



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES
ARAGON**

**TECNOLOGÍAS DE LA INFORMACIÓN APLICADAS
A EMPRESAS**

**INFORME DEL EJERCICIO
PROFESIONAL**

**QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN**

P R E S E N T A :

BEATRIZ CORIA PERALTA



**DIRECTOR DE TESIS:
M. EN C. MARCELO PÉREZ MEDEL**

MEXICO

2015



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

Deseo expresar mi gratitud a mis padres, al Sr José Esteban Coria Constantino y a la Sra. Casilda Peralta Valverde, por ser la fuente de apoyo incondicional a lo largo de mi vida y motivado mi formación académica, creyendo en mí en todo momento, confiando en las habilidades que Dios me ha dado.

A mi abuelita Jovita Valverde Lemus quien con su ejemplo de vida me motivo todos los días a continuar mis estudios, a mis hermanos quienes me aportaron sus conocimientos y enseñanzas, a mis tíos que me han dado buenos consejos en mi vida.

A mis profesores a quienes les debo, gran parte de mis conocimientos académicos, a la universidad que me permitió desarrollarme académicamente para lograr esta meta y que abre sus puertas, para preparar jóvenes para un futuro competitivo.

A mi asesor Marcelo Pérez Medel por haberme ayudado a la realización de esta.

ATENTAMENTE
Beatriz Coria Peralta

Tecnologías de la Información aplicadas a empresas

Introducción.....
Capítulo 1: Corporativo Almaba y empresa Viana
1.1 Historia de Corporativo Almaba misión y visión
1.2 Historia de Viana misión y visión
Capítulo 2:Descripción de actividades en Corporativo Almaba
2.1 Participación en el proceso de instalación de rastreo satelital
2.2 Manejo administrativo de correo electrónico en Linux.....
Capítulo 3:Descripción de actividades en Viana área de sopote técnico
3.1 Mantenimiento preventivo y correctivo de pc y laptop.....
3.2 Instalación de software en equipos pc y laptop
3.3 Configuración de terminales tontas para tiendas
Capítulo 4: Descripción de actividades en Viana área redes
4.1 Descripción general de puesto y actividades en área de redes.....
4.2 Administración de herramientas de respaldos y antivirus.....
4.3 Administración de Proxy
4.4 Administración e instalación de servidores
4.5 Administración de Active Directory.....
4.6 Administración de Exchange
Conclusiones.....
Bibliografía

Introducción

El presente trabajo contiene la descripción de la experiencia laboral adquirida en el área de sistemas.

En estas empresas se trabaja con diferentes sistemas operativos, existen diferentes tipos de sistemas operativos de los más usados son Windows, Linux, Unix y Mac os, cada uno de ellos tiene diferentes versiones. Windows es un sistema operativo multitarea, de 32 o 64 bits, los objetivos de este sistema son ofrecer extensibilidad, transportabilidad, seguridad confiabilidad, compatibilidad, desempeño y soporte internacional.

El sistema operativo Linux es parecido a Unix, que se diseñó para ejecutar el mayor número posible de aplicaciones, su código fuente se ofrece gratuitamente y existen diferentes distribuciones por mencionar algunas existen Red Hat, Debian, Fedora por mencionar algunos.

El sistema operativo Unix es un sistema operativo portable, multitarea y multiusuario, desarrollado en 1969.

El sistema operativo Mac os es un sistema operativo basado en Unix, es comercializado por la compañía Apple, es incluido en su gama de computadores Macintosh y dispositivos móviles iPhone.

Existen actividades que ayudan a mantener los equipos de cómputo trabajando de manera óptima, dichas actividades es el mantenimiento preventivo y correctivo.

El preventivo, se realiza a un equipo que se encuentra en funcionamiento, pero se realiza para prevenir alguna falla, este garantiza un periodo de uso tiene factible, en cuanto al mantenimiento correctivo es el que se realiza con el fin de corregir defectos en los equipos de cómputo.

Se utilizan antivirus, que ayudaran a bloquear, desinfectar, prevenir y proteger los equipos, de códigos maliciosos o software malintencionado que provoca fallas graves en los equipos de cómputo y servidores.

Para administrar usuarios, grupos, contraseñas, permisos, compartir archivos, políticas de acceso que permiten autenticar usuarios y equipos conocidos, se utilizan servidores controladores de dominio, este servicio en Windows se administra con Active Directory, es un servicio de directorio en una red distribuida de computadoras.

En cuanto, a lo que se refiere a correo electrónico se pueden utilizar formas diferentes de creación de correos.

En lo que se refiere a software con Windows, se utiliza un software llamado Exchange este me permite la creación de correo electrónico de un usuario, permite restricciones para que sea solo un correo de manera interna o externa, acceso al correo vía web y redireccionamiento de correo hacia otro usuario.

Como mencionaba anteriormente existe Linux que es un sistema operativo que también cuenta con herramientas para creación y administrar correo electrónico, el correo es configurable con por protocolos como SMTP y POP3.

Una base de datos es aquella que contiene datos pertenecientes a un mismo contexto y se organiza de manera sistemática, dichas bases pueden ser manejadas con software como SQL, postgresql, mysql.

Es importante contar con respaldos de la información, como bases de datos, active directory, archivos importantes, para disponer de ellos si se requieren en algún otro momento, esto se puede lograr con herramientas dedicadas.

Backup Exec es un software de copias de seguridad y recuperación, mismo que ayuda a cumplir lo antes mencionado.

Para el control de accesos y negaciones, a páginas de internet, se utiliza proxy, esto permite controlar, el consumo de anchos de banda en los enlaces para no saturarlos, evitar el óseo del personal, evitar descargas que puedan ser de riesgo para los equipos.

El presente trabajo ayudara a entender el uso y la aplicación de algunas tecnologías de la información, con ejemplos reales aplicados en empresas, el fin que se busca es obtener el mejor diseño de soluciones a los procesos operativos, que se presentan el área de sistemas dentro de las empresas.

En el primer capítulo hablo sobre las empresas en las que labore, la primera Corporativo Almaba por medio año y la segunda Viana donde preste mis servicios por cuatro años diez meses.

En el segundo capítulo describo las actividades que realice en Corporativo Almaba entre ellas la participación en la instalación del rastreo satelital.

El tercer capítulo describe las actividades que realice, en Viana en el área de soporte técnico, entre ellas el mantenimiento preventivo, correctivo equipos y la configuración de terminales tontas.

El cuarto capítulo describe las actividades que realice, en Viana en el área de redes, como la administración de herramientas de respaldo, antivirus, proxy's, active directory, Exchange y servidores.

1 Corporativo Almaba y empresa Viana

Las empresas en las que he laborado son 2 a continuación describo brevemente a que se dedican cada una de ellas.

Corporativo Almaba es una empresa dedicada a prestar servicios de rastreo satelital, seguridad privada a terceros, transporte, custodias locales y foráneas.

Viana es una empresa dedicada a la venta de muebles, colchones, línea blanca, hogar, electrónica, perfumería, calzado, ropa, celulares, juguetería, y recargas de tiempo aire.

1.1 Historia de Corporativo Almaba misión y visión.

Corporativo Almaba

Corporativo Almaba es una empresa que surge en el año de 2010 2009, surge como una empresa enfocada a prestar servicios de seguridad privada a terceros y posteriormente incursiona en seguridad en transporte de mercancía.

Visión

“Ser una empresa líder e innovadora con sistemas operativos y administrativos integrados con la capacidad de satisfacer las necesidades de seguridad de nuestros clientes; manteniéndonos como una importante opción en el mercado por versatilidad, calidad y amplia cobertura. La guía de nuestra visión es formar sociedades comerciales, cimentadas en lema ganar – ganar.

Misión

Proveer servicios y sistemas de seguridad privada de alta calidad en la nación, satisfaciendo las necesidades y expectativas de nuestros clientes con soluciones integrales de avanzada tecnología”¹.

1.2 Historia de Viana misión y visión.

Viana

Viana se fundó en el año 1953, con una sola tienda, hoy denominada tienda matriz, ubicada en el eje Central Lázaro Cárdenas # 10, frente al salto del agua y ocupando la mitad de la planta baja del actual edificio.

La razón social de la empresa fue Viana, los productos que vendía eran estufas, refrigeradores y lavadoras, en su mayoría a crédito. Paulatinamente se fueron agregando productos como televisores, equipos modulares, planchas, licuadoras, y finalmente en el año de 1962 se incorporaron a la venta la línea de mueble para completar la gama de productos que hoy ofrecemos a nuestros clientes.

En ese mismo año de 1962, Viana implanta en México el sistema de ventas al contado con fuertes descuentos en artículos para el hogar.

Como existía una gran diferencia entre el precio Viana y el precio de la competencia, se creó de inmediato un mercado de clientes de contado así se triplicó instantáneamente su volumen de ventas. Gracias a ello, en 1964 se abrieron dos sucursales más: hidalgo e insurgentes.

¹ Almaba, Junio 15 2015. <<http://www.almaba.com.mx>>

Actualmente Viana cuenta con 35 tiendas en el D.F. y área metropolitana, con 15 tiendas en el interior de la república y con 1 gran centro de distribución.

Viana es una empresa 100 % mexicana que se esfuerza por seguir ofreciendo el precio más bajo del mercado y así beneficiar a más familias mexicanas.

Visión

“Aspiramos a ocupar el primer lugar en la preferencia de nuestros clientes, a partir de la calidad y variedad de los artículos que ofrecemos, así como de una entrega oportuna y los servicios adicionales que otorgamos a fin de alcanzar el 100% de su aceptación en estos rubros.

Misión

Vender artículos del hogar al precio más bajo garantizado, contando con el mejor surtido de marcas y prestigio. Dar un servicio al cliente enfocado como una experiencia de compra y con visión de cambio. Ser los mejores en el mercado de contado y en el de crédito.

Crear fuentes de trabajo. Proporcionar el desarrollo personal y profesional de los empleados. Generar beneficios para el cliente, los empleados y los accionistas. Operar con los costos más reducidos para sostener el precio bajo y generar beneficios”².

² Viana, Junio 15 2015. <<http://www.viana.com.mx>>

2 Descripción de actividades en Corporativo Almaba

En este capítulo se describirán las actividades que desempeñaba en Corporativo Almaba a esta empresa llegue en el año de 2009, la empresa presta servicios de rastreo satelital, seguridad privada a terceros, transporte, custodias locales y foráneas.

De las actividades que desempeñaba en el área de sistemas, son la configuración de equipo de cómputo, esta actividad consistía en la instalación de sistema operativo Windows XP, paquetería de office, open office, antivirus, explorador de internet Mozilla, configuración de correo electrónico en los siguientes clientes Outlook y Mozilla thunderbird.

En los equipos de las áreas de contabilidad y nomina se instalaban aplicaciones de Contpaq i, este paquete para el área contable les ayuda a automatizar el proceso de la información contable, financiera y fiscal de la empresa, así como la recepción de comprobantes fiscales digitales; existe otro modulo que es Contpaq i bancos este, ayuda a controlar los ingresos y egresos, para integrar la información de los comprobantes fiscales digitales, facilitando la administración de tus cuentas bancarias y el flujo de efectivo, por último otro moduló que ayuda al área contable, es adminpaq facilita la administración comercial, la integración de procesos de ventas, compras, inventarios, cuentas por cobrar, cuentas por pagar y facturación electrónica.

Para el área de nómina, existe Contpaq i nóminas es un sistema para la administración de la nómina que permite realizar, los pagos conforme a las obligaciones de ley, permite hacer un pago a tiempo a los empleados.

El mantenimiento preventivo y correctivo a los equipos de cómputo, consistía en lo que refiere al preventivo, destapar el equipo para sopletear con el fin de retirar todo el polvo acumulado en tarjeta madre, fuente de poder, ventilador del procesador, limpiar con alcohol isopropílico las superficies de DVD, gabinete, monitor, también revisión del software y depuración de archivos temporales y temporales de internet.

Lo que es el mantenimiento correctivo consiste en restauración del sistema operativo a un estado anterior, eliminar virus consistía en realizar un análisis del equipo con el antivirus en las diferentes unidades de disco que tuvieran, formatear equipo, reinstalación de sistema operativo, instalación de software para drivers de periféricos de la tarjeta madre, antivirus, paquetería de office, configuración de conexiones de red, internet y correos electrónicos.

Manejo de cuentas de servicios telefónico con Telmex, Telcel y Nextel, esta actividad consistía en llevar el control administrativo de las diferentes flotillas telefónicas, a quien se le asignaban los teléfonos, descargar desglosé total de tarificación por cada compañía y configuración de correo electrónico en BlackBerry.

La administración de servidores consistía en revisar que no estuvieran alarmados, actualizados los servidores, que el espacio en disco fuera suficiente en los servidores, que las herramientas instaladas se ejecutaran de manera correcta.

La creación y baja de correo electrónico, para los usuarios de nuevo ingreso, así como los que causaban baja de la empresa, el proceso se llevaba a cabo a través de la plataforma de sistema operativo Linux Fedora, la cual se realizaba a través del modo nativo del sistema operativo que es línea de comandos o por medio de un portal que era modo gráfico.

En cuanto a supervisar la instalación de GPS³; en los vehículos, consistía en llevar las unidades de transporte con el proveedor que instala el equipo, proporcionamos el equipo GPS y el SIM que lleva para el rastreo, una vez concluida la instalación, se pasa a la siguiente fase.

La administración del portal de rastreo satelital, consistía en dar de alta las unidades de transporte para que comenzaran a reportar en el portal de rastreo satelital, se proporcionaba el dato en el sistema del número de placa de la unidad, el número telefónico de la SIM telefónica, se realizaban pruebas de paro de motor, sonido local en la cabina, capacitación al personal de monitoreo de la empresa, el personal de monitoreo reportaba algunas incidencias en caso de que algún equipo GPS no reportara de manera correcta o en ocasiones el paro de motor lo solicitaban.

2.1 Participación en el proceso de instalación de rastreo satelital GPS

El rastreo satelital permite determinar la posición de un objeto, persona o un vehículo con precisión de centímetros, el sistema GPS está constituido por 24 satélites y utiliza una triangulación para determinar en todo el globo la posición del objeto, persona o vehículo, para determinar la posición del receptor que se utiliza, localiza automáticamente como mínimo tres satélites de la red, de estos recibe señales indicando la identificación y la hora del reloj de cada uno de ellos, basado en estas señales el aparato sincroniza el reloj del GPS y calcula el tiempo que tardan en llegar las señales al equipo.

³GPS: Sistema de posicionamiento global, es un sistema que permite determinar en todo el mundo la posición de un objeto, persona o vehículo.

De tal modo mide la distancia al satélite mediante triangulación, la triangulación consiste en determinar la distancia de cada satélite respecto al punto de medición, conocidas las distancias se determina la propia posición de cada uno de ellos por la señal que emiten, se obtiene la posición absoluta o coordenadas reales del punto de medición, se consigue con exactitud la posición exacta del receptor GPS, a continuación se muestra la siguiente Figura 2.1.1, es la gráfica de cómo funciona el rastreo satelital.



Figura 2.1.1 Principio de funcionamiento de rastreo satelital.

El rastreo satelital puede reducir tiempos de entrega analizando la velocidad con la que su carga avanza, el tiempo y lugar en la que se encuentra, bloqueos y retrasos. Además reduce costos, permite saber el combustible que utiliza el vehículo, información de cuanto acelera el conductor, se puede calcular el desgaste de partes y llevar un control sobre el kilometraje recorrido; facilitando la programación de mantenimientos para reducir costos.

Esto sin mencionar ventajas como la recuperación del vehículo y la carga en caso de robo. La participación en el proceso de instalación de GPS para rastreo satelital de vehículos, consistía en llevar los vehículos con el proveedor a la instalación del equipo GPS.

Administrar el portal de monitoreo con nivel de administrador, este nivel permitía, dar de alta las unidades en el sistema, los datos solicitados eran el número de placa del vehículo, el número telefónico de la SIM telefónica, para paros de motor antes de la salida del centro de resguardo de los vehículos, revisión de sonido local en la cabina.

Capacitación del portal de rastreo satelital al personal de monitoreo para indicar uso y funcionalidad de herramientas propias del portal que permiten un mejor uso del portal, como la ubicación del vehículo, velocidad, estado de los sensores conectados a los dispositivos móviles de las redes celulares GPRS⁴; almacenamiento de información generada por el vehículo, configuración de geocercas, control de pánico, grabación de sonido local en cabina, paro de motor, visualización cartográfica del vehículo en diferentes vistas satelitales, con información detallada del vehículo como nombres de calles, ciudad, estado, velocidad, dirección, eventos relevantes, etc., configuración de rutas y generación de reportes de cada vehículo.

2.2 Manejo administrativo de correo electrónico en Linux

“El núcleo de Linux se distribuye bajo la licencia pública general”⁵ GLP⁶, es un sistema operativo basado en Unix; está desarrollado por colaboradores de todo el mundo, es software libre y de código abierto.

⁴GPRSM: General Packet Radio Service o servicio general de paquetes vía radio creado para la transmisión de datos mediante conmutación de paquetes.

⁵ Abraham Silberschatz, Sistemas Operativos, México, Addison Wesley, 1999, p. 701.

Linux se utiliza junto a un empaquetado de software, llamado distribución GNU/Linux, todo su código fuente puede ser utilizado, modificado y redistribuido libremente, el nombre de GNU, GNU's not Unix que significa GNU no es Unix, viene de las herramientas básicas de sistema operativo creadas por el proyecto GNU, iniciado por Richard Stallman en 1983 y mantenido por la FSF⁷; el nombre de Linux viene del núcleo Linux, inicialmente escrito por Linus Torvalds en 1991.

GNU/Linux puede funcionar de dos maneras modo consola que es por medio de línea de comandos, este tipo de distribución está orientada para la administración de servidores.

Otro modo es el entorno gráfico está orientado para un usuario final para pc's o laptops de escritorio este entorno se compone de ventanas, iconos y muchas aplicaciones que facilitan el uso del sistema operativo.

Existen diferentes tipos de distribuciones entre las más utilizadas son las siguientes Debian, Arch Linux, Fedora, Gentoo Linux, OpenSUSE, Ubuntu, Mandriva, Slackware, Knoppix, CentOS, Ubuntu, Linux Mint, Puppy Linux, Magela, PCLinuxOS, Red Hat Enterprise Linux, Slax, Dragora, Canaima, Tuquito, Trisquel y Android.

Los componentes típicos de una distribución GNU/Linux contienen un núcleo, herramientas y bibliotecas, software adicional, documentación, un sistema de ventanas, un administrador de ventanas y un entorno de escritorio, la mayoría de software es de fuente abierta o software libre.

⁶GPL: General Public License (Licencia Pública General de GNU).

⁷FSF: Free Software Foundation es una organización no lucrativa con la misión de defender los derechos de todos los usuarios de software libre.

Esto significa que el código fuente permite a los usuarios modificar o compilar el código original, cabe mencionar que algunas distribuciones incorporan software privativo.

La gestión de los paquetes en las distribuciones contiene una aplicación o servicio, estos son distribuidos en una versión compilada, la instalación y desinstalación de los paquetes es controlada por un sistema de gestión de paquetes, cada paquete contiene metainformación como la fecha de creación, descripción del paquete y sus dependencias, dicho sistema realiza un análisis de información que permite la búsqueda de paquetes, actualización de librerías y aplicaciones instaladas. Algunos sistemas de paquetes más usados son rpm, hat, deb, tgz, ebuilds, pacman y PET.

El correo es soportado en una distribución de Linux llamada GNU/Linux Debian, el servicio de correo electrónico permite llevar a cabo el envío y recepción de mensajes con usuarios de la red, “su función es mantenerse a la escucha del puerto 25, comunicándose con los daemons de otros sistemas para recibir el correo entrante y enviar el correo saliente. En cuanto a la aplicación TCP/IP⁸; se utiliza el protocolo SMTP (simple mail transfer protocol)”⁹, “protocolo para transferencia simple de correo” es un protocolo usado para el intercambio de mensajes solo enviando los mensajes y la recepción la realiza por medio de otros protocolos como POP o IMAP¹⁰.

La gestión de todo lo concerniente a la red por parte de IP y TCP deja a los programas de aplicación como un simple intercambio de comandos y datos.

⁸TCP/IP: Es un conjunto de protocolos de red específicos, que permiten que un equipo pueda comunicarse en una red.

⁹Cybercursos, Mayo 4 2015 <http://www.redes-linux.com/manuales/Servidor_correo/sendmail.pdf>

¹⁰IMAP: Internet Message Access Protocol (protocolo de acceso a mensajes de internet), permite el acceso a mensajes almacenados en un servidor de internet.

El programa de mail abre una conexión contra el mail server remoto, entonces, envía su nombre de máquina local, así como el nombre del emisor, el buzón de destino y un comando diciendo que empieza el texto del mensaje.

En este punto, el servidor finaliza el tratamiento de lo que ha asumido como comandos y comienza a aceptar el mensaje hasta que recibe una marca especial, después de esto, ambos programas entienden que el envío de comandos ha sido retomado.

El protocolo POP (post office protocol) " protocolo de oficina de correo" es el encargado de enviar y recoger los mensajes entre el servidor y nuestro equipo de trabajo. El cliente host es la máquina host que utiliza el servicio POP3, mientras que el término servidor host se refiere al host que ofrece el servicio POP3. Cuando un usuario agente o un cliente host introducen un mensaje en el sistema de transporte este establece una conexión SMTP al host relativo.

"Inicialmente, el servidor host comienza el servicio POP3 a través del puerto TCP 110, cuando un cliente host llama a un usuario el servicio establece una conexión TCP con el servidor host. Cuando la conexión es establecida, el servidor de POP3 envía una contestación de aceptación. El cliente y el servidor POP3 intercambian comandos y respuestas hasta que la conexión sea cerrada o abortada"¹¹.

La administración del correo consistía en la creación y bajas de correos solicitados por cada área dependiendo la necesidad, esto era realizado por medio de líneas de comando, se tenía una aplicación que permitía la consulta del correo por medio de una link de internet, se verificaban los espacios de disco duro en este servidor para evitar saturación del disco, se realizaban respaldos de correo.

¹¹Cybercursos, Mayo 4 2015 <http://www.redes-linux.com/manuales/Servidor_correo/sendmail.pdf>

3 Descripción de actividades en Viana área de Soporte Técnico

La segunda empresa donde prestó mis servicios actualmente es Viana llegué en el año de 2010, es una empresa dedicada a la venta de muebles, colchones, línea blanca, hogar, electrónica, perfumería, calzado, ropa, celulares, juguetería, y recargas de tiempo aire.

Mi participación dentro del departamento de sistemas fue primero en el área de soporte técnico, una de las primeras actividades que me tocó realizar fue armar equipo de cómputo ya que estos no venían armados o se recuperaban piezas del equipo que ya no servía para posteriormente ser usadas como repuestos en caso de requerirse, instalación de software y hardware, como antes mencione si se requería reparar un equipo por falla de alguna pieza se utilizaban piezas recuperadas de otros equipos, en cuanto a la instalación del hardware se instala la paquetería de office, antivirus, programas más específicos como winrar, adobe flash, photoshop o el sistema operativo.

En cuanto al mantenimiento preventivo y correctivo al equipo de cómputo, se lleva a cabo por medio de un programa de calendarización esto es aplicable solo al mantenimiento preventivo, el mantenimiento correctivo no es una actividad que te permita programar una fecha específica para realizarlo este se da cuando el equipo presenta alguna falla mayor.

La configuración de correo electrónico es una actividad que se realiza antes de entregar el equipo de cómputo, esto puede ser por que el usuario al que será asignado el equipo es de nuevo ingreso el área de redes debe confirmar la creación del correo para que se pueda configurar en el equipo.

Otra actividad es la instalación de impresoras que se realiza cuando el jefe inmediato del usuario requiere que este pueda imprimir, se conecta el multifuncional al usuario del área al que este corresponda, configuración de terminales tontas para tiendas y configuración de multifuncionales, esta actividad se realiza antes de que el multifuncional se coloque en tienda o en el corporativo dependiendo cuál sea su destino se le configurara con los parámetros requeridos para cada área.

3.1 Mantenimiento preventivo y correctivo de PC y Laptop

El mantenimiento es una actividad que está relacionada con la prevención de fallas, evitar incidentes, conservar los bienes productivos en condiciones seguras y operables, un estado en el cual pueda llevar a cabo alguna función requerida; en computación existen principalmente dos tipos de mantenimiento que son el preventivo y el correctivo.

El mantenimiento preventivo, como su nombre lo dice es el que se realiza, con la finalidad de prevenir alguna falla, en los equipos de cómputo pc o laptop ayuda a prevenir futuras fallas, que evita hacer cambios acelerados de pc's o laptop, esto puede evitar pérdida de información o tiempo de espera por parte de un usuario que se ve afectado en sus actividades laborales, por no contar con toda su información.

Actualmente existe software que permite conocer el estado del equipo de cómputo, como condiciones operativas y de durabilidad, aun con esto “existen fallas humanas, averías, mal uso, etc.”¹², este tipo de mantenimiento permitirá alargar la vida útil de un equipo y prevenir suspensión de actividades laborales imprevistas.

¹² Wikipedia, Mayo 5 2015 < http://es.wikipedia.org/wiki/Mantenimiento_preventivo>

Un mantenimiento que se planifica mejora la vida de un equipo, aumenta su productividad, reduce gastos, alarga la vida útil de un equipo y evita tiempos muertos; este se realiza a un equipo que se encuentra en funcionamiento, pero se realiza para prevenir alguna falla, este garantiza un periodo de uso tiene factible.

