UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

Trabajo de fin de carrera titulado:

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN TECNOLÓGICA BASADA EN METODOLOGÍA MSF PARA EMPRESAS PYMES DE COURIER

Realizado por:

JUAN JOSE ENRÍQUEZ SEGOVIA

Como requisito para la obtención del título de

INGENIERO DE SISTEMAS EN TELECOMUNICACIONES

DIRECTOR: Ing. Santiago Mena

QUITO, JULIO DE 2010

DECLARACIÓN JURAMENTADA

Yo, Juan José Enríquez Segovia, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normalidad institucional vigente.

……..……..

Juan José Enríquez Segovia

DECLARATORIA

El presente trabajo de investigación de fin de carrera, titulado
ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN TECNOLÓGICA BASADA EN METODOLOGÍA MSF PARA EMPRESAS PYMES DE COURIER
Realizado por el alumno
JUAN JOSÉ ENRÍQUEZ SEGOVIA
Como requisito para la obtención del título de
INGENIERO EN SISTEMAS Y TELECOMUNICACIONES
Ha sido dirigido por el profesor
ING. SANTIAGO MENA V.
Quien considera que constituye un trabajo original de su autor

……..
ING. SANTIAGO MENA V.
Director

Los profesores informantes
ING. VIVIANA GUERRÓN
ING. JOSÉ SANCHO
Después de revisar el trabajo escrito presentado,
Lo han calificado como apto para su defensa oral ante el tribunal examinador.

.....	…….
ING. VIVIANA GUERRÓN	ING. JOSÉ SANCHO

Quito, a 12 de Enero de 2010

AGRADECIMIENTOS

Agradezco a Dios por darme la fuerza y la sabiduría para lograr terminar mi carrera con éxitos profesionales, se que con la culminación de mi tesis se abrirán muchas puertas para mí.

Agradezco a mis padres por el apoyo brindado en esta etapa de mi vida y todas las etapas que están por venir, gracias al apoyo incondicional de ellos, estoy ahora dando este gran paso.

Agradezco a mi compañera inseparable mi esposa, que gracias a su apoyo y ánimos incondicionales que mezclados con el amor me supieron llevar por el camino del bien.

Agradezco a la Ing. Viviana Guerrón por toda la paciencia y dedicación que tuvo con la Facultad de Sistemas gracias a ella la Facultad está saliendo adelante, y en especial agradezco al Ing. Santiago Mena que a pesar de que no fue profesor mío supo guiarme en el camino de la elaboración de mi tesis.

RESUMEN EJECUTIVO

Esta tesis que se presenta a continuación tiene como título “ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN TECNOLÓGICA BASADA EN METODOLOGÍA MSF PARA EMPRESAS PYMES DE COURIER”. En primer lugar se ofrece una amplia definición de las Metodologías MSF, estructura del documento, definiciones del mismo. Modelo IOM, esquema de la encuesta, definiciones, esquema de la presentación de resultados, y esquema del archivo de resultados. Definición de servicios, definición de servicios que fueron implementados en la empresa Hermes Express.

Debido a los grandes cambios en el mundo es indispensable ser parte de la competitividad empresarial, es por eso que se debe tomar como clave de éste éxito a las tecnologías de la información para alcanzar mayor rentabilidad dentro de las empresas, es necesario para ello encontrar las mejores soluciones tecnológicas.

El objetivo de la presente tesis es analizar, diseñar e implementar soluciones tecnológicas, para el mejoramiento de la infraestructura de la empresa Hermes Express. Teniendo en cuenta que esta investigación es aplicable a cualquier empresa Pyme del mercado.

ABSTRACT

This thesis presented below is entitled “ANALYSIS, DESIGN AND IMPLEMENTATION OF TECHNOLOGY –BASED SOLUTION METHODS FOR COMPANIES MSF COURIER SMEs. First, it offers a broad definition of MSF methodologies, document structure and definitions of it. Model IOM schem of the survey, definition, outlines of the presentation results and outlines of the output file. Service definition, service definition that were implemented in the Hermes Express.

Due to major changes in the world is indispensable to be part of business competitiveness, which is why it should be taken as the key to this success at information technology to achieve greater profitability within companies, it is necessary to find the best technological solutions.

The objective of this thesis is to analyze, design and implement technology solutions to improve the infrastructure of the company Hermes Express. Given that this research is applicable to any enterprise in the SME market.

INDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

CAPITULO 1

DISEÑO CONCEPTUAL DE LA INVESTIGACIÓN

1.1 DETERMINACIÓN DEL PROBLEMA

Depender de los sistemas de información hace a las organizaciones más vulnerables contra amenazas de la seguridad.

La información es un activo que, al igual que otros de su negocio, tiene valor en las organizaciones y por consiguiente tiene que ser protegida adecuadamente. Las empresas, a través de una identificación y clasificación apropiada de los activos y una evaluación de riesgo sistemática de vulnerabilidades y amenazas, pueden optar por controles apropiados para gestionar riesgos. Demostrando que se preserva la confidencialidad, la integridad y la disponibilidad de esos activos ante clientes, consumidores, accionistas, autoridades y sociedad en general.

La experiencia en el mercado de las empresas de Infraestructura (p.e. Intergrupo, Microsoft) y la utilización del modelo IOM, determinan que las organizaciones tienen un problema en su infraestructura tecnológica; debido a la falta de conocimiento de la plataforma con la que cuentan.

La capacidad de responder rápidamente ante los cambios y optimizar procesos de negocio es un factor clave para la competitividad y el crecimiento de las organizaciones. La agilidad de éstas puede verse cuestionada si se apoya en entornos de IT que no pueden responder de forma flexible a los cambios que afectan a la actividad del negocio.

Las empresas necesitan interconectar los procesos, personas e información tanto con la propia organización, sucursales y socios comerciales. La falta de integración entre los componentes de IT (sistemas, aplicaciones y datos) hace difícil obtener una respuesta rápida y efectiva ante los cambios que afectan de forma natural a los negocios. La generación de costos, reduce la

capacidad de respuesta ante los clientes, compromete el cumplimiento de las normativas legales que afectan negativamente a la productividad de los empleados.

La infraestructura al ser deficiente, es uno de los problemas problema más importantes al que las organizaciones deben hacer frente para mantener su competitividad y garantizar su crecimiento.

Cada vez las organizaciones dependen de la infraestructura, para alcanzar sus objetivos. Pero en un entorno competitivo como el actual, aprovechar las oportunidades de negocio exige moverse con rapidez. Sin embargo, con frecuencia las Tecnologías de Información no admiten respuestas rápidas ni disponen de la flexibilidad necesaria para competir de forma efectiva. Un alto porcentaje de las ineficiencias organizativas tienen un mismo origen: el predominio de procesos manuales con un nivel de error elevado, sistemas ineficaces para compartir la información en la organización; la incapacidad de hacer un correcto seguimiento de los procesos de negocio desde principio a fin; el cumplimiento con las normativas legales aplicables obliga a manejar grandes cantidades de información y formatos complicados de utilizar; y las ineficiencias propias del servicio a clientes. Allí donde se produce cualquiera de estas situaciones, el impacto sobre la productividad de los empleados es negativo, poniendo en riesgo la capacidad de crecimiento y competencia de la propia empresa.

Liberar el potencial que poseen los recursos de IT y hacerlo disponible en forma general a toda la organización facilita la optimización de procesos y mejora la agilidad empresarial, es por eso que se plantea esta investigación que está orientada a la importancia de contar con una infraestructura IT en las empresas, llegando así a una óptima plataforma productiva y segura para mejorar el crecimiento del negocio.

La metodología propuesta para la realización de este proyecto será el modelo IOM, el cual nos permitirá conocer exactamente el estado actual de las empresas Pymes de Courier y a su vez establecer hasta que nivel de madurez puede llegar su infraestructura.

Para esto se llevara a cabo una encuesta[1] basada en el modelo IOM, el cual nos dará como resultado la situación actual de la empresa, permitiéndonos así verificar las principales debilidades y amenazas de la misma.

[1] IOM es un modelo que permite determinar el nivel de madurez de la organización mediante una sola encuesta ya que con esto realizamos el estudio e informe pertinente.

1.2 DEFINICIÓN DEL TEMA

El tema propuesto tiene como finalidad buscar una alternativa de solución al problema existente, razón por la que se plantea el siguiente tema: "Análisis, Diseño e Implementación de una solución tecnológica basado en metodología MSF para empresas Pymes de Courier."

1.3 JUSTIFICACIÓN E IMPORTANCIA

Es conocida la importancia del valor de la información en el desempeño de cualquier actividad empresarial, por ello, la integración de sistemas adquiere una gran importancia en la vida de las empresas como base para la toma de decisiones gerenciales, automatización de procesos, reducción de tiempos y costos.

Por ello se plantea el tema propuesto, con la finalidad de proveer una solución tecnológica con nuevas tendencias en infraestructura, masificando el uso de seguridades y llegando a un nivel dinámico en madurez de infraestructura, por ello la importancia de este tema ya que así se podrá mejorar y optimizar los recursos de la empresa.

El diseño de la Infraestructura Tecnológica se fundamentará en la utilización de las instalaciones de la Empresa Hermes Express, lo que permitirá presentar un análisis de costo beneficio el cual es de gran relevancia en la implementación del proyecto a desarrollar.

Como resultado de la investigación, se obtendrá sistemas seguros y una red óptima, lo que permitirá fortalecer la competencia con las otras empresas que tienen infraestructuras robustas, así mismo aportará a la solución del problema identificado y proporcionará innovaciones con la finalidad de buscar diferentes alternativas tecnológicas que posibiliten soluciones de seguridades para otros proyectos.

1.4 OBJETIVOS

1.4.1 Objetivo General

- Analizar, Diseñar e Implementar soluciones tecnológicas, para el mejoramiento de la infraestructura de la Empresa Hermes Express.

1.4.2 Objetivos Específicos

- Establecer el nivel de madurez de infraestructura mediante el Modelo IOM.
- Diseñar la red física para la Empresa Hermes Express.
- Centralizar actualizaciones automáticas del sistema operativo.
- Analizar, Diseñar e Implementar un servidor de correo electrónico.
- Analizar, Diseñar e Implementar las políticas de grupo, perfiles, accesos para un servidor de directorio activo.
- Analizar, Diseñar e Implementar un sistema para automatizar el flujo de trabajo.
- Llegar a un nivel dinámico de infraestructura.
- Realizar un análisis costo – beneficio de la solución**.**
- Diseñar un esquema de VOIP con software gratuito.

1.5 DELIMITACIÓN DEL TEMA

La empresa en la cual se va a enfocar el estudio es la Empresa Hermes Express, esta empresa se dedica al Courier local y nacional.

La delimitación de este estudio se suscribe al análisis, diseño e implementación de una solución tecnológica estableciendo seguridades, flujos de trabajo, centralizar actualizaciones, políticas de grupo, perfiles, accesos en un solo servidor el cual a su vez permitirá manejar un esquema de direcciones IP con DHCP para toda la red.

Para llevar a cabo esto se plantea la utilización del modelo IOM el cual permitirá determinar el estado actual de la infraestructura de la Empresa Hermes Express.

Se llevara a cabo el estudio y desarrollo de la metodología MSF, mediante esta metodología se presentará la propuesta económica y técnica, estipulando tiempos y manejo de recursos en el proyecto.

Por política interna la Empresa Hermes Express debe tener toda su plataforma en un ambiente Microsoft[2]; se realizará el análisis, diseño e implementación de soluciones Microsoft para el proyecto, teniendo en cuenta los lineamientos técnicos para llevar a cabo el proyecto.

La Empresa requiere que toda la red física sea inalámbrica, para lo cual se hará el análisis, diseño e implementación de la red inalámbrica teniendo en cuenta lineamientos de seguridad para evitar el ingreso de intrusos a los sistemas.

La Empresa cuenta con un sistema llamadas internacionales mediante el internet, para esto se realizará el análisis, diseñó e implementación de un software gratuito de una central telefónica.

[2] Se adjunta carta de la empresa para justificar este punto.

1.6 METODOLOGÍA

Para llevar a cabo esta investigación se utilizara como fuentes primarias: libros, revistas, cursos de certificación Microsoft, Internet, Microsoft Technet, etc. La implementación de este proyecto se realizará a cabo en las instalaciones de la empresa antes mencionada, de igual manera se lleva a cabo una simulación de cómo debería instalarse los servidores.

Y como fuentes secundarias: encuesta IOM, experiencia profesional, gente experta en el sector de las telecomunicaciones, con la finalidad de recabar toda la información posible sobre el tema.

CAPÍTULO 2
MARCO TEÓRICO

2.1 MODELO IOM

2.1.1 Introducción

Con el Modelo de Optimización se busca mejorar la infraestructura alineando las empresas con las tecnologías de la información. Este modelo permite tener un equilibrio óptimo entre la actividad personal, los procesos y la tecnología, dando como resultado una mayor seguridad, una simplificación de los procesos y la gestión permitiendo así tener un trabajo más productivo y optimizando costos y eficacia por parte de los empleados.

La Infraestructura de IT es una valiosa y decisiva estrategia de la organización con la cual, el software puede entregar servicios y aplicaciones de usuario que la organización necesita para operar eficiente y exitosamente.

Hoy en día dentro de las organizaciones, muchas empresas corren aún viejas tecnologías, gastando en procesos manuales mucho más que en técnicas de manejo de infraestructura automatizada, y típicamente, no han mantenido sus ambientes basados en Software, y actualizaciones tecnológicas disponibles para ellos.

El Modelo de Optimización de Infraestructuras aborda la evolución de las infraestructuras de IT en las organizaciones partiendo de una visión global, pero distingue cuatro niveles (Básico, Estándar, Racionalizado y Avanzado) con diferentes capacidades que delimitan el marco de trabajo de cualquier iniciativa de optimización[3]. IOM consta de las siguientes secciones:

[3] http://www.microsoft.com/spain/iom/modelo/

Niveles de madurez de IOM: El Modelo IOM consta de cuatro niveles de madurez: "Básico", "Estándar", "Racionalizado" (o "Avanzado") y "Dinámico". Cada uno de ellos, en términos generales, presenta unas características típicas:

- Nivel Básico: "Apagar incendios"
- Nivel Estándar: "Entorno bajo control"
- Nivel Racionalizado: "Las IT hacen funcionar la empresa"
- Nivel Dinámico: "Las IT son un activo estratégico"

Metodología de trabajo de IOM: La metodología utilizada para el Modelo IOM permite avanzar hacia los máximos niveles de madurez considerados como adecuados para una empresa, una organización o un entorno concreto, y consta de tres fases fundamentales[4]:

- Identificación del grado de madurez actual
- Identificación del grado de madurez óptimo para esta infraestructura
- Diseñar e implementar los proyectos de máximo impacto necesarios para progresar

2.1.2 Definición del Modelo IOM

La *optimización de infraestructura* se define como un proceso orientado fundamentalmente al uso de los activos de IT de una organización, de manera que contribuyan de forma relevante al progreso empresarial. Permite medir el nivel de optimización y guía hacia la consecución de una infraestructura verdaderamente preparada para las personas.

Microsoft ha desarrollado tres modelos, que se centran respectivamente en las infraestructuras básicas (Core IO), la infraestructura de productividad empresarial (BPIO) y la plataforma de aplicación (APIO), que establecen una línea de avance a través de cuatro niveles de optimización. Cada modelo muestra el valor estratégico y los beneficios de negocio que

[4] http://www.microsoft.com/spain/iom/modelo/

supone el paso desde el nivel básico de optimización, en el que la infraestructura se concibe generalmente como un centro de costos a una infraestructura dinámica donde su valor está plenamente asumido y se ve como un factor de negocio y un activo estratégico de la empresa.

Con estos modelos se puede evaluar el nivel actual de la infraestructura, establecer una visión tecnológica de cara al futuro y diseñar una hoja de ruta detallada que permita alcanzar ese objetivo.

Un objetivo fundamental del Modelo IOM ha sido el desarrollo de una metodología de optimización, flexible y sencilla de utilizar, que debe servir además como banco de pruebas y hoja de ruta en la mejora de las capacidades técnicas y el aumento del valor de negocio de las IT.

Se pueden conseguir ahorro de dinero al pasar desde entornos no gestionados a otros basados en una gestión totalmente automática y un uso dinámico de los recursos. Además la seguridad se ve mejorada de forma notable, ya que se pasa de un estado básico muy vulnerable hacia una infraestructura dinámica, proactiva y más optimizada. Su administración pasa de basarse fundamentalmente en la labor manual y reactiva a un modelo automático y proactivo.

El modelo IOM se alinea plenamente con ITIL (IT Infrastructure Library), la metodología de mayor aceptación para la gestión de servicios de IT, que establece una serie completa y coherente de buenas prácticas para la gestión de sistemas. Teniendo en cuenta que se alinea con ITIL este modelo IOM se adopta y adapta a ITIL.

Para empezar a aplicar el proceso del modelo IOM, Microsoft ha desarrollado una evaluación muy sencilla, que consta de varias preguntas relacionadas con cada una de las funciones de gestión, dando como resultado una vista global del grado de madurez relativo de la organización en cada capacidad. Esta evaluación es una forma rápida y sencilla de identificar áreas conflictivas en el entorno, y establece el camino para la mejora sistemática.[5]

[5] http://www.microsoft.com/spain/iom/modelo/nivelesiom.aspx

Figura 2.1 – Descripción del Modelo IOM

Fuente: http://www.microsoft.com/spain/iom/modelo/

2.1.3 Niveles de Madurez del Modelo IOM

Figura 2.2 - Niveles de Madurez del Modelo IOM

Fuente: http://www.microsoft.com/spain/iom/modelo/nivelesiom.aspx

El modelo IOM define 4 niveles de madurez de infraestructura, ellos son Básico, Estándar, Racionalizado y Dinámico:

2.1.3.1 Básico

La infraestructura básica se caracteriza por **procesos manuales y localizados, con mínimo control centralizado**. No existen políticas ni estándares, no se aplican de forma rigurosa estándares de la seguridad, backup, uso y distribución de imágenes del sistema operativo, cumplimiento de normativas y otras actividades esenciales de IT. En general hay ausencia de conocimiento con respecto a la Infraestructura que se tiene en el lugar o cuales tácticas tendrán el máximo impacto sobre estas. La información se guarda en carpetas compartidas y en los discos duros de los usuarios, y se emplean herramientas de búsqueda muy manuales. La gestión de los registros se hace mediante procesos manuales y basados en papel. Los clientes con infraestructuras básicas perciben que sus entornos son verdaderamente difíciles de controlar, sus costos de gestión de desktops y servidores son muy elevados, habitualmente son muy reactivos con respecto a las amenazas contra la seguridad, y su capacidad de obtener resultados positivos de las inversiones realizadas en IT es más bien escasa. La instalación de parches y los despliegues de software y servicios se hacen habitualmente a mano y con costes muy elevados[6].

2.1.3.2 Estándar

Una infraestructura de IT en el nivel estándar ya dispone de controles por medio de la aplicación de estándares y políticas, lo que les permite gestionar los desktops, dispositivos móviles, servidores y normalizar la forma en que se incorporan nuevas máquinas a la red. Utilizan el servicio de Directorio Activo para gestionar recursos, políticas de seguridad y control de los accesos. Generalmente todos los parches, despliegue de aplicaciones y servicios

[6] http://www.microsoft.com/spain/iom/modelo/nivelesiom.aspx

para los desktops se realizan mediante procesos semiautomáticos con un costo medio o alto. No obstante, estos clientes disponen de un inventario razonablemente preciso de sus activos de hardware y software y empiezan a gestionar sus licencias y realizan pruebas de aplicaciones utilizando entornos virtualizados. Han adoptado medidas de seguridad y disponen de una red perimetral bloqueada, aunque la seguridad interna puede estar sometida a ciertos tipos de riesgos y amenazas.

2.1.3.3 Racionalizado

Una infraestructura racionalizada es aquella donde los costos de gestión de los desktops y servidores son mínimos y los procesos y políticas están optimizados de manera que pueden empezar a desempeñar una función muy importante en el buen funcionamiento y la expansión de la empresa. La seguridad se gestiona de manera muy proactiva y la respuesta ante las amenazas y ataques es rápida y controlada. El uso de técnicas de despliegue automatizado permite reducir los costes al mínimo, así como los tiempos y problemas de la operación.

Se dispone de un inventario preciso de hardware y software, y solamente adquieren las licencias y equipos que realmente necesitan. La gestión de documentos y registros dispone de soluciones de búsqueda consideradas como activo tecnológico estratégico para la empresa. La seguridad se refuerza con políticas estrictas y medidas de control que van desde los servidores hasta el último desktop, y a los firewalls e incluso la extranet. [7]

2.1.3.4 Dinámico

Los clientes que disfrutan de una infraestructura dinámica son plenamente conscientes del valor estratégico que dicha infraestructura tiene a la hora de desarrollar de manera eficiente sus actividades de negocio y mantener sus ventajas competitivas. Los costos están totalmente

[7] http://www.microsoft.com/spain/iom/modelo/nivelesiom.aspx

controlados, existe integración entre los usuarios y los datos, desktops y servidores. La virtualización se emplea para el acceso dinámico a las aplicaciones y para la restauración de aplicaciones de desktop. Los procesos están totalmente automatizados, a menudo incorporados a la propia tecnología, con lo que las IT se pueden alinear con las necesidades de negocio y gestionarse de acuerdo a ellas. Las nuevas inversiones en tecnología generan beneficios concretos, rápidos y tangibles para la empresa.

2.1.4 Metodología de Trabajo

El Modelo de Optimización de Infraestructuras es una herramienta para ayudar a establecer y organizar las prioridades de IT y planificar de forma eficaz el proceso durante un periodo de varios años. El uso correcto de la herramienta supone seguir una serie de etapas, con el apoyo de una evaluación interna más completa que debe realizar el equipo de IT[8].

La metodología utilizada para el Modelo de Optimización de Infraestructuras permite avanzar progresivamente hacia los máximos niveles de madurez considerados como adecuados para una empresa, una organización o un entorno concreto, y consta de tres fases fundamentales[9]:

2.1.4.1 Identificación del grado de madurez actual.

Consiste en perfilar mediante una encuesta las tecnologías, procesos y políticas que actualmente tienen en marcha en su infraestructura de desktop, datacenter y red.

[8] http://www.microsoft.com/spain/iom/modelo/metodologia.aspx

[9] http://www.microsoft.com/spain/iom/modelo/metodologia.aspx

2.1.4.2 Identificación del grado de madurez óptimo para esta infraestructura.

Mediante la tabulación de la encuesta se determina el nivel de madurez de la infraestructura con la cual cuenta la empresa, permitiendo así tener una situación inicial de la infraestructura

Esta tabulación permite la planificación de presupuestos, asignación de recursos y protección de las inversiones a corto, mediano y largo plazo.

2.1.4.3 Diseñar e implementar los proyectos de máximo impacto necesarios para progresar.

Teniendo los resultados de la encuesta se realiza los posibles diseños a implementar, es decir se realiza la planificación de los proyectos a implementar para llegar a un nivel dinámico.

2.1.5 Áreas de Optimización

2.1.5.1 Infraestructura Básica (CORE-IO)

El Modelo de Optimización de Infraestructuras Básicas (Core-IO) valora la madurez en las capacidades fundamentales que habilitan las tecnologías de información: gestión de la identidad y acceso a recursos de la red, gestión de servidores y desktops, protección de datos y seguridad y, en general, la gestión de sistemas[10].

[10] http://www.microsoft.com/spain/iom/modelo/infraestructuras.aspx

Figura 2.3 – Infraestructura Básica

Fuente: http://www.microsoft.com/spain/iom/modelo/infraestructuras.aspx

2.1.5.1.1 Gestión de la identidad y acceso a recursos de la red

Se refiere a cómo debe gestionarse la identidad de las personas y los equipos y cómo proteger los datos de identificación (sincronización, gestión de contraseñas) y cómo se gestionan los accesos a recursos por parte de usuarios móviles de la empresa, clientes fuera de los límites del firewall.

2.1.5.1.2 Gestión de servidores, desktops y dispositivos

Describe cómo deben gestionarse los equipos informáticos y cómo distribuir los parches, sistemas operativos y aplicaciones por la red.

2.1.5.1.3 Gestión de Redes y Seguridad

Son todos los aspectos a considerar a la hora de implementar la infraestructura de comunicaciones que soporta todas las tecnologías de información de la empresa, así como los mecanismos de protección de la propia infraestructura de IT frente a ataques externos o internos contra la seguridad, la privacidad o la integridad de la información, siempre con el objetivo de mantener en servicio el acceso a los recursos corporativos y un tráfico de datos fluido[11].

2.1.5.1.4 Protección y Restauración de Datos

Describe los procesos y herramientas utilizados para el buen uso de las copias de seguridad, almacenamiento y recuperación de datos. Conforme aumenta la cantidad de información disponible y los almacenes de datos, las organizaciones se ven cada vez más presionadas para proteger esta información y disponer de procesos de recuperación económicos y eficientes para situaciones de emergencia[12].

2.1.5.1.5 Gestión de procesos y políticas de IT

Consiste en una guía de buenas prácticas muy probadas para llevar a cabo el diseño, desarrollo, operación y soporte de soluciones que posibiliten altos niveles de fiabilidad, disponibilidad y seguridad[13].

[11] http://www.microsoft.com/spain/iom/modelo/redes.aspx

[12] http://www.microsoft.com/spain/iom/modelo/proteccion.aspx

[13] http://www.microsoft.com/spain/iom/modelo/procesos.aspx

2.1.5.2 Productividad Empresarial (BPIO)

El modelo IOM de productividad empresarial (BPIO, Business Productivity Infrastructure Optimization) es un conjunto completo de tecnologías que ayuda a mejorar la gestión y control de contenidos, datos y procesos a lo largo de una serie de áreas de la empresa.

Contribuye a simplificar el trabajo en equipo, hace que los procesos y la gestión de contenidos sean más eficientes y mejora la calidad de los análisis internos de negocio, aparte de aumentar la capacidad de respuesta de las tecnologías de información y posicionarse como activos estratégicos para la propia empresa.

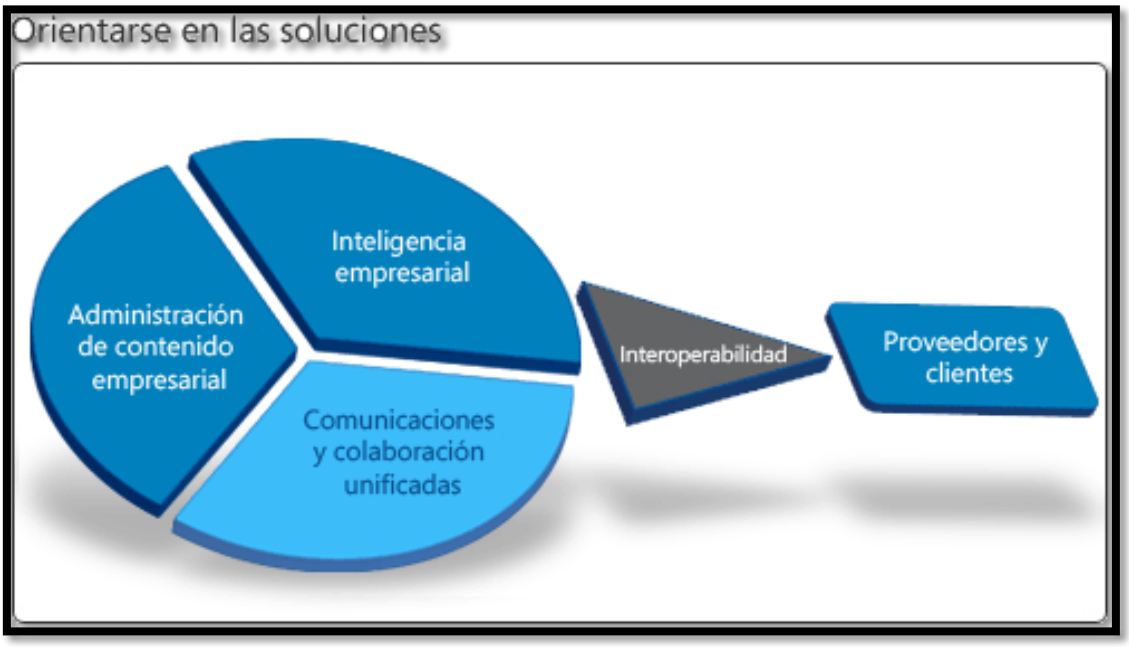


Figura 2.4 - Productividad Empresarial (BPIO)

Fuente: http://www.microsoft.com/spain/iom/modelo/colaboracion.aspx

2.1.5.2.1 Entorno de Colaboración y Trabajo en Equipo

Describe la forma en que los usuarios emplean los espacios de colaboración y portales para disponer un entorno de trabajo en equipo productivo, donde los departamentos de IT pueden definir procesos y soluciones normalizadas susceptibles de adaptación a las necesidades concretas de la empresa y se pueden ampliar para disponer de funcionalidades de red social, integración con aplicaciones de línea de negocio y federación de las identidades y relaciones con otras organizaciones[14].

2.1.5.2.2 Comunicaciones Unificadas

Describe un modelo de comunicación entre personas donde los datos estructurados y no estructurados convergen con otros tipos de comunicaciones, como la conversación de voz, control de presencia y multiconfererencia, y por ello esta capacidad establece un marco de referencia que los departamentos de IT pueden aprovechar para potenciar la infraestructura y ofrecer nuevos servicios (o mejores).

2.1.5.2.3 Gestión de contenidos corporativos

Describe todo lo se debe tener en cuenta a la hora de implementar soluciones de generación de contenidos web, formularios electrónicos, publicación de documentos, gestión de los contenidos y registro de auditoría para optimizar la labor de gestión de contenidos y los procesos vinculados. Las soluciones de administración del contenido corporativo ayudan a proteger y administrar grandes cantidades de información y contenidos en formatos diversos, de manera que se puedan usar como activos estratégicos para impulsar el crecimiento general de la empresa.

[14] http://www.microsoft.com/spain/iom/modelo/colaboracion.aspx

2.1.5.2.4 Procesos de Búsqueda

Describe cómo tiene que integrarse esta información con las funcionalidades normales de búsqueda que integran distintos formatos, orígenes de datos y aplicaciones de línea de negocio desde una infraestructura centralizada y homogénea que aproveche y saque el máximo rendimiento de una familia de soluciones estándar de productividad empresarial.

2.1.5.2.5 Business Intelligence

Permite definir procesos normalizados para la generación de informes, análisis y transformación de datos con los cuales la información puede exponerse y quedar al alcance de los usuarios mediante una interfaz avanzada (por ejemplo sus aplicaciones de ofimática).

2.1.5.3 Plataforma de Aplicaciones (APIO)

La Plataforma de Aplicación hace posible que las tecnologías de información se conviertan en factores de progreso para las empresas, mediante aplicaciones conectadas, flexibles y muy seguras. Con el modelo de optimización de la plataforma de aplicación se puede ofrecer a las organizaciones de IT un marco de referencia que les permite definir mejor y adoptar una plataforma de aplicaciones más flexible y ágil[15].

2.1.5.3.1 Experiencia de Usuario

Son todos los parámetros de interacción del usuario final con el sistema de información, y por tanto también engloba otros conceptos que, como sucede con el hardware, estabilidad de la red, exceden claramente del ámbito de la Plataforma de Aplicaciones, pero que indudablemente la afectan.

[15] http://www.microsoft.com/spain/iom/modelo/plataforma.aspx

2.1.5.3.2 Desarrollo de Aplicaciones

Orienta las necesidades de los responsables de tecnología (ITDM) y desarrolladores para la producción rápida de aplicaciones de alta calidad y seguridad que interconectan los procesos de negocio a fin de resolver las necesidades de la empresa. Una Plataforma de Aplicación dinámica debe cubrir todo el ciclo de vida de desarrollo de software, mejora el trabajo en equipo y la productividad, y permite obtener un código de mayor calidad[16].

2.1.5.3.3 Arquitectura Orientada a Servicios (SOA) y Procesos de negocio (BP)

Integra sistemas heterogéneos (EAI, Enterprise Application Integration) y también entre organizaciones diferentes (B2B). También permite gestionar procesos (BPM, Business Process Management) que afectan a personas de la propia organización, servicios de software.

2.1.5.3.4 Gestión de datos

Describe las ventajas de disponer de software integrado de gestión de datos y análisis que permita administrar de manera fiable y eficiente la información de misión crítica para las aplicaciones de negocio actual, cada vez más compleja[17].

[16] http://www.microsoft.com/spain/iom/modelo/aplicaciones.aspx

[17] http://www.microsoft.com/spain/iom/modelo/datos.aspx

2.2 METODOLOGÍA MSF

2.2.1 Introducción

Figura 2.5 - Fases de la metodología MSF
Fuente: www.microsoft.com/spanish/MSDN/estudiantes/ingsoft/planificacion/msf.mspx

MSF es una metodología desarrollada por Microsoft para un manejo optimo de los proyectos de tecnología, gracias al buen planteamiento de este modelo es posible utilizarlo para cualquier proyecto de tecnología de información (IT).

MSF es flexible e interrelaciona una serie de conceptos, modelos y prácticas de uso que controlan la planificación, el desarrollo y la gestión de proyectos tecnológicos[18].

Los componentes de MSF se pueden aplicar individualmente o en grupo para poder culminar con éxito los siguientes tipos de proyectos:

- Proyectos de desarrollo de programas, incluyendo móviles, aplicaciones WEB, servicios WEB, sistemas distribuidos, etc.

[18] http://www.microsoft.com/spanish/MSDN/estudiantes/ingsoft/planificacion/msf.mspx

- Proyectos de infraestructura, incluyendo implementaciones de escritorio, actualización de sistemas operativos, implementación de mensajería, y configuración y operación de sistemas.
- Proyectos de integración paquetes de aplicación, incluyendo productividad personal, ERP, y manejo de EPM.
- Y combinaciones de cualquiera de los proyectos mencionados anteriormente.

El modelo MSF se divide en 5 fases:

1. Visión
2. Planeación
3. Desarrollo
4. Estabilización
5. Implementación

2.2.1.1 Visión

En esta fase se pretende tener la visión general del proyecto, se identifican las tareas y los entregables que permiten al equipo cumplir con los objetivos y requerimientos del proyecto.

2.2.1.2 Planeación

En esta fase se realiza la preparación de la especificación funcional, diseño de la solución, planes de trabajo, costos estimados y calendarios para los entregables. Implica la recogida y el análisis de los requerimientos de negocio, de usuario, operaciones y sistema.

2.2.1.3 Desarrollo

La meta de esta fase es la construcción de los elementos y entregables de la solución, incluidos los códigos de los componentes, infraestructura (software, hardware, red) y la documentación para el uso de las operaciones.

2.2.1.4 Estabilización

Se determina si la solución cumple los criterios necesarios para pasar a la fase de implementación. Se reproduce las condiciones reales y el equipo se concentra en detectar y priorizar errores, preparando la solución para su implementación.

2.2.1.5 Implementación o Distribución

Es la parte final de la metodología, en la cual se instalan los componentes, se estabiliza el proyecto y se obtiene la aprobación por parte del cliente.

2.2.2 Modelo de Equipo

El modelo de Equipo describe la estructura de personas y sus actividades para que se cumpla el proyecto. El modelo define los roles, áreas funcionales, responsabilidades, y la orientación para los miembros del equipo para que se cumplan en el ciclo de vida del proyecto.

Los equipos bajo el modelo MSF son pequeños y multidisciplinarios, donde cada uno de los miembros comparte las responsabilidades y se balancea la carga de los miembros del equipo para cumplir los objetivos del proyecto.

Figura 2.6 - Modelo de Equipo
Fuente: http://www.ciinsrl.com/imagenes/equipo_trabajo3.gif

El modelo de equipo describe 6 tipos de roles que cumplen diferentes actividades los cuales se podrán ver en el anexo 1, que describe a detalle los 6 roles del modelo de equipo.

2.2.3 Modelo de Proceso

El modelo de procesos de MSF describe el nivel de secuencia de las actividades y la construcción de soluciones IT, establece el orden de las actividades del proyecto El origen de MSF se da con el proceso que utiliza Microsoft para el desarrollo de aplicaciones. El modelo MSF es utilizado principalmente para el desarrollo de aplicaciones. Este modelo combina 2 modelos de procesos: Modelo de Cascada y Modelo Espiral.

Entre los principales beneficios de este modelo tenemos las siguientes:

- Acelerar la producción ordenada de entregables del proyecto
- Tener soluciones alineadas con los objetivos del negocio
- Aumentar la predictibilidad y visibilidad.
- Proporcionar una transición en fases a producción

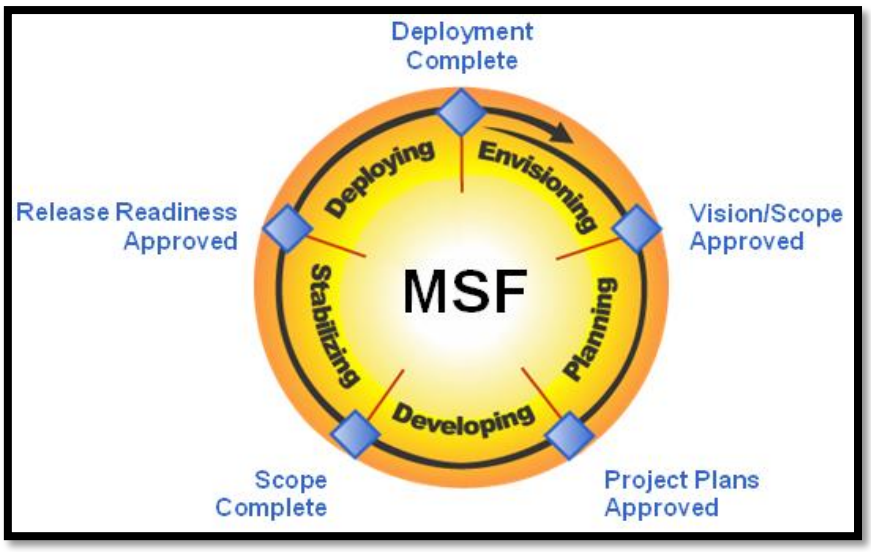


Figura 2.7 - Fases del modelo de Procesos
Fuente: http://www.jrmsoftware.com/images/msf-process-model.gif

El modelo MSF nos permite como tal realizar entregables versionados, es decir diferentes versiones de los entregables, las ventajas de poder realizar entregables versionados son las siguientes:

- Gestionar la incertidumbre y cambios de alcance
- Apoyar mejoras continuas e incrementables
- Permitir tiempos de entrega cortos
- Grupo de metas claras y que permitan motivar a los miembros del equipo
- Forzar a la clausura de los asuntos del proyecto

2.2.3.1 Modelo de Cascada

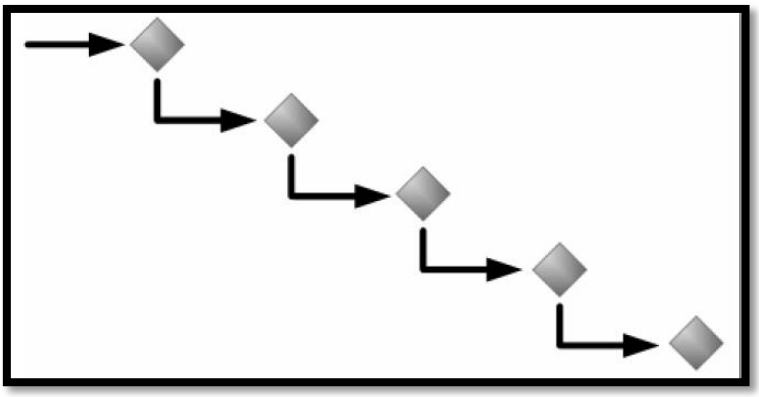


Figura 2.8 - Modelo de Cascada
Fuente: MSF Process Model v. 3.1, Getchell, Scott

En el modelo de cascada las tareas tienen que estar completadas antes de empezar una nueva tarea. Este modelo es ideal para proyectos que se encuentran bien definidos ya que este modelo se tarda mucho tiempo en pasar por todo su ciclo. Adicionalmente este modelo utiliza un punto de control para pasar a la siguiente fase.

2.2.3.2 Modelo de Espiral

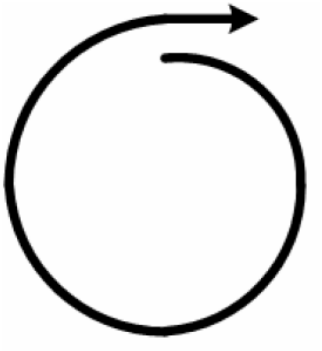


Figura 2.9 - Modelo de Espiral
Fuente: MSF Process Model v. 3.1, Getchell, Scott

Este modelo se creó con la necesidad continua de refinar los requerimientos y estimaciones del proyecto. Este modelo es efectivo para proyectos pequeños donde con la retroalimentación dada por el cliente, se aprueba en las diferentes etapas.

2.2.4 Fases del Modelo

Figura 2.10 - Fases del Modelo MSF
Fuente: http://www.pymeactual.com/desarrollo-web/imgs/msf-modelo-proceso.gif

El modelo MSF consta de 5 fases las cuales se alinean perfectamente para la elaboración de cualquier proyecto de IT. Estas fases son:

- Visión
- Planeación
- Desarrollo
- Estabilización
- Implementación

2.2.4.1 Visión

Es en esta fase en donde inicia el proceso de MSF. El objetivo final de esta fase es crear una visión compartida por todos los participantes del proyecto. En esta fase debemos definir de

manera amplia y general las metas y descripciones del proyecto; es en esta fase donde identificamos el equipo que gestionará la solución y sobre todo que es lo que este equipo debe de alcanzar para el cliente.

En esta fase se crea los objetivos del proyecto, de igual manera interviene la planificación de tiempos del proyecto. En esta fase se crea el documento de Visión y Alcance donde se estipulan como Visionamiento es una vista de lo que se quiere llegar a tener, y en el Alcance se identifican las limitaciones que se pueden suceder para llegar a la visión del proyecto.

Los entregables de esta fase son:

- Documento de Visión / Alcance
- Documento de evaluación de riegos
- Documento de la estructura del proyecto

Los roles que intervienen en esta fase son:

Rol	Enfoque
Product Management	Identificar las necesidades del cliente Requerimientos Documento de vision y alcance
Program Management	Diseñar objetivos Concepto de la solución Estructura del proyecto
Development	Prototipos Opciones de desarrollo y tecnologias Análisis de Factibilidad
User Experience	Necesidades de rendimiento y repercuciones
Testing	Estrategias de pruebas Criterios de aceptación de pruebas implicaciones
Release Management	Implicaciones de implementación Operaciones de manejo y soporte Aceptación de criterios de operación

Tabla 2.1 - Roles de la Fase de Visionamiento

2.2.4.2 Planeación

En esta fase se plantean preguntas ¿Para cuándo está listo el proyecto? Y ¿Cuánto va hacer el costo de la solución?, las cuales se tienen que definir con el cliente siempre y cuando se encuentren definidos la visión y alcance del proyecto.

En esta fase el equipo determina que se va a implementar o desarrollar y planea como crear la solución, el equipo debe preparar la especificación funcional, crear y diseñar la solución, estimar costos y cronogramas para las entregas.

En esta fase se hace el análisis de los requerimientos, estos requerimientos serán usados para diseñar la solución y validar el diseño.

El equipo debe desarrollar escenarios de uso y perfiles de usuario, aquí se deben crear los casos de uso para los distintos escenarios.

Los entregables de esta fase son:

- Especificación funcional
- Plan de la evaluación de riesgos
- Plan maestro del proyecto y cronograma maestro del proyecto

Los roles que intervienes en esta fase son:

Rol	Enfoque
Product Management	Diseño Conceptual Analisis de los requerimientos del negocio Plan de comunicaciones
Program Management	Diseño lógico y conceptual Especificaciones funcionales Plan maestro y cronograma maestro del proyecto
Development	Evaluación tecnológica Diseño lógico y físico Plan y cronograma de implementación Estimaciones de implementación
User Experience	Casos de uso Requerimientos de usuario Requerimientos de localización y accesibilidad Documentación de usuario Plan de entrenamiento Documentación de usuario Capacitación
Testing	Diseño de pruebas Requerimientos de Pruebas Cronogramas de pruebas
Release Management	Diseño de evaluación Requerimientos de Operación Cronograma para piloto e implementación

Tabla 2.2 - Roles de la Fase de Planificación

2.2.4.3 Desarrollo

Lo primero es que es la fase en la que construimos la solución propuesta. Algo importante es que en esta fase se desarrolla la infraestructura de la solución. En esta fase vamos a concretar las versiones que planificamos.

