Diseño de una Infraestructura TIC Basada en Virtualización

Trabajo fin de Grado Ingeniería Informática

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

Autor: Miguel Ángel Ortega Pérez

Tutor: Gabriel de Blasio García

Año: 2013

"Muchas veces la gente no sabe lo que quiere hasta que se lo enseñas"

Steve Jobs

"Lo maravilloso de aprender es que nadie puede arrebatárnoslo"

B.B.King

"Mira, esto es simple. Los buenos tiempos son ahora. ¿Ok? La condición humana de hoy es la mejor y la tecnología es una de las razones para ello."

Tom Clancy

"…lo llevamos en el alma y lo bailamos con el cuerpo
bailemos todos juntos este rock and roll… "

Tequila

Resumen

Las necesidades básicas de las empresas suelen ser las mismas, ya sea una empresa grande que pequeña, la infraestructura sobre la que montan sus procesos de negocio y las aplicaciones para gestionarlos suelen ser casi iguales. Si dividimos la infraestructura TIC de una empresa en hardware, sistema y aplicaciones, podemos ver que en la mayoría de ellas el sistema es casi idéntico.

Además, gracias a la virtualización, que ha entrado de manera arrolladora en el mundo de la informática, podemos independizar totalmente el software del hardware, de forma que obtenemos una flexibilidad enorme a la hora de planificar despliegues de infraestructura.

Sobre estas dos ideas, uniformidad de sistema e independencia de hardware, son sobre las que se va a desarrollar el siguiente TFG.

Para el desarrollo de la primera de ellas se realizará el estudio de la infraestructura básica (o sistema) que cualquier empresa suele tener. Se intentará dar una solución que sea válida para una gran cantidad de empresas de nuestro entorno y se realizará el diseño del mismo.

Con la segunda idea desarrollaremos un sistema basado en servicios, que sea lo suficientemente completa para poder dar respuesta a las necesidades vistas pero, a su vez, suficientemente flexible para que el crecimiento en capacidades o servicios se pueda realizar de forma sencilla sin que la estructura del sistema, o sus módulos deban modificarse para realizarlos.

Por tanto, vamos a realizar un diseño integral y completa, de forma que será tanto de hardware como de software, haciendo énfasis en la integración de los sistemas y la interrelación entre los distintos elementos de ellos. Se dará, a su vez, la valoración económica del mismo.

Por último, y como ejemplo de la flexibilidad del diseño elegido veremos dos modificaciones sobre el diseño original. El primero de ellos será una ampliación para dar mayor seguridad en cuanto a redundancia de almacenamiento y, ya en un paso definitivo, montar un CPD remoto.

El segundo de ellos será un diseño de bajo coste, en el que, mantenimiento los mismos servicios, bajaremos el coste del diseño con productos con algo menos de prestaciones, pero manteniendo la solución en conjunto unos altos niveles de calidad y servicio.

Abstract

The basic needs of companies are often the same, whether a large company that small, the infrastructure on riding their business processes and applications to manage them are often nearly equal. If we divide the ICT infrastructure of a company in hardware, system and applications, we can see that in most of them the system is almost identical.

Moreover, through virtualization, which has entered a landslide in the computer world, we can be fully detached hardware software, so that we get a huge flexibility when planning infrastructure deployments.

On these two ideas, uniformity and independence of hardware system, are about to be developing the next TFG.

For the development of the first one will be the study of basic infrastructure (or system) that any company usually has. Will try to find a solution that is valid for a lot of companies in our area and will take place on design.

With the second idea will develop a service-based system that is complete enough to be able to respond to the needs views but at the time, sufficiently flexible to growth in capabilities or services can be performed easily without the structure the system or its modules to be modified to make them.

Therefore, we will conduct a full and complete design, so that will be both hardware and software, emphasizing the integration of systems

and the interrelation between the different elements of them. It will, in turn, economic valuation of the same.

Finally, as an example of the flexibility of the design chosen will see two modifications to the original design. The first will be an extension to provide greater security for redundancy storage and, as a final step, mount a remote data center.

The second one will be a low cost design, in which maintaining the same services, we will lower the cost of product design with slightly less performance, while maintaining the solution set high standards of quality and service.

INDICE

1.- Introducción

Que la informática forma parte del día a día de la gran mayoría de las empresas es algo que a día de hoy ya nadie discute, no concibiéndose montar una empresa sin tener un soporte informático de la misma.

Es más, frente a la visión primigenia de la informática como un gasto desde el punto de vista económico, o una serie de elementos en mayor o menor medida interconectados, en mayor o menor medida útiles o ya en el peor de los casos una forma de poder despedir a personal, desde el punto de vista de la gestión, ha surgido la visión de la informática como un generador de riqueza de la propia empresa, alineándose en todo momento con las líneas de negocio de la misma, o incluso, creando sus propias líneas de negocio relacionadas con ella.

Este cambio lo hemos podido ver reflejado muy bien en el hecho en que en las grandes empresas los departamentos de informática han pasado de depender, en la gran mayoría de los casos, de los departamentos económico financieros a depender de dirección e incluso en muchos casos, los responsables de informática formar parte del Staff de la empresa, participando activamente en la toma de decisiones no solo de informática, sino de todas las líneas de negocio en la que ella interviene, es decir, en todas.

Desgraciadamente hay un sector de empresas, las PYMES, que por su tamaño y recursos les es imposible poder realizar este cambio, quedándose en muchas ocasiones atrás en cuanto a tecnología, conocimiento y posición en el mercado.

Esta falta de capacidad para poder utilizar las nuevas tecnologías y aprovecharse de ellas viene dada por dos factores, el primero de ellos el coste económico, y el segundo de ellos, que es el mas importante, el conocimiento y la formación en nuevas tecnologías.

El coste económico se explica por si solo, en cuanto al conocimiento y la formación en nuevas tecnologías, hay que entender que en esta rama de empresas es muy extraño que haya un departamento informático suficientemente grande detrás, normalmente nos podremos encontrar con un informático, chico para todo, que probablemente no tenga tiempo de formarse o, lo que es mas normal, ningún informático y algún administrativo sea el que soporte las tareas informáticas.

En este TFG trataré de dar solución a estos dos problemas para una empresa tipo.

El problema del coste económico se solventara mediante el uso de la virtualización (se explicara mas adelante), la cual nos permite un uso mas efectivo de los recursos informáticos, por lo que con menos recursos podemos dar un mejor nivel de servicios, la consecuencia directa es que el coste en equipamiento baja considerablemente.

La problemática del conocimiento y formación se solventara al realizar el diseño cerrado, completo y operativo.

VIRTUALIZACIÓN

La tecnología de virtualización ha revolucionado la informática tal y como la conocíamos hasta su llegada, convirtiéndose rápidamente en una tecnología ampliamente difundida en el sector.

Hay diferentes formas de clasificar la virtualización, vamos a ver dos de ellas:

Atendiendo a sobre que se ejecute el software de virtualización

- Hospedada (*Hosted*): El software de virtualización se instala en una maquina con un S.O. (Eje. Virtual box, VMWare Server,...), con lo que compite con este por los recursos hardware

- Nativa (Bare-metal): EL software de virtualización se instala directamente sobre el Hardware. Este software es un software específico que se llama *Hypervisor* (Ej., VMWare ESXi, Microsoft Hyper-V,...) y es en exclusiva el que gestiona el hardware

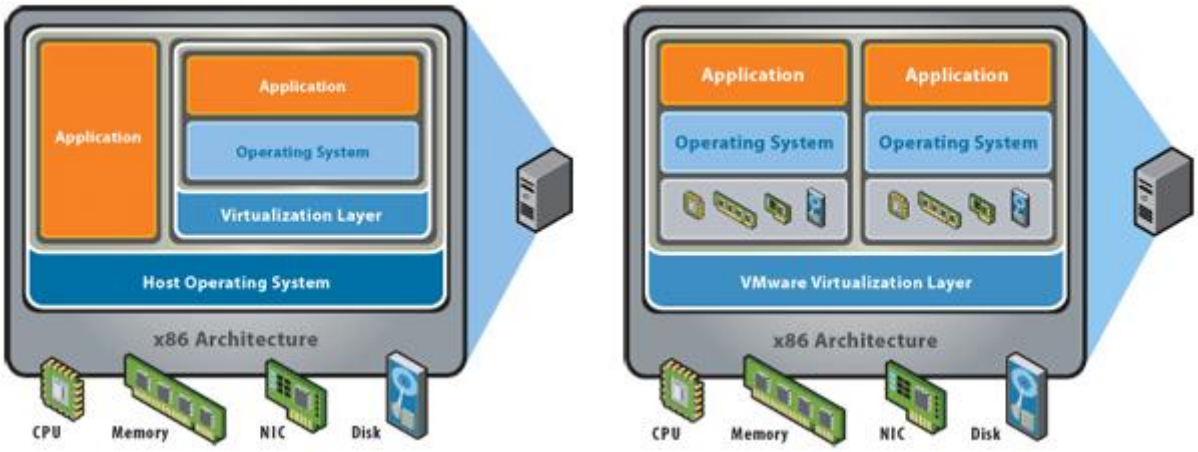


Ilustración 1: Virtualización Hospedada frente a nativa para arquitectura x86 con VMWare

Atendiendo a quien ejecute el software de virtualización

- Virtualización de servidores: Se trata de virtualizar los servidores

- Virtualización del puesto de trabajo (VDI): Se trata de virtualizar el escritorio de los clientes.

En nuestro TFG nos centraremos en la virtualización de servidores de forma nativa, por lo que a partir de este momento cuando nos referimos a virtualización nos estamos refiriendo a esta en concreto.

Simplificando mucho la virtualización se trata de ejecutar varios servidores virtuales dentro de un servidor físico, siendo estos totalmente independientes entre si, pudiendo tener distintos S.O. e incluso distinto hardware (virtual).

A estos servidores virtuales se les asignan una porción del hardware de la maquina física (memoria, disco, CPU, dispositivos de E/S,…) y corren a la vez en ellos.

Las ventajas son múltiples, citaremos a continuación las más importantes:

- Ahorro de costes: Los servidores son utilizados al máximo con lo que con tenemos que gastar menos en hardware. Además, la consiguiente disminución en el número de servidores redunda en un menor consumo energético, sobre todo en electricidad y refrigeración

- Ahorro de espacio: A menor necesidad de hardware, menor necesidad de espacio físico. Esto también puede redundar en la bajada de costes de alquileres.

- Mejora en la disponibilidad del sistema: Las maquinas virtuales se pueden copiar completas por lo que su recuperación es

sencilla. Además por su propia naturaleza son capaces de soportar *failover*([1]) de forma nativa a nivel de servidor, por lo que aplicaciones que no tengan esta capacidad la pueden adquirir a través de ella.

- CPD Remoto: Es muy sencilla la creación de CPDs remotos gracias a la virtualización.

- Creación de entornos de Preproducción y desarrollo fácilmente

- Capacidad de vuelta atrás en la aplicación de actualizaciones o parches de los sistemas.

- Mantenimiento de sistemas desfasados o que hayan dejado de estar soportados: Al poder realizar virtualizaciones de sistemas ya en producción, en caso de tener algún sistema que haya dejado de estar soportado y queramos mantenerlo mas seguro, podemos virtualizarlo y poner esa virtualización en sistemas que si tenemos soporte.

Estas son solo algunas de las mejoras que incluye la virtualización, pues son muchas más. Es una opinión muy extendida entre los administradores de sistemas que es, no solo una nueva tecnología, sino toda una revolución que ha hecho cambiar, no solo la forma de manejar la tecnología, sino la forma de pensar el diseño y gestión de los sistemas.

[1] FailOver o tolerancia a fallos es la capacidad de un sistema de seguir funcionando a pesar de un fallo, normalmente Hardware, gracias a redundar algunos o todos sus elementos. Cuando uno falla el otro asume todo el trabajo consiguiendo que no se pare el sistema completo.

En el momento actual es una tecnología suficientemente probada y con un nivel de madurez altísimo, con una gran cantidad de soluciones disponibles en el mercado, mucha información y muchas personas trabajando con ella.

Por todo ello es por lo que hemos decidido basar todo el proyecto en la tecnología de virtualización.

2.- Estado Actual y Objetivos

En el diseño que vamos a elaborar vamos a partir de la idea de una empresa de tamaño mediano (PYME) que va a implantar un sistema informático partiendo desde cero, es decir, sin nada absolutamente implantado.

Se va a realizar el estudio de las necesidades de la empresa en cuanto a infraestructura básica de informática, sobre la que irán creciendo los servicios, aplicaciones, programas y demás elementos software que darán la lógica del negocio de la misma de una forma totalmente sencilla y escalable.

El objetivo final de este TFG será el diseño completo e integral del este sistema. Integral en cuanto a que englobarán tanto la parte hardware como software y completo en cuanto a que cubrirá todas las necesidades de la empresa en cuanto a infraestructura de tecnologías de la información.

Lo primero que vamos a hacer es evaluar las necesidades básicas de las empresas, intentando sacar de este análisis los elementos que son

comunes a todas ellas y sobre los cuales van creciendo los demás elementos de la lógica de negocio.

A partir de este estudio extrapolaremos los resultados para la empresa en cuestión que estamos haciendo el diseño. El mismo, intentaremos que sea lo mas genérico posible, de forma que sirva como modelo de implantación para cualquier empresa de estas características, simplemente cambiando los componentes hardware para adecuarlos al momento en que se este realizando la implantación.

Se tratara además de dar respuesta a las nuevas tendencias del mercado en el que los dispositivos que se pueden conectar a la red ya no son simplemente PCS, sino que hay una amplia gama de dispositivos que pueden conectarse a la red, como son portátiles, tabletas, *smartphones*, clientes ligeros, etc.

También se tratara de solventar la movilidad externa. Es decir, que no solo se puedan conectar desde dentro de la red sino que, evidentemente contratando previamente con un proveedor de servicios una ip estática, se crearan los servicios necesarios para poder acceder a la red de la empresa desde cualquier sitio, mejorando la productividad del personal, permitiendo el teletrabajo y fomentando la deslocalización.

Todos estos servicios se trataran de diseñar con unos niveles de rendimiento adecuado para cada uno de ellos. También se trataran los aspectos de disponibilidad de los mismos, tratando de dar una alta disponibilidad que minimice las posibles caídas del sistema.

Como siempre no es posible evitar las caídas del sistema ni la corrupción o perdida de datos también se tratara de dar una solución para la recuperación ante desastres.

Como un inciso, vamos a explicar la diferencia entre alta disponibilidad y recuperación ante desastres. La primera de ellas trata de que el sistema no caiga. Se trata de poner todos los medios disponibles para que ante una eventual caída de alguno de los elementos de los que se compone el mismo, normalmente, a través de la duplicidad de todos aquellos elementos que se pueda. La segunda de ellas trata de, una vez ya haya ocurrido el desastre, poder recuperar tanto la información, como el sistema que lo sustenta.

Por ultimo, y no menos importante, se trataran los aspectos de seguridad del sistema. El mismo lo podemos dividir en dos, la seguridad de los accesos a los recursos, el cual lo solventaremos con un sistema de identificación y autenticación y la seguridad de las conexiones externas al sistema, el cual intentaremos solventarlo con la puesta en marcha de un sistema de certificación.

Se tratara, además, de dar un servicio de monitorización del sistema en tiempo real, el cual nos dará una visión de la salud del mismo.

3.- Aportaciones

Aportamos el capacitar a empresas que, por su infraestructura, tamaño y presupuesto no pueden acceder tecnologías en auge, la posibilidad de implantación de un sistema integral, completo y flexible, con altas prestaciones y alta disponibilidad, basadas en tecnologías de última generación.

Haremos el diseño completo, por lo que liberamos a las gerencias de estas empresas de estar buscando entre las diferentes tecnologías, cuales son las que mejor se adaptan a sus necesidades.

Con este diseño facilitaremos la tarea de la implantación de las TICS en las empresas que por su reducido tamaño, no han dado el paso hacia ellas, abrumadas, quizás, por la cantidad enorme de información, productos, servicios y diferentes ofertas comerciales existentes en el mercado.

También puede servir como base a la hora de el decidirse a montar una nueva empresa. Aporta una visión bastante clara de las necesidades básicas, sobre las cuales, se permite seguir creciendo fácilmente si la misma lo requieres.

Se derivan dos aspectos fundamentales de la implantación de estas TICS en el entorno de la mediana empresa canaria, uno, directamente en la propia empresa y el segundo, para todos aquellos que vivimos de las TICS.

El primero de ellos, y es el objetivo que más en boga esta en estos tiempos de crisis, es el aumento de la competitividad. No podemos seguir haciendo las cosas como hasta ahora, hay que dar un salto hacia delante y lanzarse a reducir costes en base a una mejor planificación y gestión de los recursos. En este TFG se darán capacidades a las empresas de teletrabajo, conexión continua y continuidad del negocio. Todas ellas claramente redundan en un aumento de la competitividad de la empresa.

También se deriva un mejor posicionamiento en el mercado. En un mundo tan rápido, el que desde cualquier dispositivo puedas conectarte a la empresa y realizar pedidos, revises stocks o puedas ver catálogos de productos puede suponer la diferencia entre conseguir una venta o perderla. Este TFG tratará de aportar estas capacidades.

El segundo de ellos es también muy evidente. El aumento del uso de las TICS en las empresas hará que la demanda de profesionales del sector aumente. Además, dado el nivel de las tecnologías utilizadas, serán profesionales que requieran un alto nivel de capacitación, como pueden ser los ingenieros o graduados en informática.

4.- Análisis

4.1.- Análisis de las necesidades Básicas de las empresas

Se procede a realizar un análisis sobre las necesidades básicas de las empresas en general y las PYMES (sector donde se encuentra la empresa de la que es nuestro TFG) en particular.

Para ello vamos a tener en cuenta que el objetivo de este TFG es crear la infraestructura básica del sistema. La misma será lo suficientemente flexible para que servicios que den mayor capacidad de lógica a la empresa, como pueden ser bases de datos, ERPs, sistemas de toma de decisiones o cualquier otra aplicación, puedan entrar a formar parte de la misma de una forma sencilla, pero que en un principio, quedan fuera del diseño propuesto.

Independientemente del tamaño de la empresa hay ciertas necesidades básicas que se dan en todas:

- Interconexión y comunicación entre equipos

- Almacenaje de información

- Acceso a la información
- Identificación de los accesos
- Seguridad en los accesos
- Continuidad del negocio
    - Necesidad de disponibilidad del sistema
    - Necesidad de recuperación ante desastres
- Gestión de los procesos de negocio

4.1.1.- Red de comunicación

Lo primero y fundamental que hay que montar en cualquier empresa es una red de comunicaciones. Hoy en día no se concibe ya la idea de estaciones de trabajo independientes, sino todos los dispositivos funcionando conectados entre ellos.

Además, el modelo más extendido es el de cliente / Servidor, donde toda la información y datos de la empresa están en una serie de servidores y los usuarios se conectan a ellos a través de PC u otros dispositivos de conexión.

Evidentemente ahora mismo no nos plantearíamos otra cosa que no fuera la implantación de una red local (LAN) con tecnología *Ethernet*.

Damos por hecho que el enrutamiento hacia el exterior es contratado con una empresa proveedora de servicios de Internet, por lo que

nosotros haremos el diseño basándonos en un par de switches de red. Notar que ponemos dos para dar la alta disponibilidad, aunque con uno es más que probable que pudiéramos haber montado una LAN para una empresa del tamaño de la que estamos estudiando.

4.1.2.- Almacenaje de la información

Tenemos dos tipos de información fundamental que guardan las empresas, datos estructurados y datos no estructurados.

Entendemos por datos estructurados aquellos que están organizados y tienen una lógica de acceso, básicamente encontramos aquí las bases de datos. Se caracterizan porque están diseñados para hacer búsquedas muy eficientes.

Por otro lado encontramos los datos no estructurados, como pueden ser las hojas de cálculo, las fotografías, correos electrónicos, videos, etc. En definitiva, todos aquellos datos que no tienen una estructura definida y que, por lo general, no tienen una lógica de acceso más que por el contenido. La búsqueda de alguno de ellos normalmente suele ser pesada.

Todas las empresas tienen, como mínimo datos no estructurados, aunque la gran mayoría hoy en día también disponen de bases de datos estructuradas para almacenar la información de la empresa.

Tanto unos como otros necesitan de servidores con suficiente capacidad de disco para poder depositar ahí la información. Llamamos normalmente a estos servidores de ficheros y suelen ser los primeros en ser implantados siempre en las empresas.

4.1.3.- Identificación de los accesos

Los accesos al sistema no solo se tienen que dar, sino que tienen que identificarse. La seguridad minima que debe cumplir cualquier sistema es que los accesos al mismo sean nominales, no pudiendo existir, o, minimizar al máximo los accesos anónimos.

Esto hay dos formas de hacerlo, usuarios locales o centralizados (servicio de directorio).

La primera de ellas, ya casi desaparecida, es crear los usuarios en el mismo sitio donde este el recurso que se va a compartir o usar. Tiene la grandísima desventaja de que cada vez que se vaya a compartir el recurso hay que crear el usuario tanto en el servidor como en el cliente, con el mismo nombre y la misma contraseña. Ante cualquier cambio de usuario o contraseña en el servidor hay que reconfigurar el cliente. El ejemplo más típico de esta configuración son los grupos de trabajo de MS Windows.

