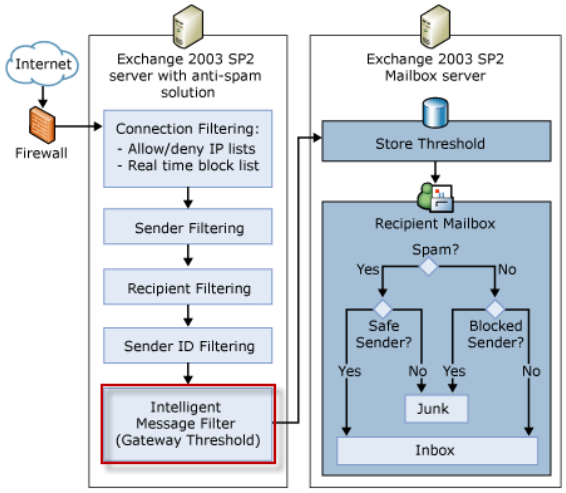

Ilustración 8: Filtrado de Spam IMF

También existen protocolos que utilizan los protocolos de las diferentes capas de manera conjunta y que actúan de manera global:

Artificial Intelligence (o Machine Learning): la inteligencia artificial aplicada al mundo antispam consiste en una serie de algoritmos que se utilizan para analizar los e-mails que llegan y que tiene en cuenta varios factores para determinar si un mail es spam o no. Este protocolo analiza la fecha-hora a la que se envían los mensajes, la dirección de correo origen, si hay mails previos entre remitente y destinatario o si el patrón del mail lo ha recibido antes (táctica de Signature networks). Además los correos que marca como spam los guarda en una bandeja de cuarentena y si el administrador los marca como buenos, toma nota del patrón y remitente para no marcarlos como spam en futuras ocasiones.

Dentro de los protocolos de inteligencia artificial se encuentra Advanced Content Management, un protocolo que utiliza análisis Bayesiano, análisis de imagen y analiza el cuerpo y el formato del correo para determinar si es posible que sea Spam o no. Este protocolo ha sido desarrollado por Sonicwall y utiliza el protocolo Advanced Reputation Management especificado anteriormente para realizar las funciones de análisis en la capa de protocolo.

De manera independiente al nivel de actuación existe una táctica que puede ir aplicada sobre todas las demás, denominada Internet Based Spam Filters. Los filtros basados en internet son compatibles con las técnicas explicadas previamente, consisten en que los repositorios de palabras prohibidas o patrones se gestionan desde un servidor en internet y los dispositivos ubicados en las sedes corporativas se actualizan sincronizando las listas con las del repositorio central.

Varias de estas técnicas antispam se pueden combinar para conseguir un filtrado eficaz que minimice los falsos positivos (correo marcado como Spam que no lo es) y falsos negativos (correo marcado como bueno pero es Spam), como se puede observar en el siguiente gráfico en el que se muestra todas las capas de filtrado del servidor Exchange de Microsoft. Una vez se analizan los protocolos de los servidores se puede ver que todos siguen la misma estructura de capas para filtrado de Spam.

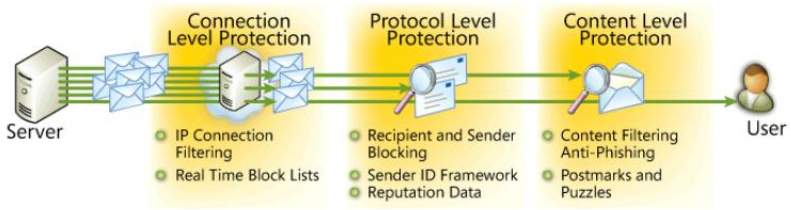

Ilustración 9: Funcionamiento global de filtrado Antispam

8.4.2 Selección de productos Antispam

Siendo el antispam un producto muy relacionado con el antivirus, se tendrá que poner especial hincapié en verificar la compatibilidad con el mismo así como los parámetros de interoperabilidad y multifunción que puedan realizarse de manera balanceada o como soporte en caso de caída. También es especialmente conveniente que sea compatible con el servidor de correo que se haya definido.

Aunque la calidad de los componentes de antispam es cada vez mayor y más universal entre fabricantes, no lo son tanto la calidad y flexibilidad de las consolas de gestión y reporting. Con lo cual este será también un punto importante que se deberá tener en cuenta.

A la hora de escoger los productos del mercado que se va a comparar se va a basar en el cuadrante de Gartner para productos antispam. En el caso concreto de antispam, para que una plataforma esté considerada dentro del análisis, ha de cumplir toda una serie de condiciones, algunas compartidas con el caso de los antivirus, algunas concretas para antispam:

- El producto ha de permitir el análisis de virus dentro del correo electrónico o integrarse con un antivirus que realice la función.
- El producto ha de permitir funciones básicas de detección de intrusos.
- También ha de permitir el escaneo de correo saliente, no solo el entrante, que sería la funcionalidad básica.
- Debe tener una expansión mínima en el mercado. Se requiere que al menos tenga 2000 instalaciones distribuidas, ya sea en particulares o empresas por todo el mundo.

En las imágenes se puede ver el cuadrante Gartner [15] y los pesos que en el caso de antispam tiene cada uno de los criterios.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	Standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	High
Marketing Execution	Standard
Customer Experience	High
Operations	Standard
Source: Gartner	

Tabla 14: Capacidad de ejecución para Antispam

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	No rating
Sales Strategy	No rating
Offering (Product) Strategy	High
Business Model	No rating
Vertical/Industry Strategy	No rating
Innovation	Standard
Geographic Strategy	Standard
Source: Gartner	

Tabla 15: Visión de mercado para Antispam

Por otro lado, a continuación se muestra el cuadrante gartner con la clasificación de todos los productos antispam.

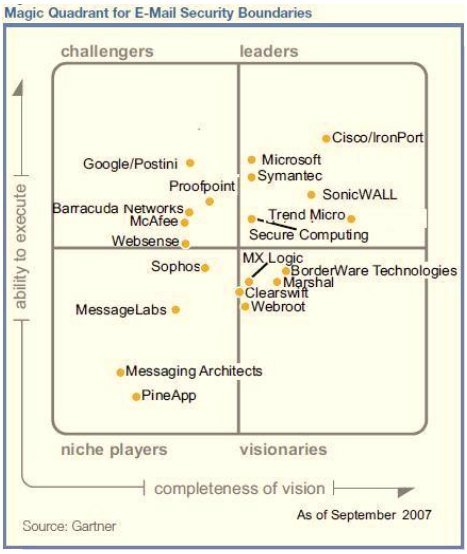

Ilustración 10: Cuadrante Gartner para Antispam

En el caso del cuadrante Gartner específico para Antispam, los fabricantes se agrupan en 4 grupos, dependiendo por un lado de su capacidad operativa y por otro lado de su visión de mercado. Los requisitos para estar en un cuadrante determinado son los mismos ya comentados en la explicación inicial acerca de los cuadrantes, pero con algunas consideraciones específicas propias de los productos antispam.

Para que una empresa sea posicionada como líder, además de ser empresas muy extendidas y demás, han de ofrecer un alto ratio comparado con la media del resto de productos en la eficiencia para descartar correo basura. Por otro lado han de ofrecer capacidades de desencriptación, DLP (Data Loss Prevention) para asegurar que no pierden ningún correo y a nivel empresarial han de invertir parte de los beneficios en investigación de malware que afecte al entorno del correo electrónico.

Analizando el cuadrante, se escogen los 5 fabricantes mejor posicionados y se procede con el análisis:

- Cisco Iron Port C370
- IMSS 5 de trend micro
- Symantec Mail Security 8380
- Sonicwall email security ES6000.
- Microsoft

8.4.3 Matriz de comparación

Como se ha definido en la metodología, se procede a incluir todos estos fabricantes en una matriz de comparación para poder visualizar de forma gráfica las diferencias entre los productos.

Funcionalidad	**Fabricantes**				
Marca	Sonicwall	Cisco/Iron port	Symantec	Trend Micro	Microsoft
Modelo	ES6000	C370	Mail Security 8380	IMSS 5.5	Exchange Antigen
Formato de aplicativo	Appliance	Appliance	Appliance	Software	Software
Detección de Antispam					
Filtrado Bayesiano	SI	SI	SI	SI	SI
Filtrado de palabras	SI	SI	SI	SI	SI
Filtrado por Black Lists	SI	SI	SI	SI	SI
Filtrado por White Lists	Nivel general y por usuario	Nivel general	Nivel General	Nivel General	Nivel General
Filtrado por categoría y contenido	Disponible	Disponible	Disponible	Disponible	Disponible
Número de Firmas reconocidas	10000	1100	900	1000	800
Actualización Firmas	Cada hora	Diaria	Diaria	Diaria	Diaria
Filtrado por Análisis de cabeceras	SI	SI	SI	SI	SI
Area de cuarentena	Opcional dentro del propio appliance o en un servidor	Opcional dentro del propio appliance o en un servidor	Opcional dentro del propio appliance o en un servidor	En disco duro de un servidor	En disco duro de un servidor
Creación de politicas a nivel usuario	Si, se pueden crear hasta 200 reglas	No soportado	No soportado	No soportado	No soportado
Encriptación de Mails	SI	SI	No soportado	SI	SI
Gestion					
Consola centralizada multiproducto	SI	NO	NO	NO	NO
Administración basada en roles	SI	Limitada	Limitada	No soportado	No soportado
Programación de updates automáticos	SI	SI	SI	SI	SI
Programación de backup base de datos automática	SI	SI	SI	SI	SI
Actualizaciones continuas	Cada hora	Diaria	Diaria	Diaria	Diaria
Control de nivel de agresividad	Intuitivo, de mayor a menor	Acciones técnicas concretas	Acciones técnicas concretas	Acciones técnicas concretas	Acciones técnicas concretas
Gestión de SPAM por usuario	SI	No soportado	No soportado	No soportado	No soportado
Soporte e incidencias					
Interoperabilidad con otros fabricantes	SI	SI	SI	SI	SI
Soporte Técnico	Barcelona, Holanda, USA	Irlanda - USA	Irlanda - USA	Irlanda - USA	USA
LOGS	email, script, syslog, snmp y pager	email, script, syslog, snmp y pager	email, script, syslog, snmp y pager	email, script, syslog, snmp y pager	email, script, syslog, snmp y pager
Reporting	Gráfico y numérico	Gráfico y numérico	Gráfico y numérico	Gráfico y numérico	Gráfico y numérico
Alta disponibilidad	SI	SI	No soportado	No soportado	No soportado
Standalone Failover	SI	SI	No soportado	No soportado	No soportado
Alimentación Redundante	Opcional	Opcional	No soportado	No soportado	No soportado
Capacidad					
Memoria	2 Gb	2 Gb	4 Gb	Depende de equipo	Depende de equipo
Disco Duro	320 Gb	150 Gb	300 Gb	Depende de equipo	Depende de equipo
CPU	Intel 3,2 GHz	Intel 2.0 GHz	Intel 2.0 GHz	Depende de equipo	Depende de equipo
Número de Dominios	Ilimitado	Ilimitado	5	5	Ilimitado

Puertos					
Puertos Comunicaciones RJ-45 10/100/1000	2	2	2	Depende de equipo	Depende de equipo
Puertos Gestión RJ-45 10/100/1000	1	1	1	Depende de equipo	Depende de equipo
Puertos HA RJ-45 10/100/1000	1	1	0	Depende de equipo	Depende de equipo
Ratios de funcionamiento					
Ratio de detección de SPAM	98,00%	95,63%	95,73%	96,71%	93,89%
Ratio de falsos positivos	0,00%	0,00%	0,00%	0,00%	0,71%
Precios y licenciamiento					
Precio del dispositivo*	4.160,75	7.804,36	7.514,99	6.840,00	504,00
Precio por usuario	--	--	--	17,1	1,26
Tipo de licenciamiento	Ilimitado por dispositivo	Ilimitado por dispositivo	Por número de dominios Ilimitado por dispositivo opcional Descuentos especiales si se dispone de Antivirus Symantec	Nominal por buzón de correo	Nominal por buzón de correo Precio por grupos de 5 usuarios

* Para los Antispam en formato Software se calcula el precio de usuario multiplicado por 400 usuarios que se espera tener

Tabla 16: Matriz de Comparación para Antispam

Los datos están extraídos por un lado de la documentación de cada uno de los productos y por otro lado de la experiencia en la instalación de todos ellos. Los datos de costes son proporcionados por los diferentes fabricantes entre febrero y marzo de 2008.

El indicador numérico que aparece, el ratio de detección de SPAM y de falsos positivos se obtiene con las siguientes consideraciones:

- Se envían 50.000 mensajes de SPAM.
- Se envían 4000 mensajes auténticos.
- El ratio de falsos positivos se obtiene como la división de mensajes auténticos detectados como SPAM respecto al total de mensajes auténticos.
- El ratio de detección de SPAM se obtiene como los mensajes considerados SPAM respecto al total de mensajes SPAM enviados.

Los datos son obtenidos del estudio de referencia [14] de la bibliografía.

8.4.4 Fortalezas y debilidades

Se realiza en este caso un análisis de fortalezas y debilidades de cada uno para intentar determinar cuál es el producto que más conviene. Para ello se utiliza la matriz de comparación desarrollada a tal fin y en el análisis de Gartner ya mencionado anteriormente [15].

Fortalezas y debilidades de Cysco Iron Port

Fortalezas	Debilidades
Cisco es uno de los líderes del mercado en soluciones de seguridad para el correo electrónico así como su solución antispam de Iron Port. Es en formato Appliance Cisco tiene uno de los mayores	El soporte solo es en inglés y no tiene un departamento de soporte exclusivo para Iron Port, sino que es compartido con otras soluciones de seguridad. No se puede definir políticas de antispam a nivel usuario.

departamentos de investigación y desarrollo dedicados a la búsqueda de soluciones Antispam. Los rangos de detección de SPAM son excelentes y tienen un bajo rango de falsos positivos. De hecho en las pruebas realizadas no se detecta ninguno.	Consola de gestión descentralizada, se tiene que acceder a una consola para cada sede. Algunas funcionalidades del producto se tienen que hacer por línea de comandos. El precio de Iron Port no es muy asequible. En la consola de Iron Port es de difícil gestión pues para cambiar el nivel de filtrado de SPAM hay que tener conocimientos técnicos acerca de lo que se quiere filtrar en concreto.

Tabla 17: Análisis de Fortalezas y Debilidades para Antispam Cisco

Fortalezas y debilidades de Symantec

Fortalezas	Debilidades
Symantec tiene una significativa cuota de mercado de la seguridad de email. La nueva generación de productos de Symantec serán appliances para la seguridad del correo. Es en formato Appliance El licenciamiento de Symantec es atractivo ya que ofrece paquetes de antivirus con seguridad de correo. La solución antispam tiene buenas referencias de funcionamiento desde 2006 y tiene una en general una buena imagen en el mercado de la seguridad de correo. Las listas de reputación utilizadas por sus filtros antispam son de gran calidad.	La solución de Symantec tiene reducidas capacidades de escaneo y detección de Spam. La versión actual en formato Appliance de Symantec, el formato escogido a instalar no ha tenido mucha demanda por parte de los clientes. La debilidad de su solución es en la parte de email Gateway ya que se han descubierto varias vulnerabilidades en el software. No tiene ninguna solución de encriptación del correo para securizarlo. Se encuentran referencias de quejas referentes a inestabilidad en el funcionamiento del producto. No soporta encriptación de mails. No dispone de posibilidad de alta disponibilidad.

Tabla 18: Análisis de Fortalezas y Debilidades para Antispam Symantec

Fortalezas y debilidades de Trend Micro

Fortalezas	Debilidades
Es líder en solución de antivirus y especialmente en el apartado de antispam tiene una amplia cuota de mercado. Además de cuota de mercado tiene buena reputación y recomendaciones de uso. El ratio de detección de correo basura y puesta en cuarentena es de los más altos analizados. Tiene una singular capacidad de detección de Spam proveniente de Asia ya que su motor de filtrado integra los lenguajes asiáticos. Los informes de detección que autopublica en HTML son de calidad elevada. Su solución incluye encriptación del correo.	Tiene formato software Según las experiencias de usuario consultadas, las nuevas versiones de los productos tienen muchos problemas ya que parece ser que no son completamente probadas antes de salir al mercado. La velocidad respuesta del departamento de soporte es muy lenta y no es de la calidad esperada para un producto de seguridad.

Tabla 19: Análisis de Fortalezas y Debilidades para Antispam Trend Micro

Fortalezas y debilidades de Sonicwall

Fortalezas	Debilidades
Sonicwall ofrece una suite de productos de seguridad que incluyen firewall, antivirus, antispyware, detector de intrusos y Antispam Es en formato Appliance A nivel empresarial es una compañía que está en pleno crecimiento y con posicionamiento bastante importante dentro de los líderes del mercado de la seguridad. El producto soporta agregar listas negras en tiempo real y sin corte de servicio como el resto pero además tiene la capacidad de utilizar listas	A nivel empresarial encuentra dificultad para acceder a las grandes corporaciones internacionales. Es especialmente debido a que tiene un canal de partners bastante limitado. La escalabilidad en sus productos es limitada especialmente para ser implantado en empresas muy grandes. Lenta sincronización total con LDAP, aunque esto no afecte el rendimiento de la solución ya que la sincronización total la hace solo al inicio del proyecto.

blancas por usuario para minimizar los falsos positivos. - La consola de gestión es de fácil manejo y permite un rápido despliegue de las principales opciones de seguridad de correo. - Los umbrales de Spam son ajustables en tiempo real, y los administradores pueden delegar la gestión de su SPAM a los mismos usuarios con un panel de control limitado a los correos propios del usuario. - El producto permite crear políticas de entrada y salida de correo de manera específica para cada compañía ideales para campañas propagandísticas a través de email de manera que no se confunda con Spam. - Utiliza diccionarios para escanear el Spam en 10 idiomas. - Las opciones de cuarentena son de las más avanzadas del mercado. - Dispone de integración con Outlook creando una carpeta exclusiva de Spam.	

Tabla 20: Análisis de Fortalezas y Debilidades para Antispam Sonicwall

Fortalezas y debilidades de Microsoft

Fortalezas	Debilidades
- Microsoft ha llegado poco a poco a ser uno de los competidores más fuertes en el mercado de la seguridad a base de adquirir empresas de antispam y antivirus. - Su producto ha probado ser una de las soluciones más efectivas de antispam en el mercado con el correo Hotmail.	- Tiene formato software - El soporte de sus productos es bastante pobre. - Al ser productos que Microsoft ha comprado, la integración y el desarrollo de los productos ha sido lenta. - La solución de Microsoft no es capaz de escanear adjuntos en el correo. - Su solución Exchange Edge debe ser comprada con servicios adicionales que hacen más cara la solución.

	▪ La consola de administración y uso no es para nada intuitiva, lo que provoca que la utilización de la misma sea complicada.

Tabla 21: Análisis de Fortalezas y Debilidades para Antispam Microsoft

8.5 Comparativa de firewalls

En este punto se plasma el trabajo realizado en cuanto a análisis de firewalls basándose en las consideraciones analizadas en el apartado 2.2.5.

De manera similar al apartado anterior, a partir del cuadrante Gartner de fabricantes se determina los productos a analizar y una vez se tienen seleccionados se procede a un análisis de debilidades y fortalezas de cada uno.

En este caso se realizó el análisis de manera conjunta tanto para el producto a instalar en servicios centrales como para el producto a instalar en las diferentes sedes, ya que son componentes que han de ser completamente compatibles entre sí. Las comparativas de productos se realizan para modelos destinados a servicios centrales y luego se escoge un producto para sede de la misma marca y gama dimensionado a las necesidades de la misma.

El primer punto es evaluar las tácticas y tecnologías de vanguardia relacionadas con los aplicativos Firewall.

8.5.1 State of the art para Firewalls

Se ha realizado un trabajo de investigación de los protocolos y técnicas más novedosas que se encuentran en el mercado. El proceso de búsqueda se basa en Internet como primera opción y a partir de ahí en documentación de diversos fabricantes.

Integración de IPS: Intrusion Prevention System o Sistema de Prevención de Intrusos engloba a todas aquellas políticas y protocolos que permiten la detección de accesos no deseados en la red. Es un servicio típicamente ofrecido por un elemento independiente o bien integrado en Antivirus. La posibilidad de disponer de detección de intrusos en el firewall refuerza de manera global la red ya que se complementa con la propia prevención que ofrece el Antivirus. En un apartado tan importante como la seguridad de la red y la protección de la privacidad de la información que circula por ella, tener redundancia de funciones es sumamente importante pues permitirá estar más seguros. Se buscará además que la integración de este servicio no sea perjudicial para el rendimiento de la red ni para el propio firewall.

DPI: Deep Packet Inspection o Inspección profunda de paquetes. Es un protocolo que examina los paquetes a nivel de aplicación. Es decir, evalúa los paquetes que pasan por la red a nivel TCP, examina a que aplicación pertenecen, los usuarios origen y destinatario, si puede haber o no fuga de datos (también denominado Data Leak Prevention), incluyendo además priorización en función de la aplicación que sea. Además sirve para recolectar estadísticas que ayuden luego a evaluar el uso de la red. En la figura se muestra un gráfico del funcionamiento de un protocolo DPI, en este caso con el apoyo de un servidor proxy para realizar el escaneo.

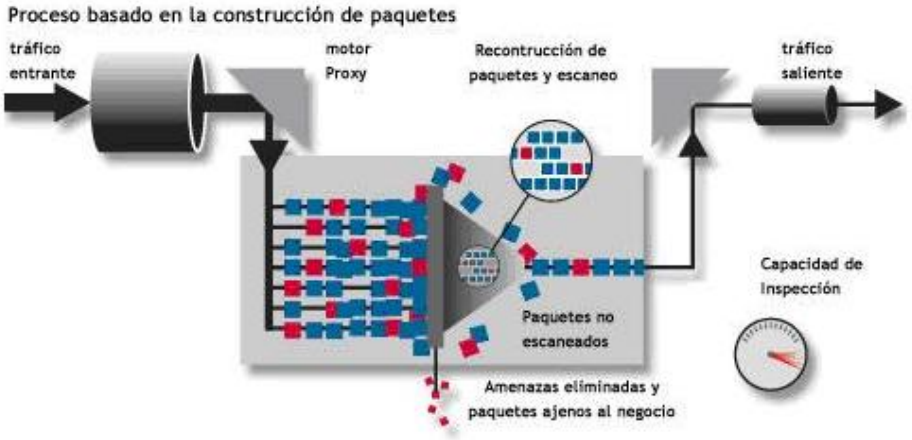

Ilustración 11: Proceso de Inspección Profunda de Paquetes

RFDPI Una evolución del protocolo DPI es el RFDPI o Reassembly-free DPI. En este caso este protocolo ha sido desarrollado por Sonicwall y optimiza el desmontaje y montaje de paquetes necesario para inspeccionarlos, permitiendo el flujo de paquetes en tiempo real. Para poder dar esta funcionalidad, ha de disponer de múltiples procesadores capaces de realizar el escaneo. En la figura se puede observar este escaneo en paralelo.