Los entregables de esta fase son:

- Pasos de instalación y configuración
- Especificación funcional
- Elementos de soporte
- Especificaciones de pruebas y casos de pruebas

Los roles de esta fase son:

Rol	Enfoque
Product Management	Espectativas del Cliente
Program Management	Manejo de espectativas funcionales Seguimiento del proyecto Plan de actualizaciones
Development	Desarrollo de la infraestructura Documentación de configuración
User Experience	Capacitación Plan de actualización de capacitación Pruebas de uso Diseño Gráfico
Testing	Pruebas de funcionalidad Identificación de problemas Documentación de pruebas Plan de actualización de pruebas
Release Management	Lista de despliegue Plan piloto y plan de despliegue Lista de preparación

Tabla 2.3 - Roles de Fase de Desarrollo

2.2.4.4 Estabilización

En la fase de estabilización el equipo optimiza la infraestructura y las pruebas en la solución. Las pruebas en esta fase hacen énfasis en el uso y operación de la solución en un ambiente de condiciones reales.

Hay que enfocarse en identificar, priorizar y resolver problemas, para que la solución pueda ser preparada para ser implementada. En esta fase existen estados de “alpha” y “beta” que describen es estado de la solución IT.

Los entregables de esta fase son:

- Versión final de la solución
- Notas

- Elementos para el soporte
- Resultados de las pruebas y herramientas usadas para las pruebas
- Documentos del proyecto
- Revisión de Hitos

Los roles de esta fase son:

Rol	Enfoque
Product Management	Ejecución del plan de comunicación Plan de implementación
Program Management	Seguimiento del proyecto Plan de actualizaciones
Development	Optimización de la infraestructura
User Experience	Estabilización de los materiales del usuario Material de capacitación
Testing	Pruebas Reporte de estatus Pruebas de configuración
Release Management	Piloto de implementación y soporte Plan de implementación Capacitación de operación y soporte

Tabla 2.4 - Roles de Fase de Estabilización

2.2.4.5 Implementación

Durante la fase de Implementación se lleva a cabo la implementación, estabilización transición de las operaciones y soporte de la solución, y se obtiene la aprobación final del cliente.

Actividades de estabilización se continúan durante esta fase realizando pruebas en producción.

Los entregables de esta fase son:

- Información de soporte y operación
- Procedimientos y procesos
- Bases de conocimiento, reportes

- Repositorios de documentación incluyendo todas las versiones
- Reporte de cierre del documento
- Versión final de todos los documentos del proyecto
- Datos de satisfacción del cliente
- Definición de los siguientes pasos

Los roles de esta fase son:

Rol	Enfoque
Product Management	Seguimiento del cliente
Program Management	Comparación de la solución con el alcance Manejo de la estabilización
Development	Resolución de problemas Escalación de soporte
User Experience	Capacitación Manejo del cronograma de capacitación
Testing	Pruebas de rendimiento Problemas
Release Management	Cambiar aprobación

Tabla 2.5 - Roles de Fase de Implementación

2.2.5 Estructura del documento

La estructura de un documento MSF se detalla en el anexo 2 del presente documento.

2.3 DEFINICIÓN DE SERVICIOS

2.3.1 Servidor

2.3.1.1 Directorio Activo

El servicio de directorio es una herramienta que conecta directorios a través de la red actúa como un gran libro de teléfonos. Usando entradas generales (p.e. donde están las impresoras), un usuario puede recibir los recursos de las listas de impresoras. Todas las versiones de Windows Server 2003 a acepción de Windows Server 2003, Web Edition, incluyen Directorio Activo como servicio de directorio.

Directorio Activo combina estándares X.500, DNS, LDAP. Directorio Activo permite un punto para la administración de recursos, incluyendo usuarios, archivos, periféricos, conexiones a la computadora, base de datos, acceso web, servicios y recursos de red.

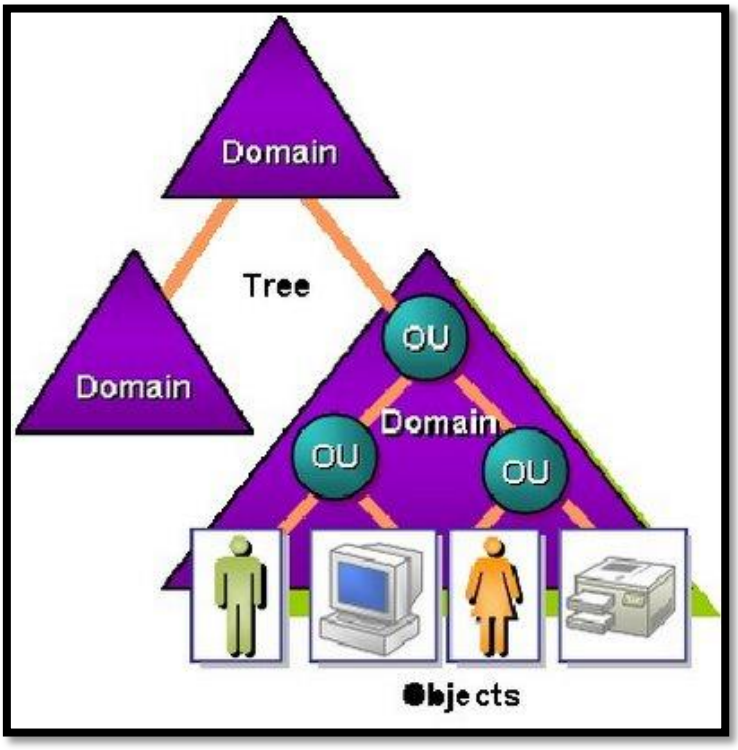


Figura 2.11 - Esquema Directorio Activo

Fuente: http://jeilg.blogspot.com/2008/07/directorio-activo.html

LDAP: Es un protocolo que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red, es un protocolo de acceso unificado a un conjunto de información sobre una red. También es considerado una base de datos a la que pueden realizarse consultas[19].

DNS: Es un servicio el cual nos permite ser identificados dentro de la red mediante nombres, es decir convierte las direcciones IP en nombres para facilitar la búsqueda de alguna computadora o periférico dentro de la red.

X.500: Es un estándar para servicios de directorio establecido por ITU (International Telecommunications Union). La ISO/IEC publico el mismo estándar. X.500 define el modelo de información usada en los servicios de directorio.

2.3.1.1.1 Estructura Lógica

La estructura lógica del Directorio Activo se centra en la administración de los recursos de red, independiente de la ubicación física de dichos recursos. La estructura lógica de la organización se basa en el concepto de dominio, que internamente tiene información sobre los recursos (usuarios, grupos, directivas, etc.) para los ordenadores que forman parte de dicho dominio. Dentro de un dominio es posible subdividir lógicamente el directorio mediante el uso de unidades organizativas, que permiten una administración independiente sin la necesidad de crear múltiples dominios.

La unidad central de Directorio Activo es el dominio que no es más que un conjunto de equipos que comparten una base de datos de directorio en común. Dentro de una organización pueden existir desde uno hasta varios dominios, los cuales deben estar controlados por un Directorio Activo.

[19] http://jeilg.blogspot.com/2008/07/directorio-activo.html

Cuando existen dos o más dominios dentro de una misma organización se debe crear relaciones de confianza que son relaciones establecidas entre dos dominios de forma que permite a los usuarios de un dominio ser reconocidos por otro controlador de dominio.

Adicionalmente, podemos organizar nuestros recursos en unidades organizativas que es un objeto del Directorio Activo que puede contener recursos del Controlador de Dominio.

2.3.1.2 DNS

DNS (Domain Name Service) es un servicio de Internet y del Protocolo de control de transmisión/protocolo Internet (TCP/IP, Transmission Control Protocol/Internet Protocol) que relaciona los números de las direcciones de red, por ejemplo 191.31.140.115, con un nombre fácil de recordar, como tbones.acme.com. Utilidades Internet y TCP/IP, entre las que se incluyen *telnet*, el Protocolo de transferencia de archivos (FTP, File Transfer Protocol) y el Protocolo básico de transferencia de correo (SMTP, Simple Mail Transfer Protocol) acceden a DNS para localizar los nombres específicos y convertirlos a direcciones de red. Cuando se selecciona un nombre, DNS traduce ese nombre a una dirección numérica y lo inserta en un mensaje para transportarlo. Una utilidad importante de DNS es que la información de dirección se almacena en muchos emplazamientos en una estructura jerárquica, no en un almacén central. Cada zona tiene un servidor de nombres de dominios que mantiene información sobre los nodos locales.

Los dominios y DNS se introdujeron en Internet cuando ésta creció. La estructura es un árbol jerárquico con subárboles que se ramifican, como se muestra en la figura 2 y que ilustra parte de Internet. Puede considerarse este árbol de la misma forma que se consideraba un sistema de clasificación jerárquico en el cual los directorios contienen otros subdirectorios. Existe un *nivel superior* en el árbol, a veces llamado *nivel raíz*, que se fragmenta en divisiones importantes, denominadas *dominios*. Aquí se enumeran algunos de los dominios Internet de nivel superior.

GOV = Agencias del gobierno

EDU = Instituciones Educativas

ORG = Organizaciones (no lucrativas o no comerciales)

COM = Comercial

MIL = Militar

NET = Proveedores de servicios de red

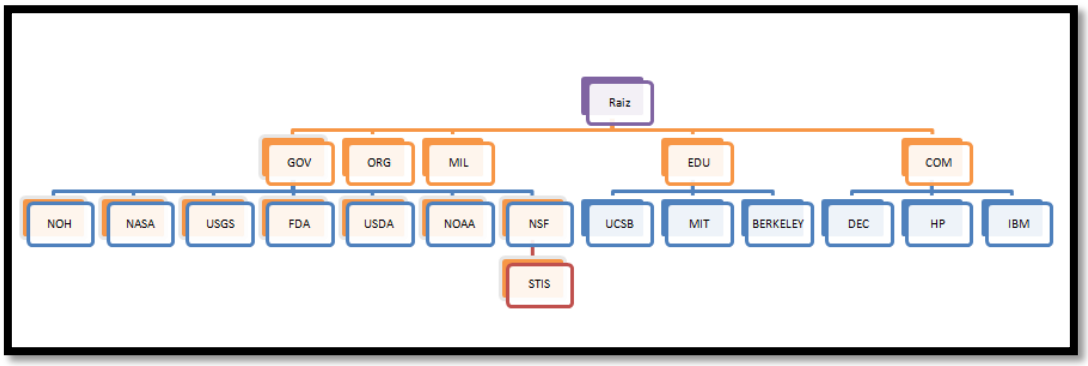


Figura 2.12 – Estructura Jerárquica de Internet
Fuente: Sheldon, Tom. LAN TIMES Enciclopedia de redes Networking

Hay dominios nacionales, como CA (Canadá), UK (Gran Bretaña), JP (Japón), EC (Ecuador). En el dominio US (Estados Unidos), se utilizan códigos formados por dos letras para cada unos de los 50 estados. Las compañías y organizaciones limitadas a un país usan estos dominios, mientras que una compañía internacional usaría el dominio COM.

2.3.1.2.1 Establecimiento de DNS

Para unirse a un dominio, se debe contactar con la organización que lo gestiona. Cada zona debe ofrecer un servidor de nombres que contenga la información DNS de otras computadoras de la red pueden consultar. También se puede acceder a uno de los muchos suministradores comerciales de servicios de internet para ejecutar un servidor de nombres. Entonces tendrán que proporcionar las conexiones a los usuarios de su dominio hacia el suministrador del servicio.

Cuando se escriben los nombres DNS, se sitúa el nombre del anfitrión (*host*) a la izquierda, seguido de los nombres de dominio raíz.

2.3.1.2.2 Ejecución de Servidores DNS locales

La estructura de nombres internos de una organización puede seguir el mismo modelo, pero incluye dominios de divisiones o departamentos. Se asignan una o más computadoras para gestionar los nombres de DNS. DNS es una base de datos distribuida que puede residir en varios servidores distintos para protegerla contra los servidores que han fallado. Hay servidores DNS primarios y secundarios.

- *Servidor DNS primario.* Es el servidor principal que mantiene una copia de la base de datos completa tanto en memoria como en disco. Si el sistema se viene abajo, la base de datos se recarga en memoria.
- *Servidor DNS secundario.* El servidor DNS secundario obtiene una copia de la base de datos desde el servidor primario. Cuando se producen cambios, es necesario una actualización desde el servidor primario.

Hay diversas ventajas en distribuir las bases de datos de esta forma. Los usuarios pueden buscar recursos y otros usuarios consultando la copia local de la base de datos. La distribución de la base de datos también proporciona tolerancia a fallos; no obstante, cada servidor de la base de datos debe tener su propia fuente de alimentación e idealmente situarse en áreas que no sufran desastres, entre los que se incluyen incendios, inundaciones o terremotos.

2.3.1.3 DHCP

La función del protocolo de configuración dinámica de sistema (DHCP, *Dynamic Host Configuration Protocol*) consiste en obtener una dirección IP en nombre del computador. El administrador de la red es el responsable de asignar las direcciones IP a los computadores conectados a la red y reasignar estas direcciones cuando se eliminan dichos computadores. De esto puede deducirse que la asignación, instalación y administración de direcciones IP puede suponer un esfuerzo considerable. Para reducir esta carga de trabajo, existe la posibilidad de autoconfiguración que permite a un computador obtener una dirección IP a través de la red y,

en el caso de equipos portátiles, puede hacer uso de esta dirección durante el tiempo que dura la sesión de trabajo.

Consiste en que el computador se comunica con un servidor de direcciones IP de la organización o empresa mediante un protocolo de aplicación denominado DHCP.

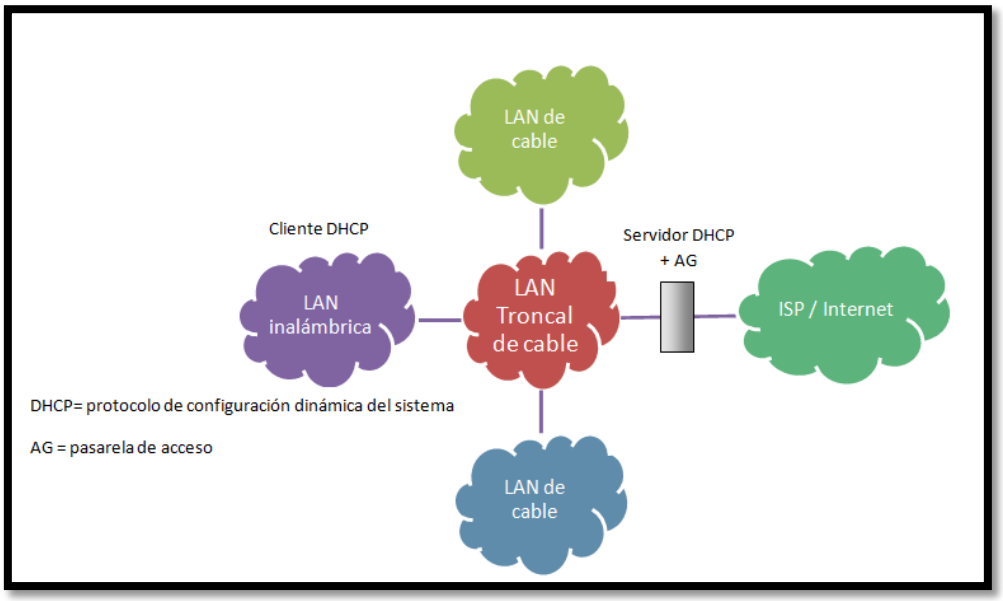


Figura 2.13 – Ejemplo de Topología de red con DHCP
Fuente: Halsall, Fred. Redes de Computadoras e Internet

En la figura 2.13, se supone que una persona conecta su computador portátil y quiere comunicarse a través de Internet para leer el correo electrónico desde la red de su domicilio. Se supone que la red soporta la autoconfiguración por medio de un servidor que ejecuta DHCP como una de sus aplicaciones.

La figura 2.14 muestra un diagrama de la secuencia de mensajes que se intercambian en relación con DHCP.

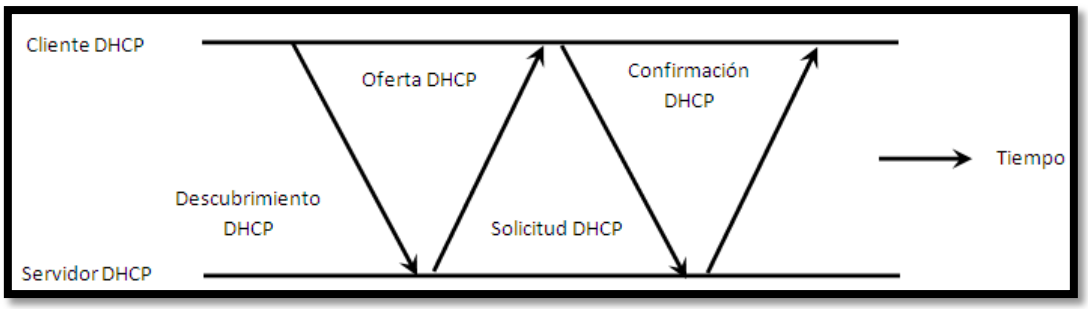


Figura 2.14 – Diagrama de secuencia de mensajes

Fuente: Halsall, Fred. Redes de Computadoras e Internet

DHCP es un simple protocolo cliente-servidor. A continuación se describen brevemente los mensajes de este protocolo.

- **Descubrimiento DHCP.** El mensaje contiene un **identificador de transacción,** de manera que el cliente puede relacionar la respuesta del servidor con su solicitud.
- **Oferta DHCP.** Este mensaje lo devuelve el servidor DHCP y contiene el mismo identificador de transacción que le mensaje de descubrimiento, la dirección IP propuesta para el cliente, la máscara de red IP y un valor de duración que indica el tiempo de validez de la dirección IP.
- **Solicitud DHCP.** Este mensaje se envía como respuesta al mensaje de oferta anterior y contiene los mismos parámetros que el mensaje de oferta DHCP.
- **Confirmación DHCP.** Este mensaje lo devuelve el servidor y contiene el mismo conjunto de parámetros, de manera que confirma la recepción de éstos por el cliente.

2.3.2 Actualizaciones del sistema operativo centralizadas

La gestión de actualizaciones es una importante función dentro del mantenimiento de cualquier sistema informático, desde un PC individual a un centro de datos corporativo. La capacidad de identificar qué actualizaciones existen y distribuirlas en el momento adecuado de forma automática permite mantener la seguridad y la productividad de los usuarios en la organización.

Microsoft ofrece tres niveles de productos de gestión de actualizaciones orientados a cubrir las necesidades de los usuarios individuales, empresas pequeñas y medianas, y grandes organizaciones.

2.3.2.1 Comparación entre Windows Update, Windows Server Update Services, y SMS

Para ver las comparaciones entre estos tres aplicativos referirse al anexo 3.

2.3.3 Seguridades

En los entornos corporativos de informática distribuida, la seguridad se ha convertido en una cuestión cada vez más importante. Los recursos de datos ya no se centralizan en un solo lugar, en el cual los mecanismos de seguridad, tanto físicos como a través de software, los podrían proteger frente al acceso no autorizado. La falta de una gestión centralizada de los datos hace que éstos sean más vulnerables a:

- La supervisión no autorizada de las transmisiones de datos
- La modificación de la información
- La suplantación de un usuario por otro no autorizado
- La repudiación, que consiste en que el emisor de un mensaje niega haberlo enviado.

Para garantizar la confidencialidad de la información se utilizan las técnicas de cifrado de claves. Una clave es un algoritmo software o un dispositivo hardware que codifica y bloquea el acceso a la información.

Existen diferentes técnicas cuya finalidad es proporcionar seguridad en entornos de informática distribuida, tales como:

- ***Servicios de autenticación.*** Estos servicios se encargan de identificar a los usuarios que inician sesiones en las redes y sirven como prueba de su autenticidad para el resto de los dispositivos de red.
- ***Servicios de autorización.*** Estos servicios proporcionan a los usuarios previamente autentificados el acceso a la red de acuerdo con los derechos de acceso según corresponda.
- ***Servicios de confidencialidad.*** Estos servicios se encargan de ocultar los datos frente a accesos no autorizados y de asegurar que la información transmitida entre el emisor y el receptor no ha sido interceptada.
- ***Servicio de integridad.*** Estos servicios sirven para garantizar que los mensajes son auténticos y no se han alterado.
- ***No repudiación.*** Estos servicios pueden servir como prueba de que un mensaje ha sido enviado por un emisor específico y así evitar que éste pueda ocultar quien es el propietario del mensaje.

Para poder tener seguridades en la red a implementar se va a utilizar el sistema ISA Server, el cual es un Gateway integrado de seguridad perimetral que protege el entorno de IT frente a amenazas basadas en internet y permite a los usuarios un acceso remoto rápido y seguro a las aplicaciones y los datos.

Los requisitos para la implementación de ISA Server son:

	PC con procesador Pentium III a 733 MHz o superior
Sistema Operativo	Microsoft Windows Server 2003 con Service Pack 1 (SP1) o Microsoft Windows Server 2003 R2
	Se recomienda 512 MB de RAM o más
Disco Duro	Partición en disco duro local con formato NTFS con 150 MB de espacio de disco disponible; puede necesitarse más espacio para cache web

	Adaptador de red para la conexión a la red interna. Otro adaptador de red adicional, modem o adaptador RDSI para cada una de las redes a las que se conecta el equipo. Otra tarjeta de red adicional para comunicaciones internas se el servidor pertenece a un array con balanceo de carga (NLB) de ISA Server 2006 Enterprise Edition.

Tabla 2.6: Requerimientos para la instalación de ISA Server

2.3.4 Servidor de correo

Cada vez son más los negocios que reconocen la enorme importancia de los sistemas de mensajería. Por esto, las distintas compañías fijan estrictos requisitos de disponibilidad y confiabilidad para los sistemas de correo electrónico. Igualmente importante es la fuerte demanda de nuevas características en los sistemas de mensajería; y es que la cada vez más obligada movilidad en el trabajo y la dispersión geográfica de los negocios indican que los requisitos del usuario están en constante evolución. Todos estos factores suponen una demanda tanto para los administradores de tecnologías de la información como para los arquitectos de sistemas, que se ven obligados a diseñar sistemas de mensajería de gran confiabilidad y disponibilidad constante para cubrir las necesidades de los usuarios.

Para llevar a cabo este punto se va a implementar Exchange Server 2007, ya que podemos encontrar las siguientes características:

- En Exchange Server 2007, la funcionalidad que ofrecen los servidores de Exchange se ha dividido en cinco funciones del servidor diferentes.
- Las funciones del servidor de Exchange Server 2007 son una agrupación lógicas de características y componentes que realizan una función concreta en el entorno de mensajería[20].

A continuación se muestra una lista de las funciones del servidor de Exchange Server 2007:

[20] Curso 5967A: Introducción a la instalación y administración de Microsoft Exchange Server 2007

- **Función del Servidor Concentrador de transporte**

Esta función es responsable del enrutamiento de los mensajes. El servidor concentrador de transporte realiza la categorización y el enrutamiento de los mensajes, y controla todos los mensajes que atraviesan una organización.

- **Función del Servidor Buzón**

Es responsable de administrar las bases de datos de buzones y de carpetas públicas. Los servidores de buzón contienen grupos de almacenamiento y almacenes, y admiten clústeres para lograr mayor confiabilidad y alta disponibilidad.

- **Función del servidor de Transporte perimetral**

Está diseñada como servidor de puerta de enlace del Protocolo simple de transferencia de correo (SMTP) entre su organización e Internet. Para garantizar la seguridad, el equipo que ejecuta la función del servidor de Transporte perimetral debe implementarse en una red perimetral y no debe ser miembro de su bosque de Active Directory.

- **Función del servidor Acceso de cliente**

Permite conexiones desde diversos protocolos cliente a los buzones de Exchange Server. Debe asignar al menos un servidor de Acceso de cliente en cada sitio de Active Directory que contenga un servidor Buzón.

- **Función del servidor Mensajería Unificada**

Proporciona la base de los servicios que integran mensajes de voz y de fax en la infraestructura de mensajería de su organización. Esta función requiere la presencia de tres funciones del servidor: Concentrador de Transporte. Acceso de cliente y Buzón. El servidor de mensajería unificada brinda acceso a mensajes de voz y faxes.

Exchange Server 2007 está disponible en dos versiones: Estándar y Enterprise. La edición Estándar está diseñada para satisfacerlas necesidades de mensajería y colaboración de pequeñas y medianas empresas. La edición Enterprise va dirigida a grandes corporaciones empresariales y permite la creación de varios grupos de almacenamiento y base de datos.

Característica	Edición Estándar	Edición Enterprise
Compatibilidad con grupos de almacenamiento	Cinco grupos de almacenamiento	50 grupos de almacenamiento
Compatibilidad con bases de datos	Cinco base de datos	50 bases de datos
Límite de almacenamiento de base de datos	Sin límite de almacenamiento de software; el límite de almacenamiento depende del hardware	Sin límite de almacenamiento de software; el límite de almacenamiento depende del hardware.
Clústeres de copia única	No compatible	Compatible
Replicación continua local	Compatible	Compatible
Replicación continua en clúster	No compatible	Compatible

Tabla 2.7: Características de cada Edición de Exchange 2007

2.3.4.1 Requisitos de infraestructura para implementar Exchange Server 2007

2.3.4.1.1 Requisitos de Active Directory

- El controlador de dominio maestro debe tener instalado Windows Server 2003 (SP1).
- Debe tener al menos un servidor de catálogo global en cada sitio del servicio de directorio Active Directory donde se piense instalar Exchange Server 2007.

2.3.4.1.2 Otros requisitos

- DNS debe estar configurado correctamente en el bosque de Directorio Activo.
- El firewall debe estar correctamente configurado antes de instalar Exchange Server.
- Se debe asignar suficiente espacio de disco duro para las bases de datos

2.3.4.1.3 Requisitos de Hardware

Recurso	Requisito
Procesador	Un equipo basado en arquitectura x64 con un procesador Pentium o Xeon con la tecnología memoria extendida 64 de Intel, o de la familia AMD Opteron o AMD Athlon 64
Memoria	Mínimo de 1 GB de memoria del sistema
Disco	1,2 GB de espacio de disco para los archivos de Exchange Server y 200 MB de espacio de disco libre en la unidad del sistema
Sistema de archivos	Unidades formateadas con NTFS para todos los volúmenes relacionados con Exchange Server

Tabla 2.8: Requisitos de Hardware para la instalación

2.3.5 Comunicaciones Unificadas

2.3.5.1 Introducción

El término **Comunicaciones Unificadas** es utilizado comúnmente por los proveedores de tecnologías de la información para designar la integración de "los servicios de telefonía, mensajería unificada (la misma bandeja de entrada para correo electrónico, correo de voz y fax), mensajería instantánea corporativa, conferencias web y estado de disponibilidad del usuario en una sola e innovadora experiencia para los colaboradores y para el personal que administra y da mantenimiento a la infraestructura".

Las tecnologías Microsoft Comunicaciones Unificadas ofrecen a los usuarios alternativas para que las comunicaciones y software de colaboración mejoren la entrega, administración y mantenimiento, uniendo su comunicación existente y herramientas (Internet, Faxes, Voice Mail, E-mail, Mensajeria Instantanea) permitiendo así la integración de los diferentes sistemas usando servidores integrados más aplicaciones y servicios para el cliente (Exchange Server 2007, Microsoft Outlook 2007, Microsoft Office Communications Server 2007).

Figura 2.15 – Descripción de Comunicaciones Unificadas
Fuente: http://www.microsoft.com/latam/uc/what.aspx

El mundo de las comunicaciones está dividido en 2, tareas que usted hace por teléfono y las cosas que hace en la computadora.

La división existe porque la mayoría de las comunicaciones (sincrónicas) en tiempo real, como las llamadas telefónicas y el correo de voz, dependen de una red, mientras que las comunicaciones (asincrónicas) basadas en mensajes, como el correo electrónico, dependen de una red diferente que es incompatible.

La división existe porque la mayoría de las comunicaciones (sincrónicas) en tiempo real, como las llamadas telefónicas y el correo de voz, dependen de una red, mientras que las comunicaciones (asincrónicas) basadas en mensajes, como el correo electrónico, dependen de una red diferente que es incompatible.

Las comunicaciones asincrónicas se ejecutan en redes basadas en paquetes, como Ethernet (IP).

La división crea muchos problemas. Los teléfonos no son tan intuitivos como solían ser: simplemente intente iniciar una llamada de tres vías sin cortar. Las computadoras pueden verificar su correo electrónico, pero no su correo de voz. Y luego existe el enorme costo de comprar, mantener y actualizar dos infraestructuras complejas.

Para que sus teléfonos y computadoras hablen entre sí, usted debería arrancar todo el sistema de telefonía, tirar su PBX, reemplazar cada teléfono de escritorio, eliminar toda la toma telefónica. En resumen, usted debería comenzar desde cero.

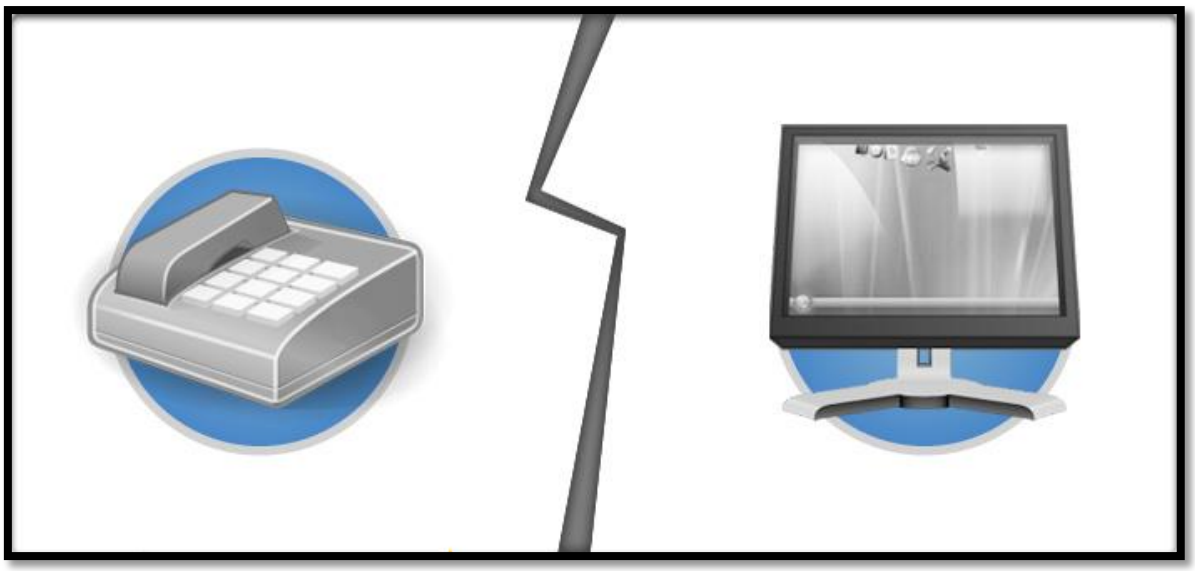


Figura 2.16 – Las comunicaciones dividen
Fuente: http://www.microsoft.com/latam/uc/what.aspx

2.3.5.2 Mensajería unificada

La funcionalidad de telefonía incluida en la mensajería unificada (UM) es nueva en la línea de productos de Microsoft Exchange. Gracias a su introducción, se combinan varias infraestructuras de mensajería en una sola.

La función del servidor de mensajería unificada es proporcionar funciones de servidor diferenciadas, acordes con la forma en la que normalmente se implementan y distribuyen los sistemas de mensajería en las organizaciones. Una función de servidor es una unidad que agrupa de forma lógica las características y los componentes necesarios para realizar una función determinada en el entorno de mensajería.

La mensajería unificada (UM) combina mensajes de voz, fax y correo electrónico en una sola infraestructura, esta introduce todos los mensajes de voz, correo electrónico y fax en un solo buzón al que se puede tener acceso desde diversos dispositivos. Cuando se han implementado los servidores de UM en la red, los usuarios pueden tener acceso a sus mensajes desde un

teléfono que use Outlook Voice Access, desde un dispositivo móvil o desde el equipo de un usuario que esté ejecutando Microsoft Windows XP.

Hoy en día, los empleados de las empresas con frecuencia administran los mensajes de voz y fax separados de los mensajes de correo electrónico. Además, los administradores de IT con frecuencia administran las redes de correo de voz o telefonía y los sistemas de correo electrónico o las redes de datos como sistemas separados. En estas situaciones, el correo de voz y el correo electrónico existen como bandejas de entrada separadas alojadas en servidores separados a los que se tiene acceso desde el escritorio para el correo electrónico y mediante el teléfono para el correo de voz. Los mensajes de fax se envían y se reciben desde aparatos físicos de fax independientes. La UM ofrece un solo lugar de almacenamiento para todos los mensajes, incluidos los mensajes de correo electrónico, voz y fax.

UM combina los mensajes de voz, fax y de correo electrónico en un solo almacén, al que se puede tener acceso desde un teléfono y un equipo, integra al servidor con redes de telefonía y lleva las características al mismo núcleo de Exchange Server. La siguiente figura ilustra la relación entre los componentes de la red de telefonía de una organización y el sistema de mensajería unificada.

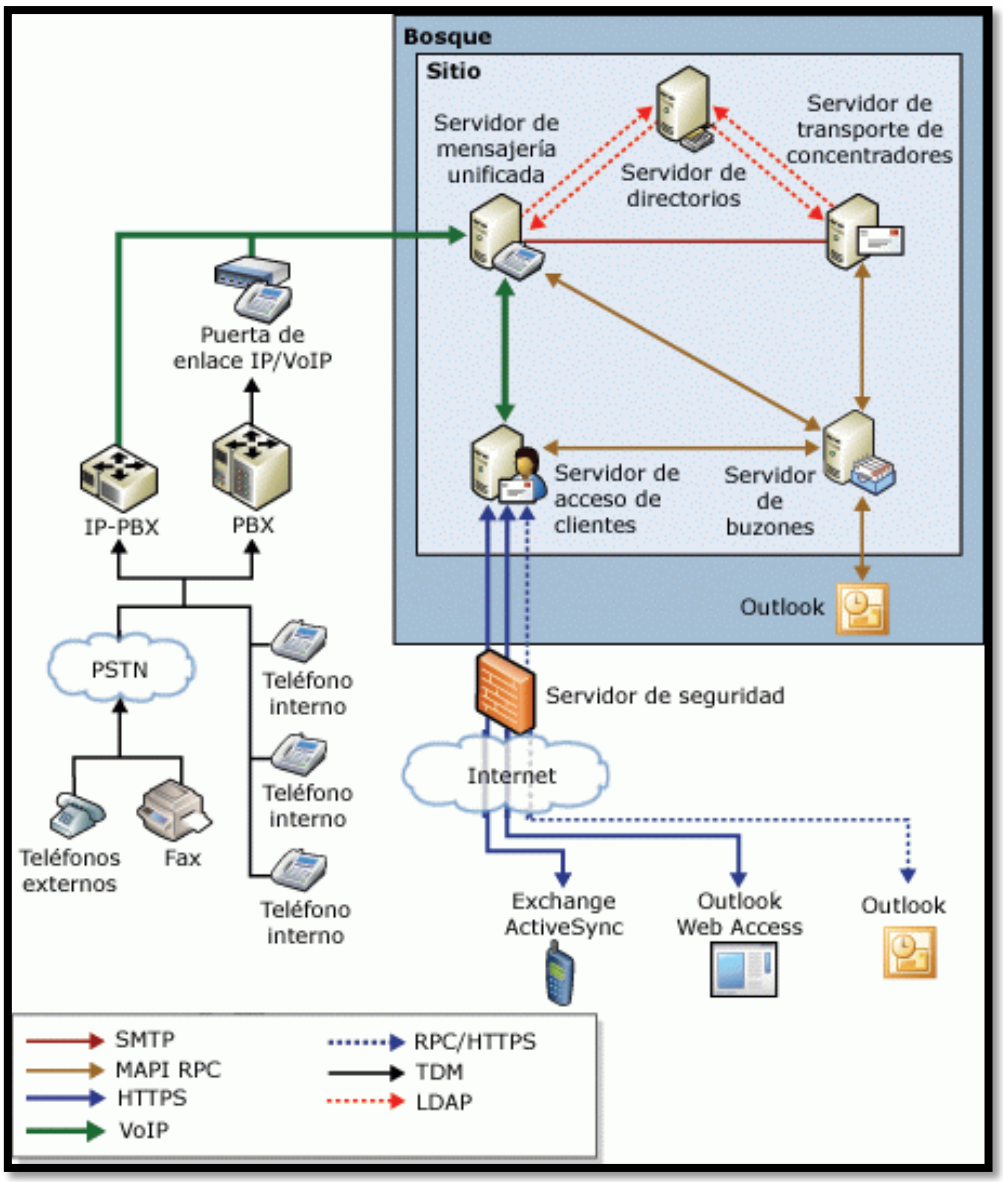


Figura 2.17 - La relación entre componentes de telefonía y la mensajería unificada de Exchange Server 2007
Fuente: http://www.valls.com.es/ocs/80.gif

Actualmente, la mayoría de los usuarios y departamentos de IT (tecnologías de la información) administran sus mensajes de correo de voz y de fax separados del correo electrónico. El correo de voz y el correo electrónico existen como bandejas de entrada separadas hospedadas en servidores separados a los que se tiene acceso desde el escritorio para el correo electrónico y mediante el teléfono para el correo de voz. Los mensajes de fax no se reciben en una bandeja de entrada del usuario, sino en máquinas de fax independientes o en un

servidor de fax centralizado. La mensajería unificada ofrece un almacén integrado para todos los mensajes y acceso al contenido mediante un equipo y el teléfono.

UM proporciona un solo punto de administración de los mensajes para los administradores de la organización. Las características incluidas permiten a un administrador de correo:

- Administrar los sistemas de correo de voz, de correo electrónico y de fax desde una plataforma única.
- Administrar la Mensajería unificada empleando comandos que se pueden utilizar en scripts.
- Construir infraestructuras de mensajería unificada de gran disponibilidad y confiables.

La función de servidor de UM permite a los usuarios tener acceso a mensajes de correo de voz, correo electrónico y fax, e información de calendario que se encuentran en su buzón, desde un cliente de correo electrónico, por ejemplo *Microsoft Outlook* o *Outlook Web Access*, desde un dispositivo móvil que tenga habilitado *Microsoft Exchange ActiveSync*, como teléfonos inteligentes o asistentes personales digitales (PDA) con *Windows Mobile*®, o desde teléfonos.

UM proporciona a los usuarios características como:

Contestar llamadas. Contestar llamadas, incluye responder a una llamada entrante en nombre del usuario, reproducir su saludo personal, grabar un mensaje y enviarlo para que se entregue en su bandeja de entrada como un mensaje de correo electrónico.

Recepción de fax. Es el proceso de enviar un mensaje de fax para que se entregue en la bandeja de entrada.

Acceso a suscriptores. Permite el acceso telefónico a los usuarios de la compañía. Dichos usuarios o suscriptores que están llamando por teléfono al sistema de mensajería unificada, pueden tener acceso a su buzón con *Outlook Voice Access*. Los suscriptores que usan *Outlook*

Voice Access pueden tener acceso al sistema de mensajería unificada mediante el teclado del teléfono o entradas de voz. Mediante el uso de un teléfono, un suscriptor o usuario puede:

- Tener acceso al correo de voz.
- Escuchar, reenviar o responder a mensajes de correo electrónico.
- Escuchar información de calendario.
- Tener acceso o llamar a contactos almacenados en la lista global de direcciones o en una lista personal de contactos.
- Aceptar o cancelar solicitudes de reuniones.
- Establecer un mensaje de correo de voz de fuera de la oficina.
- Establecer preferencias de seguridad y opciones personales.

Operador automático. Es un conjunto de mensajes de voz que proporciona a los usuarios externos acceso al sistema de mensajería unificada de Exchange 2007. El operador automático permite al usuario utilizar el teclado del teléfono o entradas de voz para navegar por la estructura de menús, llamar al usuario o encontrar a un usuario y luego llamarlo. El operador automático proporciona al administrador la capacidad de:

- Crear un conjunto personalizable de menús para usuarios externos.
- Definir saludos informativos, saludos de horario de apertura y saludos de horario fuera de oficina.
- Definir calendarios de vacaciones.
- Describir como buscar en el directorio de la organización.
- Describir como conectar con la extensión de un usuario, para que los que llaman desde el exterior puedan llamar a un usuario al especificar su extensión.

- Describir la forma de buscar en el directorio de la organización para que los que llaman desde el exterior puedan buscar en el directorio de la organización y llamar a un usuario específico.

- Permitir que los usuarios externos llamen al operador.

2.3.5.3 UC Servicios Empresariales

Las tecnologías de comunicaciones unificadas de Microsoft, ponen un puente entre computadoras y teléfonos con dos servidores integrados: *Microsoft Exchange Server 2007* y *Microsoft Office Communications Server 2007*. Se integran con el sistema de telefonía existente de la compañía y entregan servicios completos de comunicaciones usando la red de datos existente.

Las tecnologías de comunicaciones unificadas Microsoft maximizan la infraestructura existente integrando sistemas PBX existentes a través de una entrada de VoIP/PBX.

Con Microsoft las tecnologías de comunicaciones unificadas, las computadoras en la red ganan la funcionalidad de los teléfonos avanzados de VoIP. Los usuarios pueden dar clic para llamar cualquier contacto en su libreta de direcciones. Una llamada telefónica simple puede convertirse en una llamada de conferencia o una videoconferencia.

Figura 2.18 – Microsoft unifico tecnologías de comunicaciones
Fuente: http://www.microsoft.com/latam/uc/what.aspx

Microsoft unificó tecnologías de comunicaciones eliminando las paredes que separan telecomunicaciones y computadoras, y lo hacen con el software que mantiene la infraestructura de telecomunicaciones existente.

Las tecnologías de comunicaciones unificadas Microsoft son más que solo VoIP. Analizan todos los silos tradicionales de comunicaciones. El correo de voz y los faxes se mueven sobre la red como E-mail. Llegan al buzón de *Microsoft Office Outlook 2007* de donde se puede clasificar, dar prioridad, y responder, apenas como cualquier correo electrónico.

Y cuando se está fuera de la red corporativa, se puede marcar a la red interna desde cualquier teléfono para oír E-mail y citas. Se puede incluso tener acceso al directorio de *Outlook* y hacer llamadas de cualquier teléfono.

Figura 2.19: Derribando las barreras de la comunicación
Fuente: http://www.microsoft.com/latam/uc/what.aspx

Las tecnologías de comunicaciones unificadas Microsoft utilizan las ventajas del software para entregar comunicaciones completas (mensajería, voz, y vídeo) a través de las aplicaciones y de los dispositivos que la gente utiliza a diario.

Integrando las experiencias se asocia al teléfono (llamadas telefónicas, correo de voz, y comunicación) en el trabajo se hace en una computadora (documentos, hojas de balance,

mensajería inmediata, E-mail, calendarios) tiene la ventaja de cambiar de manera fundamental la manera en que el mundo trabaja.

2.3.6 Red Inalámbrica

2.3.6.1 Introducción

En general, una red de radio es un conjunto de nodos que se comunican entre sí empleando ondas de radio y el aire como soporte (no requieren de un medio físico, como sucede en otro tipo de comunicaciones, que necesitan de cables de cobre o fibra óptica para el establecimiento de la comunicación.

La tecnología sin hilos, más conocida como LAN inalámbrica, se refiere a la tecnología que permite a dos o más nodos comunicarse utilizando protocolos de red estándar y sin cableado de red.