La segunda de ellas, como yo he llamado centralizada, se basa en el uso de un servicio de directorio LDAP ([2]). Grosso modo, el mismo mantiene una base de datos centralizada de objetos (usuarios, impresoras, PCS,…) que es accesible desde toda la red. Tiene la ventaja que es un repositorio único de identificadores, con lo que solo en un sitio es donde se guardan las credenciales de usuario, normalmente, de forma cifrada.

Además de las grandes ventajas que supone la centralización de los usuarios (Creación en un único punto, cambios de contraseña

[2] LDAP en realidad no es un servicio de directorios sino el protocolo, pero a efectos de este trabajo lo usaremos como analogía.

transparentes, etc., etc.), una de las que me gustaría destacar es el hecho de que la baja de un usuario provoca su baja en un solo lugar, con lo que evitamos posibles problemas de seguridad si tenemos N sistemas en los que darle de baja.

Por supuesto se ha tenido en cuenta que la mayoría de los sistemas comerciales actuales vienen ya con la posibilidad de integrarse, ya sea en algunos de los servicios de directorios más conocidos (Active Directory, OpenLDAP) o, en su defecto, con un servicio de directorio que cumpla el estándar (LDAP).

En nuestro caso adoptaremos esta segunda forma de trabajo y diseñaremos el uso de un servicio de directorio para nuestro proyecto. Todos los usuarios que entren en el sistema tendrán que validarse contra este directorio quedando identificado unívocamente y durante todo el tiempo en que este conectado a la red.

4.1.4.- Seguridad de los accesos

Podemos hablar de dos tipos de seguridad en los accesos de un sistema. El acceso físico, es decir, que alguien pueda entrar físicamente al lugar donde tenemos el sistema o la red y pueda entrar a ver la información, y la seguridad en los accesos lógica, es decir, la seguridad en los accesos a través de la red.

Evidentemente la primera de ellas queda fuera de este estudio y en cuanto a la segunda podemos dividirla en dos, seguridad en los accesos a los recursos una vez hemos entrado al sistema y la seguridad de los accesos externos.

En la primera de ellas se trata de dar los permisos adecuados a cada usuario una vez ya han entrado en el sistema y se han identificado,

normalmente, son accesos lícitos al mismo. Trata de que el usuario solo tenga acceso a aquella información o recursos que sea necesarios para su trabajo, cumpliendo así el principio de mínimo privilegio.

Los datos y los recursos que vamos a diseñar tendrán asignados unos permisos para los usuarios, por lo que solo aquellos que cumplan los permisos adecuados podrán hacer uso de ese recurso o entrar a ver o modificar la información a la que están intentando acceder.

La forma en la que lo haremos será aprovechando la integración de los sistemas con el LDAP que hablamos en el apartado anterior. Cuando los usuarios entran en el sistema están validados por el LDAP, cuando intenten acceder a un recurso se verificarán que tiene permisos sobre el y se le permitirá o no según sea el caso.

Evidentemente la gestión de estos recursos nos la da el día a día y serán algún gestor de la empresa el encargado de asignar estos permisos.

La seguridad de los accesos externos trata sobre la forma en que se pueda acceder desde el exterior (Internet) a la red local y a todos los recursos que en ella estén.

Es una realidad la cantidad enorme de problemas de seguridad que hay en cualquier sistema conectado a la red Internet. Los mismos se ven aumentados si lo que queremos no es solo usar los servicios que la red Internet nos ofrece, sino que somos nosotros los que queremos ofertar estos servicios, como pueden ser webs de compras, portales de empleados, CRM, Extranets, etc.

En el caso que nos ocupa queremos diseñar accesos externos para el personal de la oficina. Las ventajas que nos dan son muchas,

teletrabajo, deslocalización, acceso 24 horas, conciliación familiar, y un largo etc., por lo que parece que vale la pena correr el riesgo de plantearnos un sistema de accesos remotos a pesar de los problemas de seguridad que acarrean.

Evidentemente no podemos quitar todas las amenazas, ni podremos estar seguros al 100%, pero intentaremos diseñar un sistema lo suficientemente seguro. Para ello planteamos un sistema con las siguientes características:

- Conexión VPN: Se diseñara un servidor VPN de forma que para entrar desde el exterior habrá que realizar un túnel VPN que es más seguro que una conexión directa desde Internet a la red puesto que proporciona autenticación, autorización y cifrado punto a punto.

- Único punto de entrada: Se diseñara un servidor de terminal Server. Todos los usuarios desde la VPN solo podrán entrar a este servidor y no al resto de la red, concentrando los accesos en este servidor y minimizando el espectro de un posible ataque.

- Certificación: Diseñaremos un servidor de certificación. Los usuarios que quieran conectarse desde el exterior deberán pedir estos certificados para poder conectarse. La entidad certificadora estará integrada con los usuarios del LDAP.

4.1.5.- Continuidad del Negocio

Entendemos por continuidad del negocio todas las políticas, herramientas, protocolos y planes orientados a no perder o recuperar las funciones de la empresa tras una interrupción no deseada.

Estos planes no se centran solamente en la informática, sino en todos los procesos de negocio de la empresa, pero, como no podía ser de otra forma, la informática forma una parte de fundamental de estos planes.

Reduciendo estos planes a la infraestructura TIC que nos conlleva, dividiremos en dos apartados nuestro estudio: Disponibilidad y recuperación ante desastres.

4.1.5.1.- Necesidad de disponibilidad del sistema

"El tiempo es oro" reza un adagio inglés. Si bien esto en la vida ordinaria es real, en una empresa pasa a ser algo estructural. Gran parte del trabajo de los gestores de las empresas es conseguir el mayor rendimiento posible de sus trabajadores, es decir, mayor competitividad. A mayor competitividad de mis trabajadores más competente será mi empresa y mejor posicionado estaré en el mercado.

Una de las formas de conseguir una mayor competitividad es que los trabajadores estén trabajando la mayor cantidad de tiempo efectivo posible (hay otras como mejorar los procesos de negocio, formación, adecuación de infraestructuras, etc.) y es aquí donde entra la necesidad que el sistema este la mayor parte del tiempo disponible.

Toda caída del sistema o parte de el provoca unos costes a la empresa. Los más evidentes son los costes económicos derivados de la parada en la producción de la misma, principalmente en personal no puede realizar sus tareas. Ni que decir tiene que si, además, de la disponibilidad del sistema dependen áreas como ventas o logística, una caída del mismo puede producir que no solo podamos perder ventas, sino que incluso tengamos que devolver parte del dinero que hemos

cobrado por servicios que no hemos podido realizar (véase por ejemplo una empresa de mensajería).

Menos evidente, pero asimismo igual o más dañino, puede ser la perdida de imagen. La desconfianza de nuestros clientes, unida a una mala publicidad, puede hacer mucho daño a una empresa, provocando una perdida de contratos. Ni que decir tiene que hay empresas competidoras que están dispuestas a aprovecharse para darnos mala publicidad.

Para todo ello trataremos de dar una solución de disponibilidad del sistema. La forma en la que trataremos de hacerlo será duplicar aquellos elementos del sistema que sean posibles para asegurar que la interrupción de uno de ellos no afecte al sistema en general.

Evidentemente entra en juego aquí los costes económicos. Trataremos de dar una solución de disponibilidad con un coste asumible, sabiendo que en caso de requerir una disponibilidad más alta podremos conseguirla a un coste mayor.

4.1.5.2- Necesidad de recuperación ante desastres

La disponibilidad del sistema no siempre es posible. En muchos casos hay elementos del mismo que, ya sea por su coste o ya sea por su naturaleza, no se pueden duplicar.

Además, hay errores que no son debidos a algún suceso desastroso, sino que está involucrado el factor más determinante: El factor humano. Pensemos por ejemplo en un empleado de un departamento de RRHH que elimina de la base de datos a un usuario. No es un fallo

del sistema, pero si es un desastre que es necesario recuperar para que el sistema vuelva a ser consistente.

Nuestro diseño contemplara la recuperación de desastres a través del sistema de copia de seguridad, gracias a la cual, tendremos una copia *offline*, tanto de los datos del sistema, como del sistema en si.

Aquí es donde la decisión de la virtualización se hace mas que patente. La naturaleza de las maquinas virtuales hace que estas sean físicamente ficheros. Al poder copiar estos ficheros, tenemos copias del sistema de forma que recuperar un sistema caído y no recuperables es simplemente recuperar de la copia estos ficheros.

Además, es independiente de Hardware. Lo que quiere decir que en el peor de los casos en que no podamos recuperar el hardware, podemos comprar uno nuevo y levantar nuestro sistema simplemente copiando estos ficheros en el nuevo hardware, sin necesidad de instalaciones nuevas (a excepción del propio sistema de virtualización, por supuesto).

Simplemente como comentario, pues el coste lo hace prohibitivo para el ramo de empresa a la que va orientada este TFG, decir que podríamos llevar estos ficheros a otro sistema en otro lugar y mantenerlos en estado espera. Ante un desastre absoluto (terremoto, inundación, guerra,..) se podría levantar el sistema en ese otro lugar, en definitiva, tener un CPD remoto, de una manera muy sencilla en comparación a la gestión de CPDs remotos sin virtualización.

4.1.6.- Gestión de los procesos de negocio

Como puede haberse notado, en todo este análisis hemos pasado muy de puntillas por la naturaleza propia de la empresa. No hemos analizado a que se dedica, cual es su rama o en que segmento está.

Esto es así porque como hablamos al principio, este TFG se va a centrar en crear una infraestructura mínima que tiene la empresa, sobre la cual se soportaran el resto de aplicaciones o servicios de la misma, si bien es verdad que gran parte de las empresas del segmento PYME con esta infraestructura mínima tendría de sobra para funcionar.

Por esto en este apartado simplemente definiremos a que nos referimos por gestión de procesos de negocio y nombraremos algunos ejemplos, pero no propondremos ninguno para nuestro diseño.

Entendemos como gestión de los procesos de negocio todo aquel software que lo que trata es de realizar la gestión de la empresa y el trabajo que hace. Normalmente el mismo esta alineado con las líneas de negocio y suelen reflejar alguna de ellas, o todas en caso de sistemas integrales.

Normalmente todas ellas tienen como base algún gestor de base de datos, como pueden ser *Oracle, SQL Server, Sybase, Access, MySQL, Informix, etc.*

Por encima de ellas se implantan las aplicaciones, estrechamente relacionadas con la actividad de la empresa y, precisamente por eso, poco intercambiables. Por ejemplo, una empresa de alquiler de coches tendrá una aplicación que probablemente no sirva para una empresa de pesca o un hospital.

Existe una gran cantidad de aplicaciones de gestión para líneas de negocio específicas, como son software de contabilidad, de RRHH, de gestión documental o de almacenaje.

No obstante hay intentos de software genérico en el mercado (ERP) que tratan de estandarizar los máximo posible los procesos de negocio de las empresa, como pueden ser el caso de *SAP, Microsoft Dynamics, Oracle e-Business Suite*. La idea principal de estos es a un núcleo central de módulos que tienen todas las empresas (Contabilidad, Facturación,…) ir añadiendo módulos adicionales dependiendo del ramo de la empresa (módulo de RRHH, módulo de Hospitales, módulo de Gestión logística,..), que tienen la gran ventaja de estar totalmente integrado.

No olvidar tampoco la posibilidad de que haya software hecho a medida para una determinada empresa, el cual es el caso mas evidente de software que no podemos intercambiar entre empresas.

Independientemente de que sea software estándar, aplicaciones específicas, ERP o aplicaciones a medida, la forma de integrarlas en nuestro sistema será la creación de una nueva máquina virtual dedicada para esa aplicación y meterla dentro de nuestro pool de servidores.

Una vez más, la virtualización nos muestra aquí sus ventajas en cuanto a flexibilidad.

4.1.7.- Conclusiones

En resumen, hemos visto cuales son los sistemas que tienen las empresas y cuales son los servicios necesarios para cubrir las necesidades de las mismas.

De este análisis extraemos los servicios que vamos a aportar con nuestro diseño, que son:

- Red
- Servicio de ficheros
- Servicio de directorio (LDAP)
- Servicio de VPN
- Servicio de Terminal Server
- Servicio de Certificación
- Sistema de Backup

4.2.- Análisis de la solución de alta disponibilidad

La disponibilidad del sistema puede definirse como la cantidad de tiempo que este esta accesible para los usuarios. Evidentemente lo ideal es que este tiempo sea del 100%.

La disponibilidad del sistema se ve mermada por varios factores. Entre los más importantes tenemos los tiempos de inactividad debido a

mantenimientos y los tiempos de inactividad debidos a caídas del sistema no controladas.

La primera de ellas no podemos evitarlas y se verán mejoradas con una correcta planificación de las mismas, un uso de herramientas de mantenimiento programadas y, como no, con la actuación fuera de horarios de máximo trabajo.

Las segundas son las que van a ser objeto de estudio en este apartado y trataremos de llegar a una solución lo suficientemente buena, entendiendo que no existe una capacidad de disponibilidad 100%, o, al menos, no a un coste tal que sea asumible para el segmento de nuestra empresa.

Entendemos alta disponibilidad como la capacidad del sistema de sobreponerse a la caída de alguno de sus elementos individuales, siguiendo con la actividad de forma normal o, a lo sumo, con una pequeña merma en el rendimiento, pero nunca la parada del mismo.

La alta disponibilidad es una estrategia más que una decisión de diseño, y que por su importancia, no solo engloba a todos los elementos del sistema, sino que marcara la pauta de todos los elementos futuros que se integren en el mismo, de hecho, en las grandes corporaciones la disponibilidad es medida de forma empírica, estableciéndose los tiempos máximos de indisponibilidad del sistema y creándose estándares y protocolos que cualquier elemento, hardware o software, que se quiera integrar o introducir en el mismo debe cumplir para ser aceptado.

No llegaremos a este nivel de análisis pues requeriría prácticamente un TFG completo (véase que no solo es la parte técnica, sino que incluye

mucha parte de gestión, RRHH, gestión de proveedores y empresas de servicio, etc), lo que nosotros vamos a hacer es intentar redundar todos aquellos elementos fundamentales dentro del sistema, de forma que ante la caída o el fallo del funcionamiento de alguno de ellos el otro pueda seguir haciéndose cargo del trabajo del otro.

Lo primero que tenemos que hacer es identificar los elementos susceptibles de tener un fallo y ver si tenemos posibilidad de redundarlo y como hacerlo.

Comenzaremos con un análisis desde lo más abajo (Red y Hardware) hasta lo más alto (sistemas y software). Una vez más, nos apoyaremos en la virtualización para conseguir una alta disponibilidad a un coste asumible, tanto económico como de gestión.

4.2.1.- Red

Como no podía ser de otra forma la red que vamos a crear será una red LAN Ethernet. Como elemento de interconexión de la red utilizaremos un conmutador de red o switch.

Lo normal en las empresas pequeñas del sector de la que estamos realizando el diseño es tener un único switch (cuando no todavía un HUB) y todos los equipos conectados a el.

Para conseguir una alta disponibilidad del sistema en la parte de red, lo que haremos será duplicar este switch y conectar los dos, de forma que la caída de uno de ellos hace que el otro siga funcionando.

Hacer notar aquí que la disponibilidad es relativa, si bien los servidores los diseñaremos con al menos dos tarjetas de red (se vera mas adelante)

de forma que el corte ante la caída de uno de los Switches es totalmente transparente, lo normal es que los equipos clientes (pcs, impresoras, portátiles por cable,…) tengan que ser vueltos a cablear en caso de una caída de uno de ellos.

4.2.2.- Red de almacenamiento (NAS)

Uno de los elementos más importantes a la hora de conseguir una alta disponibilidad es que el almacenamiento no dependa de ningún servidor, es decir, que este fuera de ellos.

Con esto, lo que conseguimos es que en caso de caída de un servidor o en caso de fallo de disco de alguno de ellos, el almacenamiento no se vea afectado.

Para ello vamos a proponer en el diseño montar todo el almacenamiento en una red de almacenamiento externo tipo NAS (se verá en análisis Hardware).

La misma, además, debe cumplir con los siguientes requerimientos:

- Soportar distintos niveles de redundancia de discos (RAID), como mínimo Raid1.

- Tener redundancia de fuente de alimentación: Para que el fallo de una de las fuentes de alimentación o del circuito eléctrico no haga que se nos caiga la red de almacenamiento.

- Tener redundancia de controladora: El fallo de una controladora no nos debe afectar.

- Tener redundancia de red: Teniendo en cuenta que se conecta por red a los servidores, es fundamental que esta este redundada.

- Tener redundancia de ventilación.

En el diseño que vamos a hacer, esta red de almacenamiento es el núcleo central de todo, sin ella, nada funcionará. Lo ideal sería tenerla redundada, pero es el elemento más caro de toda el diseño y su redundancia haría que el presupuesto subiera muchísimo.

De todas formas se hará un diseño en ANEXO con redundancia de red de almacenamiento.

4.2.3.- Servidor

En este apartado vamos a analizar las características que tiene que tener los servidores para la alta disponibilidad.

Notar aquí que cuando hablamos de servidor estamos hablando de servidor físico y no virtual, es decir, el que sirve de soporte a los virtuales.

Un servidor físico no deja de ser un sistema informático tipo PC (aunque con mucha más potencia). Los elementos principales que lo componen son disco, memoria y CPU. Además lo componen otros dispositivos sin los cuales no podría funcionar como son las fuentes de alimentación, los ventiladores o las tarjetas de red. También tienen una serie de buses internos, pero que en nuestro caso, no los podemos hacer participe de nuestro estudio, porque no se pueden redundar.

Para una alta disponibilidad los servidores deben cumplir con los siguientes requerimientos:

- Redundancia de fuente de alimentación: Mínimos dos fuentes de alimentación teniendo cada una capacidad suficiente para poder mantener por si sola el servidor.

- Redundancia de tarjetas de red: Dos o más tarjetas de red.

- Dos discos de sistema para poder crear un disco redundante Raid1 (espejo).

- Redundancia de ventilación.

- Redundancia de CPU: Montaremos sistemas multi-procesador además de *multicore*. La caída de uno de los procesadores hará que el sistema vaya más lento, pero no lo parará.

- Redundancia de los módulos de memoria: Como mínimo habrá dos módulos de memoria.

Cualquier fallo en uno de los elementos de esta lista no provocará la caída del servidor, sino que este seguirá funcionando, quizás con menor rendimiento, pero normalmente, dándonos tiempo para poder arreglar el error.

También, para una alta disponibilidad, contemplamos la posibilidad de una caída total del servidor, por lo que tendremos un mínimo de dos servidores, de forma que en caso de caída de uno de ellos, el otro asumiría el trabajo del otro, para ello, una vez más, nos apoyaremos en la virtualización.

4.2.4.- Sistemas Operativos y Software

Hasta ahora hemos visto la parte más "visible" en cuanto a la pérdida de disponibilidad, que es ocuparnos de una posible caída de un elemento físico del sistema.

En la mayoría de los casos estos son los fallos más comunes, pues toda la lógica, los sistemas operativos, los procesos, las aplicaciones, van sobre esta parte física y, además, es la que más suele fallar.

Por tanto, lo normal es que el fallo en una parte lógica del sistema venga de un fallo en la parte física. La alta disponibilidad de esta parte la conseguimos gracias, de nuevo, a la virtualización.

Toda la parte lógica del diseño esta montada sobre maquinas virtuales. Las mismas estarán visibles para todos los servidores físicos del sistema, gracias a que las mismas están en la red de almacenamiento que es accedida por todos los servidores.

La caída de uno de los servidores provocará que las maquinas virtuales que están en un servidor se pasen al otro y sigan funcionando, con lo que conseguimos un sistema de alta disponibilidad de la parte lógica del sistema.

Con esto obtenemos una alta disponibilidad incluso para aquellos sistemas que nativamente no la tienen.

4.3.- Recuperación ante desastres

Hemos hecho un estudio de diseño de alta disponibilidad, la idea, que el sistema se alo suficientemente robusto para aguantar la caída de algunos elementos individuales, o parte de ellos.

No obstante, siempre pueden ocurrir desastres de los que no somos capaces de recuperarnos aún habiendo aplicado la estrategia de la alta disponibilidad. Por ejemplo una caída de la red de almacenamiento, una caída de varios servidores a al vez, o, incluso, un error humano que provoque una perdida de datos o fallo del sistema (los administradores de sistemas no estamos exentos de cometer errores).

Por todo ello hay que prepara una estrategia de recuperación del sistema en caso de caída del mismo o de perdida, total o parcial, de información. En definitiva, vamos a definir los procesos de copia de seguridad.

La forma tradicional de realizar las copias de seguridad ha sido disponer de algún dispositivo de cinta magnética y copiar ahí los datos con algún software creado para ello.

La recuperación de un sistema se basaba en el hecho de, o recuperar la información que se había perdido desde este dispositivo en el caso que el sistema no hubiera caído, o, en caso de caída total del sistema, recuperar primero el sistema (normalmente una reinstalación) y a posteriori recuperar los datos.

También había estrategias para que la propia configuración del sistema se copiara, de forma que se pudiera recuperar este también sin una

reinstalación, aunque normalmente esta fallaba si no se realizaba sobre el mismo hardware.

En nuestro caso no vamos a usar un dispositivo de cinta sino que vamos a realizar las copias en una NAS de bajos coste. Esto nos permitirá tener los datos accesibles de una forma más rápida y fácil. Más rápido porque un disco es un dispositivo más rápido que la cinta, y más fácil, porque las cintas son dispositivos de búsquedas lineales, con lo que las búsquedas aleatorias de información dentro de ellas son más complicadas al tener que leer, para accedes a un dato, a un todos los datos anteriores.