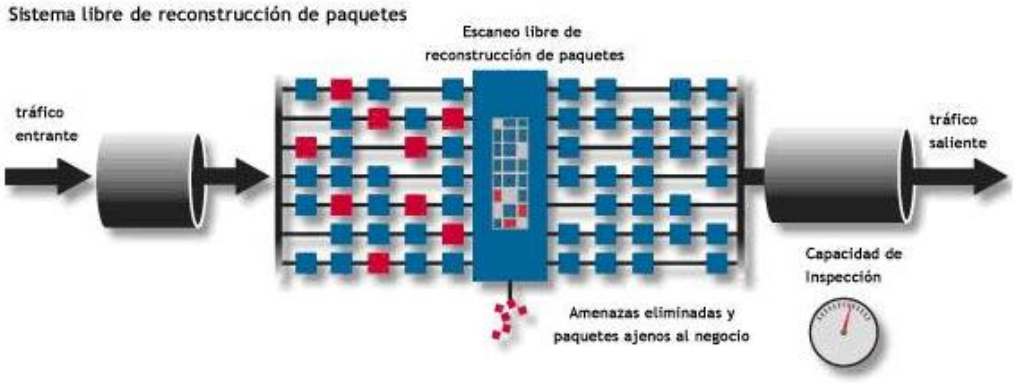

Ilustración 12: Esquema de un proceso RFDPI

UTM: Unified Threat Management o Gestión de Amenazas Unificada, consiste en agrupar múltiples elementos de seguridad dentro del propio firewall. Además de incluir IPS como en el caso anterior, para que un producto sea considerado como UTM ha de ser capaz de dar los servicios de Antivirus, Antispam, Antipishing y filtrado de contenidos. La mayor ventaja de este tipo de dispositivos es la simplicidad de uso de todo el entorno de seguridad al tener todos los servicios en un único punto de acceso. Los protocolos UTM pueden utilizar para el análisis de las amenazas protocolos como el DPI o RFDPI. Dentro de los dispositivos que ofrecen UTM se pueden encontrar evoluciones que proporcionan alguna funcionalidad extra como los explicados a continuación:

- UTM Load Balancing: Los dispositivos que proporcionan UTM con balanceo de carga son aquellos que además de incluir todas las funcionalidades UTM incluyen sistemas multiprocesador de manera que se realiza un balanceo interno de la carga para obtener un mayor rendimiento. Al ser multiprocesador también ofrecen una mayor fiabilidad. En la figura se puede observar cómo funciona el balaceo de carga en un dispositivo UTM.

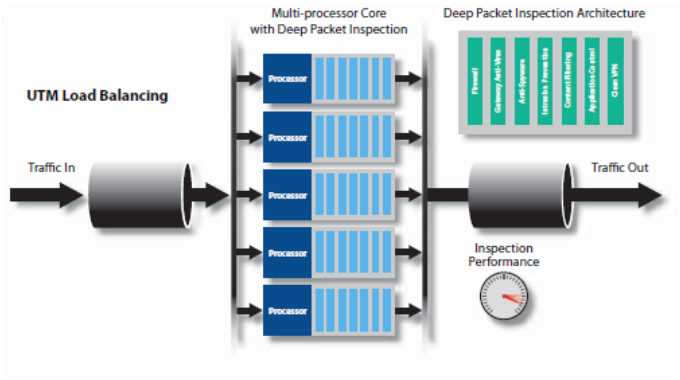

Ilustración 13: Balanceo de carga UTM

- RealTime UTM: Un problema que presentan las primeras versiones de UTM es que el dispositivo se ha de apoyar en servidores proxy que le ayuden con las tareas de verificación. Entiéndase como servidor proxy un servidor de apoyo que no necesariamente ha de ser un servidor proxy web. Los dispositivos RealTime UTM disponen de una gran capacidad hardware de manera que pueden analizar los paquetes que circulan por la red sin necesidad de desviar el tráfico ni provocar cuellos de botella. En la imagen se puede observar la estructura que sigue el tráfico a través de un dispositivo UTM.

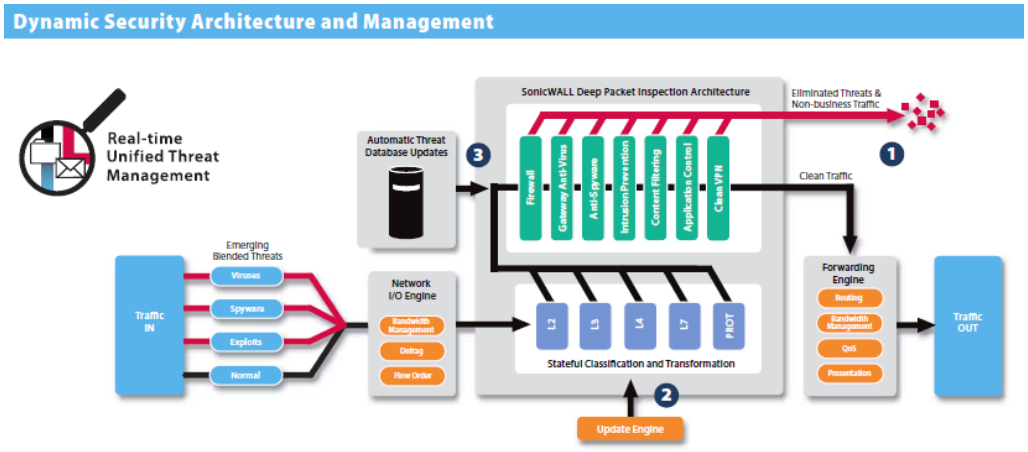

Ilustración 14: Procesado UTM en tiempo real

NGFW: Next-Generation Firewalls o firewalls de nueva generación, son aquellos firewalls que cumplen y dan servicio a una serie de funcionalidades requeridas [16]:

- Bump-in-the-wire configuration support: el firewall se puede poner no como un elemento conectado a la red que vigila los paquetes que pasan sino intercalado en la línea de manera que todo el tráfico de la red pasa por él.
- Basic Firewall functionalities: Ha de cumplir con las funcionalidades básicas de Standard First Generation Firewalls que son:
  - Filtrado de paquetes
  - Direccionamiento NAT (Network Address Translation)
  - Stateful Inspection: Son aquellos firewalls que permiten detección del estado de la red y solo gestionan tráfico a través de conexiones abiertas.
  - VPN (Virtual Private Network): Los firewalls son capaces de gestionar redes VPN para permitir la conexión remota.
- Integrated IPS: Ha de disponer de IPS integrado, de manera que el IPS proporcione al firewall datos sobre direcciones a bloquear para que directamente ya no entren en el sistema la próxima vez.
- Application Awareness: También ha de disponer de evaluación de contenidos a nivel de aplicación para poder realizar un filtrado más inteligente. Un ejemplo podría ser permitir las aplicaciones de mensajería instantánea pero cortar los envíos de ficheros a través de ellas.
- Extrafirewall Intelligence: El firewall ha de ser capaz de obtener información externa al propio firewall para añadir inteligencia al filtrado a realizar. Un ejemplo de esta propiedad sería la capacidad de conectar con el servidor Active Directory para sincronizarse con él y determinar que usuarios no pueden acceder a la red o a algunas aplicaciones en concreto.
- Upgrade paths: el firewall ha de permitir una manera sencilla para incluir nuevos orígenes de información para su base de datos de filtrado y nuevas

amenazas al sistema. Debe estar preconfigurado para que este tipo de inclusiones sean sencillas y ágiles.

Multi-administrator Capabilities: La capacidad multi-administrador no se limita al hecho de tener más de un usuario administrador, si no en la posibilidad de definir diferentes niveles de administración para los Firewalls. Al definir una estructura jerárquica de firewalls con uno central y varios distribuidos para cada sede es interesante la capacidad de tener diferentes niveles de administración pudiendo definir administradores locales, con toda esta seguridad además gestionada localmente desde servicios centrales. En la imagen se puede ver una distribución de roles y usuarios jerarquizada.

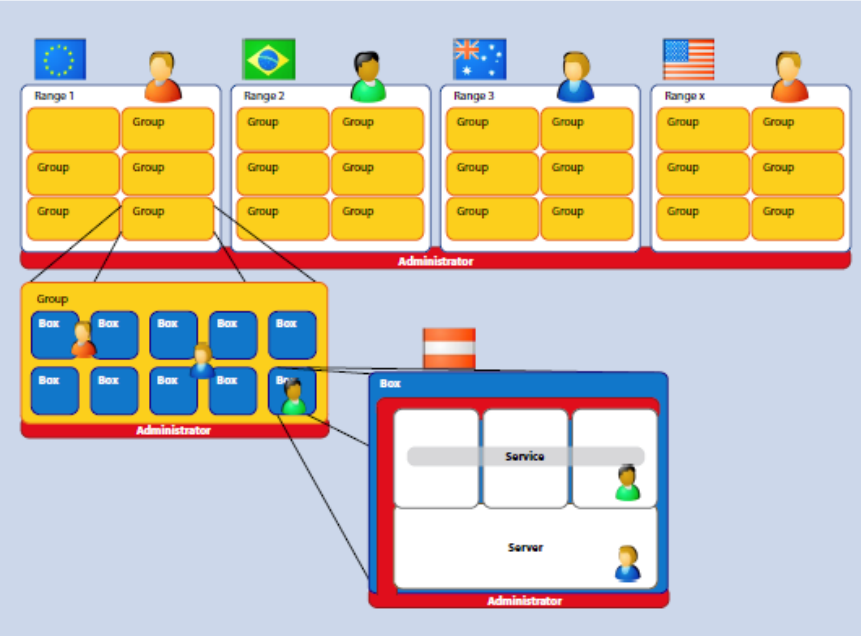

Ilustración 15: Capacidades de administración multi-administrador

8.5.2 Selección de firewalls

El proceso de selección de los firewalls que se incluirán en la comparativa también sigue los pasos establecidos en el apartado 4.1. Se buscará como primera referencia los firewalls mejor posicionados en el cuadrante de Gartner para Enterprise Firewalls.

En el caso de los Firewalls, para que un fabricante sea incluido en el análisis Gartner se tienen en cuenta toda una serie de parámetros a nivel empresa, entre ellas las opiniones de directores de empresas de IT respecto a la experiencia previa con dichos fabricantes, aquellos fabricantes con mayor cuota de mercado, un mínimo de facturación de 10 millones de dólares en el mercado del Firewall, la competitividad de la empresa y del producto y la presencia del fabricante en el mercado internacional.

También hay otra serie de requisitos a nivel de producto, como el hecho de que proporcione políticas robustas de seguridad, prevención de intrusos y reconocimiento de redes de confianza. Al ser el firewall la primera línea de defensa y la parte más expuesta a los ataques desde internet, estos requisitos son indispensables para que el producto sea tenido en cuenta. Por otro lado en este tipo de mercado la longevidad no es algo demasiado importante pues al ser la barrera de entrada en las redes de la empresa, suele ser el componente de red que se reemplaza con mayor frecuencia aun sin que tenga ningún problema de funcionamiento.

Este último punto hace que la fiabilidad del producto sea también una característica que busque el fabricante para conseguir la fiabilidad del cliente.

En las peculiaridades del firewall respecto al posicionamiento en la capacidad de ejecución y la completitud de visión de mercado, se tiene en cuenta la evolución de las redes empresariales y su cada vez más elevada complejidad, por lo que los firewalls han de ser altamente configurables para dar respuesta a esta complejidad. Por ello se tiene en cuenta también que la empresa tenga una gran variedad de modelos de diferentes capacidades y funcionalidades, ya que en un entorno multinacional, con diferentes sedes de diferentes tamaños y con diferente número de usuarios en cada una, es conveniente y necesario disponer de dispositivos ajustados a sus necesidades.

Desde la misma perspectiva se tiene en cuenta que los firewalls dispongan de funcionalidad VLAN (Virtual Local Area Network, es decir, que redes físicamente separadas se vean como conjuntas) y desde la perspectiva de poder solucionar incidencias de manera directa, los firewalls han de dar un nivel adecuado de registro de actividad y errores.

Por otro lado, se pueden ver a continuación las prioridades asignadas a cada uno de los criterios de evaluación, tanto para la capacidad de ejecución como para la completitud de visión.

En la siguiente imagen se puede ver el gráfico del cuadrante Gartner para firewalls.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	High
Operations	Standard
Source: Gartner	

Tabla 22: Capacidad de ejecución para Firewalls

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Standard
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	High
Geographic Strategy	Standard
Source: Gartner	

Tabla 23: Visión de mercado para Firewalls

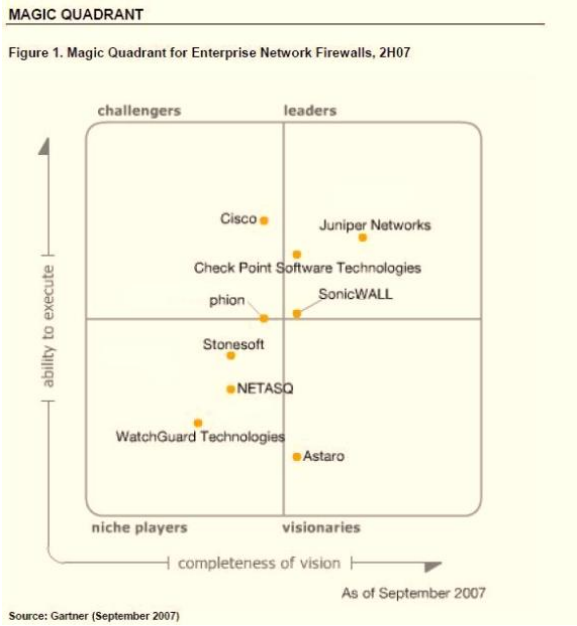

Ilustración 16: Cuadrante Gartner para Antispam

En este caso, se realiza un análisis de productos de los cinco fabricantes mejor posicionados pese a no estar incluidos todos en el grupo de challengers:

- Checkpoint
- Cisco
- Juniper
- Phion
- Sonicwall

8.5.3 Matriz de comparación

A continuación se puede encontrar anexa la matriz de comparación realizada como método de ayuda para poder realizar el posterior análisis de fortalezas y debilidades.

Propiedad	Fabricantes				
Marca	Sonicwall	Checkpoint	Cisco	Juniper	Phion
Modelo	NSA E6500	UTM-1-3070	ASA 5500-E	IDP-200	F-350
Métodos de deteccion de tráfico					
Utilización de reglas Heurísticas	SI	SI	SI	SI	SI
Reconcimiento de ataques desconocidos - Protección ante tráfico anómalo	SI	SI	SI	SI	SI
Detección de anomalías a nivel de paquetes	SI	SI	SI	SI	SI
Detección de anomalías a nivel de aplicación	SI	NO	NO	NO	NO
Autoaprendizaje para minimizar falsos positivos	SI	SI	SI	SI	SI
Detección de ataques de Spoofing	SI	SI	SI	SI	SI
Detección de ataques de denegación de servicio	SI	SI	SI	SI	SI
Protección a nivel de SYN Cookie	SI	NO	NO	NO	NO
Protección Zero-Day	SI	SI	SI	SI	SI
Aplicación de protocolo DPI	SI	SI	SI	SI	SI
Protocolos soportados					
VPN	SI	SI	SI	SI	SI
SSL/VPN	SI	SI	SI	SI	SI
VLAN	SI	SI	SI	NO	NO

Propiedad	Fabricantes				
Marca	Sonicwall	Checkpoint	Cisco	Juniper	Phion
Modelo	NSA E6500	UTM-1-3070	ASA 5500-E	IDP-200	F-350
Protocolos soportados					
VoIP	SI	SI	SI	SI	SI
QoS	SI	SI	SI	SI	SI
Capacidades de Prevención de Intrusos					
Protocolos capaz de escanear	60 protocolos 500 subprotocolos	50 protocolos	40 protocolos	50 protocolos	40 protocolos
Número de firmas disponibles o patrones de ataque	5.000	4.000	3.000	2.000	3.000
Identificación de aplicaciones maliciosas	Nivel de Aplicación	Bloqueo de puertos	Bloqueo de puertos	Bloqueo de puertos	No soportado
Capacidad de Gestión de Tráfico					
Posibles acciones ante tráfico sospechoso	Drop Packet Drop conecction Close Client Close Server Close Client/server	Drop Packet Drop conecction Close Client Close Server Close Client/server	Drop Packet Drop conecction Close Client Close Server Close Client/server	Drop Packet Drop conecction Close Client Close Server Close Client/server	Drop Packet Drop conecction Close Client Close Server Close Client/server
Marcación QoS/DiffServ	SI	No soportado	SI	No soportado	No soportado
Reglas de VLAN	SI	No soportado	No soportado	No soportado	No soportado
Routing	SI	SI	SI	SI	SI
Recomendación de acciones al administrador en base al tipo de ataque	SI	No soportado	No soportado	No soportado	No soportado
Bloqueo de IP automático de manera temporal	SI	SI	SI	SI	SI
Gestión					
Consola centralizada multiproducto	SI	NO	NO	NO	NO
Administración basada en roles	Avanzado	Suficiente	Mínimo	No soportado	No soportado
Programación automática de actualizaciones	SI	SI	SI	SI	SI
Bloqueos de Objetos cuando hay más de un administrador en paralelo	SI	No soportado	No soportado	No soportado	No soportado
Programación automática de backup base de datos	SI	SI	SI	SI	SI
Gestor de Tareas en curso y finalizadas	SI	SI	SI	SI	SI
Complejidad de administración	Media	alta	media	alta	Alta
Soporte e incidencias					
Interoperabilidad con otros fabricantes	SI	SI	SI	SI	SI
Ubicación Soporte Fabricante	Barcelona, Holanda, USA	Irlanda -USA	Irlanda - USA	USA	USA
LOGS	email, script, syslog, snmp	email, script, syslog, snmp y pager	email, script, syslog, snmp y pager	email, script, syslog, snmp y pager	email, script, syslog, snmp y pager
Reporting gráfico y numérico de estado de aplicativo	SI	SI	SI	SI	SI
Reporting gráfico y numérico de estado de red	SI	SI	SI	SI	SI
Alta disponibilidad	SI	SI	SI	SI	SI
Standalone Failover	SI	SI	SI	SI	SI
Alimentación Redundante	Opcional	Opcional	Opcional	Opcional	Opcional
Capacidad					
Memoria	1Gb	1Gb	1Gb	1Gb	1Gb
CPU multiproceso	SI	NO	NO	NO	NO
Número Máximo de Conexiones Activas	70.000	68.000	65.000	70.000	48.000
Throughput	220 Mbps	200 Mbps	200 Mbps	100 Mbps	100 Mbps
Puertos					
Puertos Comunicaciones RJ-45 10/100/1000	8	8	5	6	6
Puertos Gestión RJ-45 10/100/1000	1	1	1	1	1
Puertos HA RJ-45 10/100/1000	1	1	1	1	1
Precios					
Precio en Euros	8.275	15.700	11.930	14.615	6.575
Soporte Incluido en el precio	2 años	1 año	1 año	1 año	1 año

Tabla 24: Matriz de comparación para Firewalls

Los datos para la obtención de esta matriz de comparación se obtienen de los manuales con las especificaciones de cada producto salvo los costes, que son solicitados a los diferentes proveedores en Marzo de 2008.

8.5.4 Fortalezas y debilidades

Teniendo en cuenta la matriz de comparación, así como diferentes informes y comparativas buscadas por internet se realiza el siguiente análisis de fortalezas y debilidades de cada uno de los productos.

Análisis de fortalezas y debilidades de Checkpoint

Fortalezas	Debilidades
• Compañía con reconocimiento mundial en el apartado de firewalls y con gran implantación en el mercado. • Un excelente canal de partners, que facilita la obtención del producto y de soporte. • Check Point es primariamente un vendedor de software que se integra con hardware de Nokia y Crossbeam, ambos con gran prestigio. • Su plataforma de seguridad puede ser integrada en diferentes servidores, de manera que es fácilmente escalable. • Ha expandido su catálogo de productos de la gran empresa hacia la pequeña y mediana con lo que dispone de un amplio abanico de posibilidades. • Posee una interface de gestión bastante madura con la habilidad de manejar redes grandes y complejas con un gran número de dispositivos. • En la actualidad ha conseguido integrar con éxito una solución IPS (sistema de prevención de intrusos) dentro de la solución firewall.	• Siguen siendo los productos más caros en el mercado y con bastante diferencia en comparación con los demás fabricantes. • Tiene algunos puntos técnicos en los que la calificación por parte de usuarios y expertos es de problemática, especialmente en lo referente a su sistema de inspección de paquetes y la frecuencia con la que necesita actualizarse. • Desde el punto de vista empresarial, Check Point nunca informa de su road map (hoja de ruta) a los clientes, por lo que no se sabe que habrá en el futuro con las nuevas versiones. Hay mucho secretismo en cuanto a la evolución del producto. • En los productos que van integrados en hardware de otros fabricantes, en este caso Nokia y Crossbeam el soporte en caso de incidencias siempre es más deficiente pues implica muchas veces la colaboración entre ambas empresas para solucionar incidencias.

Tabla 25: Análisis de Fortalezas y Debilidades para Firewall Check Point

Análisis de fortalezas y debilidades de Cisco

Fortalezas	Debilidades
• Cisco ofrece grandes descuentos, especialmente si, como es el caso, se dispone de otros componentes de Cisco como routers y switches. • La nueva gama de productos ASA (sustituye al PIX) tiene un módulo IPS (sistema prevención intrusos) más	• La implantación de firewalls de Cisco es casi en exclusiva en clientes en los que disponen de otros productos Cisco, lo que hace pensar que únicamente en el coste como razón principal de implantación. • Las consolas de gestión de los firewalls

potente y evolucionado. • Cisco ofrece una integración muy potente de los firewalls ASA con switches y routers de la misma marca Cisco. • Cisco tiene una amplia red de partners y canales de distribución en todo el mundo.	Cisco no son muy potentes en comparación con las de otros productos de firewalls. • Cisco solo ofrece integración con dispositivos de red si dichos dispositivos también son Cisco. Cuando hay productos como switches y routers de otras marcas no hay compatibilidad con firewalls cisco, por ejemplo, para establecer VPNs entre Cisco y otras marcas. • En el caso de Cisco, como en el de Check Point no hay visibilidad de la evolución de los productos, lo que limita las decisiones a futuro.

Tabla 26: Análisis de Fortalezas y Debilidades para Firewall Cisco

Análisis de fortalezas y debilidades de Juniper

Fortalezas	Debilidades
• Juniper ofrece una amplia gama de productos de seguridad para cualquier tipo de empresa. • Sus appliances (hardware-software) son propios de ellos y cuando se hace una incidencia ellos mismos la resuelven sin recurrir a otro proveedor. • En el caso que interesa que es el de un firewall centralizado con una red de firewalls en fábricas, Juniper dispone de una solución integrada que encaja con las necesidades. • Juniper tiene una fuerte integración con el resto de productos de red y seguridad (routers / switches) de otras marcas. • Las referencias de clientes que tienen Juniper respecto al soporte son bastante positivas.	• Los firewalls Juniper cuando van a sustituir un firewall cisco presentan una gran serie de problemas técnicos y de compatibilidad al inicio de la implementación. • La integración de su firewall con su IPS (sistema detector de intrusos) es muy pobre. • Juniper generalmente tiene unos precios muy altos en comparación a la competencia.

Tabla 27: Análisis de Fortalezas y Debilidades para Firewall Juniper

Análisis de fortalezas y debilidades de Phion

Fortalezas	Debilidades
• PHION es un producto de seguridad (firewall) diseñado solo para grandes empresas. • Es un producto altamente extendido en Europa y su centro de soporte está en Alemania. • Su consola de gestión es amigable y bien diseñada.	• Solo dispone de soporte en inglés y alemán. • Su IPS (sistema detector de intrusos) es muy limitado • Solo está extendido su uso en Europa. • Su departamento de ventas solo tiene visibilidad para Europa. • Su familia de productos en seguridad es muy limitada.