Las ventajas de las redes inalámbricas son:

Flexibilidad. Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para dore estar comunicados por el mundo.
Poca planificación. Con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.
Diseño. Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc. También presentan un consumo de energía muy reducido.
Robustez frente eventos inesperados. (Tropezón de un usuario con un cable, terremoto, etc.) Ante los que una red cableada podría llegar a quedar completamente inutilizada. En estos casos, una red inalámbrica puede aguantar bastante mejor este tipo de percances.

Las desventajas de las redes inalámbricas son:

Calidad de Servicio. Las redes inalámbricas ofrecen una peor calidad de servicio que sus homólogas cableadas. Son velocidades que no superan los 10 Mbps, frente a los 100 Mbps que se puede alcanzar con redes convencionales.

Mayor Costo. Cada vez más se van abaratando los costos asociados a esta tecnología, todavía resultan más caras que las redes cableadas en la mayoría de los casos.

Restricciones. Estas redes requieren de la asignación de una banda dentro del espectro radioeléctrico.

Seguridad. Seguridad e integridad de la información que se transmite, esto no se puede implementar donde se corre el riesgo de que exista robo de información. Por otro lado, este tipo de redes puede interferir con otro tipo de redes.

Propiedad	**WLAN**	**LAN cableada**
Velocidad de transmisión	11-54 Mbps	100 Mbps o más
Costos de instalación	Medio	Alto
Movilidad	Sí	No
Flexibilidad	Muy Alta	Baja
Escalabilidad	Alta	Muy alta
Seguridad	Alta	Alta
Demanda	Baja	Muy alta
Configuración e instalación	Fácil	Media
Presencia en empresas	Baja	Alta
Integridad	Alta	Alta
Costo de expansión	Medio	Alto
Licencia	No está regulado	No

Tabla 2.9. Comparación entre las redes WLAN y las redes LAN convencionales

2.3.6.2 Arquitectura

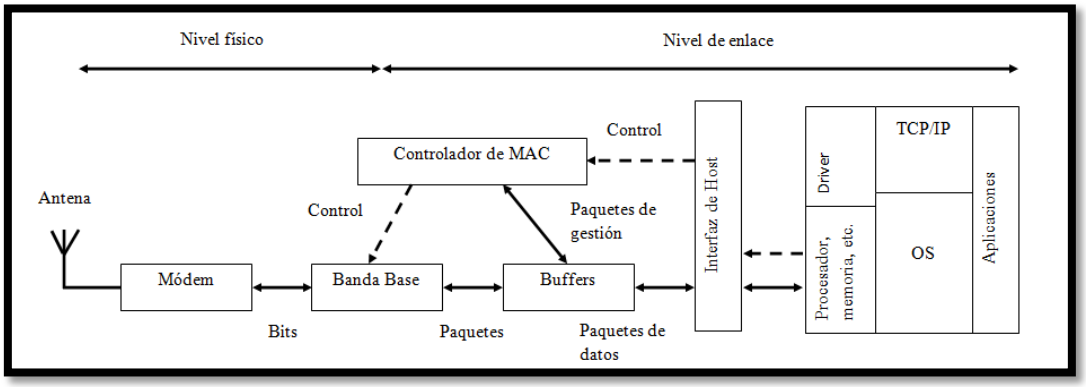


Figura 2.20 – Componentes de un nodo de red WLAN
Fuente: Huidobro, José. Redes y Servicios de Banda Ancha

Cualquier dispositivo radio está dividido en dos partes: el módem, encargado de modular y demodular a las frecuencias adecuadas y que se compone de antena, amplificadores, sintetizadores y frecuencias y filtros, y el controlador MAC, responsable de gestionar el acceso al medio del dispositivo.

La mayoría de dispositivos radio suelen ser una tarjeta que se conecta en alguna de las ranuras de expansión del PC y que interactúa directamente con el protocolo radio concreto.

Existen dos componentes más: encontramos la interfaz de *host*, cuya misión es permitir al PC comunicarse con el controlador MAC, y el *driver*, que es el software que necesita el sistema operativo para poder manejar la tarjeta de red inalámbrica.

2.3.6.2.1 Nivel Físico

En nivel físico se encarga de resolver los aspectos relacionados con las particularidades del medio de transmisión radioeléctrico.

2.3.6.2.2 Tecnologías

Las primeras WLAN trabajaban en la banda ISM (*Industrial, Scientific and Medical*), localizada a 900 MHz y 2,4 GHz. La principal característica de estas bandas es que no requieren de licencia por parte de los usuarios, ya que son de libre uso, es decir, que un usuario que desee transmitir en esta banda no necesita solicitar ni pagar por una licencia para hacerlo: basta con que el equipo que emplee esté certificado y cumpla una serie de normas. En principal problema de estas frecuencias son las interferencias.

Otra banda empleada es la situada en torno a los 5 GHz. En esta porción del espectro el ancho de banda disponible es mayor, lo que implica mayores velocidades. Sin embargo, cuando mayor es la frecuencia de trabajo, más grande es el nivel de ruido y más sensible es la propagación a los obstáculos.

Banda ISM (*Industrial, Scientific and Medical*)		
902-928 MHz	2,400-2,4835 GHz	5,725-5,850 GHZ

Tabla 2.10: Bandas de ISM

Una vez escogida la banda de frecuencia, el siguiente paso es elegir una tecnología de transmisión, según el diseño de la red se dispone de distintas opciones:

- ***Banda Estrecha.*** Se transmite y recibe en una banda de frecuencia lo más estrecha posible. Los usuarios tienen distintas frecuencias de comunicación, evitando así las interferencias.
- ***Espectro Ensanchado (SS, Spread Spectrum).*** Es el usado por la mayor parte de los sistemas. Se consume más ancho de nada, pero la señal es más fácil de detectar. El receptor conoce los parámetros de la señal que se ha difundido. Existen dos tipos de tecnología de espectro ensanchado:
    - **Salto en frecuencia (FHSS, *Frecuency-Hopping Spread Spectrum*).** Utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado, es como tener un

único canal lógico. Para un receptor no sincronizado, FHSS es como un ruido de impulsos de corta duración.

  - **Secuencia directa (DSSS*, Direct-Sequence Spread Spectrum*).** Se genera un bit redundante por cada bit transmitido. Cuanto mayor sea esta secuencia, mayor es la probabilidad de reconstruir los datos originales. Incluso si uno o más bits son perturbados en la transmisión, las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir.

- ***Infrarrojos.*** Se usan frecuencias muy altas para el transporte de datos. La luz infrarroja no puede traspasar objetos opacos, por lo que, o bien se utiliza una comunicación con línea de visión directa, o bien se difunde la señal. Los sistemas de difusión IR no requieren línea de visión pero las células están limitadas a habitaciones individuales. Este tipo de tecnología se empela, habitualmente, para conectar PC con impresoras, teléfonos móviles, PDA, etc.

La tecnología de espectro ensanchado por salto en frecuencia consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamando *dwell time*, inferior a 400 ms. De esta manera, cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo y así se combaten los efectos de las interferencias.

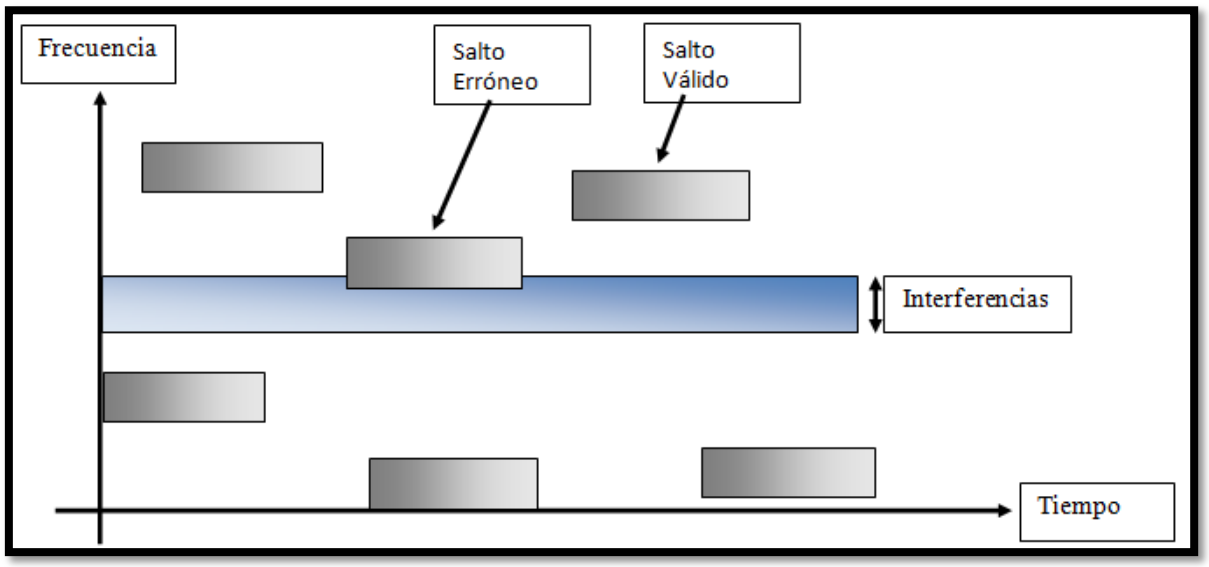


Figura 2.21 - Espectro ensanchado por salto en frecuencia
Fuente: Huidobro, José. Redes y Servicios de Banda Ancha

Cada una de las transmisiones a una frecuencia concreta se realiza utilizando una portadora de banda estrecha que va cambiando a lo largo del tiempo.

La ventaja de estos sistemas frente a los sistemas DSSS es que con esta tecnología podemos tener más de un punto de acceso en la misma zona geográfica sin que existan interferencias si se cumple que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo.

El principal problema de FHSS es que complica el diseño de la capa de MAC, pues se requiere información de control para procurar la sincronización y que entre cada salto exista un intervalo de tiempo durante el cual no se puede enviar información.

DSSS, en lugar de modificar la frecuencia de la portadora, utilizan ese patrón para codificar cada uno de los bits de datos, de manera que la pérdida de uno de ellos es causada por interferencias no implica la retransmisión del paquete entero, ya que es posible reconstruir casi completamente el patrón por técnicas estadísticas.

En el otro extremo, se recibe el canal completo y se demodula con el mismo código que se empleó en el origen. Para evitar el ruido del canal debido al resto de usuarios, se usa una técnica llamada *chipping*. Cada bit de datos es convertido en una serie de patrones redundantes de bit llamados *chips*. La redundancia inherente de cada *chip* proporciona una forma de detección y corrección de errores, puesto que incluso si en parte de la señal se produce un error, se puede recuperar, minimizando así la necesidad de retransmisiones.

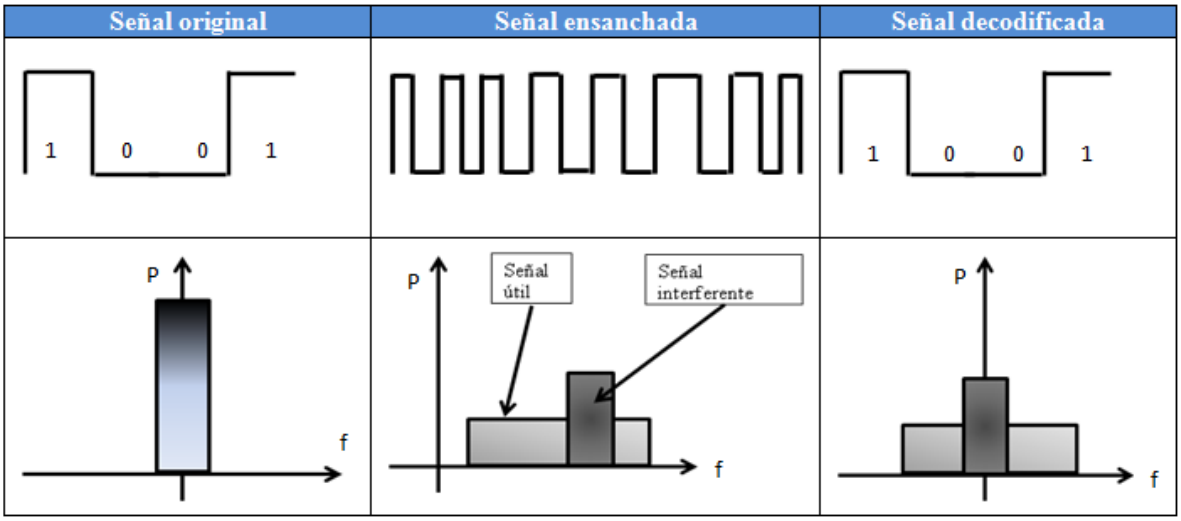


Figura 2.22 - Espectro ensanchado por secuencia directa
Fuente: Huidobro, José. Redes y Servicios de Banda Ancha

El resultado es un código de mucha frecuencia, por lo que el módem debe ser más complejo. La tecnología de espectro ensanchado por secuencia directa opera en el rango que va desde los 2,4 GHz hasta los 2,4835 GHz, es decir, con un ancho de banda total disponible de 83,5 MHz. Este ancho de banda total se divide en un total de 14 canales con un ancho de banda por canal de 5 MHz de los cuales cada país utiliza un subconjunto de los mismos según normas reguladoras para cada caso particular.

Una tercera tecnología, de momento no demasiado utilizada a nivel comercial para implementar WLAN, es la de infrarrojo. Los sistemas de infrarrojos se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Los infrarrojos tienen unas características de propagación muy particulares, ya que no pueden pasar a través de objetos opacos pero se reflejan en determinadas superficies. Las longitudes de onda de

operación se sitúan alrededor de los 850-950 nm, es decir, a unas frecuencias de emisión que se sitúan entre los 315 y los 352 GHz.

- Sistemas de corta apertura, de haz dirigido o de visibilidad directa, que funcionan de manera similar a los mandos a distancia de los aparatos de televisión. Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse información (sistemas de visión directa o LOS, *Line-Of-Sight*).
- Sistemas de gran apertura, reflejados o de difusión, que radian tal y como lo haría una bombilla, permitiendo el intercambio de información en un rango más amplio. La norma IEEE 802.11 específica dos modulaciones para esta tecnología: la modulación 16 ppm e la modulación 4 ppm, proporcionando unas velocidades de transmisión de 1 y 2 Mbps, respectivamente. Esta tecnología se aplica típicamente en entornos de interior para implementar enlaces punto a punto de corto alcance o redes locales en entornos muy localizados.

2.3.6.2.3 Topologías

Existen 2 tipos de topologías: *extremo a extremo* (P2P, *Peer To Peer*) y *basada en punto de acceso*.

Las *configuraciones P2P,* también conocidas como redes *ad-hoc*, son las más sencillas, ya que en ellas los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas. En este tipo de redes, el único requisito deriva del rango para que la comunicación sea posible. Por otro lado, no es necesario ningún tipo de gestión administrativa de la red.

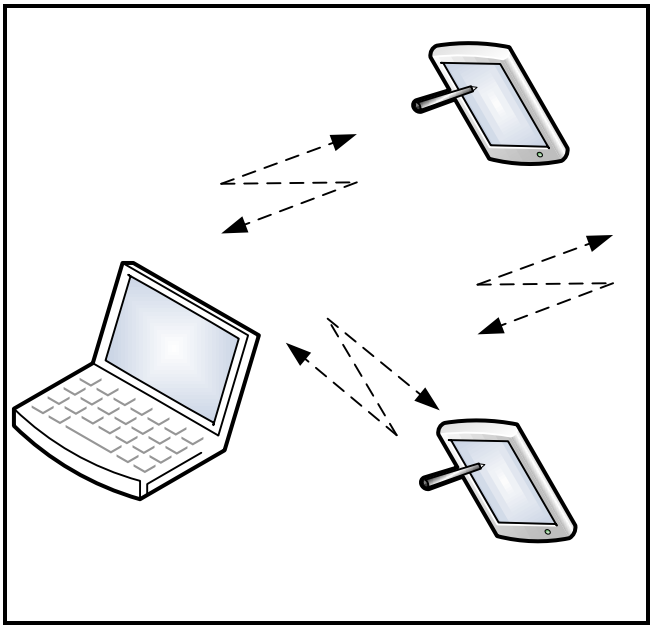


Figura 2.23 – Configuración P2P
Fuente: Huidobro, José. Redes y Servicios de Banda Ancha

La *topología con punto de acceso*, en cambio, está basada en el concepto de celda, típico de la telefonía móvil. Una celda podría entenderse como el área en la que una señal radioeléctrica es efectiva. A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión es posible combinar las celdas de estas señales para cubrir de forma casi total un área más extensa. La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados puntos de acceso, que funcionan como repetidores y que son capaces de doblar el alcance de una red inalámbrica: la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso. Los puntos de acceso deben estar situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros, en función de las condiciones de propagación.

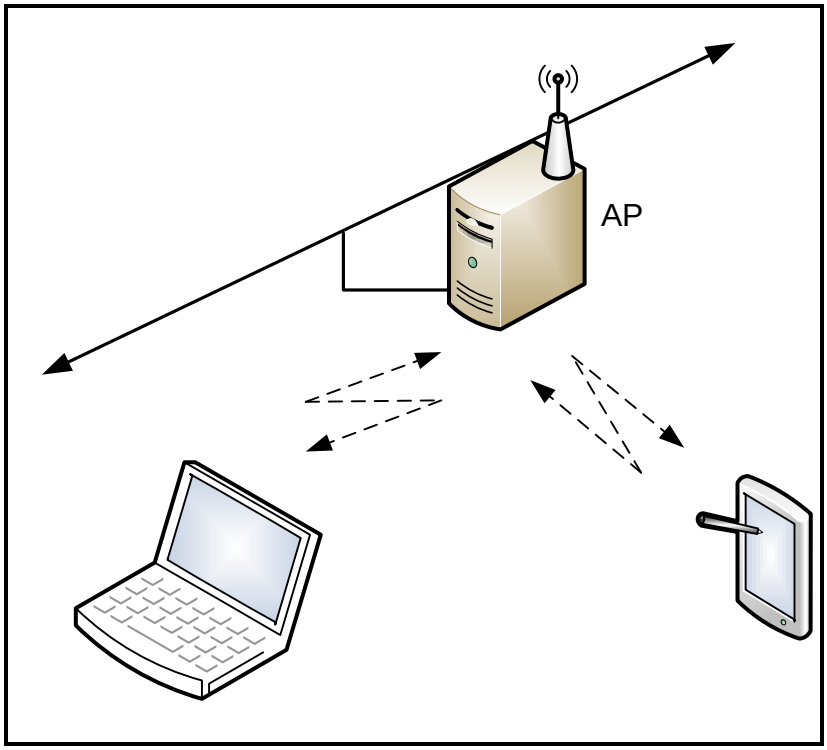


Figura 2.24 – Topología con único punto de acceso
Fuente: Huidobro, José. Redes y Servicios de Banda Ancha

La topología con punto de acceso capaz de dotar a una red inalámbrica de muchas más posibilidades. Además, favorece el evidente aumento del alcance de la red, ya que la utilización de varios puntos de acceso, y por lo tanto lo que se conoce como *roaming*, es decir, la movilidad de terminales sin pérdida de cobertura y sin sufrir cortes en la comunicación. Esto representa una de las características más interesantes de las redes inalámbricas.

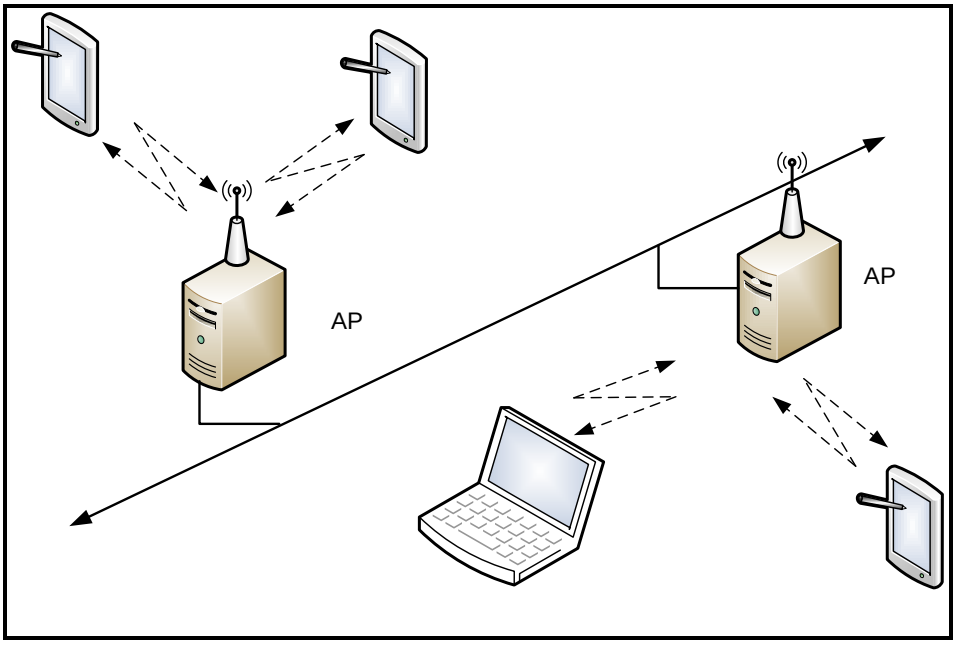


Figura 2.25 – Topología con varios puntos de acceso
Fuente: Huidobro, José. Redes y Servicios de Banda Ancha

Sin embargo, las posibilidades de las redes inalámbricas pueden verse ampliadas gracias a la interconexión con otras redes, sobre todo con redes cableadas. Los recursos disponibles en ambas redes se amplían.

Mediante el uso de antenas es posible conectar dos redes separadas por varios cientos de metros, como por ejemplo dos redes locales situadas en dos edificios distintos.

De esta forma, una LAN cableada se beneficia de la tecnología inalámbrica para realizar interconexiones con otras redes, que de otra forma serían más costosas, o simplemente imposibles.

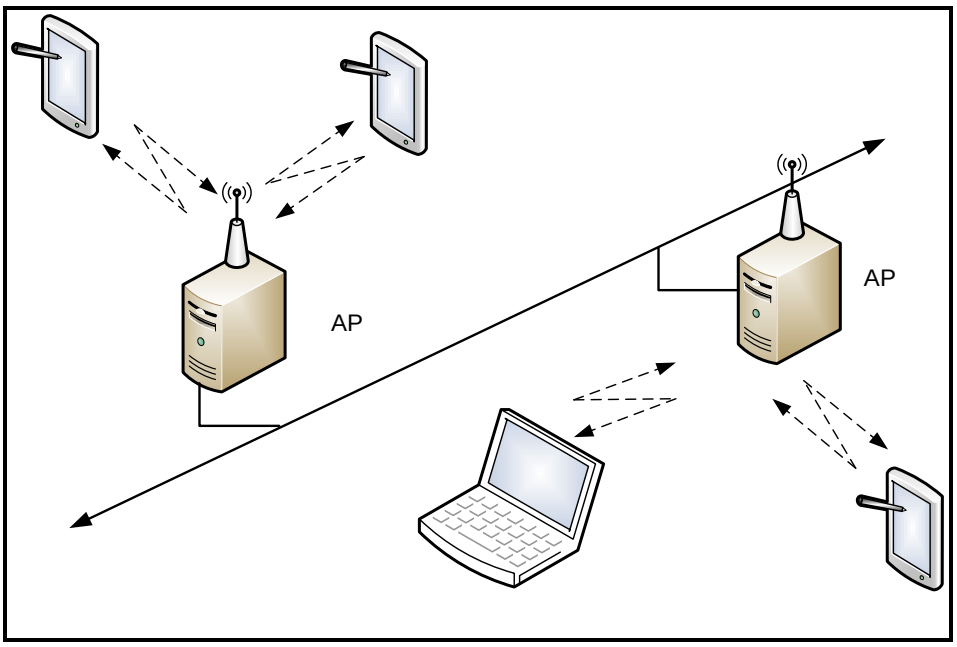


Figura 2.26 – Interconexión vía radio de redes LAN
Fuente: Huidobro, José. Redes y Servicios de Banda Ancha

2.3.6.2.4 Normalización

En 1989 se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN. En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (*Personal Communicatios Systems*). En 1993 también se constituye la IrDA (*Infrared Data Association*) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos. En 1996, finalmente, un grupo de empresas del sector de informática móvil y de servicios forman el Wireless LAN Interoperability Forum (*WLI Forum*) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Por otra parte, WLANA (*Wireless LAN Association*) es una asociación de industrias y empresas cuya misión es ayudar y fomentar el crecimiento de la industria WLAN a través de la educación y promoción.

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original; 802.11a, que define una conexión de alta velocidad basada en

ATM; 802.11b, que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y 802.11g, compartible con él, pero que proporciona aún mayores velocidades.

En junio del año 1997 el IEEE ratificó el estándar para WLAN IEEE 802.11, que alcanzaba una velocidad de 2 Mbps, con una modulación de señal de espectro expandido por secuencia directa (DSSS), aunque también contempla la opción de espectro expandido por salto de frecuencia, FHSS en la banda de 2.4 GHz, y se definió el funcionamiento y la interoperabilidad entre redes inalámbricas.

2.3.6.3 IEEE 802.11

Existen tres especificaciones dentro del estándar 802.11:

- **WLAN 802.11**

  El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2,4 GHz.

- **WLAN 802.11a**

  Alcanza velocidades de hasta 54 Mbps es la banda de 5 GHz, tiene menos interferencias, pero tiene un alcance limitado de 50 metros, lo que implica tener que montar más puntos de acceso.

- **WLAN 802.11b**

  Es una extensión del estándar 802.11 para WLAN empresariales, con una velocidad de 11 Mbps y un alcance de 100 metros, utiliza una modulación lineal compleja (DSSS).

- **WLAN 802.11g**

  Es compatible con el 802.11b, capaz de una velocidad doble, es decir, hasta 22 Mbps, y llegar incluso a 54 Mbps, para competir con los otros estándares que prometen velocidades mucho más elevadas pero que son incompatibles con los equipos 802.11b ya instalados.

Propiedades	IEEE 802.11	IEEE 802.11a	IEEE 802.11b
Aplicación	Wireless Ethernet	Wireless ATM	Wireless Ethernet
Rango de Frecuencias	2,4 GHz	5 GHz	2,4 GHz
Tasa Binaria	1-2 Mbps	20-54 Mbps	5,5 Mbps, 11 Mbps

Tabla 2.11: Estándares IEEE 802.11

2.3.6.4 Seguridad

Las redes inalámbricas son inseguras aunque sólo sea porque el medio de transporte que emplean es el aire; por tanto, un elemento esencial a tener en cuenta en este tipo de redes al utilizarse la radio es la encriptación.

En general, se utiliza WEP (*Wired Equivalent Privacy*), aunque también existen otros mecanismos. Se trata de un sistema de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso. La clave de acceso estándar es de 40 bits, pero existe otra opcional de 120 bits, y se asigna de forma estática o manual, tanto para los clientes , que comparten todos el mismo conjunto de cuatro claves predeterminadas, como para los puntos de acceso de la red, lo que genera algunas dudas sobre su eficacia. WEP utiliza un esquema de cifrado simétrico en el que la misma clave y algoritmo se utilizan tanto para el cifrado de los datos como para su descifrado.

Como parte del estándar Wi-Fi, las redes inalámbricas pueden anunciar sus nombres de red, para que sea más fácil encontrarlas y unirse a ellas. Este anuncio se conoce como el

identificador SSID. El primer paso para ofrecer cierta forma de seguridad sería no transmitir este nombre o elegir un nombre que no pudiera ser adivinado con facilidad.

2.3.7 Voz Sobre IP

2.3.7.1 Introducción

La transmisión de paquetes de voz mediante un protocolo de Internet se denomina *voz sobre IP*. VoIP puede cambiar la forma en la que nos comunicaciones a través de la Web, así como la forma en la que llevamos a cabo los negocios. Si se implementa adecuadamente, permitirá conseguir comunicaciones verdaderamente unificadas, Puede que proporcione una solución de bajo costo para la construcción de redes de transmisión y que permita acceder a diversas aplicaciones a través del mismo medio de transmisión.

La tecnología VoIP permite a los usuarios establecer conversaciones de voz a través de su equipo, mediante una conexión a Internet. Aunque el protocolo IP fue diseñado para que mostrara la efectividad con las transmisiones de datos, las aplicaciones de voz son ahora viables e incluso recomendables, gracias a que hay implementaciones de la arquitectura IP por todas partes, tanto en las redes como en los sistemas de comunicaciones.

El atractivo principal de VoIP es la posibilidad de ahorrar dinero que ofrece tanto a los clientes como a los proveedores de servicios. VoIP resulta económicamente eficiente. La posibilidad de disponer de nuevas aplicaciones y la posibilidad de evitar la red telefónica conmutada, junto con sus correspondientes tarifas, están incrementando en interés por VoIP. Para disminuir los costos de comunicaciones de las empresas que dispongan de distintas sucursales, los proveedores de servicios pueden reconfigurar las llamadas de larga distancia utilizando la infraestructura de red existente del cliente. Permitiendo así tener un ahorro de hasta un 50% en el costo de las llamadas.

2.3.7.2 Estándares

El estándar VoIP más ampliamente utilizado es H.323. Este estándar se utiliza como estándar de transmisión de paquetes en las *unidades de control multipunto* (MCU, *Multipoint Control Unit*), como son los sistemas interred, las pasarelas, los guardianes de pasarela y los terminales. El estándar H.323 fue creado por la Unión Internacional de Telecomunicaciones en junio de 1996, como resultado de una serie de modificaciones en estándares relativos a la videoconferencia. La primera versión se centraba en la transmisión a través de una red de área local que utilizara IP. Dos años más tarde, en enero de 1998, la nueva versión contemplaba la infraestructura de redes de área extensa. Hoy en día, H.323 es un estándar para otras tecnologías relacionadas con la voz y los datos multimedia.

Algunos estándares dentro del marco de trabajo de H.323 son H.225, para el control de señalización de llamadas; H.245, para el control de medios de transmisión y multimedia; H.235, para seguridad y cifrado; y H.450, para servicios suplementarios y funciones avanzadas de llamada.

Una de las principales críticas contra H.323 es el tiempo y la complejidad implicados en el establecimiento de una llamada. En primer lugar, el protocolo utiliza varios mensajes de ida y vuelta como parte del mecanismo de señalización y control de una llamada que se esté intentando establecer entre dos terminales. Además, H.323 requiere emplear conexiones TCP para transportar los mensajes, lo que obliga a otro intercambio adicional de ida y vuelta.

La versión 3, más moderna, representa una mejora sobre las anteriores e incluye tanto un procedimiento de conexión rápida, que consolida los mensajes Q.931 intercambiados entre los terminales, como un procedimiento de túnel, que permite a H.245 compartir una misma conexión TCP con Q.931. Otros estándares adicionales y emergentes actualmente en uso en las soluciones basadas en VoIP incluyen: SIP, RTP, RTPC, RRP y MGCP.

2.3.7.3 Estándares y recomendaciones de ITU-T para VoIP: señalización

Estándar	Descripción
H.323 V2	Sistemas de comunicaciones multimedia basados en paquetes
H-225.0	Protocolos de señalización de llamada y división del flujo de datos en paquetes, para multimedia basada en paquetes (incluye Q.931 y RAS).
H.225.0 Anexo G	Comunicaciones pasarela a pasarela (interdominio).
H.245	Protocolo de control para comunicaciones multimedia.
H.235	Seguridad y cifrado para los terminales multimedia compatibles con la serie H.
H.450.x	Servicios suplementarios para multimedia:
	1. Protocolo genérico funcional para el soporte de servicios suplementarios en H.323
	2. Transferencia de llamada
	3. Desviación
	4. Retención
	5. Puesta en espera y recuperación
	6. Llamadas en espera
	7. Indicación de mensaje en espera
H.323 Anexo D	Fax en tiempo real utilizando T.38
H.323 Anexo E	Conexión de llamadas sobre UDP
H.323 Anexo F	Dispositivos de un solo uso
T.38	Procedimientos para comunicaciones en tiempo real de facsímiles grupo 3 sobre redes IP
Series T.120	Protocolos de datos para conferencias multimedia

Tabla 2.12 – Estándares y protocolos para señalización

2.3.7.4 Especificaciones RFC y borradores de IETF

Estándar	Descripción
RFC 2543	SIP: Session Initiation Protocol (protocolo de inicio de sesión)
RFC 2327	SDP: Session Description Protocol (protocolo de descripción de sesión)
Internet Draft	SAP: Session Announcement Protocol (protocolo de anuncio de sesión)

Tabla 2.13 – Especificaciones RFC

2.3.7.5 Control de pasarela IETF

Control	Descripción
Internet Draft	MGCP: Media Gateway Control Protocol (protocolo de control de pasarela para medios de transmisión)
Internet Draft	MEGACO protocol
Draft	SGCP: Simple Gateway Control Protocol (protocolo simple de control de pasarela)
Internet Draft	IPDC: IP Device Control (control de dispositivo IP)

Tabla 2.14 – Control de pasarela

2.3.7.6 Transporte a través del medio: IETF

Estándar	Descripción
RFC 1889	RTP: Real-Time Transport Protocol (protocolo de transporte en tiempo real)
RFC 1889	RTCP: Real-Time Transport Control Protocol (protocolo de control de transporte en tiempo real)
RFC 2326	RTSP: Real-Time Streaming Protocol (protocolo de flujos de transmisión en tiempo real)

Tabla 2.15 – Transporte a través del medio

2.3.7.7 ITU: codificación a través del medio: Voz

Estándar	Algoritmo	Velocidad de bits (Kbps)	Retardo típico extremo a extremo (ms), excluyendo el retardo de canal	Calidad de voz resultante
G.711	PCM	48, 56, 64	<< 1	Excelente
G.723.1	MPE/ACELP	5,3; 6,3	67 – 97	Buena (6,3)
				Adecuada (5,3)
H.728	LD-CELP	16	<< 2	Buena
G.729	CS-ACELP	8	25 – 35	Buena
G.729 anexo A	CS-ACELP	8	25 – 35	Buena
G.722	ADPCM Sub-banda	48, 56, 64	<< 2	Buena
G.726	ADPCM	16, 24, 32, 40	60	Buena (40)
				Adecuada (24)
G.727	AEDPCM	16, 24, 32, 40	60	Buena (40)
				Adecuada (24)

Tabla 2.16 – Codificación a través del medio

2.3.7.8 Algoritmo estándar de video

Estándar	Algoritmo	Velocidad de bits (Kbps)	Calidad de la imagen
H.261	Transformada de coseno discreto (DCT) con compensación de movimiento	px64 (p=# de canales B RDSI)	Baja
H.263	Versión mejorada de H.261	Varias	Alta

Tabla 2.17 – Algoritmo estándar de video

Refiérase al anexo 4 para ver los estándares de la UIT mencionados en este tema.

2.3.8 Vulnerabilidades de seguridad de las redes de voz

Vamos a analizar las vulnerabilidades (amenazas que, en caso de ser explotadas, pueden dañar un sistema o una red) dividiéndolas en las siguientes características principales: físicas, naturales, hardware, software, comunicaciones y humanas. Estas vulnerabilidades no son exclusivas de VoIP, sino que afectan a todas las redes que transporten información de voz, independientemente del medio de transmisión.

Existen vulnerabilidades *físicas* en las salas de equipos que albergan las pasarelas, conmutadores, encaminadores y servidores. Las vulnerabilidades *naturales,* como por ejemplo las condiciones climatológicas extremas, pueden hacer que dejen de estar disponibles las redes sobre las que se realizan las transmisiones de voz, al destruir los centros de conmutación. Los fallos de *hardware* de los equipos, como pasarelas, conmutador y concentrador, pueden provocar una situación de denegación de servicio.

El *software* o hardware no convenientemente parcheado que contengan vulnerabilidades conocidas puede ser aprovechado por los atacantes o utilizado para instalar puestas traseras que pudieran afectar negativamente a la integridad o disponibilidad de las transmisiones de voz. Las vulnerabilidades de *comunicación* pueden permitir a personas con intenciones maliciosas interceptar, escuchar o interferir las señales de transmisión de voz. Las vulnerabilidades *humanas* incluyen los errores cometidos debido a la insuficiente formación del personal.

2.3.9 Características de Confidencialidad, Integridad y Disponibilidad

La confidencialidad, la integridad y la disponibilidad son atributos inherentes al proceso de seguridad de la información y pueden aplicarse a los sistemas y redes para tratar de evaluar su estado global de seguridad. Para que un sistema o red ofrezca confidencialidad, la información contenida, transformada o transportada por ese sistema o red no debe poder ser leída o extraída por entidades no autorizadas. El atributo de integridad proporciona una razonable certidumbre de que la información contenida, transformada o transporte. El atributo de disponibilidad

proporciona una razonable certidumbre de que la información contenida, transformada o transportada por un sistema o red está disponible para su uso con una alta probabilidad.

2.3.10 Fabricantes

Es preciso adoptar precauciones a la hora de analizar los diferentes mercados para los fabricantes de tecnología VoIP.

2.3.10.1 Fabricantes de pasarelas VoIP

Fabricante	Producto	Notas
H3Com	Total control 1000/200 Media Gateway	Pasarela VoIP
Cisco Systems	AS5300 / Voice Gateway	Pasarela VoIP
Com21	DOXphone	Pasarela VoIP GR-303
Convergent Netwoks	ICS2000 Broadband Switch	Conmutador software y pasarela VoIP
General Bandwidth	G6	Pasarela VoIP GR-303
Lucent Technologies	PathStar Access Server	Conmutador software VoIP
Lucent Technologies	IMerge NCS Gateway	Pasarela VoIP GR-303
Netspeak	ITEL	Conmutador software VoIP
Nortel Networks	Communications Server 2000	Conmutador software VoIP
Nuera	Orca	Conmutador software y pasarela VoIP
Sonus Networks	PSX6000	Conmutador software VoIP
Syndeo	Syion 426	Plataforma de conmutación software VoIP
Tellabs	SALIX 7000	Conmutador software y pasarela VoIP
Terayon	BandLeader AG-3000	Pasarela VoIP GR-303/V5.2
TollBridge Technologies	TB2000	Conmutador software y pasarela VoIP
Unisphere Networks	SMX-2100 and SRX-3000	Conmutador software y pasarela VoIP
ComMatch	Suet 3000 and 6000	Pasarela VoIP

Tabla 2.18 – Fabricantes de pasarelas VOIP

2.3.11 Interoperabilidad

No existe ningún problema con la interoperabilidad de las transmisiones si se utilizan dos pasarelas del mismo fabricante; sin embargo, cuando se utilizan pasarelas de diferentes fabricantes, puede que no se tenga tanto éxito. Los sistemas H.323 presentan variaciones de uno a otro fabricante y, de acuerdo con estudios realizados por Network World Test Alliance, sólo dos o tres fabricantes proporcionan verdadero soporte H.323; la mayoría de los fabricantes opera con versiones modificadas o ampliadas que no siempre funcionan bien entre sí. Todavía más problemática resulta la interoperabilidad entre teléfonos y conmutadores. En el mundo de los fabricantes de equipos VoIP, el término sistemas abiertos no quiere decir un idéntico cumplimiento de los estándares, por lo que no puede esperarse que los sistemas sean interoperables.

CAPÍTULO 3
ANÁLISIS Y DISEÑO DE LA INVESTIGACIÓN

3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA EMPRESA HERMES EXPRESS

Para determinar qué es lo que se tiene actualmente en la Empresa Hermes Express es necesario conocer a fondo toda la infraestructura con la que cuentan actualmente, esto permitirá realizar un análisis para verificar si es necesaria la adquisición de nuevas máquinas o ver otra solución posible para llegar a cumplir los objetivos planteados.

La Empresa Hermes Express cuenta con 6 máquinas las cuales tienen las siguientes características:

Máquina 1	
Área	Presidencia
Nombre Máquina	Ruben
Sistema Operativo	Windows XP
Procesador	Intel Celeron 2.40 GHZ
Memoria RAM	192 MB
Disco Duro	80 GB

Tabla 3.1 – Máquina Presidencia

Máquina 2	
Área	Gerencia General
Nombre Máquina	Conta
Sistema Operativo	Windows XP
Procesador	Intel Celeron 2.66 GHZ
Memoria RAM	504 MB
Disco Duro	80 GB

Tabla 3.2 – Máquina Gerencia General

Máquina 3	
Área	Contabilidad
Nombre Máquina	Contabilidad
Sistema Operativo	Windows XP

Procesador	Intel Pentium 4 1.60 GHZ
Memoria RAM	224 MB
Disco Duro	80 GB

Tabla 3.3 – Máquina Contabilidad

Máquina 4	
Área	Masivos
Nombre Máquina	casa-24107f96f9
Sistema Operativo	Windows XP
Procesador	Intel Pentium 4 1.60 GHZ
Memoria RAM	224 MB
Disco Duro	40 GB

Tabla 3.4 – Máquina Masivos

Máquina 5	
Área	Telemercadeo
Nombre Máquina	0e41195e423344d
Sistema Operativo	Windows XP
Procesador	Intel Celeron 2,40 GHz
Memoria RAM	224 MB
Disco Duro	40 GB

Tabla 3.5 – Máquina Telemercadeo

Máquina 6	
Área	Tecnología y Marketing
Nombre Máquina	Juanjo-Host
Sistema Operativo	Windows Vista
Procesador	AMD Turion™ Dual-Core Mobile RM-70 2,00GHZ
Memoria RAM	3 GB
Disco Duro	250 GB

Tabla 3.6 – Máquina Tecnología y Marketing

Todas las máquinas están conectadas en red mediante cable de red categoría 5, la máquina de Presidencia es la concentradora del internet la cual reparte el internet a todas las demás máquinas, el internet se reparte mediante un switch ADSL el cual cuenta con 5 puertos, de cada puerto salen cables UTP a cada máquina .

Actualmente la empresa cuenta con una conexión a internet de 512 MB, no se cuenta con servidores de nada, la forma de actualizar las máquinas es de forma individual al igual que el antivirus, el proceso de impresión se lo hace mediante una memoria flash ya que no existe tampoco un servidor de impresión o a su vez una impresora centralizada en alguna de las máquinas.

Se realizó la encuesta a la persona encargada de la parte sistemas y los resultados arrojaron que la empresa Hermes Express necesita una solución tecnológica completa empezando con la actualización de los equipos a unos con mejores características hasta tener la mayoría de los flujos de trabajo centralizados.

En el anexo 5 se muestra el plano de la empresa mostrando la distribución de las máquinas y la distribución del internet.

3.2 ANÁLISIS DE RESULTADOS DE LA ENCUESTA REALIZADA

Referirse al anexo 6 para visualizar la encuesta realizada al personal encargado de sistemas de la empresa Hermes Express.

Según la encuesta realizada se pudo determinar lo siguiente:

Figura 3.1 – Resultado IOM Mensajería y Colaboración Segura
Fuente: Presentación resultados IOM

En la figura 3.1 se puede apreciar los resultados que genero la encuesta en el campo Mensajería y Colaboración Segura, dando como resultado que la empresa se encuentra en un nivel de madurez Básico; ya que la empresa no cuenta con sistemas de correo electrónico y el envío de información se lo hace por clientes de correo externos como Hotmail, Yahoo, Gmail.

Es por esto que no se tiene sistemas centralizados de agendas, contactos y tareas produciendo en algunas veces conflictos en reuniones.

No se tiene un sistema de firmas digitales para garantizar la confidencialidad de los documentos importantes de la empresa.

La encuesta se determino que la empresa no tiene sistemas de antivirus para analizar correctamente la información que llega al correo electrónico.

Figura 3.2 – Resultado IOM Backup y Recuperación de Datos
Fuente: Presentación resultados IOM

En la figura 3.2 se puede demostrar que la empresa Hermes Express no cuenta con procesos de respaldo y recuperación de archivos críticos para la empresa, esto causa que en cualquier momento exista perdida de información sensible a la empresa.

Figura 3.3 – Resultado IOM Redes, Seguridad, Monitoreo
Fuente: Presentación resultados IOM

Como se aprecia en las figuras 3.3 y 3.4 la empresa en lo que respecta a redes, seguridad y monitoreo se encuentra en nivel Básico ya que no existen servidores que se encarguen del repartir los servicios de DHCP, DNS en servicios básicos de red, adicionalmente no se cuenta con políticas de seguridad ni servicios que brinden el servicio de seguridad, ni el rastreo de eventos de red.