Tiene la desventaja que normalmente son dispositivos mas caros y con mas probabilidad de errores. Al ser más caros lo normal es que se tengan menos copias que las que sueles guardar cuando tienes cintas.

De todas maneras, el diseño deja la puerta abierta para poder integrar un dispositivo de cintas y además de hacer las copias en la NAS hacerlas en cinta.

En definitiva, vamos a dividir en dos el proceso de copia de seguridad y el proceso de recuperación, la copia de seguridad del sistema y la copia de seguridad de los datos.

4.3.1.- Copia / Recuperación del Sistema

Reiteramos una vez más, en nuestro diseño todo se basara en maquinas virtuales, las cuales son las que tienen toda la lógica del sistema.

Una de las mayores ventajas de las maquinas virtuales es precisamente su facilidad a la hora de la recuperación. Esto viene dado por dos

motivos importantes, el hecho que las maquinas virtuales son ficheros y la independencia del hardware.

Las maquinas virtuales son ficheros. Estos ficheros si los copiamos y los llevamos a otro servidor fisico con el mismo software de virtualización, independientemente del hardware que tenga debajo, podemos arrancar la maquina virtual y comenzar a dar servicio.

Con esto en mente, nuestro proceso de recuperación del sistema se basa en hacer copias de nuestras maquinas virtuales completas. Es decir, copiaremos las maquinas virtuales completas en nuestra NAS de copia.

Este procedimiento de copia no interrumpirá el sistema y además será tal que el estado de la maquina virtual sea consistente.

Nuestro procedimiento de recuperación será tan sencillo de copiar la maquina virtual en algún servidor con el software de virtualización y arrancarlas.

Con esto, tendremos todo el sistema recuperado en muy poco espacio de tiempo y con todos los servicios exactamente iguales.

En el peor de los casos, tendremos que instalar el software de virtualización en un nuevo servidor, pero esto es relativamente sencillo en comparación con la recuperación de un sistema “a la antigua usanza”.

Notar aquí también que llevarnos el sistema completo a otra localización o hacer una copia de una parte de el para hacer pruebas es verdaderamente sencillo.

4.3.2.- Copia / Recuperación de los datos

Aunque al copiar las maquinas virtuales ya estamos haciendo copia también de los datos que lo contiene, haremos también un procedimiento de copia de seguridad de los datos.

Esto nos asegura que la copia es consistente, pues a veces las copias de las maquinas virtuales se realizan sobre ficheros abierto, además de poder recuperar ficheros individuales sin tener que recuperar un sistema completo.

También nos permite recuperar los ficheros que han podido ser borrados por error por un usuario.

Lo que haremos es la forma más clásica. Copiaremos los ficheros mediante algún software de copia de seguridad a nuestra red de almacenamiento. Intentaremos planificar un ciclo de copia hijo-padre-abuelo, que es el más clásico de todos.

En caso de necesidad de recuperación, simplemente copiaremos los ficheros de la NAS a la ubicación donde queramos.

Para una mayor capacidad de restauración y cubrir mas tiempo de trabajo intentaremos planificar las copias de sistemas completos y las de datos a horas disjuntas. Como las de datos si que afectan al sistema, las realizaremos en horarios nocturnos, mientras que las de datos las haremos a mediodía. Con esto, podemos reducir la ventana de perdida de datos a 12 horas en lugar de las 24 habituales.

4.4.- Análisis de la solución de de seguridad de los datos

Como vimos anteriormente, es fundamental en las empresas tener la seguridad en los accesos a los datos, para ello, debemos saber primero, quien es la persona que esta intentando acceder (identificación) y segundo, si tiene permiso sobre lo que quiere acceder (derechos de acceso).

4.4.1.- Identificación

Como vimos también anteriormente, la identificación la podemos hacer de forma local al recurso que queremos compartir o de forma remota, es decir, dejar en manos de un tercero la identificación y el manejo de credenciales.

A pesar de lo avanzado de las comunicaciones en informática, todavía muchas personas prefieren la opción local, pero esto genera una cantidad enorme de problemas como la seguridad, la integridad o el aumento de trabajo de gestión, por citar solo algunos de ellos.

En nuestro caso vamos a optar por un sistema centralizado de identificación, lo cual nos dará una serie de ventajas entre las que destacamos:

- Seguridad: Todas las credenciales de usuarios están en un único punto, evitando que sistemas individuales contengan información de credenciales almacenadas en ellos, limitando el espectro de un posible ataque.

Otra mejora en la seguridad es que los sistemas centralizados en generalmente la información de credenciales y contraseñas están cifradas, mejorando la seguridad.

- Gestión centralizada: Todos los cambios en cuanto a credenciales se hacen en un único sitio. Por ejemplo, el cambio de contraseña de un usuario lo tendría que hacer solamente una vez, mientras que en un sistema no centralizado debería ir recurso a recurso cambiando las contraseñas. Lo mismo para cambios de otros parámetros como nombre, DNI, teléfonos o direcciones.

  En empresas con muchas sedes se hace más palpable la mejora de esta gestión centralizada, pues desde un único punto geográfico puedes gestionar a todo el personal.

  Enlazando también con la seguridad, esta gestión centralizada nos permite bloquear el acceso de un usuario a todo el sistema a la vez, mientras que con la no centralizada se puede dar el caso de que se nos olvide algún recurso, evitando así el error más común que es el error humano.

- Integraciones: La mayoría de los sistemas actuales vienen preparados para que su validación pueda ser externa, con lo que no tendríamos que hacer a los usuarios aprenderse más que una contraseña. Cuando tienen más de una, los usuarios tienden a apuntarlas, con lo que volvemos a enlazar con la seguridad

- Gestión de grupos: Podemos agrupar a los usuarios, ya sea por funciones, por tipos, por localización geográfica…etc. Con esto conseguimos una mejor gestión de los usuarios.

- Aplicación de políticas: Podemos aplicar políticas de gestión, ya sea por usuarios o por grupos, por ejemplo, podemos tener varios accesos a Internet y querer que el grupo de dirección salga por el más rápido.

- Realización de consultas: Podemos realizar consultas sobre la base de datos centralizada de una forma muy sencilla, de forma que tenemos mas control sobre usuarios, servicios y recursos

- Auditoria: Podemos auditar los accesos al sistema. Esto no es solo una ventaja sino una necesidad en múltiples sistemas donde las leyes nos obligan a tener un listado de los accesos a determinados recursos (Véase LOPD).

4.4.2.- Derechos de acceso

Evidentemente no basta con saber quien es quien se ha conectado al sistema sino que es necesario saber que derechos tiene sobre que recursos.

Los recursos pueden ser variados e ir desde lo más básico que sería un fichero hasta el derecho a imprimir por determinada impresora.

Para poder dar estos derechos nos basaremos en la solución de identificación centralizada que vimos en el apartado anterior, con lo que deberemos tener un sistema de derechos de acceso que se pueda integrar con la solución de identificación.

Una vez creado el recurso, se le dará los permisos al mismo a los usuarios, normalmente, a través de la pertenencia a algún grupo,

aunque esto se dejará a la libre elección y gestión del responsable en la empresa.

4.4.3.- Solución Propuesta

En definitiva, necesitamos una solución que nos de gestión centralizada de usuarios y grupos, que nos permita aplicar políticas de derechos de acceso y seguridad. Además, queremos que sea lo mas integrable posible, al menos, integrable dentro de nuestra plataforma, segura y fiable.

Como ya hablamos anteriormente también, las soluciones que están en el mercado están basadas en el directorio LDAP (Protocolo ligero de acceso a Directorios).

Haya en el mercado varios productos basados en LDAP como pueden ser *OpenLDAP, iPlanet, Novell Directory Services* y muchos más. Nosotros vamos a optar por la solución *Active Directory* de *Microsoft*, el cual nos cubre todas las necesidades que hemos ido viendo, como son:

- Gestión de usuarios y grupos: Evidentemente se pueden crear usuarios y grupos de una forma sencilla, ágil y segura.

- Seguridad en las contraseñas: El protocolo Kerberos que utiliza el Active Directory garantiza que las contraseñas viajen en la red cifradas, por lo que este intercambio se hace de forma segura.

- Seguridad del sistema: El *Active Directory* gestiona los controladores de dominio de forma bidireccional. No hay ninguna jerarquía de funciones, por lo que duplicando el controlador de dominio ya tenemos una copia exacta de nuestro dominio.

Además, el *Active Directory* gestiona automáticamente la sincronización entre ellos de una forma eficiente.

- Gestión Centralizada: Tiene consolas de administración tanto locales como remotas, lo que nos permite gestionar el directorio desde cualquier equipo de la red. Además, estas consolas son configurables de forma que cada administrador puede crearse una a su gusto o necesidad.

- Clientes Windows: La mayoría de las empresas siguen utilizando clientes Windows en nuestro caso Windows XP o Windows 7. El *Active Directory* esta preparado para sacar el máximo rendimiento a este tipo de clientes.

- Gestión de políticas: Muy relacionado con el punto anterior, al ser los clientes Windows, existe en el *Active Directory* una gran cantidad de directivas ya preparadas para poder aplicar sobre estos clientes, con lo que prácticamente todos los parámetros del sistema los podemos manejar desde el mismo, desde salvapantallas, fondos con imagen corporativa pasando por derechos de uso sobre determinados recurso de los clientes como puertos USB o discos locales.

  Quizás esta sea la mayor ventaja del uso del *Active Directory* frente a otras soluciones LDAP, la cantidad enorme de posibilidades de configuración de los clientes que podemos hacer desde ella, ahorrando un coste enorme de recursos en hacerlos uno a uno y creando configuraciones fijas y funcionales, eliminando posibilidades de fallos por configuración.

- Auditoria: El *Active Directory* viene por defecto con la posibilidad de habilitar auditorias, tanto sobre accesos al sistema como de accesos a recursos del mismo, guardando las mismas en un formato legible.

- Consultas: Las diferentes consolas de administración te permiten crear consultas a la base de datos para poder sacar información de ella.

- Automatismos: Se pueden crear automatismos sobre objetos que ayuden a la gestión.

- Integraciones: Es un producto que es ampliamente integrable. Aparte de una integración casi total con otros productos de Microsoft como pueden ser Exchange, Terminal Server, Office, ISA, Entidades Certificadoras, etc., algunos de los cuales los usaremos en este diseño, su uso esta muy extendido, por lo que la mayoría de las casas comerciales que crean productos que se integran con LDAP vienen preparados para integrarse con el *Active Directory*.

- LDAP: Hay que tener en cuenta que *Active Directory* no es propiamente un LDAP, sino que es un producto que utiliza el protocolo. Lo que quiere decir que la integración con otros LDAP hasta ahora no era posible. En la versión del *Active Directory* de 2008 se ha añadido una funcionalidad para poder integrar *Active Directory* con un servicio LDAP nativo, por lo que tenemos aún más integración.

- Amplio uso en el mercado: El *Active Directory* de Microsoft es un producto que es ampliamente utilizado en el mercado. Existen por

tanto muchísima información al respecto, muchísimas aplicaciones que funcionan sobre el y mucha gente trabajando con y para el, lo cual es siempre un factor a tener en cuenta.

- Facilidad de Implantación: Es realmente fácil de implantar. Prácticamente cualquier puede hacerlo con lo mínimo e ir creciendo en funcionalidades a medida que vayan creciendo las necesidades de la empresa.

- Formación: Por la idiosincrasia de nuestra tierra, el salir a realizar una formación fuera de las islas, incluso entre ellas, es algo que esta muy alejado de la posibilidad de cualquier empresa. Hay que tenerlo en cuenta a la hora de elegir un producto, para no llevarnos la sorpresa que no podemos usar nuestro producto porque no sabemos como y no tenemos posibilidad de aprenderlo. Aunque es un tema más subjetivo me aventuro a asegurar que existen formadores de *Active Directory* y academias que dan formación sobre el tema en nuestra isla con una calidad excelente, sin necesidad de tener que realizar un viaje, abaratando los costes de la misma.

Por todo esto creo que queda más que justificado la elección de Active Directory como servicio LDAP para nuestro diseño.

4.5.- Análisis de la seguridad de los accesos remotos

Como ya discutimos en el análisis de los requisitos de las empresas, hoy en día las posibilidades de la conexión desde fuera de la empresa son múltiples, desde múltiples dispositivos y prácticamente desde cualquier sitio.

Como también vimos en el análisis de requerimientos, esta posibilidad de conexión prácticamente desde cualquier sitio contiene una gran cantidad de ventajas, desde el teletrabajo, pasando por la conciliación de vida laboral y familiar, pedidos online, etc., etc., pero de la misma forma que tiene todas estas ventajas, tiene una serie de problemas de seguridad inherentes, que han de ser tratados para poder aprovecharnos de estas ventajas de una forma segura.

Hay una frase relacionada con la seguridad informática y atribuida a Gene Spafford que dice algo así como "El único sistema seguro es aquel que esta apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados. Y aun así, yo no apostaría por ello".

Con esta frase lo que se quiere indicar es que un sistema, por muy buenas que sean sus medidas de seguridad siempre tendrá algún agujero por donde colarse, sobre todo, al estar interconectado.

En este apartado nosotros no solo vamos a tratar con un sistema interconectado con otros sistemas dentro de nuestra red, sino que lo que pretendemos es hacer que el sistema sea accesible desde Internet.

Los problemas de seguridad que esto nos genera es enorme y, evidentemente, no todos son evitables, por lo que lo que pretendemos aquí es dar una solución lo suficientemente segura para poder usar el sistema de forma tranquila, pero siempre, sin perder de vista que un análisis completo de la seguridad del sistema sería, posiblemente, tan grande como para poder ocupar un TFG independiente.

Dicho esto, vamos a realizar el análisis de la seguridad en los accesos remotos. El mismo, lo vamos a basar en dos conceptos o estrategias, seguridad en la conexión remota y centralización del acceso.

4.5.1.- Seguridad en la conexión remota

Entendemos la seguridad en la conexión remota, como la seguridad que tiene que existir para que nuestro sistema acepte la conexión desde Internet.

Hay distintas estrategias que podemos aplicar. Una de ellas es publicar directamente en Internet los servicios que queramos dar, como pueden ser una conexión RDP, un servicio WEB, un servidor FTP o cualquier otro que queramos. Esta estrategia puede estar bien siempre y cuando implementemos unos servicios intermedios entre nuestra LAN e Internet que sean a los que realmente se conectan los usuarios externos, lo que comúnmente llamamos DMZ o zona desmilitarizada. El problema de la implantación de una zona desmilitarizada es que requiere de una infraestructura tanto a nivel de red, servidores y almacenamiento, como unos niveles de ingeniería muy altos, por lo que quedan fuera del alcance del segmento de empresas donde esta localizada la nuestra.

Otra estrategia es asegurar los extremos de la conexión, de forma que creemos un túnel seguro entre nuestra LAN y el cliente que se quiere conectar, lo que básicamente se conoce como VPN o red privada virtual, y una vez dentro de la LAN ya el cliente puede conectarse a los distintos servicios de la red conforme lo hayamos planificado.

En nuestro caso, optaremos por esta segunda opción como estrategia para las conexiones externas. Veamos a continuación como lo haremos:

VPN

Lo primero que debemos hacer es ver, aunque de forma muy somera, que es una VPN.

Una VPN es una tecnología que nos permite extender la funcionalidad de la LAN sobre una red pública de una forma segura. Las características que debe cumplir para que sea segura son:

- Identificación: Todas las conexiones deben ser identificadas
- Integridad: Las comunicaciones deben ser integras, garantizándose que no se han modificado por el camino. Normalmente utilizamos para ello funciones de Hash.
- Confidencialidad: Las comunicaciones deben ser cifradas.
- No repudio: Todos los mensajes deben estar firmados.

Existen a su vez dos tipos de conexiones VPN, de acceso remoto o *Lan to Lan* o punto a punto. La primera de ellas sirve para conectar a usuarios con la LAN de forma remota y es la que diseñaremos nosotros. La segunda sirve para conectar dos sedes de una misma empresa de forma segura, y quedará fuera del estudio de este TFG.

Para cumplir con estos requerimientos vamos a implantar dos servicios dentro de nuestra red, el servicio VPN y el servicio de certificados o entidad certificadora.

Servicio VPN

Para dar servicio de VPN diseñaremos un servidor VPN basado en Microsoft Windows Server 2008. El mismo será un servidor virtual con el componente de Enrutamiento y Acceso Remoto.

Una vez mas, utilizamos el sistema de Microsoft dado que nos permite la integración con el Directorio Activo, verdadero núcleo de la empresa, para la aplicación de políticas de acceso y permisos sobre los mismos, es decir, integraremos el servidor de VPN con el Directorio Activo de forma que será desde este desde el que controlemos quien tiene permiso para acceder a este servicio.

Para ello integraremos el Servidor VPN con el servidor RADIUS para poder acceder a los usuarios del Directorio Activo.

También integraremos en el servidor VPN el uso de certificados digitales emitidos por nosotros mismos, de forma que solo los usuarios poseedores de los certificados sean admitidos en la red.

Servicio RADIUS

Para poder integrar el servidor VPN con el directorio Activo nos hace falta un servicio intermedio que nos haga esta integración, lo que se llama un servicio RADIUS. El mismo sirve para permitir el uso de credenciales de un sistema en otro.

En nuestro caso vamos a montar el servidor RADIUS de Windows Server 2008, IAS *o Internet Authentication Service*.

Con este servidor conseguimos que podamos usar los usuarios y grupos del directorio activo para dar permisos de acceso en el servidor VPN, o, lo que es lo mismo, cuando se le pasen las credenciales al servidor VPN, este no las tendrá consigo, sino que preguntara al RADIUS sobre las mismas. El servidor RADIUS esta integrado con el directorio Activo y a su vez, le preguntara a este sobre las credenciales suministradas.

Será a través de los grupos del Directorio Activo donde se permitirá o denegará el acceso a la red, pudiendo aplicar distintas políticas a distintos grupos, como pueden ser limitaciones horarias, de servicios, etc.

Notar aquí la simplicidad que aporta esta solución pues, una vez montada, desde la consola de gestión de usuarios controlamos también el acceso remoto.

Servicio de Entidad Certificadora

Para que todo este trasiego de información entre Internet y el servidor de VPN sea lo mas seguro posible, los clientes para poder conectarse se les exigirá tener un certificado digital.

Podríamos pedir certificados digitales de cualquier entidad certificadora, pero vamos a optar por diseñar nuestra propia entidad certificadora dentro de nuestra red por dos motivos, el primero, no dependemos de terceros a la hora de emitir los certificados, por lo que lo podremos emitir siempre que queramos sin esperas, y segundo, y más importante, de nuevo, la entidad certificadora estará integrada en el directorio activo, de forma que en realidad estamos certificando al usuario y no a la persona.

Para realizar este servicio diseñaremos un servidor de entidad certificadora de, como no, Microsoft Windows Server 2008, la cual por su propia naturaleza esta integrada en el Directorio Activo.

La misma tiene una consola de administración y se implanta como un servicio WEB al que le podemos hacer las peticiones de un certificado. Una vez nos haya llegado la petición, el administrador de la entidad certificadora aceptará o no la petición. En caso afirmativo, el usuario no tiene más que volver a entrar en la Web de la entidad certificadora y descargarse el certificado.

Evidentemente, los usuarios antes de poder acceder desde fuera a la empresa deberán pedir el certificado digital. La entidad certificadora, administrada por nosotros. Con esto, tenemos la seguridad de que, aunque las credenciales de un usuario se vean comprometidas, solamente desde aquellos equipos donde este instalado el certificado se podrá entrar, por lo que tenemos un nivel de seguridad aún mayor.

La entidad certificadora también nos servirá para emitir un certificado a nivel de maquina para el servidor RADIUS, de forma que las credenciales suministradas por este contra el Directorio Activo siempre irán cifradas dentro de la red.

Conclusión

Resumiendo, para implantar estas medidas de seguridad hemos visto que nos hacen falta los siguientes servicios / servidores:

- Servidor VPN: MS Windows 2008 RAS.

- Servidor RADIUS: MS Windows 2008 IAS.

- Servidor Entidad Certificadora: *MS Windows 2008 Certification Service*.

- Servidor LDAP: *Active Directory 2008*.

Quizás hacer notar aquí que el hecho de la integración con el Directorio Activo no es mas que la forma que las credenciales sean las mismas tanto para el acceso remoto como el acceso interno, de forma que conseguimos, por una parte, que el usuario no deba aprenderse mas de una y, por otra, que en caso de verse comprometidas las mismas solamente en un único sitio es donde debemos subsanar al amenaza.

4.5.2.- Centralización del Acceso

Como hemos visto en el punto anterior, ahora mismos estaríamos en disposición de dar acceso a los usuarios de manera remota a toda nuestra red de una manera bastante segura, el usuario esta identificado y autenticado, el equipo cuenta con el certificado digital emitido por nosotros y esta accediendo a través de un túnel VPN, con la comunicación cifrada.

Aún así, vamos a dar un paso más en la seguridad, además de la simplificación en la administración de los accesos remotos. Para ello, vamos a diseñar un servicio de escritorio compartido, de forma que los usuarios que se conecten desde fuera no tengan acceso libre a la red, sino que solamente puedan conectarse a este servicio de escritorio y desde el mismo puedan acceder a los recursos de la red.