El mantenimiento correctivo es aquel que se realiza con el fin de corregir defectos en los equipos de cómputo, este tipo de mantenimiento consiste en corregir defectos después de que se presenta una falla o avería en el equipo, por no estar planificada en tiempo representara costos por reparación y costos en tiempo por la suspensión de actividades laborales, de la persona que lo utiliza de igual manera de las personas que dependen del trabajo generado en este equipo.

Se pueden presentar fallas de hardware o software. Las fallas en hardware consisten en la avería de alguna pieza que será necesario cambiar, como lo puede ser un disco duro, fuente de poder, memorias o tarjeta madre estas son las principales, estas piezas deben conseguirse para su remplazo, en caso de no tenerse se recurrirá al cambio de equipo. Una falla de software consiste en la falla de algún programa desde el más básico hasta el más complejo como podría ser el sistema operativo, la reparación o reinstalación de alguno de ellos, llevara tiempo se deben tomar medidas, para evitar perdida de información.

Para realizar el mantenimiento preventivo se programaba un calendario donde se incluían fechas para realizarlo en las tiendas o en el corporativo, dicho mantenimiento consistía en realizar limpieza interna, externa de equipos de cómputo, sopletearlos, borrado de archivos temporales, actualización de parches de Windows, en el caso de las terminales de tienda se les actualiza la imagen del sistema operativo.

En el mantenimiento correctivo no se tenía una fecha definida este se realiza si un equipo presenta una falla grave como la falla de alguna pieza importante para el funcionamiento del equipo o hasta una falla en el arranque del sistema operativo, a continuación se muestra la figura 3.1.1 de lo descrito anteriormente.



Figura 3.1.1 Mantenimiento preventivo

3.2 Instalación de software en equipos PC y Laptop

El software es un conjunto intangible de instrucciones que se le proporciona al microprocesador para que pueda procesar datos y generar los resultados esperados. Existen diferentes tipos de software como el de sistema, programación y aplicación.

El de sistema es aquel que se encarga de proporcionar las interfaces adecuadas que permiten el funcionamiento del sistema operativo, controladores de dispositivos, herramientas de diagnóstico, sistema de ventanas, utilidades y más, el sistema operativo es un conjunto de programas que administra los recursos de la computadora y controla su funcionamiento, los controladores de dispositivos son programas que permiten a otros programas de mayor nivel, interactuar con un dispositivo de hardware, son programas añadidos al núcleo del sistema operativo, concebidos inicialmente para gestionar periféricos y dispositivos especiales, los programas utilitarios resuelven problemas específicos y tareas de mantenimiento, algunos se incluyen en el sistema operativo.

“El software de aplicación permite al usuario llevar a cabo tareas específicas y susceptibles a ser automáticas o asistidas, este tipo de software son los programas diseñados para o por los usuarios para facilitar la realización de tareas específicas en la computadora, como pueden ser las aplicaciones ofimáticas (procesador de texto, hoja de cálculo, programa de presentación, sistema de gestión de base de datos...), u otros tipos de software especializados como software médico, software educativo, editores de música, programas de contabilidad”¹³.

El software de programación es aquel que permite a un programador desarrollar programas haciendo uso de lenguajes de programación; provee herramientas de asistencia al programador, incluye editores de texto, compiladores, interprete de instrucciones y ensambladores, a continuación se muestra la figura 3.2.1



Figura 3.2.1 Tipos de software

¹³ Ruben Alberto Martinez, (2014),Nociones introductorias sobre software, de <http://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAAahUK EwjWnovcslnGAhVEGKwKHa8jAHI&url=http%3A%2F%2Ftifloinformatica.jimdo.com%2Fapp%2Fdownload%2F6742969770%2F5.-_Apunte_sobre_software_actualizado.doc%3Ft%3D1363746774&ei=Zmh6VdbTEcSwsAWvx4CQBw&usg=AFQjCNFuGMkliRys4gsCwXXNcgpdp56es7w&bvm=bv.95515949,d.b2w>>

El primer software que se instala en un equipo de cómputo ya sea pc o laptop, es el sistema operativo, este puede ser Windows o alguna versión de Linux, esto dependerá del perfil de uso de este equipo, para Windows se instala alguna de las siguientes versiones, Windows 7 o Windows 8, posteriormente se le instalara una paquetería básica que consiste en la instalación del antivirus, los controladores de sonido, video, red, Office 2010 y actualizaciones de Windows, debe tomarse en cuenta que el software debe ser compatible para no causar fallas posteriores, el antivirus es muy importante ya que ayudara a bloquear, desinfectar, prevenir y proteger el equipo de códigos maliciosos o software malintencionado que puede provocar fallas graves, los controladores o drivers de video, red, sonido, etc., ayudan a que el equipo se desempeñe mejor, con el controlador exacto, permite apreciar mejor las imágenes, sonidos y tener una estabilidad en la tarjeta de red; la paquetería de office contiene diferentes aplicaciones como Word (procesador de texto), Excel (plantilla de cálculo), PowerPoint (creación y despliegue de presentaciones), Outlook (cliente de correo), estas aplicaciones son las más utilizadas de la paquetería de Office.

Se hace la instalación de otros programas como Adobe Reader (permite visualizar archivos pdf), flash player (visualizador de videos de páginas de internet), java, herramientas de conectividad SQL, winrar (descomprimir archivos), todas las anteriores en sus versiones más recientes.

3.3 Configuración de terminales tontas para tiendas

Una terminal tonta es hardware especializado que permite hacer conexiones remotas o un servidor, que depende primeramente del servidor central para las tareas de procesamiento y se enfoca principalmente en transportar la entrada y salida entre el usuario y el servidor remoto, esta no tiene capacidad de procesamiento ni capacidad de almacenamiento, no puede funcionar como un dispositivo separado o solo, las ventajas de tener terminales tontas son que la información está centralizada, solo se guarda la información que es de la empresa, facilitando realizar los backups de la información, se reduce el riesgo de robo físico de información, si el dispositivo presenta fallas la información no se perderá puesto que esta reside en el servidor, la terminal puede ser usada en ambientes polvorientos sin la preocupación de que esta se sobrecaliente.

La terminal tonta es llamada así por qué solo pueden desplegar, enviar y recibir texto, no pueden ejecutar programas en ellas, la computadora o servidor al cual se conectan es el que tiene todos los recursos para correr procesadores de texto, compiladores, correo electrónico, juegos, etc.

Las terminales tontas son enfocadas para usuarios que no necesitan acceso a aplicaciones gráficas, por qué dichas terminales no cuentan con recursos suficientes para ejecutar interfaces gráficas, algunas terminales más recientes pueden desplegar gráficos ya que contienen versiones de Windows para terminal server que son clientes ligeros.

Existen diferentes modelos de terminales las que utilizamos específicamente son los siguientes V30L, 3150SE, V90LE, WT3125, Z90SW, marca WYSE.

La manera de configurar las terminales es la siguiente:

- 1.- Crear una conexión remota a un servidor, donde vive la sesión del usuario
- 2.- Llenar los parámetros de la sesión como nombre del usuario, password y dominio.
- 3.- Poner la ruta de donde se ejecutara la aplicación de venta, la ruta es la siguiente D:\Intelisis o D:\IntelisisR2 si la tienda es foránea.
- 4.- Configurar el puerto serial para la pin pad el parámetro de rate = 19200, date= 7, party = even, stop bits= 1
- 5.- Configurar el teclado, en spanish, activar el num lock y el display a una resolución de 800 x 600
- 6.- Configurar Networks, llenar campo de IP, mascara y Gateway.
- 7.- Configurar impresora, se debe de entrar a la opción system y en la configuración seleccionar puerto LPT1 como predeterminado.
- 8.- Como último paso se debe definir el password de administrador de la terminal.

A continuación se muestra un la figura 3.3.1 del diagrama de conexión de las terminales.



Figura 3.3.1 Diagrama de conexión terminales tontas

4 Descripción de actividades en Viana área Redes

En el área de redes se realizan actividades como administrar servidores, creación de usuarios con Active Directory, creación de políticas con active directory, creación de cuentas de correo electrónico con Exchange y Linux, asignación de IP y segmentos nuevos para tienda, administración de consola de Antivirus, administración de consola de respaldo Backup exec, administración de proxy para restricciones de Internet, monitoreo de enlaces dedicados con MPLS, asignación de dial peer para marcación a tiendas, manejo de base de datos con SQL, licenciamientos de Microsoft, creación de sitios con IIS.

4.1 Descripción general de puesto y actividades en área de redes

El puesto que desempeño en el área, es de administradora de redes llevo a cabo diferentes actividades en primer lugar administrar servidores, esto implica revisar cual es la mejor opción para la compra de dicho servidor revisando para que se requerirá, esto ayudara a determinar las capacidades que debe tener el server, como capacidad de memoria, discos duros que debe tener para realizar arreglos, procesador, revisión de número de fuentes, contratación de extensión de garantía de piezas; cuando ya se tiene el servidor se debe armar, realizar la configuración de arreglo de discos RAID¹⁴.

¹⁴RAID: Redundant array of indepent disk, conjunto redundante de discos independientes, entre los que se distribuyen o replican los datos.

Se puede escoger alguno como un RAID0, RAID1 o RAID5 dependiendo la cantidad de discos que lleve, se podrá configurar el arreglo pero mínimo deben ser 2, posteriormente cargar el sistema operativo debe ser Windows Server 2003, Windows Server 2008, Windows Server 2012 o alguna versión de Linux que puede ser Fedora, esto dependerá para que será utilizado el servidor, después se le instalara el software específico dependiendo para que sea utilizado el servidor; ya instalado todo lo necesario para su funcionamiento, se lleva al site donde se encuentran todos los servidores, se le asigna una IP de este segmento y los fines de semana son monitoreados todos los servidores verificando el espacio en disco, memoria utilizada por el procesador, arreglos de discos, log del sistema, log de aplicación y actualización de antivirus.

La siguiente actividad es la administración, manejo de la consola de respaldos de bases de datos e información importante, dicha consola se maneja con un software específico que es Backup Exec 2012, esta herramienta permite, el respaldo y restauración de bases de datos o información importante, esto se realiza creando las tareas para respaldo o restauración.

El respaldo se puede definir para que se realicen a una hora determinada de manera automática, la restauración se puede ejecutar en ese momento, en que se abre la tarea, se tiene que configurar el almacenamiento de los respaldos, estos se pueden almacenar en una unidad de disco o en un cartucho.

La administración de la consola de antivirus es otra actividad, en esta se dan de alta todos los equipos de cómputo que se les instala el antivirus, se instala un agente que es el que se encargara de hacer la comunicación entre el equipo y la consola, cuando reportan a la consola permite saber si tiene la última actualización de antivirus o desde cuando no está reportando a la consola, en la consola se tienen configuradas tareas para que proporcione un informe sobre los equipos actualizados, si alguno está contaminado e impedir ingreso de memorias USB no autorizadas.

Manejo de proxy, esta actividad es utilizada para configuración de políticas de internet, que bloquean contenidos de páginas de acuerdo con la política en la que se encuentre el usuario, se puede revisar el tráfico de la red, se puede realizar bloqueo de puertos, el proxy está en un sistema operativo Linux.

Administración de Active Directory es otra actividad, en él se crean o dan de baja los usuarios o equipos del dominio, se crean políticas de control que se aplican a los equipos del dominio, se explicaran en otro capítulo.

La creación de los buzones de correo electrónico es otra actividad, los buzones son creados con una herramienta de Microsoft llamada Exchange versión 2010, dicha herramienta permite crear el buzón de un usuario, también permite dar de baja los buzones, habilitar al usuario para que se pueda conectar por medio de un portal electrónico, redireccionamiento de correo, entre otras cosas que serán posteriormente mencionadas.

4.2 Administración de herramientas de respaldos y antivirus

El tema de respaldo y recuperación de información, trata del esfuerzo necesario para asegurar la continuidad del procesamiento de los datos, con la mínima dificultad posible ante una eventual alteración no deseada.

Un respaldo es la obtención de los datos en algún medio de almacenamiento unidad de cinta magnética o disco duro; de tal modo que a partir de dicha copia es posible restaurar el sistema al momento de haber realizado el respaldo.

Los respaldos deben hacerse con regularidad, con la frecuencia preestablecida y de la manera indicada, los respaldos son útiles ante distintos eventos, para recuperar información en caso de alguna catástrofe natural o ataque, los respaldos son guardados en ubicaciones distintas de la de los datos originales.

La recuperación es la tarea que se lleva a cabo cuando es necesario volver al estado de la aplicación al momento del último respaldo, esto debido a que se elimino información de manera accidental, se corrompió, se infecto por un virus u otras causas, se recupera a partir de la última copia realizada, esta tarea permite hacer la restauración de archivos para laboratorios y para revisar que la restauración se realiza de manera correcta.

Las políticas de respaldo son diferentes en cada empresa dependiendo la prioridad de su información, pero de manera general se debe contemplar lo siguiente, tener un plan de respaldo, que datos se van a respaldar, la periodicidad de estos respaldos, definir horarios en que se realizaran los respaldos, en donde se almacenara el respaldo ya sea en unidad de disco o en cintas magnéticas, entre otros medios, con que periodicidad se sobrescribirá el respaldo o serán conservados los respaldos por cuestiones fiscales, en algunos casos se pueden realizar, por los tipos de archivos que se respaldan.

Es importante saber que datos deben ser incluidos esto dependerá de la criticidad de los datos y el valor de los mismos, los medios de soporte a utilizar más comunes son discos duros, cintas magnéticas, cartuchos, CD-ROM y USB.

Es posible hacer diferentes tipos de respaldos, que se pueden complementar entre sí empezaremos explicando que es un respaldo completo, se realiza un respaldo de toda la base o información deseada que se mantiene en línea, otro tipo de respaldo es el incremental este tipo de respaldo consiste en solo respaldar la información que cambio desde el último respaldo completo, para realizar una recuperación se debe adicionar al último, respaldo completo, todos los respaldos incrementales sucesivos, este procedimiento es ágil y ocupa menos espacio, otro tipo de respaldo es el diferencial es similar al incremental, en este se respalda las modificaciones que han ocurrido desde el último respaldo completo, para realizar una restauración se debe adicionar el último respaldo completo y el último respaldo diferencial.

Un punto importante es cuando se debe realizar el respaldo, para determinar cuándo se deben realizar se debe conocer los tiempos que se llevara la tarea y las ventanas de tiempo disponibles o si se pueden realizar en tiempo real, los tiempos pueden ser variables porque depende también del soporte utilizado y la cantidad de datos a respaldar.

Otro factor a tomar en cuenta, es cuanto espacio se tiene disponible para almacenar los respaldos, tener establecido que respaldos deben ser guardados en cinta, en qué lugar físico se deben guardar los respaldos, debe ser bajo llave, considerando el medioambiente (temperatura, humedad, polvo, etc.), se debe tomar en cuenta por cuánto tiempo se guardaran los respaldos, tomando en cuenta situaciones legales, los respaldos pueden sobrescribirse cada cierto tiempo.

Los respaldos o copias de seguridad deben realizarse de forma automática, de acuerdo al criterio definido en el plan de respaldos, esto se logra con un programa que cada empresa define dependiendo costos y alcances de dicho programa, aquí se utiliza el programa de Backup Exec 2012. Enseguida explicaré un poco del funcionamiento de la herramienta de respaldos Backup exec 2012.

Como mencione antes es una consola de Backup Exec 2012 que se encuentra instalada en un servidor HP Proliant ML110 G7 con sistema operativo Windows server 2008 R2, Standard Edition con service pack 1.

Los dispositivos con los que este servidor cuenta para realizar los respaldos son: 2 unidades de disco externo USB, marca western digital modeló WD my book 1140 de 3 TB cada una y una unidad de cinta HP modelo storageworks ultrium 920 SAS, a continuación presento la figura 4.2.1 de la conexión del servidor de respaldos.

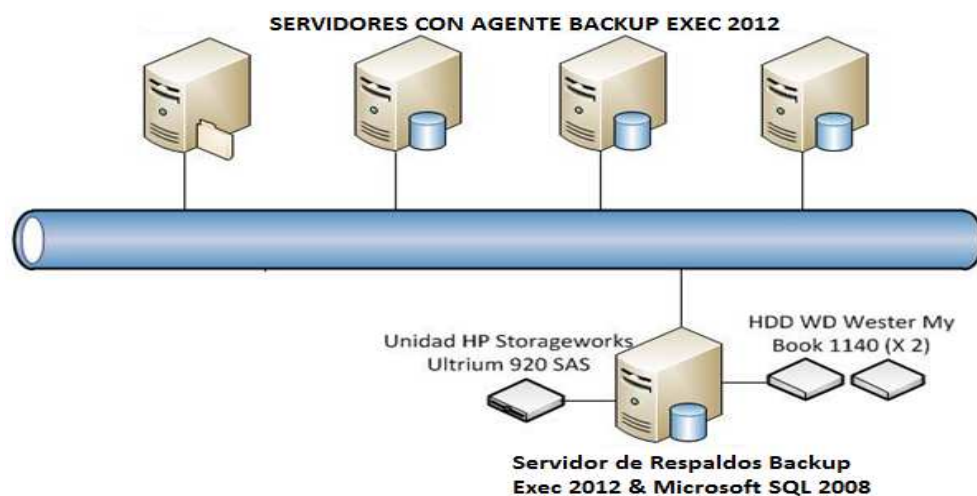


Figura 4.2.1 Conexión de servidor de respaldos

En esta consola lo que se realizan son respaldos de bases de datos o de información, de estos respaldos se realizan restauraciones de bases de datos que son utilizadas como laboratorio, para poder realizar lo antes mencionado se debe instalar un agente de la consola de Backup Exec 2012 en el servidor al que se le realizara respaldo o restauración.

Una vez instalado el agente, el servidor se verá en la consola de Backup Exec 2012, entonces podremos realizar el procedimiento de respaldo o restauración de información.

Se puede respaldar o restaurar bases de datos o información por medio de tareas programadas, a continuación muestro la figura 4.2.2 del panel de control de la consola de Backup Exec 2012.

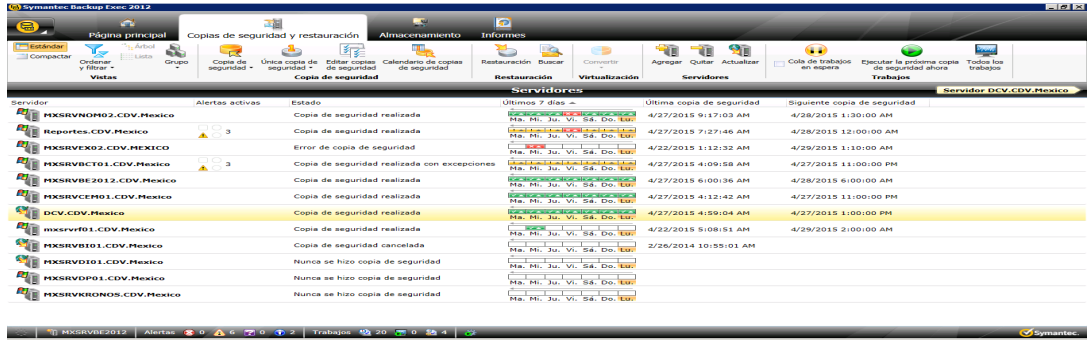


Figura 4.2.2 Panel de control de consola Backup Exec 2012

Para que estas tareas programadas se ejecuten, es necesario indicarle al programa la unidad de almacenamiento a utilizar (unidad en la cual se almacenaran los archivos de respaldo) ya por defecto, la consola tiene programados algunos dispositivos en los cuales se especifica el tiempo de duración que tendrá cada respaldo, este puede variar de acuerdo con el espacio de almacenamiento de las unidades de disco, a continuación presento la figura 4.2.3 de los almacenamientos de la consola.

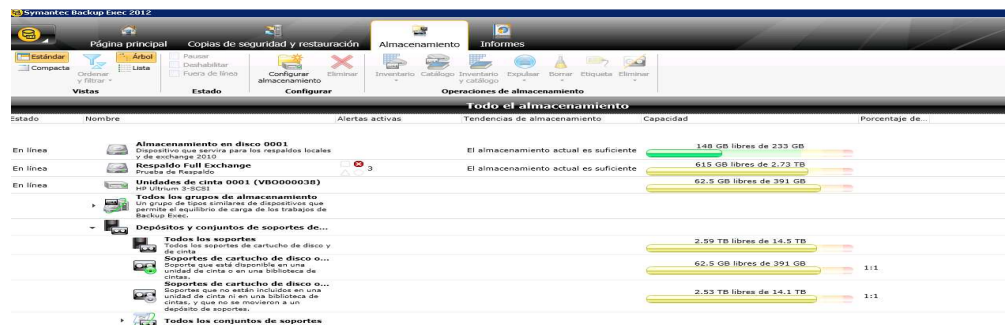


Figura 4.2.3 Panel de almacenamiento de consola Backup Exec 2012

Al abrir la consola muestra en el panel la opción de “copia de seguridad y restauración”, en ella se muestran los servidores que tienen instalado el agente, colocarnos en este servidor, se puede observar si ya este tiene alguna tarea creada de restauración o respaldo, para crear la tarea de respaldo se debe seleccionar la opción de “copia de seguridad”, escoger una de las opciones que puede ser “copia de seguridad en disco”, “hacer copia de seguridad en disco y luego duplicar en cinta”, “ hacer copia de seguridad en cinta” , en nuestro caso seleccionaremos a “copia de seguridad en disco”, se abrirá una ventana donde se tiene que dar nombre a la tarea, luego escoger que se va a respaldar base de datos o archivos, se debe escoger si se va a hacer un respaldo completo o incremental, dar clic en “editar” aparece otra ventana donde debemos llenar varios parámetros el primero será escoger en que horario se ejecutara la tarea puede ser por horas, diario, semanal, mensual o por año, como siguiente paso muestra la opción de almacenamiento, tendremos que escoger en que unidad de disco se guardara el respaldo, como paso final escoger a que personas les serán enviados los correos electrónicos cuando la tarea termine de manera satisfactoria o insatisfactoriamente.

Para crear una tarea de restauración se debe entrar a panel la opción de “copia de seguridad y restauración” colocarnos en este servidor donde crearemos la tarea, seleccionar la opción de “restauración”, aparece una ventana donde pregunta qué tipo de archivo es el que se desea restaurar “archivo, carpeta o volúmenes” o “bases de datos de Microsoft SQL”, seleccionar “bases de datos de Microsoft SQL”, dar clic en siguiente, aparece otra ventana donde tendremos que seleccionar “la base de datos que queremos restaurar”, en la siguiente ventana tendremos que seleccionar “A la hora del conjunto de copias de seguridad seleccionado”, dar clic siguiente en esta ventana que aparece se debe seleccionar la hora del respaldo con el que queremos restaurar, dar clic siguiente.

Después se escoge desde donde se desea restaurar la base, esta opción puede aparecer o no dependiendo la hora seleccionada, algunos respaldos son guardados en disco, en cinta o en ambos en el mismo respaldo, seleccionar el deseado, la opción que se ejecuta más rápido es la de disco, dar clic en siguiente, aparecerá otra ventana con opciones de donde se desea restaurar la base de datos, seleccionar la opción “redireccionar los datos a un nombre de base de datos o sesión de SQL Server diferente”, se piden datos como el nombre de la “Instancia o servidor SQL”, 2 tipos de cuentas en la primera “cuenta de inicio de sesión de servidor”, se deja la opción predeterminada, la segunda “cuenta de inicio de sesión SQL”, en esta opción se escoge la cuenta que pertenece al servidor que se enviara la restauración, esta cuenta contiene los datos del usuario (sa) y password.

A continuación dar clic en siguiente, llevó a otra ventana donde se pregunta de qué manera desea redireccionar las bases de SQL Server, se deben llenar los datos como el “nombre de la base de datos”; seleccionar la unidad o directorio donde se guardara en el servidor usar la opción de “usar esta ruta” examinar la lista de servidores y escoger el correcto así como la ubicación, dar clic en siguiente pasaremos a otra ventana donde se nos pide escoger que tipo de comprobación de la coherencia se desea ejecutar seleccionar “no ejecutar una comprobación de coherencia después de la restauración”, clic en siguiente, aparece otra ventana que pregunta que tareas adicionales deseó realizar o después de la restauración, debemos ir a la parte de notificación y seleccionar el o los destinatarios que les llegara un correo donde se especifica si la tarea concluyó satisfactoriamente o no, dar clic en siguiente para ir a la otra ventana, donde pregunta que programación y nombre de trabajo desea usar, en esta opción se debe escribir el “nombre” que se le dará a la tarea, en la parte de “programar” seleccionar “ejecutar ahora” para que la tarea se lleve a cabo, dar clic en siguiente, aparecerá la última ventana donde se describe todas las opciones de la tarea y dar clic en finalizar para que comience a ejecutar la tarea.

Ahora explicaré como se hace una restauración de archivos entrar a panel la opción de “copia de seguridad y restauración” colocarnos en este servidor donde crearemos la tarea, seleccionar la opción de “restauración”, aparece una ventana donde pregunta qué tipo de archivo es el que se desea restaurar “archivo, carpeta o volúmenes” o “bases de datos de Microsoft SQL”, seleccionar “archivo, carpeta o volúmenes”, dar clic en siguiente

Aparece otra ventana donde se pregunta que desea restaurar “copia de seguridad de archivos y carpetas” o “archivos y carpetas ubicados mediante la función de búsqueda”, seleccionar “copia de seguridad de archivos y carpetas”, dar clic en siguiente, aparecerá otra ventana donde se muestra las unidades con las que cuenta el servidor, se debe seleccionar la unidad donde se encuentran los archivos a restaurar, seleccionar el archivo a restaurar, dar clic en siguiente.