Motivo por el cual puede existir el ingreso no permitido de intrusos a la red de la empresa poniendo en riesgo la información sensible de la empresa.

No existe un sistema de detección de intrusos, firewall perimetral, seguridad de acceso a redes inalámbricas a pesar de que la empresa no posee una red de acceso inalámbrico; pero ya que se planea implementar este tipo de servicio es necesario tener un esquema de seguridad que permita la encripción de archivos, detección de intrusos, un sistema de directorio activo con políticas de autenticación, etc.

Figura 3.4 – Resultado IOM Redes, Seguridad, Monitoreo parte 2
Fuente: Presentación resultados IOM

Como se ve en la figura 3.5 no existen políticas de de distribución de software para evitar molestias al usuario final, adicionalmente no existe un inventario de software y hardware, es decir no se tiene un control de los aplicativos que tienen instalados los usuarios en sus máquinas de trabajo, permitiendo así descargar e instalar aplicativos perjudiciales para el computador y potencialmente vulnerables para que los intrusos puedan robar información o a su vez causar daños en las computadoras.

La empresa no posee una estandarización en sistemas de antivirus, cada máquina tiene sistemas de antivirus diferentes y en algunos casos existen hasta dos o más antivirus instalados en cada máquina.

Se tiene una estandarización en más del 80% de las computadoras con el mismo sistema operativo Windows XP y la misma versión del Office 2003.

Figura 3.5 – Administración de Estaciones
Fuente: Presentación resultados IOM

Figura 3.6 – Administración Identidades y Acceso
Fuente: Presentación resultados IOM

En la figura 3.6 se puede observar que la empresa no cuenta con un sistema de directorio activo, por este motivo no se tiene políticas de grupo, políticas de autenticación, es decir cada usuario que ingresa a una de las máquinas puede ver todos los archivos contenidos en cada computador, también como resultado de esta evaluación se vio que ninguna de las máquinas tiene contraseña para el ingreso a la misma.

Figura 3.7 – Procesos y Manejos de IT
Fuente: Presentación resultados IOM

Como se ve en la figura 3.7 no existe una persona encargada de definir procesos de seguridad y riesgos, definir procesos de seguridad de la información, no existe procesos de respuesta a incidentes, no existe un control de los sistemas de antivirus, no existe una política definida para los dispositivos que se conectan a la red. No existe un proceso para realizar la adquisición de nuevo software.

Todos estos incidentes acarrean que se pierda información a partir de un desastre natural, el motivo que no existan procesos de respaldos y todo lo demás expuesto en este análisis hace que la empresa en infraestructura tecnológica se encuentre en un nivel Básico.

3.3 ANÁLISIS DE LA INFRAESTRUCTURA NECESARIA PARA LA IMPLEMENTACIÓN

Para llevar a cabo este proyecto es necesario que la infraestructura sea de la siguiente manera tomando en cuenta los requerimientos mínimos de hardware para cada servidor.

Se analizo la posibilidad de virtualizar algunos de los servidores para minimizar costos de hardware y ahorrar espacio ya que la empresa no cuenta con espacio físico para la implementación de varios servidores.

3.3.1 Servidor de Directorio Activo, DNS y DHCP.

- **Sistema Operativo:** Windows Server 2003 R2 Estándar Edition (se toma en cuenta la versión estándar ya que la empresa no pasa de las 100 máquinas).
- **Computador o Procesador:** PC al menos procesador 133 MHz, se recomienda un procesador de 500 MHz o mayor.
- **Memoria:** como mínimo una memoria RAM de 128 MB, se recomienda el uso de 256 MB de memoria hasta 4 GB de RAM.
- **Disco Rígido:** 2 GB de disco duro disponible.
- **Lector:** CD-ROM o DVD-ROM
- **Licenciamiento:** cada copia instalada del software de servidor requiere la compra de una licencia de servidor Windows.

3.3.2 Servidor de Seguridad ISA Server 2006

- **Sistema Operativo:** Windows Server 2003 Estándar o Enterprise
- **Computador o Procesador:** Pentium III con procesador 733 MHZ o superior
- **Memoria:** 512 MB o superior
- **Disco Rígido:** Partición NTFS y 150 MB de disco duro

- **Lector:** CD-ROM o DVD-ROM
- **Licenciamiento:** cada copia instalada del software de servidor requiere la compra de una licencia de servidor Windows.

3.3.3 Servidor Exchange Server 2007

- **Sistema Operativo:** Windows Server 2003 Estándar o Enterprise
- **Computador o Procesador:** Pentium con procesador 800 MHZ o superior
- **Memoria:** 2 GB o superior
- **Disco Rígido:** Partición NTFS y 1,2 GB de disco duro
- **Lector:** CD-ROM o DVD-ROM
- **Licenciamiento:** cada copia instalada del software de servidor requiere la compra de una licencia de servidor Windows.

3.3.4 Servidor Sharepoint Server 2007

- **Sistema Operativo:** Windows Server 2003 Estándar o Enterprise
- **Computador o Procesador:** Pentium con procesador 800 MHZ o superior
- **Memoria:** 2 GB o superior
- **Disco Rígido:** Partición NTFS y 1,2 GB de disco duro
- **Lector:** CD-ROM o DVD-ROM
- **Licenciamiento:** cada copia instalada del software de servidor requiere la compra de una licencia de servidor Windows.

3.3.5 Servidor System Center Configuration Manager 2007

- **Sistema Operativo:** Windows Server 2003 Estándar o Enterprise
- **Computador o Procesador:** Pentium con procesador 800 MHZ o superior
- **Memoria:** 2 GB o superior
- **Disco Rígido:** Partición NTFS y 1,2 GB de disco duro

- **Lector:** CD-ROM o DVD-ROM

Licenciamiento: cada copia instalada del software de servidor requiere la compra de una licencia de servidor Windows.

3.3.6 Red Inalámbrica

Para la red inalámbrica se requiere un Access Point de alcance de 100 metros las posibles marcas a escoger son Linksys, 3Com. Adicionalmente para la conexión de cada máquina se necesita tarjetas USB para conexión inalámbrica en cada máquina.

3.3.7 VoIP

Para la solución de VoIP se necesita lo siguiente:

- Un servidor para la implementación de la central telefónica 3CX, para la implementación de esto se requiere:
    - Windows XP Pro, Vista Business, Windows Server 2003 o 2008
    - Los puertos que deben estar abiertos son 5060 (SIP), 5090 (Tunel – Opcional)
    - Los puertos libres deben ser 5480, 5482, 5483, 5485, 5486, 5487
    - Un puerto para IIS
    - .NET Framework versión 2.0 o superior
    - 1 GB de memoria RAM o superior
- 6 teléfonos USB para VoIP

3.4 ANÁLISIS DE LAS SEGURIDAD A IMPLEMENTAR

Las seguridades que se van a implementar se generaran a través del ISA Server 2006, el cual va a permitir estructurar las reglas para restringir el uso sitios Web, ejecutar programas y predeterminar horarios para el uso de Internet.

Para visualizar las políticas de seguridad a implementar con ISA Server 2006 refiérase al anexo 7.

3.5 DISEÑO DE LA RED FÍSICA

El diseño de la red física se adjunta como anexo 8 ya que el diseño se lo hizo directamente en el plano de la empresa Hermes Express.

3.6 DISEÑO DE LA RED VOIP

Para la implementación de la red VoIP se requieren los siguientes elementos:

- Central telefónica (Centralita 3CX)
- Teléfonos USB para cada usuarios
- Gateway VoIP

La distribución de todos los componentes necesarios para la red de voz se puede apreciar en el siguiente gráfico:

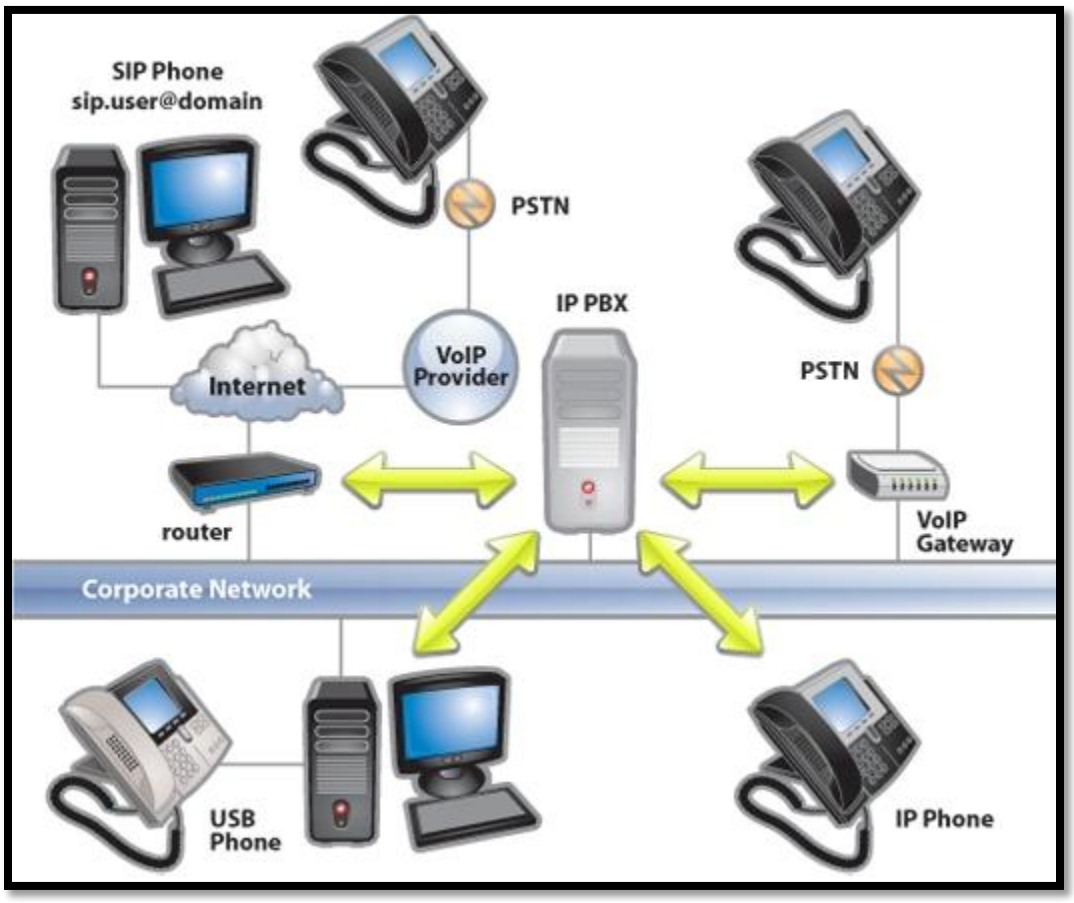


Figura 3.8 – Distribución de la Central Telefónica Centralita 3CX
Fuente: http://www.3cx.com/phone-system/images/3CX_ip-pbx-overview.jpg

CAPÍTULO 4
IMPLEMENTACIÓN Y PRUEBAS

4.1 IMPLEMENTACIÓN DEL SERVIDOR

Con el lanzamiento de la familia de productos Microsoft Windows Server 2003 se han simplificado y mejorado muchas de las características disponibles con Microsoft Windows NT 4.0.

Windows Server 2003 está disponible en cuatro ediciones. Cada edición se ha desarrollado para una función de servidor específica como se muestra en la tabla a continuación:

Edición	Situación de implementación propuesta
Windows Server 2003, Standar Edition	Pequeñas empresas y departamentos.
	Se lo utiliza si el servidor no requiere compatibilidad de hardware mejorada ni las características de clúster de Windows Server 2003, Enterprise Edition.
	Esta versión es perfecta para servidores de archivos y de impresión, servidores Web y grupos de trabajo. También mejora el acceso a redes para las sucursales.
Windows Server 2003, Enterprise Edition	Necesidades generales de las empresas de todos los tamaños. Una plataforma de aplicaciones, servicios Web e infraestructura.
	Esta versión está diseñada para los servidores que se emplean en una red empresarial de gran tamaño y para un entorno de uso intensivo de base de datos.
Windows Server 2003, Datacenter Edition	Aplicaciones esenciales para la empresa y la misión que requieren los mayores niveles de fidelidad, disponibilidad y escalabilidad.
	Esta versión de la familia Windows Server 2003 es el sistema operativo de servidores más potente. Se ha diseñado para admitir almacenes de datos de gran tamaño, el procesamiento de transacciones en línea (OLTP, *on-line Transaction Processing*) y proyectos de consolidación de servidores y simulaciones a gran escala.

Windows Server 2003, Web Edition	Esta versión proporciona una plataforma para desarrollar e implementar rápidamente servicios Web y aplicaciones mediante un servidor Web que ejecute Servicios de Microsoft Internet Information Server (IIS) 6.0.

Tabla 4.1 – Ediciones de Windows Server 2003

Para la implementación del servidor se escogió como sistema operativo a Windows Server 2003 Standard, ya que esta versión es suficiente para el tamaño de la empresa Hermes Express.

Las principales características de la versión estándar de Windows Server 2003 son las siguientes:

- Active Directory
- Administración Simplificada
- Administración flexible
- Escalabilidad
- Interoperabilidad
- Directivas de grupo
- Protocolo de actualización dinámica de Sistema de nombres de dominio (DNS, *Domain Name System*)
- Servidor de aplicaciones
- Escritorio Remoto

Los requerimientos mínimos para la implementación de Windows Server 2003, Standar Edition son los siguientes:

- **Computadora y Procesador:** Una PC cono mínimo un procesador de 133 MHz, recomendado 550 MHz o un procesador más rápido
- **Memoria:** como mínimo 128 MB, recomendado 256 MB, soporta hasta 4 GB de RAM.
- **Disco Duro:** de 1.25 a 2 GB de espacio en disco duro

Para ver los pasos de implementación refiérase al anexo 9

Una vez instalado el sistema operativo y configurado el servidor para que sea Directorio Activo, DNS y DHCP procedemos a configurar el Directorio Activo, para ver el esquema de Directorio Activo refiérase al Anexo 7.

4.2 IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDADES FIREWALL

Para llevar a cabo la implementación de las seguridades Firewall, se instalo ISA Server 2006 mediante el cual nos permite generar políticas de seguridad para cada usuario, a nivel de red, a nivel de red perimetral, a nivel de computador, para visualizar los pasos para la implementación refiérase al Anexo 9.

Predeterminadamente ISA Server bloquea todas las peticiones de los usuarios, para evitar esto se crean reglas de acceso y denegación, las cuales se muestran en el anexo 7:

4.3 IMPLEMENTACIÓN DE UN SISTEMA DE CORREO

Una vez estructurado el esquema de directorio activo se procedió a instalar el servidor de correo para esta empresa se escogió Exchange Server 2007.

Para ver los pasos de instalación de Exchange Server 2007 refiérase al anexo 10.

4.4 IMPLEMENTACIÓN DE UN SISTEMA CENTRALIZADO DE ACTUALIZACIONES

Para esta parte se instaló el sistema SCCM 2007 (System Center Configuration Manager) ya que es la versión mejorada de SMS 2003. Para llevar a cabo la implementación y configuración y ver los pasos de instalación refiérase al anexo 11.

4.5 IMPLEMENTACIÓN DE UN SISTEMA DE FLUJO DE TRABAJO

Para poder controlar el flujo de trabajo de la empresa Hermes Express se implemento un servidor de Sharepoint Server 2007. Para ver los pasos de instalación refiérase al Anexo 12.

4.6 IMPLEMENTACIÓN DE LA RED DE VOIP

La Centralita telefónica 3CX para Windows es una Centralita telefónica que reemplaza completamente a los sistemas telefónicos propietarios tradicionales; soporta teléfonos SIP virtuales/físicos de SIP estándar, servicios VOIP y líneas telefónicas tradicionales, ofreciendo numerosos beneficios:

- No hay necesidad de cableado telefónico. Los teléfonos utilizan la red de computadores.
- Es más fácil de instalar y manejar, a través de la interfaz de configuración basada en web.
- Una IP PBX basada en software es mucho menos costosa que una PBX/PABX basada en hardware.
- Los empleados mudan oficinas sin hacer cambios en el cableado o configuración de la IP PBX.
- Elija entre varios teléfonos SIP basados en hardware sin quedar atado a un solo proveedor.
- Reciba y haga llamadas a través de la red PSTN estándar utilizando pasarelas VOIP.
- Ahorre en los costos de las llamadas utilizando cualquier servicio VOIP SIP o WAN.

Para la implementación de la red de VOIP en la empresa Hermes Express se escogió la aplicación 3CX Centralita ya que es un software gratuito, para visualizar los pasos de instalación refiérase al Anexo 13.

CAPÍTULO 5
ENTREGABLES

Es muy importante que el cliente tenga como resultado de todos los trabajos realizados los entregables o memorias técnicas de todo lo que se hizo, así como también la propuesta que tiene la aceptación del cliente, resultados de las investigaciones, encuestas realizadas del modelo IOM.

A continuación se adjuntan los respectivos documentos que fueron entregados al personal de la Empresa Hermes Express. Los documentos a entregar son los siguientes:

- Propuesta de implementación de Servicios de Infraestructura, documento en el cual se describe los trabajos a realizar, así como también personas involucradas en el proyecto, costos y tiempos de entrega.
- Presentación de resultados de la encuesta IOM, este documento es una presentación realizada en PowerPoint que describe el momento actual de la Empresa Hermes Express.
- Resultados de Encuesta IOM, este documento contiene información más detallada sobre los resultados de la encuesta realizada, este documento incluye recomendación para mejorar e ir caminando por los demás niveles.

A continuación se muestran cada uno de los documentos que fueron entregados a la Empresa Hermes Express:

5.1 PROPUESTA DE SERVICIOS DE IMPLEMENTACIÓN DE INFRAESTRUCTURA

Quito, 13 de enero de 2010

Señores

Hermes Express

Atención. Sr. Rubén Enríquez

Ciudad

Asunto: Implementación de Servicios de Infraestructura.

A continuación presentamos la propuesta para Implementación de servicios de infraestructura.

Muchas gracias por permitirnos presentarle nuestros servicios y lógicamente estamos dispuestos a aclarar cualquier inquietud.

Cordialmente,

Juan José Enríquez S.

jenriquez@hermesgroup.com.ec

Consultor de Infraestructura

Hermes Express

Implementación de Servicios de Infraestructura.

Preparado para

Hermes Express

miércoles, 13 de enero de 2010

Versión 1.0

Preparado por

Juan José Enríquez S.

Consultor de Infraestructura

jenriquez@hermesgroup.com.ec

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
13/01/2010	Juan José Enríquez	1.0	Propuesta Inicial

Reviewers

Name	Version approved	Position	Date

Propuesta técnica

Implementación de Servicios de Infraestructura

2.1 Antecedentes

Requerimientos planteados por el cliente

1. Ofrecer los servicios profesionales para la Implementación de Servicios de Infraestructura sobre la plataforma Microsoft.
2. Definir procedimientos seguros que garanticen la continuidad de los servicios de red y faciliten la transición a la nueva arquitectura.
3. Definir conjuntamente con Hermes Express, políticas unificadas de administración que garanticen la disponibilidad de los servicios, mejoramiento de procesos y manejo de contingencias para la etapa de transición a la nueva arquitectura.
4. Transferencia de conocimiento para las tareas de administración de la nueva plataforma.

2.2 Servicios

Descripción de los servicios a prestar en este proyecto

Diseño de la arquitectura de Windows Server 2003

Se realizará el diseño de la plataforma Windows Server teniendo en cuenta aspectos como:

1. Visionamiento

Definición de alcances, objetivos, estrategias y entregables para el proyecto. Durante esta etapa también se definen cronogramas de trabajo, recursos y equipos de trabajo.

2. Planeación y Diseño

2.1. Análisis de la situación actual

Levantamiento te información del estado actual de la infraestructura de Windows, como servicios, estructura, conectividad, etc.

2.2. Planeación de la estructura de Bosque

Se analizarán las consideraciones necesarias para definir la estructura de bosque de la organización. Este análisis incluye la revisión de la situación actual de la Entidad y sus oficinas, y las posibles necesidades de integración al nivel de directorio que se puedan presentar en el corto y mediano plazo. Se incluyen aquí también las condiciones o recomendaciones en las cuales se debería agregar, suprimir o modificar esta estructura con nuevos dominios o controladores de dominio.

Un bosque (*forest)* es una colección de dominios y árboles de dominios (*domain trees)* que define los límites de replicación y seguridad de Windows 2000 – el directorio no puede ser más grande que el bosque.

2.3. Diseño lógico del dominio

En esta actividad se definirán las condiciones concretas de la estructura organizacional básica del Directorio Activo. El dominio es la unidad básica de la estructura lógica del *Active Directory*. Los dominios representan una partición lógica de seguridad y administración dentro del servicio de directorios.

Cada dominio requiere al menos un controlador de dominio. Cada controlador de dominio de un *bosque* dado, comparte el *schema* e información de configuración del *bosque* donde reside.

En este punto también se incluirá el diseño de nombres de dominio los dominios del servicio de directorio son nombrados con nombres DNS. Los dominios no pueden ser renombrados una vez creados, por lo que es importante determinar el nombre apropiadamente al momento de diseño.

2.4. Diseño de Unidades Organizacionales

En este punto se definirán las estructuras de Unidades Organizacionales y se propondrá una jerarquía básica significativa, acorde con la estructura de la Entidad, la topología del dominio y los requerimientos de seguridad básicos. Aquí se considera también la estructura requerida en cuanto a denominación de los diferentes objetos se refiere (convenciones de nombre).

Las unidades organizacionales son objetos del directorio que sirven como contenedores para otros objetos del directorio. Las unidades organizacionales pueden contener los siguientes tipos objetos:

- Usuarios
- Grupos
- Estaciones de trabajo
- Impresoras
- Carpetas compartidas
- Otras unidades organizacionales.

Las unidades organizacionales permiten organizar los objetos del directorio lógicamente. Cuando existen múltiples dominios cada dominio tiene su propia estructuración de OUs.

2.5. Diseño políticas de grupo

Las políticas de grupos y usuarios son el medio principal para la personalización de los puestos de trabajo y entornos de trabajo de los Usuarios bajo Windows 2003.

Será parte del alcance de este proyecto las consideraciones asociadas al uso de GPOs para el diseño de Active Directory. No se realizarán actividades en cuanto al diseño detallado de las políticas sino que solamente se tomará en cuenta su impacto a efectos del diseño lógico y físico.

2.6. Diseño físico del directorio activo

Teniendo en cuenta las redes de comunicaciones y los requerimientos de seguridad, se hará la definición de la topología de Sites para los sitios geográficos comprometidos en el proceso de actualización de los sistemas de información de Hermes Express

Esta actividad define la manera en que se aprovechará la estructura actual de red disponible para que el directorio activo no impacte las operaciones de negocio con tareas de replicación pero a la vez mantenga su disponibilidad y tolerancia a fallas. Esta tarea incluye:

- Definición de sites, site links y objetos de conexión.
- Horarios de replicación
- Tipos de links y conexiones
- Distributed File System (DFS)

2.7. Localización de Controladores de Dominios y Global Catalog Server

Los controladores de dominio del dominio serán los responsables de responder a los login de usuarios y consultas al directorio.

El Global Catalog Server almacena todos los objetos del forest con solo un conjunto de atributos, con el objetivo de incrementar el desempeño en la búsqueda de los objetos del forest.

Dentro del alcance del presente proyecto se definirán las ubicaciones necesarias para la implementación de DCs y GCs.

2.8. Operations Master Roles

Los *Operation master roles* controlan las actualizaciones críticas al servicio de directorio que se realizan en modo master, es decir, se escribe la actualización en el domain controller

configurado para esa función y este realiza la replicación hacia los demás controladores de dominios.

La localización de los *Operation master roles* debe ser considerada.

Los *Operation master roles* a considerar son:

- Schema Master
- Domain Naming
- PDC
- RID Master
- Infrastructure Master

2.9. Plan de servicios básicos de red

Se revisarán los servicios asociados con el funcionamiento básico de la entidad, tales como DNS, DHCP, WINS

- Diseño de los espacios de nombres DNS interno y externos de acuerdo con el diseño de directorio activo.
- Definición de los planes de contingencia para los diferentes servicios implementados en la plataforma dentro del proyecto.

3. Desarrollo

3.1. Laboratorio de pruebas

En esta fase se realiza una implementación fuera del área de producción para probar las configuraciones y diseños preliminares.

También se tomarán en cuenta listas de verificación de procedimientos y procesos para realizar la implementación del diseño elaborado en la etapa anterior.

4. Estabilización

4.1. Implementación de Servicios

Después de finalizar la etapa de pruebas se realiza la implementación de los servicios en el servidor que va a ser utilizado en producción, en base a los diseños realizados, incluyendo la implementación de las políticas diseñadas.

Diseño de la arquitectura de Exchange Server 2007

Se realizará el diseño de la plataforma Windows Server teniendo en cuenta aspectos como:

1. Visionamiento

Definición de alcances, objetivos, estrategias y entregables para el proyecto. Durante esta etapa también se definen cronogramas de trabajo, recursos y equipos de trabajo.

2. Planeación y Diseño

2.1. Análisis de la situación actual

Levantamiento te información del estado actual de la infraestructura de Windows, como servicios, estructura, conectividad, etc.

2.2. Definición de arquitectura

En base a la información recolectada se define la arquitectura apropiada para la organización, Front-End / Back-End

2.3. Definición de topología del sistema

De acuerdo con la estructura de la red de datos, las políticas administrativas y operacionales de Hermes Express, se definirá la topología de conectores, ubicación de servidores y demás aspectos de configuración del nuevo sistema de mensajería. La topología define también los mecanismos de

comunicación de correo dentro de la empresa así como con Internet y otros medios que la empresa defina.

2.4. Definición de otros aspectos de configuración

Se definirá otros aspectos de la configuración de Exchange requeridos para la migración, tales como:

- Protocolos a utilizar entre servidores y en interacciones cliente-servidor
- Almacenamiento (Storage Groups) requeridos para la óptima recuperabilidad de datos y disponibilidad de la información.
- Configuración de hardware para lograr la óptima configuración del sistema.
- Plan de implementación que permita identificar las actividades requeridas para la instalación minimizando el impacto en los servicios y minimizar los riesgos durante la implementación.

2.5. Protocolos y Servicios

Con el servidor Front-End se pueden prestar servicios de HTTP, MAPI, RPC sobre HTTP, OMA, Windows Mobile. Además este servidor se puede encargar de manejar el tráfico SMTP externo. En esta etapa se definen los protocolos a utilizarse dependiendo de la infraestructura actual y de las características de los equipos.

3. Desarrollo

3.1. Laboratorio de pruebas

En esta fase se realiza una implementación fuera del área de producción para probar las configuraciones y diseños preliminares.

4. Estabilización

4.1. Implementación de Servicios

Después de finalizar la etapa de pruebas se realiza la implementación de los servicios en el servidor que va a ser utilizado en producción, en base a los diseños realizados, incluyendo la implementación de las políticas diseñadas.

Diseño seguridad Perimetral

Diseño de la arquitectura de ISA Server 2006

Se realizará el diseño de la plataforma Windows Server teniendo en cuenta aspectos como:

1. Visionamiento

Definición de alcances, objetivos, estrategias y entregables para el proyecto. Durante esta etapa también se definen cronogramas de trabajo, recursos y equipos de trabajo.

2. Planeación y Diseño

2.1. Análisis de la situación actual

Levantamiento te información del estado actual de las comunicaciones, protocolos, proveedores de Internet, Zona desmilitarizada DMZ, redes actuales, publicación de servidores, etc.

2.2. Definición de arquitectura

En base a la información recolectada se define la arquitectura apropiada para la organización, ya sea Perimetral, Back to back, o adaptador de red único.

2.3. Definición de topología del sistema

De acuerdo con la estructura de la red de datos, las políticas administrativas y operacionales de ICTSI, se definirá la topología adecuada tomando en cuenta que se pueden tener las siguientes topologías:

Perímetro de 3 secciones.

- Firewall perimetral.
- Firewall Frontal
- Firewall Posterior (Servidor de servicios de fondo).

2.4. Definición de otros aspectos de configuración

Se definirá otros aspectos de la configuración de ISA Server 2006 requeridos para la implementación, tales como:

1.1 Características y configuración de Caché

- Almacenamiento en caché jerárquico.
- Caché inversa.
- Almacenamiento en caché programado.
- Comercio electrónico y publicación rápidos y escalables
- Publicación segura en Web.
- Publicación segura en el servidor de aplicaciones.

1.2 Características y servicios de un Firewall

- Directiva de acceso a la red externa.

- Detección de intrusiones
- Filtros de aplicación
- Compatibilidad con VPNs

.

2.5. Protocolos y Servicios

Con el servidor ISA Server 2006 se pueden tener el control de tráfico de todos los protocolos y puertos que Hermes Express permite, tanto en tráfico de salida como de entrada, según la topología que de detalle en el diseño, ISA 2006 podrá interactuar con otra herramienta firewall si fuese necesario.

3. Desarrollo

3.1. Laboratorio de pruebas

En esta fase se realiza una implementación fuera del área de producción para probar las configuraciones y diseños preliminares.

4. Estabilización

4.1. Implementación de Servicios

Después de finalizar la etapa de pruebas se realiza la implementación y configuración de las reglas necesarias para el control de tráfico, utilización de Caché y publicación de servidores.

2.3 Estrategia

La estrategia con la cual se enfrentará esta iniciativa de tecnología se basa en las responsabilidades asignadas a cada uno de los roles del proyecto, según Microsoft Solutions Framework. Estas responsabilidades se resumen en el siguiente cuadro, donde se ha identificado los roles asignados a Hermes Express y a Juan José Enríquez.

Rol	Responsabilidades
Gerente de Producto (Hermes Express)	▪ Priorizar requerimientos de negocio ▪ Presentar usuarios calificados para suministrar especificaciones al equipo ▪ Asegurar que las especificaciones funcionales cumplen con las expectativas de negocio ▪ Administrar las comunicaciones externas del proyecto
Gerente de Programa (Hermes Express con Asesoría de Juan José Enríquez)	▪ Confirmar avance y administración de planes de trabajo de todos los roles del proyecto ▪ Implementar control de cambios sobre el documento de especificaciones funcionales ▪ Coordinar revisiones con los responsables de cada rol, en los puntos clave del proyecto (Hitos). ▪ Asignación de Recursos
Arquitecto de Infraestructura	▪ Definir la Arquitectura de Hardware y Software de la Solución asegurando su estandarización e integración. ▪ Liderar la implementación de la Prueba de Arquitectura confirmando escalabilidad de tecnología y negocio. ▪ Revisar implementación de funcionalidad crítica dentro de la

	Prueba de Arquitectura, ▪ Definir las recomendaciones relativas al Plan de Capacidad de la Infraestructura de Hardware y Software de Base ▪ Definir la implementación de los procesos mínimos de seguridad de acceso a la información, identificación, autenticación, autorización y rasgos de auditoria
Infraestructura (Hermes Express)	▪ Asegurar una transición simple de desarrollo a producción y operación en coordinación con Arquitecto ▪ Construir planes de salida a producción, instalación y soporte en coordinación con Arquitecto
Usuario Experto (Hermes Express)	▪ Definir las especificaciones funcionales de la solución por medio de casos de uso conjuntamente con los consultores de Intergrupo ▪ Participar en pruebas de usabilidad

Plan de trabajo del proyecto

	Actividad	Tiempo Total
		(Horas)

1.	Visionamiento	6
2.	Planeación y Diseño	
2.1.	Windows 2003 – Active Directory	12
2.2.	Exchange 2007	24
2.3.	Red Perimetral	12
3.	Desarrollo	
3.1.	Windows 2003 – Active Directory	10
3.2.	Exchange 2007	16
3.3.	Red Perimetral	10
4.	Estabilización	
4.1.	Windows 2003 – Active Directory	3
4.2.	Exchange 2007	5
4.3.	Red Perimetral	4
	Total	**102**

Propuesta económica

Diseño de Arquitectura

3.1 Costo de los servicios

Horas	DETALLE	Valor
102	Implementación de Servicios de Infraestructura	$ 3570 USD

* Los valores no incluyen IVA

** La propuesta tiene una validez de 15 días

3.3 Garantía

Se ofrece una garantía de 30 días sobre el funcionamiento de la solución ofrecida siempre y cuando se conserven los mismos parámetros de diseño e implementación definidos en el proyecto (servidores, configuración, etc.)

5.2 PRESENTACIÓN DE RESULTADOS DE LA ENCUESTA IOM


Vista de Tecnología
Administración de Identidades & control de Acceso
Administración de Estaciones
Seguridad, Redes y Monitoreo
Protección y recuperación de Datos
Mensajería y Colaboración Segura
Básica
Estandarizada
Racionalizada
Dinámica


Mensajería y colaboración Segura
Correo
Agendas, Contactos, Tareas
Firmas Digitales
Herramientas Confidencialidad Información
Acceso seguro via WEB
Acceso Seguro Via Dispositivos Móviles
Antivirus Mensajeria
Publicación segura de Servicios en Internet
Librerias, Discusiones, Documentos compartidos


Backup y Recuperación Datos
Backup solo en servidores criticos
Backup para servidores (80% o mas)
Backup central para Estaciones y datos de usuario
Backup Estaciones de Trabajo
Imágenes para recuperación Manual de PCs (80%)
Imágenes para recuperación Automática de PCs (80%)
Imágenes para recuperación Automática de Servidores (80%)
Backup configuraciones de usuario
Cluster para misión Crítica


Redes, Seguridad, Monitoreo
Acceso Usuarios internos Vía VPN
IPSEC
RAS
DCHP
DNS
WINS
PKI
Integración Servicios de Red al Directorio
Análisis de Capacidad y de rendimiento
Monitoreo centralizado de eventos (80% servidores)
Reglas de monitoreo
Seguimiento a Eventos


Redes, Seguridad , Monitoreo
Bases de Conocimiento
Correlación de Eventos
Generación de alertas
Escalamiento de alertas
Consolas de gestión
Tableros de control Monitoreo
Directorios para el 80% o mas
Firewalls Personales (80% o mas)
Detección de Intrusos
Firewall perimetral
Seguridad en Wireless con AD
Encripcion de Archivos


Administracion de Estaciones
Distribución automática de Software
Imágenes estándares de Estaciones (80% o mas)
Instalación automática de Imágenes
Inventarios SW y HW
Estadísticas tendencia de uso de SW
Herramientas de Help Desk
Distribución automática de parches para 100%
Cuarentena estaciones
Antivirus (80% o mas)
Versiones N-1 De Windows (80% o mas)
Office 2003 o mayor 80%

Administración Identidades y Acceso

Políticas de Grupo
Sistema de Directorio Activo (80% o mas)
Sistema de Aprovisionamiento
Políticas para autenticación
Auditorias acceso a la red
Passwords Seguros o fuertes
Plantillas de Seguridad

Procesos y manejos de TI

Persona encargada de procesos de seguridad y manejo de riesgos
Persona define procesos seguridad
Manejo de riesgos de seguridad
Respuestas a incidentes
Identidad de usuarios, dispositivos o servicios
Controles de Antivirus
Deployar las actualizaciones de seguridad para dispositivos conectados a la red
Políticas de seguridad para dispositivos conectados a la red
Revisión de seguridad para la adquisición de SW
Clasificación control de seguridad de datos

ITIL/COBIT

Manejo y operación de la infraestructura

Recomendaciones

- Mensajería y Colaboración:
  - Implementar un servidor de Correo con Dominio
  - Implementar Certificados digitales para el acceso al servicio de OWA
  - Implementar firmas digitales para asegurar la identidad del remitente y la integridad del documento.

Recomendaciones

- Mensajería y Colaboración:
  - Implementar firmas digitales para asegurar la identidad del remitente y la integridad del documento.
  - Implementación de una solución de colaboración documental
  - Implementar un sistema de antivirus para el correo

Recomendaciones

- Backup y Recuperación de datos
  - Implementar políticas y mecanismos de respaldo para las PCs de los usuarios
  - Establecer mecanismos para asegurar datos y configuraciones de los PCs
  - Implementar solución de respaldo de información de usuarios
  - Crear imágenes de Servidores y estaciones como solución de respaldo y recuperación de manera automática

Recomendaciones

- Administración de estaciones
  - Analizar la utilización de herramientas de distribución del software y deployment de Sistema Operativo, esto permitirá bajar los costos de operación
  - La empresa debe conocer sus Activos de Software y Hardware, por tal motivo es importante que cuente con un sistema que permita de manera automática obtener reportes de dichos recursos.
  - Implementación de políticas de grupo para administrar y controlar el escritorio de los usuarios

Recomendaciones

- Administración de estaciones
  - Evaluar mecanismos para distribución automática de software y parches.
  - Implementar una herramienta de directorio que permita administrar de forma centralizada las configuraciones y seguridad de sus PC's (ej. Políticas de Grupo)
  - Estandarizar a un sistema de antivirus en todas las PCs y Servidores y su vez centralizar las actualizaciones del sistema antivirus

Recomendaciones

- Redes, Seguridad y Monitoreo
  - Implementar servicios de VPN´s para clientes móviles, esto dar una valor agregado al negocio.
  - Es mandatorio implementar una solución de seguridad perimetral que permita hacer cache, VPN´s y mantener servicios que requieren se expuestos al Internet de manera confiable.
  - Aprovechar funcionalidades como IPSEC para asegurar tramos críticos en la red de datos.
  - Mantener una base de conocimiento de eventos y resolución de problemas

Recomendaciones

- Redes, Seguridad y Monitoreo
  - Evaluar la utilización de firewalls locales en las estaciones de trabajo, implementados mediante GPO's
  - Implementar un plan, para gestionar la capacidad de operación de servidores
  - Implementar Infraestructura de Claves públicas para el manejo de certificados digitales
  - Publicar los recursos de red en el directorio activo
  - Implementar una solución de monitoreo de servicios críticos

Recomendaciones

- Redes, Seguridad y Monitoreo
  - Mantener una base de conocimiento de eventos y resolución de problemas
  - Habilitar políticas y herramientas de auditorias sobre el uso de las redes.
  - Implementar DNS y DHCP
  - Implementar directorios en el servidor para cada uno de los usuarios permitiendo así centralizar la información.

Recomendaciones

- Redes, Seguridad y Monitoreo
  - Utilizar Escritorio Remoto para movilidad y soporte
  - Establecer mecanismos y herramientas de Monitoreo centralizado de servicios en la plataforma Windows Con capacidades como las ofrecidas por MOM

Recomendaciones

- Administración de Identidades
  - Utilizar plantillas de objetos en directorio activo
  - Revisar plantillas de seguridad basado en rol de servidores
  - Uso intensivo de Políticas de Grupo.
  - Auditar el uso de los recursos en la red mediante políticas de directorio y herramientas.
  - Implementar una política de manejo de contraseñas (contraseñas fuertes, expiración, historial de contraseñas).

Recomendaciones

- Administración de Identidades
  - Implementar Directorio Activo
  - Definir auditorias de acceso a la red evitando así en ingreso de intrusos a la red.

Recomendaciones

- Procesos de Manejo IT
  - Implementar un control sobre el manejo de incidentes, problemas y generar conocimiento escrito de cómo se ha resuelto
  - Establecer un procedimiento de respuesta a incidentes y escalación de los mismos
  - Definir un procedimiento para creación y borrado de usuarios en los sistemas
  - Permisos específicos de acceso
  - Designar una persona encargada del departamento de IT de la empresa

Recomendaciones

- Procesos de Manejo IT
  - Estableces una política se seguridad para dispositivos conectados a la red
  - Establecer un procedimiento para la adquisión de software y análisis de seguridad
  - Implementación de la solución para establecer seguridad a nivel documental y establecer

Recomendaciones

- ITIL/COBIT
  - La operación de la plataforma debe basarse en mejores prácticas internacionales a fin de garantizar el buen funcionamiento de la misma
  - Estudiar la posibilidad de adoptar ITIL, MOF entre otras

Siguientes pasos

- Establecer las áreas donde se desea hacer foco
- Revisión detallada de Hallazgos & recomendaciones
- Definición prioridades
- Establecimiento de plan de trabajo para
  - 3 meses
  - 6 meses
  - 1 año
- Definición de responsables

5.3 RESULTADOS DE LA ENCUESTA IOM

A continuación se muestra el archivo entregable al cliente sobre los resultados de la encuesta realizada

Quito, 13 de enero de 2010

Señor

Rubén Enríquez

Presidente

HERMES EXPRESS

Ciudad.-

REFERENCIA: Resultados y Recomendaciones del Modelo IOM Ejecutado en HERMES EXPRESS.

Apreciado señor:

Adjunto encontrarán los resultados y recomendaciones que sacamos a partir de la ejecución del Modelo IOM que se realizó en días pasados en HERMES EXPRESS.

Cordialmente,

Juan José Enríquez

jenriquez@hermesgroup.com.ec

Consultor de Infraestructura

IOM

Resultados y recomendaciones del modelo IOM (Infraestructure Optimization Model) ejecutado en HERMES EXPRESS

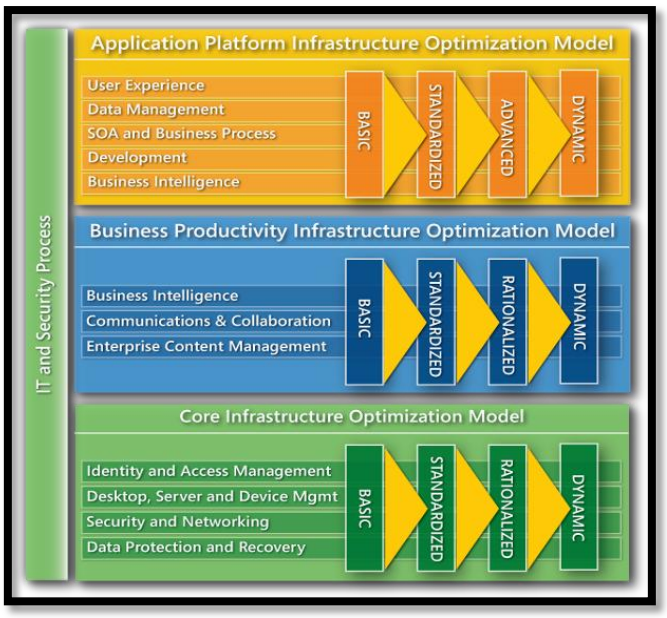
Descripción del Modelo

Para medir y ayudar a los clientes a optimizar y asegurar su Infraestructura tecnológica, crear agilidad y reducir costos, Microsoft ha desarrollado tres modelos de optimización basado en la Industria y análisis de trabajo. La optimización de Infraestructura puede ser vista en tres perspectivas:

- Optimización del Core de Infraestructura
- Optimización de la Infraestructura de Productividad y Negocios
- Optimización de Infraestructura de Plataforma de aplicación

En este documento nos enfocaremos en la optimización del CORE de infraestructura. Esta plataforma está compuesto por diferentes procesos que fueron calificados independientemente, es decir que cada uno se ubicará en uno de los 4 niveles del modelo. Los procesos involucrados en la optimización del CORE de infraestructura son:

- Administración de Identidades y Acceso
- Administración de Estaciones, Dispositivos y Servidores
- Seguridad, Redes y Monitoreo
- Protección y Recuperación de Datos
- Mensajería y Colaboración Segura
- Procesos y Manejos de IT



El Modelo define 4 niveles de optimización: (Básico, Estandarizado, Racionalizado y Dinámico) para cada una de las capacidades de IT. Las características de estos niveles de optimización son las siguientes:

1. **Básico -** Este nivel está caracterizado por tener procesos localizados y manuales, control central minino y la no existencia de políticas y estándares de IT respecto a seguridad, respaldos, administración, desarrollo de imágenes, niveles de cumplimiento y otros estándares de IT comunes. En general hay ausencia de conocimiento con respecto a la Infraestructura que se tiene en el lugar o cuales tácticas tendrán el máximo impacto sobre estas. En general la salud de aplicaciones y servicios es desconocida por la ausencia de herramientas y recursos, además de no existir un medio para la comparación de conocimiento acumulado en IT. Empresas con Infraestructura Básica, encuentran sus ambientes extremadamente difíciles de controlar teniendo altos costos en la administración de escritorios y servidores siendo muy reactivos a brechas de seguridad. Estas empresas tienen un mínimo impacto positivo sobre la habilidad de beneficiar al negocio desde IT. En General, todos los ajustes en Infraestructura, implementación de software, servicios, proveen un alto impacto y altos costos.