Tabla 28: Análisis de Fortalezas y Debilidades para Firewall Phion

Análisis de fortalezas y debilidades de Sonicwall

Fortalezas	Debilidades
• Sonicwall tiene productos a precios muy competitivos. • Su productos son de gama baja, media y alta ideales para cualquier tamaño de empresa. • Entre todos los firewalls, Sonicwall, tiene un centro de soporte internacional de los más avanzados y grandes del mundo. El soporte es en 10 idiomas (incluyendo castellano). Dispone también de presencia física en la mayor parte de países del mundo. • La opción de NBD (next bussiness day), pionera en el mercado, resulta atractiva para los clientes. Mediante esta opción, Sonicwall se compromete a remplazarte el equipo dañado al día siguiente estés en donde estés. • En una agresiva política comercial, Sonicwall ofrece la recompra de componentes de la competencia a muy buen precio a cambio de instalar los suyos propios.	• Los productos Sonicwall no son enfocadas a la pequeña empresa • El Firewall de Sonicwall en ocasiones provoca problemas de unicidad de componentes pues dispone de muchas funcionalidades integradas. Dependiendo del producto asociado que se elija para Antispam, antivirus o IDS puede provocar pérdidas de servicio, han de ser completamente compatibles.

• El appliance (hardware) es propio de Sonicwall e integra la mejor solución de IPS (sistema detector de intrusos) en el mercado de la seguridad. • Único en integrar dentro del mismo hardware un antivirus(mcafee), antispyware, gestor de contenidos web, balanceo de carga de salida y filtrado con listas RBL para minimizar el SPAM.	

Tabla 29: Análisis de Fortalezas y Debilidades para Firewall Sonicwall

8.6 Comparativa de proveedores para líneas de comunicaciones

A continuación se analizan tanto las opciones en las modalidades de conexión a la red como una serie de proveedores para poder elegir con cierto criterio cuál de ellos dará el servicio necesario.

8.6.1 State of the art para ISPs

Uno de los elementos clave para poder disponer de ancho de banda asegurado, así funcionalidades integradas de VPN que no penalicen este ancho de banda es el protocolo de red utilizado. Por ello en este apartado se van a revisar las tendencias del mercado en este sentido para poder buscar un ISP que ofrezca servicio utilizando un protocolo adecuado.

MPLS: Multi-Protocol Label Switching o Multi-Protocolo de Conmutación de Etiquetas. Este protocolo aparece con dos objetivos básicos, mejorar el rendimiento de los protocolos previos y aportar nuevas funcionalidades en los protocolos de su nivel. Para ubicarlo correctamente, MPLS está asociado a una mezcla de los niveles 2 (enlace de datos) y 3 (red) del modelo OSI (Open System Interconnection o Interconexión de Sistemas Abiertos) de protocolos de comunicación. Este protocolo está definido en la norma de la IETF *RFC-3031*.

La mejora de rendimiento se consigue a través de la encapsulación de la información a nivel 2, por debajo del nivel IP, asignando una etiqueta que tiene ya calculada la ruta que ha de seguir. Esta etiqueta representa lo que se denomina FEC (Forward Equivalence Class) y que identifica el conjunto de paquetes que viajarán a través de la misma ruta.

Cuando entra una conexión nueva en la red MPLS, en el punto de entrada se le asigna una etiqueta que depende de destino (entendiendo como destino el punto de salida de la red MPLS, aunque luego vaya más allá), depende de la prioridad (Calidad de Servicio QoS) asignada y si pertenece o no a una VPN. Por ello las etiquetas MPLS solo tienen significado a nivel interno de la red, de hecho solo tienen sentido a nivel local, la etiqueta puede ir cambiando conforme se acerca al destino. Dentro de la red MPLS, las etiquetas no contienen información sobre el destinatario real, esta información está encapsulada dentro de los paquetes, lo que contienen es información sobre la dirección del router MPLS más cercano a su destino.
La ganancia respecto a los sistemas tradicionales de enrutamiento IP es significativa pues no se ha de desmontar el paquete de capa 2 en cada router para evaluar en la capa 3 cuál es el siguiente punto del camino, si no que directamente entra por un puerto, se verifica la etiqueta, opcionalmente se le cambia por otra y se envía por el puerto que según la etiqueta ha de ir.

Las etiquetas las puede asignar un tipo de router denominado LER (Label Edge Router), que son los puntos de entrada y salida de la red que conectan la red MPLS con otras redes, ya sean LANs, redes de Internet de otros protocolos, o cualquier otro tipo de red. Los puntos intermedios de la red y que solo tienen conexión con otros nodos MPLS se denominan LSR (Label Switching Router) y simplemente se encargan de redirigir el tráfico que reciben hacia su destino. En la figura se puede observar un ejemplo de tráfico MPLS:

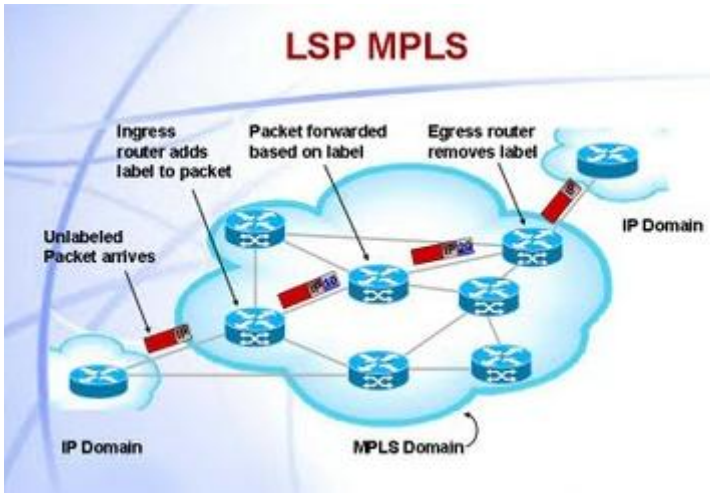

Ilustración 17: Ejemplo de Tráfico MPLS

Cuando un nuevo router se añade a la red, a través de una serie de protocolos de comunicación interna, como serían OSPF (Open Shortest Path First), RIP (Routing Information Protocol) o BGP (Border Gateway Protocol), se define una etiqueta para el nuevo router y se actualizan las tablas de encaminamiento del resto de

componentes de la red para que sepan hacia dónde dirigir el tráfico asociado con el nuevo nodo.

En referencia a las novedades que ofrece este protocolo respecto a otros es que permite utilizar clases de servicio (CoS, Classes of Service) de manera que se puede tener calidad de servicio (QoS, Quality of Service), Ingeniería de Tráfico (TE, Traffic Engineering) y VPN basadas en IP.

La capacidad de definir clases de servicio permite luego asignar diferentes prioridades en función de la clase de servicio asociada y por lo tanto disponer de Calidad de Servicio. La calidad de servicio es la capacidad de poder priorizar paquetes en función de lo que contengan. Es decir, si es tráfico de voz, de videoconferencia o de streaming, es necesario un retardo mínimo para poder dar un servicio a tiempo real, ya que en caso contrario la conversación o la imagen se verían cortadas. Sin embargo el tráfico de descargas o de mailing no necesita de esa inmediatez con lo que se le puede asignar una prioridad menor. En definitiva, lo que permite QoS es gestionar el ancho de banda mejorando la eficiencia y controlar la latencia de la red para asegurar un correcto servicio.

Otra ventaja de MPLS es que las rutas no se mantienen fijas. En los protocolos ya mencionados que cuando entra un nodo nuevo asignan una ruta se asigna la ruta más corta o más óptima. Sin embargo, la Ingeniería de Tráfico, permite variar on-demand esa ruta cuando se detecta problemas de conexión o tráfico excesivo en algún enlace. Ello minimiza la pérdida de paquetes reduciendo el ancho de banda consumido en reprocesamiento de paquetes y elevando la garantía de recepción.

Como su nombre indica, es un sistema multiprotocolo, por ello aunque MPLS surge en principio como una red compatible con ATM (Asynchronous Transfer Mode) ya que es capaz de encapsular paquetes de este protocolo y transportarlo, pero en realidad es cada vez más una alternativa a ATM ya que cubre por completo las funcionalidades de ATM pero también da otras ventajas ya comentadas.

Por último, la otra gran ventaja de MPLS es la facilidad de creación de VPN, ya que para crear un túnel VPN simplemente hay que asignar una etiqueta o FEC que no pueda ser compartida por otro tráfico aunque tengan tramos a recorrer en común. Esta gestión de VPN sobre MPLS está definida en el standard de la IETF *RFC 4364 BGP/MPLS IP VPNs*. El tráfico de VPN sobre MPLS también se conoce como VPLS o Virtual Private LAN Service.

MPLS es un protocolo en desarrollo y ampliación ya que se busca la compatibilidad total con todas las redes del mercado. Como evoluciones del mismo se encuentra GMPLS, Generalized MPLS que consiste en una extensión del protocolo MPLS para que además de funcionar sobre dominios de conmutación de paquetes funcione sobre dominios de conmutación sobre longitud de onda, es decir, la posibilidad de

extender el protocolo MPLS sobre redes ópticas, pero al igual que en los dispositivos de conmutación de paquetes sin necesidad de llegar al paquete de nivel de red para poder determinar a qué dirección IP se dirige.

Realizar un análisis de comparativas del protocolo MPLS con otros se hace difícil porque no está exactamente en ninguno de los niveles OSI, cubre funcionalidades varias de varios niveles. Por ello la competencia con el protocolo MPLS se puede evaluar por partes. Una comparación posible sería en el apartado de VPN, se realiza en este caso una comparativa con VPN sobre IPSec.

IPSec es un protocolo de capa de red (capa 3 de los niveles OSI) que dota de opciones de seguridad y cifrado a los protocolos más extendidos de nivel 3, IPv4 e IPv6. Inicialmente nació asociado a IPv6 pero el lento desarrollo de este provocó la adaptación al protocolo realmente más extendido que es IPv4.

IPSec puede funcionar en dos modos de operación, modo de transporte y modo túnel. En el primero se cifra la información pero las cabeceras donde se aloja la dirección de destino no, con lo que el cifrado se decide entre el ordenador origen y destino y se intercambian los paquetes ya cifrados entre ellos. En el modo túnel se define un túnel entre dos nodos de la red, se cifran los paquetes enteros y se encapsulan en otro paquete que tiene como dirección destino la salida del túnel. El segundo modo sirve para establecer conexión segura entre dos redes LAN mientras que en el modo de transporte se utiliza para que la conexión sea segura entre dos ordenadores. Es estándar básico IPSec está definido en la recomendación IETF RFC-4301 - Security Architecture for the Internet Protocol, pero tiene muchos más estándares asociados de la propia IETF como se puede ver en la tabla adjunta (solo se muestran los vigentes, ya que ha habido varios que han ido sustituyendo a otros)

Standard	Descripción
RFC 2367	PF_KEY Interface
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2410	The NULL Encryption Algorithm and Its Use With IPsec
RFC 2411	IP Security Document Roadmap
RFC 2412	(sustituye a RFC 1829) The OAKLEY Key Determination Protocol
RFC 2451	The ESP CBC-Mode Cipher Algorithms
RFC 2857	The Use of HMAC-RIPEMD-160-96 within ESP and AH
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3706	A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3715	IPsec-Network Address Translation (NAT) Compatibility Requirements
RFC 3947	Negotiation of NAT-Traversal in the IKE
RFC 3948	UDP Encapsulation of IPsec ESP Packets
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 4301	Security Architecture for the Internet Protocol
RFC 4302	IP Authentication Header

RFC 4303	IP Encapsulating Security Payload (ESP)
RFC 4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
RFC 4306	Internet Key Exchange (IKEv2) Protocol
RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
RFC 4308	Cryptographic Suites for IPsec
RFC 4309	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)
RFC 4478	Repeated Authentication in Internet Key Exchange (IKEv2) Protocol
RFC 4543	The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
RFC 4555	IKEv2 Mobility and Multihoming Protocol (MOBIKE)
RFC 4621	Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol
RFC 4718	IKEv2 Clarifications and Implementation Guidelines
RFC 4806	Online Certificate Status Protocol (OCSP) Extensions to IKEv2
RFC 4809	Requirements for an IPsec Certificate Management Profile
RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 4945	The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

Tabla 30: Estándares RFC asociados al protocolo MPLS

El establecimiento de redes VPN a través de IPSec se puede realizar en ambos modos de funcionamiento, sin embargo el más utilizado es en modo túnel entre entornos para la definición de VPN entre LANS o VLANS.

Cada protocolo tiene una serie de ventajas frente al otro. En el caso de IPSec, su principal ventaja es que al ser un protocolo que funciona con el protocolo IP, su implantación es mucho más rápida al ser el protocolo más extendido del mercado. En el lado negativo IPSec es un protocolo complejo de difícil configuración y es necesaria la configuración desde el cliente.

MPLS por su parte es un protocolo más óptimo a la hora de gestionar el tráfico ya que como se ha comentado anteriormente no necesita desencapsular los paquetes IP para saber la dirección que han de llevar. La configuración se realiza desde la red troncal del proveedor con lo que no es necesaria ninguna configuración dentro de las instalaciones del cliente.

8.6.2 Selección de proveedores

A la hora de seleccionar con qué ISPs se va a trabajar se optó por comparar los ISPs que ya estaban contratados por las centrales de España y de Gran Bretaña, con la única condición que ofreciesen MPLS en todas las fábricas. Con estos criterios los ISPs que entraron en análisis los servicios ofrecidos por BT, Colt y Telefonica.

8.6.3 Matriz de Comparación

Se anexa la matriz de comparación en la que se pueden observar los apartados evaluados para los diferentes proveedores de comunicaciones.

	Proveedores		
Requisitos	TELEFONICA	COLT	BRITISH TELECOM
Presencia Internacional Todos los paises requeridos	Parcial	Total pero con partners	Total
Independencia de linea principal y línea de Backup	No proporciona linea de backup	SI	SI
Disponibilidad	SI	SI	SI
Help Desk y Procedimientos Escalación	SI	SI	SI
Monitorización	Parcial (No cubre todos los requerimientos)	SI, pero como servicio aparte	SI, pero como servicio aparte
Rendimiento	No se cumple en todos los paises	SI	Si
Soporte	No se cumple en todos los paises	Si, pero con partners	SI
Equipo de enrutamiento	SI	SI	SI
SLA´s	NO	SI	SI
Tiempo de entrega	9 meses	8 meses	6 meses
Valor añadido ofrecido por el ISP	Ninguno	Si en el futuro se implementaba un proyecto de Disaster Recovey usando Madrid como Datacenter de Backup ofrecian 20% de descuento.	Descuento de 25%, si en el futuro se implementaba un proyecto de Disaster Recovery usando Madrid como datacenter de Backup

Tabla 31: Matriz de comparación de proveedores de servicio

8.6.4 Fortalezas y debilidades

Análisis de fortalezas y debilidades de Telefónica

Fortalezas	Debilidades
• Es el proveedor actual de las líneas de comunicaciones, previo a la expansión internacional de la empresa. • A nivel local el tiempo de entrega de las líneas de comunicaciones es casi inmediato comparado con el resto de proveedores (apenas 15 días).	• No cubre todos los países en los que se quiere implantar, con lo que no puede ser proveedor común para todos. • Solo proporciona línea de backup a nivel español. • Los requisitos de rendimiento y soporte solo los cumple en determinados países de los que da cobertura. • El tiempo de entrega fuera de España es superior al resto.

Tabla 32: Análisis de Fortalezas y Debilidades para Telefónica

Análisis de fortalezas y debilidades de Colt

Fortalezas	Debilidades
• Proporciona línea de backup del ancho de banda necesario • Tiene presencia en todos los países aunque sea a través de partners • Ofrece descuento en caso de una posterior puesta en marcha del datacenter de backup en Madrid • Cumple con los parámetros de SLA exigidos • Da soporte en todos los países, pero a través de partners	• La presencia y el soporte en algunos países no es directo si no a través de partners, lo que implica que la calidad se puede resentir. • El tiempo de entrega de las líneas es ligeramente mayor al de sus competidores • La monitorización que ofrece es un servicio añadido, con coste a sumar al de la línea en sí.

Tabla 33: Análisis de Fortalezas y Debilidades para Colt

Análisis de fortalezas y debilidades de British Telecom

Fortalezas	Debilidades
• Tiene presencia propia en todos los países. • Proporciona línea de backup del ancho de banda necesario • Ofrece descuento en caso de una posterior puesta en marcha del datacenter de backup en Madrid • Cumple con los parámetros de SLA exigidos • Da soporte en todos los países a través de su propia red de soporte. • El tiempo de entrega es menor al del resto.	• La monitorización que ofrece es un servicio añadido, con coste a sumar al de la línea en sí.

Tabla 34: Análisis de Fortalezas y Debilidades para British Telecom

9 Diseño del proyecto

Se define una configuración de red que servirá como modelo a seguir en cada una de las implementaciones posteriores en fábricas.

9.1 Soluciones escogidas

En el apartado anterior se ha realizado un análisis pormenorizado de varios elementos de la red. A partir de dichos análisis se recomienda a la dirección tecnológica los productos que han de comprar para implementar e instalar la red según las recomendaciones.

En este apartado se propone el producto concreto para cada uno de los apartados anteriores junto con las justificaciones que llevan a escogerlo.

9.1.1 Portal

En el apartado referente a portales, el producto elegido es Citrix puesto que ofrece muchas más funcionalidades que Terminal Server. Los elementos diferenciadores que aporta Citrix son:

- Facilidad de mantenimiento: El software se instala únicamente una vez y a partir de ahí se replica en toda la granja de servidores.
- Escalabilidad: El usuario final solo ve un punto de acceso, independientemente de la cantidad de servidores que haya por debajo. Además el número de usuarios por servidor es el triple que con Terminal Server.
- Las posibles debilidades que pueda tener que son el coste y la instalación inicial no suponen graves dificultades. La dirección tecnológica está convencida de la necesidad del producto y no pone impedimentos para adquirirlo y la instalación es sencilla y prácticamente automática.
- La conectividad con el ordenador cliente y la posibilidad de acceder a discos locales del mismo da mucha flexibilidad de configuración, permite la descarga del mail a local y en general permite el uso de todo aquello que necesite disponer de almacenamiento de manera local evitando usar el disco de manera centralizada salvo para aplicaciones críticas.

9.1.2 Antivirus

El producto elegido en este apartado es McAfee Enterprise V7

Tiene toda una serie de elementos diferenciadores que hacen decantarse por esta solución:

- Es un producto totalmente compatible con la solución de firewalls seleccionada (sonicwall). Es una elección conjunta de ambos elementos.
- A la hora de administrarlo es un único producto y la consola de gestión está integrada con el firewall de Sonicwall.
- Permite disponer de otros servicios en caso de necesidad puesto que integra antivirus, antispyware, firewall personal y antiphising en la misma solución.
- El fabricante ofrece soporte en castellano y además con un menor tiempo de respuesta (4 horas) para resolución de incidencias que los demás fabricantes.
- De todos los fabricantes es la única solución con soporte local a nivel de todas y cada una de las sedes en Europa.
- Es el único producto que permitía tener consolas de gestión en cada sede de manera descentralizadas. De este modo cada administrador tiene la capacidad de ser el responsable de la misma de manera independiente si lo se considera adecuado.
- En las pruebas realizadas sobre tiempo de arranque del sistema y de la aplicación es el producto que presenta mejores cifras de todo el mercado de antivirus evaluado.

9.1.3 Antispam

En lo referente a la solución Antispam, se escoge Sonicwall email security ES6000 como mejor opción a implementar por los siguientes motivos:

- Es una solución totalmente compatible con la solución de correo y antivirus seleccionada (Exchange y McAfee).
- La consola de gestión de Sonicwall permite realizar todas las tareas de mantenimiento y configuración desde una misma interfaz web.
- En un mismo dispositivo físico, este producto integra antivirus y antispyware.
- La empresa dispone para el caso que sea necesario, de soporte en los diferentes idiomas nativos de las regiones que se tiene que cubrir:
  - Castellano
  - Inglés
  - Turco
  - Alemán
  - Francés
  - Griego
  - Rumano
  - Ruso
  - Italiano

- Ofrece también en el departamento de cambios de la opción de NBD (next bussiness day) para este producto.
- La monitorización y el reporting de Sonicwall permite conocer la cantidad de spam, virus y troyanos detectados en el correo electrónico tanto en tiempo real como para realizar un análisis histórico.
- Las pruebas efectuadas fueron la de detectar el mayor porcentaje de spam en el correo simulando diversos ataques de internet. El producto más efectivo fue el appliance de sonicwall.
- La instalación y configuración del appliance sonicwall fue rápida y sencilla.
- A pesar de no ser la opción más económica, la relación calidad/precio es bastante buena.
- EL soporte es multilenguaje y el nivel técnico del personal es bastante fiable.
- La forma de licenciamiento de sonicwall es más sencilla que por ejemplo el de Symantec.

9.1.4 Firewall

El producto elegido en el caso del firewall fue SONICWALL NSA E6500 para la central, para las sedes se elige el modelo concreto en función de las necesidades de ancho de banda. Como principales elementos diferenciadores ofrece:

- La solución Sonicwall es totalmente compatible con la solución de antivirus seleccionada (McAfee).
- Dispone de una solución que ofrece una consola de gestión del firewall sonicwall desde la que es posible la gestión de la consola de antivirus Mcafee.
- El dispositivo físico integra antivirus, antispyware, IPS (sistema de prevención de intrusos), gestor de contenidos web y balanceo de carga por línea en el mismo appliance.
- Al igual que en el caso de Antispam, la empresa dispone para el caso que sea necesario, de soporte en los diferentes idiomas nativos de las regiones que se tiene que cubrir:
  - Castellano
  - Alemán
  - Rumano
  - Inglés
  - Francés
  - Ruso
  - Turco
  - Griego
  - Italiano
- También garantiza el servicio con la opción de NBD (next bussiness day) en todas las sedes.
- Al igual que en el caso de Antivirus, cada firewall puede ser gestionado por el administrador local de cada sede de una manera distribuida o bien desde servicios centrales de manera global. Permite una gestión de seguridad en la consola de gestión de manera que se pueden conceder accesos en modo

lectura o administración total, dependiendo de las necesidades de cada sede.

- El throughput teórico que presenta es el más elevado de los productos comparados.
- La relación calidad/precio de sonicwall en este caso también era la mejor.
- Durante el proceso de selección de los firewalls sólo el equipo técnico de sonicwall colaboraba en todo momento disponible a resolver todas las dudas que aparecían.
- Facilidad de configuración: Con la interfaz web, sonicwall es fácil de configurar, haciéndolo ideal para administradores no muy avanzados. Además cuenta con guías web de rápida y fácil instalación. Este producto también permite la posibilidad de hacer la configuración en modo export/import de un fichero de parámetros de manera que desde la oficina central se puede definir cómo ha de ir configurado y desde allí se envía por correo en un fichero encriptado a las fábricas para que se importe al firewall.
- Tecnología multiprocesador: El producto de Sonicwall ofrece doble procesador multicore Cavium Octeon (x8) gestionado por un sistema operativo propio, con lo que el rendimiento esperado no debería verse limitado por la CPU.
- Control mediante políticas de aplicación: El firewall evaluado es capaz de hacer la identificación y calificación del tráfico de red a partir del contexto, la aplicación y el usuario.
- Gestión centralizada: el fabricante ofrece una opción denominada Global Management System (GMS) que permite realizar la gestión de todos los componentes Sonicwall de la red desde un único punto.
- Informes centralizados: A su vez, desde GMS se puede obtener la información asociada a todos los puntos de la red y realizar un reporting gráfico y numérico de todos los elementos.