La ventana que se muestra es donde se desea restaurar los datos se debe seleccionar “en una ubicación diferente” en esta opción se debe escribir los siguientes datos donde se pide la unidad: \\servidor\unidad, en el otro renglón pide el directorio: \\ruta ->examinar, después aparece otra opción para llenar que es la cuenta de inicio de sesión del servidor, se debe dejar la opción predeterminada, dar clic en siguiente para pasar a otra ventana, donde se pregunta de qué manera se desea mantener la integridad del archivo, jerarquía y seguridad para los datos restaurados, seleccionar en la opción de “restaurar archivos existentes” se debe escoger la opción de “sobrescribir el archivo solo si es más antiguo”.

En la opción de “restaurar información de seguridad y permisos de sistema de archivos”, se debe escoger la opción “restaure los archivos sin su información de seguridad ni sus permisos del sistema.....”, dar clic en siguiente, aparecerá otra ventana.

En esta ventana se pregunta de qué manera desea que se restauren las funciones del sistema operativo en esta solo se debe seleccionar “conservar puntos de unión, puntos de montaje y vínculos simbólicos existentes, restaurar archivos y directorios”, dar clic en siguiente; en esta ventana se pregunta qué tareas adicionales desea realizar antes o después de la restauración, en la parte de “notificación” se debe escoger a que usuarios se les mandara correo de notificación de cuando se complete el trabajo, dar clic en siguiente, en esta ventana pregunta sobre que programación, almacenamiento y nombre de trabajo se desea usar, primer campo se llena “nombre” que se le dará a la tarea, en la opción “programar” se debe seleccionar “ejecutar ahora” , dar clic en siguiente, en esta ventana, se describe la tarea, dar clic en finalizar y la tarea se ejecutara.

Por último, se debe llevar un registro de los respaldos que se realizan, así como también los eventuales, este registro es una historia de los respaldos llevados a cabo.

La Administración de la consola de Antivirus

Una consola de administración de antivirus centralizado sirve para la implementación de políticas, la gestión de alertas de seguridad y la presentación de reportes automáticos. La consola está instalada en un servidor con sistema operativo Windows Server 2003, con SQL 2005, el icono de acceso se encuentra en el escritorio y se identifica con el siguiente nombre “launch McAfee ePolicy Orchestrator 4.6.6 console”, otra forma de localizarlo en el escritorio es porque está en forma de escudo de color rojo

Para abrirla solo bastara con dar doble clic sobre el icono, se podrá tener acceso colocando la siguiente dirección en el explorador de internet <https://antiviana:8443/core/orionSplashScreen.do>, pedirá un usuario, contraseña, e idioma en el que se quiere ver la consola, dar clic en aceptar, abrirá una ventana de un navegador de internet, enseguida se muestra la figura 4.2.4 del panel de la consola.

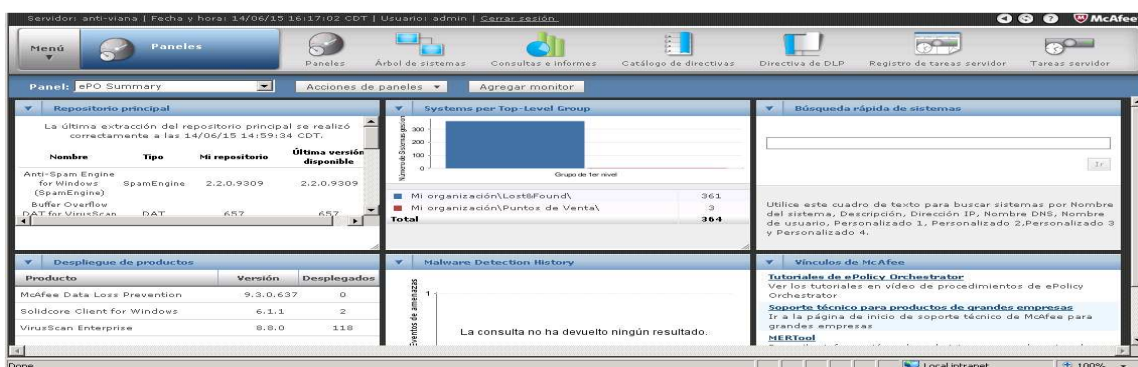


Figura 4.2.4 Panel de la consola de antivirus

En la consola encontraremos en la parte superior los diferentes menús, el primero es “paneles” en se encuentran gráficas de los reportes de la actualización de los equipos, versión de repositorio y detección de equipos contaminados, el siguiente es árbol de sistemas, en este menú se encuentra como su mismo nombre lo indica, el árbol de equipos que se reportan a la consola, las directivas asignadas a los equipos, detalles de los grupos, otra pestaña del menú es el catálogo de directivas en esta se muestra todas las políticas que se aplican a los equipos, en esta se puede editar, eliminar, exportar, duplicar, compartir y crear nuevas políticas.

La siguiente pestaña del menú es la de “directivas DLP¹⁵” aquí se define las reglas de dispositivos de restricción de USB que serán aplicadas a los equipos, se pueden definir por áreas o departamentos, estas reglas permiten que no se puedan leer dispositivos USB diferentes a los dados de alta en las reglas definidas, de manera que no se pueda extraer información de una pc, laptop o servidor, la siguiente pestaña es “registro de tareas servidor” aquí se observara el nombre de la tarea, la fecha de inicio, fecha de finalización, nombre de usuario, estado, origen y duración, con la información de estos campos sabremos si las tareas se ejecutan de manera correcta o si alguna falló; en la última pestaña se encuentra la opción de “tareas Servidor” donde se muestra el nombre, el estado, tipo, planificación, próxima ejecución, ultima ejecución, acciones como ver, editar y ejecutar, en esta pestaña se encuentran las tareas como la actualización de la firma de antivirus, replicación de repositorios y reportes que se envían a correos, existe otra pestaña que se llama menú, donde se presentan las siguientes opciones, “informes”, “sistemas”, “directiva”, “software”, “automatización”, “protección de datos”, “admin de usuarios”, “configuración”, “application control”.

A continuación, explicaré algunas de las tareas dentro de la consola del Epo de McAfee en la parte del menú → automatización → tareas servidor, en esta parte encontraremos tareas programadas que se utilizan como complemento de algunas acciones que se requieren para depurar y realizar consultas con el fin de obtener reportes, alertas de actualización de los repositorios, principal y distribuido o en caso de detección de algún virus, existen algunas tareas que se encuentran incluidas en este panel por qué son propias de la consola, se pueden identificar por qué en la columna de “tipo” mencionan que son de sistema, otro tipo es la que un usuario puede crear, veremos unos ejemplos de los 2 tipos de tareas.

¹⁵DLP: Data Loss Prevention, solución designada a detectar y prevenir intentos no autorizados para copiar o enviar datos sensibles

Ejemplo de una tarea del sistema

Update master repository

Esta tarea lo que realiza es la descarga desde el sitio de http de McAfee: “update.nai.com/Products/CommonUpdater”, la primera verificación se realiza a las 14:20 horas y posteriormente se realiza una nueva a las 15:00, esto con el fin de garantizar que se está instalando la nueva versión del archivo DAT¹⁶.

En caso de que exista alguna falla desde la página http, McAfee ofrece la alternativa de realizar la descarga del DAT desde un sitio FTP¹⁷: ftp.nai.com/CommonUpdater. Una vez culminada la tarea se genera una entrada del evento en la consola.

Ejemplo de unas tareas creada por un usuario.

Replicación de archivos a los repositorios distribuidos

La descarga e instalación de los diferentes productos en la consola, el sistema procede a “repartir” entre 3 repositorios distribuidos, los paquetes de actualización, esto con el fin de evitar que en los puntos donde se concentran la mayor parte de los equipos tengan que realizar la comunicación del agente hasta el repositorio principal, los sitios en donde se encuentran estos 3 repositorios distribuidos son el almacén que se encuentra ubicado en Tecámac, el corporativo concluida de Tecamachalco y el corporativo de Iturrigaray. Dependiendo del ancho de banda de cada sitio, los tiempos de actualización oscilan entre los 6 minutos y hasta 15 minutos.

¹⁶DAT: Es un archivo de datos usado para almacenar información de varios tipos de software.

¹⁷FTP: File Transfer Protocol, es un protocolo de transferencia de archivos.

Para crear la tarea de replicación debemos ir a menú → automatización → tareas servidor, en la parte inferior se debe seleccionar nueva tarea, aparecerá una ventana donde se debe poner el nombre de la tarea, seleccionar si estará activa o desactivada, siguiente mostrara otra ventana escoger que tipo de acción se requiere en este caso debe ser “replicación del repositorio”, más abajo seleccionar el tipo de replicación “incremental”, elegir en donde se debe replicar “repositorios seleccionados”, escoger el repositorio deseado, clic en aceptar → siguiente, pasara otra ventana que es la descripción de la planificación de la tarea, seleccionar “cada día”, “sin fecha de finalización” y determinar a qué hora se llevara a cabo la ejecución, clic en siguiente donde se mostrara la opción de guardar, se aplicara conforme a los parámetros definidos por el usuario.

Despliegue de los archivos de actualización del antivirus a los equipos, esta es una tarea del cliente. La tarea de actualización de los equipos se realiza en un horario comprendido de las 16.00 a las 20:00, cabe aclarar que no todos los equipos en sus diferentes ubicaciones comienzan a actualizarse dentro de este horario, sino que dentro de las propiedades de McAfee es posible habilitar la opción que permite que los mismos se actualicen dentro de ese horario comprendido, pero de manera aleatoria.

Para realizarla se debe uno colocar en menú → sistemas → árbol de sistemas, de la organización se debe elegir el grupo al que quiero que le aplique la actualización, una vez escogido, seleccionar la pestaña de “tareas cliente asignadas” en la parte inferior esta la opción de “acciones” dar clic y aparecerá diferentes opciones seleccionar “nueva asignación de tarea cliente” aparecerá una ventana donde se presentara las opciones para definir si se requiere aplicar esta tarea a toda la organización o interrumpir la herencia.

Luego se debe dar un nombre a la tarea, seleccionar que tipo de acción se realizara, escoger enviar esta tarea a todos los equipos de la organización, dar clic en siguiente aparecerá otra ventana donde se habilita por defecto la opción “todos los paquetes” aunque de cierta forma aquellos productos que están adquiridos y que cuentan con las licencias de McAfee, son los únicos que se actualizan, dar otro clic que nos mostrara otra ventana.

En esta sección de planificación, es donde habilitamos la opción de permitir ejecución aleatoria (cada 30 minutos) así como la ventana de tiempo durante el cual, los equipos comenzaran a actualizarse, esto por qué existe la opción del tipo de planificación que se quiere “cada día”, seleccionar la casilla de permitir ejecución aleatoria, seleccionar repetir entre que horario y se guarda la tarea, esta comenzara aplicarse conforme a los parámetros seleccionados.

En la consola se pueden configurar alertas, está alerta se encarga de avisar mediante un correo electrónico, a los usuarios del departamento de redes y soporte, en caso de que algún tipo de virus se haya infiltrado en cual quiera de los equipos del corporativo, llámese equipo de tiendas, almacenes, corporativo, etc.

Esto con la intención de conocer el tipo de virus, método de empleo de su detección, la acción que el antivirus ejecutó, etc., y ver si la acción que el antivirus tomo fue la más adecuada o si finalmente el usuario tiene o no, que tomar medidas para la erradicación del virus.

Para esta opción debemos entrar a la consola y seleccionar menú → automatización→ respuestas automáticas, llevara a una ventana donde se observaran las alertas configuradas, para crear una se debe de ir a la parte inferior de la ventana y buscar la opción de “nueva respuesta”, pasara a la ventana donde podremos empezar a realizar la configuración.

Primero pedirá el nombre de la alerta, la descripción, el idioma, el grupo de eventos de notificación de Epo, tipo de evento “amenaza”, el estado desactivada o activada, dar clic en siguiente, aparecerá otra ventana donde se tiene que definir los parámetros de la gravedad de la amenaza, la acción que se realizara frente a la amenaza, así como la categoría de amenaza, dar clic en siguiente, en esta ventana se muestran las opciones para “activar esta respuesta si se producen varios eventos”, “cuando el número de eventos es como mínimo” cierto número de eventos, “agrupar eventos agregados por ” acción realizada frente a la amenaza, “como máximo activar una respuesta una vez cada” ciertos minutos, dar clic en siguiente.

En la ventana que aparecerá, se pide determinar qué acciones debe realizar la respuesta cuando se activa, lo primero será seleccionar “enviar mensaje”, después llenar el campo de “destinatarios” con los correos de los contactos a los que será mandado el mensaje, realizaré una breve pausa para explicar cómo se crea un contacto de correo, clic sobre el icono de menú→ administración de usuario→ contactos→ nuevo contactó, llenar los datos que solicitan como “nombre”, “apellido”, “dirección de correo electrónico” → guardar, con esto terminamos el proceso para dar de alta un contacto , proseguiremos con la Importancia del mensaje, “asunto” el nombre con el que se recibirá el correo, por último, el “cuerpo” de correo, dar clic en siguiente→ guardar.

En el menú de la consola existe una opción que se llama directiva DLP, explicaré esta herramienta.

El software McAfee host data loss prevention protege a las empresas del riesgo asociado a la transferencia no autorizada de información, ya sea desde dentro o desde fuera de la organización. La fuga de datos se define como la salida de información confidencial o privada de la empresa como resultado de comunicaciones no autorizadas a través de canales tales como aplicaciones, dispositivos físicos y protocolos de red.

Los dispositivos conectados a los equipos gestionados de la empresa, como smartphones, dispositivos de almacenamiento extraíbles, dispositivos bluetooth, reproductores de MP3 o dispositivos plug-and-play, pueden supervisarse o bloquearse mediante reglas de dispositivos, que permiten supervisar y controlar su uso en la distribución de la información confidencial. Para muchas organizaciones, este nivel de prevención de fuga de datos es el objetivo principal. Se trata del nivel de protección proporcionado por McAfee device control.

Para configurar el módulo del device control es necesario posicionarnos en directiva dlp. Menú→protección de datos→directiva dlp, abrirá una ventana donde se muestra el módulo de device control, este consta de tres opciones para la administración de dispositivos como son:

- Clases de dispositivos
- Definición de dispositivos
- Reglas de dispositivos

Clases de dispositivos

La lista inicial de clases de dispositivos se genera de forma automática. No obstante, cuando añade un nuevo dispositivo, es necesario definir una clase de dispositivo para él si no coincide con la clase existente. Existen tres estados de clases de dispositivos:

- **Gestionado:** Dispositivos plug-and-play o de almacenamientos extraíbles específicos, definidos por clase de dispositivos, que puede gestionar el software McAfee host data loss prevention.

- **No gestionado:** Clases de dispositivos no gestionadas por el software McAfee host data loss prevention, pero cuyo estado puede cambiar a gestionado por el administrador del sistema.
- **No gestionable:** Clases de dispositivos que el software McAfee host data loss prevention no puede gestionar debido a que los intentos para gestionarlas pueden afectar al equipo gestionado, al funcionamiento o a la eficacia del sistema. No se pueden agregar nuevas clases de dispositivos a la lista.

Para modificar una clase de dispositivo existente, haga doble clic en la definición. Para agregar nuevas definiciones, utilice el menú contextual. Los nuevos dispositivos siempre se añaden con el estado *no gestionado* como medida de precaución. Cambie el estado del dispositivo ha gestionado/no gestionado con el menú contextual.

Definición de dispositivos

Las definiciones de dispositivos identifican y agrupan los dispositivos según distintos criterios, como las propiedades del dispositivo. Los dos tipos de dispositivos admitidos son:

- **Dispositivos plug-and-play:** Pueden agregarse al equipo gestionado sin necesidad de realizar configuraciones. Entre los dispositivos plug-and-play se incluyen la mayoría de los dispositivos Windows. Las definiciones de dispositivos plug-and-play permiten gestionar y controlar la mayoría de dispositivos disponibles.

- **Dispositivos de almacenamiento extraíble:** Un dispositivo externo que contiene un sistema de archivos que aparece en el equipo gestionado como una unidad. Las definiciones incluidas para McAfee endpoint encryption y McAfee encrypted USB facilitan el uso de dichos productos.

Dispositivos plug-and-play de la lista blanca

El objetivo de incluir dispositivos plug-and-play en la lista blanca es gestionar aquellos que no llevan a cabo la administración de dispositivos de forma óptima y que pueden provocar que el sistema deje de responder y otros problemas de gravedad.

Para la creación de una definición para dispositivo de almacenamiento extraíble debemos seguir los siguientes pasos en la pestaña de directiva dlp ir a → nuevo → definición de dispositivo de almacenamiento extraíble en esta podremos dar el nombre a la definición para este dispositivo, se debe dar clic seleccionar la opción editar, aparece una ventana donde se pide el “nombre” de la definición, seleccionar la opción “tipo de bus” (por ejemplo, USB, PCI) dar clic en los puntos suspensivos (...). De esta opción, abrirá otra ventana donde se tiene que seleccionar la casilla de “USB”, el proceso anteriormente explicado es la creación de una definición para bloqueo de un dispositivo “USB”.

A continuación, explicaré la “creación de una definición para lectura y escritura de dispositivo USB”, colocarnos sobre la definición de dispositivo de lectura y escritura creada dar un clic → editar, seleccionar en la ventana que aparece las siguientes opciones “acceso al sistema de archivos (solo lectura, lectura-escritura)” dar clic en los puntos suspensivos que se encuentran al final de esta línea.

Abrirá una ventana donde se escogerá la opción de “lectura-escritura” → aceptar, ir a la opción de “tipo de bus (por ejemplo, USB, PCI)”, dar clic en los puntos suspensivos abrirá una ventana donde debemos seleccionar “USB” → aceptar nuevamente → aceptar con esto se termina la creación de la definición antes mencionada.

Reglas de dispositivos

Las reglas de dispositivos definen la acción realizada cuando se utilizan determinados dispositivos. Permite bloquear o supervisar los dispositivos, así como notificar al usuario la acción realizada. Además, las reglas de dispositivos de almacenamiento extraíbles pueden definir un dispositivo como "solo lectura".

Para crear una nueva regla de dispositivo, utilice el menú contextual. Una vez que se cree la regla, defínala haciendo doble clic en ella y siguiendo los pasos que se indican en el asistente. Todas las reglas deben definir como mínimo un dispositivo y una acción.

Para la creación de una regla para un dispositivo de almacenamiento extraíble debemos hacer lo siguiente ir a “reglas” → nuevo → regla para dispositivos de almacenamiento extraíbles, colocarse en la nueva definición creada para dispositivo USB para realizar la creación de una regla para bloqueo de un dispositivo USB → editar, abrirá una ventana seleccionar “removable storage device definition USB bloqueo” dar clic en agregar grupo mostrara otra ventana donde se seleccionarán las casillas “bloquear”, “supervisar”, “notificar al usuario”, clic en siguiente → finalizar.

A continuación, explicaré la creación de una regla para lectura de un dispositivo USB ir a “reglas” → nuevo → “regla para lectura de un dispositivos USB”, colocarse en la nueva definición creada para dispositivo USB → editar, abrirá una ventana seleccionar “removable storage device definition USB lectura” dar clic en agregar grupo mostrara otra ventana donde se seleccionarán las casillas “supervisar”, “notificar al usuario”, “solo lectura”, clic en siguiente → finalizar.

Se explicara una regla más, se creara una “regla para lectura y escritura de un dispositivo USB”, ir a “reglas” → nuevo → regla para dispositivos de almacenamiento extraíbles, colocarse en la nueva definición creada para dispositivo USB para realizar la creación de una regla para lectura y escritura de un dispositivo USB → editar, abrirá una ventana seleccionar “removable storage device definition USB lectura y escritura” dar clic en agregar grupo mostrara otra ventana donde se seleccionarán las casillas, “supervisar”, “notificar al usuario”, clic en siguiente → finalizar.

Asignación de Directiva a un equipo

Para asignar directiva del device control a un equipo, es necesario ir al árbol de sistemas.

>Menú>Sistemas>Árbol de sistemas

Colocarse en la organización, buscar el equipo al que se le aplicara la directiva seleccionarlo, ir a la parte inferior de la organización dar clic en acciones → agente → modificar directivas en un solo sistema, editar la directiva con el nombre de Viana, pasará a otra ventana en esta debemos seleccionar “interrumpir herencia para que solo aplique en este equipo”, elegir “editar directiva”, seleccionar la regla para el dispositivo de almacenamiento extraíble, en este caso permite la lectura y escritura de USB → guardar.

Instalación del Agente DLP

Ya que se encuentra asignada la directiva en el equipo, se procede a la instalación del agente dlp, aparece otra ventana donde debemos colocar en “despliegue device control” → editar configuración → siguiente, mandara a otra ventana en esta se debe seleccionar “interrumpir herencia y asignar la directiva y la configuración a partir de este punto”→ siguiente, aparecerá otra ventana en esta se tiene que configurar las siguientes opciones para la tarea de despliegue del agente dlp.

En esta se selecciona la casilla de Windows, seleccionar en productos y componentes el producto de McAfee data loss prevention →acción →instalar →idioma →ingles → rama →actual →siguiente esta ventana que aparecerá debemos seleccionar que este “activado”, “ejecutar inmediatamente”, clic en siguiente aparecerá una ventana donde muestra la descripción de la tarea, por último, es necesario despertar los agentes para que comience la ejecución para la instalación del agente dlp, tenemos que seleccionar el equipo y clic en activar agente para que se despliegue la instalación.

Es importante resaltar que para que un equipo reporte a la consola es necesario que tenga instalado el antivirus de McAfee y el agente que es el que realiza la comunicación con la consola, cumpliendo con estos requisitos se debe dar de alta el equipo en la consola para esto se debe ingresar a la consola seleccionar menú→sistemas → árbol de sistemas, colocarse en la organización a la que ingresaremos el equipo, ir a la parte inferior izquierda seleccionar “acciones en el sistemas” → sistemas nuevos, abrirá una ventana en ella seleccionaremos el campo de “insertar agente y agregar sistemas al grupo actual (mi organización)”.

Poner el nombre de host del equipo, tener activa la casilla “desactivar clasificación del árbol de sistemas en estos sistemas”, seleccionar agente para Windows →McAfee agent for Windows 4.8.0 (actual)” , poner enseguida las credenciales para la instalación del agente se pide dominio, nombre de usuario, contraseña y confirmar la contraseña clic en aceptar y la tarea será mandada al equipo.

Para que pueda reportar a la consola el equipo. Para verificar que la tarea se está ejecutando la tarea correctamente debemos ir a menú →automatización → registro de tareas servidor, abrirá una ventana donde se puede observar el nombre de la tarea, fecha de inicio, fecha de finalización, nombre de usuario, estado, origen y duración, en el campo de estado muestra el porcentaje que lleva de ejecución, cuando termina pone un estado de finalizada, lo que restara realizar es regresar a la organización a donde colocamos el equipo para verlo en la consola.

4.3 Administración de proxy

La administración de proxy, se realiza por medio de dos herramientas un proxy con sistema operativo Linux fedora y un appliance, a continuación muestro la figura 4.3.1, el diagrama de conexión de los dos servidores.

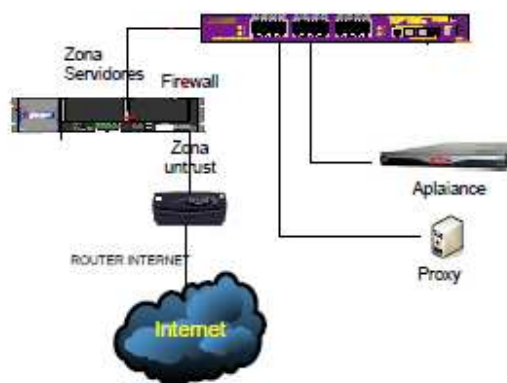


Figura 4.3.1 Diagrama de conexión servidores proxy

Explicaré primero el de Linux fedora, “un proxy de conexión a Internet es un servidor que hace de intermediario entre los pc’s de la red y el router de conexión a Internet, de forma que cuando un usuario quiere acceder a Internet, su pc realiza la petición al servidor proxy, el proxy es quien realmente accede a Internet. El proxy enviará los datos al pc del usuario para que los muestre en su pantalla. El pc del usuario no tendrá conexión directa con el router, sino que accederá a Internet por medio del proxy”¹⁸.

Las ventajas de un proxy las menciono a continuación:

Los equipos de cómputo de los usuarios no tienen acceso al router, todas las comunicaciones exteriores pasarán por el proxy, lo que permitirá tener las comunicaciones bajo control. Se puede permitir o denegar el acceso web, ftp, email, messenger, p2p, etc.

Las páginas se guardan en la memoria temporal del proxy lo cual acelera la descarga cuando varios usuarios acceden a las mismas páginas a la vez. Es fácil crear una lista de urls prohibidas a las que el proxy denegará el acceso.

Permite crear listas de palabras prohibidas en urls. Se puede permitir o denegar el acceso a subredes o a equipos de cómputo en concreto.

El proxy guarda informes de todas las conexiones que hacen los usuarios. Se puede capturar el tráfico que pasa por el proxy, de esta manera se sabe a qué páginas de contenido inadecuado acceden los usuarios, para agregarlas a la lista de urls prohibidas.

Los equipos de cómputo en nuestra red están más seguros de ataques externos ya que el proxy hace de barrera cortafuegos.

¹⁸Ite, Junio 15 2015,
<http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html>

Linux dispone del proxy squid. Se trata de una aplicación que dispone de cientos de posibilidades para personalizar su funcionamiento de acuerdo a nuestras necesidades y configurarlo con las reglas que nosotros consideremos.