2. **Estandarizado –** Este nivel introduce control a través del uso de estándares y políticas en el manejo de escritorio, dispositivos móviles y servidores, y como estos elementos son introducidos en la red. Aquí ya se utiliza servicios de directorio para administrar recursos, políticas de seguridad y control de accesos. Generalmente todos los ajustes, implementación de software y servicios de escritorio son provistos con un impacto medio y un costo entre medio y alto. Por otro lado las empresas en este nivel poseen un razonable inventariado de Software y Hardware y están iniciándose en la administración de licencias. La medida de seguridad es provista con el bloqueo de la zona perimetral, aunque la seguridad interna puede aún estar en riesgo.

3. **Racionalizado -** En este nivel es donde los costos involucrados en la administración de escritorio y servidores están entre los más bajos, los procesos y políticas han sido optimizados para empezar a jugar un rol importante en el soporte y expansión de negocios. La seguridad es muy pro activa y la respuesta hacia amenazas y cambios es rápida y controlada. El no tener impacto en implementaciones ayuda a minimizar costos, tiempo de implementación. El número de imágenes es minino y el proceso de administración de escritorio tiene un costo muy bajo. La empresa tiene un inventariado de Software y Hardware limpio y únicamente adquiere computadoras y licencias que necesita. La seguridad aquí es extremadamente proactiva con estrictas políticas y control desde maquinas de escritorio, servidores hasta firewalls y extranets.

4. **Dinámico –** Las empresas con infraestructura dinámica son completamente conscientes del valor estratégico que su infraestructura provee, ayudándoles a correr sus negocios eficientemente y manteniéndose a la cabeza respecto a sus competidores. Los Costos son completamente controlados existiendo integración entre: usuarios, datos, desktops y servidores; la colaboración entre usuarios y departamentos es intensa, los usuarios móviles tiene fácilmente niveles de servicio y capacidades sin importar su ubicación. Los procesos son completamente automatizados y siempre incorporados dentro de la tecnología como tal, permitiendo a IT estar alineados y administrados de

acuerdo a las necesidades del negocio. Adicionalmente las inversiones en tecnología es de manera específica, rápida y medible para las necesidades del negocio. El uso de aprovisionamiento autónomo de software y sistemas de cuarentena para el aseguramiento en la administración de actualizaciones de seguridad acompañados a políticas de seguridad permiten a las organizaciones automatizar procesos, así ayuda a proveer fiabilidad, bajar costos e incrementar los niveles de servicio.

Resultados

Administración de Identidades y Control de Acceso: Básico

En este proceso se ha evaluado las siguientes variables:

- Active Directory para el 80% de usuarios
- Políticas de Grupo
- Solución basada en directorio para proteger contenido
- Sistema de Aprovisionamiento
- Herramienta basada en directorio para accesos autentificados a cuentas de usuarios

El resultado del análisis refleja el siguiente estado:

- Active Directory para el 80% de usuarios: **No tiene**
- Políticas de Grupo: **No tiene**
- Solución basada en directorio para proteger contenido: **No tiene**
- Sistema de Aprovisionamiento: **No tiene**
- Herramienta basada en directorio para accesos autentificados a cuentas de usuarios: **No tiene**

Administración de Estaciones, Dispositivos y Servidores: Básico

Este proceso comprende las siguientes variables:

- Distribución automática de actualizaciones para el 80% de PC's
- Imágenes estándares para el 80% de PC's
- Imágenes estándares para el 80% de laptops
- Solución centralizada para actualización de dispositivos móviles
- Solución para protección de datos si se pierde dispositivos móviles
- Solución de imágenes que incluya antivirus, SO, herramientas de productividad
- Plan para manejar máximo 2 versiones de SO en 80% de PC's

- Distribución automática de software 80% PC’s
- Seguimiento automatizado de software y hardware en 80% de PC’s
- Windows XP o 2000 en 80% de PC’s
- Windows XP con SP2 en 80% de PC’s
- Versión de Office 2003 o mayor en 80% de PC’s
- Pruebas de certificación para distribuciones de software en 80% de PC’s
- Manejo de solución de actualizaciones para el 80% de sus servidores
- Manera segura para verificar comunicaciones entre la red corporativa y los dispositivos móviles
- Accesos WEB vía WAP o HTTP para dispositivos móviles
- Consolidación de servidores mediante la virtualización
- Imágenes anidadas para las imágenes de PC’s
- Estandarizado N o N-1 versiones de S.O. para PC’s
- Analizador de capacidades para servicios corporativos
- Solución para actualizar las características y aplicaciones de dispositivos móviles
- Solución de actualizaciones automáticas para dispositivos móviles
- Virtualización para mover el flujo de carga entre servidores

El resultado del análisis refleja el siguiente estado:

- Distribución automática de actualizaciones para el 80% de PC’s: **No tiene**
- Imágenes estándares para el 80% de PC’s: **No tiene**
- Imágenes estándares para el 80% de laptops: **No tiene**
- Solución centralizada para actualización de dispositivos móviles: **No tiene**
- Solución para protección de datos si se pierde dispositivos móviles: **No tiene**
- Solución de imágenes que incluya antivirus, SO, herramientas de productividad: **No tiene**
- Plan para manejar máximo 2 versiones de SO en 80% de PC’s: **No tiene**
- Distribución automática de software 80% PC’s: **No tiene**

- Seguimiento automatizado de software y hardware en 80% de PC's: **No tiene**
- Windows XP o 2000 en 80% de PC's: **Racionalizado**
- Windows XP con SP2 en 80% de PC's: **Racionalizado**
- Versión de Office 2003 o mayor en 80% de PC's: **Racionalizado**
- Pruebas de certificación para distribuciones de software en 80% de PC's: **No tiene**
- Manejo de solución de actualizaciones para el 80% de sus servidores: **No tiene**
- Manera segura para verificar comunicaciones entre la red corporativa y los dispositivos móviles: **No tiene**
- Accesos WEB vía WAP o HTTP para dispositivos móviles: **No tiene**
- Consolidación de servidores mediante la virtualización: **No tiene**
- Imágenes anidadas para las imágenes de PC's: **No tiene**
- Estandarizado N o N-1 versiones de S.O. para PC's: **Racionalizado**
- Analizador de capacidades para servicios corporativos: **No tiene**
- Solución para actualizar las características y aplicaciones de dispositivos móviles: **No tiene**
- Solución de actualizaciones automáticas para dispositivos móviles: **No tiene**
- Virtualización para mover el flujo de carga entre servidores: **No tiene**

Seguridad, Redes y Monitoreo: Básico

En este entorno se evaluaron las siguientes variables:

- Antivirus en el 80% de sus PC's
- Firewall centralizado 80% de sus sistemas
- DHCP
- DNS
- Monitoreo del 80% de sus servidores críticos
- Firewall con políticas de administración en 80% de servidores
- Firewall con políticas de administración en 80% de PC's
- Acceso seguro a recursos internos (VPN)
- IPSEC

- Monitoreo de SLA para el 80% de servidores
- Mecanismo de comunicación segura
- Red inalámbrica segura con Active Directory e IAS/RADIUS para autentificación
- PKI
- Optimización WAN
- Solución para mitigación de amenazas
- Solución de cuarentena

El resultado del análisis refleja el siguiente estado:

- Antivirus en el 80% de sus PC's: **No tiene**
- Firewall centralizado 80% de sus sistemas: **No tiene**
- DHCP: **No tiene**
- DNS: **No tiene**
- Monitoreo del 80% de sus servidores críticos: **No tiene**
- Firewall con políticas de administración en 80% de servidores: **No tiene**
- Firewall con políticas de administración en 80% de PC's: **No tiene**
- Acceso seguro a recursos internos (VPN): **No tiene**
- IPSEC: **No tiene**
- Monitoreo de SLA para el 80% de servidores: **No tiene**
- Mecanismo de comunicación segura: **No tiene**
- Red inalámbrica segura con Active Directory e IAS/RADIUS para autentificación: **No tiene**
- PKI: **No tiene**
- Optimización WAN: **No tiene**
- Solución para mitigación de amenazas: **No tiene**
- Solución de cuarentena: **No tiene**

Protección y Recuperación de Datos: Estandarizado

Se evaluaron las siguientes variables:

- Solución de Backup y Restore para 80% de servidores críticos
- Backup centralizado
- Backup y Restore vía SLA

El resultado del análisis refleja el siguiente estado:

- Solución de Backup y Restore para 80% de servidores críticos: **No tiene**
- Backup centralizado: **No tiene**
- Backup y Restore vía SLA: **No tiene**

Procesos y Manejos de IT: Básico

Se evaluaron las siguientes variables:

- Persona encargada de procesos de seguridad y manejo de riesgos
- Manejo de riesgos de seguridad
- Respuestas a incidentes
- Identidad de usuarios, dispositivos o servicios
- Controles de Antivirus
- Distribuir las actualizaciones de seguridad para dispositivos conectados a la red
- Políticas de seguridad para dispositivos conectados a la red
- Revisión de seguridad para la adquisición de SW
- Clasificación control de seguridad de datos

El resultado del análisis refleja el siguiente estado:

- Persona encargada de procesos de seguridad y manejo de riesgos: **No tiene**
- Manejo de riesgos de seguridad: **No tiene**
- Respuestas a incidentes: **No tiene**
- Identidad de usuarios, dispositivos o servicios: **No tiene**
- Controles de Antivirus: **No tiene**

- Distribuir las actualizaciones de seguridad para dispositivos conectados a la red: **No tiene**
- Políticas de seguridad para dispositivos conectados a la red: **No tiene**
- Revisión de seguridad para la adquisición de SW: **No tiene**
- Clasificación control de seguridad de datos: **No tiene**

ITIL/COBIT: Racionalizado

Se evaluó lo siguiente:

- Opción que describe mejor la administración y operación de la infraestructura TI

El resultado del análisis refleja el siguiente estado:

- Opción que describe mejor la administración y operación de la infraestructura TI: **No tiene**

Recomendaciones

Administración de Identidades y Control de Acceso

- Utilizar plantillas de objetos en directorio activo
- Revisar plantillas de seguridad basado en rol de servidores
- Uso intensivo de Políticas de Grupo.
- Auditar el uso de los recursos en la red mediante políticas de directorio y herramientas.
- Implementar una política de manejo de contraseñas (contraseñas fuertes, expiración, historial de contraseñas).
- Implementar Directorio Activo
- Definir auditorias de acceso a la red evitando así en ingreso de intrusos a la red.

Administración de Estaciones, Dispositivos y Servidores

- Analizar la utilización de herramientas de distribución del software y deployment de Sistema Operativo, esto permitirá bajar los costos de operación
- La empresa debe conocer sus Activos de Software y Hardware, por tal motivo es importante que cuente con un sistema que permita de manera automática obtener reportes de dichos recursos.
- Implementación de políticas de grupo para administrar y controlar el escritorio de los usuarios
- Evaluar mecanismos para distribución automática de software y parches.
- Implementar una herramienta de directorio que permita administrar de forma centralizada las configuraciones y seguridad de sus PC's (ej. Políticas de Grupo)
- Estandarizar a un sistema de antivirus en todas las PCs y Servidores y su vez centralizar las actualizaciones del sistema antivirus

Seguridad, Redes y Monitoreo

- Implementar servicios de VPN´s para clientes móviles, esto dar una valor agregado al negocio.
- Es mandatorio implementar una solución de seguridad perimetral que permita hacer cache, VPN´s y mantener servicios que requieren se expuestos al Internet de manera confiable.
- Aprovechar funcionalidades como IPSEC para asegurar tramos críticos en la red de datos.
- Mantener una base de conocimiento de eventos y resolución de problemas
- Evaluar la utilización de firewalls locales en las estaciones de trabajo, implementados mediante GPO’s
- Implementar un plan, para gestionar la capacidad de operación de servidores
- Implementar Infraestructura de Claves públicas para el manejo de certificados digitales

- Publicar los recursos de red en el directorio activo
- Implementar una solución de monitoreo de servicios críticos
- Mantener una base de conocimiento de eventos y resolución de problemas
- Habilitar políticas y herramientas de auditorias sobre el uso de las redes.
- Implementar DNS y DHCP
- Implementar directorios en el servidor para cada uno de los usuarios permitiendo así centralizar la información.
- Utilizar Escritorio Remoto para movilidad y soporte
- Establecer mecanismos y herramientas de Monitoreo centralizado de servicios en la plataforma Windows Con capacidades como las ofrecidas por MOM

Protección y Recuperación de Datos

- Implementar políticas y mecanismos de respaldo para las PCs de los usuarios
- Establecer mecanismos para asegurar datos y configuraciones de los PCs
- Implementar solución de respaldo de información de usuarios
- Crear imágenes de Servidores y estaciones como solución de respaldo y recuperación de manera automática

Mensajería y Colaboración Segura

- Implementar un servidor de Correo con Dominio
- Implementar Certificados digitales para el acceso al servicio de OWA
- Implementar firmas digitales para asegurar la identidad del remitente y la integridad del documento.
- Implementar firmas digitales para asegurar la identidad del remitente y la integridad del documento.
- Implementación de una solución de colaboración documental

- Implementar un sistema de antivirus para el correo

Procesos y Manejos de IT

- Implementar un control sobre el manejo de incidentes, problemas y generar conocimiento escrito de cómo se ha resuelto
- Establecer un procedimiento de respuesta a incidentes y escalación de los mismos
- Definir un procedimiento para creación y borrado de usuarios en los sistemas
- Permisos específicos de acceso
- Designar una persona encargada del departamento de IT de la empresa
- Estableces una política se seguridad para dispositivos conectados a la red
- Establecer un procedimiento para la adquisión de software y análisis de seguridad
- Implementación de la solución para establecer seguridad a nivel documental y establecer

Beneficios

Administración de Identidades y Control de Acceso

Beneficios de avanzar al nivel Estandarizado:

- Reducción en el número de identidades digitales, se centralizó la administración de identidades.
- Menor volumen de llamadas al departamento de soporte técnico.
- Mayor seguridad.
- Menores costos de administración de cuentas de usuario.

- Mayor productividad de los usuarios al habilitar una experiencia de inicio de sesión más sencilla.
- Primer paso para implementar sistemas que cumple con las regulaciones.

Beneficios de avanzar al nivel Racionalizado:

- La introducción de la administración basada en roles (políticas de grupo) reduce la carga de trabajo de administración.
- Las investigaciones muestran que al aplicar Políticas de grupo para evitar que los usuarios modifiquen las configuraciones ahorra US$30 a los clientes al año.
- Es posible una administración rápida de cambios y configuraciones.
- Paso importante para establecer una plataforma para implementar sistemas que cumplen con las regulaciones.
- Experiencia consistente del usuario en diversos PCs basados en roles de negocios.
- Realizar cambios al sistema y agregar funcionalidades es muy sencillo.
- Es posible una seguridad mejorada al implementar una administración de revisiones y un bloqueo de seguridad basado en políticas.
- Es posible una recuperación de datos y del sistema del usuario a través de la administración de perfiles.
- Menores costos operativos.
- Menores costos de soporte del escritorio.
- Menores tiempos de paro para el usuario final.
- Menores interrupciones para los usuarios finales.

Beneficios de avanzar al nivel Dinámico:

- Administración centralizada de contraseñas.
- El inicio de sesión único entre múltiples sistemas reduce los costos de administración e incrementa la productividad del usuario. Las investigaciones muestran que los clientes

pueden ahorrar US$29 por PC al implementar un restablecimiento automatizado de contraseñas entre los sistemas.

- Puesta en servicio / anulación de la misma de la cuenta automatizada de identidades y administración del ciclo de vida.
- Menores costos de administración debido a la administración de menos almacenes de identidades.
- Varios depósitos de identidades están conectados, federados dentro del firewall o son confiables para permitir la puesta en servicio del flujo de trabajo de identidades.
- Menores costos de soporte y menores tiempos de paro del usuario final.

Administración de Estaciones, Dispositivos y Servidores

Beneficios de avanzar al nivel Estandarizado:

- Construcciones y experiencia de escritorio consistentes en toda la organización.
- La estandarización del sistema operativo reduce los costos de administración y eleva la productividad del usuario (las investigaciones muestran que los clientes pueden ahorrar US$52 por escritorio al implementar una sola imagen de sistema operativo de escritorio).
- Experiencia mejorada para el usuario.
- Procesos optimizados de soporte.
- Establecimiento de estándares de H/W y S/W y del ciclo de vida.
- Implementación más rápida y más económica.
- Mayor productividad.
- Mejores niveles de Seguridad del escritorio.
- Reducción en el volumen de llamadas al Departamento de soporte técnico y menores costos para el Departamento de soporte técnico.
- Mayor éxito de soporte de primer nivel.
- Aumento de la confianza del usuario en el Departamento de soporte técnico.
- Tiempos de respuesta más rápidos a incidentes.

- Menos Interrupción del usuario.
- Menor costo de Implementación por PC.
- Menores Costos operativos.
- Menores costos de Administración de revisiones.
- Menor riesgo de Amenazas a la seguridad.
- Las adquisiciones centralizadas beneficiarán al Costo total de propiedad (TCO).

Beneficios de avanzar al nivel Racionalizado:

- Entorno de escritorio Móvil, Seguro, Administrado centralmente.
- Mayor capacidad para automatizar la implementación de escritorios nuevos, reconstrucciones de escritorio y migraciones de usuario.
- Aumentan los niveles de seguridad en el escritorio y el departamento de TI los administra de manera más eficiente.
- El Departamento de soporte técnico cambió de Reactivo a Proactivo con tiempos de respuesta más rápidos, y cuenta con acceso remoto a las máquinas de los usuarios para realizar diagnósticos y brindar soluciones.
- Una experiencia consistente del perfil del escritorio para usuarios móviles, tanto dentro como fuera de la red (Marcas, Mis documentos, apariencia del Escritorio). Al estandarizarse en Windows XP SP2, se puede conseguir un ahorro del 9% por escritorio al año.
- Menores Tiempos de paro del usuario debido a que sus PCs se mantienen actualizados con las revisiones y actualizaciones más recientes de los Sistemas operativos.
- Medidas de seguridad de defensa profunda ampliamente implementadas.

Beneficios de avanzar al nivel Dinámico:

- Los usuarios invierten menos tiempo con el soporte de primera línea debido a que tanto la aplicación como los Sistemas operativos utilizan pruebas automatizadas antes de su implementarlas en la producción.
- Alto grado de automatización para todos los servicios de TI.

- La Organización de TI se considera como un activo estratégico para el negocio.
- Experiencia de soporte consistente.
- La automatización de los procesos de TI reduce los costos, agrega consistencia.
- La seguridad y estabilidad del entorno del Escritorio es consistente tanto dentro como fuera del firewall corporativo.

Seguridad, Redes y Monitoreo

Beneficios de avanzar al nivel Estandarizado:

- Una infraestructura más estable y segura como resultado de la tecnología de revisiones y seguridad y actividades de revisión que administra de manera central el Departamento de TI.
- Los estándares para políticas proporcionan un entorno más consistente.
- Los clientes mejoran la seguridad de su entorno de escritorio a través de la entrega rápida y confiable de revisiones para vulnerabilidades encontradas en los activos de software.
- Las mediciones de control con estrategia de aplicación proporcionan un esquema estructurado.
- Las 'capas' de seguridad a nivel perímetro, servidor, escritorio y aplicación proporcionan un entorno controlado y robusto listo para soportar los intentos de explosiones.
- La menor complejidad en las operaciones de hardware y software resulta en procesos sin problemas de administración de cambios.
- La configuración eficiente y confiable de la red TCP/IP (Servicios DHCP) ayuda a evitar que la dirección IP entre en conflicto y conserve el uso de las direcciones IP a través de la administración centralizada de asignación de direcciones.
- Se reducen las llamadas al Departamento de soporte técnico como resultado de las explosiones.

Beneficios de avanzar al nivel Racionalizado:

- Se reduce la complejidad asociada con la administración de entornos de infraestructura de TI y se logran menores costos operativos.
- Los empleados tienen la capacidad de utilizar una conexión segura hacia los recursos de la organización sin importar su ubicación.
- El Departamento de TI está vinculado a la empresa a través de SLAs verdaderos.
- Se logra un control substancial sobre la infraestructura a través de procesos de administración efectivos.
- Las políticas y procesos proactivos para seguridad, configuración y administración incrementan la estabilidad.
- Mayor productividad del Departamento de TI, Departamento de soporte técnico y Usuarios como resultado del mejoramiento del 'estado'.
- Administración de activos mejorada de escritorios a nivel H/W y S/W debido a que se cuenta con procesos efectivos de administración.
- Los procesos de Administración de cambios mejoran la estabilidad y el control.
- Los niveles de seguridad se elevan con la administración y supervisión mejorada de la infraestructura del servidor y del cliente.
- Se utilizan Políticas de grupo centralizadas basadas en Active Directory para distribuir Políticas y filtros IPSec, elevando el nivel de seguridad en los PCs de los empleados.
- El Departamento de TI invierte menos tiempo en manejar las crisis y más tiempo en brindar nuevos servicios a la empresa.
- Los servicios de supervisión ayudan a simplificar la identificación de problemas, agilizan el proceso para determinar la causa raíz del problema y facilitan una resolución rápida para restaurar los servicios y evitar problemas potenciales de TI.
- Las políticas IPSec ayudan a elevar la seguridad de los entornos de red al limitar el tráfico que puede ingresar a un servidor.
- Al reducir el número de operaciones de alertas, los trabajadores pueden responder de manera más rápida y efectiva a las que necesitan atención.

Beneficios de avanzar al nivel Dinámico:

- Control y visibilidad rentables sobre todos los PCs individuales.
- Permite que el Departamento de TI resuelva proactivamente problemas antes de que afecten a los usuarios (tales como fallas en el disco duro).
- Se logra una seguridad proactiva con políticas explícitas y control del escritorio, al firewall, a la extranet.
- El Departamento de TI es considerado un socio con valor de negocios.
- Aumenta la productividad del usuario como resultado de un entorno estable y seguro.
- Respuestas proactivas y rápidas a los problemas de seguridad.
- Supervisión y generación de informes absolutos de la infraestructura del Servidor, con capacidades similares para escritorio.
- Se resuelve por completo el cumplimiento con las regulaciones.
- La representación de la empresa se refleja a través de las políticas de seguridad.
- Se entrega a la empresa un esquema completo de seguridad empresarial.
- Los usuarios móviles pueden viajar a varios lugares - salas de reunión, pasillos, cafeterías, etcétera, y siguen teniendo un acceso seguro a los datos y recursos de la red (correo electrónico, Internet, aplicaciones corporativas).

Protección y Recuperación de Datos

Beneficios de avanzar al nivel Estandarizado:

- Una estrategia empresarial de administración de datos impulsa la estabilidad en la organización, mejorando la productividad.
- La introducción de estándares para la administración de datos permite la aplicación de políticas y la definición SLA, mejorando la relación de la empresa con la organización de TI.
- Un enfoque estratégico para la Administración de datos habilita procedimientos de recuperación de datos, brindando soporte a la empresa con una plataforma robusta.

- Primer paso para implementar sistemas que cumplen con las regulaciones.
- La protección de datos de aplicaciones de Misión crítica se mantiene en un lugar seguro fuera de la ubicación del Departamento de IT, así mismo se establecieron políticas básicas que garantizan el acceso a los medios físicos (cintas, dispositivos ópticos) cuando se requiere.

Beneficios de avanzar al nivel Racionalizado:

- Se celebraron Contratos de nivel de servicio entre la Empresa y el Departamento de TI. La Centralización de la administración de datos del usuario y de la aplicación de misión crítica reduce los costos en las operaciones.
- La consolidación de la Administración de datos empresariales habilita procesos de soporte optimizados.
- Evolución hacia el cumplimiento con las regulaciones.
- Rendimiento mejorado de los servicios de respaldo, lo cual estabiliza el entorno, mejorando la productividad.
- Mejor uso de las 'ventanas' de respaldo, manteniendo el proceso de soporte agilizado y minimizando el impacto para la empresa.
- Se logran ahorros de tiempo en las operaciones de respaldo y recuperación de datos.
- Adopción de la tecnología de instantáneas de precisión para respaldo y archivo (Servicios de instantáneas de volumen (VSS). Este servicio, también conocido como toma de 'instantáneas', permite que se copien todas las modificaciones a nivel bloque, lo que protege a los objetos en un servidor de producción desde la última replicación).
- Evolución continúa hacia el Cumplimiento con las regulaciones.

Beneficios de avanzar al nivel Dinámico:

- La flexibilidad de la protección de datos del usuario final mejora la estabilidad y eleva la productividad.

- Una Protección continua de los datos garantiza la continuidad del negocio y la alta disponibilidad al restaurar el acceso a los datos en minutos con capacidades de falla para mantener un entorno de trabajo transparente.
- El cumplimiento con las regulaciones se vuelve una posibilidad.
- Se implementan los Servicios de continuidad de negocios e incluyen: Clasificación de datos, Definición de políticas, Selección de hardware y software, Diseño, implementación y administración, Documentación del proceso, Supervisión de la infraestructura, Administración diaria, Generación de informes y auditoría, Escalación de soporte.

Mensajería y Colaboración Segura

Beneficios de avanzar al nivel Estandarizado:

- Se lograría una seguridad avanzada al contar con un antivirus para la mensajería.

Beneficios de avanzar al nivel Racionalizado:

- Al poder compartir documentos y generar discusiones de manera segura se protege la información y se ahorra tiempo y costo.
- La publicación segura de servicios en Internet ahorra tiempo y costo porque se les está dando la oportunidad a los usuarios de acceder a la información rápidamente y sin intervención del área de IT.
- Menos llamadas al departamento de soporte técnico.

Beneficios de avanzar al nivel Dinámico:

- Se gana movilidad al dar acceso seguro vía Web o dispositivos móviles.
- Se asegura la identidad del remitente por medio de firmas digitales.

Procesos y Manejos de IT

Beneficios de avanzar al nivel Estandarizado:

- La organización está protegida contra riesgos y ofensas al contar con un proceso de manejo de seguridad de información.
- Se ahorra tiempo y se bajarían circunstancialmente las interrupciones a los usuarios al tener previamente establecido un proceso de respuesta a incidentes.
- Se puede garantizar el cumplimiento consistente de políticas de seguridad en los dispositivos conectados a la red en el sitio.

Beneficios de avanzar al nivel Racionalizado:

- Se cuenta con políticas de seguridad de defensa profunda.
- Se sigue un proceso consistente de evaluación de riesgos con personas y otros recursos lo que mejora la seguridad de la información dentro de la organización.
- Se tiene un proceso documentado en el sitio donde las identidades afectadas del usuario/servicio/dispositivo se puedan evaluar de manera consistente.
- Se ahorra tiempo al tener un proceso documentado para identificar y restaurar todas las redes conectadas afectadas.

Beneficios de avanzar al nivel Dinámico:

- Se optimiza la administración de seguridad del servidor Web para una mayor eficiencia, se cuenta en el sitio con todos los Procesos y políticas de seguridad, se impartió una capacitación efectiva y rigurosa de habilidades al personal de TI, se enviaron informes a los dueños de la empresa. Se proporcionó a los dueños de la empresa un análisis del costo/beneficio.

Pasos a Seguir

1. Revisión detallada de hallazgos & recomendaciones.
2. Definición de prioridades.
3. Establecimiento de plan un de trabajo para:
    - 3 meses
    - 6 meses
    - 1 año
4. Definición de responsables.

CAPÍTULO 6
CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Con la evaluación con el modelo IOM se pudo determinar que la Empresa Hermes Express se encuentra en un nivel de madures básico, ya que no cuenta con los principales componentes para que la infraestructura funcione correctamente.
- Mediante el diseño de la red física se pudo determinar cuál sería el diseño más óptimo para las instalaciones de la Empresa Hermes Express.
- Se llego a la conclusión de que al momento de centrar las actualizaciones automáticas de Sistema Operativo, Antivirus, Aplicaciones se pudo reducir en un 60% el uso del internet, ya que el proceso se lo realizaba manualmente haciendo que la conexión a internet sea limitada y lenta.
- Teniendo un optimo servidor de correo electrónico se pudo concluir que es más efectivo trabajar con servidores propios como Exchange Server ya que la información de correos electrónicos se la tiene a cualquier momento, adicionalmente se logró centralizar libreta de direcciones, tareas y el calendario permitiendo así tener un mejor control sobre las citas.
- Se concluyó que teniendo un servidor correctamente configurado de Directorio Activo se pudo restringir el acceso a usuarios externos a los archivos importantes de la empresa, se pudo generar contraseñas seguras para cada usuario, se pudo tener un esquema de políticas que permiten tener más control del sistema operativo por parte del personal de sistemas.
- Teniendo un sistema de flujos de trabajo se pudo centralizar los archivos importantes de la Empresa en un solo servidor, permitiendo así generar políticas de acceso a los diferentes archivos que tiene la empresa evitando así que personas externas a la Empresa o empleados tengan acceso a información sensible.

- Se concluyó que llegando a un nivel dinámico de infraestructura se puede ahorrar a la Empresa en tiempo y en dinero, ya que todos los procesos se los realiza automáticamente y de forma inteligente.
- En la propuesta de servicios presentada a la Empresa Hermes Express se pudo ver claramente que el análisis costo-beneficio es muy optimo ya que con teniendo en cuenta los resultados de la implementación se determino que la empresa ahorraría mucho dinero, reduciendo costos en personal y tiempo.
- Una vez diseñado el esquema de VOIP con software gratuito se determinó que la empresa ahorraría un 60% en costos de telefonía entre sucursales ya que las llamadas dentro de la empresa son gratuitas, adicionalmente se concluyó que utilizando utilitarios gratuitos se puede tener el mismo resultado que adquiriendo aplicativos costosos, y como la empresa es una empresa Pyme la solución se ajusto perfectamente a las necesidades.

6.2 RECOMENDACIONES

- Se recomienda utilizar modelos como el modelo MSF ya que es un modelo que se adapta a cualquier proyecto no solo tecnológico, ya que su metodología permite adaptar a las necesidades del cliente.
- Se recomienda utilizar el modelo IOM para determinar en qué nivel de madurez se encuentra la infraestructura permitiendo así analizar las prioridades necesarias para comenzar a mejorar.
- Se recomienda diseñar la red mediante el uso adecuado de los recursos con los que cuentan las empresas, permitiendo así ahorrar costos y tiempo al momento de realizar las implementaciones.
- Se recomienda centralizar actualizaciones ya que así se evita la perdida de las conexiones a internet, que el internet se vuelva lento. Centralizar actualizaciones permite que el proceso sea transparente al usuario.
- Se recomienda utilizar servidores para el correo electrónico ya que es más seguro que utilizar clientes externos como Hotmail, Yahoo, Gmail, etc.
- Se recomienda utilizar Directorio Activo ya que permitirá tener un control sobre quien entra a las computadoras de cada persona, se recomienda también realizar procesos de capacitación al personal para que tengan conocimiento de cómo mantener seguros los archivos tanto personales como de la empresa.
- Se recomienda centralizar en un servidor los archivos importantes de la empresa, el modo recomendado de acceso a los mismos es mediante portales los cuales son amigables y fáciles de manejar para el usuario final.
- Se recomienda seguir las conclusiones y recomendaciones presentadas en el modelo IOM, ya que siguiendo las recomendaciones se puede llegar a un nivel dinámico en infraestructura, permitiendo tener procesos automáticos ahorrando tiempo y dinero.
- Se recomienda realizar diseños de soluciones VOIP de bajo costo y robustos ya que este tipo de soluciones es más accesibles para las empresas Pymes.

GLOSARIO DE TERMINOS

AD-HOC: una red ad-hoc es aquella en la que no hay un nodo central, sino que todos los ordenadores están en igual de condiciones.

Amenaza: es un riesgo alto al que estas expuestas las empresas del mundo al correr daños y perdidas irrecuperables en sus datos que es lo más valioso que tienen al no contar con los equipos adecuados están expuestas a ser estafadas, dañadas y vulnerables a cualquier tipo de ataque informático.

APIO: Abreviación de Plataforma de Aplicaciones en el Modelo IOM y se refiere a que La Plataforma de Aplicación de Microsoft hace posible que las tecnologías de información se conviertan en factores de progreso para las empresas, mediante aplicaciones conectadas, flexibles y muy seguras.

ARPANET: Arpanet fue el origen de Internet como lo conocemos hoy en día. Sus inicios están absolutamente relacionados con la Guerra Fría que asoló Europa durante la segunda mitad del siglo pasado. La red Arpanet nació en mil novecientos sesenta y nueve como resultado de un proyecto de investigación del Departamento de Defensa norteamericano, que trataba de encontrar una vía de comunicación alternativa a la comunicación a través de radio, ya que se preveía que en el caso de una guerra nuclear, temor con fundamento en aquella época, las comunicaciones por radio se verían fuertemente afectadas.

Asincrónicas: Es aquella comunicación que se establece entre dos o más personas de manera diferida en el tiempo, es decir, cuando no existe coincidencia temporal.

ATM: Modo de Transferencia Asìncrona o Asynchronous Transfer Mode (ATM), es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

BPIO: Abreviación de Productividad Empresarial en el modelo IOM que es un conjunto completo de tecnologías que ayuda a mejorar la gestión y control de contenidos, datos y procesos a lo largo de una serie de áreas de la empresa.

BPM: Abreviación de Business Process Management o Gestión de procesos de negocio, es una metodología empresarial cuyo objetivo es mejorar la eficiencia a través de la gestión sistemática de los procesos de negocio, que se deben modelar, automatizar, integrar, monitorizar y optimizar de forma continua, BPM se enfoca en la administración de los procesos del negocio.

CoreIO: Abreviación de Infraestructura Básica en el modelo IOM, este nivel valora la madurez en las capacidades fundamentales que habilitan las tecnologías de información: gestión de la identidad y acceso a recursos de la red, gestión de servidores y desktops, protección de datos y seguridad y, en general, la gestión de sistemas.

Datacenter: Se denomina centro de procesamiento de datos o Datacenter a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

Demodular: engloba el conjunto de técnicas utilizadas para recuperar la información transportada por una onda portadora, que en el extremo transmisor había sido modulada con dicha información.

DHCP: es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

DNS: Es un servicio el cual nos permite ser identificados dentro de la red mediante nombres, es decir convierte las direcciones IP en nombres para facilitar la búsqueda de alguna computadora o periférico dentro de la red.

Driver: es un programa informático que permite al sistema operativo interactuar con un periférico, haciendo una abstracción del hardware y proporcionando una interfaz para usarlo. Por tanto, es una pieza esencial, sin la cual no se podría usar el hardware.

DSSS: Siglas de Espectro Ensanchado por Secuencia Directa, En esta técnica se genera un patrón de bits redundante para cada uno de los bits que componen la señal. Cuanto mayor sea este patrón de bits, mayor será la resistencia de la señal a las interferencias.

EAI: Enterprise Application Integration (EAI) o Integración de Aplicaciones de Empresa se define como el uso de software y principios de arquitectura de sistemas para integrar un conjunto de aplicaciones.

EPM: La solución EPM sirve para organizar el trabajo y las personas según las prioridades empresariales para administrar el trabajo de forma eficaz desde proyectos ad-hoc a programas complejos.

ERP: son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía comprometida en la producción de bienes o servicios.

Ethernet: es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

FHSS: es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible.

Firewall: un elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

FTP: es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

Gateway: es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Host: Son los computadores conectados a la red, que proveen y/o utilizan servicios a/de ella. Los usuarios deben utilizar hosts para tener acceso a la red. En general, los hosts son computadores mono o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores WWW, etc. Los usuarios que hacen uso de los hosts pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red.

IEEE 802.11: El protocolo **IEEE 802.11** o **WIFI** es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local

IOM: El Modelo de Optimización de infraestructuras (IOM) propone una vía para alinear las empresas y las IT que permita crear una infraestructura madura con un equilibrio óptimo entre la actividad personal, los procesos y la tecnología, dando como resultado una mayor seguridad, una simplificación de las operaciones y la gestión y una mejor relación coste/eficiencia para sus puestos de trabajo.

IP: Siglas de Protocolo de Internet (Internet Protocol) que forma parte de la serie de protocolos TCP/IP que fue creada para proporcionar interconectividad entre una serie de sistemas anfitriones independientes.

ISO/IEC: es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

IT: Acrónimo de Tecnologías de la Información.

ITDM: Information Technology Decision Maker

ITIL: es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (IT). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de IT. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de IT.

ITU: Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

LAN: Una red de área local, red local o LAN (del inglés Local Area Network) es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de hasta 200 metros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

LDAP: Es un protocolo que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red, es un protocolo de acceso unificado a un conjunto de información sobre una red. También es considerado una base de datos a la que pueden realizarse consultas.

LOS: es un enlace de radio que debe tener visibilidad directa entre antenas, por lo que no debe haber obstáculo entre ambas. También se utiliza en ocasiones su denominación en inglés, Line of Sight, o su acrónimo LOS.

MAC: dirección MAC (siglas en inglés de Media Access Control o control de acceso al medio) es un identificador de 48 bits (6 octetos) que corresponde de forma única a una Ethernet de red.

MSF: MSF es un compendio de las mejores prácticas en cuanto a administración de proyectos se refiere. Más que una metodología rígida de administración de proyectos, MSF es una serie de modelos que puede adaptarse a cualquier proyecto de tecnología de información.

NIDS: Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneo de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real. Para ello, analiza todos los paquetes, buscando en ellos patrones sospechosos.

P2P: Una red peer-to-peer (P2P) o red de pares, es una red de computadoras en la que todos o algunos aspectos de esta funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre si. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

PDA: Personal Digital Assistant (Asistente Digital Personal), es un computador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

ROAMING: es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra. Roaming es una palabra del idioma inglés que significa vagar o rondar. El término más adecuado en castellano es "itinerancia".

Seguridad de Información (SI): preservación de la confidencialidad, integridad y disponibilidad de la información; adicionalmente autenticidad, responsabilidad, no repudio y confiabilidad.

Seguridad: la seguridad generalmente consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió.

SGSI: La parte del Sistema de Gestión Global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorizar, revisar, mantener, y mejorar la seguridad de la información.

SMTP: Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.).

SOA: Arquitectura Orientada a Servicios (en inglés Service Oriented Architecture), es un concepto de arquitectura de software que define la utilización de servicios para dar soporte a los requisitos del negocio.

SSID: Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

UC: Comunicaciones Unificadas es un término comúnmente utilizado por los proveedores de tecnologías de la información para designar la integración de diferentes sistemas de comunicaciones, ordenadores, aplicaciones y dispositivos móviles. Esto, en potencia, incluye la integración de la voz, tanto fija como en movilidad, con e-mail, mensajería instantánea, escritorio y aplicaciones especializadas del negocio. Se basa en presentar tecnologías como voz sobre IP (VoIP), telepresencia, fax, conferencias a través de audio, vídeo y web, mensajería instantánea unificada, buzón de voz unificado, etc. en un solo entorno, ofreciendo al usuario una experiencia más completa, al mismo tiempo que más sencilla.

VOIP: es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol). Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (acrónimo de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

WEP: acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

WiFi: es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11.

WLAN: (*Wireless Local Area Network*) es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

X.500: Es un estándar para servicios de directorio establecido por ITU (International Telecommunications Union). La ISO/IEC publico el mismo estándar. X.500 define el modelo de información usada en los servicios de directorio.

MCU: Multipoint Control Unit es gestionar la comunicación entre diferentes terminales en un esquema de transmisión multipunto.

MGCP: Media Gateway Control Protocol, es un protocolo interno de VoIP cuya arquitectura se diferencia del resto de los protocolos VoIP por ser del tipo cliente – servidor.

RTP: son las siglas de Real-time Transport Protocol (Protocolo de Transporte de Tiempo real). Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia.

RTPC: Es el conjunto de elementos que hacen posible la transmisión conmutada de voz, con acceso generalizado al público.

SIP: Session Initiation Protocol (SIP o Protocolo de Inicio de Sesiones) es un protocolo desarrollado por el IETF MMUSIC Working Group con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

BIBLIOGRAFIA

- 802.12 WLAN's and IP Networking Security, QoS, y Mobility, Autores: Anand R. Prasad y Neeli R. Prasad, Editorial: Artech House
- Curso - 1846a Microsoft Solutions Framework Essentials
- Curso - 2283 Managing and Maintaining a Microsoft® Windows Server™ 2003 Environment
- Curso - 2284 Managing a Microsoft® Windows® Server 2003 Environment
- Curso - 2286B Implementing a Microsoft® Windows® Server 2003 Network Infrastructure: Network Hosts
- Curso - 2288 Implementing, Managing, and Maintaining a Microsoft® Windows® Server 2003 Network Infrastructure: Network Services
- Curso - 2288B Planning and Maintaining a Microsoft® Windows® Server 2003 Network Infrastructure
- Curso - 2289B Planning, Implementing, and Maintaining a Microsoft® Windows® Server 2003 Active Directory® Infrastructure
- Curso - 5061A Implementing Microsoft Office SharePoint Server 2008
- Cursos - 5061A: Implementing Microsoft® Office SharePoint® Server 2007
- Experiencia Profesional
- Getchell, Scott. MSF Process Model v. 3.1. USA: Microsoft Press, 2002.
- http://cristianmr.wordpress.com/2009/02/26/
- http://es.wikipedia.org/wiki/
- http://fferrer.dsic.upv.es/cursos/Windows/Avanzado/ch03s02.html
- http://jeilg.blogspot.com/2008/07/directorio-activo.html
- http://office.microsoft.com/es-es/epmsolution/FX101935293082.aspx?ofcresset=1
- http://studies.ac.upc.edu/FIB/CASO/seminaris/2q0304/M6.pdf
- http://technet.microsoft.com/es-es/library/bb944804.aspx
- http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/ISOIEC-27001/
- http://www.gpicr.com/msf.aspx

- http://www.microsoft.com
- http://www.microsoft.com/spain/iom/
- http://www.microsoft.com/spain/iom/modelo/nivelesiom.aspx
- http://www.microsoft.com/spain/windowsserver2003/
- http://www.microsoftio.com/
- http://www.perifel.com.mx/porqueperifel/O360/iom-itil/Pages/default.aspx
- http://www.scribd.com/doc/7331778/MSFMartinLuisReq?__cache_revision=1235867715&__user_id=-1&enable_docview_caching=1
- http://www.tipolisto.com/Informatica/ARPANET.html
- http://www.willydev.net/descargas/articulos/general/MSF.aspx
- Managing Microsoft Systems Management Server 2003, Delivery guide, Autor Microsoft Corporation
- MCSA / MCSE: Managing and Maintaining a Microsoft Windows Server 2003 Environment Study Guide, Autor: Lisa Donald, Editorial Sybex
- MCSA / MCSE: Windows Server 2003 Network Security Administration Study Guide, Autores: Russ Kaufmann y Bill English, Editorial: Sybex
- Microsoft Virtual Labs, Deploying Forefront Client Security – Part 1, Autor: Microsoft Corporation
- Microsoft Virtual Labs, Deploying Forefront Client Security – Part 2, Autor: Microsoft Corporation
- Microsoft Windows Server 2003 Administrator's Companion, Autores: Charlie Russel; Sharon Crawford; Jason Gerend, Editorial: Microsoft Press
- Paul, Haynes. «MSF Team Model v. 3.1.» USA, 2002.
- Press, Microsoft. «Curso 1846A Microsoft Solutions Framework Essentials.»
- Propuestas de IOM para clientes de la empresa Intergrupo
- Redes y Computadores e Internet, Autor: Fred Halsall, Editorial: Addison Wesley
- Redes y Servicios de Banda Ancha, Autores: José M. Huidobro y David Roldán, Editorial: Mc Graw Hill
- Seguridad para Comunicaciones Inalámbricas, Autores: Randall K. Nichols y Panos C. Lekkas, Editorial: Mc Graw Hill

- Sheldon, Tom. LAN TIMES Enciclopedia de redes Networking. Primera. Madrid: McGraw-Hill, 1994.
- Turner, Michael S. V. Microsoft® Solutions Framework Essentials: Building Successful Technology Solutions. Canada: Microsoft Press, 2006.
- Windows Server 2003 Weekend Crash Course, Autor: Don Jones, Editorial: Wiley Publishing, Inc.
- www.ifi.uio.no/in331/foiler/msf.pdf
- www.malagadnug.org/ficheros/MSFMartinLuisReq.pdf
- www.naturastock.com/rsdotnet/iic3140/materia/iic3140_04.pdf

ANEXOS

ANEXO 1

MODELO DE EQUIPO MSF – ROLES

Rol	Función	Áreas Funcionales	Responsabilidades
Product Management	Satisfacción del Cliente	Marketing Valor del Negocio Defensor del Cliente Product Planning	Actuar en Defensa del Cliente Manejar la visión del Proyecto Manejar los requisitos del Cliente Manejar las expectativas del Cliente Manejar las decisiones según las características, tiempos y recursos Manejar el Marketing y las Relaciones Públicas Crear, mantener y ejecutar un plan de comunicaciones
Program Management	Entregar la solución acorde al proyecto	Project Management Arquitectura de la Solución Garantía del Proceso Servicios Administrativos	Llevar el proceso de desarrollo para entregar el producto a tiempo Manejar las especificaciones primarias de la arquitectura del proyecto Facilitar la comunicación y la negociación con el equipo Mantener el cronograma del proyecto y el reporte de avences del proyecto Crear, mantener y ejecutar el plan maestro del proyecto y su cronograma Manejar y mantener la evaluación del riesgo y el Risk Management
Development	Construir según especificaciones	Consultor de Tecnología Diseño e Implementación de la Arquitectura Desarrollo de Aplicaciones Desarrollo de Infraestructura	Especificar las características del diseño físico Estimar tiempos y mejoras para el cumplimiento de las características Construir y supervisar la construcción de la solución Preparar el producto para su despliegue Proveer la materia tecnológica e importancia para el equipo
Test	Aprobar la versión de prueba unicamente después de que la calidad del producto es identificada y se solucionaron los problemas	Plan de Pruebas Ingenieria de Pruebas Reporte de Pruebas	Asegurarse de que todos los problemas sean conocidos Crear planes y estrategias de pruebas Controlar las pruebas
User Experience	Aumento de efectividad del usuario	Informes Técnicos Capacitación Diseño Gráfico Accesibilidad	Manejar la definición de requerimientos del usuario Diseñar y crear sistemas de soporte Proveer las especificaciones para características de ayuda y archivos Diseñar y Proveer una capacitación al usuario
Release Management	Despliegue y Operaciones en marcha	Infraestructura Soporte Operaciones Versión Comercial	Manejo de Adquisiciones Manejo del despliegue del producto Manejar las relaciones de operaciones, soporte y canales de entrega Proveer un soporte de logística al equipo del proyecto

ANEXO 2

MODELO DE ENTREGABLE MODELO MSF

Fecha

Señores
Nombre Cliente
Atención. Dirigido a
Ciudad

Asunto: Nombre Proyecto.