9.1.5 ISP

En el caso del ISP a escoger, hay detrás una decisión política de que la relación con los proveedores sea de multiproveedor. Descartando Telefonica por no tener presencia en todos los países donde se necesita, se optó por una solución conjunta entre BT y Colt, ya que según se observa en el análisis de fortalezas y debilidades, el servicio ofertado es muy similar en casi todos los aspectos. En referencia al coste ni siquiera aparece en la comparativa por ser el mismo coste entre los tres proveedores.

Por ello la solución que se adopta es tener el Datacenter productivo en Barcelona en manos de Colt y el futuro Datacenter de backup se montará en Madrid en las

instalaciones de BT. Además se decide realizar una diferenciación entre líneas existentes y nuevas líneas a implementar. Las líneas existentes serán gestionadas por Colt y las nuevas líneas de comunicaciones que se tengan que implementar serán gestionadas por BT.

Se acuerda en ambos casos la monitorización que se va a realizar de los sistemas por parte del proveedor de servicio, que se detallará en la sección de protocolo.

Por otro lado se decide tener una línea extra de backup contratada con un proveedor local, con la prioridad de mantener el proveedor que la fábrica pudiera tener con anterioridad.

9.2 Topología de red interna

En este apartado se definen todos los elementos que van a formar parte de la red LAN de cada fábrica, tanto elementos físicos como elementos lógicos.

En el siguiente esquema se muestra la topología que se va a implementar para una nueva fábrica en Italia:

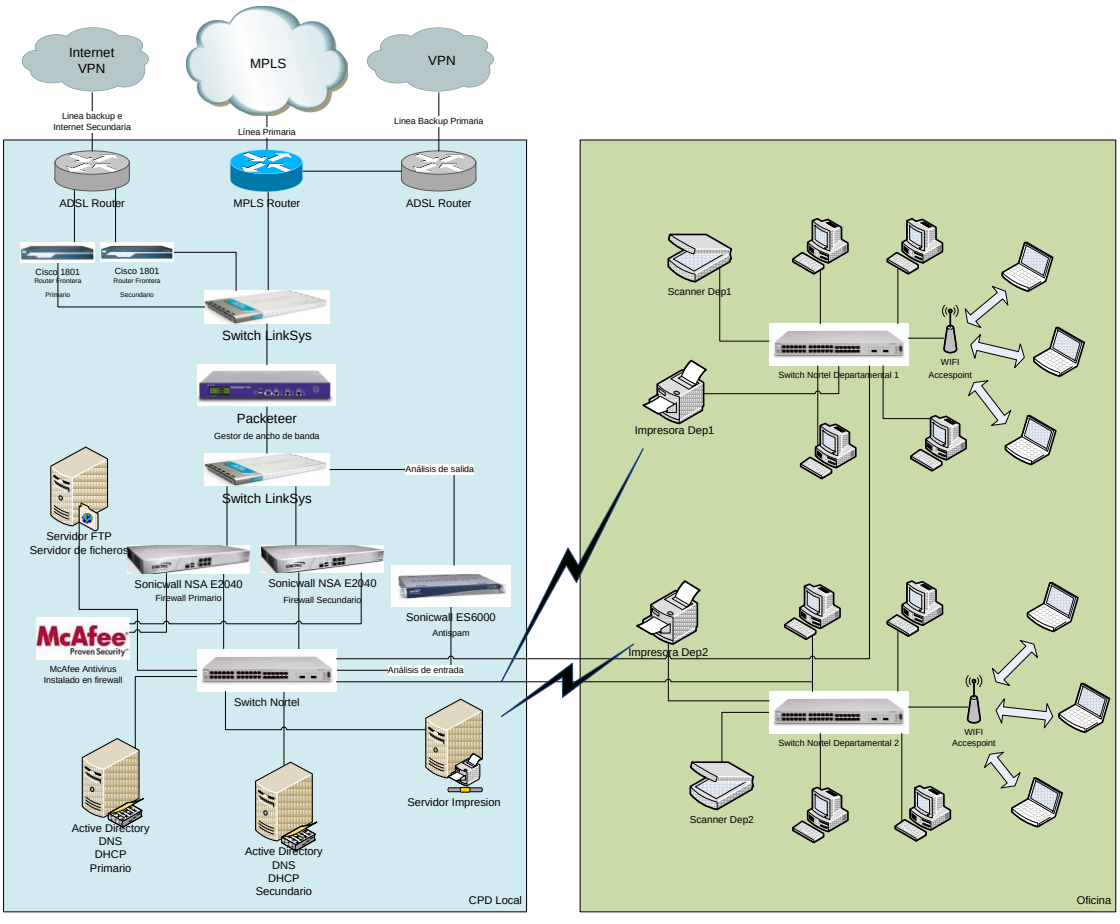

Ilustración 18: Topología Interna definida

Como se puede ver, se disponen de diferentes elementos, los que se consideran más importantes con backup y el resto como elementos únicos.

En la siguiente figura se pueden ver las interconexiones entre los elementos instalados dentro del CPD:

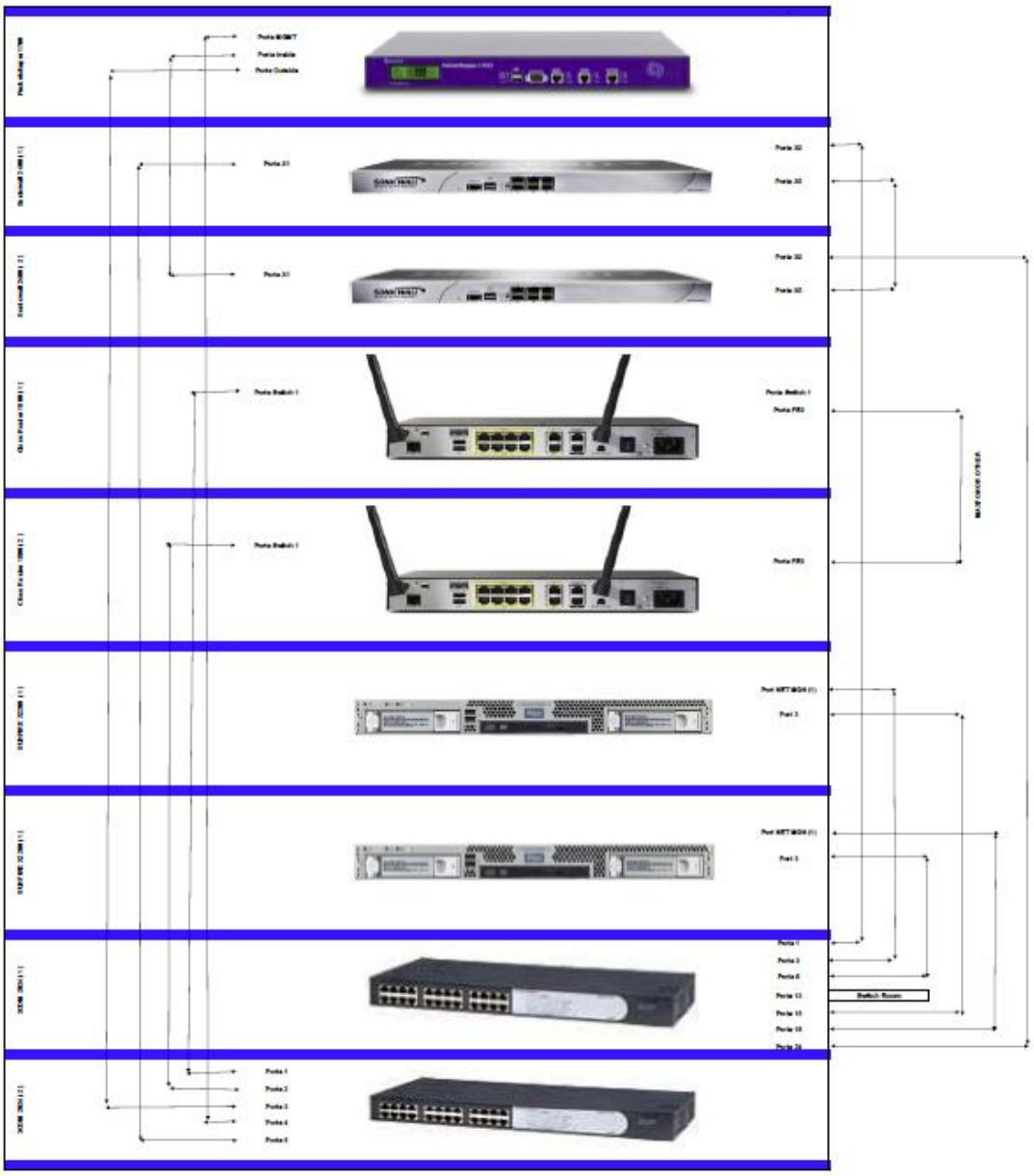

Ilustración 19: Interconexiones entre componentes

Líneas de comunicaciones

Se define una triple conexión con el exterior a través de tres líneas diferentes:

- Conexión MPLS: La línea principal o primaria es la línea que operará en circunstancias normales. Es una línea con protocolo MPLS conectada con el

CPD central en Barcelona y operada por British Telecom, pues se trata del diseño para una nueva fábrica. La capacidad necesaria para esta red se calcula en el apartado de 5.4 de estimación de capacidades. La conexión con el mundo MPLS está bajo responsabilidad de BT y lo establece con una línea de fibra dedicada.

- Conexión de backup Primaria: Es la conexión que se utilizará en caso de caída de la red principal. Esta conexión está tunelizada con un protocolo VPN hacia el CPD central y también estará operada por BT. Se realizará a través de un ADSL convencional.

- Conexión de backup secundaria: en este caso, la diferencia con la conexión de backup primaria es que tiene la posibilidad de salida directa a internet además del túnel VPN con central. De esta manera si hubiera una caída del CPD central se permite cuanto menos el tráfico desde Internet. También está pensada la posibilidad de dar salida a administradores o gente autorizada que no tenga la obligación de pasar por el proxy de servicios centrales. Como añadido, se decidió que para tener backup en caso de caída general de BT, esta conexión se contratase con los operadores locales de cada país. En el caso italiano se gestiona con Telecom Italia ya que era el operador que hasta el momento estaba dando servicio a la fábrica. Se mantiene el formato ADSL convencional que se estaba utilizando hasta el momento.

Firewall

El Firewall se instala por duplicado, con uno de ellos trabajando como primario y con otro idéntico preparado para actuar automáticamente en caso de caída del primero. En el firewall irá instalado el antivirus y realizará además las tareas UTM, es decir, antispyware, IPS y control de contenidos.

Routers ISP

Los routers ISP son los routers que proporciona el proveedor de servicios que realizan la conexión con el exterior y la adaptación al tráfico de internet de los paquetes que circulan por ellos.

Routers Frontera

El Router frontera es donde se decide, utilizando reglas de verificación de estado de las redes, el camino de salida de la información, enviando todo el tráfico a través de la línea primaria en condiciones normales y desviando el tráfico a las secundarias en función de los elementos que hayan caído. En este caso el modelo

que se implanta es el Cisco 1801. Se disponen dos routers, actuando uno como principal y el otro para el caso de caída del primero.

Switches

Se instalan diferentes switches en diferentes puntos que permitan implementar todas las interconexiones necesarias en la red:

- Switch de entrada: Es un switch de marca LinkSys que se sitúa entre los routers de salida a Internet y el gestor de ancho de banda. En este switch están también conectados los routers de frontera.
- Switch de compresión: Este switch también es de marca LinkSys y está situado entre el gestor de ancho de banda o compresor y los firewalls barrera del CPD.
- Switch central: Este switch, de marca Nortel, realiza la interconexión entre los principales elementos del CPD y los switches departamentales.
- Switches departamentales: Este es el último punto de distribución. Conecta el CPD con los ordenadores de los usuarios. También está conectado a un punto WIFI utilizado especialmente por los ordenadores portátiles. Independientemente de si el ordenador del usuario es portátil o fijo, todos los puestos de trabajo disponen de toma de red conectada al switch departamental y de una toma de red sin conectar para poder ser utilizada en caso de fallo de la primera.

Gestor de ancho de banda

El gestor de ancho de banda de marca Packeteer se sitúa por delante del firewall para que en el lado de conexiones con el exterior esté todo el tráfico ya comprimido salvo el que salga a Internet directamente por la salida secundaria. Lo distingue en función del protocolo de comunicación y del puerto utilizado.

Antivirus

Como se comentó en el momento de la elección del producto para antivirus, el software de McAfee va instalado en el Firewall. Por ello funciona de la misma manera, es decir, está duplicado y en caso de caída de uno se activa el otro.

Antispam

El dispositivo de antispam tiene redundancia por la ubicación escogida. Está instalado de manera que se conecta para analizar el tráfico de salida al switch de compresión y al switch central para analizar el tráfico de entrada, de manera que al pasar todo el tráfico por el firewall este ya realiza un primer filtrado antispam.

Servidor de Active Directory

En este caso este servicio si tiene redundancia, está instalado también de manera que uno de ellos actúa como principal y el otro como secundario. Este dispositivo físico tiene activado además el servicio de DNS y DHCP, tanto en el principal como en el secundario, de manera que todos ellos están en el sistema de manera redundante.

Servidor de ficheros y FTP

A la hora de poner un servidor de ftp y ficheros se opta por instalar ambos servicios en un mismo dispositivo físico al ser servicios complementarios. A la hora de acceder a ficheros guardados se puede acceder vía recurso compartido o bien a través de ftp, con lo que tiene sentido que si el dispositivo dispone de la potencia hardware necesaria y de una gran capacidad de almacenaje se realicen ambas funciones desde el mismo sitio.

Servidor de Impresión

Desde un único servidor de impresión se gestionan todas las impresoras de la oficina. Este servidor está conectado al switch central y realiza la gestión de las mismas a través de un protocolo TCP/IP, sin estar conectado físicamente a ellas.

Impresoras

Hay una impresora en cada departamento conectada al switch departamental y ubicada de manera cercana y accesible al personal del departamento. La gestión de las mismas, como se ha comentado en el punto anterior la realiza de manera centralizada el servidor de impresión.

Escáneres

Al igual que en el caso de las impresoras hay un escáner en cada departamento. En este caso son dispositivos con dirección IP y visibles desde los ordenadores de los usuarios del departamento.

Punto de acceso WIFI

En cada departamento se dispone de al menos un punto de acceso WIFI para que los usuarios que dispongan de ordenador portátil puedan estar conectados sin necesidad de cables en salas de reuniones o bien directamente en su lugar de trabajo.

9.3 Topología de red global

La topología de red global es la estructuración de la red que se tiene, teniendo en perspectiva todas las sedes de la empresa. Desde el punto de vista global se asignaron todos los rangos de IP para cada una de las sub-redes locales.

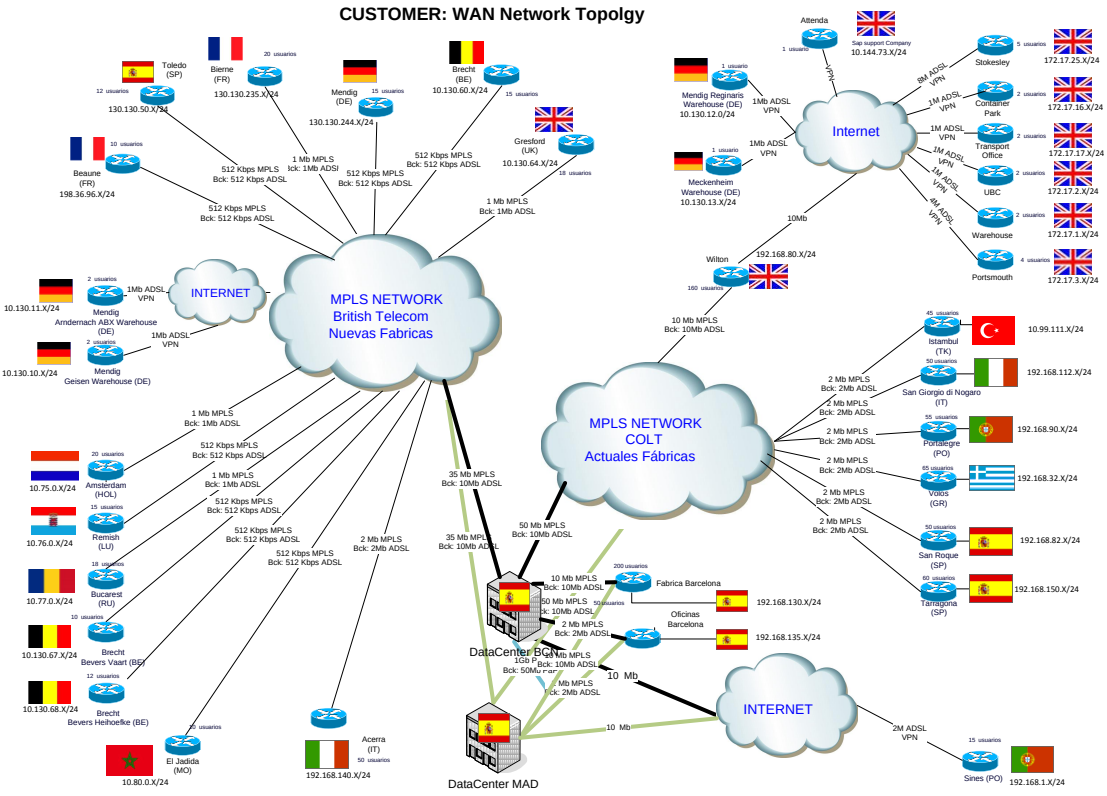

Ilustración 20: Topología Global definida

De la gráfica destacar una serie de consideraciones:

- La situación mostrada corresponde al momento de finalización de la colaboración con el proyecto del cliente. En ese momento no todas las sedes se conectan siguiendo las recomendaciones proporcionadas en el presente proyecto
- La conexión de las fábricas ya existentes se realiza a través de MPLS bajo la red de COLT.
- La conexión de las fábricas recién adquiridas se realiza a través de MPLS bajo la red de BT.
- El CPD de Madrid tiene las mismas conexiones que el CPD de Barcelona y además están conectados entre sí.
- Hay dos fábricas nuevas en Alemania pendientes de incorporar a las recomendaciones. En el momento de la foto seguían utilizando conexión a través de ADSL con VPN para llegar a la red central.

- Las sedes ya existentes en Inglaterra utilizan la conexión a través de una de ellas, la sede más importante tras la de Barcelona y que tiene consideración similar a la de servicios centrales. Por ello la conexión entre esta sede y la de Barcelona ha de tener en cuenta el tráfico del resto de sedes. Además ninguna de estas sedes ha tenido en cuenta todavía las recomendaciones del presente proyecto.
- Destacar que el ancho de banda de la conexión troncal del CPD con la red MPLS ha de ser mayor o igual que la suma de todos los anchos de banda de las sedes que vayan a circular por ella para poder garantizar que entre todas las sedes y el CPD hay el ancho de banda MPLS contratado.

Las velocidades detalladas para cada una de las conexiones de las sedes se calculan en el siguiente apartado de dimensionamiento.

9.4 Capacidad del sistema

En base a los elementos que contempla la red estudiados en los puntos anteriores y teniendo en cuenta las diferentes variables que influyen en cada caso se define para diferentes parámetros una estimación de recursos mínimos de los que deberá disponer en cada caso.

En concreto se realizará el cálculo para la fábrica italiana ubicada en Acerra. Esta fábrica tiene en el momento del dimensionamiento 33 usuarios, pero se cree por parte del cliente que puede crecer en breve con lo que los cálculos se realizan para 50 usuarios. La estructuración de estos 33 usuarios es en 6 departamentos con un máximo de 8 personas por departamento.

Dimensionamiento CPD: A continuación se muestra la tabla estudiada en el punto 2.1.1 para valorar la potencia necesaria. Según se evalúa caben todos los dispositivos dentro de un mismo Rack y en la tabla adjunta se pueden ver el estudio de la capacidad de alimentación necesario:

RACK A		SAI A			SAI B			TOTAL		
Servidor / Dispositivo	Modelo	Numero Enchufes	Consumo Máximo (W)	Consumo Máximo (A)	Numero Enchufes	Consumo Máximo (W)	Consumo Máximo (A)	Numero Enchufes	Consumo Máximo (W)	Consumo Máximo (A)
Router MPLS		1	15,00	1,50						
Router Backup 1		1	12,00	1,20						
Router Backup 2		1	12,00	1,20						
Router Frontera	Cisco 1801	2	15,00	1,50						
Switch	Lynsys	2	20,00	1,00						
Gestor Ancho Banda		1	25,00	2,50						
Firewalls	Sonicwall NSA E6500				2	130,00	8,00			
Switch	Nortel				2	270,00	5,00			
Servidor ficheros					1	150,00	2,00			
Active Directory								2	300,00	5,00
Antispam								1	250,00	4,00
Servidor Impresión								1	150,00	3,00
Switch departamental								6	810,00	15,00
Total		8	99,00	8,90	5	550,00	15,00	10	1510,00	27,00
Máximo		16	3600,00	16,00	16	3600,00	16,00	32	7200,00	32,00
Diferencial		8	3501,00	7,10	11	3050,00	1,00	22	5690,00	5,00

Tabla 35: Dimensionamiento del RAC de Italia

Ancho de banda de la red MPLS: Para realizar el cálculo de la velocidad se aplica la fórmula detallada en el apartado de estimación de capacidades:

- Consumo de conexión Citrix: 20Kbps. Es un dato ofrecido en las especificaciones de Citrix.
- Número de conexiones Citrix en paralelo por usuario: En el caso de Italia 4 conexiones, una para SAP, descarga de ficheros, Internet Explorer y correo electrónico.
- Número de usuarios: 50 usuarios
- Porcentaje de usuarios en paralelo: Se calcula que un 70% de los usuarios estarán trabajando en paralelo. Este ratio se aplica para todas las sedes.
- Ratio de compresión del gestor de ancho de banda: El ratio que consigue Packeteer es aproximadamente de 35%.
- Ancho de banda extra: Se aplica un ratio del 1,5 sobre el cálculo.

$$BW = 20Kbps * 4 * 50 * 0,7 * 0,35 * 1,5 = 1470Kbps$$

Ecuación 1: Cálculo del ancho de banda de red

Se escogen 2Mbps pues es la mínima oferta comercial que ofrece el proveedor de servicios que se adapta a las necesidades calculadas.