Para la realización de estos accesos nos vamos a basar en el servidor de Terminal Server de MS Windows Server 2008.

Servicio de Terminal Server

El servicio de terminal Server es un servicio de escritorio remoto compartido.

El funcionamiento del mismo, grosso modo, se basa en que varios usuarios pueden usar un mismo servidor como si fueran ellos los únicos que están trabajando dentro de el, accediendo a un escritorio compartido y teniendo acceso a todos los programas y características instaladas en el.

Se basa en el protocolo RDP que es nativo de MS Windows y esta muy extendido su uso, pues las ventajas que aporta son muchas, entre ellas, las más destacadas son la centralización de aplicaciones, la facilidad en la administración, la posibilidad de funcionar desde distintos clientes y aumento de la seguridad.

Las ventajas de la centralización de las aplicaciones son muy visibles, la instalación de las mismas, la aplicación de parches, la búsqueda de errores y absolutamente todo lo que normalmente hacemos para una aplicación en cada cliente, con esta forma de trabajo solamente tendríamos que hacerla una vez. El ahorro de trabajo, desplazamientos y perdidas de disponibilidad son considerables.

La facilidad de la administración tiene mucho que ver con la centralización de las aplicaciones, es más fácil arreglar un problema en un único sitio que en tener que ir a todos los clientes arreglándolo. Además, desde la consola de administración podemos ver exactamente lo que están haciendo los usuarios dentro del servidor, facilitando la tarea de resolución de incidencias.

La posibilidad de trabajar con distintos clientes y la seguridad son los dos factores que tenemos que tener en cuenta para el diseño que estamos planeando.

En cuanto al primero de ellos, hoy dia existen prácticamente clientes de RDP para casi cualquier plataforma software o hardware, como pueden ser Linux, Mac IOS, Windows XP, Vista o 7 o Android, con lo que implantando un acceso desde un servidor de RDP, haces accesible tu sistema casi para cualquier plataforma actual.

La seguridad nos la da el hecho que frente a un ataque que suframos solamente tenemos un único punto de entrada, es decir, si aun teniendo en cuenta todas las medidas de seguridad adoptadas para que la conexión con nuestra LAN sea segura, la misma se ha visto comprometida, solamente debemos apagar o revisar el servidor de Terminal Server para atajar la posible amenaza.

Como siempre, el servidor de Terminal Server estará integrado en el Directorio Activo, y dejaremos para este, con las políticas de usuarios y grupos, los permisos de acceso al mismo, una vez más, desde la misma consola que controlamos todo, facilitando y simplificando muchísimo la tarea del administrador.

Servicio de Licencias de Terminal Server

El servicio de terminal Server tiene una peculiaridad con respecto a los demás servicios que proveen los servidores de MS Windows, y es que para que pueda funcionar requiere de unas licencias extras (TSCall) por cada usuarios que quiera acceder a el.

Estas licencias, una vez han sido compradas deben ser instaladas en un servicios que se llama Licencias de Terminal Server. El mismo es el que se encargar de darlas a los clientes cuando estos intentan conectarse. Una vez se desconectan, las mismas se liberan. Si algún cliente intenta conectarse y no quedan licencias, no podrá hacerlo.

Estas licencias son de dos tipos, por usuario o por dispositivo, dependiendo si la misma la asocias a un usuario conectado o a un equipo conectado. Por el tipo de conexión que nosotros vamos a diseñar, optaremos por las licencias por usuario.

En definitiva, diseñaremos un servidor de licencias de terminal Server, al que los clientes harán sus peticiones de TSCall.

Como con todos los servicios que estamos analizando y diseñando, estará integrado con el Directorio Activo y se le podrá aplicar políticas a los distintos usuarios o grupos en el.

Conclusión

Para desarrollar un único sitio donde se conecten los accesos remotos nos hace falta los siguientes servicios / servidores:

- Servidor RDP: *MS Windows 2008 Terminal Server*.
- Servidor de Licencias: *MS Windows 2008 Terminal Service Licencing*.
- Servicio LDP: *Active Directory 2008*.

4.6.- Análisis de las tecnologías Hardware

A continuación pasamos a realizar el análisis de las tecnologías hardware que vamos a utilizar en nuestro diseño.

Evidentemente la gran variedad de tecnologías existentes en el mercado hacen que el análisis de todas ellas sea una tarea inabarcable, al menos desde el punto de vista de este TFG.

Además, nuestro diseño se ve altamente restringido por el análisis de alta disponibilidad que vimos en apartados anteriores, lo que directamente nos elimina algunas de las tecnologías del mercado.

Esto hace que no vayamos a analizar las diferentes posibilidades que tenemos pues, repito, sería prácticamente imposible realizar esa labor. Nos limitaremos a justificar, desde el punto de vista tanto del rendimiento, la seguridad y la alta disponibilidad, las tecnologías elegidas.

4.6.1.- Servidores

Existe gran variedad de servidores en el mercado, de una gran cantidad de marcas.

Como vimos en nuestro análisis de alta disponibilidad lo mínimo que debe contemplar nuestros servidores es tener redundancias a nivel de fuente de alimentación, de tarjetas de red, de discos, de ventilación, de CPU y de memoria.

Chasis

Desde el punto de vista físico los servidores pueden ser de tres tipos, de torre, enracables o tipo *Blade*.

Los de torre son los mas voluminosos si bien no necesitan de ninguna otra infraestructura para poder funcionar además de presentar una disipación del calor más efectiva, precisamente debido a este volumen, lo que los hace muy efectivos para oficinas con poca o nula refrigeración a costa de perder espacio.

Los enracables son más pequeños, aunque para poder funcionar necesitan que exista un soporte (rack) donde va colocado, precisamente de ahí su nombre. También por regla general disipan más calor, por lo que necesitan un sitio más ventilado o con refrigeración. Su facilidad de colocación y capacidad de ampliación hacen que sean muy utilizados.

Los tipo *Blade* requieren un tipo especial de rack llamado Chasis. Estos servidores se basan en la idea de compartir ciertos elementos del servidor como la comunicación, la alimentación y la refrigeración, los cuales son proporcionados por el propio chasis. Gracias a esto los servidores *Blade* son altamente escalables, ya que en muy poco espacio se puede añadir gran cantidad de servidores (hasta 16 en 8 Us), eliminando además gran cantidad de espacio en cableado y facilitando enormemente la administración de los mismos y reduciendo el número de fallos.

Desgraciadamente para nosotros, a pesar que los servidores Blade suelen ser más económicos que los servidores enracables, la inversión inicial en el chasis hace que tengamos que descartar este tipo de tecnología por costes.

En cuanto a la elección entre enracable y de torre, vamos a quedarnos con la solución enracable por ser más modular, limpia, elegante e integrada, teniendo en cuenta que también aportaremos al diseño de la solución un pequeño armario rack donde montaremos todos los elementos del diseño.

Discos

El primer elemento hardware dentro del servidor al que vamos a realizar el análisis son los discos.

Como ya vimos en el análisis de la alta disponibilidad, en cada uno de los servidores necesitaremos un mínimo de un par de discos, de forma que ante la caída de uno de ellos el otro o los otros puedan seguir funcionando sin dificultad.

Para ello lo que se suele hacer es crear discos con niveles de redundancia, lo que se conoce como niveles RAID, que pueden ser 0, 1, 5,6 o más dependiendo de fabricante.

En una configuración muy clásica, los niveles más normales de RAID suelen ser RAID 1 para el sistema y RAID 5 o 6 para datos. Esto es debido a que el RAID 1 es un espejo entre dos discos, es decir, lo que se copia en un disco es copiado en el otro. Evidentemente se pierde la mitad de la capacidad de los discos con esta configuración, por ello aparece el nivel 5, que permite una redundancia perdiendo solamente 1 disco del pool completo que pongas a partir de 3 discos, es decir, con 3 discos perderías el 33% de espacio, con 4 disco el 25% y así sucesivamente. Esta configuración tiene unos altos niveles de rendimiento y una perdida de espacio aceptable, por lo que supuso la favorita para los discos de datos.

Una variante es el nivel RAID6, que es un RAID 5 aumentando un disco más de redundancia.

En el diseño que hemos planteado desde el principio, los datos no estarán ubicados en el servidor físico, sino que estarán en una red de almacenamiento NAS. Por ello, no tenemos una gran necesidad de espacio en los servidores, sino simplemente lo mínimo para instalar el sistema y que vaya rápido. Por ello la configuración que nos interesa es una configuración de dos discos en RAID 1.

Para poder realizar los niveles de RAID el servidor tendrá que tener una controladora que permita hacerlo. Hoy en día la mayoría de los servidores, incluso algunos pcs, ya la tienen incorporada, pero es un punto a tener en cuenta.

En cuanto a tecnología de discos podemos distinguir básicamente en tres, discos SATA, discos SAS y discos SSD.

Los discos SATA (*Serial Advanced Technology Attachement*) son los contemporáneos de los discos serie IDE, van a un máximo de 7.200 rpm y son mayoritariamente usados en la configuración de los pcs. En nuestro caso los desechamos porque no están preparados para entornos empresariales, careciendo de niveles de RAID, chequeo y recuperación de errores, así como una alta velocidad.

Los discos SSD (*Solid State Disk*) o discos de estado sólido son la ultima generación de discos. Son discos que carecen de cabezales al estar formados básicamente por chips. Son prácticamente memorias muy grandes con la implantación de los protocolos de discos. Son discos de muy muy rápido acceso, por carecer de elementos móviles y serían los ideales a implementar en nuestro diseño. Lamentablemente, el precio

actual de estos discos todavía los hace no aptos para lo que estamos diseñando.

Los discos SAS (*Serial Attached SCSI*), son la evolución de los discos paralelos SCSI que durante años han sido los que más usamos en los servidores. Proporciona alta velocidad de acceso, niveles de RAID, detección y corrección de errores, etc, lo cual los hacen los mejores en entornos productivos empresariales. Además, los ciclos de vida son mucho mas grandes, se estima que los discos SAS pueden durar 1,2 millones de horas de tiempo funcionando 24 horas al día, mientras que los SATA ofrece 1 millón de horas de tiempo, pero funcionando 8 horas al día. En nuestro diseño los servidores los seleccionaremos con discos SAS.

Mostramos a continuación una comparativa de los SAS y SATA (no incluimos los SSD ya que los hemos descartado).

Requirement		SAS	SATA
Operational Availability		24 hours/day - 7days/week	8 hours/day - 5days/week
Workload		100%	10-20%
Cost Sensitivity		Moderately sensitive to cost	Sensitive to low cost
Performance	Latency and Seek	5.7 msec @ 15K rpm	13 msec @ 7200rpm (or smaller)
	Command Queuing and Reordering	Full	Limited
	Rotational Vibration Tolerance	Up to 21 rads/sec/sec	Up to 5 to 12 rads/sec/sec
	Typical I/Os per sec/drive	319	77
	Duplex Operation	Full	Half
Reliability	Bad Sector Recovery	Typical time out 7-15 sec only	Time outs up to 30 sec
	Misalignment detection	Dedicated Servo and data path processors	Single combined servo/data path processor or none
	Vibration Sensors	RV Compensation Feedback Mechanism	No RV Compensation
	Variable Sector Size	Utilizes a 528 byte sector and allow the I/O controller	Do not utilize a variable sector size (locked at 512 bytes)
	MTBF	1.2M hours at 45 degrees C	700K hours at 25 degrees C
	Internal Data Integrity Checks	End to End	Limited, none in memory buffer
	Maximum Operating Temperature	~60 degrees C	~40 degrees C
	Warranty	~5 years	~ to 3 years

Han aparecido recientemente en el mercado una mezcla de los discos SAS y SATA, que se llaman *Near Line SAS*. Estos son discos SATA con una controladora SAS los que los provee de algunas funciones de los discos SAS. No los tendremos en cuenta para el servidor, pues todavía su implantación es reciente y no podemos valorar su fiabilidad, aunque si que los nombraremos en las redes de almacenamiento como una posibilidad de implantación.

Procesadores

Básicamente hay dos fabricantes de procesadores que copan casi todo el mercado, Intel y AMD.

Hay muchas y muy variadas estadísticas y estudios sobre cual de ellos es mejor, casi siempre decantándose del lado del quien es el que haya puesto el dinero para dicho estudio. Pero en la realidad, a no ser que hagas un uso intensivo de la maquina, uno u otro suelen ir bastante bien.

En nuestro caso vamos a plantear un mínimo que se debe cumplir para cada procesador, y a partir de ahí, en el diseño elegiremos la mejor opción teniendo siempre en cuenta el coste.

De entrada, hay que distinguir entre procesador o *socket* y *core*. Actualmente todos los procesadores vienen con mas de un *core*, es decir, más de un procesador en la misma pastilla (lo que llamaremos *socket*). Para el caso que nos ocupa, en un sistema de alta disponibilidad, no solo buscaremos el rendimiento con mas *cores*, sino que la disponibilidad nos la da el tener mas de un *socket* físico, en caso contrario, la caída del *socket* hace que todos los *cores* dejen de

funcionar. Por tanto, en nuestro diseño tendremos como mínimo dos procesadores físicos o *sockets*.

En el estado actual de la tecnología, cada uno de estos *sockets* deberá tener, cuanto menos, 4 *cores* internos, de forma que podamos crear hasta 8 maquinas virtuales con 1 *core* en cada servidor (esto en la realidad no es así, pero es para que gráficamente se vea mejor).

La velocidad será de cómo mínimo 2.5 GHz con un mínimo de 8MB de cache.

Estas son las principales características mínimas que deben cumplir los procesadores de nuestro diseño, si bien sabemos que hay muchos más que se tendrían que analizar ya en la fase de diseño.

Memorias

Las memorias suelen ser bastante complicadas de elegir. Vienen muy fijadas por la placa base, el reloj del sistema y lo que el procesador es capaz de aceptar.

Además, normalmente la tecnología de las memorias suele ser la misma en un punto en el tiempo, es decir, que en un determinado momento hay una tecnología y lo único que las diferencia son las velocidades de la misma.

Por ello no vamos a dedicarle mucho a su análisis pues casi vendrán fijas por el equipo que elijamos (placa) y la velocidad del procesador.

Eso si, en cuanto a la capacidad de las memorias, teniendo en cuenta que sobre los servidores físicos van a ir maquinas virtuales, deberá ser

suficiente para cada uno de ellos ser capaz de mantener todos los servidores virtuales levantados en uno de ellos. También, aunque es la configuración más normal y tampoco hace falta hacer mucho hincapié en ello, como mínimo deberá haber un par de módulos de memoria por servidor de forma que en caso de rotura de uno de ellos el servidor pueda seguir funcionando.

Tarjetas de red

En cuanto a las tarjetas de red, al igual que con todos los elementos que estamos viendo en la configuración de nuestro diseño deberá tener como mínimo dos tarjetas de red por servidor. Esto nos permite no solo defendernos de una posible caída de una de las tarjetas o uno de las conexiones a esa tarjeta, sino que dado que lo que vamos a montar en estos servidores son maquinas virtuales, el propio software de virtualización nos permite crear conjuntos de tarjetas funcionando como una sola, de forma que no solo tenemos alta disponibilidad, sino también balanceo de carga entre las tarjetas, lo cual aumenta el rendimiento.

Sobra decir que la tarjeta de red deberá ser una tarjeta de red Ethernet, pues es la tecnología de red abusivamente predominante actualmente. El conector deberá ser RJ45 y la velocidad de las tarjetas será a GigabitEthernet.

Fuentes de alimentación

Las fuentes de alimentación deberán ser dobles, como todo, redundado para el caso de que una caiga el servicio no se pare y además, también nos proteja de caídas del circuito eléctrico si lo tenemos también redundado.

También bueno que estas fuentes de alimentación se pudieran cambiar en caliente, de forma que no interrumpamos el servicio si tenemos que cambiar una de ellas.

4.6.2.- NAS y NAS de respaldo

Como vimos en el apartado de alta disponibilidad, para poder lograr esta lo que necesitamos es separar el procesamiento de los datos. Esto se consigue a través de redes de almacenamiento, ya sean tipo NAS o SAN.

Además en un entorno virtualizado como el que estamos planteando se hace mas visible la necesidad de separar el almacenamiento de la capacidad de procesamiento, pues al tener las maquinas virtuales en un almacenamiento independiente de los servidores, la caída de uno de ellos no afecta al servicio prestado, pudiendo levantar las maquinas virtuales en otro de los servidores que tengan acceso a esos datos.

Indicar aquí que cualquier sistema de alta disponibilidad, ya sea en cluster, RAC, virtualización, *FailOver*, etc, se basan en poder tener datos separados de servidores y ser accesibles desde varios de ellos.

Las redes de almacenamiento tipo SAN (*Storage Area Network*) se basan en ser una red independiente, normalmente de tecnología de *Fiber Channel* y con conexiones de fibra entre los elementos. Nos da un alto rendimiento y disponibilidad al crear caminos virtuales dedicados entre los servidores y el almacenamiento. El problema que tiene son los costes, porque además de la adquisición de la propia SAN se tiene que adquirir switches específicos de *Fiber Channel* así como tarjetas específicas en los servidores (HBA) que hace que su precio, mas costes añadidos sea muy alto.

Las redes NAS (*Network Attachement Server*) son redes que no son dedicadas sino que se aprovechan de la misma red Ethernet que se utiliza para las comunicaciones entre los servidores.

Básicamente son como servidores con una alta capacidad de almacenamiento que implementan. Son servidores dedicados, es decir, no se les puede instalar cualquier software, sino que tiene un software implementado que les da unas capacidades de funcionar como red de almacenamiento, como son compartición de ficheros, implementación de protocolos de almacenamiento sobre ip como puede ser iscsi, seguridad, alta disponibilidad, gestión remota, etc.

En nuestro caso descartaremos las redes SAN por coste, por lo que nos quedaremos con la solución NAS. Estas, hoy en día, han alcanzado un punto de madurez muy bueno haciendo posible la alta disponibilidad en empresas del ámbito en el que estamos haciendo este estudio a un coste bastante asequible, cosa que con las SAN no se produce.

Dentro de las redes SAN que nos podemos encontrar, las hay de distinta gama. En nuestro diseño vamos a introducir dos redes de almacenamiento SAN, una de mas alta gama que será donde estén corriendo nuestras maquinas virtuales y otra de gama mas baja donde mantendremos las copias de seguridad. Evidentemente los requerimientos de una u otra serán diferentes, vamos a continuación a analizar cada una de ellas por separado.

NAS producción

En ella serán donde estén corriendo en producción nuestras maquinas virtuales, por ello los parámetros que mas nos interesan son la seguridad y el rendimiento.

Para conseguirlo la red de almacenamiento deberá de contar como mínimo con los siguientes elementos:

- Doble fuente de alimentación.
- Doble controladora de disco: Las redes de almacenamiento tienen una controladora que es la que hace todo el trabajo. Para tener seguridad deberá tener dos.
- Doble tarjeta de red: Como mínimo (siempre será deseable mas) dos tarjetas de red a GigabitEthernet.
- Redundancia a nivel de ventilación.
- Implementar el protocolo ISCSI: Para poder conectar por ISCSI los discos a los servidores.
- Niveles de RAID: Se deberá poder crear niveles de RAID con los discos dentro de ella. Como mínimo que pueda implementar niveles RAID1, RAID5 y RAID6.
- Consola de administración: Por supuesto deberá tener algún tipo de consola de administración donde podamos gestionar los recursos de almacenamiento.

- Detección y Corrección de errores: Deberá ser capaz de detectar errores, corregirlos si es posible y sino, dar una alarma.

- Permisos: Deberá tener la capacidad de asignar recursos por usuario y por maquina en caso necesario, para que un servidor no pueda ver los recursos de otro.

- Asignación múltiple de recursos: Deberá ser capaz de asignar un recurso a varios servidores a la vez, de forma que puedan compartir almacenamiento.

- Aceptar distintas tecnologías de discos: SAS, SATA, Near-Line SAS.

NAS respaldo

Evidentemente la NAS de respaldo debe ser un sistema con unos requerimientos menores para así poder bajar el coste.

Los requerimientos mínimos son:

- Alta capacidad de almacenamiento aunque sea a bajo rendimiento.

- Consola de administración: Por supuesto deberá tener algún tipo de consola de administración donde podamos gestionar los recursos de almacenamiento.

- Conexión de red a GigabitEthernet

- Capacidad de discos SATA o Near-Line SAS.

Los demás requerimientos de la NAS de producción, como son doble controladora, doble tarjeta, doble fuente de alimentación, etc. no son necesarios.

4.6.3.- Red

Para construir nuestra red Ethernet el elemento hardware que debemos usar es un conmutador de redes o switch, el cual es un dispositivo que trabaja en la capa dos del modelo OSI.

El mismo es un dispositivo que tiene una serie de puertos donde se conectan los equipos, ya sean pcs, impresoras, servidores u otros switches y es capaz de conectarlos entre sí, además de poder conectar varios segmentos de red.

Este es un elemento netamente de hardware, aunque dependiendo de las necesidades que tengamos pueden tener diferentes funcionalidades, normalmente dadas por el software que viene con el equipo.

De entre estas funcionalidades las más destacadas son:

- VLAN (*Virtual LAN*): capacidad de crear redes virtuales entre los distintos puertos del switch. Con esto se consigue evitar los dominios de colisión, mejorando la velocidad de la red. Además, nos permite aislar segmentos de red dentro del mismo switch, lo que nos permite aumentar la seguridad.