A continuación presentamos la propuesta para Nombre Proyecto.

Muchas gracias por permitirnos presentarle nuestros servicios y lógicamente estamos dispuestos a aclarar cualquier inquietud.

Cordialmente,

Consultor

Correo Electrónico

Cargo

Nombre Cliente

Nombre Proyecto

Preparado para

Nombre Cliente

jueves, 14 de enero de 2010

Versión #

Preparado por

Consultor

Cargo

Correo Electrónico

Parte

1

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference

Reviewers

Name	Version approved	Position	Date

Parte

2

Propuesta técnica

Nombre Proyecto

2.1 Antecedentes

Requerimientos planteados por el cliente

1. Requerimientos que el cliente necesita

2.2 Servicios

Descripción de los servicios a prestar en este proyecto

Nombre Servicios

Descripción corta:

1. Visionamiento

Definición de alcances, objetivos, estrategias y entregables para el proyecto. Durante esta etapa también se definen cronogramas de trabajo, recursos y equipos de trabajo.

2. Planeación y Diseño

2.1. Análisis de la situación actual

Levantamiento te información del estado actual de la infraestructura de Windows, como servicios, estructura, conectividad, etc.

2.2. Planeación de la estructura de Bosque

Se analizarán las consideraciones necesarias para definir la estructura de bosque de la organización. Este análisis incluye la revisión de la situación actual de la Entidad y sus oficinas, y las posibles necesidades de integración al nivel de directorio que se puedan presentar en el corto y mediano plazo. Se incluyen aquí también las condiciones o recomendaciones en las cuales se debería agregar, suprimir o modificar esta estructura con nuevos dominios o controladores de dominio.

Un bosque (*forest)* es una colección de dominios y árboles de dominios (*domain trees)* que define los límites de replicación y seguridad de Windows 2000 – el directorio no puede ser más grande que el bosque.

2.3. Diseño lógico del dominio

En esta actividad se definirán las condiciones concretas de la estructura organizacional básica del Directorio Activo. El dominio es la unidad básica de la estructura lógica del *Active Directory*. Los dominios representan una partición lógica de seguridad y administración dentro del servicio de directorios.

Cada dominio requiere al menos un controlador de dominio. Cada controlador de dominio de un *bosque* dado, comparte el *schema* e información de configuración del *bosque* donde reside.

En este punto también se incluirá el diseño de nombres de dominio los dominios del servicio de directorio son nombrados con nombres DNS. Los dominios no pueden ser renombrados una vez creados, por lo que es importante determinar el nombre apropiadamente al momento de diseño.

2.4. Diseño de Unidades Organizacionales

En este punto se definirán las estructuras de Unidades Organizacionales y se propondrá una jerarquía básica significativa, acorde con la estructura de la Entidad, la topología del dominio y los requerimientos de seguridad básicos. Aquí se considera también la estructura requerida en cuanto a denominación de los diferentes objetos se refiere (convenciones de nombre).

Las unidades organizacionales son objetos del directorio que sirven como contenedores para otros objetos del directorio. Las unidades organizacionales pueden contener los siguientes tipos objetos:

- Usuarios
- Grupos
- Estaciones de trabajo
- Impresoras
- Carpetas compartidas
- Otras unidades organizacionales.

Las unidades organizacionales permiten organizar los objetos del directorio lógicamente. Cuando existen múltiples dominios cada dominio tiene su propia estructuración de OUs.

2.5. Diseño políticas de grupo

Las políticas de grupos y usuarios son el medio principal para la personalización de los puestos de trabajo y entornos de trabajo de los Usuarios bajo Windows 2003.

Será parte del alcance de este proyecto las consideraciones asociadas al uso de GPOs para el diseño de Active Directory. No se realizarán actividades en cuanto al diseño detallado de las políticas sino que solamente se tomará en cuenta su impacto a efectos del diseño lógico y físico.

2.6. Diseño físico del directorio activo

Teniendo en cuenta las redes de comunicaciones y los requerimientos de seguridad, se hará la definición de la topología de Sites para los sitios geográficos comprometidos en el proceso de actualización de los sistemas de información de Hermes Express

Esta actividad define la manera en que se aprovechará la estructura actual de red disponible para que el directorio activo no impacte las operaciones de negocio con tareas de replicación pero a la vez mantenga su disponibilidad y tolerancia a fallas. Esta tarea incluye:

- Definición de sites, site links y objetos de conexión.
- Horarios de replicación
- Tipos de links y conexiones
- Distributed File System (DFS)

2.7. Localización de Controladores de Dominios y Global Catalog Server

Los controladores de dominio del dominio serán los responsables de responder a los login de usuarios y consultas al directorio.

El Global Catalog Server almacena todos los objetos del forest con solo un conjunto de atributos, con el objetivo de incrementar el desempeño en la búsqueda de los objetos del forest.

Dentro del alcance del presente proyecto se definirán las ubicaciones necesarias para la implementación de DCs y GCs.

2.8. Operations Master Roles

Los *Operation master roles* controlan las actualizaciones críticas al servicio de directorio que se realizan en modo master, es decir, se escribe la actualización en el domain controller configurado para esa función y este realiza la replicación hacia los demás controladores de dominios.

La localización de los *Operation master roles* debe ser considerada.

Los *Operation master roles* a considerar son:

- Schema Master
- Domain Naming
- PDC
- RID Master
- Infrastructure Master

2.9. Plan de servicios básicos de red

Se revisarán los servicios asociados con el funcionamiento básico de la entidad, tales como DNS, DHCP, WINS

- Diseño de los espacios de nombres DNS interno y externos de acuerdo con el diseño de directorio activo.
- Definición de los planes de contingencia para los diferentes servicios implementados en la plataforma dentro del proyecto.

3. Desarrollo

3.1. Laboratorio de pruebas

En esta fase se realiza una implementación fuera del área de producción para probar las configuraciones y diseños preliminares.

También se tomarán en cuenta listas de verificación de procedimientos y procesos para realizar la implementación del diseño elaborado en la etapa anterior.

Estabilización

3.2. Implementación de Servicios

Después de finalizar la etapa de pruebas se realiza la implementación de los servicios en el servidor que va a ser utilizado en producción, en base a los diseños realizados, incluyendo la implementación de las políticas diseñadas.

2.3 Estrategia

La estrategia con la cual se enfrentará esta iniciativa de tecnología se basa en las responsabilidades asignadas a cada uno de los roles del proyecto, según Microsoft Solutions Framework. Estas responsabilidades se resumen en el siguiente cuadro, donde se ha identificado los roles asignados a Hermes Express y a Juan José Enríquez.

Rol	Responsabilidades
Gerente de Producto (Hermes Express)	▪ Priorizar requerimientos de negocio ▪ Presentar usuarios calificados para suministrar especificaciones al equipo ▪ Asegurar que las especificaciones funcionales cumplen con las expectativas de negocio ▪ Administrar las comunicaciones externas del proyecto
Gerente de Programa (Hermes Express con Asesoría de Juan José Enríquez)	▪ Confirmar avance y administración de planes de trabajo de todos los roles del proyecto ▪ Implementar control de cambios sobre

	el documento de especificaciones funcionales ▪ Coordinar revisiones con los responsables de cada rol, en los puntos clave del proyecto (Hitos). ▪ Asignación de Recursos
Arquitecto de Infraestructura	▪ Definir la Arquitectura de Hardware y Software de la Solución asegurando su estandarización e integración. ▪ Liderar la implementación de la Prueba de Arquitectura confirmando escalabilidad de tecnología y negocio. ▪ Revisar implementación de funcionalidad crítica dentro de la Prueba de Arquitectura, ▪ Definir las recomendaciones relativas al Plan de Capacidad de la Infraestructura de Hardware y Software de Base ▪ Definir la implementación de los procesos mínimos de seguridad de acceso a la información, identificación, autenticación, autorización y rasgos de auditoria
Infraestructura (Hermes Express)	▪ Asegurar una transición simple de desarrollo a producción y operación en coordinación con Arquitecto ▪ Construir planes de salida a producción, instalación y soporte en coordinación con Arquitecto
Usuario Experto (Hermes Express)	▪ Definir las especificaciones funcionales de la solución por medio de casos de uso conjuntamente con los consultores de Intergrupo ▪ Participar en pruebas de usabilidad

Plan de trabajo del proyecto

	Actividad	Tiempo Total (Horas)
1.	Visionamiento	6
2.	Planeación y Diseño	
2.1.	Windows 2003 – Active Directory	12
2.2.	Exchange 2007	24
2.3.	Red Perimetral	12
3.	Desarrollo	
3.1.	Windows 2003 – Active Directory	10
3.2.	Exchange 2007	16
3.3.	Red Perimetral	10
4.	Estabilización	
4.1.	Windows 2003 – Active Directory	3
4.2.	Exchange 2007	5
4.3.	Red Perimetral	4
	Total	**102**

Propuesta económica

Diseño de Arquitectura

3.1 Costo de los servicios

Horas	DETALLE	Valor
# Horas	Nombre del Proyecto	COSTO

* Los valores no incluyen IVA

** La propuesta tiene una validez de 15 días

3.3 Garantía

Se ofrece una garantía de 30 días sobre el funcionamiento de la solución ofrecida siempre y cuando se conserven los mismos parámetros de diseño e implementación definidos en el proyecto (servidores, configuración, etc.)

ANEXO 3

COMPARACIONES ENTRE WINDOWS UPDATE, WSUS Y SMS

Información general			
	Microsot Update	**WSUS**	**SMS 2003**
Precio y sistemas de licencia	Gratuito	Necesita Licencia de Acceso de Cliente (CAL) para Windows Server	CAL de Windows Server CAL de SMS Licencia de Servidor SMS Licencia de SQL Server
Entorno al que se orienta	Usuarios individuales y equipos domésticos	Organizaciones pequeñas y medianas.	Organizaciones de tamaño medio
		Organizaciones que disponen de otras soluciones de distribución e software pero necesitan además gestión de actualizaciones	Grandes corporaciones
		Organizaciones que tienen previsto utilizar SMS en el futuro, pero necesitan una solución de actualización ahora mismo	
		Organizaciones que tienen SMS 2003 u otras herramientas de gestión pero necesitan controlar actualizaciones en equipos externos (p.ej. consultores o estudiantes)	

Software y contenidos soportados			
	Microsoft Update	**WSUS**	**SMS 2003**
Contenido de actualización automática soportado	Windows Server 2003	Windows Server 2003	Windows Server 2003
	Windows XP Professional	Windows XP Professional	Windows XP Professional
	Windows 2000	Windows 2000	Windows 2000
	Office 2003	Office 2003	Office 2003
	Office XP	Office XP	Office XP
	Exchange Server 2003	Exchange Server 2003	Exchange Server 2003
	SQL Server 2000	SQL Server 2000	SQL Server 2000
	Microsoft SQL Server Desktop Edition (MSDE)	MSDE	MSDE
	Otros productos de Microsoft en el futuro	Otros productos de Microsoft en el futuro	Otros productos de Microsoft en el futuro
Tipos de contenidos	Actualizaciones de seguridad	Actualizaciones de seguridad	Cualquier actualización de software, service packs o feature packs obtenidos por el administrador
	Actualizaciones críticas y no críticas; grupos de actualizaciones	Actualizaciones críticas y no críticas; grupos de actualizaciones	Actualizaciones e instalación de aplicaciones para cualquier software basado en Windows
	Service packs	Service packs	Actualizaciones disponibles de BIOS para hardware (Dell)
	Feature packs	Feature packs	
	Actualizaciones críticas de drivers	Actualizaciones críticas de drivers	
	Otros tipos de contenido	Otros tipos de contenido	

Posibilidades de gestión de actualizaciones			
	Microsoft Update	**WSUS**	**SMS 2003**
Distribución de actualizaciones a equipos preseleccionados	**No aplicable**	**Simple**	**Avanzado**
		Soporta la distribución selectiva basada en grupos de destino definidos en el servidor a partir de listas de nombres de máquina, y definiciones de clientes (configurables de forma centralizada mediante Políticas de Grupo o scripting) realizadas en la máquina de destino, en base a su pertenencia a	Soporta la selección basada en consultas de hardware o software, grupos o usuarios del Directorio Activo o atributos WMI.
Control centralizado de la distribución de actualizaciones	**No aplicable**	**Simple**	**Avanzado**
		Utiliza un mecanismo de petición donde los sistemas cliente contactan con el servidor para solicitar las actualizaciones aprobadas. Los administradores pueden configurar la frecuencia con la que los clientes contactan al servidor, o pueden usar herramientas de línea de comandos o scripts para activar la búsqueda de nuevas actualizaciones aprobadas.	Utiliza mecanismos de petición y permite un control adicional para determinar los casos en que las actualizaciones deben distribuirse a los clientes y en qué orden deben realizarse. Las actualizaciones pueden enviarse con una configuración "obligatoria", que obliga a que se instale en un periodo corto de tiempo.
Flexibilidad en la instalación y planificación de la actualización	**Controlado por el usuario final**	**Simple**	**Avanzado**
	Permite a los usuarios especificar si prefieren descargar e instalar automáticamente las actualizaciones, si deben instalarse en momentos previamente definidos o si prefieren que se les notifique e instalar las actualizaciones cuando el usuario lo indique. Además los usuarios pueden iniciar y seleccionar las actualizaciones optativas en cualquier momento.	Permite que los administradores definan una fecha tope en la cual una actualización debe estar instalada en un sistema. Se puede configurar para determinar cuándo se instalan las actualizaciones y si deben diferirse los reinicios y esperar, en caso necesario, a que el usuario apague el equipo.	Permite especificar ventanas de tiempo para ejecutar las actualizaciones. Por ejemplo, los administradores pueden determinar que una instalación se ejecute entre la 01:00 AM y las 05:00 AM, y si no fuera posible en ese periodo, entre las 12:00 PM y la 01:00 PM. Además los administradores pueden definir una fecha tope en la cual la actualización debe estar
Desinstalación forzada de actualizaciones	**No**	**Si, si lo soporta el paquete de actualización**	**Si, si lo soporta el paquete de actualización**
Informe de estado de la instalación de actualizaciones	**Básico**	**Simple**	**Avanzado**
	Informa de errores en la instalación y enumera las actualizaciones no realizadas al usuario.	Dispone de informes estándar predefinidos sobre estado de las instalaciones. Los datos del informe están disponibles mediante una API.	Dispone de informes predefinidos y de la posibilidad de crear informes personalizados.
Planificación de la distribución de forma centralizada	**No aplicable**	**Simple**	**Avanzado**
		Permite que los administradores identifiquen los sistemas que necesitan actualizaciones concretas y evalúa rápidamente la necesidad de actualización de los sistemas gestionados por el servidor WSUS. Los administradores pueden distribuir actualizaciones en modo "solo-detección", para permitir una mejor planificación.	Mantiene un inventario de estado de la instalación para todos los sistemas cliente, permitiendo la definición de configuraciones de línea de base (qué actualizaciones han de instalarse en según qué categoría de equipos) e incluye funciones de planificación de la secuencia en la que deben producirse los procesos de actualización.
Gestión de inventario	**No aplicable**	**Básico**	**Avanzado**
		Puede hacer descubrimiento de datos básicos de inventario de hardware: nombre de máquina, versión de sistema operativo, idioma y dirección IP	Puede hacer descubrimiento de datos básicos de inventario de hardware: nombre de máquina, versión de sistema operativo, idioma y dirección IP
	No	**Básico**	**Avanzado**

Infraestructura			
	Microsoft Update	**WSUS**	**SMS 2003**
Soporte para usuarios móviles	**Sí**	**Opcional**	**Sí**
	Permite la conexión del PC al servidor Microsoft Update a través de Internet, para descargas de contenido.	Permite que los clientes se conecten a los servidores para descargar actualizaciones en base a política. La definición de la Política de Grupo que controla a qué servidor WSUS debe conectarse un cliente puede variar dependiendo de la ubicación del cliente (a nivel de site). Además se puede configurar una opción para que se descargue contenido siempre desde Microsoft Update.	Permite que los usuarios puedan descargar actualizaciones desde su punto de distribución más cercano.
Tiene en cuenta el emplazamiento de las máquinas	**No**	**Sí**	**Sí**
		Permite utilizar Políticas de Grupo para configurar el comportamiento del proceso de actualización a nivel de site.	Puede emplear las definiciones preexistentes de site y subred dentro del Directorio Activo para identificar el punto desde el cual los clientes deben descargarse las actualizaciones.

Funciones de gestión avanzadas			
	Microsoft Update	**WSUS**	**SMS 2003**
Funcionalidad de Help Desk remoto	No	No	Sí
			Soporta control remoto, reinicio remoto y chat.
Distribución de software en general	No	No	Sí
Monitorización de utilización de software	No	No	Sí
Distribución de sistemas operativos	No	No	Sí
Gestión de dispositivos móviles	No	No	Sí
Descubrimiento de topología de la red	No	No	Sí

ANEXO 4

RECOMENDACIONES DE LA UIT

Ya que las recomendaciones son muy extensas para la impresión este anexo 4 se lo puede encontrar en un CD adjunto.

Las recomendaciones que se encuentran en medio digital son las siguientes:

- **H.323 – Sistemas de comunicaciones multimedia basados en paquetes**

Esta recomendación describe terminales y otras entidades que proporcionan servicios de comunicaciones multimedia por redes por paquetes que pueden no proporcionar una calidad de servicio garantizada. Las entidades H.323 pueden proporcionar comunicaciones de audio, video y/o datos en tiempo real.

- **H.225.0 – Protocolos de señalización de llamada y división del flujo de datos en paquetes, para multimedia basada en paquetes (incluye Q.931 y RAS)**

Esta recomendación trata los requisitos técnicos de los servicios videotelefónicos de banda estrecha definidos en aquellas situaciones en las que el trayecto de transmisión incluye una o más redes de paquetes, cada una de las cuales está configurada y gestionada para ofrecer una calidad de servicio (QoS) no garantizada que no es equivalente a la de la RDSI de banda estrecha, de manera que los mecanismos de protección o recuperación adicionales han de proporcionarse en los terminales.

- **H.225.0 Anexo G – Comunicaciones pasarela a pasarela (interdominio)**

El presente anexo describe métodos que permiten la resolución de dirección entre dominios administrativos en los sistemas H.323 para completar llamadas entre dominios administrativos. Un determinado dominio administrativo se presenta a los otros dominios administrativos a través de un tipo de elemento lógico conocido como elemento de frontera.

- **H.245 – Protocolo de control para comunicaciones multimedia**

Esta recomendación específica la semántica y sintaxis de la terminal de mensajes de información a si como los procedimientos para las negociaciones de banda durante el principio de la comunicación. El mensaje protege las capacidades de transmisión y recepción así como también el modo de preferencia desde el final de la recepción, señalización lógica de canal, y Indicación & Control.

- **H.235 – Seguridad y cifrado para los terminales multimedia compatibles con la serie H**

Esta Recomendación describe mejoras dentro del marco de las especificaciones de las Recomendaciones de la serie H.3xx para incorporar servicios de seguridad tales como *autenticación* y *privacidad* (criptado de datos). El esquema propuesto es aplicable a conferencias punto a punto y multipunto para cualesquiera terminales que utilicen la Rec. UIT-T H.245 como su protocolo de control.

- **H.450.1 – Protocolo genérico funcional para el soporte de servicios suplementarios en H.323**

Esta Recomendación describe los procedimientos y los protocolos de señalización entre entidades H.323 (Sistemas de comunicaciones multimedios basados en paquetes) para el control de servicios suplementarios. El protocolo de señalización que se define en esta Recomendación es común a todos los servicios suplementarios de la Recomendación H.323.

- **H.450.2 – Transferencia de Llamada**

Esta Recomendación describe los procedimientos y el protocolo de señalización para el servicio suplementario de transferencia de llamadas en redes conformes a la Recomendación H.323 (Sistemas de comunicaciones multimedios por paquetes).

H.450.3 – Desviación

Esta Recomendación describe los procedimientos y el protocolo de señalización para el servicio suplementario de desviación de llamadas en redes conformes a la Recomendación H.323 (Sistemas de comunicaciones multimedios por paquetes). Esta Recomendación comprende los servicios de Reenvío de llamada incondicional, Reenvío de llamada en caso de ocupado, Reenvío de llamada en caso de ausencia de respuesta y reflexión de llamadas.

- **H.450.4 – Retención**

Este servicio suplementario describe los procedimientos y el protocolo de señalización para el servicio suplementario retención de llamada en redes conformes a la Recomendación H.323 (Sistemas de comunicación multimedios basados en paquetes).

- **H.450.5 – Puesta en espera y recuperación**

Esta Recomendación describe los procedimientos y los escenarios del protocolo de señalización de los servicios suplementarios depósito de llamada y extracción de llamada conformes a la Recomendación H.323.

- **H.450.6 – Llamada en espera**

Este servicio suplementario describe los procedimientos y el protocolo de señalización para el servicio suplementario llamada en espera en redes conformes a la Recomendación H.323 (sistemas de comunicaciones multimedios basados en paquetes).

- **H.450.7 – Indicación de mensaje en espera**

Esta Recomendación describe los procedimientos y el protocolo de señalización para el servicio suplementario indicación de mensaje en espera en redes conformes a la Recomendación H.323 (Sistemas de comunicaciones multimedios por paquetes).

- **H.323 Anexo D – Fax en tiempo real utilizando T.38**

Este anexo describe un protocolo de facsímil que utiliza el sistema H.323 de comunicación multimedios basados en paquetes.

- **H.323 Anexo E – Conexión de llamadas sobre UDP**

Este anexo describe un formato de paquetización y un conjunto de procedimientos (algunos de los cuales son facultativos) que pueden utilizarse para implementar protocolos basados en UDP y TCP.

- **H.323 Anexo F – Dispositivos de un solo uso**

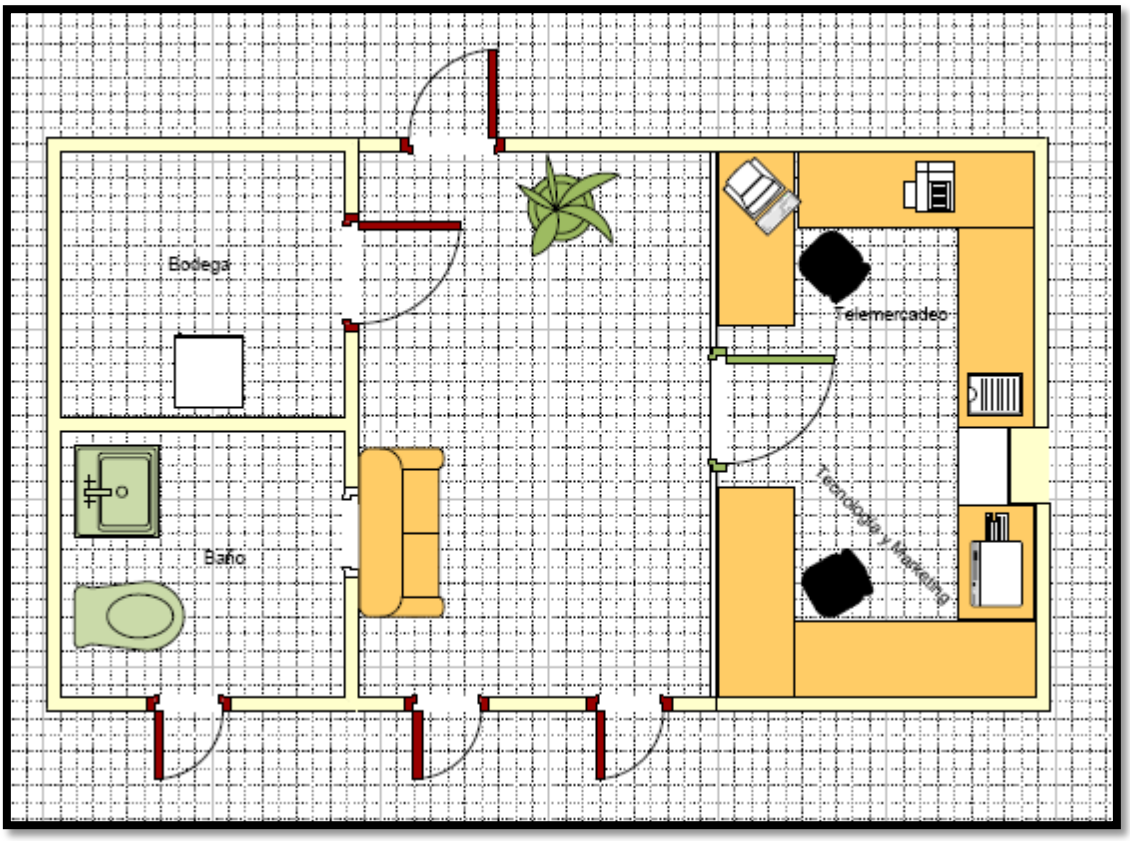
En este anexo se presenta el concepto de tipo de punto extremo simple diseñado para funcionar en configuraciones bien definidas y con funcionalidades restringidas, a diferencia de los sistemas multimedios plenamente equipados de la Recomendación H.323, reduciendo de esta forma explícitamente el sistema general y, por consiguiente, la complejidad de la implementación. En particular, en este anexo se definen los tipos de punto extremo simple para comunicación audio que funcionan utilizando un subconjunto bien definido de protocolos H.323 y se adaptan sin problemas a las aplicaciones de telefonía IP, manteniendo al mismo tiempo el interfuncionamiento con los dispositivos normales de la Recomendación H.323.

- **T.38 – Procedimientos para comunicaciones en tiempo real de facsímiles grupo 3 sobre redes IP**

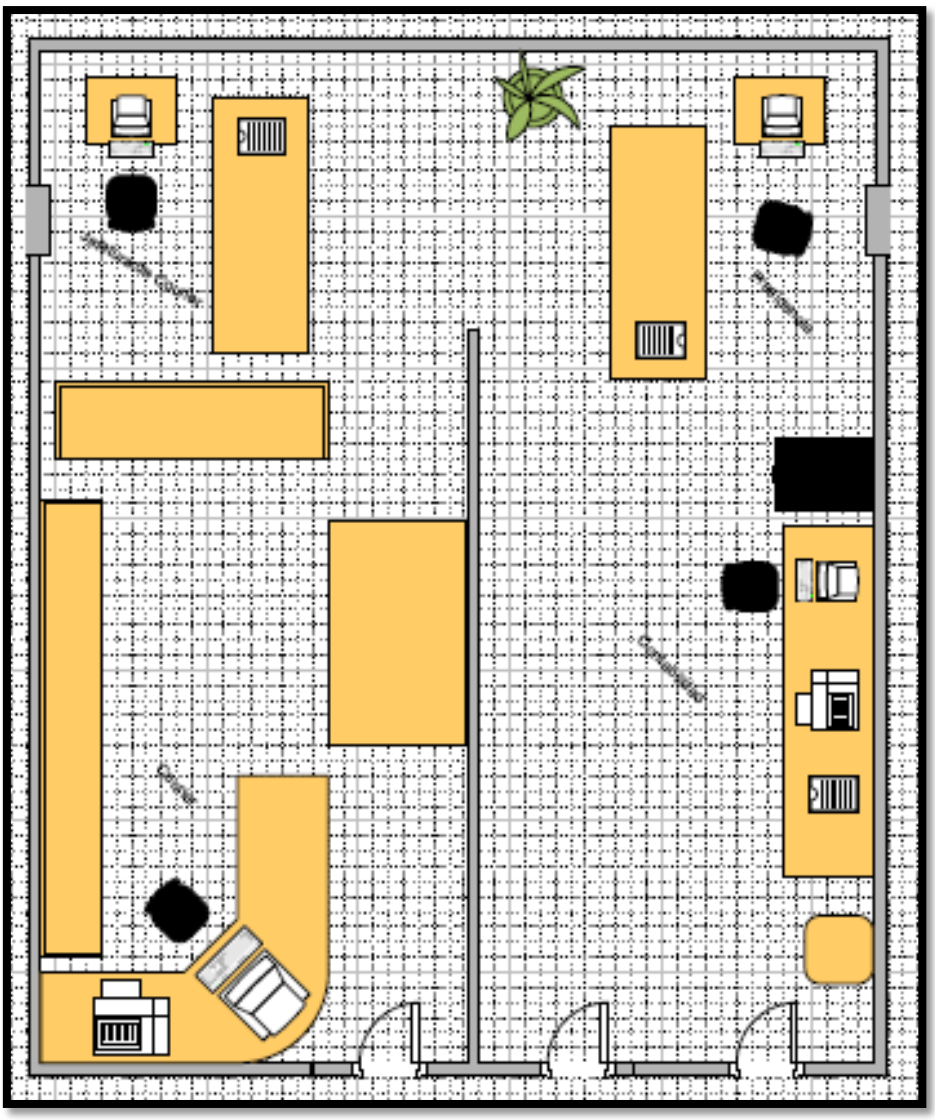
Esta Recomendación define los procedimientos que son aplicados para permitir la transmisión de facsímil de grupo 3 entre terminales PSTN o RDSI y una porción del camino de la transmisión usada entre terminales incluyendo las redes IP.

ANEXO 5

PLANO DE LA EMPRESA HERMES EXPRESS



En esta parte del anexo se puede observar la distribución de la parte frontal de la oficina, donde se puede observar que en esta parte se encuentran las áreas de Telemercadeo y Tecnología



En la parte posterior de la oficina se puede apreciar los demás departamentos de la empresa.

ANEXO 6

ENCUESTA DEL MODELO IOM

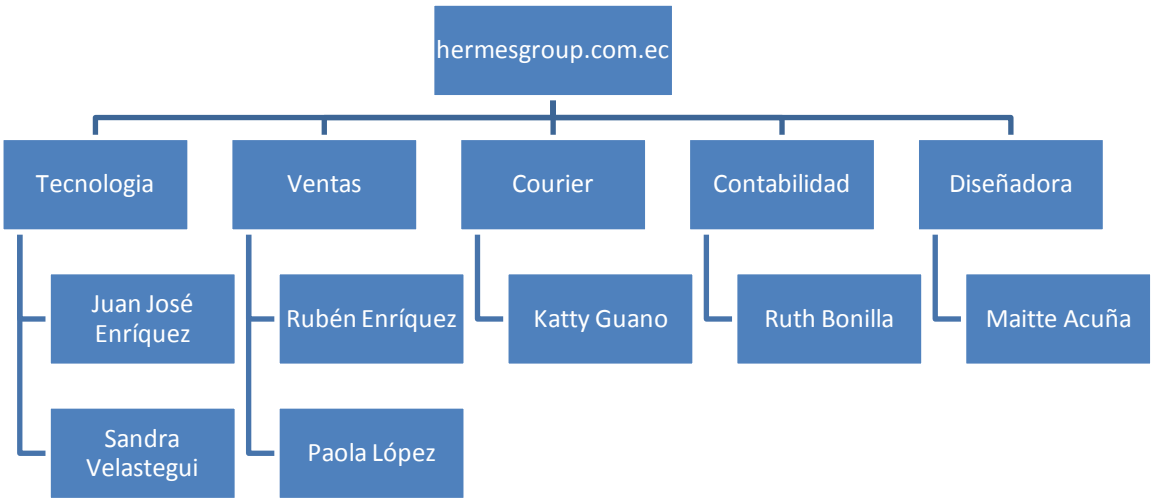
Tecnología		
ID	**Preguntas**	**Respuestas**
1	¿Usa su empresa Active Directory para autentificar el 80% o más de sus usuarios?	No
2	**Usa en su empresa una herramienta de directorio para administrar de forma centralizada las configuraciones y seguridad del 80% o más de sus PC's (ej. Políticas de Grupo)**	**No**
3	¿Su empresa tiene una herramienta centralizada para automatizar el aprovisionamiento de los usuarios (publicar nuevas cuentas, cambiar contraseñas, sincronizar permisos, abilitar el acceso a las aplicaciones de la empresa) al rededor del 80% de los sistemas heterogeneos?	No
4	**¿Usa Herramientas de Autentificación para habilitar el acceso externo a el 80% o más de sus recursos de red, clientes o socios de negocio?**	**No**
5	Cuenta su empresa con Herramientas de Auditoria de Acceso a la red, por usuarios, Pc´s, con eventos de Sucesos, fallas y violación de acceso?	No
6	**¿Su organización tiene una solución automatizada de la distribución del software para el despliegue del S.O.?**	**No**
7	¿Su organización tiene automatizado la distribución de parches cubriendo el 80% o mas de sus computadoras?	No
8	¿Su organización tiene un seguimiento automatizado de los activos de Hardward y de Software del 80% o más de sus comutadoras de escritorio?	No
9	**Su organización tiene definido el estandar basico de imágenes en al menos el 80% de sus computadoras de escritorio?**	**No**
10	**Su organización tiene definido el estandar básico de imágenes en al menos el 80% de sus portátiles?**	**No**
11	**¿Su organización tiene en mas del 80% de sus maquinas de escritorio corriendo Windows XP o 2000 como su principal S.O.?**	**Si**
12	**¿Su organización tiene en mas del 80% de sus maquinas de escritorios XP con SP2?**	**Si**
13	**¿Su organización tiene en mas del 80% de sus maquinas de escritorios corriendo Office 2003 o una versión mas actual?**	**Si**
14	**¿Su organización usa aplicaciones compatibles con la solución de certificación de pruebas para verificar al menos el 80% de las distribuciones de Software en sus computadoras?**	**No**
15	¿Su organización tiene una solución para el manejo de parches para el 80% o mas de sus servidores?	No
16	**¿Su organización tiene un analizador de capacidades de sus servicios empresariales (como el email)?**	**No**
17	**¿Su organización tiene centralizado el manejo y actualizaciones de los dispositivos moviles?**	**No**
18	**¿Su organización tiene una solución para la validaciones de usuario y la protección de datos si es que se pierden sus dispositivos moviles?**	**No**
19	**¿Su organización requiere una via segura y garantizada para verificar comunicaciones seguras con su red coorporativa y dispositivos moviles (certificados)?**	**No**
20	¿Su organización ofrece acceso a aplicaciones Web vía WAP or HTTP para dispositivos mobiles?	No
21	**¿Su organización esta buscando la manera activa de consolidación de sus servidores con virtualizacion?**	**No**
22	¿Su organización usa una solución automatizada para la continua actualización de la configuración y/o las aplicaciones de los dispositivos mobiles?	No
23	**¿Su organización tiene automatizado la solución de manejo de parches para sus dispositivos móviles?**	**No**
24	**¿Su organización usa la virtualizacion para mover dinámicamente el flujo de carga entre servidores basado en recursos y reglas del negocio?**	**No**
25	Su organización tiene una estrategia de administracion de imagenes de escritorios que incluyen S.O., Antivirus, herramientas administrativas, herramientas de productividad (como Office) asi como aplicaciones LOB?	No
26	**¿Su organización usa una estrategia de imágenes continuas o anidades para el manejo de sus Equipos de escritorio?**	**No**
27	**¿Su organización tienen un plan para manejar como maximo 2 versiones de S.O. en un 80% de sus maquinas de escritorio?**	**No**
28	¿Su organización tiene estarizado n o n-1 versiones de S.O. de todos sus escritorios?	Si
29	**¿Su organización tiene Antivirus (con automatización de actualizaciones) en al menos 80% de sus tableros de escritorio?**	**No**

30	¿Su organización tiene el manejo de politicas de firewall (BlackICE, Windows Firewall, Zone Alarm) corriendo en un 80% de sus servidores?	No
32	**¿Su organización provee la seguridad de sus empleados en accesos remotos hacia recursos internos y aplicaciones LOB mas allá de un email (VPN y/o Servicios Terminales)?**	**No**
33	¿Su organización usa una vía segura y garantizada para verificar la comunicación entre servidores para asegurar comunicaciones de la red entre los servidores criticos tales como controladores de dominio y servidores de mail? (Un ejemplo de comunicaciones seguras es	No
34	**¿Su organización tiene un firewall centralizado (no por maquina) para la protección de su empresa en un 80% de sus sistemas (ISA, Checkpoint, Nokia)?**	**No**
35	¿Su organización tiene un servidor interno para servicios basicos de red (DNS, DHCP)?	No
36	**¿Su organización tiene integrada la administracion y mitigación de amenazas a través del cliente y servidores de servicio?**	**No**
37	¿Su organización tienen la supervisión para el 80% o más de sus servidores críticos para asegurar las experiencias constantes y confiables del usuario (el asegurarse que el email esté siempre disponible)?	No
38	**¿Su organización tiene monitoreo de SLA para al menos el 80% de sus servidores con capacidades de servicios de reportes?**	**No**
39	¿Su organización provee un mecanismo de comunicación segura (como SIP)?	No
40	**¿Su organización despliega una red wireless segura usando Active Directory y IAS/RADIUS para la autentificación y autorización?**	**No**
41	¿Su organización tiene una infraestructura centralizada del manejo de certificados (PKI)?	No
42	**¿Su organización maneja proactivamente el ancho de banda para las sucursales (Optimización WAN)?**	**No**
43	¿Su organización tiene soluciones de cuarentena para computadoras infectadas y no parchadas?	No
44	**¿Su organización tiene una solución de backup y restore para al menos el 80% de los servidores criticos de su empresa?**	**No**
45	¿Su organización maneja centralizadamente los backups de datos de las sucursales?	No
46	**¿Su organización tiene backups y restore y define tiempos de recuperación vía SLA para al menos 80% de sus servidores?**	**No**
TI y Procesos de Seguridad		
47	**¿Su organización tiene una persona quien maneja la seguridad de la información y quien define los procesos de manejo de riesgos para la organización?**	**Ninguno**
48	¿Esa persona tiene la autoridad para definir los procesos de seguridad y definir los medios para las aplicaciones de la organización?	No
49	**¿Su organización tiene la información formal de los manejos de riegos de seguridad?**	**Ninguno**
50	¿Su organización tiene un proceso de respuestas a incidentes?	Ninguno
51	**¿Su organización tiene un proceso para manejar la identidad de usuarios, dispositivos o servicios?**	**Ninguno**
52	¿Su organización tiene procesos para manejar controles de antivirus?	Ninguno
53	**¿Su organización tiene procesos para deployar las actualizaciones de seguridad de los dispositivos activos conectados a la red IT?**	**Ninguno**
54	¿Su organización tiene un proceso para verificar las politicas de seguridad para todos los dispositivos conectados a la red?	Ninguno
55	**¿Su organización sigue un proceso de revisión de seguridad para la adquisición de software (disponible en el mercado, personalizada y desarrollada internamente)?**	**Ninguno**
56	¿Su organización tiene procesos para clasificar los datos y un apropiado control de seguridad de datos?	Ninguno
Proceso Administrativo con Base en ITIL/COBIT		
57	**¿Cuáles de los siguientes describe mejor el manejo y la operación de su infraestructura IT?**	**Ninguno**
Función Administrativa de la Tecnología en la Organización		
58	¿Cuales de los siguientes describe mejor como su organización define la estrategia de despliegue de PC?	Sistema Operativo estandarizado en una versión
59	**¿Cuál de los siguientes describe mejor como su organización maneja su estrategia TI?**	**Planes estratégicos de Tecnología estratégica de 1 año o más**

ANEXO 7

POLÍTICAS DE SERVIDORES

7.1. ESQUEMA DE DIRECTORIO ACTIVO



Unidades Organizativas

- Tecnología
- Ventas
- Mensajería
- Contabilidad
- Diseño Gráfico

Usuarios

- **Tecnología**
  - jenriquez (Juan José Enríquez)

- a.tecnologia (Asistente de Tecnología)

- **Ventas**
  - renriquez (Rubén Enríquez)
  - plopez (Paola López)
  - dtorres (Diana Torres)
  - atiempo.ventas (Ventas)
- **Courier**
  - a.courier (Asistente de Courier)
- **Contabilidad**
  - contabilidad (Contabilidad)
- **Diseño Gráfico**
  - macuna (Maitte Acuña)

Políticas y Privilegios

- El único usuario que tiene privilegios de Administración de Dominio es jenriquez ya que es el encargado de la infraestructura de la empresa.