En la siguiente tabla se pueden observar los valores de las diferentes conexiones correspondientes al gráfico de red global

					Cálculo de ancho de banda		
SEDES	**Antigüedad**	**Red Actual**	**Direccionamiento**	**Standard**	Número de usuarios	Ancho de banda mínimo (Kbps)	Red Resultante
Gresford	Nueva	MPLS - BT	10.130.64.X/24	SI	18	529,2	1 M
Brecht	Nueva	MPLS - BT	10.130.60.X/24	SI	15	441	512 Kb
Mendig	Nueva	MPLS - BT	130.130.244.X/24	SI	15	441	512 Kb
Bierne	Nueva	MPLS - BT	130.130.235.X/24	SI	20	588	1 Mb
Toledo	Nueva	MPLS - BT	130.130.50.X/24	SI	12	352,8	512 Kb
Beaune	Nueva	MPLS - BT	198.36.96.X/24	SI	10	294	512 Kb
Mendig Arndernach ABX Warehouse	Nueva	Internet VPN	10.130.11.X/24	NO	2	58,8	128 kb
Mendig Geisen Warehouse	Nueva	Internet VPN	10.130.10.X/24	NO	2	58,8	128 kb
Amsterdam	Nueva	MPLS - BT	10.75.0.X/24	SI	20	588	1 Mb
Remish	Nueva	MPLS - BT	10.76.0.X/24	SI	15	441	512 Kb
Bucarest	Nueva	MPLS - BT	10.77.0.X/24	SI	18	529,2	1 Mb
Brecht Bevers Vaart	Nueva	MPLS - BT	10.130.67.X/24	SI	10	294	512 Kb
Brecht Bevers Heihoefke	Nueva	MPLS - BT	10.130.68.X/24	SI	12	352,8	512 Kb
El jadida	Nueva	MPLS - BT	10.80.0.X/24	SI	10	294	512 Kb
Acerra	Nueva	MPLS - BT	192.168.140.X/24	SI	50	1470	2 Mbps
Enlace Troncal BT					**229**	**6732,6**	**35 Mbps**

Sines	Actual	Internet VPN	192.168.1.X/24	NO	15	441	512 Kb
Tarragona	Actual	MPLS - COLT	192.168.150.X/24	SI	60	1764	2 Mbps
San Roque	Actual	MPLS - COLT	192.168.82.X/24	SI	50	1470	2 Mbps
Volos	Actual	MPLS - COLT	192.168.32.X/24	SI	65	1911	2 Mbps
Portalegre	Actual	MPLS - COLT	192.168.90.X/24	SI	55	1617	2 Mbps
San Giorgio di Nogaro	Actual	MPLS - COLT	192.168.112.X/24	SI	50	1470	2 Mbps
Istambul	Actual	MPLS - COLT	10.99.111.X/24	SI	45	1323	2 Mbps
Warehouse	Actual	Internet VPN	172.17.1.X/24	NO	2	58,8	128 kb
UBC	Actual	Internet VPN	172.17.2.X/24	NO	2	58,8	128 kb
Transport Office	Actual	Internet VPN	172.17.17.X/24	NO	2	58,8	128 kb
Container Park	Actual	Internet VPN	172.17.16.X/24	NO	2	58,8	128 kb
Stokesley	Actual	Internet VPN	172.17.25.X/24	NO	5	147	256 kbps
Portsmouth	Actual	Internet VPN	172.17.3.X/24	NO	4	117,6	128 kb
Attenda	Actual	Internet VPN	10.144.73.X/24	NO	1	29,4	128 kb
Mendig Reginaris WH	Actual	Internet VPN	10.130.12.0/24	NO	1	29,4	128 kb
Meckenheim Warehouse	Actual	Internet VPN	10.130.13.X/24	NO	1	29,4	128 kb
Wilton	Actual	MPLS - COLT	192.168.80.X/24	SI	160	4704	10 Mbps
Enlace Troncal COLT					**520**	**15288**	**50 Mbps**
Fábrica Barcelona	Actual	MPLS - COLT	192.168.130.X/24	SI	200	5880	10 Mbps
Oficinas Barcelona	Actual	MPLS - COLT	192.168.135.X/24	SI	50	1470	2 Mbps

* Las velocidades resultantes marcadas en naranja corresponden a la velocidad teórica.
Al no estar dentro de las recomendaciones no cuadran con el valor del gráfico real

Tabla 36: Asignación de rangos IP del esquema global

Ancho de banda de la red de backup primaria: Aplican los mismos cálculos que se aplican para la red principal pero se busca una alternativa de menor coste. **En este caso se escoge una conexión ADSL asimétrica, se asigna la misma velocidad de bajada, 2Mbps, pero por tema de coste se decide coger una opción con 300Kpbs de subida.**

Ancho de banda de la red de backup secundaria: De manera similar al caso anterior, se busca una opción de menor coste que la principal. Es ligeramente la velocidad de subida que en el caso de la línea de backup primaria por su uso como salida alternativa a internet para determinados usuarios. **La opción contratada**

en este caso es una velocidad asimétrica de 2Mpbs de bajada y 512Kbps de subida.

En todas las conexiones de backup para el resto de la red global se aplica una política similar, se utiliza un ADSL de la misma velocidad de bajada pero menor velocidad de subida.

Throughput mínimo del firewall: El modelo de firewall escogido en el apartado 5.1 atiende al firewall que irá ubicado en servicios centrales. El modelo exacto de cada sede ha de asegurar que tiene una capacidad suficiente para servir al número de usuarios que tenga dicha sede. El cálculo para dicha capacidad es muy similar al del ancho de banda de la red salvo que como se puede observar en la topología está ubicado tras el gestor de ancho de banda, por lo que el ratio aplicado no se puede utilizar.

$$BW = 20Kbps * 4 * 50 * 0,7 * 1,5 = 4,200Mbps$$

Ecuación 2: Cálculo del throughput del Firewall local

Es decir en este caso será necesario que el throughput mínimo del firewall local sea de 4,2Mbps

De igual manera se verificó que el throughput estimado para el firewall central era inferior al throughput teórico del modelo evaluado. Teniendo en cuenta que a nivel global se espera tener unos 400 usuarios repartidos entre todas las sedes, el valor resultante quedaría:

$$BW = 20Kbps * 4 * 400 * 0,7 * 1,5 = 33,6Mbps$$

Ecuación 3: Cálculo del throughput del Firewall central

Lo cual queda bastante por debajo del throughput teórico del aplicativo (220Mbps).

Puntos de red necesarios: A la hora de calcular los diferentes puntos de red que habrá en el sistema se tendrá en cuenta que a todos los usuarios se les asignará dos puntos de red, uno para el equipo fijo y otro para el caso de que necesiten conectar un portátil o simplemente para que tengan un backup en caso de problemas con alguno de ellos.

Además se ha de tener en cuenta todas las conexiones necesarias para el resto de elementos de la red. En la tabla adjunta se ven los valores del número mínimo de conexiones necesarias.

	Switches			
Conexiones	Entrada	Compresión	Central	Departamental
Router MPLS	1			
Router Frontera Primario	1			
Router Frontera Secundario	1			
Packeteer	1	1		
Firewall Primario		1	1	
Firewall Secundario		1	1	
Antispam		1	1	
Servidor FTP de ficheros			1	
Active directory Primario			1	
Active directory Secundario			1	
Servidor de Impresión			1	
Switches Departamentales			6	
Switch Central				1
Punto de Acceso WIFI				1
Impresora				1
Scanner				1
Usuarios por departamento X 2 *				16
Capacidad Mínima requerida	**4**	**4**	**13**	**20**

* Se tiene en cuenta el número de usuarios del departamento mayor

Tabla 37: Dimensionamiento de conexiones necesarias

Puntos de Acceso a Red:

Servidor de ficheros: A la hora de calcular el espacio necesario para alojar ficheros en el servidor se va a optar por un cálculo de cuotas compartidas. Es decir, se calcula una cuota máxima para los usuarios pero el disco disponible será menor de la multiplicación de usuarios por cuota máxima pues se prevé que no todos los usuarios ocuparán su espacio al máximo si no que en media ocuparán un volumen determinado. Asimismo se tendrá en cuenta el uso de dispositivos de almacenamiento fácilmente escalables para poder ampliar la capacidad de manera sencilla y económica sin tener que sustituir el equipo si no simplemente ampliándolo. Para tener además redundancia de seguridad se quiere configurar el disco en Raid 5. Las variables del cálculo son las siguientes:

- La cuota máxima designada por usuario es de 50Gb en recurso compartido.
- La estimación de uso por parte de usuarios es del 60%
- El número de usuarios es 50
- El ratio para implementar un Raid 5 es de 5/4

El cálculo resultante queda:

$$Tamaño = 50\,Gbytes\ /\ usuario * 0{,}6 * 50 * 1{,}25 = 1875\,Gbytes$$

Ecuación 4: Tamaño de disco necesario

Viendo los productos comerciales que hay en el mercado, la unidad mínima que se puede adquirir es de 2Tbytes. En el caso del cliente proporciona la posibilidad de disponer de dispositivos del fabricante IOMEGA. Se escoge para la implantación en Italia el modelo StorCenter ix2-200 de 2Tbytes, ampliable hasta 4Tbytes.

9.5 Procedimientos

En este apartado de procedimientos se detalla toda una serie de procesos a seguir tanto para la implantación del proyecto como para el correcto desarrollo del mismo.

9.5.1 Ciclo de vida del proyecto

Todo proyecto ha de tener un ciclo de vida desde su concepción inicial hasta el traspaso final y la firma de fin de proyecto. En este caso se establece el ciclo de vida que han de seguir todas las implantaciones que se realizarán.

Es importante destacar que la instalación no se realiza desde cero, pues la fábrica ya dispone de una infraestructura funcionando. Lo que se debe hacer es verificar que la instalación cumple las especificaciones y gestionar con el equipo de técnicos de instalación las modificaciones necesarias para poder instalar y configurar los equipos según las especificaciones.

Para realizar la planificación del proyecto se realiza un análisis FETA (Fases, Etapas, Tareas y Actividades) para estructurar el proyecto por partes y poder definir fechas y recursos necesarios para cada una de estas partes. Las fases principales son:

1) Fase Previa: En esta fase se fijan la fecha de inicio, el responsable del proyecto, la empresa consultora que va a participar, se firma la propuesta de servicio por parte de dicha empresa consultora y se realiza un acta con una enumeración de requerimientos del proyecto. Además se realizan las peticiones de servicio a los proveedores ISP y se verifica el stock de dispositivos en servicios centrales solicitando todos los que sean necesarios a los diferentes fabricantes. Esta fase previa ha de suceder con al menos un mes de antelación del resto de fases.

2) Fase de Preparación del Servicio: esta fase del proyecto se divide en dos etapas, una a cargo del equipo de consultoría, la etapa de kick-off o punto de partida, y por otro lado una etapa a cargo del cliente que es la validación de las conclusiones obtenidas en la fase de kick-off.

   a) Etapa de Kick-Off: Durante la etapa de kick-off o puesta en marcha del proyecto, se concretan los requerimientos que tiene la fábrica en concreto en cuanto a servicios que van a cubrir por citrix, número de usuarios, número de departamentos, etc. Se realiza una planificación detallada de cada una de las tareas [17] y se levanta la correspondiente acta de puesta en marcha.
   b) Etapa de Validación de Requerimientos: Se entrega al cliente todos los requerimientos detallados en el punto anterior y el cliente valida o renegocia los aspectos que crea conveniente.

3) Fase de Realización del Servicio

   a) Etapa de investigación y auditoría: Se verifican los requerimientos que aplican sobre el terreno y se estudia las características de la sede en concreto realizando un estudio de campo para poder acabar de perfilar los requerimientos contrastándolos con los proporcionados inicialmente.
   b) Etapa de propuesta de solución: Se realiza una propuesta con todos los componentes ya detallados en cuanto a modelos exactos, dimensionamientos, estructura, etc.
   c) Etapa de implantación de la solución: Con la propuesta previa ya aceptada se pasa a la implantación en sí. Esta etapa se divide en varias tareas:

      i) Comunicaciones: en lo que a comunicaciones se refiere se han de conectar y validar las tres líneas de comunicación, la principal MPLS con BT y las dos de backup, una con BT y otra con Telecom Italia
      ii) Instalación de Switches y puntos de acceso: Esta tarea es la puesta en marcha y verificación de funcionamiento de los switches del CPD y los puntos de acceso wifi de la fábrica y oficinas.
      iii) Instalación de Firewall: La tarea de puesta en marcha del firewall incluye la puesta en marcha del primario y del secundario, la configuración de ambos teniendo en cuenta la configuración de las reglas en sí del firewall, la puesta en marcha del motor antivirus, la configuración de antispyware y la configuración IPS. A destacar en este punto que para la configuración del antivirus hay que activar la opción de licencia compartida. De esa manera el firewall se conecta al firewall central y reserva el número de licencias que necesite la sede.
      iv) Instalación de Packeteer: Instalación y compresión del gestor de ancho de banda, definiendo los segmentos de ancho de banda y prioridades de tráfico.

v) Despliegue de antivirus: En esta tarea se tienen en cuenta todas las actividades para instalar el antivirus cliente en los ordenadores cliente de los usuarios, entre ellas la distribución del software al responsable del servicio de atención informática a usuarios y la creación y distribución de un manual específico de instalación con los parámetros de la sede.
vi) Instalación del resto de servidores: En esta tarea se incluye la instalación y configuración del servidos antispam, Active directory, servidor de ficheros, servidor de impresión, impresoras y escáner.

4) Fase de Pruebas: En la fase de pruebas se realizan pruebas puntuales de todos los elementos que se han instalado y configurado en el punto anterior.
5) Fase de Verificación de la solución: La fase de verificación es una fase de pruebas pero extendida un mínimo de cinco usuarios para que realicen pruebas simultáneas.
6) Fase de Gestión del Cambio: En esta fase se documentan todos los cambios respecto a la infraestructura anterior y se definen reuniones de traspaso al equipo técnico de la sede.
7) Fase de Conclusión: En la fase de conclusión se realiza una documentación detallada de la configuración y de funcionamiento del sistema y se firma el documento de finalización y aceptación del proyecto, junto con los albaranes para la facturación del mismo.

El detalle de todas las fases con todas las tareas se puede observar en el documento adjunto ***Ciclo_de_vida_proyecto_Fábricas.mpp*** [17].

9.5.2 Definición de Servicio de los ISP

Si bien en el resto de componentes el servicio de soporte es importante para el caso de incidencias, en el caso de los ISP se vuelve determinante puesto lo que se adquiere no es un producto si no un servicio del cual se ha de garantizar su calidad y su correcto funcionamiento.
Para ello se acuerda con los proveedores de ISP el nivel de servicio de han de proporcionar un servicio de HelpDesk al que poder dirigirse en caso de tener una incidencia, se definen la monitorización que ha de realizar sobre el sistema de comunicaciones y por último también se define la gestión que se ha de realizar de las incidencias que puedan aparecer y del servicio proporcionado.

Servicio de Service Desk

Se requiere que la empresa disponga de un servicio de atención al cliente con atención telefónica y por e-mail 24x7. El servicio de Service Desk se requerirá

que cumpla con los procedimientos de ITIL en concreto los relatados en el libro de Gestión del Servicio.

En la siguiente figura podemos ver cual es la definición de gestión de servicio según el libro de referencia [18]

> *La **Gestión de Servicios** es un conjunto de capacidades organizativas especializadas cuyo fin es generar valor para los clientes en forma de servicios.*

Ilustración 21: Definición de Gestión del Servicio

En la imagen mostrada a continuación se puede ver el flujo que siguen las incidencias en un sistema de gestión ITIL.

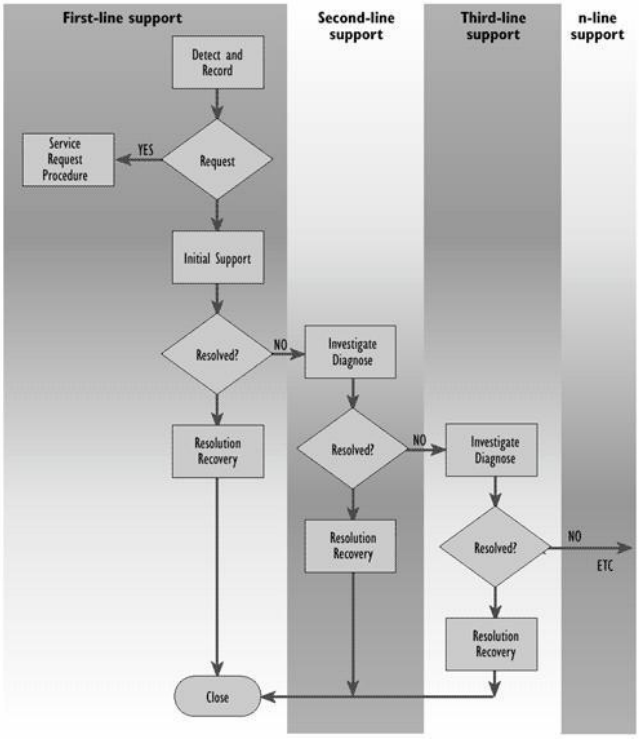

Ilustración 22: Flujo de tratamiento de incidencias ITIL

Es importante destacar que el equipo de Service Desk ha de disponer de una base de datos de conocimiento centralizada para poder disponer de la metodología de resolución, detectar incidencias repetidas que puedan llegar por diferentes canales y tener conocimiento en todo momento de las incidencias abiertas y su estado. Dicho servicio se encargará de las siguientes tareas:

- Recibir, registrar y priorizar las incidencias recibidas tanto por correo como por teléfono.
- Realizar un control y seguimiento de todas las incidencias.

- Remitir las incidencias al grupo encargado de solucionarlas en cada caso.
- Informar al solicitante del estado, prioridad asignada y tiempo máximo de resolución.
- Mantener actualizada la base de datos de conocimiento y gestión de incidencias.
- Cerrar las incidencias cuando estén solucionadas.
- Realizar informes mensuales con un resumen de las incidencias detectadas, origen, motivo y tiempo de resolución.

Los diferentes niveles de severidad para poder priorizar las incidencias serán los mostrados en la siguiente tabla.

Criticidad	Descripción
Severidad 1	Pérdida de servicio total. Los usuarios no pueden acceder al servidor o al tiempo de respuesta es tan elevado que la sensación para el usuario es que no puede trabajar. No existe mecanismo alternativo.
Severidad 2	Pérdida parcial de servicio. Entre un 20% y 30% de los usuarios, no pueden acceder al servidor o el servicio se presta con degradación a través de un método alternativo.
Severidad 3	No hay pérdida de servicio o el servicio se está prestando por un medio o solución alternativa. Los usuarios no se ven afectados de manera colectiva.
Severidad 4	Se utiliza para diversidad de situaciones relacionadas con el servicio y que no son una avería. Por ejemplo consultas de clientes sobre el servicio, características, etc.

Tabla 38: Severidades de incidencias en el servicio

Monitorización

Los objetivos de la monitorización es asegurar que los servicios que se definan están disponibles 24x7 y detectar las incidencias si es posible incluso antes que el cliente, dando sensación de reactividad ante el servicio ofrecido.

Los objetivos principales de esta monitorización serán:

- Monitorizar en tiempo real la disponibilidad de los servicios
- Monitorizar en tiempo real determinadas capacidades del sistema asegurando que se mantienen dentro de unos umbrales determinados
- Ejecución diaria de las tareas que se determinen para asegurar la disponibilidad de elementos que no puedan tener una monitorización continuada.

Los servicios y tareas objeto de monitorización que se establecen como mínimo para las sedes por parte del ISP se muestran en la siguiente tabla.

Origen	Monitorización
Monitorización MPLS	
MPLS	Detección de pérdida de conectividad entre central y delegación

MPLS	Caída de interfaz en central
Monitorización ADSL de Backup	
ADSL Backup	Detección de caída del caudal ADSL
ADSL Backup	Detección de pérdida de conectividad
Monitorización de servicios de Internet	
Internet	Detección de pérdida de rendimiento en los servicios Internet del cliente. Respuesta de conexión >1s
Internet	Detección de caída del caudal Internet en central
Monitorización de los routers ADSL y MPLS	
Router	Detección del aumento de la carga de la CPU en el router por encima del 95% durante más de 5 minutos
Router	Detección del aumento de carga en el enlace WAN del router por encima del 60% durante más de 10 minutos
Router	Detección de caída del interfaz de LAN del router
Monitorización de los servicios de voz	
Voz	Detección de caída del enlace de voz

Tabla 39: Elementos a monitorizar por el ISP

Las incidencias han de quedar registradas dentro de la misma base de incidencias de HelpDesk de manera que aparezcan de manera conjunta en el informe mensual.

Gestión de incidencias

Los pasos por los que ha de seguir toda incidencia, ya sea abierta por el cliente a través del equipo de HelpDesk o ya sea abierta por el proveedor a partir de una alerta de monitorización ha de seguir siempre los mismos pasos:

- Alta de la incidencia en el sistema.
- Asignación de severidad y de equipo responsable
- En caso de severidades 1 y 2 comunicación al cliente por correo electrónico sobre la incidencia incluyendo el responsable.
- Intento de resolución
- En caso afirmativo comunicación al cliente con información acerca de la solución y el tiempo de resolución de la misma
- Si no se puede encontrar solución definitiva y es de severidad 1 o 2 intentar buscar alternativa que permita rebajar la severidad
- Escalado de la incidencia al equipo de soporte avanzado
- Registro de toda actividad en la base de datos para su posterior seguimiento y análisis.

Gestión de servicio

El proveedor ha de proporcionar un servicio ágil y adecuado a las necesidades del proyecto. Para ello se definen una serie de requisitos que ha de cumplir la gestión del servicio proporcionado:

- Punto de contacto único para la gestión de servicio.
- Punto de contacto de backup.

- Si hay algún cambio planificado o sustitución temporal planificada del punto de contacto para el servicio o de su backup ha de avisar con 15 días de antelación.
- El gestor del servicio ha de proporcionar al cliente los informes mensuales acordados en los puntos anteriores
- También se ha de encargar de comprobar que los indicadores de calidad del servicio se mantienen en los establecidos y en caso de haber anomalías ha de poder justificarlas.
- Ha de revisar las incidencias graves o repetitivas para mejorar el servicio ofrecido.
- Ha de gestionar además del servicio los componentes ofrecidos por el proveedor, en caso de necesidad de cambio de algún componente físico ha de gestionar dicho cambio intentando que se produzca dentro de los márgenes acordados.

10 Pruebas de calidad de las recomendaciones

Una vez se ha implantado la solución en Italia, se verifican las recomendaciones para comprobar que no hay problemas de rendimiento o de alguno de los procedimientos.

10.1 Monitorización de disponibilidad de las comunicaciones

Se establece un reporting mensual con el proveedor de comunicaciones en el que envía la información asociada a disponibilidad de la red. En base a ese reporting se evalúa la calidad de la solución.

El reporting consiste en un listado de las incidencias que ha habido durante todo el mes que muestra el tiempo de indisponibilidad, la afectación y el tiempo medio de recuperación de la línea:

Código: 00202 Enero 2009

Averia	Núm. Averia	Fecha Creacion Caso	Severidad	Municipio de Site	Diagnostico Correcto	Modo de	Duracion
MPLS+ LINEA DE DATOS CAIDA	5432332	05/ene/09 12:36:16	1- URGENTE	MENDIG	SEVERIDAD ERRÓNEA	Teléfono	0,00
MPLS+ LINEA ESTA INACTIVA/ CAÍDA	5436606	12/ene/09 13:40:36	1- URGENTE	BRECHT	FALLO ALIMENTACIÓN	Teléfono	1,00
MPLS+CAIDO	5436952	12/ene/09 17:18:00	1- URGENTE	MENDIG	OPERACIÓN INCORRECTA	Teléfono	0,00
Cuenta:	3						
MPLS+ LINEA DE DATOS CAIDA	432332 c sv 00	05/ene/09 12:36:16	3- MEDIA	MENDIG	TRAS PRUEBAS NO SE PUDO REPRODUC	Teléfono	0,00
Cuenta:	4				Total tiempo en gestion mensual:		1,00
					T.M.R:		0,25

Tabla 40: Listado mensual de incidencias reportado por BT

La monitorización se realiza desde los centros de control del operador siguiendo la siguiente gráfica, en la que se puede ver como desde una consola de gestión centralizada se envían señales de monitorización y se analizan las respuestas.