- QoS (*Quality of Service*): Calida de servicio. Nos permite asignar anchos de banda por protocolo o por elementos, de forma que podemos priorizar dependiendo de que trafico de red. Esta opción es importantísima en aquellas empresas con telefonía IP.

- Enrutamiento: A pesar de ser elementos de capa 2 del modelo OSI algunos switches ya vienen con capacidad de enrutamiento en capa 3 del mismo modelo OSI.

- STP (*Spanning Tree*): Permite en redes muy grandes que no se produzcan bucles. En una red no puede haber bucles pues sino los paquetes no sabrían como llegar a un sitio o podrían llegar por duplicados.

- Trunking: Capacidad de agrupar varios puertos en uno de forma que funcione como si fuera uno solo aumentando su ancho de banda y creando redundancias.

Evidentemente hay muchas mas, como detección de intrusos, detección de errores, dhcp spoofing([3]), etc, pero estas son las más relevantes.

En cuanto a la velocidad de los puertos también nos podemos encontrar con Switches FastEthernet, si sus puertos van a 100 Mbps o GigabitEthernet, donde sus puertos pueden llegar a 1000Mbps.

Para el diseño que estamos haciendo nos valdría con un switch sin tanta capacidad de gestión, no vamos a crear redes virtuales, ni necesitamos calidad de servicio. Tampoco vamos a tener tantos switches como para necesitar el protocolo *Spanning Tree* y, en cuanto a la redundancia de red, como vimos en el apartado anterior, vamos a dejar al software de virtualización que sea el que se encargue de generar el conjunto de tarjetas o *teaming* de red.

[3] Protocolo que evita que puedan poner un servidor DHCP en la red.

En cuanto a la velocidad de los puertos, sería mas que recomendable que los mismos ya fueran a GigabitEthernet dado que varios servicios correrán dentro de un servidor físico, en forma de maquina virtual.

Queda un poco fuera del alcance de este TFG pero simplemente nombrar que para que la velocidad de la red alcance el GigabitEthernet, el cableado debe ser mínimo de categoría 5e, siendo deseable que sea de categoría 6.

4.6.4.- Conclusión

Resumimos todo lo que hemos visto en el apartado hardware. Como conclusión tenemos lo siguiente:

Servidores

- Tipo enracables.
- Discos SAS dos o mas. Nivel de RAID 1 o RAID6.
- CPU Intel o AMD. Dos Quad-Core o superior a 2.5 GHz o superior con un mínimo de 8MB de cache.
- Memorias replicadas.
- Mínimo dos fuentes de alimentación.
- Dos o más tarjetas de red a GigabitEthernet.

Redes de Almacenamiento

- Tipo NAS.
- Una de producción con altas prestaciones y redundancia y una de respaldo con menos capacidad de gestión.
- Discos tipo SAS, SATA y Near-Line SAS.
- Aceptación de niveles RAID.
- Consola de Gestión.
- Capacidad de asignación de varios servidores a la cabina.

Red de comunicaciones

Switch de puertos a GigabitEthernet.

4.7.- Análisis de las tecnologías Software

En este apartado vamos a analizar las tecnologías software. Si era complicado en las tecnologías hardware hacer un estudio pormenorizado dado la cantidad de tecnologías que hay, no digamos ya en cuanto a tecnologías software.

Además también hay que tener en cuenta que durante el análisis de los requerimientos del sistema se analizaron bastantes soluciones de software que, en cierta medida, también es un análisis de las tecnologías software o, al menos, nos centra en que tecnologías son las que tenemos que analizar.

Evidentemente nos centraremos en esas soluciones que son las que hemos visto y analizaremos posibilidades de software dentro de esas soluciones. Como hemos visto en otros apartados, nuestro TFG es el diseño de una infraestructura, es decir, un soporte para las aplicaciones más dedicadas a las tareas de la empresa como pueden ser una intranet, un CRM, un ERP o cualquier otro software, con lo que estas no estarán dentro de este análisis.

Básicamente de lo que vamos a realizar el análisis es de los sistemas operativos, puestos que son estos los que dan soporte o funcionalidad al resto de las aplicaciones y servicios de la empresa.

En nuestro análisis de los requerimientos de la empresa habíamos vistos que lo que nos hacían falta eran los siguientes servicios:

- Red.
- Servicio de ficheros.
- Servicio de directorio (LDAP).
- Servicio de VPN.
- Servicio de Terminal Server.
- Servicio de Certificación.
- Sistema de Backup.

Para todo ello hemos seleccionado la plataforma de Windows Server 2008. Hemos justificado, sobre todo en el análisis de la seguridad de los

datos así como en el análisis de la seguridad de los accesos remotos el porque hemos elegido esta plataforma, no vamos a volver a repetir los argumentos, simplemente los desarrollaremos un poco mas.

Básicamente se trata de elegir entre soluciones propietarias y soluciones *Open Source*. El porque nosotros hemos elegido las soluciones propietarias de Microsoft se basan sobre todo e dos pilares, integración y conocimiento.

La primera de ellas, la integración, ya se ha ido viendo a lo largo de todo este TFG. La idea es intentar que todos los sistemas estén integrados, es decir, desde un único punto poder gestionarlo todo. Esto se consigue con el directorio activo. Todos los demás productos y servicios que montamos, es decir, el servidor de ficheros, el servidor de VPN, el servidor de Terminales y la certificación se hacen valer del directorio activo, tanto para funcionar como para dar permisos a los usuarios de la empresa sobre ellos.

Con una política de grupos bien diseñada, dando permisos sobre los recursos de la empresa a ellos en lugar de directamente a usuarios, podremos conseguir que desde un único punto, el directorio activo y, más concretamente, la consola de usuarios y equipos del directorio activo, se gestionen todos los recursos TIC de la empresa.

Además es lo suficientemente flexible y tiene la suficiente introducción en el mercado para que la mayoría de las aplicaciones de nivel superior se puedan integrar con el, con lo que aún ganamos más en cuanto a la integración.

Es fundamental en una empresa, y más en una del tipo PYME que probablemente no tenga un departamento informático detrás que pueda

respaldarlo que la asignación de recursos sea lo más sencilla posible, y además que sea en un único punto.

Además, siempre para los usuarios será mucho más sencillo poder mantener una única contraseña para todos los servicios que muchas. El tener muchas contraseñas provoca que los usuarios terminen apuntándolas, creando un problema de seguridad. En caso de pérdida o riesgo que las credenciales estén en entredicho, la forma de solventarlo desde este punto de vista es mucho más sencilla, aumentando la seguridad en base a minimizar el área de actuación.

El segundo de los pilares sobre el que se basa la elección del software propietario se basa en el conocimiento o formación. Una de las cosas más caras que existe en el mundo de las TICs, es el conocimiento o *How-To* de los sistemas. Muchas veces los sistemas son mejores o peores simplemente por el grado de conocimiento de los mismos y, por tanto, el nivel de despliegue de posibilidades que ellos te ofrecen. El desconocimiento de los sistemas lleva muchas veces a implantaciones que no son del todo seguras o del todo optimas.

En nuestro caso poseemos un conocimiento amplio de las soluciones que estamos proponiendo. Si bien el coste de la propiedad de la solución es mas alta que el haberlo hecho con una solución *Open Source*, el nivel de conocimiento de la misma compensa este coste.

El coste en la implantación de proyectos con *Open Source* se pasa del coste de la propiedad al coste del conocimiento. Hay infinidad de estudios que demuestran que uno es más alto que el otro, y viceversa, como siempre, dependiendo del color de quien haya pagado dicho estudio o las preferencias de la persona que haga dicho estudio.

Sin entrar a valorar cual esta en lo cierto, en el caso que hubiéramos optado por las soluciones *Open Source* nosotros si que hubiéramos tenido que hacer una inversión en conocimiento previo, por tanto, nos justifica el hacerlo con las tecnologías que mas conocemos en estos momentos.

Además, y volviendo a contar las virtudes de la virtualización, las licencias de servidores se ven reducidas enormemente en cuanto al coste, ya que con una única licencia física podemos montar hasta cinco servidores virtuales, por lo que este coste se ve reducido enormemente.

Conclusión

Como conclusión, vamos a implantar la plataforma basándonos en los servicios del servidor Windows Server 2008.

4.8.- Análisis de las tecnologías de Virtualización

Al ser la base sobre la que vamos a realizar todo nuestro diseño, haremos una mención aparte a las tecnologías de virtualización a pesar de ser elementos software y poder haber hecho el análisis en el apartado anterior.

Como habíamos visto en el alcance de este TFG, nos centraremos en la virtualización de los servidores, y más concretamente, en la virtualización bare-metal, dejando de lado la virtualización del entorno de escritorio de trabajo, lo que se llama VDI.

Recordando un poco lo visto anteriormente, la virtualización de los servidores trata de crear en lo que siempre se ha considerado como servidor desde el punto de vista físico, más de un servidor, los cuales

llamamos virtuales. Para ello se provee de un software específico de virtualización, que puede ser de dos tipos dependiendo de si requiere un sistema operativo previamente instalado o no. En caso necesario se llama virtualización hospedada, mientras que en caso que no sea necesario sería virtualización nativa o bare-metal (precisamente porque se instala directamente sobre el servidor ([4])).

En la segunda de estas formas de funcionamiento de la virtualización, el software de virtualización recibe un nombre específico que es *hypervisor*, ya que no es un sistema operativo al uso que le da recursos a las aplicaciones que corren encima de el, sino que simplemente pasa hacia las maquinas virtuales los recursos hardware de la maquina.

En cuanto a elegir una u otra opción de virtualización nosotros nos vamos a quedar con la virtualización nativa.

El rendimiento de la virtualización nativa es superior a la virtualización hospedada. Esto se ve claro al pensar en que en esta segunda, el sistema operativo compite por los recursos de la maquina con las mismas maquinas virtuales, por lo que evidentemente, el rendimiento mermará.

También se ve en el hecho que el sistema operativo impone su propio sistema de fichero, mientras que las soluciones bare metal implantan sus propios sistemas de ficheros, optimizados precisamente para soportar sobre ellos la virtualización.

[4] Como nota "graciosa" comentar que en muchos ámbitos, sobre todo a la hora de pedir presupuestos o servicios a la hora de llamar a los servidores físicos se les suele catalogar como "hierro".

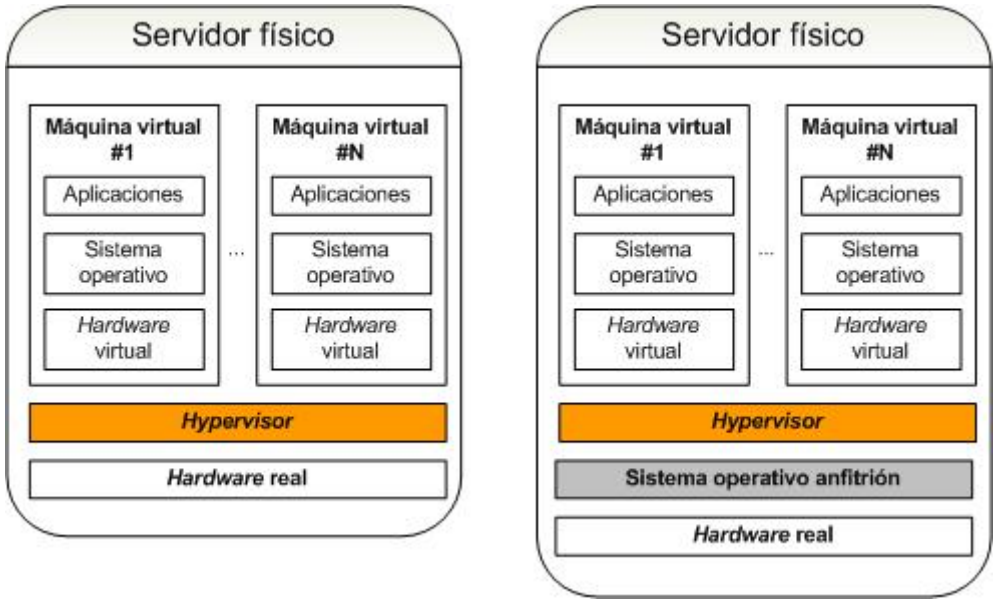
En cuanto a la alta disponibilidad, en caso de las soluciones hospedadas, estas quedarían supeditadas a las que te podría ofrecer el propio sistema operativo (hacer notar que todas las soluciones de alta disponibilidad dependen en gran medida de la capacidad de compartir almacenamiento, por lo que es una consecuencia directa, que si las maquinas están montadas en almacenamiento del sistema operativo, dependa de este la alta disponibilidad) mientras que en las soluciones bare-metal la alta disponibilidad viene de fabrica, sin necesidad depender de terceros.

Igualmente a la alta disponibilidad de las maquinas virtuales, tenemos el caso de la alta disponibilidad de los dispositivos de red. En la virtualización hospedada dependería totalmente del sistema operativo proveer a las maquinas virtuales de una solución de alta disponibilidad a nivel de tarjetas de red, mientras que en las soluciones bare metal estas soluciones vienen implantadas de forma nativa, dándonos además, balanceo de carga.

Entre la gran cantidad de productos de de virtualización que existen actualmente, destacamos entre la hospedada *VirtualBox* y *VirtualServer*, mientras que en la parte de virtualización bare-metal podemos encontrar *Hyper-v, Red Hat, Xen Server y VMWare*, entre otros muchos.

La mayoría de las soluciones bare-metal, tienen la ventaja que ofrecen el hypervisor de forma gratuita, de forma que solamente deberíamos pagar, en caso de quererlo, por el soporte oficial de la casa comercial y una consola de administración centralizada, y esta ultima, no en todos los casos.

Mostramos a continuación un esquema con la diferencia entre la solución hospedada y la nativa, donde se puede apreciar, en el segundo de los casos, como el sistema operativo opera entre el software de virtualización y el hardware, restando rendimiento.



De todos estos productos nosotros nos vamos a quedar con *VMWare VSphere Essentials*, que nos ofrece capacidades de virtualización y un precio realmente bajo, que es prácticamente despreciable.

Nos decantamos por VMWare por ser los líderes indiscutibles en el entorno de virtualización. Sus productos son muy buenos, ofrecen gran calidad y rendimiento y además el precio en los últimos años, añadiendo algunas versiones menores, hace que ya sean asequibles para el entorno de empresas en el que nos movemos.

Además son los que más tiempo llevan en el entorno de virtualización, esto hace que la cantidad de información que podemos encontrar de ella en la red sea mucha, mientras que con otras soluciones no es tan

abundante. Esto hace que mucha gente ya sepa trabajar con VMWare, lo cual siempre es un grado de tranquilidad para las empresas.

Frente a soluciones como Hyper-v permite cualquier tipo de maquina virtual, ya sea con sistema operativo Microsoft Windows, Solaris o Red Hat, dando soporte sobre el, por lo que no estaremos ligados a una tecnología.

Permite combinar distintos tipos de procesadores en distintos servidores. Si bien, ahora mismo en el origen de la instalación esto no es importante porque elegiremos la misma configuración para los servidores físicos, en un futuro puede ser importante si queremos ampliar nuestra granja y no queremos estar limitados en tecnología.

Acepta todo tipo de redes de almacenamiento. Desde redes SAN por Fiber Chanel a redes NAS por ISCSI o NTFS de forma nativa. El descubrimiento de los recursos de red se hace de forma automática.
La consola se integra dentro del Directorio Activo, por lo que seguimos proporcionando un único punto de validación y de credenciales, por lo que seguimos ganando en sencillez.

Por ultimo, aunque no menos importante, al igual que en la parte de software, contamos con un amplio conocimiento de la solución, con lo que toda la parte de formación de la misma para su implantación la tenemos. Sabemos los procedimientos a seguir y que y como nos da la solución. Este amplio *how-to* se traduce en una reducción en el tiempo de implantación al igual que una mejor implantación del sistema.

Conclusión

Como conclusión, vamos a montar la plataforma virtual con VMWare VSphere Essentials.

5.- Diseño

En el punto actual ya tenemos todo lo que necesitamos para realizar el diseño de nuestra plataforma. Por un lado, tenemos los requerimientos que necesitan las empresas, que se transforman en servicios que tenemos que implementar.

Por otro lado, hemos analizado el software y el hardware que sería necesario para poder implementar estos servicios y hemos hecho un análisis de que tecnologías existentes son las que vamos a implementar.

Para realizar el diseño empezaremos por el diseño del software, debido a que la implementación de los servicios en servidores virtuales nos dará la medida del hardware necesario para soportar esos servicios, sobre todo en cuanto a memoria, almacenamiento y procesamiento.

En segundo lugar pasaremos a realizar el diseño de la plataforma de virtualización, la cual esta a caballo entre la parte Software, puesto que es software y soporta las maquinas virtuales, y la parte hardware, ya que es el que se encarga de dar el hardware a las maquinas virtuales.

Por ultimo, ya conociendo el diseño del software y la plataforma de virtualización, podemos pasar a realizar el diseño hardware, para por ultimo dar la valoración económica.

5.1.- Diseño de la solución software

A continuación vamos a realizar el diseño de los servidores, los servicios que soportaran cada uno y las interrelaciones entres ellos.

Habíamos visto los siguientes servicios que teníamos que prestar y los servidores que requieren

- Servicio de ficheros.
    - Servidor de Ficheros.
- Servicio de directorio (LDAP).
    - Servidor controlador de dominio Windows Server 2008.
- Servicio de VPN.
    - Servidor de VPN MS Windows 2008 RAS.
    - Servidor Radius MS Windows 2008 IAS.
- Servicio de Terminal Server.
    - Servidor de Terminal Server MS Windows 2008.
    - Servidor de Licencias de Terminal Server MS Windows 2008.
- Servicio de Certificación.

- Servidor de entidad certificadora MS Windows 2008.

- Servicio de Backup.

  - Servidor de Backup.

Pasamos a analizar cada uno de los servidores necesarios para al final ver el diseño de todo conjuntamente.

5.1.1.- Servicio de Ficheros

Para el servicio de fichero nos valdría con un servidor de ficheros, ya que la alta disponibilidad nos la da la plataforma de virtualización.

En el lo que vamos a almacenar son los datos no estructurados de la empresa, es decir, todos aquellos que no son bases de datos, como pueden ser imágenes, videos, hojas de cálculo, etc.

También, por mejorar la seguridad de los datos de la empresa, implementaremos un sistema de redirección de carpetas hacia este servidor. Esto significa que cuando un usuario abre una sesión en un pc de la empresa, los datos que guarde en mis documentos o el escritorio no se guardaran en local, sino que estas carpetas, junto al perfil, estarán redirigido a este servidor de ficheros.

Con esto se consiguen dos cosas, primero, que todos los datos estén en el servidor, por lo que la rotura de un pc, normalmente más delicado que los servidores, no provoca una perdida de datos, y por otra parte, que el usuario siempre tenga sus datos, vaya donde vaya y se conecte donde se conecte, consiguiendo movilidad interna.

El servidor de ficheros es un servidor que no tiene excesivos requerimientos en cuanto a rendimiento, pues el servir los ficheros no consumen gran cantidad de CPU ni de memoria, aunque si consume bastante ancho de banda de red, dependiendo de la carga de usuarios que tenga.

Evidentemente, también consume un alto grado de almacenamiento, como su propio nombre indica.

Con estos requerimientos podemos plantearnos un servidor de ficheros con:

- CPU: 2 CPU virtuales.
- Memoria: 2 GB.
- Disco de Sistema: 30 GB.
- Disco de Datos: 2 TB.
- Red: 1 GigabitEthernet.

A este servidor lo llamaremos SFicheros.

5.1.2.- Servicio de Directorio

Para el servicio de directorio vamos a implementar dos servidores controladores de dominio. Cada uno de ellos ira sobre un servidor físico distinto.

Además del servicio de directorio tendrán también los siguientes roles dentro de la organización:

- Servidor DNS.
- Servidor DHCP.
- Servidor de Licencias.

Todos estos servicios son servicios que si bien no tienen un consumo muy alto en cuanto a requerimientos de procesamiento, memoria ni almacenamiento, si que son fundamentales para el buen funcionamiento de la organización, dado que todo reposa sobre el directorio activo, de ahí que lo dupliquemos.

Hacer notar que estos dos servidores se replicaran automáticamente ya que el directorio activo automáticamente mantiene una sincronización entre todos los controladores de dominio.

La única diferencia que puede existir entre estos dos controladores de dominio es que uno de ellos tiene que tener una serie de roles únicos en el sistema, aunque simplemente es una función que se puede pasar en cualquier momento de uno a otro.

Con estos requerimientos podemos plantearnos los controladores de dominio con:

- CPU: 2 CPU virtuales.
- Memoria: 2 GB.

- Disco de Sistema: 30 GB.

- Red: 1 GigabitEthernet.

A estos dos servidores los llamaremos SDC1 y SDC2, estableciendo en SDC1 los roles de los que hemos hablado.

5.1.3.- Servicio de VPN

Para implementar un servicio de VPN en el entorno de Microsoft Windows Server 2008 necesitamos implantar una función que se llama RAS (Remote Access Server), el cual será el encargado de recibir las peticiones de VPN externas y, conforme a una serie de reglas que le estableceremos, aceptar o rechazar la petición.

Una vez aceptada la petición, creara un túnel con el cliente que ha hecho la petición y le dará una dirección IP de la red interna de la empresa.

Para integrar estas reglas de validación con el directorio activo necesitamos que las peticiones sean enviadas a un servidor Radius, el cual es un servidor de autenticación. Microsoft implementa esta función con el servidor IAS (*Internet Authentication Service*).