7.2. POLITICAS DE ISA SERVER 2006

- **Navegar por Internet**
  - **Nombre de Regla:** Internet Total
  - **Acción:** Permitir
  - **Desde:** Red Interna
  - **Hacia:** Red Externa
  - **Usuarios:** por política interna los usuarios que tienen acceso a internet son los siguientes (dtorres, renriquez, jenriquez y macuna)
- **Uso de Messenger**
  - **Nombre de Regla:** Acceso MSN
  - **Acción:** Permitir

- **Desde:** Red Interna
- **Hacia:** Red Externa
- **Usuarios:** por política interna los usuarios que tienen acceso a MSN son los siguientes (dtorres, renriquez, jenriquez y macuna)

- **Bloqueo Messenger**
  - **Nombre de Regla:** Bloqueo MSN
  - **Acción:** Denegar
  - **Desde:** Red Interna
  - **Hacia:** Red Externa
  - **Usuarios:** por política interna los usuarios que tienen restricción acceso a MSN son los siguientes (atiempo.ventas, a.tecnologia, a.courier. contabilidad, plopez)
- **Bloqueo Internet**
  - **Nombre de Regla:** Bloqueo MSN
  - **Acción:** Denegar
  - **Desde:** Red Interna
  - **Hacia:** Red Externa
  - **Usuarios:** por política interna los usuarios que tienen restricción acceso a Internet son los siguientes (atiempo.ventas, a.tecnologia, a.courier. contabilidad, plopez)

ANEXO 8

PASOS PARA IMPLEMENTAR WINDOWS SERVER 2003

Pasos Previos

- Verificar requerimientos del sistema
- En el caso de contar con clústeres, revisar el proceso para la instalación en nodos
- Decidir qué tipo de licenciamiento se va a utilizar: Por dispositivo, por usuario o por servidor
- Decidir qué tipo de sistema de archivo se va a utilizar: NTFS, FAT, o FAT32
- Decidir las particiones que se van a utilizar o si se necesita crear nuevas particiones
- Decidir los parámetros de red, direcciones IP y resolución de nombre TCP/IP
- Decidir si se crea dominio o grupos de trabajo para los usuarios

Pasos a seguir de instalación

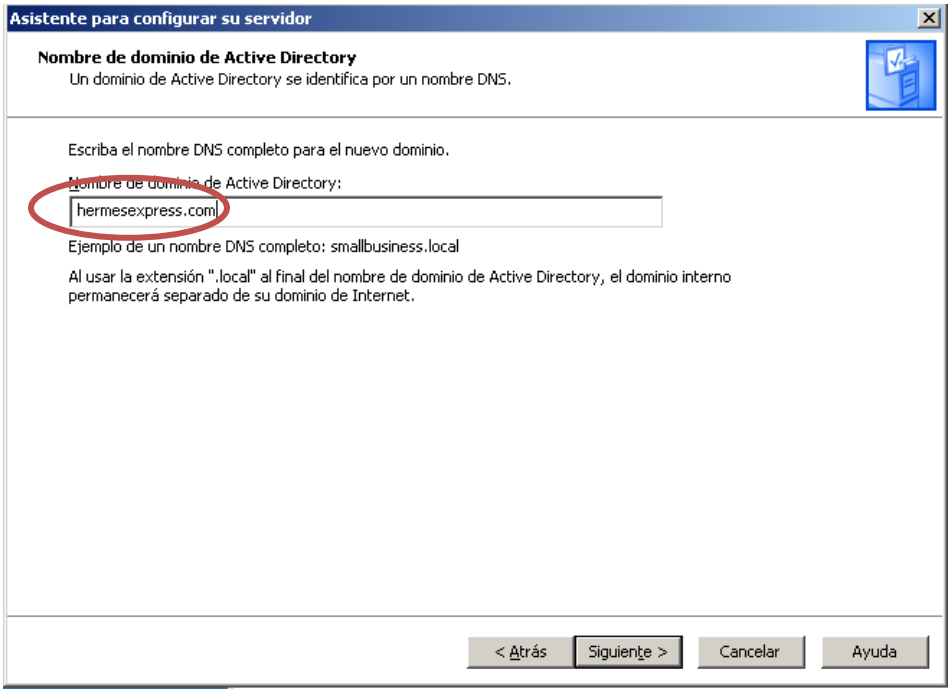
- Insertar el CD de instalación
- Presionar una tecla para ingresar a la consola de instalación
- Aceptar la licencia de Windows
- Crear la partición o particiones para la instalación
- Comenzar la instalación, esperar a que termine la instalación, ingresar la licencia del sistema operativo y configuraciones de idioma.
- Una vez instalado el sistema operativo, instalar todas las actualizaciones del sistema operativo.

Directorio Activo

Para llevar a cabo la implementación de Directorio Activo, seguir los siguientes pasos:

- El momento que se inicia el servidor se muestra la ventana “Administre su Servidor”
- Hacer clic en “Agregar o quitar función”
- En la siguiente ventana hacer clic en “Siguiente”

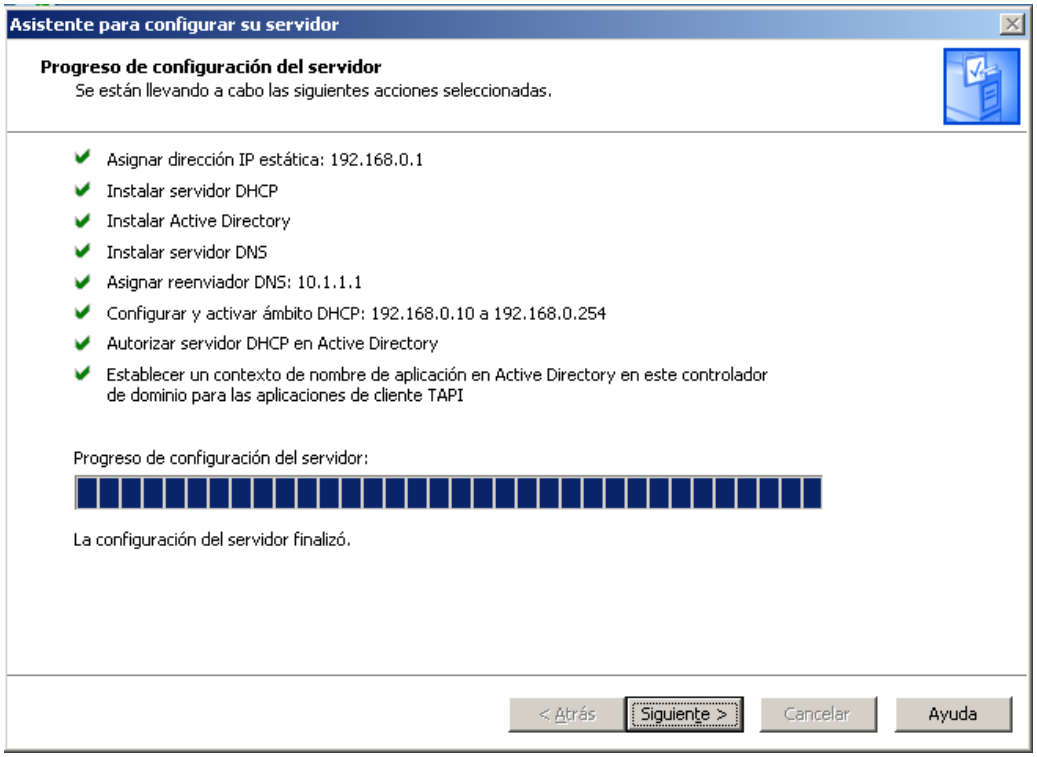
- Esperar a que inicie el asistente
- Seleccionar “Configuración típica para un servidor principal”, esto configurara Directorio Activo, DHCP y servidor DNS.
- En la siguiente pantalla poner el nombre del Dominio a implementar como se muestra en la siguiente pantalla.



- En la siguiente pantalla dejar los valores por defecto y hacer clic en Siguiente
- Esperar a que finalice la configuración.

Nota: Para que la configuración empiece se debe tener el CD o DVD de instalación de Windows Server 2003 R2.

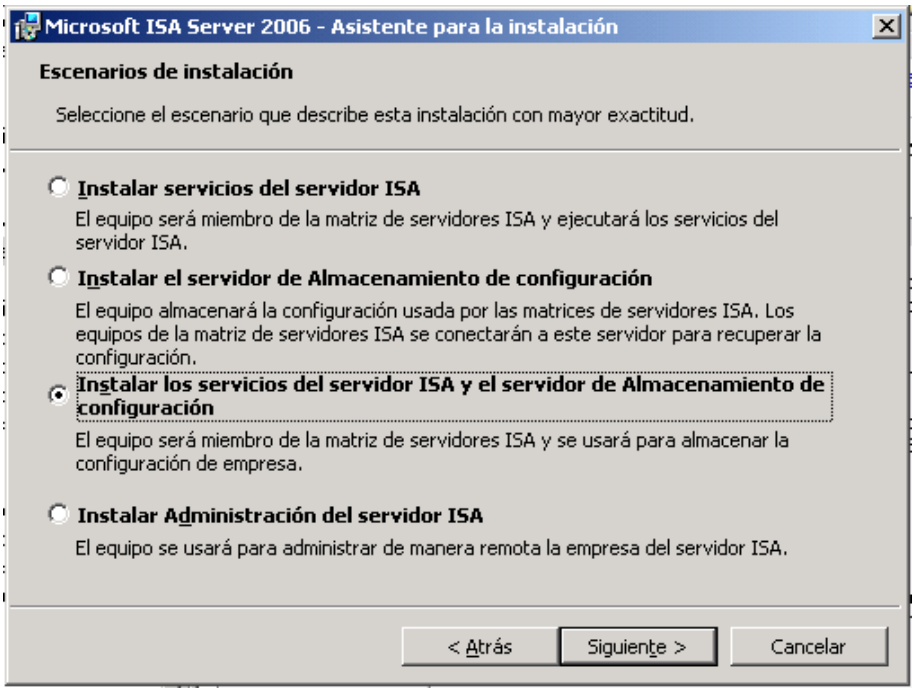
- Una vez finalizada la configuración se mostrará una pantalla como la siguiente, con esto se sabrá que se encuentra configurado el servidor.


Asistente para configurar su servidor
Progreso de configuración del servidor
Se están llevando a cabo las siguientes acciones seleccionadas.
Asignar dirección IP estática: 192.168.0.1
Instalar servidor DHCP
Instalar Active Directory
Instalar servidor DNS
Asignar reenviador DNS: 10.1.1.1
Configurar y activar ámbito DHCP: 192.168.0.10 a 192.168.0.254
Autorizar servidor DHCP en Active Directory
Establecer un contexto de nombre de aplicación en Active Directory en este controlador de dominio para las aplicaciones de cliente TAPI
Progreso de configuración del servidor:
La configuración del servidor finalizó.
< Atrás
Siguiente >
Cancelar
Ayuda

ANEXO 9

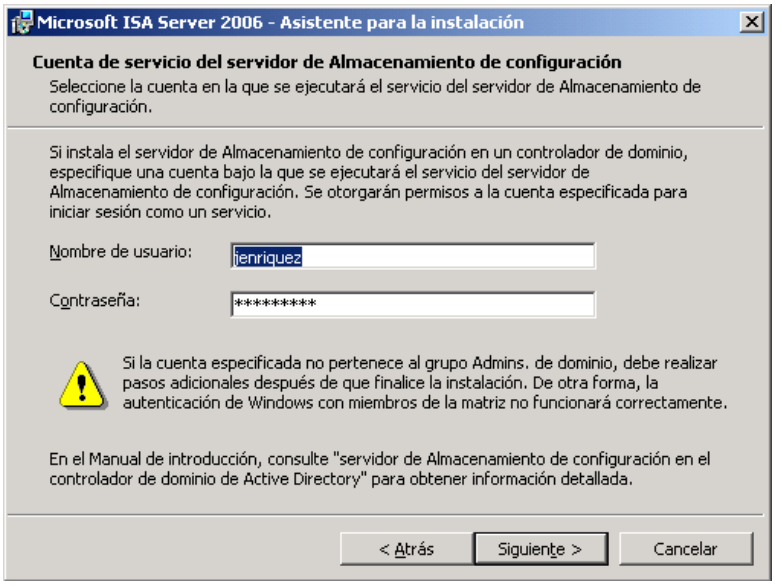
PASOS PARA IMPLEMENTAR ISA SERVER 2006

- Insertar el CD de instalación de ISA Server 2006
- En la siguiente pantalla aceptar la licencia
- Ingresar el número de licencia de instalación para la versión
- En la siguiente pantalla se escoge que es lo que se desea instalar:



Para este punto de la instalación escoger la tercera opción para poder almacenar la configuración de seguridad de la empresa.

- En la siguiente pantalla seleccionar donde se va a instalar ISA Server 2006.
- En la siguiente seleccionar "Crear una nueva empresa ya que es el primer servidor de ISA Server para la empresa"
- En la siguiente pantalla poner el usuario el cual va administrar ISA Server



- En la siguiente pantalla poner los intervalos de direcciones IP
- Esperar a que termine la instalación de ISA Server 2006.

ANEXO 10

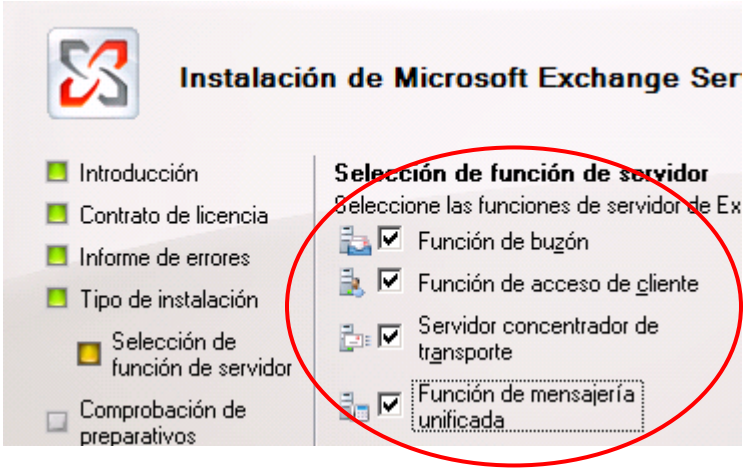
PASOS PARA IMPLEMENTAR EXCHANGE SERVER 2007

Para instalar se requieren algunos prerrequisitos los cuales se muestran a continuación:

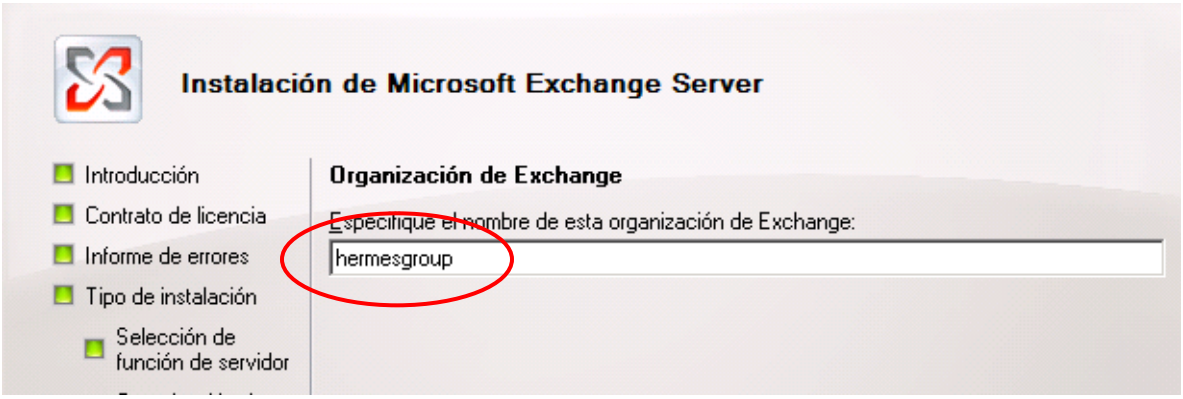
1. Tener instalado .NET Framework 2.0
2. Tener instalado la última actualización de .NET Framework 2.0
3. Tener instalado Microsoft Management Console (MMC)
4. Tener instalado Microsoft Windows PowerShell
5. Tener instalado Internet Information Server 6.0
6. Tener instalado MSXML 6.0
7. Tener instaladas todas las actualización del Sistema Operativo

Una vez instalado todos los prerrequisitos proceder a instalar y configurar Exchange Server 2007, siguiendo los siguientes pasos:

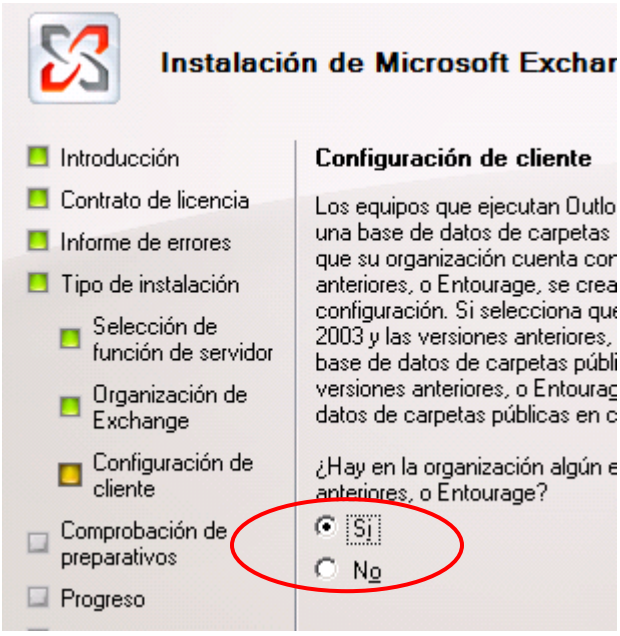
- Introducir el DVD de Exchange Server 2007
- En la primera pantalla hacer clic en siguiente
- Aceptar los términos de la licencia
- Seleccionar instalación personalizada, escoger lo que se va a instalar como se muestra en la siguiente pantalla:



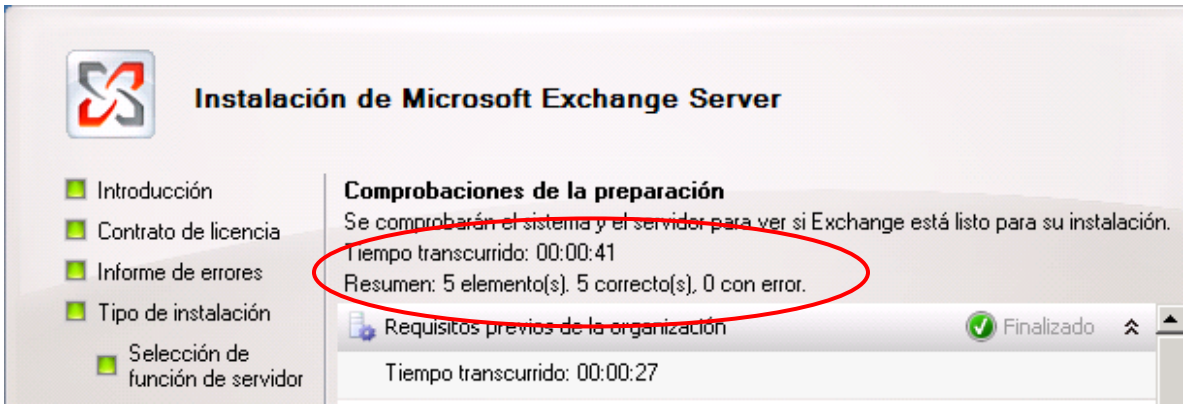
- En la siguiente pantalla especificar la organización de Exchange para este caso se utilizó hermesgroup



- Como la empresa cuenta con versiones anteriores a Office 2007, es necesario en la siguiente pantalla seleccionar que si, ya que con esto Exchange Server 2007 creará una base de datos de carpetas públicas para que puedan estas maquinas conectarse a Exchange Server 2007



- En la siguiente pantalla el programa va a verificar si todo se encuentra correcto para llevar a cabo la implementación.
- Una vez finalizada la comprobación aparecerá una pantalla como la siguiente

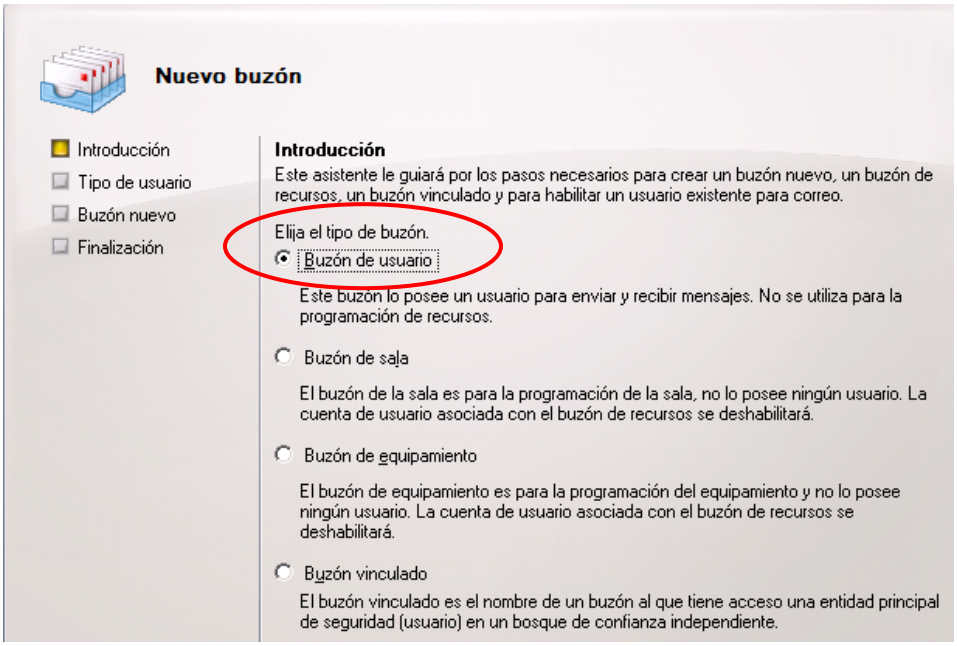


Nota: en el caso de que exista algún error durante la comprobación, el asistente nos mostrara las soluciones posibles.

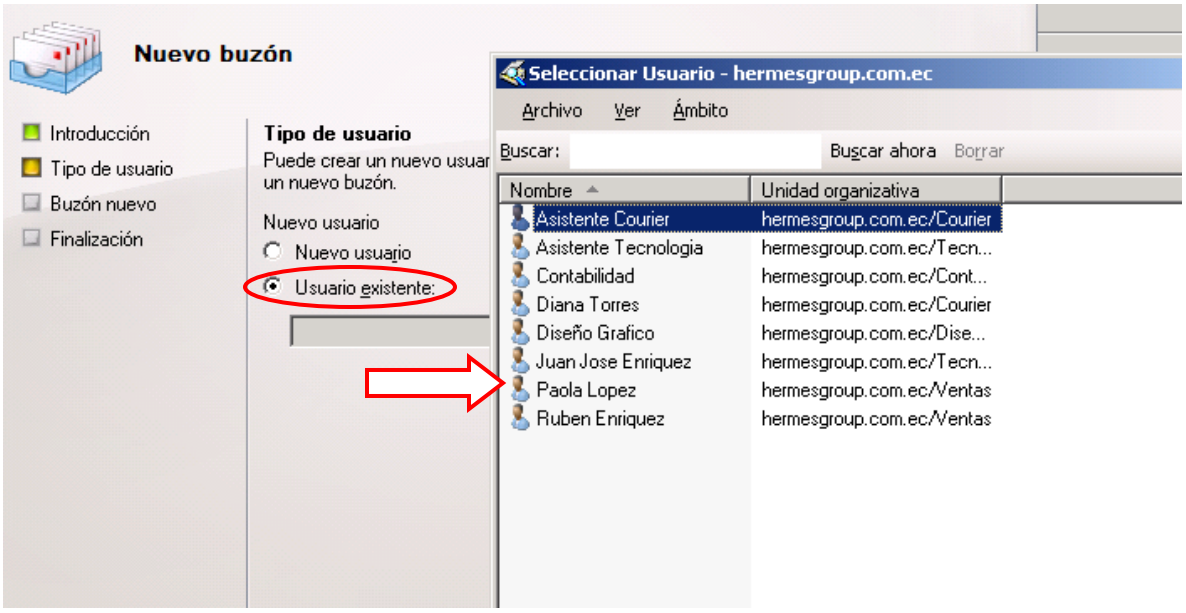
- Dar clic en el botón de Instalar el asistente empezara a instalar Exchange Server 2007
- Para configurar las cuentas de cada usuario y el acceso OWA seguir los siguientes pasos.

Configuración de Exchange Server 2007

- Para configurar los buzones de correo abrir la Consola de Administración de Exchange.
- En el panel de la izquierda seleccionar Configuración de destinatarios
- Y dentro de Configuración de Destinatarios seleccionar Buzón
- En el panel de la derecha seleccionar Buzón Nuevo y seleccionar Buzón de usuario



- Seleccionar siguiente, en la siguiente pantalla en el caso de que el usuario no se encuentre en la Directorio Activo seleccionar Nuevo Usuario, caso contrario seleccionar Usuario Existente y buscar los usuarios dentro del dominio.

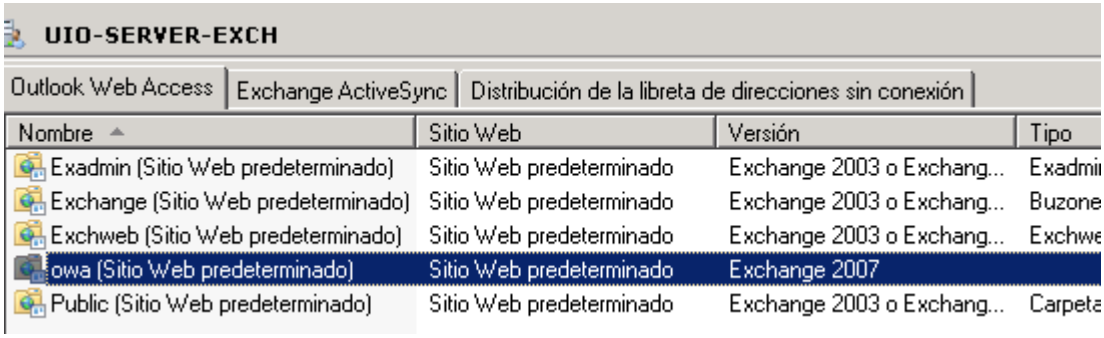


- Una vez seleccionado el usuario hacer clic en siguiente.

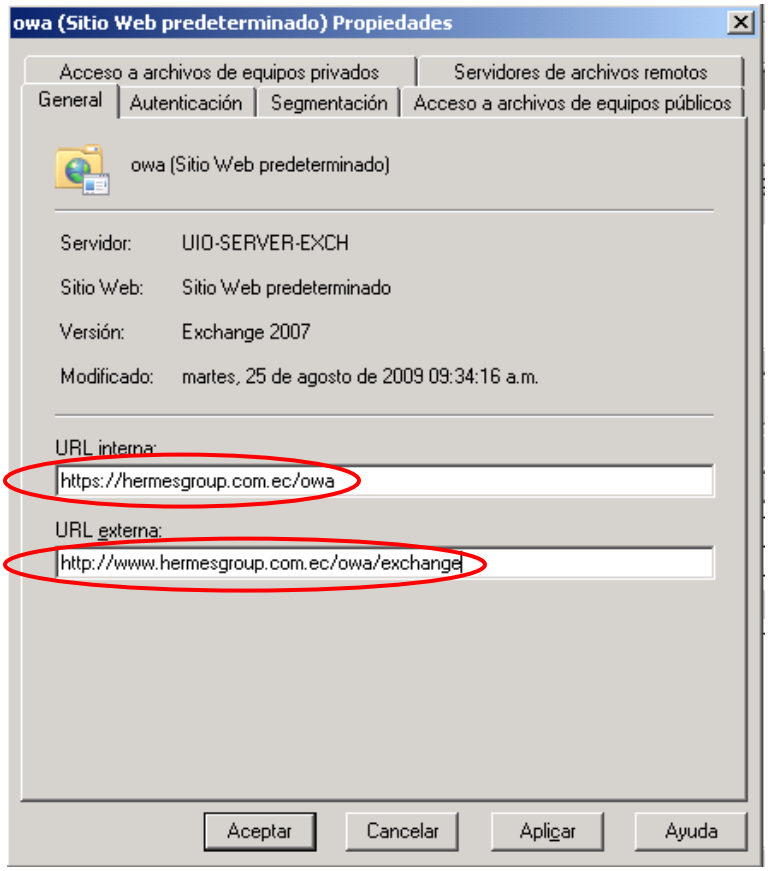
- Dejar los valores predeterminados, con esto ya se tiene creado el primer usuario, para crear los demás usuarios repetimos los pasos anteriormente mencionados.

Configuración OWA

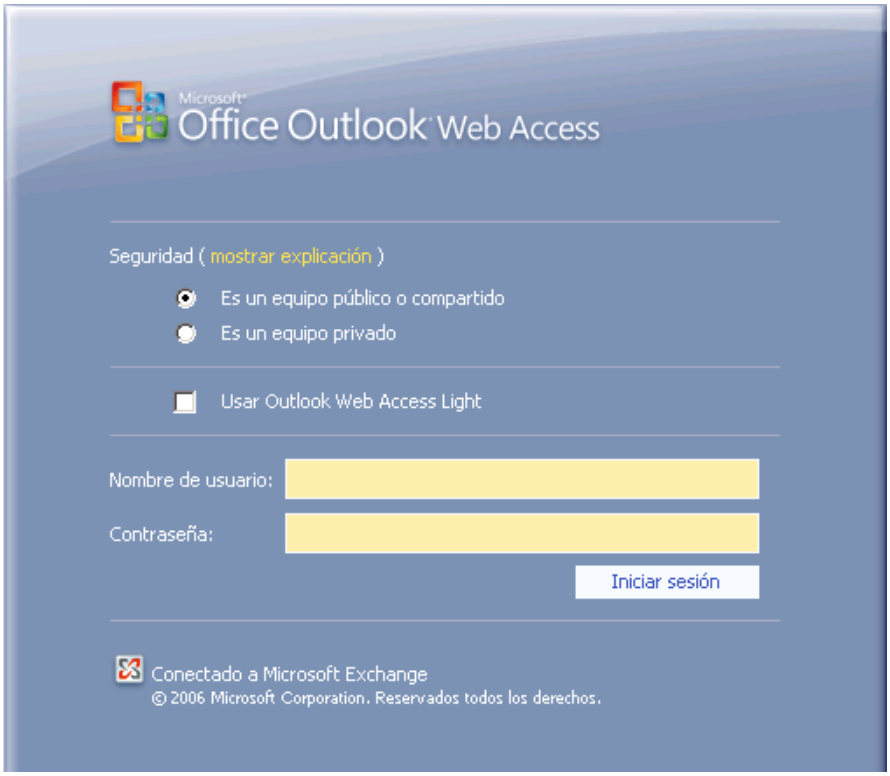
- Para la configuración de los buzones de correo abrir la Consola de Administración de Exchange.
- En el panel de la izquierda seleccionar Configuración de Servidores
- Y dentro de Configuración de Servidores seleccionar Acceso de cliente



- Dar doble clic en la opción OWA
- Verificar la dirección que permitirá ejecutar OWA, para la empresa Hermes Express se configuró la dirección https://hermesgroup.com.ec/owa como dirección interna y https://www.hermesgroup.com.ec/owa/exchange como dirección externa.



- Para saber que se configuró correctamente el servidor Exchange, en Internet Explorer poner la dirección https://hermesgroup.com.ec/owa, se mostrará la siguiente pantalla:


Microsoft
Office Outlook Web Access
Seguridad (mostrar explicación)
Es un equipo público o compartido
Es un equipo privado
Usar Outlook Web Access Light
Nombre de usuario:
Contraseña:
Iniciar sesión
Conectado a Microsoft Exchange
© 2006 Microsoft Corporation. Reservados todos los derechos.

ANEXO 11

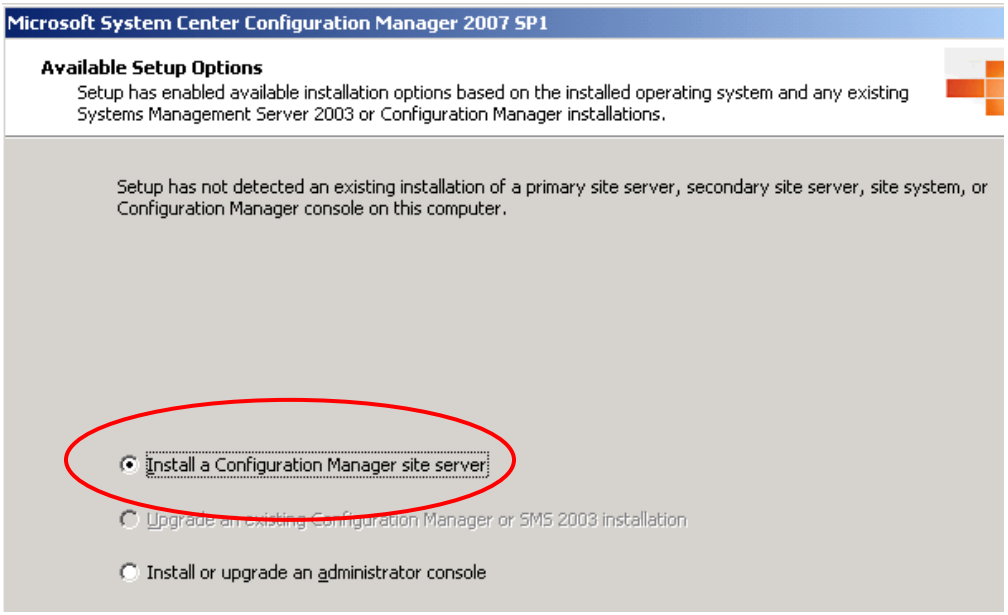
PASOS PARA INSTALAR SCCM

Los requisitos previos para la instalación de SCCM son:

- Tener instalado IIS
- Componentes: BITS, Internet Information Services Manager, ASP, WebDAV, WWW.
- Tener instalado SQL Server 2005 con Service Pack 2
- Tener Instalado WSUS 3.0 con Service Pack 1
- Tener actualizado el Esquema del Directorio Activo

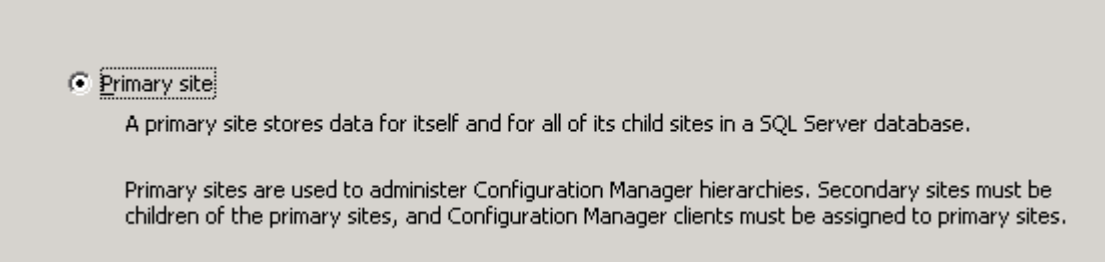
Una vez instalado todos los prerrequisitos seguir los siguientes pasos para llevar a cabo la instalación de SCCM 2007:

- Insertar el DVD de SCCM 2007
- En la primera pantalla poner Siguiente
- Seleccionar Install a Configuration Manager site server

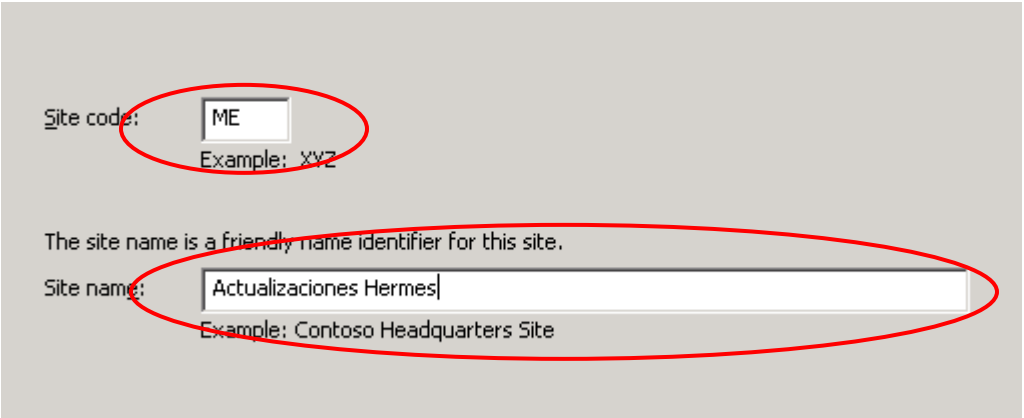


- En la siguiente pantalla aceptar la licencia

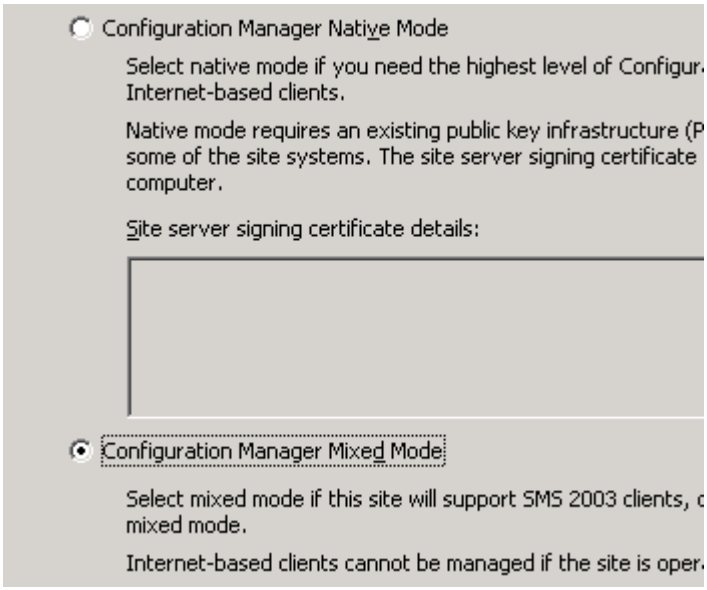
- En la siguiente pantalla seleccionar Custom Settings
- En la siguiente pantalla seleccionar Primary site, porque es el primer servidor que se está implementando de System Center Configuration Manager 2007



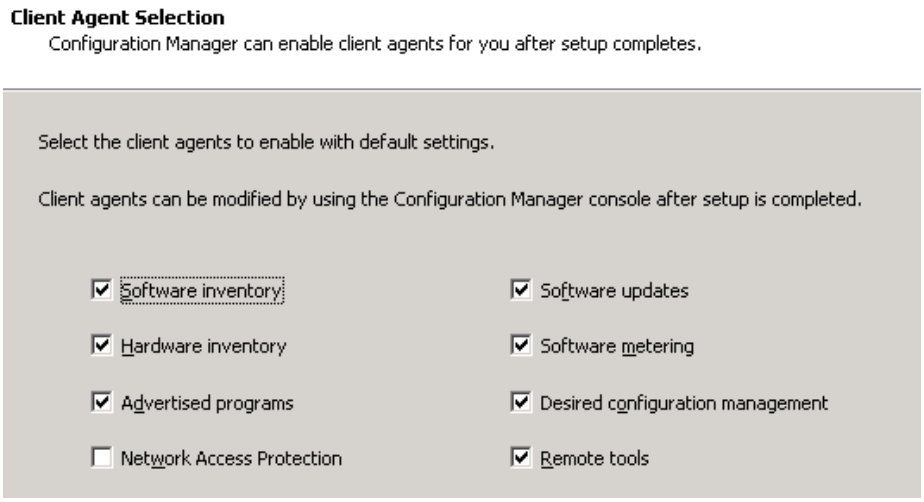
- En la siguiente pantalla dejar predeterminadamente
- En la siguiente pantalla se verá la licencia con la cual va a instalar
- Aceptar predeterminadamente el lugar en el disco duro donde se instalará SCCM
- En la siguiente pantalla poner el código de sitio, esto nos permitirá reconocer el sitio como único y el nombre del sitio



- En la siguiente pantalla seleccionar Configuration Manager Mixed Mode

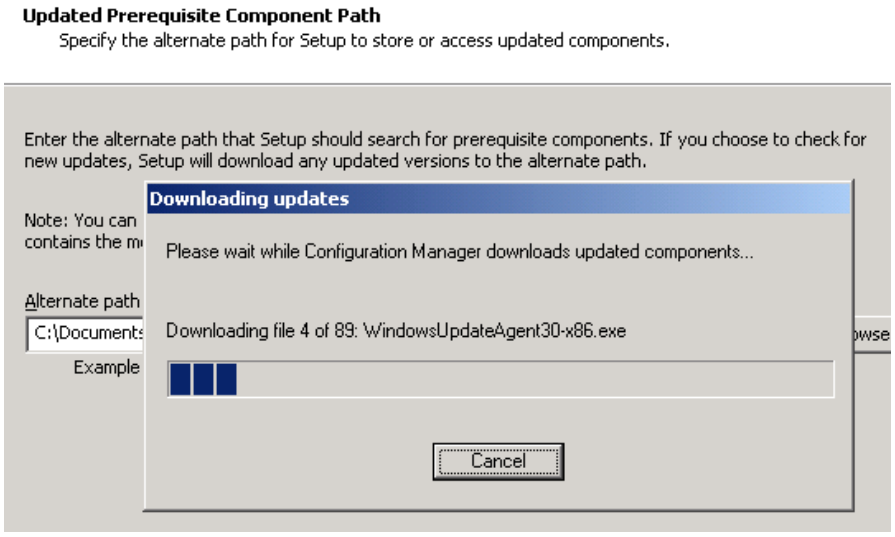


- En la siguiente pantalla ver la selección de los componentes que se van a implementar con la instalación.

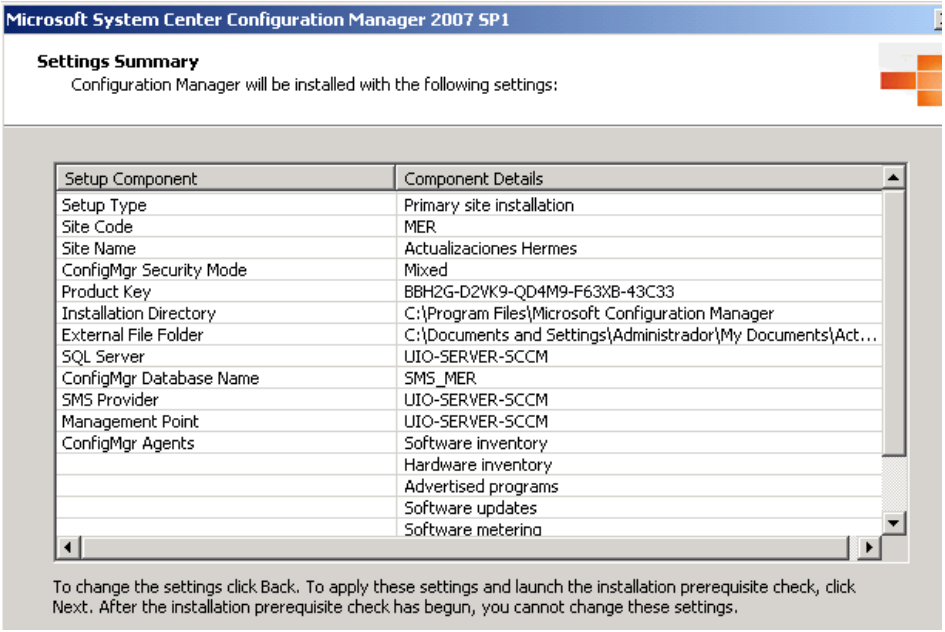


- En la siguiente pantalla se verá las configuraciones que el instalador va hacer en SQL Server 2005 dejar predeterminadamente como se muestra
- En la siguiente pantalla escoger si management point
- En la siguiente pantalla seleccionar el puerto que va a permitir realizar la comunicación con los clientes predeterminadamente es el puerto 80 pero este valor es configurable

- En la siguiente pantalla poner el lugar o la carpeta donde se va a tener acceso a las actualizaciones, en este punto SCCM descarga las actualizaciones automáticamente desde el internet. Esperar hasta que se descarguen todas las actualizaciones.