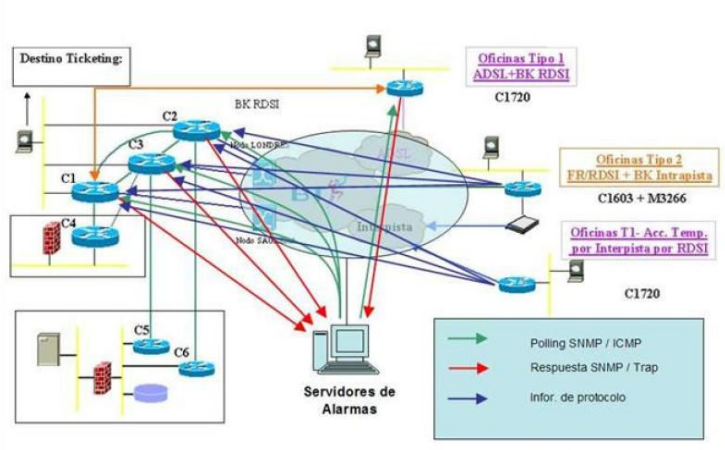

Ilustración 23: Monitorización implementada por BT

10.2 Monitorización de rendimiento de red

En referencia al ancho de banda de red consumido se pueden consultar informes del Firewall o bien informes que envía BT bajo petición, especialmente cuando se detecta algún tipo de problema de rendimiento.

En el caso que se analizará a continuación se intenta detectar comportamientos anómalos en cuanto al rendimiento de la red. Se solicitan informes a BT y se observa que el ancho de banda consumido tiene una periodicidad concreta. Los informes que se generan desde el firewall serán analizados con mayor detalle en el apartado 6.4.

Los gráficos que se van a analizar a continuación los obtiene BT con la herramienta MRTG (Multi Router Traffic Grapher) para monitorización de tráfico SNMP. MRTG es un script de Perl que utiliza SNMP para leer el tráfico que pasa por los routers y programas en C que graban las lecturas realizadas en logs. Luego estos logs son mostrados de una manera gráfica. Permite recoger datos con una latencia mínima de hasta un segundo, y luego mostrar los datos de manera agregada según el periodo que se defina.

En el primer gráfico se observa el consumo de ancho de banda de un periodo de 24 horas:

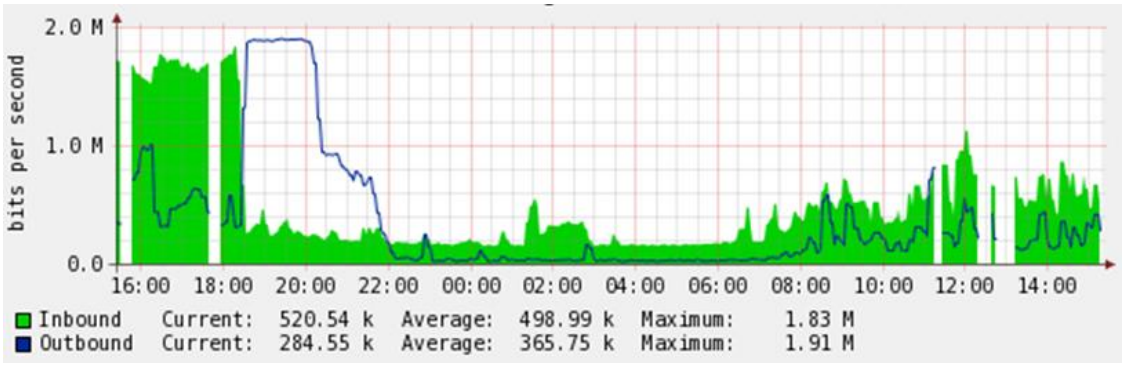

Ilustración 24: Gráfica de consumo de ancho de banda diario

Como se puede observar entre las 18:30 y las 20:10 hay un elevado consumo de ancho de banda de salida, mientras que entre las 15:50 y las 18:30 hay un elevado consumo de ancho de banda de entrada.

Para comprobar si es algo que sucede periódicamente se va a consultar la gráfica semanal que también envía BT:

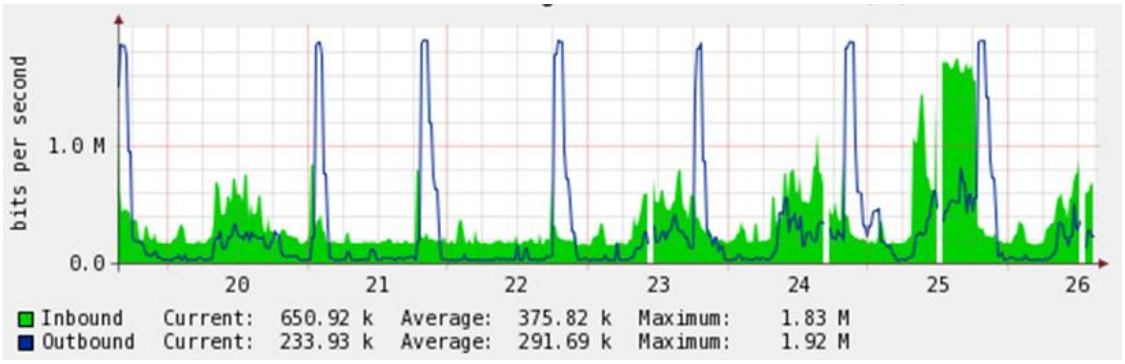

Ilustración 25: Gráfica de consumo de ancho de banda semanal

Como se puede observar el tráfico de salida sí tiene una periodicidad diaria, pero el tráfico de entrada no, o cuanto menos no tan marcada como el de salida.

Para acabar de verificar la periodicidad se consulta el gráfico mensual:

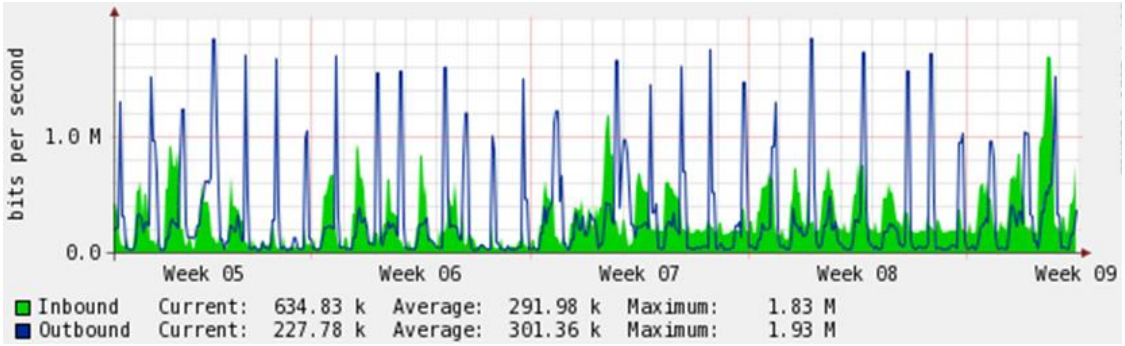

Ilustración 26: Gráfica de consumo de ancho de banda mensual

En este caso se puede observar un tráfico fijo de salida diario y un tráfico de entrada más variable pero también diario.

Realizando un análisis de tareas se detectó que la afectación entre 18:30 y 20:10 obedecía a un backup realizado fuera del horario establecido para ello, que fue modificado para ejecutarse a partir de las 2:00.

El tráfico de entrada se considera dentro de un consumo normal salvo para el primer día de análisis, que se atribuye a alguna descarga de software de gran tamaño.

10.3 Pruebas del portal

Una vez instalada la red se realizan toda una serie de validaciones para verificar el correcto funcionamiento del portal Citrix.

La primera prueba es de conectividad, se accede a la dirección del portal a través de un explorador Web y se verifica que se instala correctamente el plugin necesario y que se puede acceder a la consola del usuario

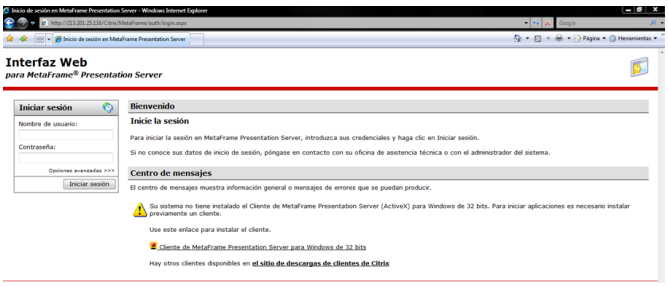

Ilustración 27: Prueba de conectividad con el servidor Citrix

Una vez comprobado el acceso a la consola nos identificamos y verificamos el acceso a aplicaciones:

Ilustración 28: Prueba de acceso a aplicaciones en Citrix

Y por último se prueba que se pueden abrir correctamente todas las aplicaciones definidas que irán a través de la red:

- Correo
- SAP GUI
- Apertura de ficheros de Office
- Internet Explorer

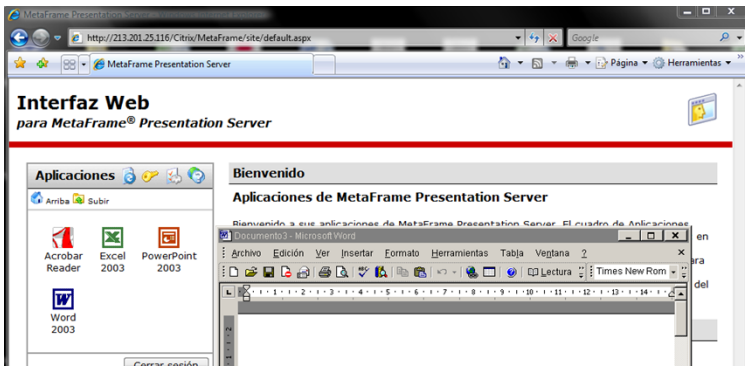

Ilustración 29: Prueba de apertura de sesiones de aplicación cliente citrix

Además de realizar las pruebas básicas de conectividad y ejecución de programas críticos una vez instalada la plataforma, cuando esta pasa a ser la plataforma de producción también se realizan mediciones periódicas de número de conexiones en paralelo, ancho de banda consumido por citrix, tiempo de latencia de la red (ping desde central a las sedes), número de usuarios en paralelo, consumo de bytes, picos de ocupación y así hasta un total de 300 reports diferentes, los cuales se pueden consultar en la base de datos de conocimiento de Citrix [19]. Estas mediciones se realizan con el paquete de Citrix EdgeSight que permite la obtención de reports como los mostrados en la figura. Por los motivos comentados en la introducción, no se dispone de acceso al reporting del cliente.

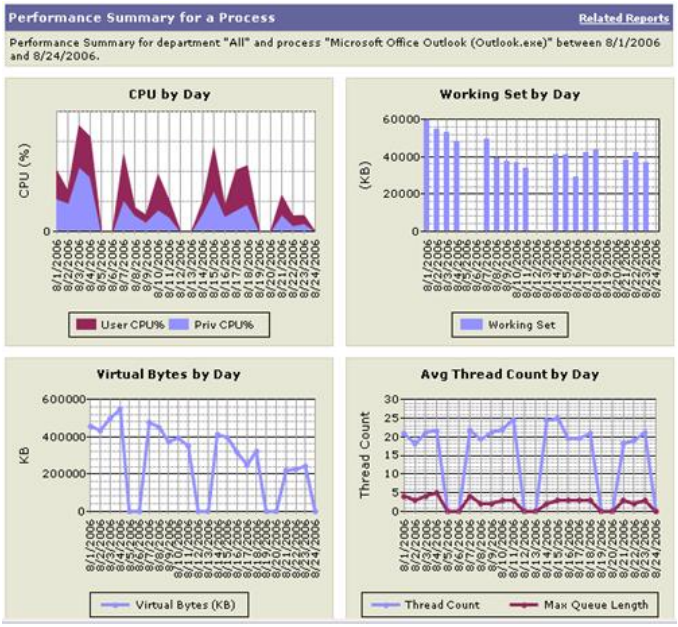

Ilustración 30: Ejemplo de gráficos que permite obtener Citrix

El único informe del se dispone con datos reales de la instalación es la tabla de disponibilidad de servicios en base a las incidencias detectadas para el sistema ERP de producción proporcionado través de Citrix. Para obtenerlo el sistema de reporting interno verifica mediante sentencias del estilo KeepAlive (ping) la respuesta del servidor cada minuto. En la siguiente tabla se puede ver el informe de disponibilidad para el mes de Junio de 2009.

Fecha Indicencia	Tipo Incidencia	KeepAlive	Duración
08/06/2009 20:31	Pérdida	1	1
10/06/2009 22:13	Pérdida	2	2
23/06/2009 18:03	Pérdida	2	2
Total mes		**5**	**5**
Minutos por mes			43200
Porcentaje de Pérdida			0,0116%
Porcentaje de Disponibilidad			**99,9884%**

Tabla 41: Disponibilidad de ERP a través de Citrix

10.4 Pruebas Antispam

En este punto se detalla los resultados de las pruebas realizadas con el dispositivo antispam Sonicwall ES6000, desde la instalación hasta la monitorización de rendimiento una vez instalado, incluyendo las ya comentadas en el apartado 4.4 obtenidas en Internet:

- La instalación y configuración del dispositivo se realizaron sin problemas utilizando los asistentes proporcionados por el fabricante.
- El dispositivo antispam se ubicó en la red de manera que la función antispam fuese distribuida entre el propio dispositivo y el firewall. Previo a su instalación el firewall recibía un 40% de tráfico SMTP, mientras que una vez instalado este porcentaje se redujo al 5% del tráfico.
- Se estableció una política prohibiendo los archivos ejecutables de un determinado grupo de usuarios y se limitó el tamaño de los mensajes entrantes. Posteriormente se realizaron pruebas para comprobar dicho filtrado y el los correos fueron rechazados por el antispam.
- Se realizaron pruebas de acceso por parte de usuarios finales no administradores para verificar la consola de gestión de correo de usuario.
- Se envían 50.000 correos spam, 4.000 correos supuestamente correctos y se obtiene un ratio de detección de spam del 98% y un ratio de falsos positivos del 0%.
- A través del sistema de reporting se extrae la información de funcionamiento sumarizada a nivel mensual que posteriormente se envía al cliente. Los ejemplos mostrados a continuación son con datos extraídos del sistema de reporting pero con gráficos desarrollados en Excel. Los dominios de correo han sido falseados para mantener la privacidad del cliente. En el momento de la redacción del proyecto no se dispone de acceso a la consola por haber finalizado el proyecto y no se dispone de imágenes de la propia consola. Se adjunta eso sí un ejemplo del reporting de la consola extraído de las especificaciones del producto, pero simplemente a modo de muestra. Los datos se obtienen de la consola de gestión de antispam que registran el número de mails procesados por el servidor de antispam a nivel diario, segmentado por dominio, por dirección (entrante o saliente) y con marca de spam o virus.

Mails enviados por periodo y dominio:

Dominio	ene-09	feb-09	mar-09	abr-09	may-09	jun-09
XXX.es	12.309	14.203	14.374	11.879	13.410	13.086
XXY.es	21.598	22.492	24.562	22.227	22.382	24.211
XXZ.es	282	625	515	413	480	583
XYX.es	1.156	1.831	1.713	1.342	1.583	1.275
XZX.com	729	662	631	698	528	515
XZY.com	1.094	1.293	1.193	1.124	1.272	1.232
XZZ.com	13.029	12.433	12.541	11.493	10397	10.130
ZXX.com	6.736	6.433	5.700	4.480	5.474	5.290
ZXY.es	2.206	2.207	2.549	2.217	2.156	2.002
ZXZ.com	9.248	13.301	9.661	9.028	8.358	7.765
ZYX.com	116	361	369	187	399	484
TOTAL	**68503**	**75841**	**73808**	**65088**	**66439**	**66573**

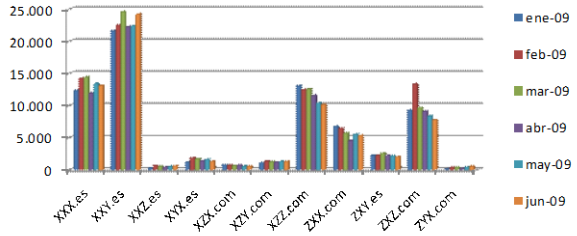

Tabla 42: Mails enviados por periodo y dominio

Mails recibidos por periodo y dominio:

Dominio	ene-09	feb-09	mar-09	abr-09	may-09	jun-09
XXX.es	17.815	20.283	21.071	20.551	20.576	18.980
XXY.es	40.077	42.071	45.027	41.923	41.591	44.978
XXZ.es	600	921	786	717	863	762
XYX.es	2.042	2.393	2.084	1.765	2.059	1.625
XZX.com	3.259	4.214	4.170	4.618	4.146	4.273
XZY.com	7.718	8.075	8.136	8.099	8.718	7.889
XZZ.com	25.216	25.021	24.594	24.044	21360	20.585
ZXX.com	9.208	9.372	10.285	9.775	9.030	9.709
ZXY.es	4.214	4.477	5.275	4.950	5.779	5.424
ZXZ.com	13.444	18.108	14.575	13.926	13.430	12.348
ZYX.com	73	339	496	250	460	466
TOTAL	**123666**	**135274**	**136499**	**130618**	**128012**	**127089**

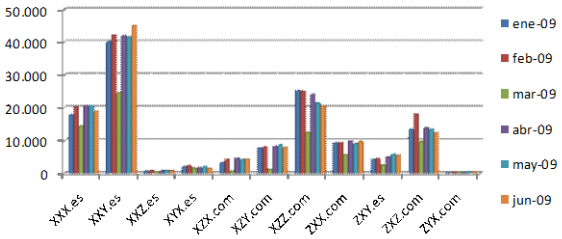

Tabla 43: Mails recibidos por periodo y dominio

Mails de Spam recibido:

Dominio	ene-09	feb-09	mar-09	abr-09	may-09	jun-09
XXX.es	178.191	150.812	286.310	493.185	828.841	497.275
XXY.es	4.395	4.565	4.224	5.563	5.042	3.653
XXZ.es	267	262	802	2.076	5016	2606
XYX.es	202	506	2.689	8.000	10.744	8.234
XZX.com	667	669	692	6.988	18.151	8.255
XZY.com	8.408	7.148	8.515	27.822	59.548	463
XZZ.com	17.629	17.040	15.468	35.535	70415	42.073
ZXX.com	3.582	3.903	3.670	14.535	30.514	16.767
ZXY.es	24.121	23.297	46.620	94.121	168.878	100.625
ZXZ.com	4.748	3.699	3.664	15.341	33.367	14.694
ZYX.com	1	13	19	12	226	13
TOTAL	**242211**	**211914**	**372673**	**703178**	**1230742**	**694658**

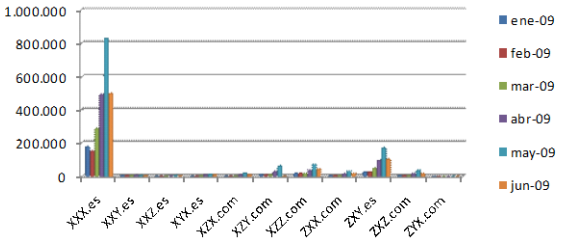

Tabla 44: Spam recibido por periodo y dominio

Mails recibidos con virus:

Dominio	ene-09	feb-09	mar-09	abr-09	may-09	jun-09
XXX.es	17	42	33	40	40	325
XXY.es	4	3	10	18	23	13
XXZ.es	0	0	0	0	0	2
XYX.es	4	4	4	4	2	7
XZX.com	0	4	2	7	3	289
XZY.com	1	0	0	7	4	463
XZZ.com	29	25	36	26	11	882
ZXX.com	2	1	10	15	12	576
ZXY.es	0	2	2	35	12	15
ZXZ.com	1	0	5	9	14	509
ZYX.com	0	0	0	0	0	0
TOTAL	**58**	**81**	**102**	**161**	**121**	**3081**

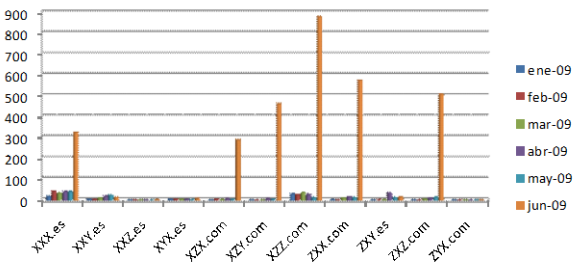

Tabla 45: Virus recibidos por mail por dominio y periodo

Ejemplos de la consola de reporting de Sonicwall antispam

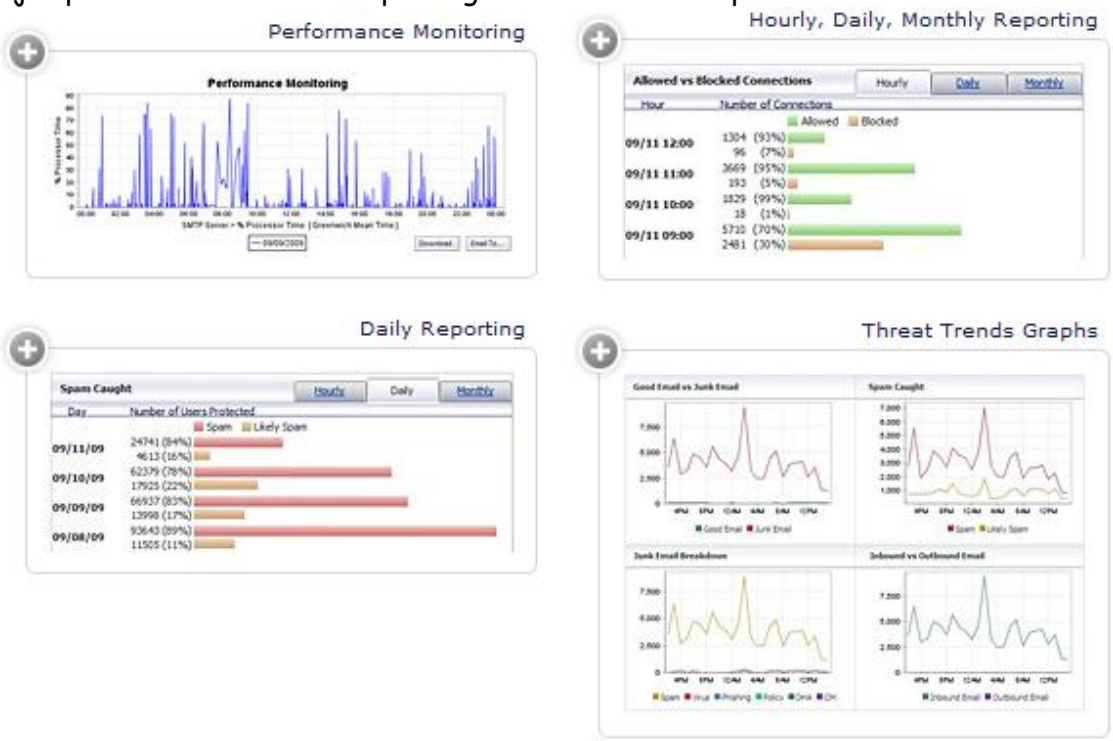

Ilustración 31: Ejemplos de gráficos de la consola de reporting del servidor antispam

10.5 Pruebas del Firewall

A la hora de realizar pruebas en el firewall se realizan tanto para el modelo escogido para servicios centrales, Sonicwall NSA E6500 como para el modelo escogido para la fábrica italiana Sonicwall NSA PRO 2040. Las pruebas realizadas son las siguientes:

- Verificación de alta disponibilidad: Se provoca la caída del firewall principal verificando que el firewall de backup entra en funcionamiento correctamente.
- Verificación de retorno al firewall primario: Se conecta de nuevo a la red el firewall primario y se observa como retoma el control correctamente y el firewall secundario vuelve al estado de Stand-by
- Verificación de rendimiento a través de VPN: Se conectan 50 usuarios en paralelo y se realiza una conexión al correo y a la aplicación corporativa de reporting y se verifica que no hay penalización de rendimiento, manteniéndose la CPU del firewall siempre por debajo del 10%
- Pruebas de IP-Spoofing: se envían ataques de IP spoofing desde internet utilizando una IP falsa que simula ser de la red interna. Ambos firewalls lo detectan y lo comunican por e-mail automáticamente.