Cuando las peticiones de VPN lleguen al servidor RAS, este enviará la petición al IAS para verificar que el usuario tiene los permisos necesarios para poder crear el túnel VPN.

También implantaremos una verificación de certificado. Emitiremos, para cada usuario que quiera abrir el túnel VPN un certificado digital asociado a su cuenta del dominio. El servidor RAS verificará que el

cliente que esta intentando conectarse tiene un certificado válido emitido por nuestra entidad certificadora. Solo en el caso que la tenga lo dejará pasar.

Con esto tenemos una doble seguridad, primero, el usuario tendrá que tener el certificado instalado en su maquina y, en segundo lugar, deberá tener los permisos necesarios que se los daremos a través de grupos del directorio activo.

Los requerimientos de estos servidores son mínimos, ya que solo actuaran cuando les llegue alguna petición.

Con estos requerimientos podemos plantearnos un servidor de IAS y RAS con:

- CPU: 2 CPU virtuales.
- Memoria: 1 GB.
- Disco de Sistema: 30 GB.
- Red: 1 GigabitEthernet.

A estos servidores los llamaremos SRAS y SIAS.

5.1.4.- Servicio de Terminal Server

Como habíamos visto, para aumentar más la seguridad y minimizar el espectro de un posible ataque exterior todos los accesos desde fuera de la empresa no se darán a toda la red, aunque tenemos esa posibilidad gracias a la VPN.

En su lugar implementaremos un servicio terminal Server. Este es un servidor de comparte escritorio para múltiples usuarios. Es decir, muchos usuarios se conectan a un mismo servidor y trabajan conjuntamente sin molestarse entre ellos.

Para poder implementar este servicio nos hacen falta dos servidores, uno de terminal Server, que es el servidor donde se van a conectar y otro, de licencias de terminal Server.

El servidor de licencias de terminal Server es necesario puesto que cuando un usuario se va a conectar a un servidor de terminal Server se requiere que haya una licencia de terminal Server disponible. Estas tienen que estar instaladas en un servidor de licencias de terminal Server y es el servidor de terminal Server el que consulta con este si tiene licencias disponibles para asignárselas al usuario.

El servidor de Terminal Server es un servidor que tienen unos grandes requerimientos tanto de memoria como procesamiento, aunque no así de disco, ya que por definición, en nuestro diseño los datos de la empresa estarán guardados en el servidor de ficheros.

Además, al igual que los pcs, los perfiles de los usuarios estarán redirigidos, por lo que estos tampoco ocuparan espacio en disco.

Con esto tenemos que para implementar el servidor de terminal Server necesitaremos:

- CPU: 4 CPU virtuales.

- Memoria: 4 GB.

- Disco de Sistema: 30 GB.

- Red: 1 GigabitEthernet.

A este servidor lo llamaremos STerminal.

El servidor de licencias, como vimos anteriormente, lo vamos a implementar junto con el controlador de dominio, ya que es un servicio que consume muy poco y sería innecesario gastar un servidor para esta función tan pequeña.

5.1.5.- Servicio de entidad Certificadora

Para poder realizar la conexión por VPN a través de certificados digitales tenemos dos opciones, o comprar certificados a una entidad externa o, mucho mejor, instalarnos una entidad certificadora a nivel de empresa.

Con esta podemos emitir nuestros propios certificados digitales que, si bien, no nos serviría para el exterior, cumplirían completamente el propósito que nos hemos planteado de certificar la entrada de nuestro personal.

Para ello, emitiremos certificados para aquellos usuarios del dominio que queramos que entren por VPN, dejando solamente a estos permisos para poder entrar por esta vía.

Evidentemente, podemos utilizar estos certificados para mucho más, como establecer IPSEC en la empresa (encriptación a nivel de red) o cualquier otro servicio que queramos dar con certificados.

Este servidor tampoco requiere una gran capacidad ni de procesamiento, ni de memoria ni de disco, ya que probablemente no lo usaremos más que unas pocas veces.

- CPU: 1 CPU virtuales.
- Memoria: 1 GB.
- Disco de Sistema: 30 GB.
- Red: 1 GigabitEthernet.

A este servidor lo llamaremos SCert.

5.1.6.- Servicio de Backup

Para realizar las copias de todo el sistema, tanto de maquinas virtuales como de datos, vamos a crear un servidor en exclusiva, el cual tendrá la conexión con la red de almacenamiento de copias y el software para realizar las copias.

Vamos a realizar varios tipos de copias de seguridad. Primero, copias del dominio, luego copia de los datos y por ultimo copias de las maquinas virtuales.

Las copias del dominio las haremos de la siguiente forma. Con el software nativo de copias de seguridad de Microsoft haremos las copias en local en cada uno de los controladores de dominio. Luego moveremos esa copia, la cual es un fichero, a la red de almacenamiento de Backup. En este caso, el servidor de backup no realiza ninguna función.

Para las copias de maquinas virtuales vamos a proceder de la siguiente forma. Crearemos un repositorio en la NAS de backup (esto se verá mejor en la parte de diseño de la plataforma de virtualización) y se lo presentaremos a los servidores de VMWare vía NFS. Gracias a un script llamado Ghetto realizaremos copias de las maquinas virtuales realizando previamente unos *snapshots*([5]), lo que hace que no sea necesario parar las maquinas y no afecta a la producción.

Este script, que lo provee directamente VMWare, realiza las copias directamente en la NAS de backup, por lo que no hay que realizar ningún movimiento posterior.

En este segundo caso, el servidor de copias será el encargado de lanzar estas copias a través de una tarea programada. Para ello, debe conectarse al servidor VMWare (recordar que el servidor de copias será un Windows mientras que el VMWare es un *hypervisor*). Para ello necesitamos dos programitas extras, el putty.exe, para poder conectarnos vía ssh al servidor VMWare y el plink.exe, para permitir lanzar comandos externos.

Con estos tres programas realizaremos un script para poder lanzar las copias, creando una tarea programada.

Por ultimo, y no menos importante, son las copias de los datos de la empresa. En el punto en el que estamos simplemente lo que tenemos que copiar es el servidor de ficheros, pero cuando se añadan servicios a la plataforma, se encargará también de copiar estas otras aplicaciones.

[5] Un *snapshot* es una imagen del sistema en un instante dado. En virtualización, realizas un *snapshot* en un instante en el tiempo y puedes regresar a el en caso de fallo de forma inmediata.

Para realizar esta última copia utilizaremos el software Cobian Backup, el cual es gratuito y nos permite hacer planificación de copias, distintos tipos de copias (totales, incrementales y diferenciales), guardar más de un juego de copias, etc.

En este último caso, el servidor de copias será el encargado de realizar la copia del servidor de ficheros a la NAS de backup.

Con todos estos requerimientos vemos que el servidor de copias también tiene que tener unas altas prestaciones en cuanto a procesamiento, red y almacenamiento, aunque algo menos en cuanto a memoria, con lo que tendríamos:

- CPU: 2 CPU virtuales.
- Memoria: 4 GB.
- Disco de Sistema: 30 GB.
- Red: 2 GigabitEthernet.

A este servidor lo llamaremos SBackup.

5.1.7.- Servidor VCenter

El sistema de virtualización requiere que haya un servidor que sea el que lleve la consola de administración de la plataforma. Esta consola se llama VCenter y puede estar en un servidor virtualizado.

Este servidor al ser de gestión no requiere que tenga unas grandes especificaciones técnicas, pero quizás si un poco más de

almacenamiento para poder guardar los logs del sistema, con lo que tendríamos:

- CPU: 2 CPU virtuales.
- Memoria: 2 GB.
- Disco de Sistema: 70 GB.
- Red: 1 GigabitEthernet.

5.1.8.- Servidor de Monitorización

No entraba dentro de los requerimientos de la empresa y no es algo que sea fundamental en el trabajo diario de ella, pero desde el punto de vista técnico, es importante saber que esta pasando en el sistema y que es lo que puede fallar en algún momento.

Para ello vamos a crear un servidor virtual con un software de monitorización de los recursos del sistema, de forma que seamos capaces de detectar fácilmente los errores y, en algunos casos, incluso minimizarlos o evitarlos.

Esto creemos que nos aporta un gran valor añadido, dado la complejidad del sistema y el ámbito al que va dedicado, donde el personal puede no se muy técnico.

Para ello vamos a montar el servicio de Nagios, el cual es *Open Source* y es uno de los más usados para monitorización. Entre las principales características que hace que nos decantemos por él esta:

- Ampliamente usado y con gran documentación.
- Integrable con del directorio activo.
- Agentes específicos para Windows, VMWare y NAS.
- Posibilidad de ampliación de características vía SNMP.
- Posibilidad de chequeos de dispositivos distintos de servidores como switches o redes de almacenamiento.
- Posibilidad de envío de alertas por correo o SMS.
- Interfaz Web de fácil uso.
- Clientes integrables con dispositivos móviles tipo IOS o Android.

Lo que montaremos será un servidor virtual con las siguientes características:

- CPU: 1 CPU virtuales.
- Memoria: 1 GB.
- Disco de Sistema: 30 GB.
- Red: 1 GigabitEthernet.
- S.O.: Centos.

- Servidor Web: Apache.

Con esto tendremos una página Web donde veremos todos los servicios que monitorizaremos, en verde si están dentro del rango especificado y en rojo en caso contrario. Estos rangos de errores los estableceremos nosotros en la configuración.

A todos los servidores le instalaremos un agente de Nagios, el cual nos permitirá ir más allá de la simple monitorización de los parámetros básicos.

En caso de error de alguno de ellos, configuraremos una dirección de correo donde mandaremos un mensaje de error.

Servidores

De cada servidor monitorizaremos:

- Estado Activo (*Uptime* o ping).
- Espacio de todos sus discos.
- Espacio de memoria.
- Consumo de CPU.
- Estado de las tarjetas de red.
- Servicio Servidor.

- Temperatura.
- Estado del RAID de discos.
- Estado de las fuentes.
- Estado de los módulos de memoria.

Nótese aquí la importancia la monitorización de los discos RAID y las fuentes. Gracias a la redundancia, un error no causa la caída del sistema, pero si no estamos atentos este puede pasar por alto y si se produce otro error, si que habrá una caída, que puede ser fatal.

Además de esto que es general para todos los servidores, también monitorizaremos servicios distintos de cada servidor, estos serán:

De los controladores de dominio además monitorizaremos

- Servicio DNS activo.
- Servicio DHCP activo.
- Servicio Licencias de terminal Server activo.
- Servicio LDAP activo.
- Puerto peticiones LDAP (TCP 389) abierto.

De la entidad certificadora además monitorizaremos

- Servicio IIS.
- Servicio de Certificación.

Del servidor Radius además monitorizaremos

- Servicio de autenticación.

Del servidor Ras además monitorizaremos

- Servicio de enrutamiento y acceso remoto.

Del servidor Terminal además monitorizaremos

- Servicio de terminal Server.
- Servicio de cola de impresión.
- Puerto de RDP (3389) abierto.

Del servidor de Backup monitorizaremos

- Proceso de Cobian Backup.

Del servidor VCenter monitorizaremos

- Servicio VCenter.

- Servicio BBDD SQLServer Embebido.

Switches

De los switches monitorizaremos que estén activos (*Uptime*)

NAS

De las NAS monitorizaremos:

- Que estén activos (*Uptime*).
- Espacio en disco.
- Estado de las controladoras.

En la NAS de Backup, a través del servidor de Backup, también monitorizaremos que se generan diariamente las copias.

SAI

De la SAI podremos monitorizar si esta activa, la carga que están, la temperatura y el nivel de las baterías.

A este servidor lo llamaremos SNagios.

5.1.9.- Servicio de WSUS

Entendemos que para la mayoría de las empresas que estamos realizando este diseño serán redes en las que los clientes, es decir, los

pcs, serán de la plataforma Microsoft, principalmente Microsoft Windows 7 y 8, aunque todavía con algunos Windows Vista y XP.
Estos equipos reciben actualizaciones desde Internet. Para evitar que todos ellos vayan hacia Internet a buscar las actualizaciones vamos a montar un servicio de actualizaciones dentro de la red.

El mismo se encarga de, dadas unas políticas establecidas, descargarse las actualizaciones desde la Web de Microsoft y aplicarlas a los equipos. Estos, a través de una directiva del dominio, en lugar de ir a buscar las actualizaciones a Internet, irán a buscarlas a este servidor.

Esto hace que se reduzca el uso de ancho de banda de la empresa, además de permitirnos un control exhaustivo de las actualizaciones dentro de la misma.

El servicio que vamos a instalar para que esto funcione es el WSUS. El mismo nos proporciona una consola de administración Web donde le diremos que paquete nos descargaremos y cuando.

También crearemos una serie de políticas de aprobación automática de parches, de forma que no tengamos que aprobarlos todos manualmente. Solo aquellos paquetes que estén aprobados serán los que se instalen en los pcs. Por defecto aprobaremos todas aquellas actualizaciones que sean críticas y de seguridad.

Por ultimo, crearemos una política de aplicación de parche en la que estableceremos que se instalen todas las actualizaciones aprobadas sin necesidad que el usuario de su aprobación, pidiéndole a este permiso para reiniciar el equipo una vez finalizada la actualización.

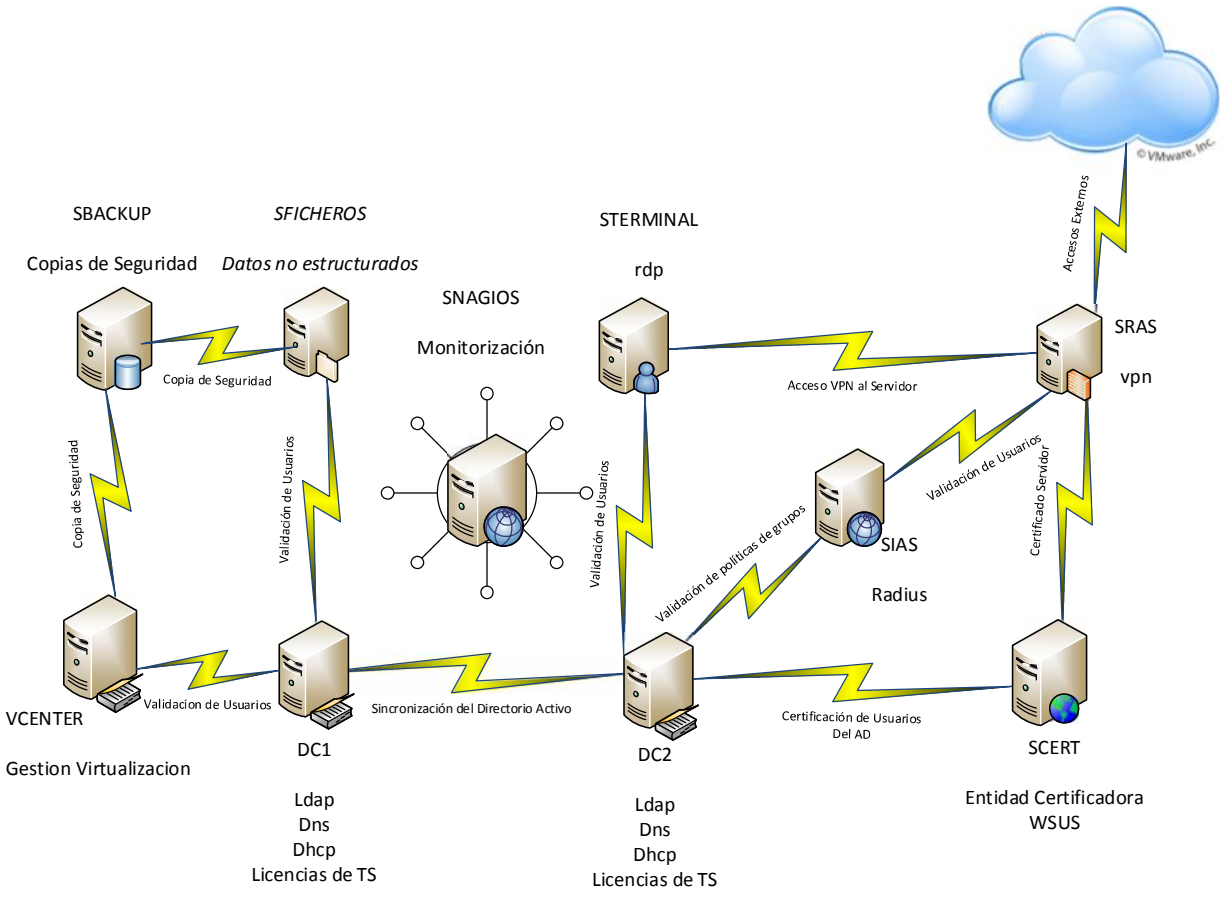
Con este servicio aumentamos la seguridad de nuestra red al tener los equipos siempre con los parches de seguridad, lo que en caso de propagación de algún virus por una debilidad del sistema estaremos protegidos.

Al igual que el servicio de monitorización, este servicio no esta en las necesidades de las empresas, pero da un valor añadido al diseño desde el punto de vista de las tecnologías de la información.

Este servicio no requiere muchos recursos, por lo que vamos a aprovechar el servidor de entidades certificadoras, cuyo trabajo se limita a situaciones muy puntuales y en el instalaremos este servicio.

5.1.10.- Diseño completo

Presentamos a continuación el diseño completo.



Evidentemente estos servidores son virtuales, simplemente se muestran aquí como servidores para la compresión del diseño.

5.2.- Diseño de la plataforma de virtualización

A continuación vamos a proceder a presentar la plataforma de virtualización.

Hemos seleccionado VSphere 5 como plataforma de virtualización. El hypervisor que utiliza esta plataforma es el ESXi. Por tanto, los dos servidores físicos que vamos a poner lo instalaremos con ESXi.

La instalación de este software es bastante sencilla, simplemente tendremos en cuenta varias cosas en la configuración:

- Todas las tarjetas de red estarán dentro de un switch virtual en modo activo.

- Le pondremos una contraseña de entrada.

- Habilitaremos el acceso vía ssh a los servidores para poder entrar a realizar las copias.

En cuanto al almacenamiento de las maquinas virtuales, las mismas las pondremos en la NAS y nunca en los discos locales de los servidores ESXi.

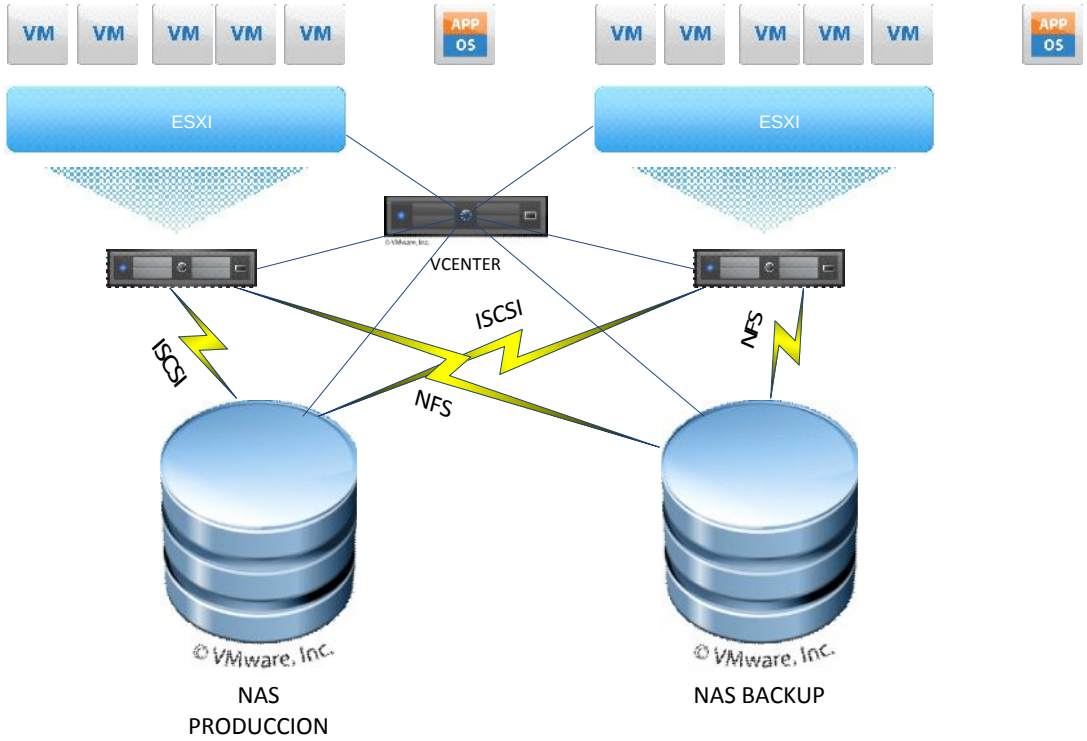
Por tanto crearemos los volúmenes en la NAS y se los presentaremos a los servidores ESXi por ISCSI. Una vez realizado esto los servidores los formatearan en el sistema VMFS y ya podremos poner en ellos maquinas virtuales.

El número de volúmenes a crear dependerá del almacenamiento, pero en principio crearemos tantos como sean necesarios de 1 TB en 1TB, y como mínimo uno por cada servidor. Es decir, en la configuración original crearemos dos volúmenes de 1 TB y le pasaremos a cada servidor uno de ellos.

Por ultimo, la red de almacenamiento de Backup también creará un volumen lógico y se lo presentara a los servidores, en este caso vía NFS. En este volumen será donde se realicen las copias de seguridad de las maquinas virtuales completas.