Configuración básica del proxy squid

El archivo de configuración del proxy es el archivo **/etc/squid/squid.conf**. Dicho archivo, es muy extenso pero para una utilización básica, son unos pocos los parámetros que debemos configurar, destacaremos los siguientes:

Access Control (Control de Acceso)

En esta sección estableceremos los permisos de acceso, quien puede navegar y quién no. Lo primero que tendremos que hacer es crear listas de control de acceso (access control list - acl) y luego dar permisos a dichas listas.

Una lista de control de acceso (acl) se crea utilizando la palabra acl seguido del nombre que queramos dar a la lista y seguido de una condición que cumplirán los miembros de la lista. Entre las condiciones más utilizadas destacamos: src "(ips o urls origen)", dst "(ips o urls destino)", port (puertos) y proto (protocolos).

Cuando creamos acls, podemos sustituir el rango de ips por el nombre de un archivo externo, y de esa manera podemos indicar en el archivo externo el rango o los rangos de ips a los que queremos referirnos, sin necesidad de estar continuamente modificando el archivo squid.conf, daré ejemplos de las diferentes formas de crear acl.

Ejemplos:

```
aclSafe_portsport "numero del puerto que se desea abrir" #comentario
```

```
aclSafe_portsport 80 # http
```

```
acl(nombre de la acl) src "ruta donde se encuentran las ip's para esta regla"
```

```
acl PCsDirectores src "etc/squid/IPDirectores"
```

```
acl(nombre de la acl) src "IP a la que se le aplicara esta regla"
```

```
aclPCsPedroPerezsrc192.168.110.150/255.255.255.255
```

```
aclPCsPedroPerezsrc192.168.110.150/32
```

```
acl(nombre de la acl)dst (ruta donde se encuentran las ip's para esta regla)
```

```
acl dominiosPermitidos dstdomain "etc/squid/acl/dominiosPermitidos.acl"
```

```
# Insert your own rule(s) here to allow access from your clients
```

En este parámetro se tendría que dar permiso a las listas. Para ello se utiliza la palabra clave **http_access** seguido del permiso allow (permitir) o deny (denegar) y seguido del nombre de la lista.

Ejemplos:

Si quiero dar permiso una acl que contiene una lista de usuarios para que navegue por Internet:

```
http_access allow (Nombre de la acl que contiene la lista de usuarios).
```

```
http_accessallowPCsDirectores
```

Si quiero dar permiso a una acl que solo afecta a un equipo de cómputo.

http_access allow (nombre de la acl que afecta solo a un equipo) (nombre de la regla que contiene la URL a la que tendrá permitido navegar el usuario).

http_accessallowPCsDirectoresURLPermitidas

Para denegar acceso a una lista de url

http_access deny (nombre de acl creada que contiene la lista de páginas que se deniegan)

http_access deny Hotmail

#Network options(opciones de red)

En esta sección estableceremos con el parámetro http_port, el puerto en el que escucha el proxy.

Comando para configurar squid en el puerto 8080

http_proxy 8080

Memory cache options

En esta sección estableceremos la memoria RAM utilizada para la caché. Nuestro sistema tiene 512 MB de memoria RAM, utilizar el siguiente comando para indicar cuanta memoria será utilizada por el squid:cache_mem 8 MB

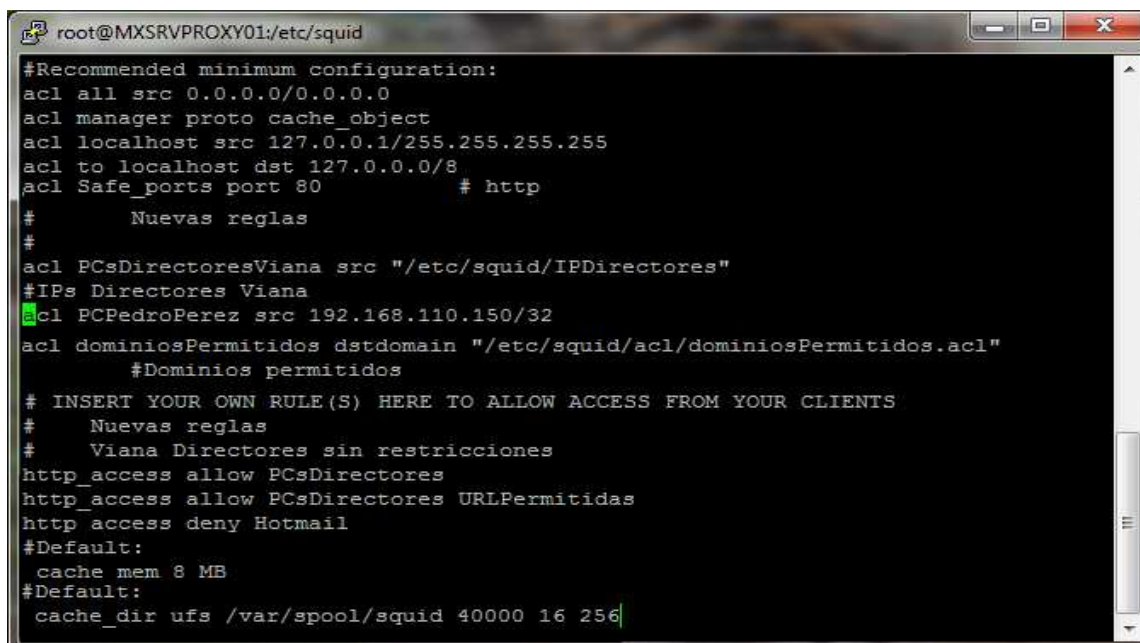
Disk cache options

En esta sección estableceremos el espacio de disco duro utilizado para la caché, nuestro sistema tiene 80 GB de memoria, utilizar 40 GB.

Deberemos utilizar la palabra clave `cache_dir` seguida de la palabra `ufs` que es el formato utilizado por squid, de la carpeta donde queremos que se almacene la cache, el tamaño de la caché en MB, el número de subdirectorios de primer nivel y el número de subdirectorios de segundo nivel. Queremos que la caché se guarde en `/var/spool/squid`, que utilice 40 GB y que cache hasta 16 subdirectorios de primer nivel y hasta 256 subdirectorios de segundo nivel, escribiremos el siguiente comando:

```
cache_dir ufs /var/spool/squid 40000 16 256
```

A continuación se presenta la figura 4.3.2 de la configuración del archivo squid.



```
root@MXSRVPROXY01:/etc/squid
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl Safe_ports port 80          # http
#
#   Nuevas reglas
#
acl PCsDirectoresViana src "/etc/squid/IPDirectores"
#IPs Directores Viana
acl PCPedroPerez src 192.168.110.150/32
acl dominiosPermitidos dstdomain "/etc/squid/acl/dominiosPermitidos.acl"
#Dominios permitidos
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
#   Nuevas reglas
#   Viana Directores sin restricciones
http_access allow PCsDirectores
http_access allow PCsDirectores URLPermitidas
http_access deny Hotmail
#Default:
cache mem 8 MB
#Default:
cache_dir ufs /var/spool/squid 40000 16 256
```

Figura 4.3.2 Configuración de archivo squid.

Análisis de conexiones

Una de las funcionalidades principales que nos ofrece squid es que registra todos los accesos a Internet. Cada vez que un equipo accede a Internet, squid registrará en el archivo `/var/log/squid/access.log` la fecha y hora, el equipo y la url a la que ha accedido.

Configuración del navegador de los equipos clientes, para que utilicen el proxy

Nuestro servidor proxy tiene la IP 192.168.10.144 y el servidor squid está escuchando en el puerto 8080. Con estos dos datos, la IP y el puerto, ya podemos configurar el navegador de Internet de los equipos clientes.

Para indicar a Internet Explorer que debe utilizar un proxy para realizar conexiones, debemos ir a Inicio →panel de control →opciones de internet→conexiones→configuración de LAN y activar la casilla 'usar un servidor proxy para la LAN'. En la casilla 'dirección' pondremos la IP de nuestro proxy y el 'puerto' el puerto.

Administración de Appliance

Appliance es un proxy de forma gráfica es parte de la familia McAfee secure content management, McAfee WebShield 3000 Series Appliance, es una solución para el gateway de Internet, que solo es preciso configurar una vez y que exploran el tráfico de entrada y de salida en busca de protocolos SMTP, HTTP, FTP y POP3.

El dispositivo cuenta con la capacidad de detección y limpieza de virus, así como de protección contra el correo no deseado de tipo spam y el contenido desechable.

El link para ingresar al appliance es: <https://192.168.10.6> se debe colocar en un explorador de internet, abrirá la consola de administración en ella se visualiza la primera opción que es el Panel se encuentra el monitoreo de:

- Correo electrónico
- Detecciones Web
- Mantenimiento a sistema
- Índices de detección actuales
- Red
- Colas de correo electrónico
- Análisis de directivas
- Tareas

Mencionaré algunas de estas opciones que se encuentran en el panel. En la opción de correo electrónico se puede configurar las preferencias de detecciones de correo electrónico, se pide llenar que protocolos mostrar seleccionar “SMTP”, “POP3”, seleccionar que contadores mostrar, “mensajes”, “conexiones bloqueadas”, “virus”, “pup¹⁹”, “spam²⁰ y phishing²¹”, “autenticación de remitente”, “contenido filtrado”, “otros”.

¹⁹PUP: Programa potencialmente no deseado

²⁰Spam: En términos informáticos es correo basura.

²¹Phishing: En términos informáticos es la suplantación de identidad

Las preferencias de detecciones web, se pide llenar que protocolos mostrar seleccionar “http”, “icap²²”, “FTP” seleccionar que contadores mostrar, “solicitudes”, “virus”, “pup”, “URL filtrada”, “SiteAdvisor²³”, “contenido filtrado”, “otros”.

En preferencias de red, deben seleccionarse los protocolos siguientes “SMTP”, “POP3”, “http”, “icap”, “FTP”, clic en aceptar.

Existe otra pestaña que se llama Informes, donde encontraremos como su mismo nombre dice informes, son los siguientes.

- Informes programados
- Informes de correo electrónico
- Informes web
- Informes del sistema

Los informes programados son los que se han configurado para ser enviados por correo electrónico. Los informes de correo electrónico, genera un reporte únicamente de la actividad del correo electrónico con características como:

- Descripción general de correo electrónico.
- Perfil de correo electrónico
- Principales remitentes de spam
- Principales virus

²²ICAP: Es el protocolo de adaptación de contenidos de internet, se utiliza para la redirección de contenidos con fines de filtrado y conversión.

²³SiteAdvisor: Es un servicio que informa sobre la seguridad de los sitios en busca de malware y spam.

- Bloqueados
- Correos electrónicos entregados
- Correos electrónicos bloqueados
- Correos electrónicos devueltos

En Informes web, genera un informe de actividad web, de:

- Lista de url principales
- Supervisados
- Modificados
- Bloqueados

El informe de sistemas, despliega informes de actualización de dat / reglas, actualiza dat.

En otra pestaña del panel principal se encuentra correo electrónico, tiene otras pestañas la primera es:

Descripción general de correo electrónico donde se muestra el resumen de correo electrónico entrante y correo electrónico en cola.

La segunda pestaña de esta opción es configuración de correo electrónico que tiene otras opciones de configuración que las menciono:

- Configuración de protocolos
- Recepción de correo electrónico
- Envío de correo electrónico

En la configuración de protocolos, permite realizar la configuración de los puertos que se les permitirá el acceso por la red.

En la recepción de correo electrónico se permite configurar que conexiones permitidas o bloqueadas por medio de su dirección IP, nombre de dominio o puerto y especificar el tiempo de permitida o bloqueada la conexión.

La pestaña de envío de correo electrónico, se configuran los dominios, host de transmisor conocidos y los transmisores de respaldo para dominios inaccesibles.

Continuando con la pestaña de correo electrónico la tercera son directivas de correo electrónico, en esta opción existen dos pestañas en la primera que es “análisis de directivas” aquí se muestran las directivas y su configuración, la segunda pestaña es la de “diccionarios”, se agregan diccionarios de correo electrónico.

Siguiendo en correo electrónico la cuarta pestaña es la de configuración de cuarentena en ella encontramos las opciones para realizar la configuración de lo que se va a cuarentena:

- Opciones de cuarentena
- Opciones de resumen de cuarentena
- Contenido del mensaje de resumen

Pasando a otra pestaña del menú principal continuaré con la de web, aquí se encuentra la opción de “configuración web” para las siguientes opciones en cada una de ellas se puede agregar un puerto seguro si así se desea:

- HTTP,
- ICAP
- FTP

La otra opción de la pestaña web es la de “directiva web”, en ella encontramos las opciones de:

- Administración de directivas

Aquí se crea la directiva, se configuran las url a las que podrá ingresar y se puede restringir por medio del tipo de contenido al que se puede navegar.

- Diccionarios

Se agregan diccionarios de correo electrónico primera de ellas es:

Configuración de dispositivo

En otra pestaña del menú principal encontramos la de “sistema” aquí diferentes opciones que iremos mencionando a continuación la

→ General

La configuración básica general del sistema es:

- Nombre del dispositivo: **McAfee**
- Dominio: **viana.com.mx**
- Puerta de enlace: **192.168.10.250**

→ DNS y Enrutamiento

En esta pestaña se coloca la dirección IP de los DNS²⁴, si se tiene algún enrutamiento aquí se debe agregar los datos de IP de la dirección de la red, la máscara y puerta de enlace.

La segunda opción es la:

Administración de sistema

Gestionar dispositivo se puede realizar una copia de seguridad de los registros y configuración de copia de seguridad. Así mismo es posible realizar una restauración ya sea desde archivo volver a valores de configuración predeterminados, realizar configuración de fecha y hora.

La tercera opción es:

Usuarios, grupos y servicios

En los grupos de directivas se incluye la dirección IP que se desea pase por el appliance, dependiendo el grupo que se haya creado y el departamento.

Para agregar una IP se debe uno de colocar en la directiva deseada dar clic y la opción “agregar regla”, escribir la dirección IP y aceptar, dar clic en el icono verde para modificar la directiva y aplique el cambio correctamente, aquí también encontraremos la sección de “cuentas de usuario basadas en la función”, en esta sección se puede crear cuentas de usuario así como el tipo de permisos.

²⁴DNS: DomainName System en español Sistema de Nombre de Dominio.

La cuarta opción es:

Registros, alertas y SNMP

- Alerta de correo electrónico.
- Configuración de alertas SNMP²⁵.
- Configuración del monitor SNMP.
- Configuración de registros del sistema.

Como su mismo nombre los menciona en estas pestañas se configuran alerta de correo electrónico y alertas.

4.4 Administración e instalación de servidores

La administración de servidores requiere diversas actividades previas, como cuál será la mejor opción de compra, esto dependerá de la necesidad de operación que el servidor tenga que soportar, así que se tendrá que buscar que marca, modelo, capacidad de discos duros, memorias, procesador, tarjetas de red con las que debe contar, número de fuentes de poder, contratación de extensión de garantía de piezas que puedan dañarse con esto se evita alguna caída en la operación, una vez realizada la compra se debe realizar el armado del servidor, configurar el arreglo de Discos que llevara.

²⁵SNMP: Simple Network Management Protocol, es el protocolo simple de administración de red, facilita el intercambio de información de administración entre dispositivos de red

Este puede ser de varios tipos RAID 0, RAID 1, RAID 5 y RAID 0+1, los arreglos son utilizados para la protección de la información o el incremento del desempeño al acceso de los discos duros, RAID es un método de combinación de varios discos duros para formar una unidad lógica única en la que se almacenan los datos de forma redundante, es tolerante a fallos y más alto nivel de rendimiento que un solo disco duro o un grupo de discos duros independiente, explicaré en qué consiste cada uno de ellos.

RAID 0. Este arreglo se utiliza en un sistema que utiliza los discos como uno solo, teniendo un conjunto de cabezas independientes para su uso, la información es dividida en bloques de datos que se distribuyen en todos los discos duros del arreglo, este arreglo incrementa el desempeño, la lectura y escritura de la información al escribir un solo dato con varias cabezas de forma simultánea, este arreglo no tiene nivel de protección, en caso de la falla de un disco duro, se perderá toda la información.

RAID 1. Se conoce como espejo ya que el conjunto de discos los utiliza como espejos, su nivel de protección es alto, porque cada disco tiene una copia idéntica de la información de cada disco, en este arreglo se tiene un incremento en el desempeño de la lectura de la información, pero puede llegar a degradar el desempeño de la escritura.

RAID 5. A este tipo de arreglo se le denomina como distribuido con paridad, con este arreglo se distribuye la información en todo el conjunto de discos, elabora un bit de paridad con el cual es posible reconstruir la información del arreglo en caso de la pérdida de alguno de los discos, así se garantiza que siempre se encontrarán en discos distintos, si un disco falla, el desempeño de la lectura se degrada.

RAID (0+1). Es una mezcla del arreglo distribuido y espejo. La información se distribuye en un conjunto de discos como un RAID 0 y a su vez este conjunto de discos es espejado a otro conjunto de discos como un RAID 1, RAID (0+1).

Provee el nivel de protección y desempeño más alto para escritura y lectura que cualquier otro arreglo, debido a que contiene los beneficios de los arreglos distribuidos y espejo, el costo de este arreglo es elevado ya que se usa siempre dobles discos.

Teniendo definido que arreglo se utilizara se debe configurar, esto puede ser por la herramienta del propio fabricante del servidor o por el medio de las opciones del BIOS²⁶; para realizar el arreglo, el siguiente paso será instalar el sistema operativo puede ser Windows Server 2003, Windows Server 2008, Windows Server 2012 o alguna versión de Linux que puede ser Fedora, esto dependerá por el que tipo de aplicación que correrá en el servidor, una vez instalado el sistema operativo en el servidor, se procederá en el siguiente orden a la preparación del servidor con las políticas de seguridad requeridas por la empresa

A continuación se muestra la figura 4.4.1 de un arreglo de disco con la herramienta del servidor.

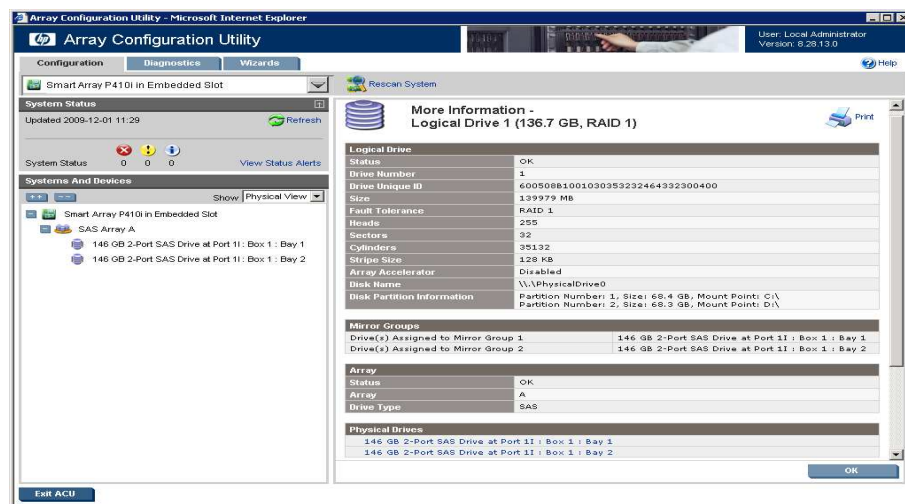


Figura 4.4.1 Arreglo de disco con herramienta de servidor

²⁶BIOS: Basic input/output system, el software BIOS es el primer programa que se ejecuta cuando se enciende la computadora

Es necesario configurar una conexión de red con los parámetros que se requieran para el servidor, es decir, con la IP designada para este servidor.

Para ello es necesario conectar el cable de red, estar seguros de que el nodo de red tiene conectividad y que el cable funciona; si ya se verificó esto, en el panel de control del servidor en la opción conexiones de red, en el icono de la tarjeta que se ha conectado se da doble clic; aparecerá una pantalla en esta ubica la opción señalada como Internet protocoló (TCP/IP) y se le da doble clic, lo que conducirá a otra pantalla.

Aquí se habilitan las opciones de “use the following IP address” y “use the following DNS server address” se escriben los parámetros de red que se han designado para el servidor, los parámetros requeridos son IP address, subnet mask, default Gateway, preferred DNS server y alternate DNS Server. Al terminar de configurar los parámetros, se da clic en el botón “ok”.

Instalación del cliente del antivirus

El segundo punto es la instalación del antivirus, para ello es necesario el acceso a la siguiente ruta \\192.168.10.229\anti-virus\Antivirus 8.7\VSE870LML.

Deberá de salir una pantalla, aquí se debe de poner un usuario y una contraseña válidos para el dominio CDV, es necesario tomar en cuenta que antes del usuario se debe de escribir el nombre del dominio “CDV”, seguido por una diagonal invertida (ALT + 92), a continuación se muestra la figura 4.4.2.



Figura 4.4.2 Credenciales validas de dominio.

Si los datos introducidos son válidos, aparecerá una ventana se debe ubicar el archivo ejecutable llamado “setupVSE”, una vez ubicado hay que ejecutarlo dando doble clic sobre el icono, se muestra a continuación la figura 4.4.3.

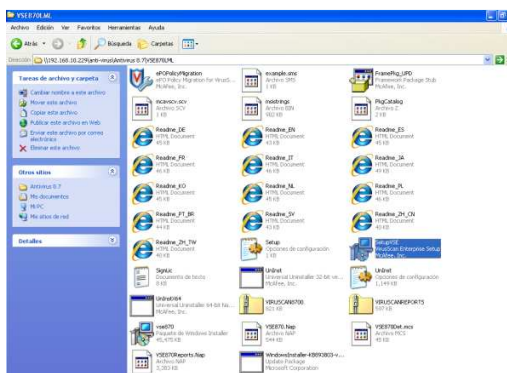


Figura 4.4.3 Archivo setupVSE

Aparecerá otra ventana donde se debe dar clic sobre el botón “run”, tardara un momento y aparecerá otra ventana, aquí indica que se ha solicitado la inhalación del antivirus, así es que solo es necesario dar clic sobre el botón “next”, mostrara una ventana en esta es necesario tomar en cuanto tres modificaciones a realizar, la primera es que en la parte en donde dice “license expiry type” en la parte superior izquierda de la ventana se debe de seleccionar la opción “perpetual”. La segunda modificación que se debe de hacer es en la parte superior derecha en la opción que se titula “select location where” se debe de seleccionar la opción “México”. Finalmente, la tercera modificación que se debe de realizar es en la parte inferior izquierda de la pantalla, se debe de seleccionar la opción “iaccept the terms...” cuando se han hecho estos cambios se debe de dar clic con el mouse en el botón ok”, llevara a otra ventana en esta solo se debe de verificar que el tipo de instalación sea “typical” y continuación se debe de dar clic en el botón “next”.

Saldrá otra ventana en la cual indica el nivel de protección requerido para iniciar sesión, se debe de verificar que el nivel este seleccionado “standard protection” ya que la máxima protección bloquea algunas aplicaciones requeridas para el funcionamiento del servidor. Posteriormente se debe de dar clic en el botón “next”, a continuación iniciara el proceso de instalación del software y al finalizar aparecerá una ventana aquí es necesario deshabilitar las dos opciones disponibles; “update now” y “run on-demand scan”. Una vez verificado esto, se debe de dar clic en el botón “finish”. Aparecerá la siguiente ventana, está alerta indica que es necesario reiniciar el equipo, por lo que es necesario aceptar la alarma dando clic en el botón “ok” y posteriormente es necesario reiniciar el servidor de manera manual.

Una vez terminada la primera parte de la instalación del antivirus es necesario reiniciar el servidor.

Instalación del parche

Cuando se termina de reiniciar el servidor se debe de entrar a la siguiente ruta \\192.168.10.229\anti-virus\Antivirus 8.7\VSE870P2, aparecerá una pantalla al igual que en la primera parte de la instalación será necesario introducir un usuario y una contraseña válidos para el dominio CDV, se debe tomar en cuenta que antes del usuario hay que escribir el nombre del dominio "CDV", seguido por una diagonal invertida (ALT + 92). Si los datos introducidos son válidos, aparecerá una pantalla se debe de ubicar el archivo ejecutable llamado "setup", una vez ubicado hay que ejecutarlo dando doble clic sobre el icono. Aparecerá una ventana, aquí se solicita autorización para ejecutar el archivo, solo es necesario dar clic en el botón "run", aquí se da inicio al proceso de instalación del parche de McAfee, solo es necesario dar clic en el botón "siguiente".

Una vez que se ha terminado el proceso de instalación de la aplicación, dar clic en el botón "finalizar" para salir del asistente de instalación.

Instalación del antispymware

Una vez terminada la instalación del parche, ya no es necesario reiniciar el equipo. Se procede a la instalación del antispymware²⁷. Para ello se debe ir a la siguiente ruta, \\192.168.10.229\anti-virus\antivirus 8.7\ASEM870LALL, al entrar en esta ruta, aparecerá una pantalla, en esta pantalla es necesario introducir un usuario y una contraseña válidos para el dominio CDV, se debe tomar en cuenta que antes del usuario hay que escribir el nombre del dominio "CDV", seguido por una diagonal invertida (ALT + 92). Si los datos introducidos son válidos, saldrá otra pantalla, se debe de ubicar el archivo ejecutable "VSE87MAS" y dar doble clic para que se ejecute.

²⁷Antispymware: Aplicación que se encarga de buscar, detectar y eliminar espías en el sistema.