- Pruebas de detección de denegación de servicio: Se envían paquetes de 1500 bytes desde dos puntos diferentes de la red intentando simular un ataque DoS y ambos firewalls lo detectan enviando el correspondiente mail de alerta.
- Conectividad de aplicaciones: Se conectan las principales aplicaciones de los usuarios y se verifica el funcionamiento de las mismas, abriendo conexiones Citrix, SAP, Exchange y aplicaciones de fábrica y todas funcionan correctamente. El único inconveniente detectado es de desconexión por timeout por inactividad de SAP. Se implementa una regla en el firewall para permitir un mayor tiempo (de 30 minutos a 2 horas) de inactividad.
- Gestión centralizada: Se comprobó que desde el firewall principal de la central se podía acceder al firewall de sede. La prueba se realizó desde el firewall principal y desde el secundario de manera que incluso en stand-by el firewall permite conectarse a las sedes remotas, es decir, la consola de gestión sigue activa aunque el firewall esté detenido.
- Verificación de antivirus: Se enviaron ficheros infectados por el virus Good Times y los archivos fueron detectados y eliminados.
- Verificación de antispyware: Se enviaron ficheros infectados con el troyano SubSeven y el firewall los detectó y eliminó.
- Control de ancho de banda de salida: Se puso una cuota de un máximo del 40% para el tráfico http en el tráfico de salida.
- Reporting: A continuación se muestran diversos gráficos que ofrece la consola de reporting de Sonicwall. En el caso del firewall sí que se dispone de un informe real extraído de la consola del cliente. En los ejemplos mostrados a continuación se observa la información sumarizada para el mes de Junio de 2009 que proporciona el firewall. En todas las gráficas se puede observar datos entre el 1 de Junio y el 23 de Junio y luego el 30 de Junio. Es debido a que por una incidencia el resto de días faltantes estuvo funcionando el firewall secundario.

Informe de ancho de banda consumido: En el siguiente informe se puede ver el tráfico en Mbytes que pasa por el firewall día a día.

Total Utilization:	1785171,464 MBytes
Max Utilization:	137654,266 MBytes
Average Utilization:	71406,859 MBytes

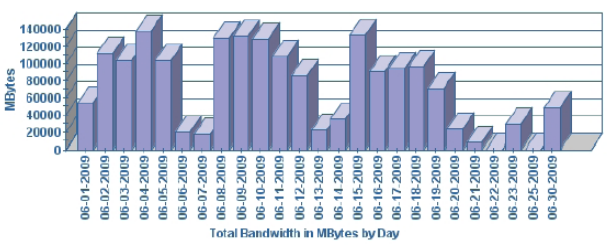

Ilustración 32: Gráfico de uso del firewall

En la siguiente tabla se muestran gráficos obtenidos de la consola de reporting del firewall con su descripción.

Disponibilidad del Firewall

Muestra la cantidad de horas diarias durante las que ha estado disponible el firewall. Se puede observar el día 23 de Junio una parada que se realizó de manera programada.

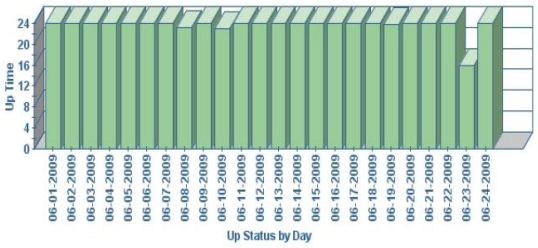

Ilustración 33: Gráfico de disponiblidad de firewall

Distribución de consumo por usuario

En este gráfico se puede observar la distribución del tráfico consumido a lo largo del mes distribuido por dirección IP

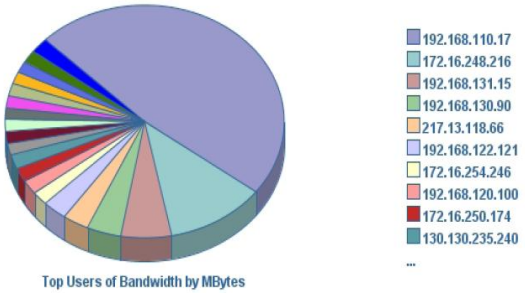

Ilustración 34: Distribucion de consumo por usuario

Consumo de tráfico web (http)

Esta gráfica nos muestra la distribución del tráfico http consumido por parte del los usuarios de la sede.

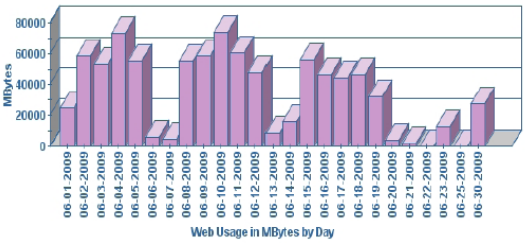

Ilustración 35: Consumo de tráfico http

Consumo de internet por usuario

En este gráfico se observa la distribución por usuario del tráfico de red destinado a consumo de internet. Como se puede observar hay claramente una dirección que realiza un consumo superior al resto

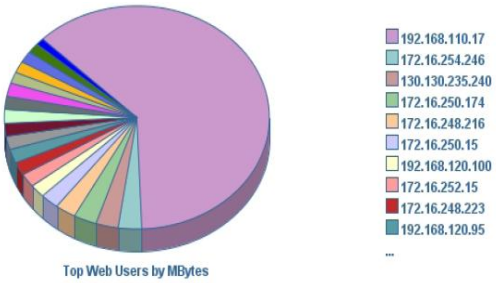

Ilustración 36: Consumo de internet por usuario

Sitios más visitados

En este gráfico circular se puede observar el tráfico http distribuido por los sitios más visitados. Como se puede observar, los dos mayores porcentajes corresponden a la página de actualizaciones de Microsoft y a la página principal del cliente.

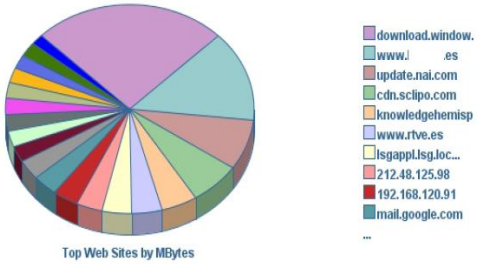

Ilustración 37: Sitios más visitados

Actividad del filtro de contenidos

En este gráfico de barras se puede ver con una distribución diaria el informe de actividad que realiza el gestor de contenidos en base al número de intentos de acceder a páginas catalogadas como prohibidas dentro del las políticas de seguridad del firewall. Junto con los tres informes de tráfico http permite determinar si se está realizando un consumo anómalo de Internet, por parte de quien y donde accede.

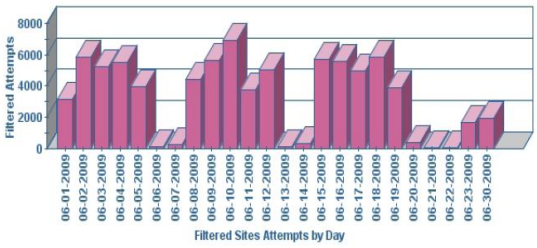

Ilustración 38: Actividad del filtro de contenidos

Consumo de tráfico ftp

En esta gráfica se puede observar con distribución diaria el tráfico ftp que circula a través del firewall de la sede.

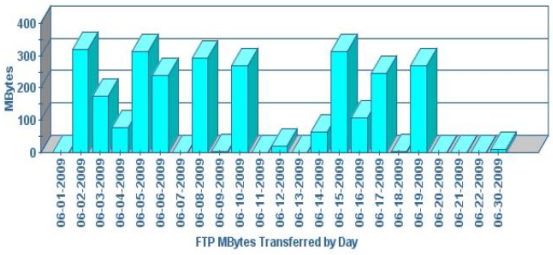

Ilustración 39: Consumo de tráfico ftp

Consumo de ftp por usuario

En el gráfico de ftp por usuario se puede observar la distribución por dirección IP del tráfico consumido durante todo el mes.

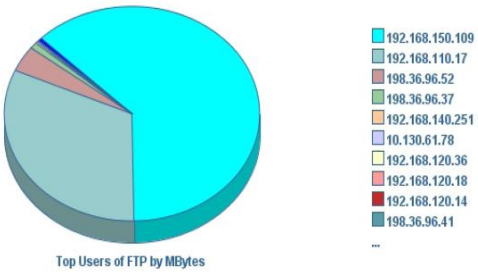

Ilustración 40: Distribución de tráfico ftp por usuario

Consumo de mail

En el gráfico de consumo de tráfico email a través de una distribución diaria contabilizado en MBytes.

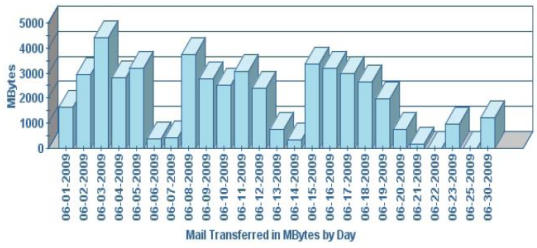

Ilustración 41: Consumo de mail por dia

Consumo de mail por usuario

La distribución de tráfico de correo a través de las diferentes direcciones IP de origen se muestra en la siguiente gráfica circular.

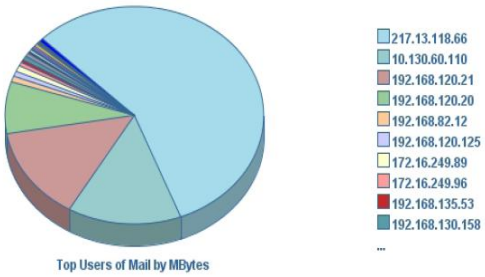

Ilustración 42: Consumo de mail por usuario

Ataques por día

En el gráfico de barras de la derecha se puede observar la cantidad de ataques detectados por el firewall día a día.

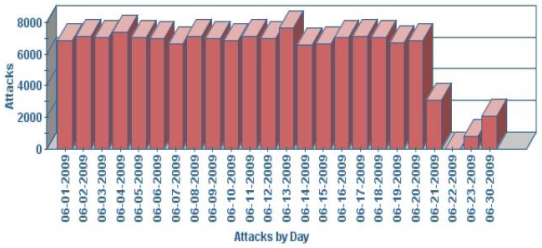

Ilustración 43: Ataques por día

Ataques por categoría

En la gráfica circular de la derecha se puede observar la distribución por tipo de ataque detectado. Como se puede observar la mayoría de ataques detectados son de la categoría TCP Syn/Fin Packets. Son un tipo de mensaje enviado por las páginas web para ver si el cliente que estaba conectado sigue en línea.

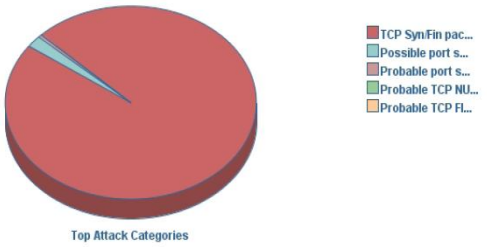

Ilustración 44: Ataques por categoría

No son un ataque grave pero se consideran como ataques por ser tráfico no deseado.

Errores de tráfico

En la gráfica de barras de la derecha se muestran los errores de tráfico producidos. Son paquetes perdidos por colisiones o por desconexiones puntuales.

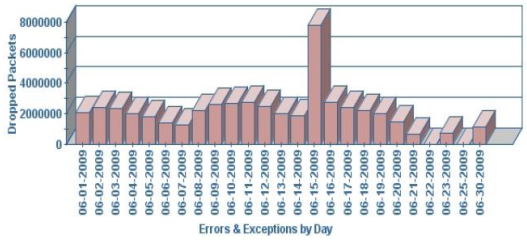

Ilustración 45: Errores de tráfico por día

Detecciones de intruso detectadas

El gráfico de la derecha muestra las detecciones de intruso detectadas por el componente IPS del firewall cada día.

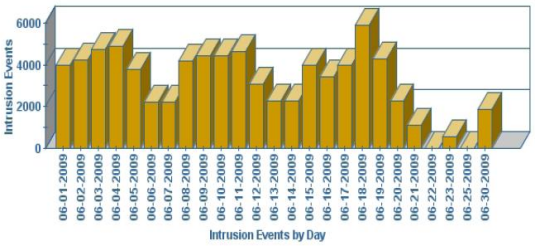

Ilustración 46: Detecciones de intruso detectadas

Detecciones de intruso por categoría

Se puede observar en la gráfica de la derecha la distribución por categoría de intrusión que detecta el firewall

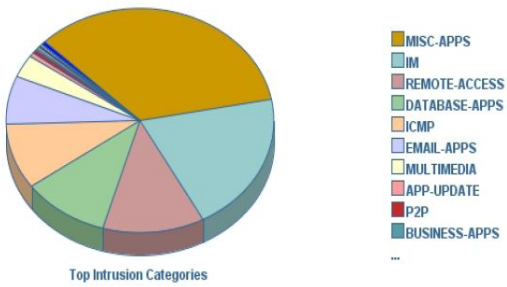

Ilustración 47: Detecciones de intruso por categoría

Ataques de virus detectados

En esta gráfica se observa la distribución diaria de ataques de virus detectados.

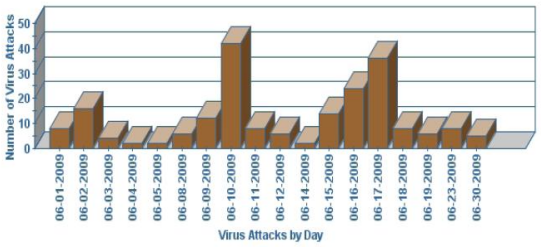

Ilustración 48: Ataques de virus detectados por día

Distribución por virus

Aquí podemos observar que virus son los que han intentado atacar el sistema.

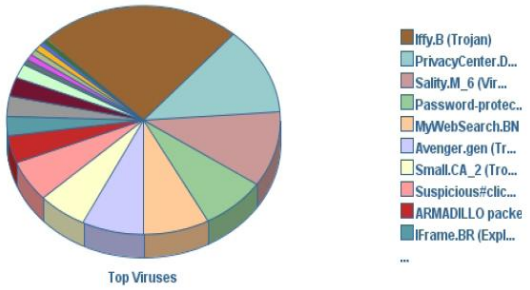

Ilustración 49: Virus detectados

Detección de spyware por día

En la gráfica se puede ver el número de ataques recibidos de spyware en una distribución diaria. Como se puede ver solo hubo intento de ataque dos días de todo el mes de Junio

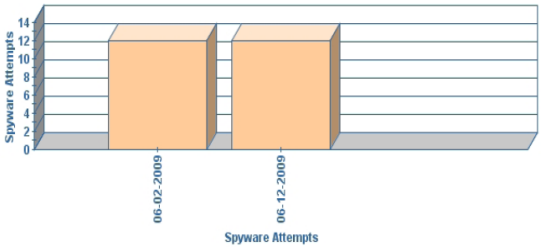

Ilustración 50: Spyware detectado por día

Consumo VPN

Como se puede observar en esta gráfica de distribución diaria, el consumo de tráfico VPN es especialmente elevado durante un fin de semana de Junio en el que hubo una migración de servidores.

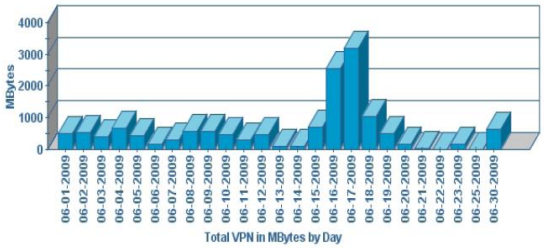

Ilustración 51: Consumo de VPN por día

Consumo VPN por usuario

En cuanto a usuarios VPN se puede observar como el usuario del equipo encargado de dicha migración es el que presenta un volumen más elevado de consumo VPN.

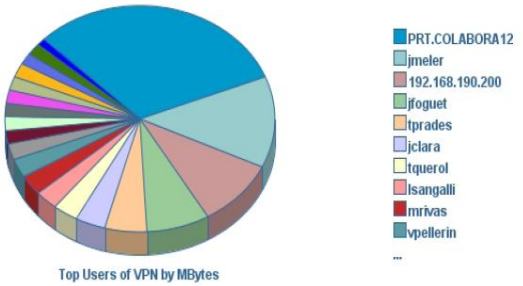

Ilustración 52: Consumo de VPN por usuario

11 Coste

En el presente apartado, una vez proporcionada e implantada una solución se van a dar números acerca del coste tanto del desarrollo del proyecto como de la implantación de las recomendaciones en la sede italiana. Además se tendrá en cuenta la diferencia entre costes iniciales y costes periódicos para tener una idea del coste que ha representado.

A la hora de considerar el esfuerzo humano requerido en la consecución de estos estándares se ha de tener en cuenta que la prioridad principal para el cliente era el correcto funcionamiento de sus sistemas, por lo que este proyecto de estandarización tenía una prioridad baja asignada. Con lo cual el proyecto se fue desarrollando por partes y en un segundo plano. De ahí se justifica que haya una elevada diferencia entre esfuerzo dedicado y duración del proyecto y que se haya colaborado por parte del alumno en la elección de solo algunos de los productos.

Las personas que aparecen en la tabla de dedicación han colaborado en la siguiente medida (al igual que durante el resto de proyecto, los nombres y referencias al cliente se evitarán por temas de confidencialidad):

Juan Valladares Perales: Durante estos cuatro años ha desarrollado labores de campo en el cliente y ha implementado y desarrollado todo lo redactado en el presente proyecto, con responsabilidades especialmente importantes en los ámbitos así marcados en la matriz de responsabilidades del proyecto. La redacción de la presente memoria se ha realizado de manera separada a las funciones laborales y fuera de horario laboral. Dichas funciones además cambiaron completamente de entorno y de cliente durante la redacción, complicando aún más si cabe la misma.

Ricardo Gilberto Hurtarte Carrillo: Durante todo el periodo que ha durado el proyecto, de hecho ya lo era previamente, ha sido el director del proyecto empresarial en el cliente, el responsable de todo el personal del mismo y el consultor de referencia para cualquier duda que haya podido surgir durante la realización del proyecto y la redacción de la memoria. Su función básica en cuanto al proyecto académico ha sido el de director de proyecto.
Destacar y agradecer su esfuerzo extra pues la colaboración con la parte de redacción del proyecto ha sido también fuera de horario laboral.

Xavier Hesselbach Serra: Ha estado colaborando activamente durante todo el proceso de redacción de la memoria que ha durado más de un año, desde la redacción del índice inicial hasta la corrección final del documento y adaptación a

las recomendaciones de presentación de proyecto de fin de carrera, sobrepasando con mucho las responsabilidades iniciales como ponente del presente proyecto.

Otros colaboradores: El proceso de definición de recomendaciones para el resto de puntos en los que se ha participado de manera más teórica ha sido llevado a cabo por un consultor de T2C (Albert Clarà) más alguna aportación puntual de otros consultores, que también han aportado sugerencias varias a la parte desarrollada por el alumno.

Cliente: El equipo cliente compuesto de un director del proyecto desde el punto de vista empresarial y un técnico que colaboraba con todas las instalaciones y configuraciones varias ha sido de gran ayuda especialmente porque fueron los que marcaron los requisitos del proyecto a gran escala. El detalle de requisitos presentados en el presente proyecto ha sido realizado íntegramente por el equipo de T2C.

Concepto	Fecha Inicio	Fecha fin	Coste (Jornadas)	Colaboradores	Colaboración Alumno
Desarrollo de recomendaciones	18/06/2007	27/11/2009	110	Juan Valladares Perales Ricardo Hurtarte Carrillo Albert Clarà Millan Jefe de proyectos Cliente Técnico Cliente	45%
Implementación en fábrica de Italia	01/09/2008	14/01/2009	40	Juan Valladares Perales Ricardo Hurtarte Carrillo	80%
Total Implementación (Facturado)	**18/06/2007**	**27/11/2009**	**150**		
Redacción de la memoria	16/01/2010	10/01/2011	35	Juan Valladares Perales Ricardo Hurtarte Carrillo Xavier Hesselbach Serra	70%

Tabla 46: Resumen de dedicaciones al proyecto

De estas fechas cabe destacar que la implementación en Italia se hizo teniendo en cuenta que no estaban todas las recomendaciones definidas, en concreto no se había desarrollado el análisis de proveedores de servicio, último punto en ser desarrollado y se conectaron las sedes con VPN sobre ADSL inicialmente. En una aplicación posterior de la recomendación de proveedor de servicios se procedió con la contratación definitiva de BT dando de baja una línea RDSI de backup de la que se disponía con Telecom Italia y manteniendo la hasta entonces línea productiva como línea de backup.

Téngase en cuenta que en este coste de implementación se tiene en cuenta la formación necesaria al técnico que luego va a mantener la instalación. Se estiman unas 40 jornadas de mantenimiento a un precio de 220 Euros por jornada.