Al igual que la NAS de producción, se crearan tantos volúmenes como sean necesarios en tamaños de 1 TB. Como mínimo uno por cada servidor y volumen de producción que tenga el servidor.

El diseño quedaría como mostramos a continuación.

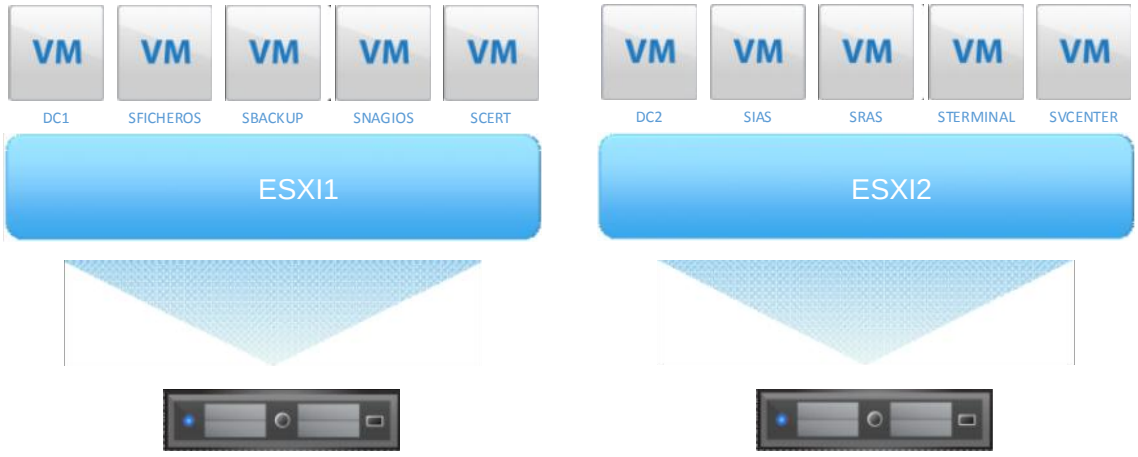


Como se puede ver en el diseño, toda esta infraestructura esta gestionada desde el VCenter. El mismo es la consola de administración de una infraestructura virtual. Desde el mismo hacemos la gestión centralizada de todos los recursos de la plataforma, desde los servidores físicos, los servidores virtuales, el almacenamiento etc, etc.

Por motivos meramente ilustrativos el VCenter aparece aquí como una máquina física, pero será una máquina virtual más dentro de la infraestructura.

A pesar que las maquinas virtuales, por su propia naturaleza pueden estar en los distintos servidores físicos, presentamos a continuación la configuración inicial con la ubicación que le daremos al principio a cada servidor virtual, es decir, en que servidor físico esta que virtual.

Para ello intentaremos que la carga (cpu y memoria) estén balanceadas entre los dos servidores, de forma que no haya ninguno que trabaje más que el otro.



5.3.- Diseño de la solución Hardware

Vamos a continuación a realizar el diseño de la solución hardware que de soporte a toda la infraestructura que hemos visto anteriormente.

5.3.1.- Servidores

En este caso si que estamos hablando de servidores físicos, es decir, de "hierro".

Las principales características que deben cumplir los servidores como habíamos visto en los apartados anteriores son los siguientes:

- Enracable.
- Doble CPU Quad Core o superior.
- Más de un módulo de memoria. Cada uno con capacidad de aguantar todos los servidores virtuales.
- Doble o más tarjetas de red GigabitEthernet.
- Doble fuente de alimentación.
- Doble ventilación.

Teniendo en cuenta los servidores virtuales que tenemos, sería:

- CPU: 20 VCPU.
- Memoria total: 20 GB.
- Discos de Sistema: 310 GB.

Hemos seleccionado para nuestro diseño:

Dell PowerEdge R420		
	Item	**Ctd**
Procesador	Intel® Xeon® E5-2407 2.20GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W	2
Memoria	4GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x8 Data Width	8
Controladora	PERC H310 Integrated RAID Controller, Mini-type	1
Discos	300GB, SAS 6Gbps, 2.5-in, 10K RPM Hybrid Hard Drive (Hot Plug) in 3.5-in Carrier	2
Fuente	Dual Hot Plug Power Supplies 550W	1
Red	On-Board Broadcom 5720 Dual Port 1GBE	1
SO	Windows Server 2008 R2 SP1, Enterprise Edition, Spanish, Incl. 10 CALs, No Media	1
Guías del Rack	ReadyRails™ Sliding Rails Without Cable Management Arm	2
Chásis	3.5" Chassis with up to 4 Hot Plug Hard Drives	1
Red de Gestión	iDRAC7 Express	1

Con esto tenemos cubiertos los requerimientos que habíamos visto anteriormente.

Hacer notar varias cosas. Evidentemente el numero de procesadores que nos sale es bastante inferior a los procesadores virtuales, pero hay que entender que no es una relación directa core-vcpu, sino que el

software de virtualización realiza una gestión de los recursos con la que un core corresponde a mas de una CPU.

En cuanto a la memoria tampoco salen exactamente las cuentas, en este caso, sobrepasándola con creces (2 x 32 vs 19), pero el caso es que como hemos visto, esto es la plataforma, con lo que entendemos que sobre ella se montaran más aplicaciones que serán las que consuman el resto de la memoria.

Normalmente, cuando compras servidores es más barato adquirir junto a él el S.O. que comprándolo luego por libre. Es por eso por lo que esta incluido en la lista a pesar que ser software.

Lo que hemos llamado red de gestión es una tarjeta de red que la mayoría de los fabricantes ya incluyen en sus productos. La misma permite acceder al servidor a través de la red como si se estuviera en la consola de la misma. Nos permite acceder a la pantalla del servidor e incluso hacer un apagado y encendido eléctrico.

Por ultimo justificar la elección de DELL. Es un fabricante de los más conocidos en el mercado, tiene una cuota de mercado muy amplia y además, lo mas importante dada la situación periférica de las islas, *partner* local, soporte en plaza y servicio 24x7 real, es decir, en caso de avería de alguna pieza en un día tendríamos el repuesto en nuestra empresa.

5.3.2.- Red

Como habíamos visto en el análisis de requerimientos, en cuanto a la red nuestro diseño no tiene unos requerimientos muy grandes en cuanto a gestión, esto es, no necesitamos montar diferentes rede

virtuales (VLANs), ni calidad de servicio (QoS), ni enrutamiento (Layer 3) ni siquiera DHCP, pues como vimos en el diseño de la solución software, dejaremos a los servidores Windows que hagan esta función.

Entonces básicamente el único requerimiento, más allá de la propia función de switch, es que sea GigabitEthernet.

Para esto hemos elegido el D-Link EasySmart 24-Port Managed Gigabit Switch (DGS-1100-24), el cuál tiene las siguientes características:

D-Link EasySmart 24-Port	
Capa OSI	Layer 2
Número de Puertos	24
Capacidad de Switching	48Gb
Tamaño tabla MAC	8k
VLAN	Si
QoS	Si
Disposición	Enracable
Gestionable	Si

En este caso el modelo seleccionado tiene características que hemos dicho que no son estrictamente necesarias para nuestro diseño, pero que vienen de serie con el switch.

Notar la capacidad de Switching. Este dato no se suele tener mucho en cuenta a la hora de realizar un diseño de una red y es fundamental, pues es la capacidad que tiene el switch de cambiar traspasar información de un puerto a otro. Al tener 24 puertos a GigabitEthernet podemos tener conectados 24 Gb. Al tener 48GB de capacidad de

Switching nos aseguramos que el switch, en caso de que todos enviasen a la vez, sería capaz de atender todas estas peticiones.

Vamos a montar dos switches de estas características para mantener la redundancia. Por ello no especificamos que requieran una segunda fuente de alimentación, un switch completo será suficiente respaldo.

5.3.3.- NAS

Tenemos que ver dos tipos de NAS, la NAS de producción, que será una NAS de altas prestaciones y la NAS de backup, que solo requerirá de almacenamiento.

NAS de producción.

Hay que hacer notar aquí que el almacenamiento es el núcleo de la empresa y es, fundamentalmente, el culpable que podamos montar la alta disponibilidad a nivel de maquinas virtuales gracias a la compartición de recursos por red. Por tanto, se da por hecho que el mayor gasto en la empresa se hará en este apartado.

Para ello hemos elegido el siguiente producto: EMC VNXe 3150 con una configuración preconfigurada que es la que sigue:

EMC VNXe 3150	
Controladora	Doble controladora y procesador
Discos Soportados	SSD, SAS y NL-SAS
Niveles RAID	10, 5 y 6
Max. Tamaño de LUN	2 TB
Tamaño	2 U
Red	2 GigabitEthernet

Protocolos	ISCSI, NFS, CIFS
Sistemas Soportados	Windows, Linux, VMWare
Gestión	EMC Unisphere
Integración con A.D.	SI
Tamaño por defecto	15.6 TB SAS y NLSAS

Con esto cubrimos todos los requerimientos en cuanto a red de almacenamiento que habíamos visto en el análisis de los requerimientos del almacenamiento.

NAS de Backup

Para la NAS de Backup no necesitamos unos requerimientos de rendimiento tan altos como para la NAS de producción. Por ello, seleccionaremos una NAS con discos SATA en lugar de SAS, lo que hace que el precio de este baje bastante.

Hemos elegido el siguiente producto: QNap TS-869U-RP con la configuración siguiente:

QNap TS-869U-RP	
Controladora	Simple
Discos Soportados	SATA
Niveles RAID	10, 5 y 6
Max. Tamaño de LUN	2 TB
Tamaño	2 U
Red	2 GigabitEthernet
Protocolos	ISCSI, NFS, CIFS
Sistemas Soportados	Windows, Linux, VMWare
Gestión	Sí

Integración con A.D.	SI

Esta NAS no tiene almacenamiento por defecto por lo que habrá que añadirle los discos, para lo cual hemos elegido:

8 x Disco Seagate 3Tb 3.5" SATA3 64Mb 7200rpm.

Esto nos deja un almacenamiento total bruto de 24 TB.

5.3.4.- RACK

Para que todo este en su sitio y no haya nada fuera de lugar vamos a meterlo todo dentro de un armario RACK.

El estándar son los armarios de 19” de 600mm de ancho, aunque hay distintas variantes. También según si van en suelo o en pared, llamándose estos últimos armarios murales.

El mismo se mide en número de Us o huecos que posee, en nuestro caso necesitamos:

	Us	**Ctd**	**Total**
Servidores	1	2	2
Switches	1	2	2
NAS	2	2	4
Total			8

Elegimos el siguiente producto Armario Rack de 19 MobiRack de 18U y fondo 600. Las características son:

- Armario de 19 pulgadas.

- Ruedas y pies de nivelación.
- Regleta de 6 enchufes schucko.
- Puerta frontal con cristales tintados y trasera metálica.
- Paneles laterales .
- Rejilla superior con ventilación.
- Tornillería incluida.

5.3.5.- SAI (Opcional)

Un SAI o UPS es un sistema de alimentación ininterrumpida. Tiene dos funciones principales, la primera, en caso de una caída de corriente alimenta durante un tiempo limitado a los elementos electrónicos y otra, servir corriente eléctrica de forma más limpia a los elementos electrónicos, eliminando las subidas y bajadas de tensión.

Originalmente no es función de el diseño el incluir una SAI, pues habíamos dejado la parte de infraestructura de la empresa y lo ideal es que este montado de forma integrada con le edificio u oficina.

No obstante incluimos de forma opcional en el diseño la inclusión de una SAI específica para el mismo, de forma que en los casos que la empresa no tuviera este sistema se le pueda incluir fácilmente.

Para poder realizar el diseño de un SAI tenemos que analizar los consumos de los elementos individuales de los que consta el diseño para poder calcular el voltaje necesario.

Tenemos los siguientes datos sacados de las especificaciones de los productos:

	W	Ctd	Total
Servidores	500	4	2000
NAS	440	1	440
NAS Backup	75	1	75
Switches	15	2	30
Total			2545 W

Para dar solución de continuidad eléctrica seleccionamos el siguiente producto, APC Smart-UPS 3000VA LCD RM 2U 230V, el cual nos da una salida de 2700, lo cual cubre nuestras necesidades, además también tiene las siguientes características:

- Enracable.
- Tamaño 2 U.
- Tiempo de recarga 3 horas.

5.3.6.- Diseño Completo

Una vez visto todos los componentes de la solución hardware presentamos el diseño completo dentro de su armario Rack.

En la parte superior del armario colocaremos la electrónica de red.

En la parte inferior colocaremos la SAI. Es el elemento que mas pesa de toda la infraestructura y si lo colocáramos en la parte superior se nos podría volcar el armario.
Luego colocaremos las dos redes de almacenamiento y por ultimo colocaremos los dos servidores.

En el diseño, como se puede ver, quedan bastantes huecos libres dentro del armario por si queremos seguir ampliando la infraestructura. También podríamos haber puesto un switch KVM enracable para controlas los servidores, pero teniendo solamente dos servidores no lo estimamos oportuno

En definitiva el diseño queda más o menos así:

Switches		D-Link EasySmart 24-Port
Servidores		Dell PowerEdge R420
NAS Backup		QNap TS-869U-RP
NAS		EMC VNXe 3150
SAI		APC Smart-UPS 3000VA

Como podemos observar es un diseño totalmente compacto, cerrado y modular. Podríamos incluso motarlo todo antes de entregarlo en las oficinas del cliente.

5.4.- Valoración Económica

Por ultimo, vamos a realizar una valoración económica de todo el diseño de la infraestructura.
La misma se hará sobre precios en PVP, sin tener en cuenta posibles descuentos que podamos conseguir u ofertas de última hora.

Evidentemente, la flexibilidad del diseño estriba en que todos los elementos son intercambiables, es decir, podemos seleccionar en un momento dado elegir entre una NAS u otra o cambiar un servidor por otro.

Con esto lo que quiero decir es que la valoración económica es en este momento del tiempo, pudiendo variar en un futuro próximo.

Concepto	PVP (€)	Ctd	Total (€)
Servidor + S.O.	4529	2	9058
Red	150	2	300
NAS	12000	1	12000
NAS Backup	1926	1	1926
Discos Backup	96	8	768
Rack	263	1	263
VMWare	450	1	450
TSCals	90	5	450
Ingeniería([6])	2000	1	2000
Total			27215
SAI	1625	1	1625
Total + SAI			28840

[6] Montaje de la solución hardware e implementación de la solución Software.

6.- Normativa y Legislación

Una vez realizado el diseño vamos a realizar el estudio de la normativa y la legislación para analizar el cumplimiento de las mismas por parte del diseño.

Se van a presentar la normativa y la legislación que debe aplicar este TFG sin hacer un desarrollo profundo en las mismas, dado que esta fuera del alcance de este TFG.

También, en los casos que sean necesarios, se presentaran los estándares que cumplen los productos.

6.1.- Legislación Nacional

6.1.1.- LOPD y Rea Decreto 1720/2007

Nos referimos a la LOPD y al real decreto que desarrolla la ley a:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD).

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Descripción de la ley

El organismo en España encargado de velar por el cumplimiento de las Leyes de protección de datos personales la Agencia de protección de datos. Regulada por el título VI de LOPDCP 15/1999 y Estatutos de

APD (R.D. 428/1993 de 26 de marzo BOE 106 de 4 de mayo de 1.993). Son funciones de la agencia: inspectora, ordenadora, de publicidad, sancionadora, inmovilizadora, reguladora, unificadora y de relaciones con el exterior.

En la Ley Orgánica de Protección de Datos de Carácter Personal se establece la creación de un Registro General de Protección de Datos que será administrado por la Agencia de Protección de Datos. Se notificará a esta la creación por personas o entidades de ficheros de datos de carácter personal, y los detalles relativos a:

- Responsable del fichero.
- Finalidad.
- Ubicación.
- Tipo de datos contenidos.
- Medidas de seguridad aplicadas. Clasificadas en tres niveles, básico, medio, alto.
- Cesiones que se prevean realizar.

En el Real Decreto 994/1999 se detalla el reglamento de seguridad para dichos ficheros. Se exige que el responsable del fichero elabore e implante la normativa de seguridad mediante un documento llamado Documento de Seguridad. El documento constará al menos de las siguientes partes:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

- Medidas, normas, procedimientos el, reglas y estándares encaminados a garantizar el nivel de seguridad exigido.

- Funciones y obligaciones del personal.

- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

- Procedimiento de notificación, gestión y respuesta ante las incidencias.

- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Niveles de seguridad:

En lo relativo a niveles de seguridad ya hemos advertido que la ley estable tres niveles, básico, medio y alto, según sea la sensibilidad de los datos almacenados.

- Nivel básico: Todos los ficheros o tratamientos de datos de carácter personal.

- Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).

- Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

Aplicación de la ley

En nuestro caso los únicos datos que tenemos son de nivel básico, por lo que debemos cumplir:

Para todos los ficheros (automatizados o no).

Personal:

- Definir las funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios.

- Definir las funciones de control y las autorizaciones delegadas por el responsable.

- Difundir entre el personal, de las normas que les afecten y las consecuencias por su incumplimiento.

Incidencias:

- Llevar un registro de incidencias en el que se detalle: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras.

- Elaborar un procedimiento de notificación y gestión de las incidencias.

Control de acceso:

- Disponer de una relación actualizada de usuarios y accesos autorizados.
- Controlar los accesos permitidos a cada usuario según las funciones asignadas.
- Implantar mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.
- Conceder permisos de acceso sólo el personal autorizado.
- Adoptar las mismas medidas para personal ajeno con acceso a los recursos de datos.

Gestión de soportes:

- Crear un inventario de soportes.
- Identificar el tipo de información que contienen los soportes.
- Restringir el acceso al lugar de almacenamiento de los soportes.
- Autorizar las salidas de soportes (incluidas a través de e-mail).
- Implantar medidas para el transporte y el desecho de soportes.

Solo para ficheros automatizados.

Identificación y autenticación:

- Implantar mecanismos de identificación y autenticación personalizada de los usuarios.

- Crear un procedimiento de asignación y distribución de contraseñas.

- Almacenar las contraseñas de forma ininteligible.

- Cambiar las contraseñas con una periodicidad mínima de 1 año.

Copias de respaldo:

- Hacer una copia de respaldo semanal.

- Establecer procedimientos de generación de copias de respaldo y recuperación de datos.

- Verificar semestralmente los procedimientos.

- Reconstruir los datos a partir de la última copia o grabarlos manualmente en su caso, si existe documentación que lo permita.

- Realizar copia de seguridad y aplicar el nivel de seguridad correspondiente, si se realizan pruebas con datos reales.

Solo para ficheros no automatizados

Criterios de archivo:

- El archivado de documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Almacenamiento:

- Dotar a los dispositivos de almacenamiento de mecanismos que obstaculicen su apertura.

Custodia de soportes:

- Establecer criterios de diligente y custodia de la documentación por parte de la persona a cargo de la misma, durante su revisión tramitación, para evitar accesos no autorizados.

Como hemos visto a lo largo del proyecto, todos nuestros sistemas se basan en la integración con el directorio activo, a través del cual estableceremos los permisos sobre los ficheros a las personas autorizadas. En el mismo tendremos una relación perfectamente actualizada de los usuarios que pertenecen a nuestra empresa y desde el mismo asignaremos los permisos solo a aquellas personas que tengan, por sus funciones, que acceder a ellos.

Además, también se establece desde el directorio activo una política de cambios de contraseña periódica, además de una complejidad mínima que debe cumplir, de forma que se cumple la periodicidad de la contraseña. El almacenamiento de esta contraseña será de forman ininteligible, pues el propio sistema esta diseñado para ello.

En cuando a los accesos externos, hemos visto en el diseño que las comunicaciones del personal desde el exterior de la empresa serán a

través de un mecanismo de certificado digital, por lo que toda la comunicación irá cifrada. Además, como todo en nuestro diseño, estos accesos estarán dados desde la validación del usuario contra el directorio activo.

El registro de los accesos de los usuarios se realiza a través de los registros de seguridad de los controladores de dominio. En estos se guardan los accesos al sistema de todos los usuarios, el tiempo de conexión y la hora de desconexión.

Activando las auditorias sobre los ficheros guardaremos los accesos a los mismos del personal de la empresa. Los mismos se guardaran en el mismo registro de seguridad de los controladores de dominio que hablábamos antes.

En cuanto a las copias de seguridad se ha creado la plataforma para la realización de las mismas, de forma que podamos almacenarlas. El propio sistema de copias permite cifrarlas en caso que fuera necesario (datos de nivel alto).

6.1.2.- Real Decreto Legislativo 1/1996 (LPI)

Estamos hablando en este caso del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (LPI), regularizando, aclarando y armonizando las disposiciones vigentes en la materia.

En cumplimiento de esta ley todo el contenido de este diseño es original, siendo los autores las personas que figuran en su nombre.

6.2.- Legislación Europea

Básicamente son dos las que nos pueden afectar

Directiva 2009/136/CE/ del Parlamento Europeo y del Consejo, de 25 de noviembre.

Directiva 2009/136/CE/ del Parlamento Europeo y del Consejo, de 25 de noviembre.

La Directiva 2009/136/CE modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

La Directiva 2009/140/CE modifica la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

6.3.- Normativas

Se explican a continuación las normativas seguridad para el desarrollo de este diseño.

6.3.1.- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Regula la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos y los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas.