- Una vez que termina la descarga de las actualizaciones ver la pantalla de resumen



ANEXO 12

PASOS PARA LA INSTALACIÓN DE SHAREPOINT SERVER 2007

Los requisitos previos para la implementación son:

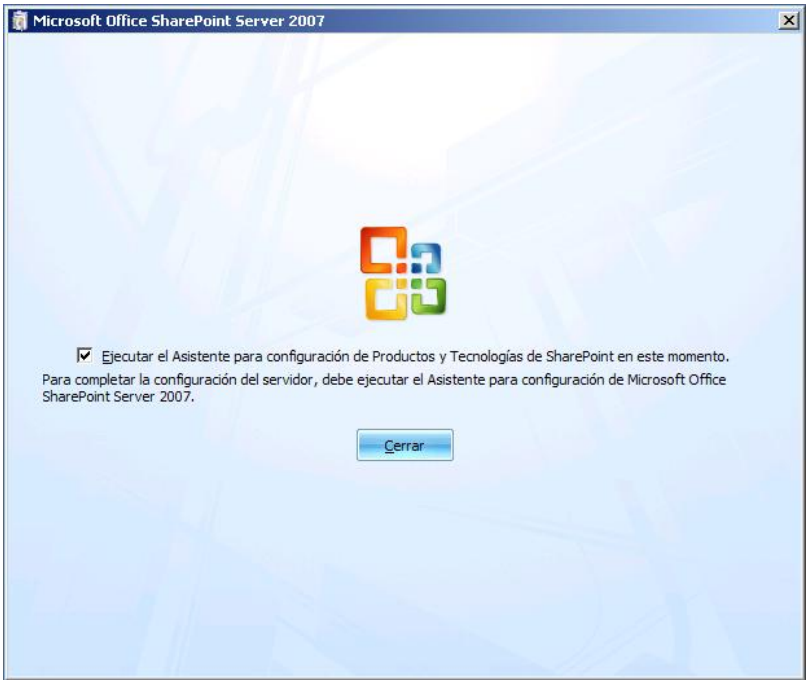
- Tener instalado Internet Information Server 6.0
- Tener instalado .NET Framework 3.0
- Tener habilitado ASP.NET 2.0
- Tener instalado SQL Server 2005 Express Edition

Para realizar la instalación realizar los siguientes pasos:

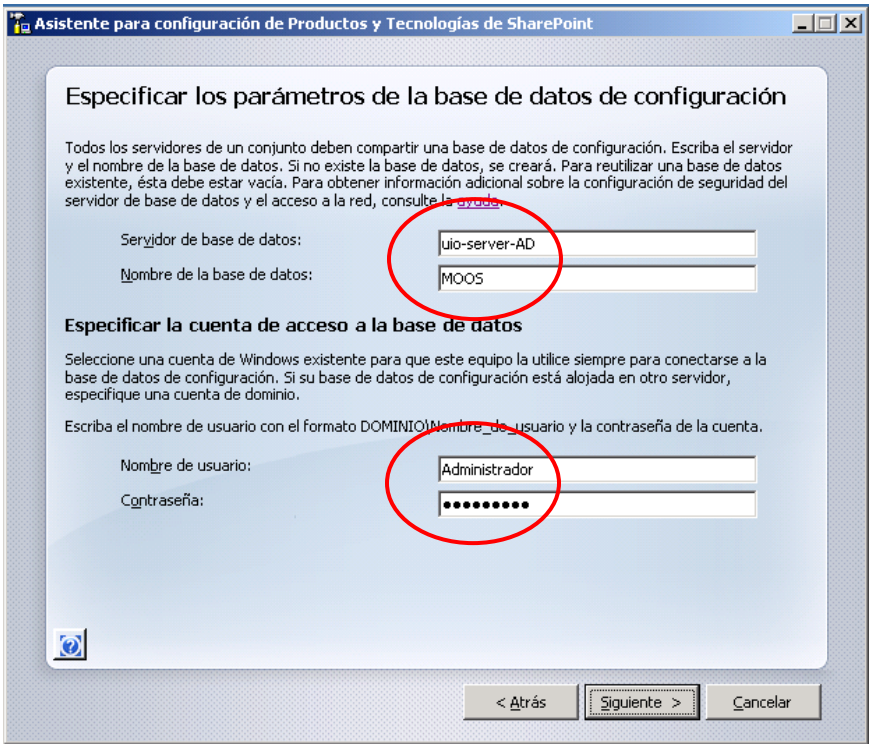
- En la primera pantalla poner el numero de serial
- En la siguiente pantalla aceptar la licencia
- Hacer clic en Avanzadas
- En la siguiente pantalla seleccionar la opción Completa, para poder instalar todos los componentes de Sharepoint Server
- Esperar a que se complete la instalación

Para realizar la configuración realizar los siguientes pasos:

- Una vez finalizada la instalación aparecerá una pantalla como la siguiente, esta pantalla nos dará la apertura de la pantalla para continuar con la configuración.

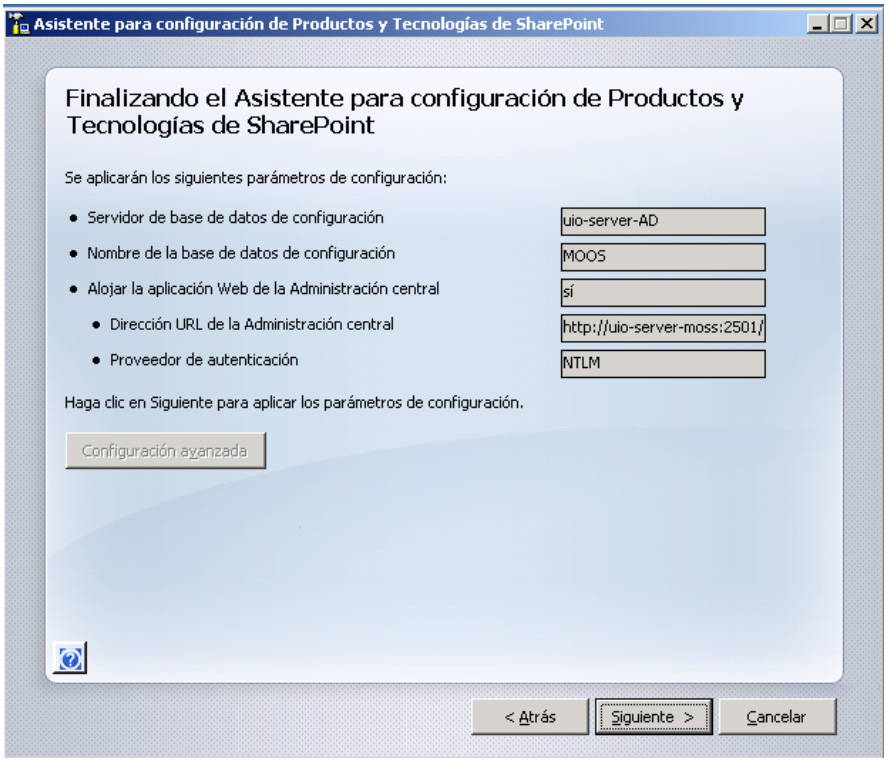


- En la primera pantalla hacer clic en siguiente
- En la siguiente pantalla especificar los valores de la base de datos.

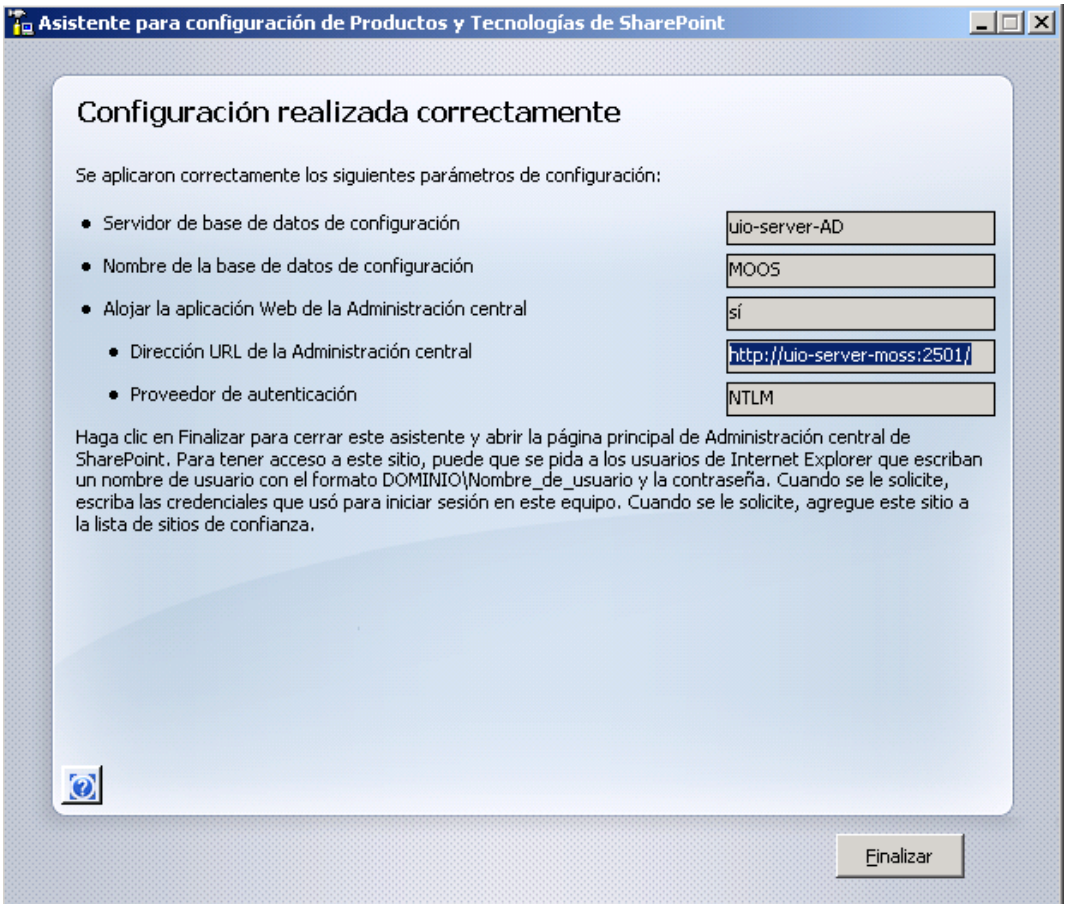


- En la siguiente pantalla especificar el número de puerto para la administración del servidor, y la configuración de seguridad.

- Una vez realizadas las configuraciones pertinentes, se verá una pantalla de resumen mostrando los parámetros del servidor



- Hacer clic en siguiente y esperar a que se apliquen todas las configuraciones.



Crear Aplicación Web

Una vez instalado y configurado el servidor es necesario crear los sitios para tener un flujo de carga en la empresa Hermes Express. Para esto realizar los siguientes pasos:

- En un navegador web ingresar al sitio http://uio-server-moss:2501/, esto abrirá la página de administración de Sharepoint Server
- En la barra de de vínculo superior, hacer clic en Administración de Aplicaciones
- En la página Administración de aplicaciones, en la sección Administración de aplicaciones Web de SharePoint, haga clic en Crear o extender una aplicación Web.
- En la página Crear o extender una aplicación Web, en la sección Agregar una aplicación Web de SharePoint, hacer clic en Crear una nueva aplicación Web.
- En la página Crear una nueva aplicación Web, en la sección Sitio Web de IIS, seleccionar una de estas opciones:

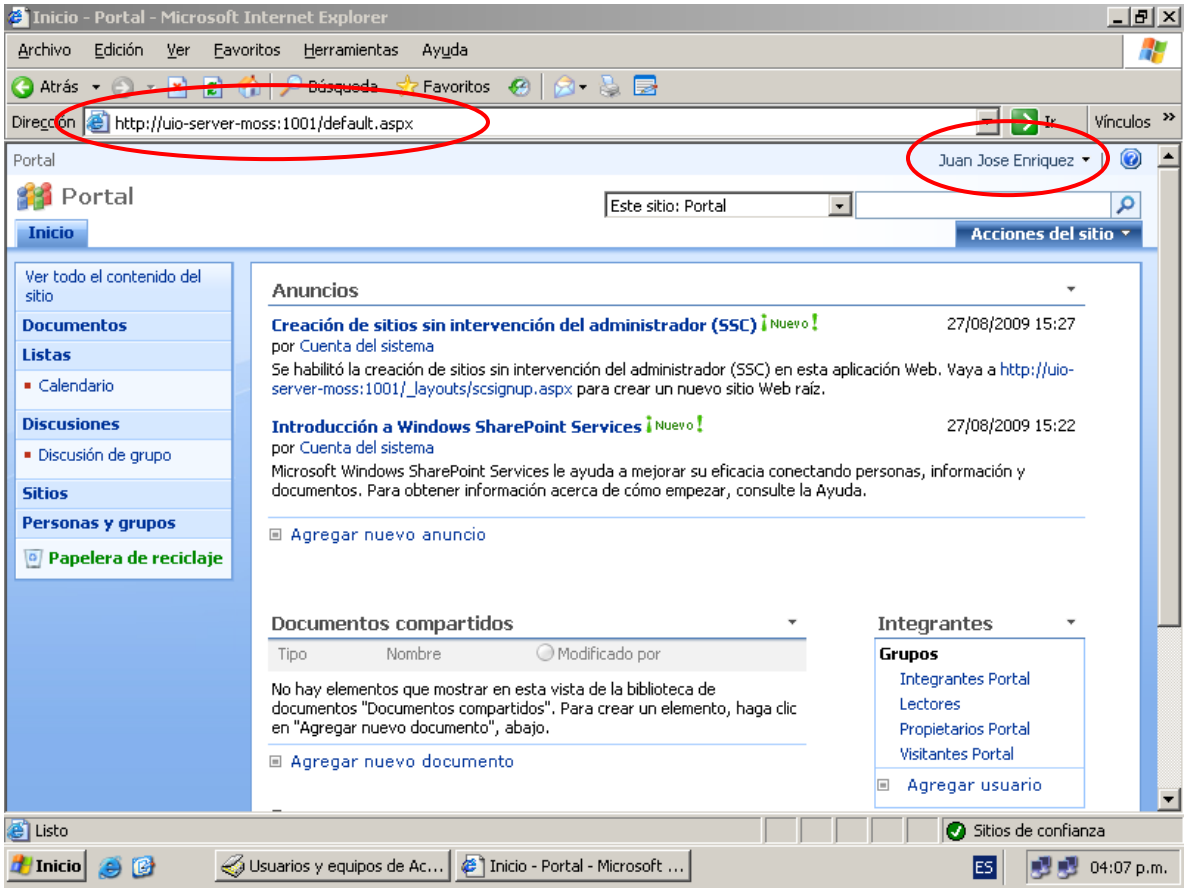
- Usar un sitio Web de IIS existente. Si se selecciona esta opción, hacer clic en el sitio Web de IIS existente en la lista correspondiente.
- Crear un nuevo sitio Web de IIS. Si se selecciona esta opción, configurar lo siguiente:

- En el cuadro Descripción, aceptar la descripción proporcionada o escribir una nueva para la aplicación Web.
- En el cuadro Puerto, aceptar el valor proporcionado o escribir uno nuevo para el puerto que utilizará la aplicación Web.
- En el cuadro Encabezado de host, escribir un encabezado de host.
- En el cuadro Ruta de acceso, aceptar la ruta proporcionada o escribir una nueva.
- En la sección Configuración de seguridad, en Proveedor de autenticación, seleccionar Negociar (Kerberos) o NTLM.
- En Permitir anónimo, seleccionar Sí o No.
- En Usar Capa de sockets seguros (SSL), seleccionar Sí o No.
- Importante Si usa SSL, se tiene que agregar el certificado apropiado en cada servidor mediante las herramientas de administración de IIS.
- En la sección Dirección de URL de carga equilibrada, en el cuadro Dirección URL, escribir la dirección URL que se usará para tener acceso a la aplicación Web. La dirección URL debería estar en formato http://nombre de servidor:puerto. Si se han configurado en el servidor varias zonas, se puede hacer clic en una zona opcionalmente en la lista Zona.
- En la sección Grupo de aplicaciones, seleccionar una de las siguientes opciones:
  - Usar grupo de aplicaciones existente. Si se selecciona esta opción, hacer clic en el grupo de aplicaciones para utilizarlo desde la lista correspondiente.
  - Crear un grupo de aplicaciones nuevo. Si se selecciona esta opción, configurar lo siguiente:
    - En el cuadro Nombre del grupo de aplicaciones, escribir el nombre del nuevo grupo de aplicaciones.
    - En Seleccione una cuenta de seguridad para este grupo de aplicaciones, seleccionar Predefinida o Configurable. Si se selecciona Predefinida,

hacer clic en la cuenta de seguridad para usarla en la lista correspondiente. Si se selecciona Configurable, escribir las credenciales de la cuenta en los cuadros Nombre de usuario y Contraseña.

- En la sección Nombre y autenticación de base de datos, en Autenticación de base de datos, seleccionar una de estas opciones:
  - Autenticación de Windows (recomendada)
  - Autenticación de SQL. Seleccionar esta opción si ha creado previamente la base de datos y se desea utilizar la autenticación de SQL. Si se selecciona esta opción, escribir las credenciales de la cuenta en los cuadros Cuenta y Contraseña.

- Hacer clic en Aceptar.
- Para el caso de la empresa Hermes Express la dirección de la aplicación web es http://uio-server-moss:1001
- Una vez que se ingresa al sitio se debe escribir el nombre de usuario y contraseña.


Inicio - Portal - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección http://uio-server-moss:1001/default.aspx
Vínculos
Portal
Juan Jose Enriquez
Portal
Este sitio: Portal
Inicio
Acciones del sitio
Ver todo el contenido del sitio
Documentos
Listas
Calendario
Discusiones
Discusión de grupo
Sitios
Personas y grupos
Papelera de reciclaje
Anuncios
Creación de sitios sin intervención del administrador (SSC) ¡Nuevo!
27/08/2009 15:27
por Cuenta del sistema
Se habilitó la creación de sitios sin intervención del administrador (SSC) en esta aplicación Web. Vaya a http://uio-server-moss:1001/_layouts/scsignup.aspx para crear un nuevo sitio Web raíz.
Introducción a Windows SharePoint Services ¡Nuevo!
27/08/2009 15:22
por Cuenta del sistema
Microsoft Windows SharePoint Services le ayuda a mejorar su eficacia conectando personas, información y documentos. Para obtener información acerca de cómo empezar, consulte la Ayuda.
Agregar nuevo anuncio
Documentos compartidos
Tipo Nombre Modificado por
No hay elementos que mostrar en esta vista de la biblioteca de documentos "Documentos compartidos". Para crear un elemento, haga clic en "Agregar nuevo documento", abajo.
Agregar nuevo documento
Integrantes
Grupos
Integrantes Portal
Lectores
Propietarios Portal
Visitantes Portal
Agregar usuario
Listo
Sitios de confianza
Inicio
Usuarios y equipos de Ac...
Inicio - Portal - Microsoft ...
ES
04:07 p.m.

ANEXO 13

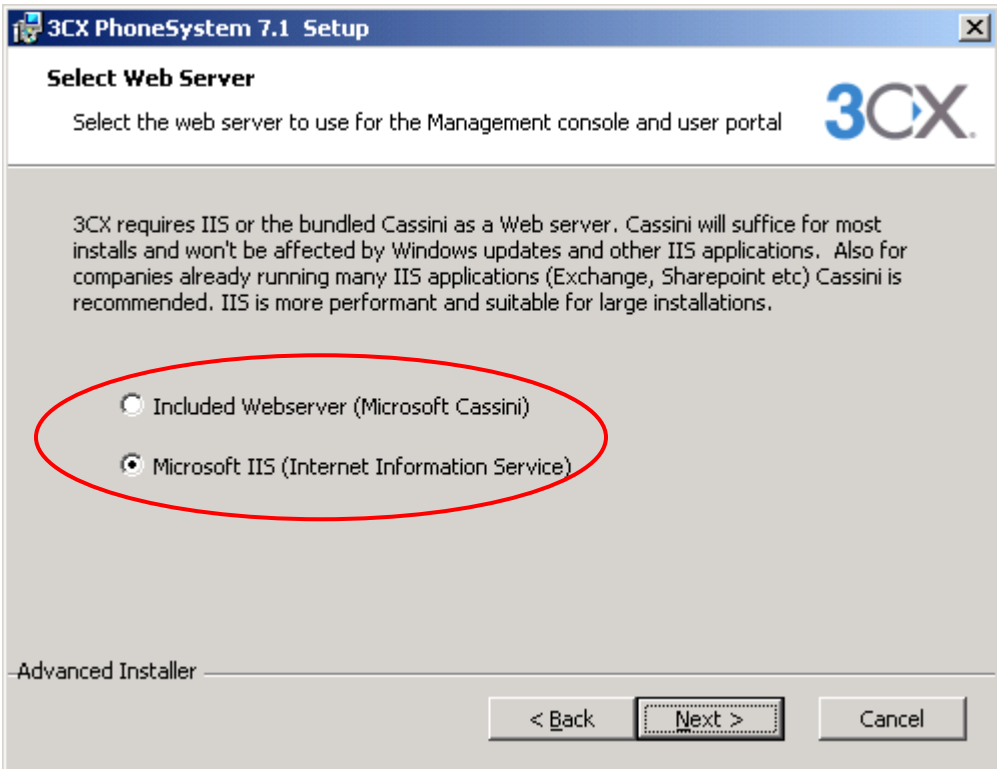
PASOS PARA LA INSTALACIÓN DE LA CENTRAL TELEFONICA 3CX

Para llevar a cabo la instalación de este software se necesita tener los siguientes prerrequisitos:

- Internet Information Services 6.0
- .NET Framework 2.0
- Tener habilitado ASP.NET 2.0
- Una IP publica estática

Una vez que se tiene todos los prerrequisitos instalados seguir los siguientes pasos para la implementación:

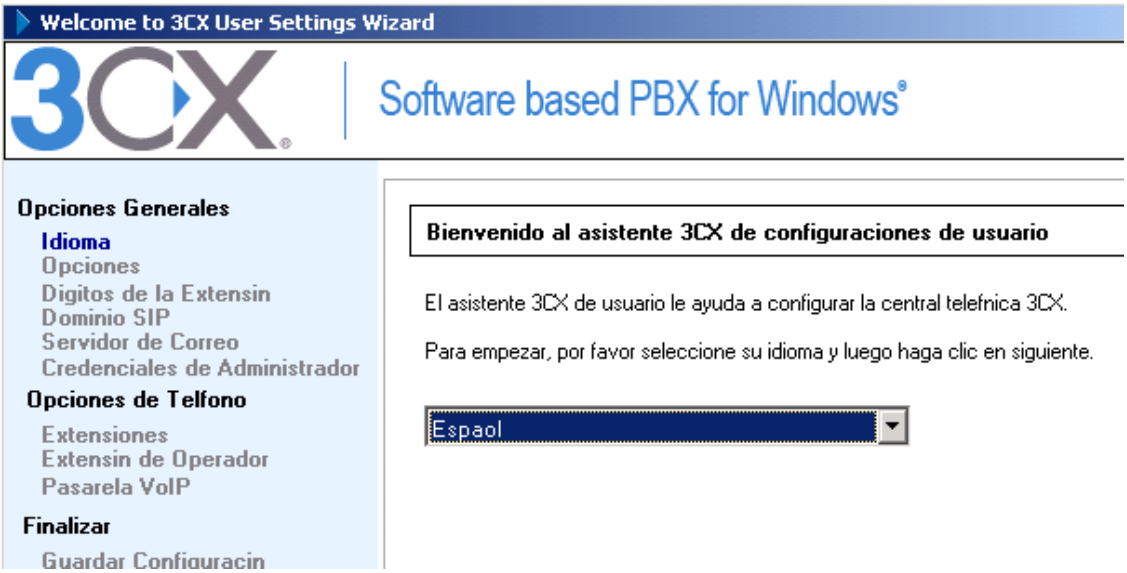
- Descargar el programa para servidor de la siguiente página:
  - http://www.3cx.es/centralita-telefonica/download.html
- En la primera pantalla están los prerrequisitos para la implementación
- En la siguiente pantalla aceptar la licencia
- En la siguiente pantalla verificar el lugar donde se va a implementar el programa
- En la siguiente pantalla seleccionar la opción de IIS, ya que con esta configuración se tendrá acceso a la consola de manejo y los portales de usuario.



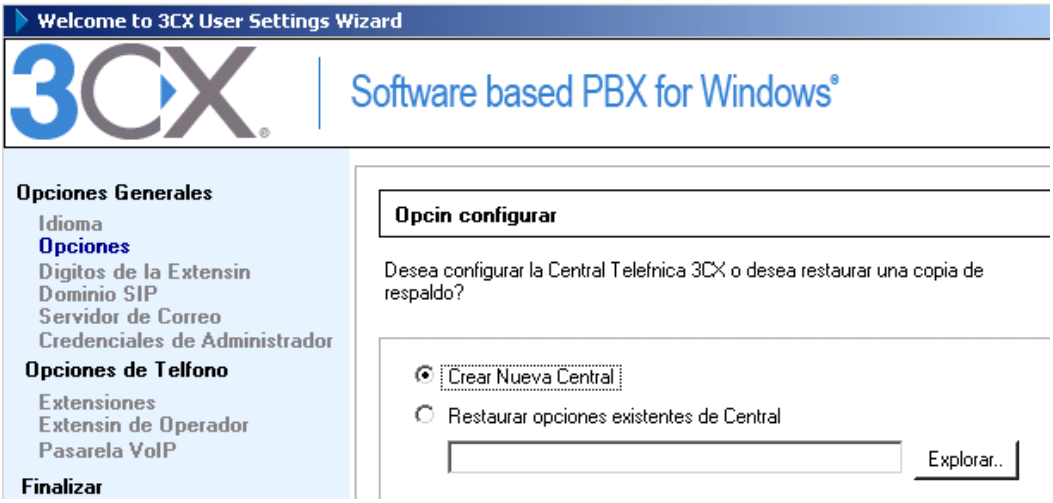
- Con esto en la siguiente pantalla poner Instalar y esperar hasta que el programa termine su instalación.

Una vez instalado continuar con la configuración para esto realizar lo siguiente:

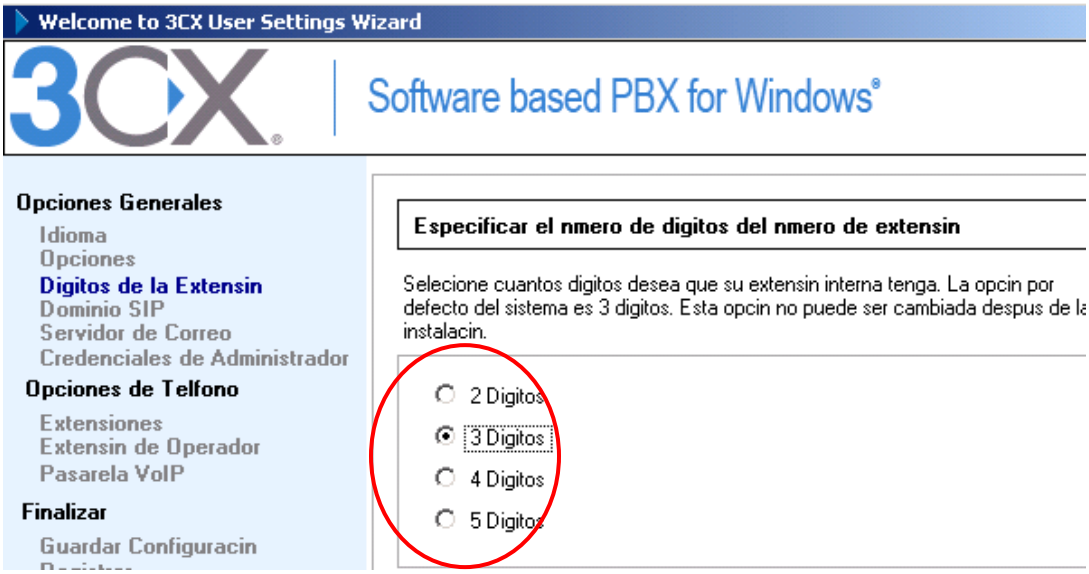
- Esperar que se inicie automáticamente el asistente para la configuración
- Se desplegara la pantalla para la configuración, en la primera pantalla seleccionar el idioma en el cual se va a configurar.



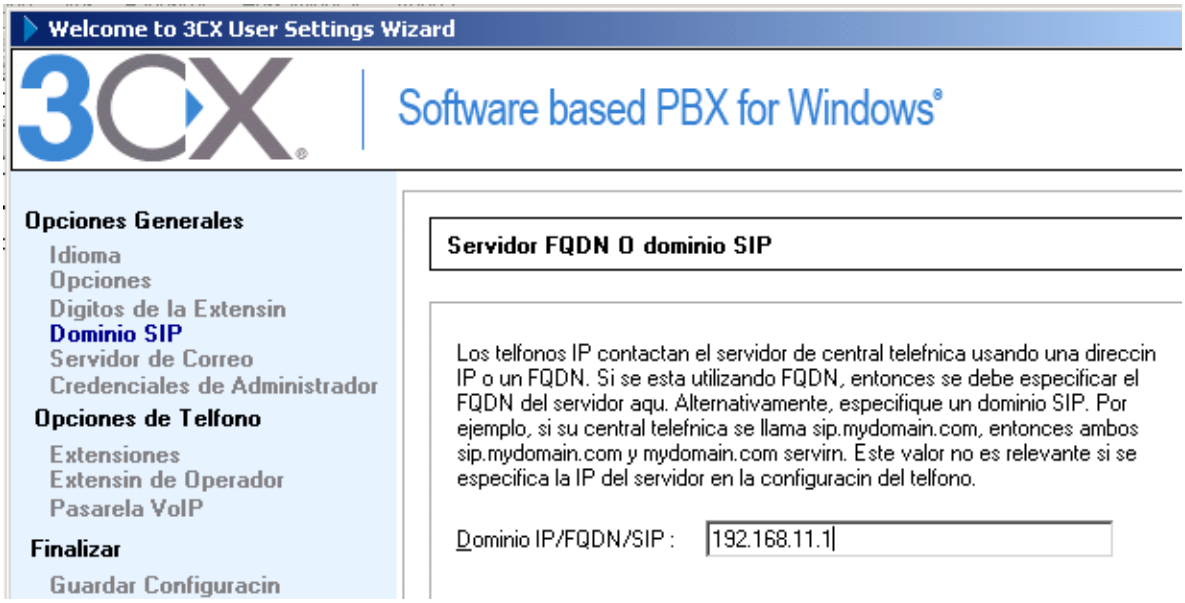
- Como es la primera central telefónica que se implementa seleccionar en la siguiente pantalla Crear nueva Central



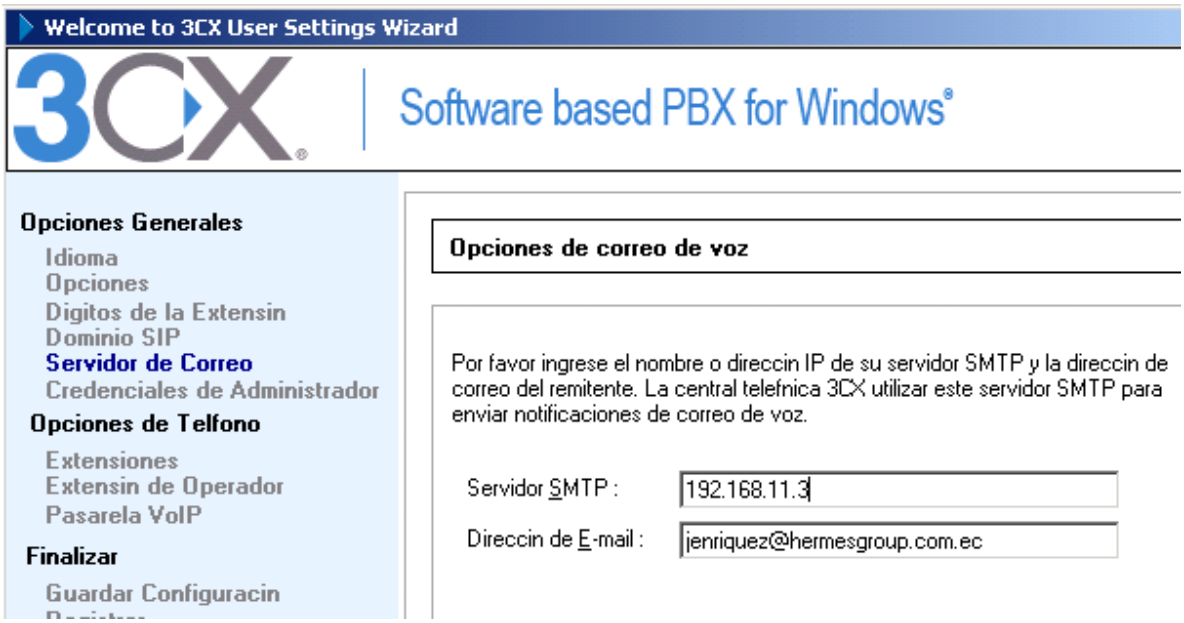
- En la siguiente pantalla especificar cuantos dígitos se desea tener para las extensiones, para la empresa Hermes Express de definió que las extensiones sean de 3 dígitos



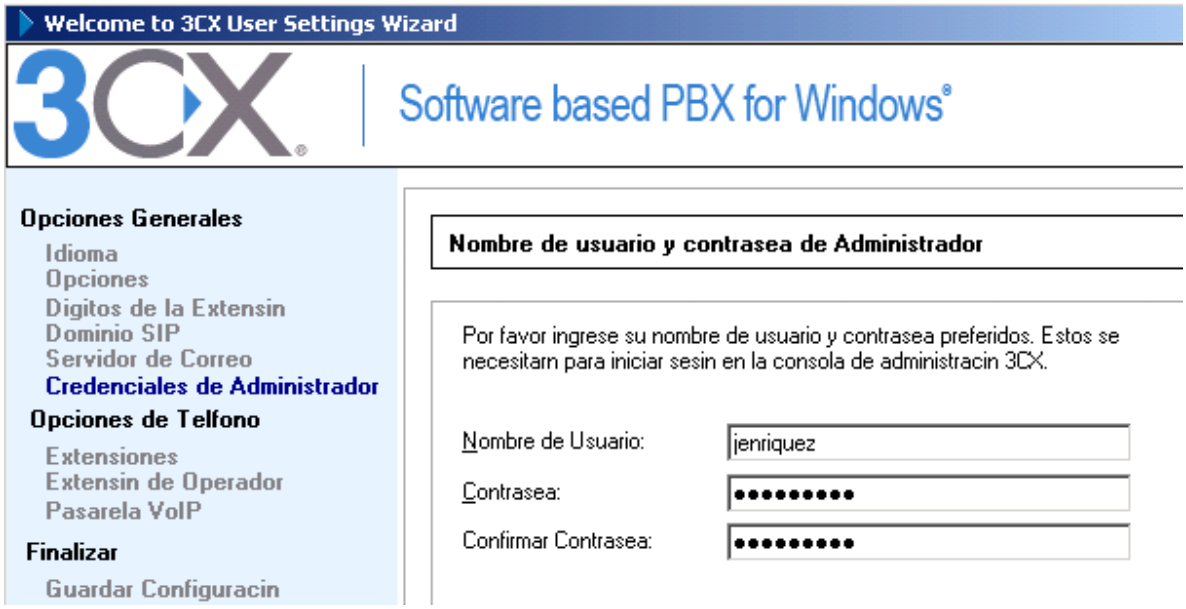
- En la siguiente pantalla especificar la dirección IP del servidor SIP, el cual va a permitir tener llamadas salientes de nuestro servidor, la estructura de las extensiones es la siguiente:
- Operadora 100
- Rubén Enríquez 101
- Juan José Enríquez 102
- Asistente de Tecnología 103
- Diana Torres 104
- Asistente de Courier 105
- Diseñador 106
- Extensiones libres desde la 107 a la 125



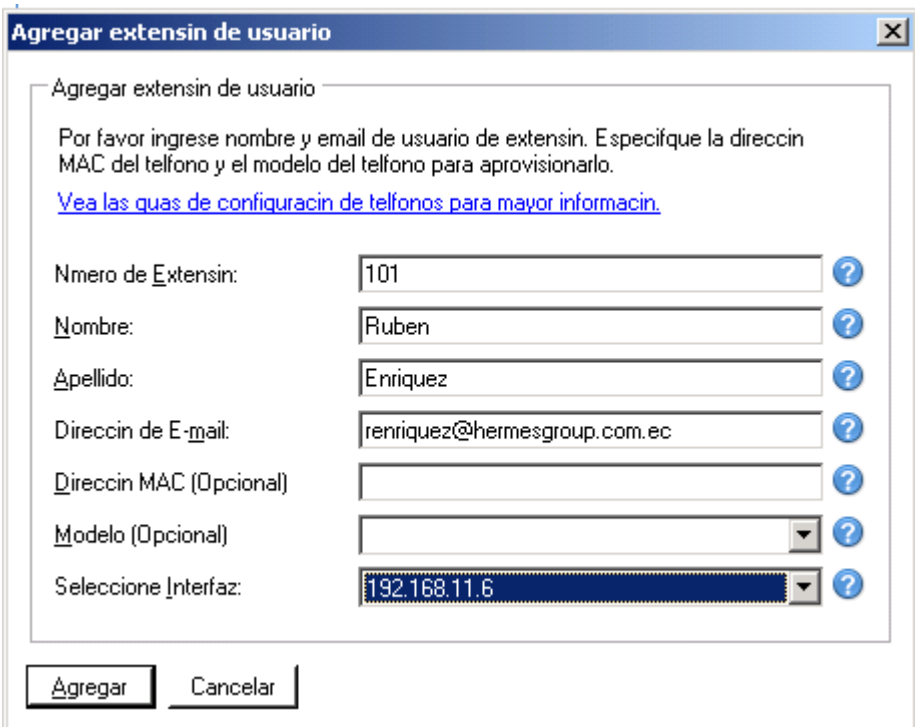
- En la siguiente pantalla especificar la dirección IP del servidor de correo, permitiendo así la integración con Exchange 2007.



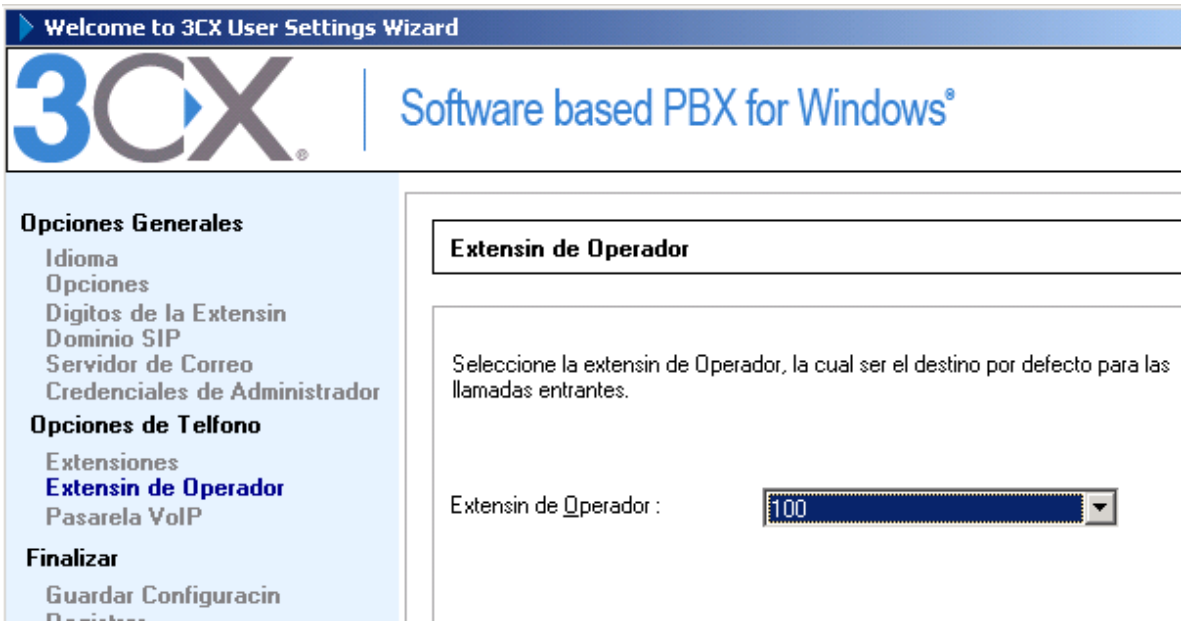
- En la siguiente pantalla especificar el nombre de usuario del administrador del sistema y la contraseña



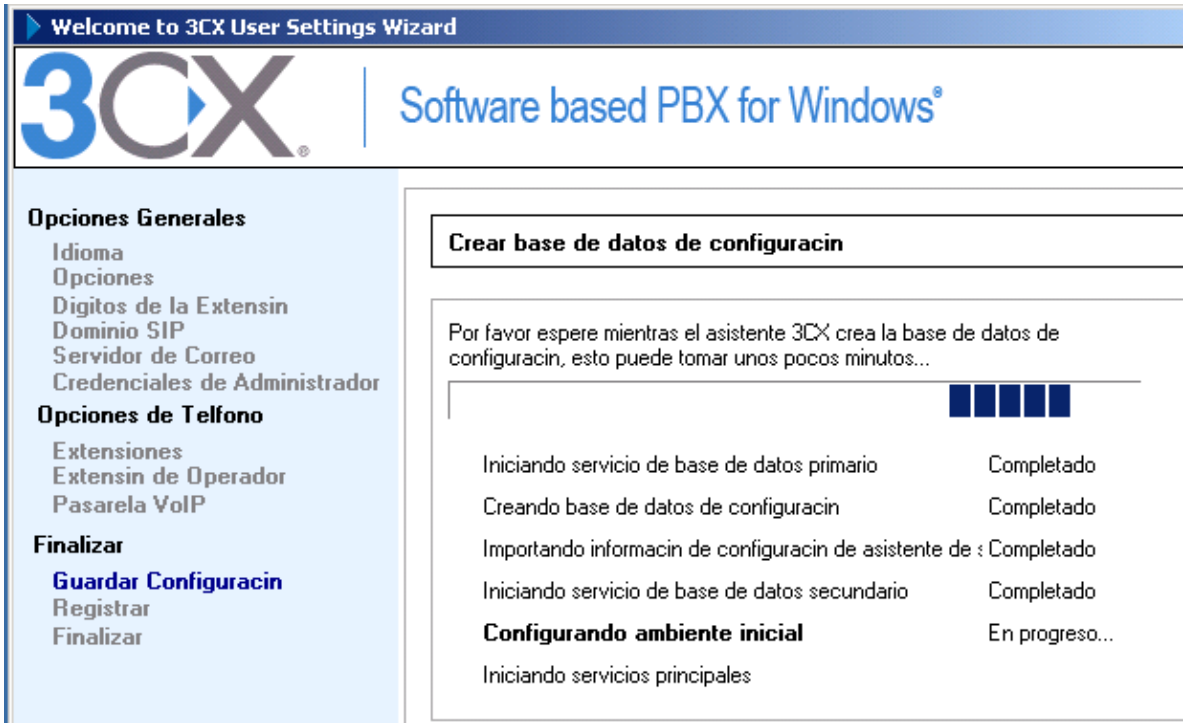
- En la siguiente pantalla se configuran las extensiones como se ve en la siguiente pantalla



- Una vez configuradas todas las extensiones estructuradas y creadas en la siguiente pantalla es necesario especificar la extensión de la operadora.



- Una vez realizadas las configuraciones anteriores, esperar a que la aplicación Cree la Base de Datos de Configuración



- Una vez completado el proceso se encuentra instalado el servidor de VOIP para el funcionamiento.

ANEXO 14

CARTA DE AUSPICIO POR LA EMPRESA HERMES EXPRESS

Quito, 30 de junio de 2010

A quien interese

Por medio de la presente la Empresa Hermes Express auspicia el desarrollo de la tesis titulada "Análisis, Diseño e Implementación de una Solución Tecnológica basada en Metodología MSF para empresas Pymes de Courier" desarrollada en nuestras instalaciones por el Sr. Juan José Enríquez con C.I. 171672306-7.

La empresa se compromete a permitir utilizar la infraestructura necesaria para el cumplimiento del trabajo presentando.

Atentamente;

Paola López

Gerente General

ANEXO 15

CARTA PARA USO DE MATERIAL MICROSOFT

Quito, 30 de junio de 2010

A quien corresponda

Por medio de la presente Business IT (Gestiontec S.A.) autoriza al señor Juan José Enríquez con C. I. 171672306-7 a utilizar material Microsoft para la elaboración y defensa de tesis titulada "Análisis, Diseño e Implementación de una Solución Tecnológica basada en Metodología MSF para empresas Pymes de Courier", este certificado tiene 6 meses de validez.

Atentamente

Ing. Boris Arciniegas

Presidente Business IT (Gestiontec S.A.)