Una vez ejecutado el archivo aparecerá una ventana, se solicita autorización para ejecutar el instalador del agente antispyware, solo es necesario dar clic sobre el botón “run” que se encuentra en la parte inferior derecha de la ventana. Aparecerá una ventana de aviso de la instalación del agente antispyware de McAfee, solo es necesario dar clic en el botón “next” y pasar a la siguiente ventana, en esta es necesario tomar en cuenta tres modificaciones a realizar, la primera es que en la parte en donde dice “license expiry type” en la parte superior izquierda de la ventana se debe de seleccionar la opción “perpetual”. La segunda modificación que se debe de hacer es en la parte superior derecha en la opción que se titula “select location where...” se debe de seleccionar la opción “México”. Finalmente, la tercera modificación que se debe de realizar es en la parte inferior izquierda de la pantalla, se debe de seleccionar la opción “i accept the terms...” Cuando se han hecho estos cambios se debe de dar clic con el mouse en el botón “ok” de esta ventana, con esto iniciara el proceso de instalación de los archivos, una vez terminado el proceso dar clic en el botón “finish” que se encuentra en la parte inferior de la ventana.

Instalación del agente de actualización

Ahora será necesario instalar el agente para la conexión al servidor que contiene las actualizaciones del antivirus. Para ello es necesario entrar a la siguiente ruta, \\192.168.10.229\anti-virus\Antivirus 8.7.

En esta pantalla es necesario introducir un usuario y una contraseña válidos para el dominio CDV, se debe tomar en cuenta que antes del usuario hay que escribir el nombre del dominio “CDV”, seguido por una diagonal invertida (ALT + 92).

Si los datos introducidos son válidos, aparecerá una ventana se debe de ubicar el archivo "FramePkg.exe" y se debe dar doble clic para ejecutarlo, se solicita autorización para ejecutar el archivo, es necesario dar clic en el botón "run", una vez que se termina de instalar el agente, aparece una ventaba donde se indica que el agente se instaló correctamente, solo es necesario dar clic en el botón "ok" para finalizar la instalación.

Ahora el antivirus está completamente instalado y es necesario actualizarlo, para ello es necesario ubicar el icono del cliente de McAfee, este se encuentra en la esquina inferior derecha de la pantalla principal de Windows; junto al reloj, se puede identificar como un escudo del lado izquierdo. Se coloca el cursor sobre el icono de McAfee y se presiona el botón derecho del mouse, con esto aparecerá un menú debe de seleccionarse, la opción "actualizar ahora..." que es la segunda opción, contando de abajo hacia arriba, una vez terminado el proceso se deberá cerrar la pantalla y con esto concluye la instalación del antivirus.

Instalación de office

Después debemos realizar la instalación de la paquetería de Office esta se puede realizar por medio de la unidad de CD o por medio de USB, debemos ubicar el archivo ejecutable llamado "setup.exe" y dar doble clic sobre el icono de este archivo para que inicie el proceso de instalación, aparecerá una ventana en esta únicamente solicita autorización para ejecutar el programa de instalación. Será necesario dar clic en el botón "run" que se encuentra en la parte inferior de la ventana. Mostrará otra ventana, aquí será necesario introducir un código de licencia valido para office.

Una vez que se ha introducido este código llave, se da clic en el botón “next” que se encuentra en la parte inferior de la ventana, llevara a otra ventana donde es necesario escribir los datos de la compañía de la siguiente manera; user name: Viana, organization: Viana Descuentos S. A. de C. V.

Ya que se han introducido estos datos hay que dar clic en el botón “next”, aparecerá una ventana, aquí se indica el contrato de licencia de usuario para este software, es necesario aceptar el contrato, palomeando la opción “i accept the terms...” y posteriormente dando clic sobre el botón “next”. Lleva a otra ventana, en esta se configura el tipo de instalación que se requiere para el software, se debe de seleccionar la opción “custom install”, se da clic en el botón “next”, mostrara otra ventana, en esta se requiere que se quite, la selección de tres programas, “publisher”, “access” e “infopath”. También será requerido palomear la opción “choose advanced customization...”.

Si ya se han hecho estos cambios, se debe dar clic en el botón “next” que está en la parte inferior derecha de la ventana, aparecerá una nueva ventana, aquí se debe instalar todas las funciones de la aplicación en el disco duro local, para ello se debe dar un clic con el botón izquierdo del mouse, con lo que aparecerá un cuadro de diálogo en él se muestra un cuadro de opciones, se debe de seleccionar la opción de “run all from my computer”, esto provocara que el icono de la herramienta a instalar cambie de color a blanco.

Como nota importante se debe de tomar en cuenta que los iconos que tiene tache son los iconos de los programas que no se desean instalar así es que este procedimiento para instalar todo desde la PC solo se debe de realizar con los iconos que no poseen una (X), una vez que se ha terminado de hacer la selección de los programas que se van a instalar completos en el disco duro local, se debe de dar clic en el botón “next”.

Inmediatamente pasaremos a otra ventana. En esta ventana se hace una recopilación y pre confirmación de lo que se desea instalar y con qué características se desea instalar, es importante verificar que esta ventana cumpla con las especificaciones, solo se debe instalar Word, Excel, Power Point y Outlook. Si se ha validado que se van a instalar los cuatro programas y que se van a correr desde el equipo local se debe de dar clic sobre el botón "install" esto iniciara el proceso de instalación de office, una vez finalizado el proceso de instalación, solo resta dar clic en el botón "finish", a continuación se muestra la figura de la penúltima pantalla final de la instalación de office.

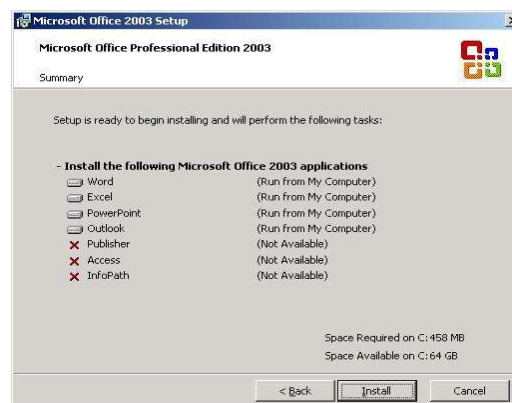


Figura 4.4.4 Penúltima pantalla instalación de office

Cambio de idioma del sistema

A continuación, es necesario cambiar el lenguaje del sistema operativo, para ello se debe de ir al panel de control y abrir las opciones de "regional and language", aparecerá una ventana en la que debemos seleccionar "spanish (México)" y "México" en los espacios correspondientes; "spanish (México)" en donde está la opción "select an ítem to match its..." y en "México" en donde dice "to help services provide you...".

Una vez realizados estos cambios de debe dar “apply” que se encuentra en la esquina inferior derecha de la ventana. Después es necesario ir a la segunda pestaña de la ventana esta segunda pestaña es “languages” que se encuentra en la parte superior de la ventana en esta ventana solo es necesario hacer el cambio del lenguaje de los menús al español, para esto solo se debe seleccionar la opción “español” en la parte de “languages used in menus and dialogs”, una vez hechos los cambios pertinentes se deben dar clic en el botón “apply” y luego “ok” , aplicados los cambios el equipo pedirá reinicio del sistema confirmarlo, una vez terminado el reinicio ingresar a la sesión y verificar que los menús estén en español con esto finalizamos este cambio, a continuación se presenta la figura 4.4.5 de la configuración de idioma.

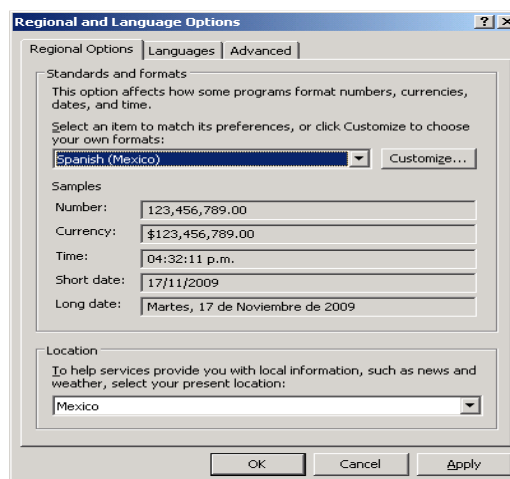


Figura 4.4.5 Configuración de idioma

Instalación de intelisis

Ahora es necesario instalar los aplicativos que harán funcionar de manera correcta Intelisis, para ello es necesario acceder a la siguiente ruta \\192.168.10.215\ParchesWin\BDadmin\Instalación BDE 5.0.

Donde aparecerá una pantalla, aquí se debe de poner un usuario y una contraseña válidos para el dominio CDV, es necesario tomar en cuenta que antes del usuario se debe de escribir el nombre del dominio "CDV", seguido por una diagonal invertida (ALT + 92). Si los datos introducidos son válidos, aparecerá otra pantalla.

Instalación del BAdmin

En esta ventana se instalara el "BAdmin" para ello se debe de ubicar el archivo ejecutable "setup" y ejecutarlo dando doble clic sobre este icono, aparecerá una pantalla, en esta se solicita permisos para instalar el programa, así es que solo es necesario dar clic sobre el botón "run", lo cual llevara una ventana solo hay que dar clic en el botón "next", mostrara otra ventana hay que seleccionar la opción "i accept the terms..." y dar clic en el botón "next" para avanzar a la siguiente ventana, donde es necesario escribir los datos de la compañía de la siguiente manera; username: "Viana", organization: "Viana Descuentos S. A. de C. V." También es necesario seleccionar la opción "anyone who uses this computer". Ya que se han hecho estos cambios hay que dar clic en el botón "next" para que aparezca la siguiente ventana, aquí solo informa que el programa está a punto de ser instalado, así es que solo hay que dar clic en el botón "install". Una vez que termine de instalar la aplicación, solo será necesario dar clic sobre el botón "finish" para salir del asistente de instalación.

Instalación del cliente SQL

Se debe de acceder a la siguiente ruta:

\\192.168.10.215\ParchesWin\BAdmin\BDEadmin4\Disk1, aparecerá una ventana en la cual se colocan los datos de usuario y contraseñas válidas del dominio, si los datos son válidos llevara a otra ventana, se deberá de ubicar el archivo ejecutable "setup.exe" y se deberá dar doble clic sobre el icono para ejecutarlo

Aparecerá una ventana con un aviso para solicitar autorización para iniciar la instalación del software, se debe de dar clic en el botón “run” para iniciar el asistente de instalación, en la siguiente ventana se inicia el asistente para la instalación del software. Solo es necesario dar clic en el botón “next”, para avanzar hacia la siguiente ventana. En esta es necesario escribir los datos de la compañía de la siguiente manera; name: Viana, company: Viana Descuentos S. A. de C. V.

Ya que se han hecho estos cambios hay que dar clic en el botón “next” para que aparezca la siguiente ventana, en esta ventana indica donde se va a instalar el software, se deja la opción que esta predeterminada y se da clic sobre el botón “next”, aparecerá otra ventana donde se indica que nombre se va a poner a la carpeta que contenga los archivos, se debe de dejar la opción que esta predeterminada, se da clic en el botón “next”, lleva a otra ventana, en esta se indica la confirmación de las anteriores, indica el lugar donde se van a instalar los archivos, el nombre de la carpeta y el nombre del usuario del software. Solo se debe dar clic en el botón “next”.

Una vez que se finalizó el proceso de instalación aparecerá una ventana, es necesario seleccionar la opción “yes, launch the program file” y dar clic en el botón “finish”.

Instalación de librerías intelisis

Terminado el proceso anterior, se debe de copiar un archivo en la carpeta del sistema, para ello se debe de ir a la siguiente ruta:

\\192.168.10.215\ParchesWin\BDadmin\BDEadmin4, pedirá autenticarnos en el dominio con un usuario y contraseña válida, una vez introducidos los datos correctos, se debe de seleccionar y copiar el archivo llamado “ntwdblib.dll”.

Después se debe de ir a la siguiente ruta C:\Windows\system y C:\Windows\system32, se debe pegar el archivo “ntwdblib.dll” en estas carpetas, se vuelve a esa misma ruta y se debe volver a seleccionar y copiar los archivos llamados “ntwdblib.dll”, “diCrPKI.dll”, “instalación cfd Windows”, “intelisisCFD.dll” después se debe de ir a la siguiente ruta C:\Windows\system32 y pegar los archivos, posteriormente buscar el archivo “instalación cfd Windows” en la ruta anterior y ejecutarlo como administrador con esto se concluye, a continuación se muestra la figura 4.4.6 de la colocación la librería “ntwdblib.dll” en una de las rutas.

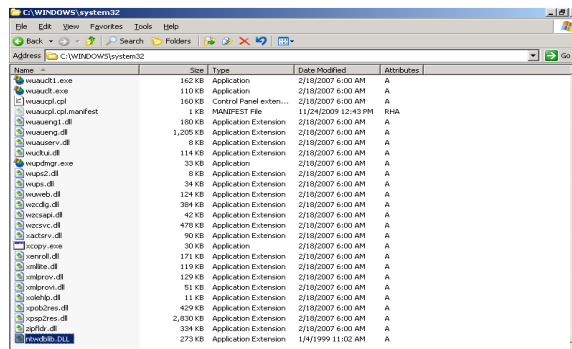


Figura 4.4.6 Librerías de Intelisis

Instalación de carpetas de intelisis

Ahora es necesario copiar las carpetas de las bases de datos que están en producción, para poder iniciar el trabajo de en intelisis con los movimientos actualizados. Estas carpetas deben de ser copiadas de la dirección \\192.168.10.252\D\$, aparecerá una ventana, donde se debe escribir un usuario y una contraseña de dominio válido.

Si los datos son correctos lleva a una ventana, de aquí se deben de copiar las carpetas “intelisis” e “intelisisR2” a la unidad D: local del servidor, una vez que se han copiado las dos carpetas es necesario compartirlas y aplicarles permisos especiales para el usuario de administración de intelisis.

Para hacer esto, se debe de hacer lo siguiente dar clic con el botón derecho del mouse sobre la primera carpeta “intelisis” y se debe de seleccionar la última opción “propiedades”, aparecerá una ventana, aquí es necesario entrar a la segunda pestaña “compartir” y se debe de seleccionar la opción “compartir esta carpeta”, posteriormente se debe de entrar a la ventana de “permisos”, para ello se debe de dar clic en el botón permisos que se encuentra en la parte central de la ventana, ubicar el botón agregar, que se encuentra en el centro de la ventana.

Con esto aparecerá esta ventana, aquí se debe de escribir el nombre de cuenta “actualización intelisis (aintelisis@CDV. México)” y se debe de dar clic en el botón “aceptar”, pedirá proporcionar un usuario y una contraseña válida del dominio una vez introducida, pasara a otra ventana se debe de dar todos los permisos, esto se hace palomeando todas las casillas de la parte inferior de la ventana. Finalmente, se deben de quitar los permisos generales de la cuenta “todos” quitando las palomas de la opción “control total”, “cambiar”, solo se debe de quedar activa la opción “leer”, ahora solo es cuestión de cerrar la ventana dando clic en el botón “aceptar”, ahora hay que entra a la pestaña “seguridad”, en esta pestaña se debe de entrar a la opción “agregar”, dando clic en el botón “agregar” que se encuentra en la parte superior de la ventana, aquí se debe de escribir el nombre de cuenta “actualización intelisis (aintelisis@CDV. México)” y se debe de dar clic en el botón “aceptar”, se abrirá una ventana donde se debe de poner un usuario y contraseña válida del dominio, si los datos son correctos llevara a otra ventana y aparecerá el usuario en la ventana de nombres de grupos o usuarios.

Se deben de dar todos los permisos, esto se hace palomeando todas las casillas de la parte inferior de la ventana, se deben de habilitar todas las opciones de permisos que están en la parte inferior de la ventana. Ahora solo es cuestión de cerrar la ventana dando clic en el botón “aceptar”. Se debe de repetir todo el proceso de otorgamiento de permisos al administrador de intelisis con la otra carpeta que fue copiada “intelisisR2”.

Unión a dominio

Unir a dominio el servidor, una vez que ya se tienen los software y el antivirus instalado, se puede unir a dominio el servidor, para ello es necesario acceder a las propiedades de “Mi PC” dando clic con el botón derecho sobre el icono de “Mi PC”, iremos a la siguiente ventana en esta se debe de pasar a la segunda pestaña, dando clic en donde dice “nombre de equipo (computer name)” y a continuación se debe dar clic en el botón “cambiar (change)” aparecerá una ventana, aquí se debe de poner el nombre completo del dominio en el campo donde dice “nombre de dominio (domain)”, el nombre completo del dominio es CDV.

México cuando el nombre del dominio este puesto, se debe de presionar el botón aceptar, lo cual llevara a la ventana de autenticación de credenciales, se coloca un usuario y contraseña válida del dominio, una vez introducidos los datos se da la bienvenida al dominio CDV solo es necesario dar clic en el botón aceptar y hacer lo mismo con todas las ventanas que estaban atrás, una vez que se ha dado aceptar a la última ventana, se indica que se va a reiniciar el equipo para que las nuevas funciones del dominio puedan ser validadas. Se debe de dar clic en el botón aceptar, posteriormente se indica que el equipo se va a reiniciar, para ello es necesario aceptar este procedimiento dando clic en el botón “si (yes)”.

Esto provocara que el servidor se reinicie automáticamente. Una vez que el equipo se ha reiniciado y está en dominio, se debe de ingresar con una cuenta que pertenezca al dominio CDV, y que tenga privilegios para administrar funciones del equipo.

Instalación de terminal server

El siguiente paso es instalar el servidor de terminal server, para ello será necesario entrar al panel de control e ir a la opción que dice “agregar o quitar componentes de Windows”, aparecerá otra ventana, en esta se debe de ubicar la opción “terminal server” y activar la opción palomeado con el mouse la casilla que se encuentra del lado izquierdo de la opción, una vez que se ha hecho esto se debe de dar clic sobre el botón “siguiente” lo que llevará a una ventana, aquí se muestra el contrato de licencia para este paquete de terminal services, solo es necesario dar clic en el botón “siguiente”. En esta ventana muestra el nivel de seguridad para la compatibilidad de la aplicación con otros programas y usuarios, se debe de seleccionar la opción “seguridad media” y se debe dar clic en el botón “siguiente”, a continuación muestro la figura 4.4.7 para configurar el servicio de terminal server.

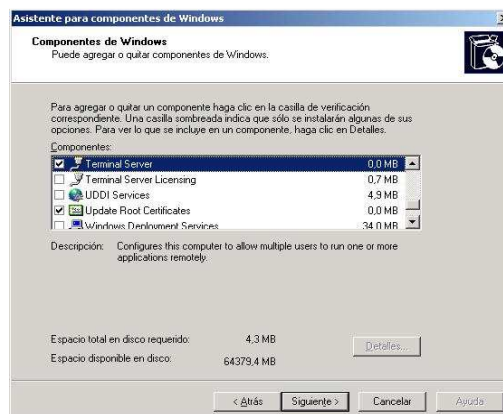


Figura 4.4.7 Configuración de terminal server

Esta es la ventana donde valida el nombre del servidor de terminal server al que se va a conectar para obtener las licencias, se debe de escribir "mxsrvdc01,dc001" todo junto y sin espacios, debe de tomarse en cuenta que la coma que va en medio es indispensable que se escriba correctamente, una vez que se validó que este bien escrito el nombre de los servidores, se debe de dar clic en el botón "siguiente" para avanzar a la siguiente ventana, aquí se debe de indicar el modo en el que se van a administrar las licencias que se tomen del servidor, se debe de especificar la opción "modo de licencia por dispositivo" y se debe de dar clic en el botón "siguiente". Una vez que se ha terminado de instalar todos los servicios de terminal server, se debe de dar clic en el botón "finalizar" para ir a la siguiente ventana, en esta ventana se indica que el servidor se debe de reiniciar para que la configuración tenga efecto, se debe de dar clic en el botón "sí" el servidor se reiniciara automáticamente.

Una vez que se ha reiniciado el servidor se debe de configurar los permisos y parámetros de las conexiones de terminal server. Para ello en el menú de herramientas administrativas se encuentra la opción "configuración de servicios del terminal server", en esta ventana se debe de abrir el contenido de la carpeta "conexiones" y en el icono que aparece del lado derecho de la pantalla se debe de dar clic con el botón derecho del mouse, y se debe de seleccionar la opción "propiedades".

Aparecerá la siguiente ventana, en esta se debe de ubicar la pestaña "sesiones". Aquí se tiene que seleccionar la opción "reemplazar la configuración del usuario", Se debe seleccionar en la opción "finalizar una sesión desconectada:" 5 minutos. Limite de sesión activa se debe seleccionar "nunca", limite de sesión inactiva se debe seleccionar 30 minutos. Posteriormente se debe activar la otra casilla denominada "reemplazar la configuración del usuario" y debe de estar seleccionada la opción "terminar la sesión".

Una vez que esto está validado, se debe de ubicar la pestaña “permisos”, mostrara una ventana donde se tiene que de dar clic en el botón agregar, y se deben de agregar dos usuarios con sus respectivos permisos.

Se debe de agregar el usuario “terminal migración” y “terminal migración 2” se debe de dar “aceptar”. Los permisos que se deben de asignar a los nuevos usuarios agregados son “acceso de usuario” y “acceso de invitado”, una vez que se ha hecho esto, se debe de ubicar la pestaña “control remoto”.

Se debe de activar la opción “usar control remoto con la siguiente configuración”, y se debe de quitar la opción “requerir el permiso del usuario” y finalmente se debe seleccionar la opción “interactuar con la sesión”.

Confirmados los cambios que se acaban de describir, se debe de dar clic en el botón “aceptar” y se debe cerrar la ventana principal, a continuación se presenta la figura 4.4.8 de algunas ventanas de configuración de conexión de terminal server.

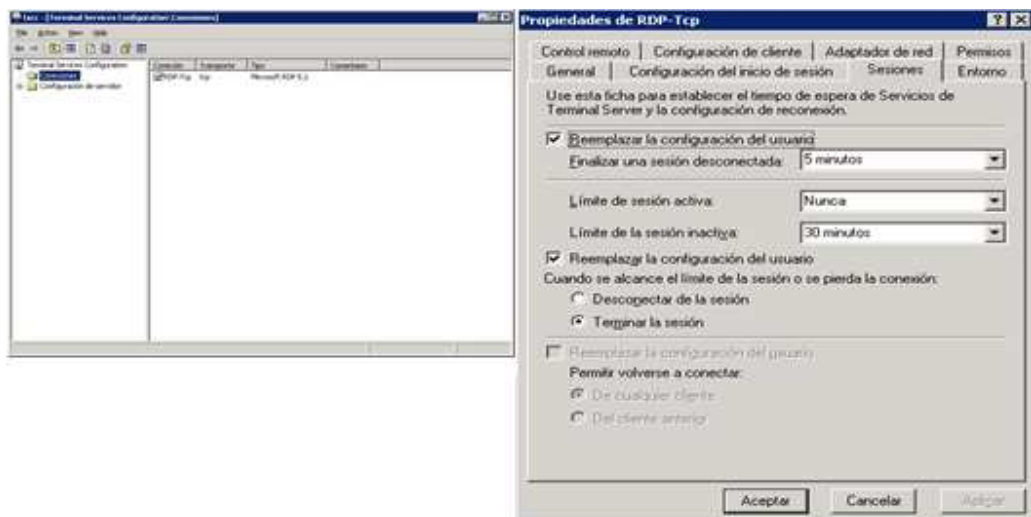


Figura 4.4.8 Conexión de terminal server

Instalación de conectividad de SQL

Una parte sumamente importante para la instalación de un servidor es la conectividad de los servicios de SQL, para instalar este paquete de conectividad se debe de tener el CD de instalación de SQL2000, ya que este es el que manejan las bases de datos para trabajar en intelisis, una vez que se ha insertado el disco de instalación de SQL 2000 aparecerá una ventana, aquí se debe dar clic en el botón “componentes de SQL server 2000” y lleva a otra ventana será necesario dar clic en el botón “instalar servidor de bases de datos”.

En esta ventana muestra un mensaje que indica que la versión de sistema operativo no es la más adecuada para este software, pero este es un mensaje de advertencia y puede ser ignorado, se debe dar clic en el botón “continue”. En la siguiente ventana indica que el software va a ser instalado, solo debe darse clic en el botón “siguiente”. En la ventana que aparecerá, se solicita indicar el lugar de la instalación, por lo que es necesario seleccionar la opción “equipo local” y a continuación dar clic en el botón “siguiente”, en la ventana siguiente se indica las opciones de instalación, es necesario seleccionar la primera opción, “crear una nueva instalación...”. En esta ventana es necesario escribir los datos de la compañía de la siguiente manera; usuario: Viana, compañía: Viana Descuentos S. A. de C. V.

Ya que se han hecho estos cambios hay que dar clic en el botón “siguiente” para que aparezca la siguiente ventana, esta ventana muestra el contrato de licencia para el uso del software. Solo es necesario dar clic en el botón “sí”, lleva a la siguiente ventana, esta es la parte vital de este procedimiento, es aquí en donde se indica que componentes de SQL server se desean instalar, aquí es muy importante seleccionar la opción solo conectividad, ya que está hecho esto, se debe dar clic en el botón “siguiente”.

Aparecerá una ventana donde se indica que se está a punto de iniciar el proceso de instalación del software de conectividad de SQL server. Se debe de dar clic en el botón “siguiente”. Muestra la siguiente ventana, aquí se indica que se ha concluido la instalación satisfactoriamente, solo es cuestión de dar clic en “finalizar” para salir del asistente de instalación.