Tiene como principios básicos la seguridad integral, la gestión de riesgos, la prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada.

A pesar que nuestro diseño no tiene como finalidad tratar con la administración pública, se ha seguido el esquema nacional de seguridad como guía de buenas maneras y procedimientos.

Además, tampoco podemos descartar que el mismo termine siendo parte de alguna administración, ya sea local, autonómica o estatal, por lo que siempre es mejor que el propio diseño cumpla la mayor cantidad de normativas posibles.

6.3.2.- Normativas y estándares hardware.

Producto	Normativa
SAI	Ciclo C, CE, EN 60950, EN/IEC 62040-1-1, EN/IEC 62040-2, GOST, Marca GS, IR, VDE, WEEE.

Armario RACK	DIN 41494 parte 1 y 7, UNE-20539 parte 1 y parte 2 e IEC 297 parte 1 y 2, EIA 310-D. RoHS.
NAS EMC VNX	IEC320-C14. FCC clase A EN55022 clase A. UL 60950;CSAC 22.2-60950, EN 60950; ISO 9000; ETSI EN 300 386
Switch DLink	IEEE802.3az Energy Efficient Ethernet.
Servidor DELL	Advance Configuration and Power Interface Specification, v2.0c. IEEE 802.3-2005. Intelligent Platform Management Interface, v2.0. Power System Management Protocol Specification, v1.2.

6.3.2.- Otra normativas consultadas

- Los TCSEC (*Trusted Computer Security Evaluation Criteria*) definidas por el Departamento de Defensa de EEUU (conocido como el Libro Naranja).Suministra especificaciones de seguridad relativas a sistemas operativos y gestores de base de datos.

- El ITSEC (*Information Technology Security Evaluation Criteria*) que es el equivalente europeo del libro Naranja, pero más moderno y con mayor alcance que aquel, conocido como Libro Blanco.

- El ITSEM (Information Technology Security Evaluation Manual).

- Las definidas por el subcomité 27 del JTC-1 de la ISO/IEC.

- Las definidas por la ECMA (*European Computer Manufacturing Association*).

- El estándar ISO 7498-2 (*OSI, Security Architecture*).

7.- Competencias

Vemos a continuación las competencias que debemos cumplir y como las cumplimos.

CII01	
Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.	Estas capacidades quedan demostradas en este trabajo. Se ha realizado el análisis pormenorizado de sistemas informáticos, evaluando diferentes tecnologías y productos existentes en el mercada y seleccionando aquellos que mejor convengan en cada caso, haciendo especial hincapié en la seguridad y la calidad del servicio prestado así como en las prestaciones y la disponibilidad del mismo, diseñando, tras este análisis, un sistema integro, fiable, seguro y de alta disponibilidad que tiene una alta calidad y cumple la normativa vigente.

CII02	
Capacidad para planificar, concebir, desplegar y dirigir proyectos, servicios y sistemas informáticos en todos los ámbitos, liderando su puesta en marcha y su mejora continua y valorando su impacto económico y social.	El desarrollo de una infraestructura TIC de una empresa se ha realizado en base al análisis de los requerimientos de la misma para, a través de ellos, idear el sistema, desarrollarlo y planificar su concepción y puesta en marcha. Además se ha realizado un diseño modular, dejado la puerta abierta para nuevos servicios y realizar así una mejora del sistema propuesto. Se ha tenido en cuenta las tecnologías más punteras, intentando acercar estas a las empresas a un coste relativamente bajo, para mejorar así su competitividad y capacidad de trabajo.

CII04	
Capacidad para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes.	Se ha especificado en cada apartado del diseño, tanto software o hardware, los requisitos técnicos mínimos para cumplir con los estándares de seguridad, disponibilidad e integridad que hemos exigido así como la normativa vigente. En cada caso hemos expuesto la necesidad de un sistema seguro y de alta disponibilidad, condicionando los productos seleccionados a los que cumplían este requisito. En cuanto al software hemos condicionado la implantación de este a la necesidad de integración en nuestro servicio de directorio. En ambos casos, hemos especificado que sean productos que cumplan con los estándares del mercado, sean ampliamente usados y que cumplan con la normativa vigente.

CII18	
Conocimiento de la normativa y la regulación de la informática en los ámbitos nacional, europeo e internacional.	Se ha especificado un apartado con la normativa vigente y el cumplimientote la misma por parte del diseño realizado, cumpliendo así esta competencia.

8.- Bibliografía

[1] Administración de Windows Server 2008. Agustín Morales Hernández.

[2] Administración de Active Directory Windows Server 2008. Agustín Morales Hernández.

[3] Servicios de red de Windows Server 2008. Agustín Morales Hernández.

[4] Windows Server 2008. Guía del administrador. William R. Stanek. Anaya. Microsoft Press.

[5] Configuración de Windows Server 2008 Active Directory. Dan Holme. Nelson Ruest. Danielle Ruest. Anaya. Microsoft Press.

[6] VMWare ESX Server in the Enterprise. Planing and Securing Virtualization Servers. Edward L. Haletky. Prentice Hall.

[7] Active Directory. Joe Richards. Robbie Allen. Alistair G. Lowe-Norris. Anaya.O´Reilly.

[8] Group Policy, Profiles and IntelliMirror. Jeremy Moskowitz. Sybex

[9] Manuales de referencia y especificaciones de los fabricantes de Hardware.

[10] Wikipedia, Google y paginas webs de referencia (www.hispasec.com, www.josemariagonzalez.es, www.bujarra.com, www.windowstecnico.com, www.josepros.com).

ANEXO A.- Redundancia en NAS y CPD remoto.

Redundancia en NAS

Hemos visto durante todo el TFG la forma de crear un diseño altamente seguro y fiable. Hemos realizado todo el diseño teniendo en mente la disponibilidad como gran pilar y la seguridad como segundo.

La alta disponibilidad la hemos conseguido diseñando las soluciones redundadas, es decir, cada elemento crítico individual del sistema tiene un par que es capaz de asumir su carga (lo cual no es excluyente de tener una solución de recuperación ante desastres, que también diseñamos).

El único elemento que de alguna forma no se adapta en su totalidad a este paradigma es la red de almacenamiento (NAS) que hemos llamado de producción.

Esto no es un caso aislado del diseño que hemos realizado. La mayoría de las empresas solamente mantienen una red de almacenamiento al ser el elemento más caro de todas las infraestructuras. Para valorar este hecho hay que tener en cuenta un detalle, todos los elementos de la NAS están redundados. Tiene dos controladoras, dos fuentes de alimentación, dos tarjetas de red y los discos tienen sus niveles de RAID que permiten el fallo de algunos de ellos, aumentado con la capacidad de poder poner alguno de ellos como hot-spare, con lo que en caso de fallo de un RAID se reconstruiría solo.

Lo que queremos hacer ver que las redes de almacenamiento son elementos altamente redundados y estables, suelen ser la parte de la

infraestructura más segura, con la tecnología más alta, y con la mejor calidad. Aún siendo normal la caída de algunos de sus elementos individuales, la caída de la NAS, como conjunto, es muy muy poco probable.

Aún así habrá empresas que ni siquiera puedan o quieran permitirse esta pequeña probabilidad, por lo que vamos a realizar la ampliación del diseño con otro con dos redes de almacenamiento idénticas, de forma que ante la caída de la primera la segunda pasaría a funcionar con una mínima parada.

Esto se diferencia de la red de almacenamiento de backup en el hecho que en la red de almacenamiento de backup tenemos una copia, normalmente del día anterior, de los datos. En caso de caída deberemos hacer una restauración, tras haber conseguido recuperar la red de almacenamiento original. En el caso que vamos a ver ahora estamos hablando de no perder datos o, como mucho, los datos que no se hayan copiado que han sido de minutos y, además, estar listos en el mismo momento para ser accedidos, sin tiempo de recuperación.

En el caso del diseño que hemos realizado habíamos elegido como red de almacenamiento principal una EMC VNXe 3150. La misma, de forma nativa en su software permite la replicación de volúmenes en otra NAS del mismo tipo.

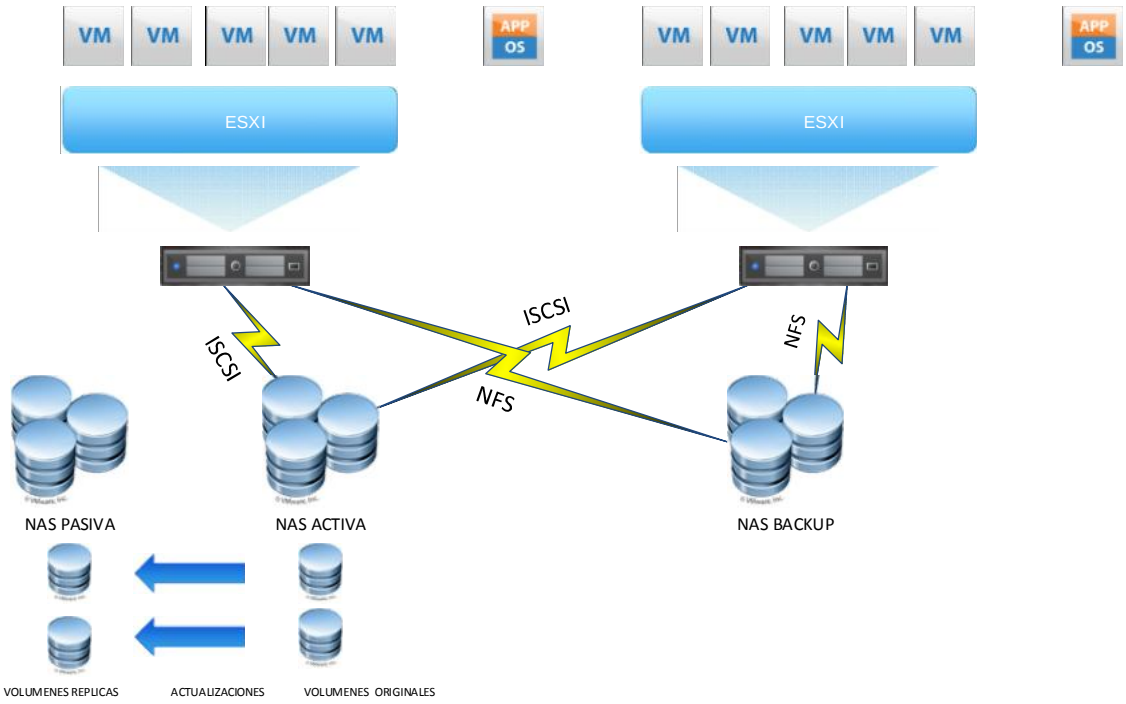
Para ello lo primero que tenemos que hacer es configurar el segundo dispositivo de NAS dentro del primero. Una vez son capaces de verse, cada vez que creemos un nuevo volumen (NFS, CIFS o ISCSI) le especificaremos que cree una replica en este dispositivo de destino.

Podemos especificarle el nivel de replica que queremos, por defecto creará una replica al día, pero nosotros le configuraremos para que cada 15 minutos genere una replica en destino.

Esto lo que provoca es que cada 15 minutos se trasladen los cambios de los volúmenes de la NAS original a la replica.

En caso de caída de la red de almacenamiento, lo único que deberemos hacer será presentar estos volúmenes replicados a los servidores y levantar en ellos las maquinas virtuales. Al ser los cambios a nivel de bloque, estos son consistentes, por lo que tendremos los servidores al estado en el que estaban hace 15 minutos.

Hay que notar que la replica se hace a nivel de volumen, por lo que es fundamental ser disciplinado y cada ez que se cree un volumen realizar la configuración de la replica. Veamos el diseño:



CPD Remoto

Nótese lo fácilmente que sería en este caso tener un CPD de respaldo. En caso de tener dos oficinas en lugares distintos podríamos llevarnos a cada uno de ellos un servidor y una de las NAS y seremos capaces de, en caso de desastre en una de las oficinas (incendio, inundación, robo,…etc) levantar el servicio en la otra.

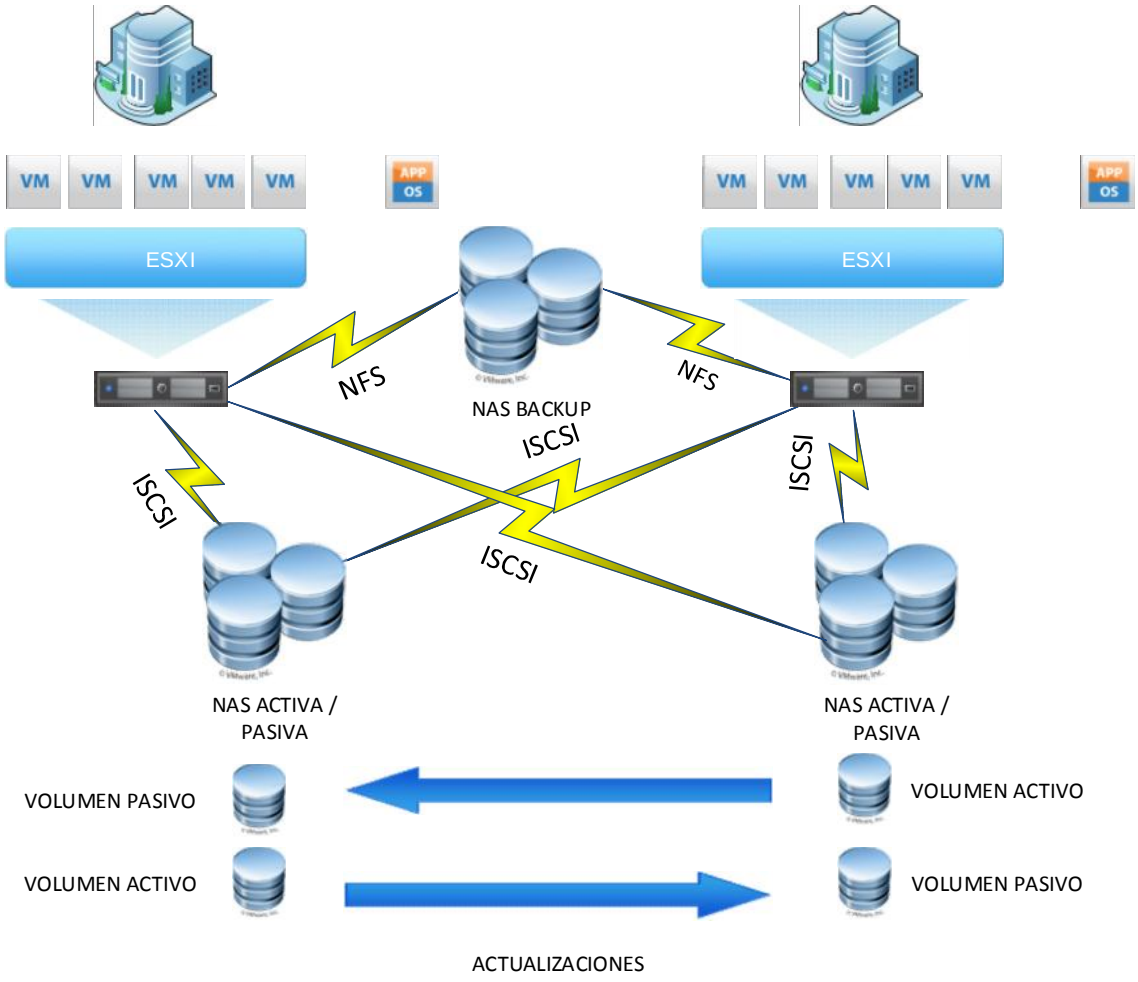
Evidentemente, la velocidad de las comunicaciones entre las distintas sedes de la empresa es fundamental para que las replicas sean buenas. Probablemente en este caso no podremos mantener los 15 minutos de diferencia y habrá que bajar a 1 hora, pero sigue siendo un tiempo más que aceptable.

En el diseño de un CPD remoto hay que hacer ciertos cambios en el diseño. Evidentemente, si nos llevamos un servidor a una sede y otro a otra, las maquinas virtuales que estén en cada uno de ellos deberán acceder a los volúmenes de la NAS que estén en esa sede.

En este nuevo diseño, no habrá una NAS activa y otra pasiva, sino que los volúmenes se replicaran de forma cruzada, es decir, los que están en producción en una se replicaran en la otra y viceversa.

Solo en caso de caída de una de las sedes la otra tomará el control completamente.

El diseño sería el siguiente



Costes

Como hemos visto, la NAS trae de forma nativa el software de replica entre redes de almacenamiento, por lo que el coste de ampliar el diseño en redundancia de NAS será simplemente duplicar este coste, con lo que quedaría:

Concepto	PVP (€)	Ctd	Total (€)
Servidor + S.O.	4529	2	9058
Red	150	2	300
NAS	12000	2	24000
NAS Backup	1926	1	1926
Discos Backup	96	8	768
Rack	263	1	263
VMWare	450	1	450
TSCals	90	5	450
Ingeniería	2500	1	2500
Total			37715
SAI	1625	1	1625
Total + SAI			40890

En cuanto al CPD remoto, como hemos visto no habría más costes adicionales que los propios de montar una nueva oficina y simplemente un nuevo armario RACK, con lo que quedaría:

Concepto	PVP (€)	Ctd	Total (€)
Servidor + S.O.	4529	2	9058
Red	150	2	300
NAS	12000	2	24000
NAS Backup	1926	1	1926
Discos Backup	96	8	768
Rack	263	2	526
VMWare	450	1	450
TSCals	90	5	450
Ingeniería	2500	1	2500

Total			39978
SAI	1625	1	1625
Total + SAI			41603

Conclusión

La duplicación de la red de almacenamiento es bastante cara, como hemos visto. Por eso esta en un Anexo para aquellas empresas que lo requieran y puedan permitírselo.

Me gustaría hacer hincapié en dos cosas, la modularidad del diseño y las virtudes de la virtualización. Gracias a estos dos conceptos hemos visto como pasar a un sistema de replicación de CPD con unos costes bastante razonables y de una forma muy muy sencilla.

ANEXO B.- Diseño de bajo coste

El diseño que hemos propuesto y realizado puede parecer a simple vista algo caro. Nosotros entendemos que no, que la informática de la empresa es algo fundamental en la que no se deberían es tantos recursos, prácticamente al precio de lo que podría ser un coche de empresa.

Aún así, a lo mejor habrá empresas que no requieran tanta capacidad o no puedan (o quieran) permitirse ese costo. Para estas vamos a realizar un diseño en el que, salvaguardando los niveles de seguridad, calidad y disponibilidad, conseguiremos bajar los costes considerablemente, a costa de reducir un poco el rendimiento del sistema.

Una vez más, gracias a la virtualización, no será necesario ningún cambio en el sistema software, por lo que, manteniendo todo el diseño software y la plataforma de virtualización simplemente cambiaremos algunos componentes Hardware.

Lo primero que proponemos es cambiar la red de almacenamiento y en lugar de mantener una NAS de gama media y una de gama baja para backup tendremos dos de gama baja. En este caso no serán replicadas sino una de copia y la otra de backup, pues no traen replicación nativa.

Evidentemente los discos serán SATA y bajará un poco el rendimiento de la misma, pero, como es lógico, a menor coste menor rendimiento.

En segundo lugar cambiaremos el tipo de servidor. Pasaremos a un servidor de gama más baja con un solo procesador. Mantendremos la redundancia de CPU al poder el segundo servidor asumir toda la carga.

También pasaremos los discos de SAS a SATA, lo cual mermará algo el rendimiento.

Por ultimo también quitaremos la doble fuente de alimentación.

Dell PowerEdge R210II		
	Item	**Ctd**
Procesador	Intel® Xeon® E3-1220, 4C/4T, 3.10GHz, 8M Cache, 80W TDP, Turbo	1
Memoria	4GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x8 Data Width	8
Controladora	PERC H310 Integrated RAID Controller, Mini-type	1
Discos	500GB, SATA, 3.5-in, 7.2K RPM Hard Drive	2
Fuente	Hot Plug Power Supplies 550W	1
Red	Broadcom NetXtreme II 5709 Dual Port 1GbE NIC with TOE, PCIe-4	1
SO	Windows Server 2008 R2 SP1, Enterprise Edition, Spanish, Incl. 10 CALs, No Media	1
Guías del Rack	2/4-Post Static Rack Rails	2
Chásis	PowerEdge R210 II Chassis, 2x3.5" Cabled HDDs, LED Diagnostics	1

Evidentemente, al cambiar estos elementos el consumo eléctrico cambia, por lo que podemos cambiar el modelo de la SAI, Esto quedaría:

	W	Ctd	Total
Servidores	250	2	500
NAS	75	2	150
Switches	15	2	30
Total			680 W

Seleccionamos la APC Smart-UPS RT 1000VA RM 230V.

En total, el coste del diseño de bajo coste sería:

Concepto	PVP (€)	Ctd	Total (€)
Servidor + S.O.	2175	2	4350
Red	150	2	300
NAS Backup	1926	2	3582
Discos Backup	96	16	1536
Rack	263	1	263
VMWare	450	1	450
TSCals	90	5	450
Ingeniería	2000	1	2000
Total			12931
SAI	919,00	1	919,00
Total + SAI			13850

Como vemos, el coste se ve altamente reducido, pudiendo llegar con el mismo diseño a más empresas.

En cuanto a la redundancia perdida en los elementos del servidor, hay que notar que simplemente estamos trasladando esa redundancia a

nivel de servidor completo, por lo que el sistema completo en sí sigue siendo redundante, aunque, evidentemente, menos seguro y con un rendimiento menor.