Teniendo también en cuenta el coste de la implementación en la fábrica italiana y añadiéndolo como un concepto más, el coste de implementación de las recomendaciones en una sede es el siguiente:

Concepto	Periodicidad	Coste Hardware	Coste Software	Coste Personal	Cantidad	Total
Conexión MPLS con BT	Inicial	330,00			1,00	330,00
Conexión Backup Primaria con BT	Inicial	75,00			1,00	75,00
Conexión Backup Secundaria con Telecom Italia	Inicial	90,00			1,00	90,00
Router Frontera Cisco 1801	Inicial	748,00			2,00	1.496,00
Switch Linksys SRW2008P	Inicial	274,15			2,00	548,30
Gestor de Ancho de Banda Packeteer 1700	Inicial	10.032,00			1,00	10.032,00
Firewall Sonicwall NSA E2040	Inicial	4.995,00	5.616,00		2,00	21.222,00
Antivirus McAfee Enterprise V7	Inicial		22,00		50,00	1.100,00
Servidor FTP *	Inicial	418,90	0,00		1,00	418,90
Antispam	Inicial	4.160,75			1,00	4.160,75
Switch Nortel Central	Inicial	466,99			1,00	466,99
Switch Nortel Departamental	Inicial	466,99			6,00	2.801,94
Servidor de Impresión *	Inicial	418,90	0,00		1,00	418,90
Servidor active directory *	Inicial	418,90	460,00		2,00	1.757,80
Impresora HP Laserjet CP2025DN	Inicial	339,00			6,00	2.034,00
Scanner HP G2710	Inicial	74,00			6,00	444,00
Puntos de acceso WIFI Netgear 54Mbps 802.11g	Inicial	57,84			6,00	347,04
Licencia Citrix Presentation Server V4	Inicial		187,99		50,00	9.399,50
Consultoría Implementación Fábrica Italiana	Inicial			480,00	40,00	19.200,00
Total Coste Inicial						**76.343,12**
Antivirus McAfee Enterprise V7	Anual		4,00		50,00	200,00
Licencia Citrix Presentation Server V4	Anual		24,44		50,00	1.222,00
Conexión MPLS con BT	Mensual		650,00		12,00	7.800,00
Conexión Backup Primaria con BT	Mensual		40,00		12,00	480,00
Conexión Backup Secundaria con Telecom Italia	Mensual		40,00		12,00	480,00
Firewall Sonicwall NSA E2040 **	Anual		1.374,00		1,00	1.374,00
Coste Personal Mantenimiento	Anual			220,00	40,00	8.800,00
Packeteer 1700	Anual			1.500,00	1,00	1.500,00
Licencias Active Directory	Anual		83,00		2,00	166,00
Total Coste Anual						**22.022,00**

* Se utiliza el mismo modelo de servidor físico HP 333704

** Incluye un año de mantenimiento y High availability pack

Se pagan actualizaciones y mantenimiento de High Availability a partir del segundo año

Tabla 47: Desglose de costes de implementación en sede

Todos los precios reflejados en la tabla de costes son los precios conseguidos para el cliente durante los pasos previos a la puesta en marcha de Italia, entre Junio y Septiembre de 2008.

12 Conclusiones

Como cierre de proyecto se detallan las conclusiones a las que se llega después de realizar el estudio, desarrollo e implementación del presente proyecto.

12.1 Conclusiones generales del proyecto

Un proyecto centrado en el mundo empresarial como ha sido el presente proyecto tiene una serie de condiciones que lo caracterizan y diferencian de un proyecto estándar de investigación y desarrollo. Además de los objetivos académicos de formación del estudiante ha de proporcionar resultados plausibles a la empresa en la cual trabaja el estudiante y al cliente bajo cuyo marco se ha desarrollado el proyecto. Con lo cual en el momento de evaluar las conclusiones del proyecto se ha de medir tanto los resultados técnicos en base a las pruebas realizadas, los desarrollos implementados y demás funciones realizadas por el alumno, como los niveles de satisfacción y percepción del trabajo realizado desde la empresa y desde el cliente.

En referencia a los objetivos técnicos del proyecto se considera que se han alcanzado los objetivos propuestos en el inicio del mismo, consiguiendo el establecimiento de unas recomendaciones que permiten desarrollar una infraestructura correctamente dimensionada en cuanto a red, sistemas y seguridad.

Durante todas las pruebas de verificación y rendimiento del sistema se extrae que la elección en cuanto a capacidades y funcionalidades ha sido cuanto menos suficiente pues no se detectan deficiencias ni de rendimiento ni de funcionamiento.

Se ha conseguido en base a buscar compatibilidad basada en cumplimiento de estándares una infraestructura base completamente compatible entre sí, sin que se haya detectado ningún tipo de problema de compatibilidad al ponerlo las recomendaciones en marcha en las sedes en las que ya se han implantado.

Por otro lado se ha dotado al modelo de una escalabilidad que ofrece la posibilidad de mejora continua al haber sido diseñado con fabricantes que disponen de una amplia gama de productos de manera que permiten utilizar el mismo fabricante con modelos de la misma familia pero de diferentes tamaños, lo que volviendo al punto anterior asegura la compatibilidad entre ellos. Además la posibilidad de disponer de un entorno centralizado que ofrece Citrix permite asignar recursos

virtualmente tanto a las consolas de los usuarios como a los servidores sin necesidad de añadir nuevo hardware. En caso de ser necesario nuevo hardware se instala centralizadamente y luego se va repartiendo en función de las necesidades.

El propio sistema Citrix, combinado con la solución de VPN, ha permitido al implantar un modelo de arquitectura de software centralizado un mejor rendimiento de los usuarios finales, con máxima disponibilidad y posibilidad de movilidad para los usuarios.

Combinando este último punto con los ratios de conectividad proporcionados por los proveedores de servicio se ha conseguido un alto grado de estabilidad en el servicio ofrecido, consiguiendo un ratio de disponibilidad de 99.9888% para la aplicación ERP de producción operada de manera centralizada.

En términos de seguridad se ha conseguido implantar un sistema blindado, resistente a ataques externos e internos. Respecto a ataques externos, la actuación conjunta del Firewall, el antivirus y el antispam proporcionan un perímetro interno de seguridad en el que hasta la fecha no se han detectado fisuras para las sedes que han ido adaptando las recomendaciones. Respecto a posibles ataques internos, los ordenadores que se conectan a la red han de disponer del antivirus corporativo y correctamente actualizado para permitirles el acceso a cualquier IP interna o externa. Esto se consigue desde opciones de configuración avanzadas del firewall.

En cuanto a monitorización e información de estado de los diferentes componentes de la red, se ha conseguido disponer de monitorización y aviso inmediato a los administradores vía e-mail o mensaje de texto en cuanto se detecta alguna de las alertas definidas en las consolas de los productos instalados y la obtención de informes detallados para poder analizar incidencias de mal funcionamiento o mal uso de la infraestructura.

En referencia a la homogeneización de infraestructuras y proveedores, hasta el momento de finalización de la colaboración con el cliente se ha conseguido una homogeneización parcial de las sedes que se han ido incluyendo en el estándar definido. Si el cliente sigue las recomendaciones establecidas para todas las sedes se conseguirá una homogeneización total que abaratará los costes de administración y mantenimiento y minimizará la necesidad de conocimiento de los administradores al realizarse toda la administración para productos iguales.

Por otro lado, como se ha comentado en la introducción de este apartado, se ha de tener en cuenta la satisfacción de la empresa y del cliente. Por parte de la empresa la satisfacción con el resultado obtenido ha sido notable, promoviendo una evolución profesional más que satisfactoria para ambas partes a partir de la

finalización de la colaboración con el cliente. Por parte del cliente se obtiene un grado de satisfacción medio entre todos los apartados de 8,5 sobre 10 en las encuestas anuales realizadas por parte de la empresa, ligeramente por encima de la media del grado de satisfacción obtenido entre todos los clientes de la empresa.

12.2 Posibles mejoras en las recomendaciones

Durante el desarrollo e implementación del proyecto se han detectado ciertos puntos en los que se podría mejorar tanto en las propias recomendaciones como en la aplicación de las mismas que se ha realizado.

Un punto que ha implicado un sobrecoste para el cliente, si bien ha sido en parte promovido por él mismo ha sido el sobredimensionamiento. Muchos de los dispositivos han sido escogidos muy por encima de las necesidades calculadas en el apartado de dimensionamiento. Un ejemplo sería tanto el firewall central como los firewalls de sede. En el análisis de consumo de red y de CPU se puede observar que funcionan prácticamente sin actividad durante todo el día. En este sentido el problema viene dado por la intención del cliente de implementar una solución perdurable en el tiempo sin necesidad de modificaciones, pero a nuestro entender debería reducirse el coste de implementación inicial y apostar por un plan de renovación con menores plazos temporales.

También se han detectado fallos en la planificación realizada. Durante la implementación se sufrieron demoras por culpa de una mala planificación sin tener en cuenta el tiempo máximo de respuesta de los ISP, que provocó que no se dispusiera de línea para la fecha en la que se quería comenzar con la instalación. También se demoró la entrega de algunos componentes de los que no se disponía en stock en servicios centrales y el proveedor de los mismos tardó más tiempo del esperado en proporcionarlos.

Respecto a la planificación también destacar que no se consideró la formación necesaria para los administradores de sedes y eso supuso problemas para la adopción de la gestión de la nueva plataforma por parte de los administradores locales y rechazo al cambio de productos que ya tenían.

Otra de las mejoras a realizar en cuanto a recomendaciones es que en ocasiones las medidas que se han querido adoptar han sido demasiado estrictas para las posibilidades de las sedes. Por ejemplo las especificaciones del CPD referentes a una sala dedicada, la disposición de grupos electrógenos o la seguridad 24x7 no se pudieron cumplir en algunas de las sedes por no disponer de espacio o recursos para ello.

12.3 Líneas Futuras

Como líneas futuras de evolución de las recomendaciones se plantea al cliente la inclusión en las mismas nuevos apartados para homogeneizar o implementar en los casos en los que no se disponga de ello los siguientes puntos:

Videovigilancia: Se plantea el uso de cámaras IP para implementar videovigilancia en las sedes de manera que todas las imágenes queden almacenadas en un servidor centralizado del CPD de servicios centrales.

VoIP: Durante las presentes recomendaciones se ha tenido en cuenta que los componentes de la red dispusieran de soporte para VoIP y que el servicio de red proporcionado con MPLS dispusiera de QoS. Con lo cual es sencillo implementar Voz sobre IP en las diferentes sedes y así se le propone al cliente.

PDA: En la actualidad algunos usuarios ya disponen de dispositivos PDA con el correo configurado. Se le propone al cliente implementar un sistema de uso de PDA's para la gestión de pedidos a través del ERP.

13 Listado de Acrónimos

Durante la presente memoria se ha ido haciendo referencia a una serie de acrónimos que listamos a continuación por orden alfabético. Se detalla su significado y en caso de ser en inglés se muestra su traducción al castellano.

AD: *Active Directory*. Directorio Activo

AES: *Advanced Encryption Standard.* Estándar de Encriptación Avanzada.

AI: *Artificial Intelligence.* Inteligencia Artificial.

ARM*: Advanced Reputation Management.* Gestión de Reputación Avanzada.

B/N: Blanco/Negro.

BRS: *Backup Recovery Services.* Servicio de Recuperación de Copia de Seguridad.

CPD: Centro de Procesado de Datos

DHCP: *Dynamic Host Configuration Protocol.* Protocolo de configuración de Host Dinámico

DLP: *Data Loss Prevention*. Prevención de Pérdida de Datos.

DMZ: *Demilitarized Zone.* Zona desmilitarizada

DNS: *Domain Name System.* Sistema de Nombres de Dominio

DoS: *Denial of Service.* Denegación de Servicio.

ERP: *Enterprise Resource Planning.* Planificación de Recursos Empresariales

FTP: *File Transfer Protocol.* Protocolo de Transmisión de Ficheros

GDE: *Generic Decryption Engine.* Motor de Desencriptación Genérico.

HTML: *HyperText Markyp Language.* Lenguaje de Marcado de HiperTexto.

ICA: *Independent Computing Architecture.* Arquitectura de Computación Independiente.

IDS: *Intrusion Detection System.* Sistema de Detección de Intrusos.

IEEE: *Institute of Electrical and Electronics Engineers*. Instituto de Ingenieros Electricos y Electrónicos.

IETF: *Internet Engineering Task Force.* Grupo Especial sobre Ingeniería de Internet.

IMF: *Intelligent Message Filter.* Filtrado de Mensajes Inteligente.

IP: *Internet Protocol.* Protocolo de Internet.

IPS: *Intrusion Prevention System.* Sistema de Prevención de Intrusos.

ISP: *Internet Service Provider.* Proveedor de Servicios de Internet.

IT: *Information Technology.* Tecnología de la Información

ITIL: *Information Technology Infrastructure Library.* Biblioteca de Infraestructura de Tecnologías de Información.

LAN: *Local Area Network.* Red de Área Local.

MITM: *Man In The Middle.* Hombre en el Medio.

MPLS: *Multi Protocol Label Switching.* Conmutación de Etiquetas Multi Protocolo.

NAS: *Network Attached Storage.* Almacenamiento Adjunto en Red.

P2P: *Peer to Peer*. Punto a Punto.

PC: *Personal Computer.* Ordenador personal.

PDA: *Personal Digital Assistant.* Asistente Personal Digital.

RAM: *Random Access Memory.* Memoria de Acceso Aleatorio.

RBL: *Realtime Black Lists.* Listas Negras en Tiempo Real.

RDNS: *Reverse Domain Name System.* Sistema de Nombres de Dominio Inverso.

RDP: *Remote Desktop Protocol.* Protocolo de Escritorio Remoto.

RPD: *Recurrent Pattern Detection.* Detección de Patron Recurrente.

SCL: *Spam Confidence Level.* Nivel de Confianza Spam.

SIDF: *Sender ID Framework.* Plataforma de Identificador de Remitentes.
SLA: *Service Level Agreement.* Acuerdo de Nivel de Servicio.

SNMP: *Simple Network Management Protocol.* Protocolo Simple de Administración de Red.

SONAR: *Symantec Online Network for Advanced Response.* Red Online de Symantec de Respuesta Avanzada.

SPF: *Sender Policy Framework.* Marco Legal de Remitente.

SSL: *Secure Sockets Layer.* Capa de Conexión Segura.

TCO: *Total Cost of Ownership*. Coste Total de Propiedad.

TCP: *Transmission Control Protocol.* Protocolo de Control de Transmisión.

UDP: *User Datagram Protocol.* Procolo de Datagramas de Usuario.

UPD: *Universal Printer Driver.* Controlador Universal de Impresión.

VLAN: *Virtual Local Area Network.* Red de Área Local Virtual.

VOIP: *Voice over IP.* Voz sobre IP.

VPN: *Virtual Private Network*. Red Privada Virtual.

WAN: *Wide Area Network.* Red de Área Amplia.

WLAN: *Wireless Local Area Network.* Red de Área Local Inalámbrica.

14 Bibliografía

14.1 Referencias

En el apartado de referencias incluimos los documentos citados a lo largo de la presente memoria.

[1] Gustavo García Enrich. El estándar TIA-942. Una visión general. Disponible en: http://www.areadata.com.ar/pdf/El%20standard%20TIA%20942%20-vds-11-4.pdf

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley y E. Schooler. SIP: Session Initiation Protocol. Disponible en: http://tools.ietf.org/html/rfc3261

[3] P. Mockapetris. Domain Names - Implementation and Specification. Disponible en: http://www.ietf.org/rfc/rfc1035.txt

[4] R. Droms. Dynamic Host Configuration Protocol. Disponible en: http://www.faqs.org/rfcs/rfc2131.html

[5] L. Howard. An Approach for Using LDAP as a Network Information Service. Disponible en: http://tools.ietf.org/html/rfc2307

[6] Microsoft Corporation. Active Directory LDAP Compliance. Disponible en: http://www.google.es/url?sa=t&source=web&cd=1&ved=0CBcQFjAA&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2Fd%2Fc%2F8%2Fdc83e0b8-fc2c-4af4-bd27-45b5963ad98d%2Fad%2520ldap%2520compliance.doc&rct=j&q=ad%20ldap%20compliance&ei=FZkpTdWzApGu8QOoteiJAw&usg=AFQjCNFaxsDZkqtX4avijMsLXYjQw8mwkw&cad=rja

[7] M. Horowitz. FTP Security Extensions. Disponible en: http://tools.ietf.org/html/rfc2228

[8] RDP vs ICA: What is the Proper Protocol? Disponible en: http://findarticles.com/p/articles/mi_m0FOX/is_1998_Nov_18/ai_53209280/

[9] Trafico en conexiones ICA. Disponible en: http://ctxdom.wordpress.com/2007/11/25/trafico-en-conexiones-ica/

[10] Propalms. Product Comparison Matrix. Disponible en: http://www.channelconcepts.nl/fileupload/propalms-product-vergelijking-2.pdf

[11] Magic Quadrant for Enterprise Antivirus, 2006. Gartner RAS Core Research, NOTE G00141873

[12] J. Lyon y M. Wong. Sender ID: Authenticating E-Mail. Disponible en: http://www.elstir.com/archivos/rfc-4406_sender-id.txt

[13] W. Schlitt y M. Wong. Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1. Disponible en: http://www.elstir.com/archivos/rfc-4408_spf.txt

[14] Antispam Comparison Reports. Westcoast Lab. Disponible en: http://de.trendmicro.com/imperia/md/content/uk/whitepaper/wp06_wclantispamrpt_090317us.pdf

[15] Magic Quadrant for e-mail Security Boundaries, 2008. Gartner RAS Core Research, NOTE G00160125

[16] Defining the Next-Generation Firewall. John Pescatore and Greg Young. Disponible en: http://www.paloaltonetworks.com/literature/research/Gartner-NGFW-Report.html

[17] Planificación de ciclo de vida del proyecto. Documento Adjunto.

[18] Jan van Bon et al. Fundamentos de la Gestión del Servicio basada en ITIL v3. ISBN: 978 90 8753 060 0.

[19] List of Standard Reports Included in EdgeSight 4.5. Disponible en: http://support.citrix.com/article/CTX111282&searchID=41958830

14.2 Documentación consultada

1.- Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información. Consejo superior de Administración Electrónica. Ministerio de Política Territorial y Administración Pública. Gobierno de España. Disponible en: http://www.csi.map.es/csi/metrica3/

2.- Análisis Heurístico: detectando malware desconocido. David Harley & Andrew Lee. Disponible en:

http://www.eset.com.pa/threat-center/articles/analisis_heuristico_detectando_malware_desconocido.pdf

3.- Magic Quadrant for Endpoint Protection Platforms, 2007. Gartner RAS Core Research, NOTE G00153291

4.- Magic Quadrant for Enterprise Network Firewalls, 2007. Gartner RAS Core Research, NOTE G00151129

5.- Citrix Presentation Server Comparative Feature Matrix. Disponible en: http://www.citrix-download.com/NE/Experience_NL/CPS_ComparativeMatrix.pdf

6.- Matriz comparativa de soluciones Anti-Spam - Octubre 2006. Disponible en: http://www.seguridaddigital.info/images/stories/CompMatrix_191006.pdf

7.- Netfence Security Management Whitepaper. Phion. Disponible en: http://www.phion.com/INT/support/documentation/Product%20Documentation/WP_netfence_Management_en.pdf

8.- Niveles de disponibilidad según estándar TIA-942. Disponible en: http://www.unitel-tc.com/?m=15&p=47

9.- Tobias Oetiker. What is MRTG? Disponible en: http://oss.oetiker.ch/mrtg/doc/mrtg.en.html

10.- IPSec vs. MPLS VPNs. Tim Greene. Disponible en: http://www.networkworld.com/newsletters/vpn/2001/01101980.html

11.- MPLS (MultiProtocol Label Switching). José Manuel Huidobro Moya & Ramón Jesús Millán Tejedor. Disponible en: http://www.ramonmillan.com/tutoriales/mpls.php

12.- Tecnologías de Redes Privadas Virtuales (VPN). Julio Alba Soto. Disponible en: http://www.coit.es/publicac/publbit/bit131/sociedad2.htm

13.- Niveles de RAID. Disponible en: http://www.smdata.com/NivelesRAID.htm

Para complementar información en diferentes apartados se utiliza como referente la siguiente entrada:
14.- Wikipedia. Disponible en: www.wikipedia.org
De esta página se consultan muchas entradas, entre ellas:

14.1.- http://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos

14.2.- http://es.wikipedia.org/wiki/IPsec
14.3.- http://es.wikipedia.org/wiki/MPLS
14.4.- http://es.wikipedia.org/wiki/Unified_threat_management
14.5.- http://es.wikipedia.org/wiki/Spoofing
14.6.- http://en.wikipedia.org/wiki/SONAR_(Symantec)
14.7.- http://es.wikipedia.org/wiki/Cable_de_categor%C3%ADa_6

15.- Firewall Comparison Guide. IT Security. Disponible en: http://www.itsecurity.com/whitepaper/pdf/Firewall_Comparison_Guide.pdf

16.- Comparative Firewall Study. Torsten Höfler, Christian Burkert and Martin Telzer. Disponible en: http://www.google.es/url?sa=t&source=web&cd=1&ved=0CBsQFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.114.6615%26rep%3Drep1%26type%3Dpdf&rct=j&q=Comparative%20Firewall%20Study&ei=Juv7TPPTGYOs8gOAmJ2DDA&usg=AFQjCNFEXnmWsv3RG6tQUOeagWFcIfdMgQ&cad=rja

17.- SonicWALL Application Intelligence and Control. Disponible en: http://www.sonicwall.com/downloads/DS_ES_Application_Intelligence_A4.pdf

18.- SonicWALL Email Security 6.0 Administrator's Guide. Disponible en: http://www.sonicwall.com/downloads/Email_Security_6.0_Administrators_Guide_Appliance.pdf

19.- SonicWall Enforced Client Anti-Virus and Anti-Spyware. Disponible en: http://www.sonicwall.com/es/772.html

20.- NOD32 User guide. Disponible en: http://download.eset.com/manuals/ESET_EAV4_User_Guide_ENU.pdf

21.- The evolution of anti-spam technology. Ron Herardian. Disponible en: http://www.dominopower.com/issues/issue200408/00001340001.html

22.- Exchange Server 2003 Anti-Spam Framework Overview. Disponible en: http://www.google.es/url?sa=t&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F0%2Fe%2F6%2F0e6a7113-dda4-4fd7-aaba-b9e264700225%2Fanti-spam.doc&rct=j&q=Exchange%20Server%202003%20%20Anti-Spam%20Framework%20Overview%20&ei=Qe37TKqPOsnA8QOunNzzCw&usg=AFQjCNGqlZht9ax_QEXyok7SbD5806Eruw&cad=rja

23.- Integración de redes ópticas e IP mediante GMPLS. Disponible en: http://www.networkworld.es/%28S%28051oqw55umvv1ozwk2t24u55%29%29/Articulo.aspx?ida=143406&seccion=

24.- Citrix ICA Priority Packet Tagging. Disponible en: http://support.citrix.com/article/CTX19314

25.- Juniper Networks IDP 50/200/600/1100. Disponible en: http://www.lcmsecurity.com/site/pdfs/Intrusion%20Prevention/Juniper_IDP.pdf

26.- Rootkits: Risks, Issues and Prevention. Disponible en: http://www.virusbtn.com/pdf/conference_slides/2006/MartinOvertonVB2006.pdf

27.- McAfee® GroupShield™ version 7.0 For Microsoft® Exchange Disponible en: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/20000/PD20100/en_US/gse_70_user_guide_en_us.pdf

28.- Sender ID Framework. Disponible en: http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

29.- Evaluation Program for Symantec™ Mail Security Appliances. Disponible en: http://a248.e.akamai.net/f/248/3214/1d/www.zones.com/images/pdf/symantec_eval_brochure.pdf

30.- Técnicas anti-spam: Presente y Futuro. Irontec. Disponible en: http://documentacion.irontec.com/tecnicas_anti_spam_EnpresaDigitala.pdf

31.- Informe Anual Telefónica Investigación y Desarrollo – 2007. Disponible en: http://www.telefonica.com/es/about_telefonica/pdf/tid-informe-anual-2007.pdf

32.- Advanced Virus Detection Scan Engine and DATs. Network Associates. Disponible en: http://www.crswann.com/2-NetSecurity/VirusDetectionTechnology%28McAfee%29.pdf

33.- BOB - The future of branch office networking. Phion. Disponible en: http://www.phion.com/INT/support/documentation/Product%20Documentation/WP_netfence_BOB_en.pdf

34.- Eduardo Pierdant. ¿Qué es el Costo Total de Propiedad?. Disponible en: http://blogs.msdn.com/b/eduardop/archive/2006/05/29/610441.aspx