Crear sesiones de usuario

Para que cada usuario pueda iniciar sesión de forma normal es necesario iniciar sesión con cada uno de los usuarios que van a trabajar en este servidor, para ello se debe de tener una lista de los usuarios y las estaciones de servicio que van a iniciar sesión en el servidor, tomando como regla general lo siguiente.

El nombre de usuario y el número, (usuario01), las contraseñas son las siguientes para los usuarios (usuario01) la contraseña es el nombre de la tienda en minúsculas y sin espacios, para los usuarios de crédito como (usuariocredito01) la contraseña es crédito.

Usuarios del DF

Una vez que se ha iniciado sesión, se debe de abrir el explorador de Windows dentro de esta sesión de escritorio remoto, se debe de ubicar la unidad D: y la carpeta intelisis, tomando en cuenta la siguiente regla. Para los usuarios de las tiendas del DF se debe de instalar el que está en la primera carpeta “intelisis”, se debe de abrir la carpeta y se debe de ejecutar el archivo llamado “intelisis.exe”.

Una vez que se da doble clic en el archivo para ejecutarlo, aparecerá una ventana en esta se debe de poner un número de estación de trabajo, asignado por el administrador de red, la carpeta temporal debe de estar ubicada en la carpeta D: y se debe de borrar la subcarpeta intelisis y se debe de sustituir por el nombre de usuario que se usó para iniciar sesión, finalmente, se debe de usar el sistema operativo Windows 2000 en la parte inferior de la ventana.

Una vez que se validaron los datos de esta ventana, se debe de dar clic en el botón “aceptar” que está en la parte inferior de la ventana del lado izquierdo.

Una vez que aparece esta ventana, se puede iniciar sesión en intelisis, a continuación se presenta la figura 4.4.9 de configuración de intelisis.

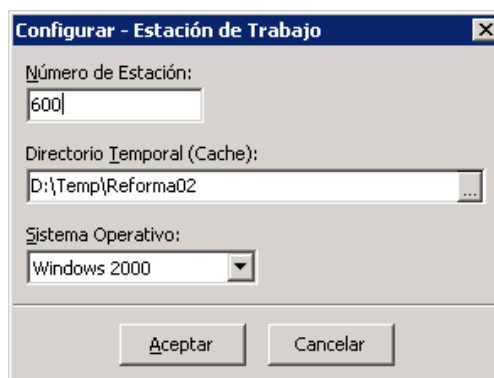


Figura 4.4.9 Configuración estación de trabajo intelisis

Usuarios foráneos

Para el caso de los usuarios de tiendas que no se encuentran en el DF, es decir, foráneos, se debe de instalar la versión R2 de intelisis, que se encuentra en la unidad D: del disco duro local. En esta carpeta al igual que en la de los usuarios locales, se debe de localizar el archivo ejecutable “intelisis.exe” y continuar con el mismo proceso exactamente igual que si fuera un usuario de tienda del DF.

Instalación de impresora

Es necesario instalar las impresoras de las tiendas, cada impresora debe de darse de alta por separado, y se le deben de dar permisos solamente al grupo de la tienda que la va a ocupar.

Para ello es necesario entrara al menú de impresoras y faxes que se encuentra en la carpeta de panel de control, cabe hacer mención que para poder hacer este procedimiento se debe de tener un usuario y una contraseña de administrador en el dominio CDV. También es necesario tener a la mano el nombre exacto de la impresora, la IP de la impresora y el driver correcto para el modelo de la impresora. Al dar clic en agregar impresora, se abre una ventana de bienvenida, solo es necesario dar clic en el botón “siguiente”.

En la siguiente ventana se debe de seleccionar la opción “impresora local” y se debe deshabilitar la opción “detectar e instalar la impresora”. Una vez validado esto, se da clic en el botón “siguiente”.

Nos lleva a otra ventana, esta es para la configuración del puerto de conexión a la impresora en esta ventana es necesario seleccionar la opción “crear nuevo puerto” y seleccionar de la lista la opción “standard TCP/IP port”.

Cuando están validados los datos, se debe dar clic en el botón “siguiente”, muestra una ventana donde se hace un recuento de las configuraciones del puerto que se va a agregar, y se solicita la confirmación del usuario para crear el puerto de conexión con la impresora, se debe dar clic en el botón “siguiente”, pasara a otra ventana, aquí se solicita la dirección IP de la impresora, se debe de colocar una dirección IP válida para la impresora y el segmento de la tienda que va a hacer uso de la impresora.

El nombre que la computadora le asigna al puerto que se va a crear es automático y así se debe de quedar, si los datos están correctos se debe dar clic en el botón “siguiente”, lleva a la siguiente ventana, se debe indicar el tipo de adaptador que se va a usar para conectar la impresora a la red, como predeterminado se encuentra la opción “generic network card”, de la opción estándar, así debe de quedarse, solo se debe de dar clic en el botón “siguiente”, en la siguiente ventana se mostrara la lista de todas las características que tendrá configurado el puerto, tales como dirección IP, nombre del puerto, adaptador, etc. En esta ventana se debe dar clic en el botón finalizar.

Aparecerá una ventana se debe de seleccionar el controlador adecuado para la impresora y se debe dar clic en el botón “siguiente”. Si es necesario se debe de buscar el driver de la impresora en el disco de instalación de la impresora.

En esta ventana se debe de escribir el nombre de la impresora, es muy importante este nombre, ya que las terminales están configuradas para apuntar directamente a la impresora en las diferentes aéreas de la empresa, por lo que es necesario dar especial cuidado a la escritura de este nombre. También se debe de seleccionar la opción de no ser la impresora determinada, ya que como está alojada en un servidor, los servidores no deben de tener impresoras predeterminadas.

Una vez hecho esto, se debe dar clic en el botón “siguiente”, mostrara la siguiente ventana donde se debe de seleccionar la opción de “no compartir la impresora”, y se debe dar clic en el botón “siguiente”, la siguiente ventana se solicita imprimir una página de prueba, no es necesaria esta prueba y podría afectar al usuario, por lo que se debe seleccionar la opción “no” y se debe dar clic en el botón “siguiente”, aparecerá una ventana aquí se muestra la recapitulación de toda la instalación, por lo que solo se debe dar clic en el botón “finalizar”.

Políticas de permisos de las impresoras

Ahora es necesario dar permisos a las tiendas y quitar el permiso a todos los demás usuarios. Para ello es necesario entrar en el menú de propiedades de la impresora, dando clic con el botón derecho del mouse sobre el icono de la impresora que se ha instalado, aparecerá una ventana en esta se debe de ubicar el usuario “todos” y debe de ser eliminado de la lista de usuarios permitidos.

Para ello una vez que se ha seleccionado el usuario, se debe dar clic en el botón “quitar”, que se encuentra en la parte central de la ventana, el usuario seleccionado se borrara de la lista, a continuación se debe de dar clic en el botón “agregar”, lleva a otra ventana, aquí se debe de escribir el nombre de la tienda que está autorizada a imprimir en esta impresora.

La nomenclatura para el grupo de cada tienda debe de ser “nombre del grupo seguido del nombre de la tienda, con espacios”. Una vez que se ha escrito el nombre del grupo autorizado para la impresora, se debe dar clic en el botón aceptar, aparecerá una pantalla, ya con el nuevo usuario agregado, se debe de ubicar el nuevo usuario o grupo agregado, y se debe de verificar que únicamente tenga habilitado el permiso de impresión en la parte inferior de la ventana.

Cuando se ha verificado esto, se debe de dar clic en el botón aceptar y se cerrara la ventana, a continuación se presenta la figura 4.4.10 de cómo deben quedar los permisos de la impresora.

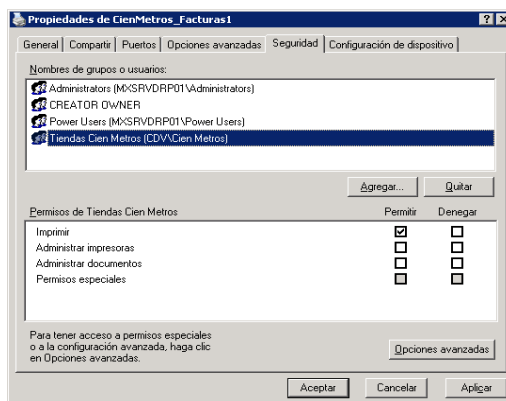


Figura 4.4.10 Permisos de impresora

Políticas de iconos de inicio de sesión

Los servidores tienen rutas predeterminadas para las diferentes estaciones de trabajo, por regla general, las estaciones número cinco, tienen configurado el correo de contacto de la tienda, por lo cual, una vez que se han copiado los iconos de acceso a cada carpeta de usuario se debe reingresar a esta cuenta desde una conexión de escritorio remoto, y se debe de configurar el correo de la tienda.

En esta parte de la instalación también deben de colocarse los iconos de la carpeta de inicio de los usuarios con terminal 05 y los que tienen terminal crédito, estos pueden ser jalados de las carpetas del servidor que está en producción, los más comunes son iconos de intelisis, Word, Excel, PowerPoint y Outlook.

El departamento de desarrollo, tiene la responsabilidad de crear los archivos *.ini que indican la dirección de la base de datos hacia donde apuntan las estaciones de intelisis, a continuación se presenta la figura 4.4.11 de los accesos que lleva una terminal de correo.

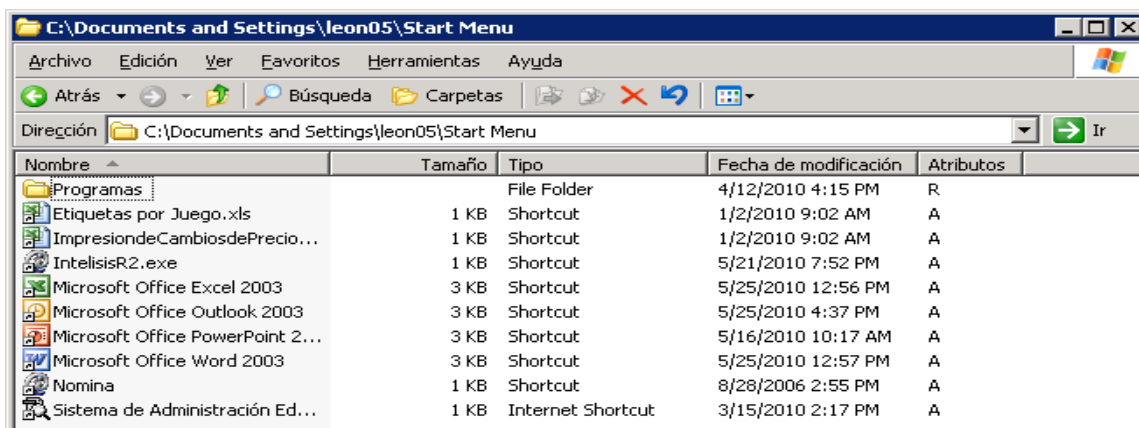


Figura 4.4.11 Accesos de terminal de correo

Instalación de aplicaciones Acrobat y Flash Player

En este paso se deben de instalar las aplicaciones de Flash Player y Adobe Acrobat, para ello es necesario primero desbloqueará el servicio de navegación segura. Esto se hace entrando al panel de control y a la opción agregar o quitar programas y se debe de dar clic en el botón “agregar o quitar componentes de Windows”, aparecerá una siguiente ventana, en esta se debe de ubicar la opción “Internet Explorer enchanced...” y quitar la marca de selección que tiene en el cuadro que está del lado izquierdo de la opción. Después se debe de dar clic en el botón “next”, pasara a otra ventana donde se muestra que se han quitado los servicios de Internet seguro de forma satisfactoria y se debe de dar clic en el botón “finish”.

Ahora será necesario indicarle al navegador de Internet cual es la IP de salida a Internet, para ello se debe de ir a las propiedades del explorador de Internet abriendo el explorador y entrando al menú “herramientas” y al submenú “herramientas de internet”. Aparecerá otra ventana en esta ventana se debe de acceder a la pestaña “conexiones” dando clic en el título de “conexiones”, de los títulos que se encuentran en la parte superior de la ventana.

Después se debe ubicar la opción “configuración LAN” y dar clic en esta opción, se abrirá una ventana, se deben de activar las opciones “usar un servidor proxy...” y “no usar servidor proxy para direcciones locales” y en la dirección del servidor proxy se debe de indicar la 19.168.10.144, y en los puestos de comunicación se debe de escribir el 8080.

Una vez hecho esto, se debe de dar clic en el botón aceptar, de igual manera se debe dar clic en el botón aceptar de la otra ventana que está abierta, con esto ya se estableció la puerta de salida y el puerto se conexión a Internet no será necesario reiniciar el navegador.

Instalación de Adobe Flash Player

Para comenzar la instalación de Adobe Flash Player, solo se debe de ir a la siguiente dirección, <http://get.adobe.com/es/flashplayer/?promoid=DAFYL>, aparecerá la ventana donde se debe de quitar la opción “barra google gratuita” y después se debe de dar clic en el botón “aceptar e instalar ahora” con esto aparecerá otra ventana, donde una vez que se ha terminado de descargar e instalar la aplicación será necesario dar clic en el botón “cerrar download manager”.

Instalación de Adobe Acrobat Reader

Una vez que está instalado el controlador de Flash Player se debe de instalar Adobe Acrobat, para ello se debe de entrar a la siguiente dirección, <http://get.adobe.com/es/reader>, y aparecerá una ventana esta una advertencia de que se ha detectado una ventana que se desea abrir, solo se debe dar clic en el botón “aceptar” y aparecerá una ventana, en esta se solicita que se instale el control ActiveX²⁸.

Para la instalación de Adobe, para instalarlo se debe de dar clic en la barra de color amarillo que aparece debajo de la barra de direcciones web, se debe de seleccionar la primera opción, “instalar control ActiveX...”, mostrara otra ventana esta es una advertencia de que se va a instalar un control en el explorador, para ello es necesario dar clic en el botón “instalar”, pasaremos a la siguiente ventana, aquí se debe de quitar la selección de la opción “barra de google gratuita”, y se debe de dar clic en el botón “descargar”, una vez que se ha instalado el software de Adobe, se debe de cerrar esta ventana.

Instalación y configuración de CtrlApiCommSetup

En el servidor a instalar y configurar, se deberá crear a nivel raíz la siguiente carpeta C:\archivos de programas, el siguiente paso es copiar y pegar la carpeta que se encuentra localizada en \\server02cont\c\$ al servidor que operara con subtech, estas carpetas contienen los archivos ejecutables para instalar el CtrlApiCommSetup y stunnel.

²⁸ActiveX: Es un pequeño programa, denominado complementos, que se usan en Internet, permiten animaciones o pueden ayudar con tareas de actualización de seguridad de Microsoft.

Una vez copiada la carpeta al servidor entramos a la ruta C:\inter-red\CtrlApiCommSetup y procedemos a ejecutar el archivo de aplicación, da un clic a next para continuar con el proceso de instalación. Aparece una pantalla, a la cual le haremos unas modificaciones en los parámetros de instalación, se re direccionara a la ruta de instalación de C:\program files a la carpeta de C:\archivo de programas que creamos al principio y no tocamos los demás parámetros, tal y como se muestra en la segunda pantalla, por último activamos la casilla de everyone, da un clic a next, con esta parte terminamos el proceso de instalación.

Ahora solo resta hacer algunos ajustes a nuestra instalación, el siguiente paso es entrar al servidor \\server02conti\c\$\archivos de programa\intelisis\CtrlApiCommSetup, seleccionar todos los archivos, copiarlos al servidor donde se lleva a cabo la instalación.

Esta copia se realiza con el fin de modificar el archivo de gpay.wsdl, el cual ya contiene los parámetros modificados para poder llevar a cabo la comunicación. Ahora procederemos a instalar y configurar el stunnel para poder realizar esto requerimos entrar nuevamente a la ruta C:\inter-red\stunnel-4.15 installer.exe y proceder a ejecutar el archivo de aplicación, seguimos el proceso de instalación dando clic, en la pantalla siguiente haremos unas modificaciones en los parámetros de instalación, se re direccionara a la ruta de instalación de C:\program files a la carpeta de C:\archivo de programas que creamos al principio y proseguimos con la instalación.

Aquí repetiremos el mismo proceso que con la instalación anterior, entras al servidor \\server02conti\c\$\archivos de programa\intelisis\stunnel, seleccionar todos los archivos, los copias, después pegar los archivos en la ruta C:\archivos de programa\stunnel del servidor que estás instalando, esta copia se realiza con el fin de modificar el archivo de stunnel.conf, el cual ya contiene los parámetros necesarios para poder llevar a cabo la comunicación.

Para concretar esta instalación, solo nos resta hacer estos últimos pasos.

1. Instalar servicios
2. Levantar servicios
3. Correr servicios.

Con esto hemos concluido la instalación de la Inter-red. Y concluye el procedimiento de preparación de un servidor para tienda.

Terminado el procedimiento de instalación de un servidor, se debe llevar al site donde se encuentran los servidores de producción, los fines de semana se realiza un checklist, con el fin de monitorear los servidores, verificando el espacio en disco, memoria utilizada por el procesador, arreglos de disco, log del sistema, log de aplicación y actualización de antivirus, también se considera programar calendario de mantenimiento preventivo y correctivo a los servidores.

4.5 Administración de Active Directory

“Active directory es el término que usa Microsoft para referirse a su implementación de servicio de directorio activo en una red distribuida de computadoras”²⁹, este servicio es establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, administración de políticas en toda la red.

Su estructura jerárquica permite mantener una serie de objetos relacionados con los componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de accesos.

²⁹ Wikipedia, Mayo 16 2015, Acive Directory, <https://es.wikipedia.org/wiki/Active_Directory>

Active directory permite a los administradores establecer políticas a nivel empresa, desplegar programas en muchas computadoras y aplicar actualizaciones críticas a una organización entera. Active directory almacena información de una organización en una base de dato central, organizado y accesible, se pueden encontrar desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos. El directorio activo utiliza distintos protocolos principalmente (LDAP³⁰, DNS, DHCP³¹ y Kerberos³²).

Active Directory permite que las aplicaciones encuentren, utilicen y administren recursos de directorio en un ambiente de cómputo distribuido. Al crear una arquitectura active directory, debe considerar cuidadosamente los límites de seguridad del ambiente, planear adecuadamente la delegación y el programa de implementación de seguridad de una organización resultará en un diseño de active directory mucho más seguro para la organización. Active directory está basado en una serie de estándares llamados X.500. Dominios y subdominios se identifican utilizando la misma notación de las zonas DNS razón por la cual active directory requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red.

³⁰LDAP: LightweightDirectoryAccess Protocol, en español Protocolo Ligero/Simplificado de Acceso a Directorios.

³¹DHCP: Dynamic Host ConfigurationProtocol, en español protocolo de configuración dinámica de host, protocolo que permite a los clientes de una red obtener sus parámetros de configuración automáticamente.

³²Kerberos: Es un protocolo de autenticación de redes de computadoras, que permite a dos computadoras en una red insegura demostrar su identidad mutuamente de manera segura.

Los objetos del Active Directory se dividen en tres categorías:

- Recursos (impresoras, escáner, etc.)
- Servicios (correo, impresión, etc.)
- Usuarios, grupos, unidades organizacionales.

Enseguida proporcionaré el funcionamiento de algunos de los objetos del active directory.

Usuarios: Pertenecen al dominio Windows y pueden tener acceso a recursos compartidos en la red.

Grupos: Los grupos de usuarios que pueden ser usados para agrupar políticas de seguridad.

Computadoras: Son las computadoras que se unen al dominio Windows en las cuales se pueden hacer Deploy de políticas de seguridad.

Unidades organizacionales: Son contenedores de objetos dentro del active directory, aunque también las OU son llamadas objetos dentro del active directory.

Impresoras: Son recursos que pueden ser compartidos en la red para que todos tengan acceso o no a ellas.

Para asegurarse de que puede crear un diseño eficiente y confiable de active directory, se necesita conocer tanto la estructura lógica como la física de la red. El conocimiento de la estructura empresarial de la organización también resulta importante. Active directory separa la estructura lógica del dominio de la estructura física real.

Estructura lógica

La estructura lógica de una red se compone de objetos, dominios, árboles y bosques. El bloque de construcción básico de active directory es el objeto, un conjunto de atributos diferenciado y con nombre que representa un recurso de la red. Los objetos se pueden organizar en clases, que son agrupaciones lógicas de objetos, los usuarios, grupos y equipos son clases de objeto diferentes.

“En el nivel más bajo, algunos objetos representan entidades individuales de la red, como un usuario o equipo. Estos objetos se denominan hoja y no pueden contener otros objetos”³³. Para facilitar la administración y simplificar la organización del directorio, se colocan objetos hoja dentro de otros objetos denominados objeto contenedor. Los objetos contenedores pueden contener otros contenedores de forma anidada, o jerárquica.

El objeto contenedor es una unidad organizativa (OU, organizational unit). Puede usar una unidad organizativa para organizar objetos de un dominio en algún tipo de agrupación lógica administrativa. La estructura y jerarquía de una unidad organizativa dentro de un dominio es independiente de la estructura de cualquier otro dominio.

Todos los objetos de la red, solo pueden existir dentro de un dominio. Los dominios se usan para agrupar objetos relacionados con el fin de reflejar la red de una organización. Cada dominio crea y almacena información acerca de los objetos que contiene.

³³ Microsoft, Junio 17 2015, Introducción a Active Directory, <<https://support.microsoft.com/es-mx/kb/196464/es>>

El límite admitido para el número de objetos que puede mantener en un dominio es de un millón. Cada dominio representa un límite de seguridad, el acceso a los objetos dentro de cada dominio se controla mediante entradas de control de acceso (ACE, access control entries) contenidas en listas de control de acceso (ACL, access control lists). Estas opciones de seguridad no cruzan los límites de los dominios. Dado que un dominio es una partición física de la base de datos de active directory, puede estructurarlos por la función empresarial como (recursos humanos, ventas, contabilidad o sistemas) o por la ubicación (geográfica o relativa).

Cuando se agrupan dominios relacionados para permitir el uso compartido de los recursos globales, se está creando un árbol. Aunque un árbol se puede componer de un único dominio, se pueden combinar varios dentro del mismo espacio de nombres en una estructura jerárquica. Los dominios del árbol se conectan de forma transparente a través de relaciones de confianza de dos sentidos con seguridad basada en kerberos. Esta relación de confianza es permanente, no se puede eliminar y transitiva. En otras palabras, si el dominio A confía en un bosque confía en el dominio B en un bosque y el dominio B en un bosque confía en el dominio C en un bosque, entonces el dominio A en un bosque confía en el dominio C en un bosque, a continuación se presenta la figura 4.5.1 de representación.



Figura 4.5.1 Relación de confianza entre bosques de dominio

Dentro de un árbol determinado, todos los dominios comparten el catálogo global, que es un repositorio central para los objetos del árbol. Cada árbol también se representa por un espacio de nombres contiguo. Si el dominio raíz de una compañía es "patito.com" y crea dominios diferentes para las divisiones de ventas y sistemas, los nombres de dominio serían "ventas.patito.com" y "sistemas.patito.com". Estos dominios se les denominan secundarios.

En el nivel más alto, se pueden agruparse árboles dispares para formar un bosque. Un bosque permite combinar divisiones diferentes en una organización o, pueden agruparse organizaciones distintas, estas no tienen que compartir el mismo esquema de denominación, pueden operar de forma independiente y seguir comunicándose entre sí. Todos los árboles de un bosque comparten el mismo esquema, catálogo global y contenedor de configuración. La seguridad basada en kerberos proporciona las relaciones de confianza entre los árboles.

Para convertir un servidor miembro en un controlador de dominio, basta con que ejecute la herramienta DCPROMO con el fin de agregar el servidor active directory. Para quitar el servidor active directory, se ejecuta la herramienta DCPROMO nuevamente.

Estructura física

Los controladores de dominio y los sitios son los dos componentes básicos que tienen que ver con la estructura física de una configuración de red de área local. En las redes empresariales donde se abarcan varias ubicaciones geográficas, las implicaciones del diseño y la estructura de una red de área son importantes por el efecto que la replicación de la base de datos del directorio, un mal diseño puede afectar el rendimiento de la red y los controladores de dominio.

Espacios de nombres

Un espacio de nombres es un área designada que tiene límites específicos donde se resuelve un nombre lógico asignado a un equipo. Su principal uso es organizar las descripciones de los recursos para permitir a los usuarios localizarlos por sus características o propiedades. La base de datos del directorio para un espacio de nombres determinado se puede usar con el fin de localizar un objeto sin conocer su nombre.

El diseño del espacio de nombres determina, a la larga, el grado de utilidad que la base de datos representará para los usuarios a medida que crezca.

En active directory se almacenan dos tipos principales de información:

- La ubicación lógica del objeto.
- Una lista de atributos acerca del objeto.

Los objetos tienen atributos asignados, como un número de teléfono, ubicación de oficina, etc., y estos se pueden usar para localizar objetos en la base de datos del directorio. “Cuando se agregan objetos, clases de objetos o atributos de esos objetos a la base de datos del directorio, su estructura determina su utilidad para los usuarios del directorio”³⁴.

Cada contenedor y objeto de un árbol tiene un nombre único. Un espacio de nombres es una colección de la ruta completa de todos los contenedores, objetos, ramas y hojas del árbol. La ubicación de un objeto en un árbol determina el nombre completo.

³⁴ Microsoft, Junio 17 2015, Introducción a Active Directory, <<https://support.microsoft.com/es-mx/kb/196464/es>>

Un nombre completo (DN) se compone, de la ruta de acceso completa desde el principio de un espacio de nombres específico, a través de la jerarquía completa del árbol. Como los nombres diferenciados, son útiles para organizar la base de datos de un directorio, pero pueden no resultar de utilidad para recordar el objeto, en active directory también se usan nombres en referencia relativa (RDN). Un RDN es la parte del nombre de un objeto que es un atributo del propio objeto.

“La base para el espacio de nombres usado en muchas redes se fundamenta en el sistema de nombres de dominio (DNS, domain name system) usado en Internet. Esta conexión con DNS contribuye a determinar la forma del árbol de active directory y la relación de los objetos entre sí. Los controladores de dominio son los dominios que se enumeran como nombres completos, mientras que los nombres comunes (CN) son las rutas de acceso específicas de los objetos usuarios del directorio”³⁵.

Catálogo global

El catálogo global contiene una réplica parcial de cada dominio del directorio y es generado automáticamente por el sistema de replicación de active directory. Esto permite a los usuarios y aplicaciones buscar objetos en un árbol de dominios de active directory. El catálogo también contiene el esquema y la configuración de las particiones del directorio. Esto implica que el catálogo global contiene una copia de cada objeto de active directory, con solo una pequeña cantidad de sus atributos.

³⁵ Microsoft, Junio 17 2015, Introducción a Active Directory, <<https://support.microsoft.com/es-mx/kb/196464/es>>

Los atributos del catálogo global son los que se usan en las operaciones de búsqueda, como el nombre, los apellidos de los usuarios, los nombres de inicio de sesión y los requeridos para localizar una copia completa del objeto.

Con esta información común, los usuarios pueden encontrar objetos de interés rápidamente sin conocer qué dominio los contiene y sin requerir un espacio de nombres contiguo en la empresa. Si el objeto no se puede encontrar en el catálogo global, la búsqueda puede consultar la partición de su dominio local para buscar información.

Dado que el catálogo global, replica los cambios realizados, a todos los servidores de catálogo global, es aconsejable limitar la cantidad de atributos almacenados, en las particiones locales para no afectar al rendimiento, ni a las tareas de mantenimiento.

Integrar DNS con Active Directory

La integración de DNS y active directory, los dominios DNS y los dominios de active directory usan nombres idénticos para espacios de nombres diferentes. No son el mismo espacio de nombres incluso aunque los dos compartan una estructura de dominios idéntica. Cada uno almacena datos diferentes y administra objetos distintos. DNS usa zonas y registros de recursos mientras que active directory usa dominios y objetos de dominio.

“La integración entre active directory y DNS es efectuada por cada servidor active directory que publica su propia dirección en los registros de recursos de servicios en un host DNS”³⁶.

³⁶ Microsoft, Junio 17 2015, Introducción a Active Directory, <<https://support.microsoft.com/es-mx/kb/196464/es>>

Identificador único global

Como cada objeto de una red debe identificarse mediante una propiedad única, active directory lo consigue mediante la asociación de un identificador único global (GUID, global unique identifier) con cada objeto. Así se garantiza que este número es único y la base de datos del directorio no lo cambia nunca, ni siquiera si cambia el nombre lógico del objeto. El GUID se genera cuando un usuario o aplicación crea por primera vez el nombre completo (DN) en el directorio.

Replicación

Con active directory, todos los controladores de dominio replican dentro de un sitio de forma automática, admiten la replicación con múltiples maestros y replican información de active directory entre todos los controladores de dominio. La replicación con múltiples maestros significa que los administradores pueden hacer actualizaciones en active directory o en cualquier controlador de dominio.

“La replicación de bases de datos con múltiples maestros también contribuye a controlar las decisiones de cuándo se sincronizan cambios, cuya información es más actual, y cuándo detener la replicación de los datos para evitar su duplicación o redundancia. Para determinar qué información tiene que actualizarse, active directory usa números de secuencia de actualización (USN, update sequence numbers) de 64 bits. Estos números se crean y asocian con todas las propiedades. Cada vez que se modifica un objeto, se incrementa su USN y se almacena con la propiedad”³⁷.

³⁷ Microsoft, Junio 17 2015, Introducción a Active Directory, <<https://support.microsoft.com/es-mx/kb/196464/es>>

Cada servidor active directory, mantiene una tabla de los números de secuencia de actualizaciones más recientes, de todos los asociados de replicación de un sitio. Esta tabla se compone del, USN mayor para cada propiedad, cuando se alcanza el intervalo de replicación, cada servidor solicita solo los cambios, con un USN mayor que el que aparece en su propia tabla.

Se puede hacer cambios, a dos servidores active directory diferentes, para la misma propiedad, antes de replicar todos los cambios. Esto provoca una colisión de replicación, uno de los cambios debe declararse, como más preciso y se debe usar, como origen de todos los demás asociados de replicación. Para solucionar esto, active directory usa, el valor de un número de versión de propiedad (PVN, property version number) para todo el sitio. Este número se incrementa cuando, tiene lugar una escritura de origen.

Esta escritura es la que ocurre directamente en un servidor active directory en particular. Cuando dos o más valores de propiedad, con el mismo PVN se han cambiado en ubicaciones diferentes, el servidor active directory que recibe el cambio, comprueba las marcas de tiempo y usa la más reciente para la actualización. Este problema es porque no se tiene una adecuada configuración y mantenimiento de un reloj central en la red.

“Otro problema de la replicación, es la aparición de bucles. Active directory permite a los administradores, configurar varias rutas por motivos relacionados con la redundancia. Para impedir que los cambios, no terminen nunca de actualizarse, active directory crea listas de pares de USN, en cada servidor. Estas listas se denominan vectores de actualización (UDV, up-to-date vectors)”³⁸.

³⁸ Microsoft, Junio 17 2015, Introducción a Active Directory, <<https://support.microsoft.com/es-mx/kb/196464/es>>

Contienen el mayor USN de cada escritura de origen. Cada vector de actualización enumera el resto de los servidores dentro del propio sitio. Cuando se produce la replicación, el servidor solicitante envía su propio vector de actualización al servidor que realiza el envío. Para determinar si el cambio sigue teniendo que replicarse se usa el mayor USN para cada escritura de origen. Si el número USN es igual o mayor, no se requiere hacer ningún cambio porque el servidor solicitante ya está actualizado.

Cambios con grupos

Otro aspecto del proceso de planeamiento para active directory es el concepto de grupos, a continuación se mencionan:

- Grupos con ámbito local
- Grupos con ámbito local de dominio
- Grupos con ámbito global
- Grupos con ámbito universal

Los grupos globales ahora pueden contener otros grupos globales, aunque los grupos globales se siguen usando para recopilar usuarios, la capacidad de colocar un grupo dentro de otro permite a los administradores ubicarlos en cualquier lugar de un bosque, con la finalidad de facilitar el mantenimiento. No obstante, los grupos globales solo pueden contener usuarios y grupos de un dominio del bosque de active directory.

Debido a que muchas redes pueden contener una mezcla de servidores con distintas versiones de sistemas operativos Windows, antes de crear grupos debe determinar el número y el tipo de dominios de la red y cuáles de esos dominios son de modo mixto y cuáles de modo nativo:

- Dominio de modo mixto. Un dominio de modo mixto es un conjunto de equipos conectados en red en los que se ejecutan controladores de dominio tanto de Windows NT 4.0 como de Windows 2000.
- Dominio de modo nativo. Puede convertir un dominio al modo nativo cuando solo contiene controladores de dominio de Windows 2000 server y pueden considerarse también Windows 2003, las relaciones de confianza son automáticas y pueden administrar todo tipo de grupos.

El grupo universal puede contener todos los demás grupos y usuarios de cualquier árbol del bosque y se puede usar con cualquier lista de control de acceso (ACL) dentro del mismo.

Los grupos locales, de dominios locales y universales se pueden combinar para controlar el acceso a los recursos de la red. Su principal uso es la organización de usuarios en contenedores administrativos que representan sus dominios respectivos.

“Los grupos universales se usan para contener grupos globales de los diversos dominios para administrar además la jerarquía de dominios cuando se otorgan permisos. Los grupos globales se pueden agregar a grupos universales y, después, asignar permisos a los grupos de dominio local donde exista el recurso físicamente”³⁹.

Al estructurar los grupos de esta forma, los administradores pueden agregar o quitar usuarios de cada grupo global del dominio para controlar el acceso a los recursos en toda la empresa sin tener que hacer cambios en varias ubicaciones.

³⁹ Microsoft, Junio 17 2015, Introducción a Active Directory, <<https://support.microsoft.com/es-mx/kb/196464/es>>

Establecer los límites de directorio de Windows Server 2003

Existen diferentes tipos de límites dentro de active directory. Estos límites definirán el bosque, el dominio, la topología del sitio y la delegación de permisos. Para mantener un equilibrio adecuado entre la seguridad y la funcionalidad administrativa, puede subdividir aún más los límites de delegación de permisos en límites de seguridad y límites administrativos.

Límites de seguridad

Los límites de seguridad ayudan a definir la autonomía o el aislamiento de diferentes grupos dentro de una organización. Para lograr exitosamente este equilibrio, se debe ponderar las amenazas, contra las implicaciones de seguridad de delegar los permisos de administración y otras selecciones.

Límites de seguridad de bosque vs dominio

El bosque es el verdadero límite de seguridad. Se recomienda crear bosques separados para mantener su ambiente seguro libre de administradores sin escrúpulos en vez de crear dominios por separado para proporcionar seguridad y aislamiento de este tipo de administradores y otras amenazas potenciales.

Un dominio es el límite de administración de active directory. Con una organización de personas bien intencionadas, el límite de dominio proporcionará una administración autónoma de servicios y datos dentro de cada dominio de la organización.

Límites administrativos

Debido a la necesidad potencial de segmentar los servicios y datos, se debe definir los diferentes niveles de administración requeridos. Además de administradores que puedan realizar servicios únicos para la organización, se recomiendan los siguientes tipos de administradores.

Administradores de servicios: Los administradores de servicios de active directory son responsables de configurar y ofrecer el servicio de directorio.

A continuación se presentan algunos otros grupos de administradores de servicios de servicios active directory:

- Un grupo de administración de dominios principalmente responsable de los servicios de directorio.
- El administrador de bosques es responsable de seleccionar el grupo para administrar cada dominio. Debido al acceso de alto nivel otorgado al administrador para cada dominio, estos administradores deben ser personas altamente confiables. El grupo que realiza la administración de dominios controla los dominios a través del grupo de administración de dominios y otros grupos integrados.
- Grupos de administradores responsables de la administración del sistema de nombres de dominio (DNS). El grupo de administradores DNS es responsable de completar el diseño DNS y administrar la infraestructura DNS. El administrador DNS maneja la infraestructura DNS a través del grupo de administradores DNS.

- Grupos de administradores responsables de la administración de la OU. El administrador de la OU designa un grupo o persona como un administrador para cada OU. Cada administrador OU es responsable de administrar los datos almacenados dentro de la OU de active directory asignada. Estos grupos pueden controlar la manera en la que se delega la administración, y cómo se aplica la política a objetos dentro de sus OUs. Además, los administradores de OUs pueden también crear nuevos subárboles y delegar la administración de las OUs de las que son responsables.
- Grupos de administradores responsables de la administración de servidores de infraestructura. El grupo responsable de la administración de servidores de infraestructura es responsable de administrar Microsoft Windows® Internet name service (WINS), el protocolo de configuración de host dinámico (DHCP) y, potencialmente, la infraestructura DNS. En algunos casos, el grupo que maneja la administración de dominios manejará la infraestructura DNS, ya que active directory está integrado en DNS, se almacena y administra en los controladores de dominio.

Administradores de datos

Los administradores de datos active directory son responsables de administrar datos almacenados en active directory o en PCs que se unen a active directory. Estos administradores no tienen control sobre la configuración o servicios de directorio. Los administradores de datos son miembros de un grupo de seguridad creado por la organización. Algunas de las tareas diarias de los administradores de datos incluyen:

- Controlar un subconjunto de objetos en el directorio. A través de un control de acceso a nivel atributo que se hereda, se puede otorgar a los administradores de datos control sobre secciones muy específicas del directorio, pero no tienen control sobre la configuración del servicio mismo.
- Administrar las PCs miembro en el directorio y los datos que residen en las mismas.

Estructura de OU para facilitar la administración y delegación de políticas de grupo

Se requiere cierta información de diseño para proporcionar un entendimiento sobre el uso de las Políticas de grupo para administrar de manera segura los dominios, controladores de dominio y roles de servidor específicos de su organización.

Aunque las OUs ofrecen una manera fácil de agrupar usuarios y otros mandantes de seguridad, también proporcionan un mecanismo efectivo para segmentar los límites administrativos.

El uso de OUs para proporcionar diferentes objetos de Políticas de grupo (GPOs) con base en el rol de servidor es una pieza clave de la arquitectura de seguridad general para la organización.

A continuación se muestra la figura 4.5.2 de un diseño de estructura de una unidad organizativa.

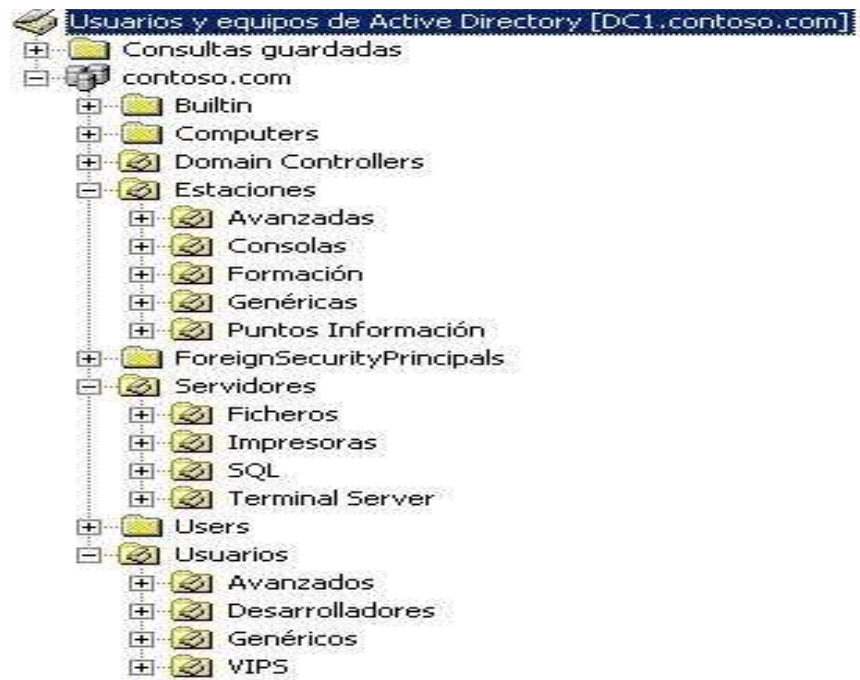


Figura 4.5.2 Estructura unidad organizativa Active Directory

Directiva de Grupo

Una política de grupo es simplemente la forma más sencilla de alcanzar y configurar opciones de usuario y de equipo en redes basadas en Servicios de dominio de active directory. Los requisitos para usar la directiva de grupo son las siguientes.

- Al menos un servidor debe tener instalado el rol de active directory.

- Los equipos que desean administrar deben estar unidos al dominio y los usuarios que se desean administrar deben usar credenciales de dominio para iniciar sesión en sus equipos.
- Tener permiso para editar la directiva de grupo en el dominio

Delegar la administración y aplicar las Políticas de grupo

Una OU es simplemente un contenedor dentro de un dominio. Se puede delegar el control sobre una OU a un grupo o persona al establecer listas de control de acceso específicas (ACLs) en cada uno de estos contenedores.

Los administradores que delegan el control sobre OUs específicas probablemente sean administradores de servicios. A un nivel inferior de autoridad, los usuarios que controlan las OUs son generalmente administradores de datos. Se puede administrar todos los aspectos de la directiva de grupo mediante la consola de administración de directivas de grupo (GPMC) se utiliza para crear, mover y eliminar los GPO, a continuación se muestra la figura 4.5.3 de la consola de administración de directivas de grupo.



Figura 4.5.3 Consola de administración de directivas de grupo

El GPMC, verá todos los GPO del dominio en la carpeta de objetos de directiva de grupo, se explican los siguientes que se señalaron en la figura 4.5.3, de color naranja.

- Accounting security (seguridad de cuentas).
- Default domain controller policy (directiva predeterminada de controladores de dominio). La instalación del rol de servicio de active directory crea esta directiva de forma predeterminada, contiene opciones de configuración de directiva que se aplican específicamente a controladores de dominio.
- Default domain policy (directiva predeterminada de dominios). La instalación del rol de servicio de active directory crea esta directiva de forma predeterminada, contiene las opciones de configuración de directiva que se aplican a todos los equipos y usuarios del dominio.

Aplicación de las políticas de grupo

Las Políticas de grupo se utilizan para delegar la administración, para aplicar configuraciones, derechos y comportamientos específicos a todos los servidores dentro de una OU. Al utilizar las Políticas de grupo en lugar de pasos manuales, es fácil actualizar varios servidores con cualquier cambio adicional requerido en el futuro.

Las políticas se aplican primero en el nivel de políticas de máquina local de la PC. Después de eso, se aplican los GPOs a nivel del sitio, y después a nivel del dominio.

Para crear y vincular un GPO en el dominio o en una OU, se debe hacer lo siguiente en el GPMC, se debe dar clic con el botón secundario en el dominio o la OU donde desee crear y vincular un GPO. Luego, haga clic en create a GPO in thisdomain, and link it here (crear un GPO en este dominio y vincularlo aquí), en el cuadro name (nombre) del cuadro de diálogo new GPO (nuevo GPO), escriba un nombre descriptivo para el GPO y haga clic en ok (aceptar), con estos paso queda creada la política de grupo.

Para editar la política de grupo se deben realizar los siguientes pasos, en el panel izquierdo de GPMC, haga clic en group policy objects (objetos de directiva de grupo) para mostrar todos los GPO del dominio en el panel derecho. También puede hacer clic en el dominio o cualquier OU para mostrar los GPO de ese contenedor en el panel derecho.

En el panel derecho de GPMC, haga clic con el botón secundario en el GPO que desee editar y haga clic en edit (editar) para abrir el GPO en GPME editor de administración de directivas de grupo. En GPME, se modifican las configuraciones de directiva de grupo que desea cambiar, se cierre la ventana del editor cuando haya acabado, no es necesario que guarde los cambios, ya que GPME los guarda automáticamente.

Para vincular un GPO a un dominio o unidad organizativa, se debe ir a la consola GPMC, dar clic con el botón secundario en el dominio o la OU donde desee vincular el GPO y, a continuación, clic en link anexisting GPO (vincular un GPO existente). En el cuadro de diálogo select GPO (seleccionar GPO), hacer clic en el GPO que desee vincular al dominio o la OU y, a continuación, haga clic en ok (aceptar).

A continuación se presenta la figura 4.5.4 del orden de precedencia de la política de grupo.



Figura 4.5.4 Precedencia de política de grupo

Respaldar y Restaurar GPOs

“Realizar una copia de seguridad de archivos importantes es una buena práctica, si por error se cambia o elimina accidentalmente un GPO, se podrá restaurar rápidamente a partir de una copia de seguridad, mediante GPMC, se podrá hacer una copia de seguridad de los GPO en cualquier ubicación”⁴⁰.

En GPMC, haga clic en la carpeta group policy objects (objetos de directiva de grupo), haga clic con el botón secundario en el GPO del que desee hacer la copia de seguridad y, a continuación, haga clic en back up (hacer copia de seguridad).

⁴⁰ Microsoft, Junio 17 2015 Directiva de grupo para principiantes, <<https://technet.microsoft.com/es-es/library/hh147307%28v=ws.10%29.aspx>>

En el cuadro location (ubicación) del cuadro de diálogo back up group policy object (copia de seguridad de objeto de directiva de grupo), escriba la ruta de acceso de la carpeta donde desee crear la copia de seguridad del GPO. Se puede hacer clic en browse (examinar) para elegir una carpeta.

Además, en el cuadro description (descripción), escriba una breve descripción del GPO y haga clic en back up (hacer copia de seguridad). En el cuadro de diálogo backup (copia de seguridad), confirme los resultados y haga clic en ok (aceptar).

A continuación se muestra la figura 4.5.5 de los parámetros que se solicitan para crear el backup.

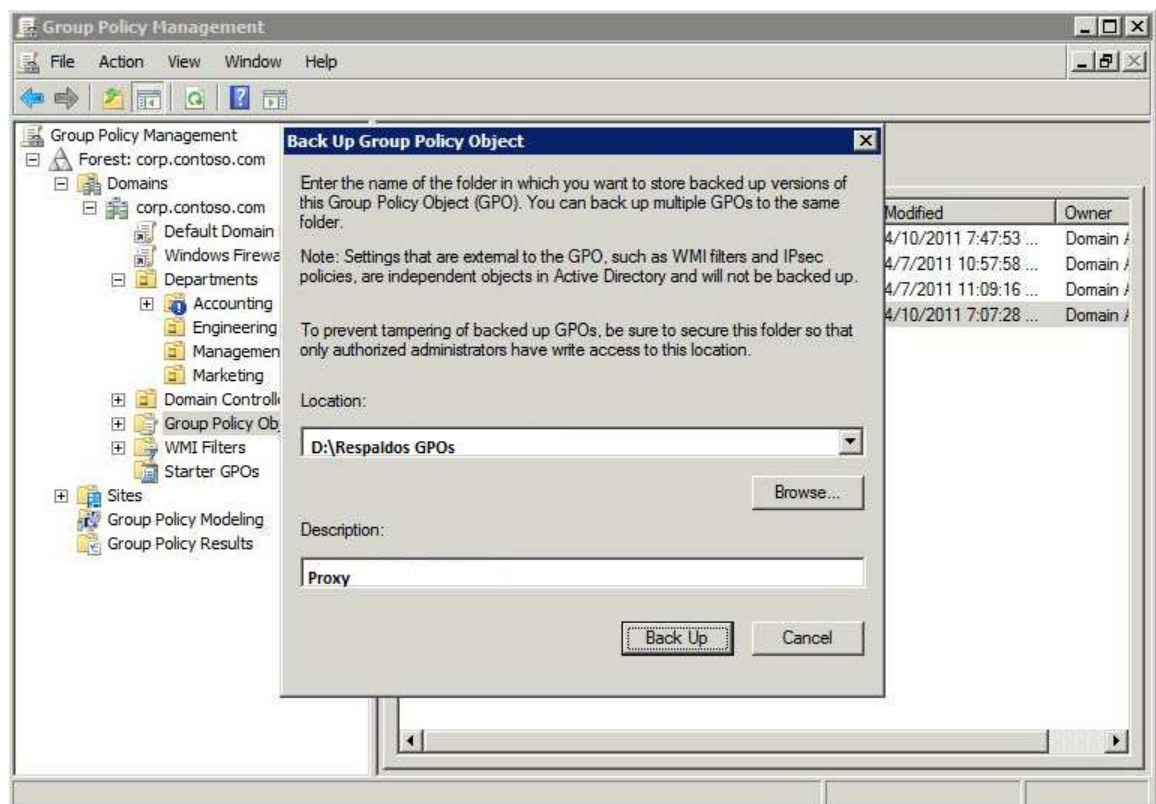


Figura 4.5.5 Parámetros para backup

Para restaurar un GPO del que se ha hecho copia de seguridad, se debe abrir la consola GPMC, haga clic en la carpeta group policy objects (objetos de directiva de grupo) para ver los GPO del dominio, haga clic con el botón secundario en la carpeta group policy objects (objetos de directiva de grupo) y, a continuación, haga clic en manage backups (administrar copias de seguridad).

“En la lista backup location (ubicación de la copia de seguridad) del cuadro de diálogo manage backups (administrar copias de seguridad), haga clic en una ubicación de copia de seguridad que haya usado anteriormente. Puede hacer clic en browse (examinar) para elegir una carpeta que contenga copias de seguridad de GPO”⁴¹.

En la lista backed up GPOs (objetos de directiva de grupo con copia de seguridad), elija uno o varios GPO que desee restaurar y haga clic en restore (restaurar). Si ve varias versiones de cada GPO y solo desea ver las copias de seguridad más recientes de cada GPO, active la casilla show only the test version of each GPO (mostrar solo la versión más reciente de cada GPO). En el cuadro de diálogo restore (restaurar), confirme que la operación se ha realizado correctamente y haga clic en ok (aceptar).

Plantillas de seguridad

Las plantillas de seguridad son archivos basados en texto. Se pueden cambiar estos archivos utilizando el complemento de las plantillas de seguridad de Microsoft management console (MMC) o al utilizar un editor de texto, como el bloc de notas.

⁴¹ Microsoft, Junio 17 2015 Directiva de grupo para principiantes, <<https://technet.microsoft.com/es-es/library/hh147307%28v=ws.10%29.aspx>>

Algunas secciones de los archivos de plantillas contienen ACLs específicos escritos en lenguaje de definición de descriptor de seguridad (SDDL).

Administración de plantillas

De manera predeterminada, los usuarios autenticados tienen el derecho de leer todas las configuraciones dentro del objeto de políticas de grupo. Por lo tanto, es muy importante almacenar las plantillas de seguridad utilizadas para un ambiente de producción en una ubicación segura a la que solo puedan acceder los administradores responsables de implementar las políticas de grupo.

El objetivo es no evitar que se puedan ver los archivos *.inf, sino evitar cambios no autorizados a las plantillas de seguridad fuente. Para lograr esto, todos los pc's que ejecutan Windows Server 2003 almacenan plantillas de seguridad en la carpeta %SystemRoot%\security\templates.

Sin embargo, esta carpeta no se duplica entre varios controladores de dominio. Por lo tanto, se necesitará designar un controlador de dominio para que retenga la copia maestra de las plantillas de seguridad, de manera que no tenga problemas con el control de las versiones de las plantillas. Esto asegura que siempre se modifique la misma copia de las plantillas.

Importar las plantillas de seguridad

El siguiente procedimiento se importa las plantillas de seguridad. Antes de implantar el siguiente procedimiento en un controlador de dominio, se deben localizar los archivos de políticas (*.inf) específicos en el ambiente en un sistema Windows Server 2003.

► **Para importar las plantillas de seguridad de las políticas de dominios**

1. En usuarios y pc's de active directory, haga clic con el botón alterno del mouse en dominio, y después seleccione propiedades.
2. En la pestaña políticas de grupo, haga clic en nuevo para agregar un GPO nuevo.
3. Escriba cliente empresarial – políticas de dominio, y después presione intro.
4. Haga clic con el botón alterno del mouse en cliente empresarial – políticas de dominio, y después seleccione sin anular.
5. Seleccione cliente empresarial – políticas de dominio, y después haga clic en editar.
6. En la ventana Políticas de grupo, haga clic en configuración de pc's\configuraciones Windows. Haga clic con el botón alterno del mouse en configuraciones de seguridad, y después seleccione importar política.
7. En el cuadro de diálogo importar política, navegue hasta \guía de seguridad\ayudas de trabajo, y después haga doble clic en cliente empresarial - domain.inf.
8. Cierre las políticas de grupo que se modificaron.
9. Cierre la ventana propiedades de dominio.
10. Obligue la duplicación entre los controladores de dominio de tal forma que se aplique la política a todos al hacer lo siguiente:

Abra un indicador de comando y utilice la herramienta de línea de comando gpupdate.exe para obligar al controlador de dominio a que actualice la política de dominio con el comando: gpupdate /force.

11. Verifique en el registro de sucesos que se hayan descargado exitosamente las Políticas de grupo y que el servidor se pueda comunicar con los otros controladores de dominio en el dominio.

Política de dominio

Se puede aplicar configuraciones de seguridad de la Política de grupo a diferentes niveles en una organización. Se pueden aplicar configuraciones en los siguientes tres niveles jerárquicos en la infraestructura de dominio:

- **Nivel de dominio** – Para tratar requisitos de seguridad comunes, como políticas de cuenta de contraseñas que se deben implantar para todos los servidores en el dominio.
- **Nivel de línea de base** – Para tratar los requisitos de seguridad de servidor específicos que son comunes para todos los servidores en la infraestructura de dominio.
- **Nivel específico de rol** – Para tratar los requisitos de seguridad para roles de servidor específicos. Para servidores que ejecutan Microsoft Internet information services (IIS).

Descripción general de la política de dominio

La política de grupo es extremadamente poderosa ya que permite a un administrador configurar una pc de red estándar. Al permitir a los administradores realizar cambios de seguridad simultáneamente en todos los pc's en el dominio, o subconjuntos del dominio, los GPOs pueden proporcionar una parte significativa de una solución de administración de configuraciones para cualquier empresa.

Los tipos de cambios de seguridad que puede aplicar simultáneamente vía la política de grupo incluyen:

- Modificar permisos del sistema de archivos.
- Modificar permisos en objetos del registro.
- Cambiar configuraciones en el registro.
- Cambiar asignaciones de derechos de usuario.
- Configurar los servicios del sistema.
- Configurar los registros de auditoría y eventos.
- Configurar las políticas de cuenta y de contraseñas.

Políticas de cuentas

Las políticas de cuentas, las cuales incluyen configuraciones de seguridad de la política de contraseñas, política del bloqueo de las cuentas y política de kerberos, la política de contraseñas proporciona un vehículo para establecer la complejidad y los programas de cambios para contraseñas de ambientes altamente seguros.

La política del bloqueo de las cuentas permite rastrear intentos de registros de contraseña no exitosos para iniciar bloqueos de cuenta en caso necesario. Las políticas de kerberos se utilizan para cuentas del usuario del dominio. Determinan las configuraciones relacionadas con kerberos, como lo son los tiempos de vida y su cumplimiento.

Políticas de contraseñas

Las contraseñas complejas que cambian regularmente reducen la posibilidad de un ataque a contraseñas exitoso. Las configuraciones de las políticas de contraseñas controlan la complejidad y la vida útil de las contraseñas.

Crear requisitos estrictos para la longitud y complejidad de las contraseñas no necesariamente se traduce en usuarios y administradores que utilizan contraseñas sólidas. Con las políticas de contraseñas activadas, los usuarios del sistema pueden satisfacer los requisitos de complejidad técnica para una contraseña definida por el sistema, pero se requieren políticas de seguridad empresarial sólidas adicionales para cambiar los malos hábitos uso de las contraseñas. Hola12, podría satisfacer los requisitos de complejidad de las contraseñas. Pero esta no es una contraseña muy difícil de descifrar.

Al conocer a la persona que crea su contraseña, es posible adivinar su contraseña con base en su comida, automóvil o película favoritos. Una estrategia de un programa de seguridad empresarial para educar a los usuarios en la selección de contraseñas sólidas es crear un cartelón que describa las contraseñas deficientes y mostrarlo en áreas comunes, como el área de café o de la copiadora. Su organización debe establecer lineamientos de seguridad para crear contraseñas sólidas, los cuales deben incluir lo siguiente:

- Evitar utilizar palabras de un diccionario, faltas de ortografía comunes o juegos de palabras y palabras extranjeras.
- Evitar utilizar contraseñas en aumento con un dígito.
- Evitar preceder o anexar un número a contraseñas.
- Evitar utilizar contraseñas que otros puedan adivinar fácilmente viendo su escritorio (como los nombres de sus mascotas, equipos deportivos y familiares).

- Evitar utilizar palabras de la cultura popular.
- Evitar pensar en las contraseñas como palabras en sí – piense en códigos secretos.
- Imponer el uso de contraseñas que requieran escribir con ambas manos en el teclado.
- Imponer el uso de letras mayúsculas y minúsculas, números y símbolos en todas las contraseñas.
- Imponer el uso de espacios y caracteres que solo se pueden producir utilizando la tecla Alt.

Estos lineamientos también se deben utilizar para todas las contraseñas de cuentas de servicio en su organización.

Política de Kerberos

Las políticas de kerberos se utilizan para las cuentas del usuario del dominio. Estas políticas determinan las configuraciones relacionadas con el protocolo kerberos versión 5, como vidas útiles y aplicación de los boletos.

Las políticas kerberos no existen en la política de los pc's locales. Reducir la vida útil de los boletos kerberos disminuye el riesgo de que un agresor se robe las contraseñas y después se haga pasar por una cuenta legítima de usuario.

Sin embargo, mantener estas políticas aumenta los costos de autorización. En la mayoría de los ambientes, no se deben cambiar los valores predeterminados para estas políticas. Las configuraciones kerberos se incluyen en la Política de dominio predeterminada y se aplican en la misma.

Creación de un usuario en Active Directory

Para la creación de un usuario se debe ingresar al directorio activo ya sea mediante el servidor de dominio (MXSRVDC01 192.168.10.211) o desde las herramientas administrativas (siempre y cuando se encuentren instaladas), una vez abierta la ventana de active directory, ubicarse en la unidad organizativa en donde se creara el usuario de acuerdo con el departamento que pertenece, dar → clic derecho → nuevo → usuario, se abrirá una ventana en esta se debe, llenar la información requerida para el usuario, “primer nombre, apellidos y logon name que debe ser primer nombre.primer apellido”, dar clic → next, nos pasa a la siguiente ventana donde se solicita contraseña, se maneja el estándar que es “P@ssw0rd” con la primera opción seleccionada clic en → next → finalizar.

Para hacer a un usuario miembro de un grupo de seguridad o de distribución se debe realizar lo siguiente, dependiendo del departamento al que pertenece el usuario, puede aplicar directivas o grupos de correo, dar → clic derecho → propiedades, abrirá una ventana en esta se debe ir en la pestaña de miembro de clic en agregar y seleccionar el grupo al que se anexara el usuario, agregar grupo de correo una vez seleccionado el grupo, finalmente, clic en aceptar.

4.6 Administración de Exchange

Exchange server 2010 está dividida en 5 funciones, el hecho de agrupar varias tareas de mensajería en torno a una serie de roles o funciones que los administradores pueden desplegar y gestionar por separado, permite reducir la superficie potencial de ataque en un entorno Exchange. Además, les permite escalar Exchange para satisfacer las necesidades específicas de la organización.

Las cinco funciones de servidor de Exchange 2010, son las siguientes:

- Servidor de buzones de correo
- Servidor de acceso cliente (CAS)
- Servidor de transporte de concentradores (Hub)
- servidor de transporte perimetral o EDGE
- servidor de mensajería unificada.

Función de servidor de buzones de correo: El servidor de correo es el repositorio del back-end de Exchange 2010 y contiene items de contenido como buzones de correo, carpetas públicas, listas de direcciones, calendarios de recursos y elementos para reuniones.

Función servidor de acceso cliente (CAS): La función CAS gestiona las conexiones entre todos los clientes externos que necesitan acceso al servicio de correo electrónico. Todos los protocolos necesarios para el acceso cliente, es manejado mediante el CAS, incluyendo los protocolos POP3, Internet message access protocol 4 (IMAP4), messaging application programming interface (MAPI) y HTTPS. El CAS soporta también Microsoft Outlook, Outlook Anywhere, Outlook Web App (OWA) y Exchange ActiveSync (EAS).

Función servidor de transporte de concentradores (Hub): Esta función de servidor procesa, enruta y entrega todo el correo enviado a través de Exchange 2010. El servidor de transporte de concentradores supervisa el filtrado y formateo de los mensajes y comprueba la validez de los archivos adjuntos, proporcionando así la capacidad de verificación que necesita la organización Exchange para el control del correo electrónico interno y externo.

El servidor de transporte de concentradores también registra por diario los mensajes de correo electrónico, añade descargos de responsabilidad de las empresas y otras acciones necesarias para cumplir los requisitos legales. Esta función puede operar junto con un servidor de transporte perimetral.

Función de transporte perimetral o EDGE: Proporciona una capa adicional de seguridad entre la organización que utiliza Exchange Server 2010 y la red exterior. El servidor de transporte perimetral comprueba que los mensajes enviados desde fuera de una organización estén libres de spam y virus antes de enrutarlos hacia el servidor de transporte de concentradores.

El correo saliente del servidor de transporte de concentradores es enrutado hacia el transporte perimetral antes de salir de la organización que utiliza Exchange, esta función es opcional.

Función de servidor de mensajería unificada: El servidor UM, que también es opcional, integra el sistema PBX de las organizaciones con Exchange Server 2010. Dicho servidor almacena datos de la empresa, como mensajes de voz y faxes con correos electrónicos, calendarios y contactos en los buzones de correo de los usuarios. Los usuarios también obtienen prestaciones como respuesta de llamadas, contestadores automáticos, grabación de mensajes y soporte de fax.

Distribución de los roles de servidor de Exchange 2010

La flexibilidad de distribuir las funciones entre distintas plataformas de hardware. Un despliegue básico de Exchange server 2010 incluye buzón de correo, acceso cliente y servidor de transporte de concentradores en la misma caja física.

Este es el conjunto mínimo de funciones necesarias para almacenar, enrutar, entregar mensajes dentro y fuera de una organización. La distribución de roles entre servidores múltiples permite escalarlos según sus necesidades específicas.

Cuando aumenta la demanda de rendimiento, se recomienda segregar las funciones asignadas en servidores separados para aprovechar al máximo la potencia disponible. También se pueden agrupar los servidores para mejorar el rendimiento y la resistencia; otra posibilidad es la migración de funciones a cajas de mayor tamaño y capacidad según las cargas de tráfico existentes.

Topología de la red Active Directory

Exchange 2010 utiliza la pertenencia al site active directory para conocer cuáles son los catálogos globales y controladores de dominio que van a tratar sus consultas. El objeto Exchange actual tiene un atributo de site que permite a otros servidores Exchange que lo soliciten, extraer su nombre desde la base AD sin tener que preguntar a DNS, Exchange utiliza la información de pertenencia al site active directory de la siguiente manera:

Ingreso del correo electrónico: El servidor de buzón de correo busca los servidores de transporte Hub que se encuentran en el mismo active directory que él y transmite los mensajes para el enrutamiento.

Entrega del correo electrónico: La entrega del correo electrónico está asegurada por el servidor de transporte Hub, que efectúa una resolución del destinatario entre la dirección del mensaje y el destinatario. El nombre del destinatario también incluye el nombre del servidor del buzón de correo del usuario. El servidor de transporte hub pregunta a active directory para conocer el site en el que está situado el servidor de buzón de correo o lo transmitirá al servidor de transporte situado en el mismo site que el servidor de buzón de correo del usuario.

Enrutamiento de los mensajes: El enrutamiento de los mensajes se realiza mediante los servidores de transporte hub, que van a realizar acciones en el siguiente orden:

- 1.- Búsqueda del servidor de buzón de correo del usuario.
- 2.- Identificación del site.
- 3.- Si el servidor de transporte hub está en el mismo site que el servidor de buzón de correo, restablece el mensaje.
- 4.- Si el servidor de transporte hub no está en el mismo site, restablece el mensaje en el servidor de transporte hub más cercano del servidor de buzón de correo.

Conexiones al servidor de acceso a cliente: Cuando un usuario se conecta a un servidor de acceso a cliente, el servidor pregunta a active directory para conocer la ubicación de la base de datos del buzón de correo del usuario.

Redirecciones de carpetas públicas: Las carpetas públicas también se hacen a través de la consulta de la ubicación del site en el que se encuentra el servidor de buzón de correo.

- Los servidores de transporte hub se deben poder comunicar con un servidor de catálogo global para efectuar sus búsquedas.
- Los servidores de buzón de correo se deben situar en el mismo site físico que los servidores de transportes hub.
- Los servidores de acceso a cliente deben estar situados en cada site que albergue un servidor de buzón de correo.

Creación de buzón de correo para usuario

Para crear el buzón de correo de un usuario, se debe ingresar al servidor de correo y dentro de este abrir la consola (Exchange management console).

Expandimos el árbol del lado izquierdo hasta llegar a la siguiente ubicación Microsoft Exchange/recipient configuration/mailbox, en las acciones mailbox del lado derecho seleccionamos la opción new mailbox, seleccionamos la primera opción (user mailbox)→ clic en next, a continuación se presenta la figura 4.6.1 de la consola de Exchange.

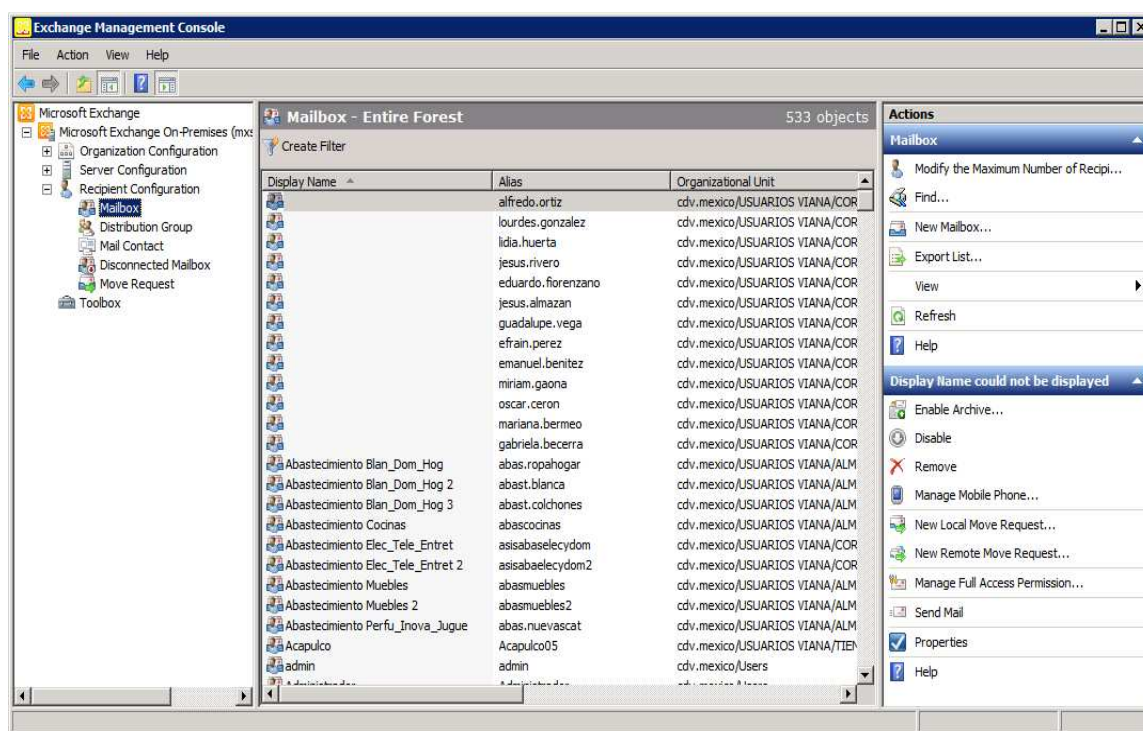


Figura 4.6.1 Consola de Exchange 2010

Nos pasa a una ventana seleccionamos el usuario existing users, clic en add. Y en la siguiente ventana buscamos el usuario al cual se le generara una cuenta de correo, clic en ok, en esta ventana nos colocara el usuario buscado, clic en next.

Pasaremos a otra ventana en mailbox settings seleccionamos el primer check y clic en browse para seleccionar la base en la que se alojara esta cuenta, clic ok, y después en next, nos mostrara otra ventana donde seleccionamos finish, con esto queda lista la cuenta de correo, ahora se muestra en la consola el alta de la nueva cuenta de correo, a continuación se presenta la figura 4.6.2 de la última ventana de configuración de un buzón de correo electrónico.

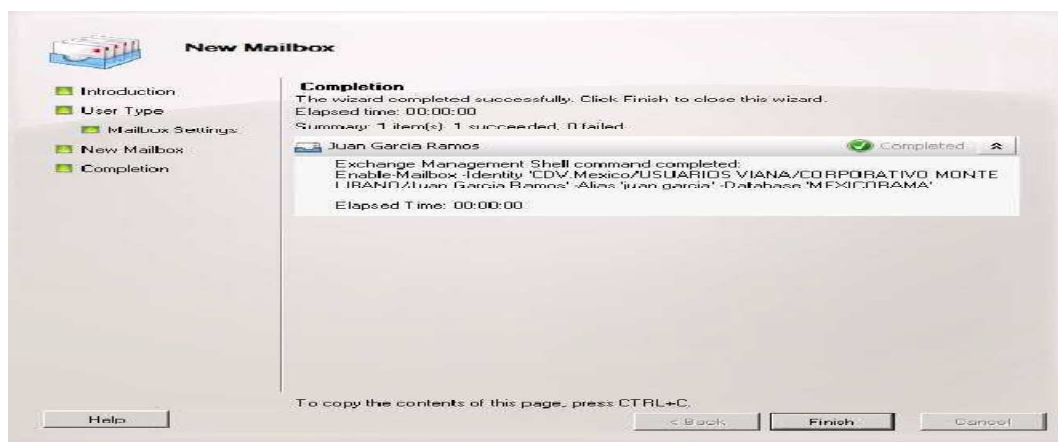


Figura 4.6.2 Configuración de buzón de correo electrónico

Para activar o desactivar la opción del OWA, se debe clic derecho sobre el usuario>properties>mailbox features, seleccionamos Outlook Web App, clic en disable o enable y clic en ok, con esto se finaliza la creación de un buzón para un usuario, a continuación se muestra la figura para activar o desactivar OWA.

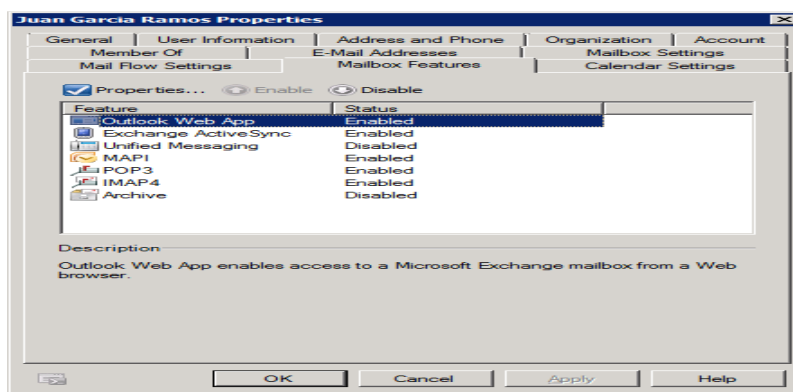


Figura 4.6.3

Conclusión

Actualmente las empresas requieren dotar de infraestructura informática que garantice el continuo desarrollo y sostenibilidad de las actividades que en ella se desarrollen, en este sentido, se requiere una atención importante al hecho de contar con nuevas tecnologías de información que permitan implementar y gestionar de manera más eficaz el sistema de la empresa, con la finalidad de protegerlo.

Se debe aprender a escoger las mejores tecnologías de la información de acuerdo con la necesidad requerida, con el fin de poder adoptar soluciones de almacenamiento de información, acceso de datos, procesos rápidos con pocos errores y comunicaciones automáticas entre procesos, para que las tecnologías de la información aporten mejores métodos para realizar las tareas y obtener la mayor productividad de ellas.

Es importante considerar que las tecnologías de la información afectan a toda la empresa, por tal motivo se debe coordinar el avance de las tecnologías de la información con las áreas de la empresa a las cuales se afecte directamente para que puedan adaptarse, de esta manera, se evita el rechazo por parte de los usuarios.

En las tecnologías de la información se debe considerar los objetivos generales de la empresa, para que con ayuda de las tecnologías de la información se pueda tener el mejor diseño de soluciones a los procesos operativos, alcanzando así a percibirse no como una inversión sin retorno, más bien se puede ver como una inversión con retorno a la empresa, un elemento más de la política de negocio.

Para definir que tecnología de la información se debe elegir, se tiene que evaluar todas las alternativas posibles, de realizar de forma interna o externa, analizando la relación costo-beneficio, considerando tiempos, personas, equipos, etc. Una vez elegida e implementada se debe monitorear y reevaluar constantemente para revisar que entregue los resultados esperados. Este trabajo permite conocer el uso, aplicación e implementación de algunas herramientas útiles para la tecnología de la información.

Bibliografía

Emmanuel Vinazza, Exchange Server 2010 diseño de la infraestructura, implementación y administración, España, Ediciones ENI, Marzo 2011, 35-41, 44-60, 128-147, 220,334 pp.

Andrew S. Tanenbaum, Redes de computadoras, México, Prentice Hall, Marzo 1997, 419-420, 610, 622 630, 662, 642-643, 748 pp.

Abraham Silberschatz, Sistemas Operativos, México, Addison Wesley, 1999, 3, 501, 647-687, 697-739.

Sistema de posicionamiento global:

(http://es.wikipedia.org/wiki/Sistema_de_posicionamiento_global).

Servicio general de paquetes vía radio:

(http://es.wikipedia.org/wiki/Servicio_general_de_paquetes_v%C3%ADa_radio).

Rastreo Satelital, (<http://www.max4systems.com/rastreo-satelital.html>).

GNU/Linux, (<http://es.wikipedia.org/?title=GNU/Linux>),
(<http://www.gnu.org/gnu/linux-and-gnu.es.html>)

Proxy squid,

(http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html).

Correo Linux, (http://www.redes-linux.com/manuales/Servidor_correo/sendmail.pdf),
(http://es.wikipedia.org/?title=Modelo_TCP/IP),

(http://es.wikipedia.org/wiki/Internet_Message_Access_Protocol)

Mantenimiento Preventivo, (http://es.wikipedia.org/wiki/Mantenimiento_preventivo).

Mantenimiento Correctivo (<http://www.buenastareas.com/materias/justificacion-de-la-aplicacion-de-mantenimiento-correctivo/0>)

Software,

(http://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAAahUKEwjWnovcsInGAhVEGKwKHa8jAHI&url=http%3A%2F%2Ftinfoinformatica.jimdo.com%2Fapp%2Fdownload%2F6742969770%2F5.-_Apunte_sobre_software_actualizado.doc%3Ft%3D1363746774&ei=Zmh6VdbTEcSwsAWvx4CQBw&usg=AFQjCNFuGMkliRYs4gsCwXXNcgpd56es7w&bvm=bv.95515949,d.b2w).

Terminales tontas, (<https://www.freebsd.org/doc/es/books/handbook/term.html>).

Cliente liviano, (http://es.wikipedia.org/wiki/Cliente_liviano)

RAID, (<http://es.wikipedia.org/wiki/RAID>)

Copia de seguridad (http://es.wikipedia.org/wiki/Copia_de_seguridad).

Respaldo y restauración (<http://www.monografias.com/trabajos90/respaldo-informacion/respaldo-informacion.shtml>).

Backups incrementales vs diferenciales
(<https://murci.wordpress.com/2008/09/24/backups-incrementales-vs-diferenciales/>).

DLP, (<http://www.mcafee.com/mx/products/total-protection-for-data-loss-prevention.aspx>).

DAT, (<http://pyme.lavoztx.com/cmo-ver-un-archivo-dat-6571.html>)

PUP, (http://malware.wikia.com/wiki/Potentially_unwanted_program).

Spam, (<http://es.wikipedia.org/wiki/Spam>).

Phishing, (<http://es.wikipedia.org/wiki/Phishing>)

BIOS, (<http://es.wikipedia.org/wiki/BIOS>).

Antispyware, (<http://www.alegsa.com.ar/Dic/antispyware.php>).

ActiveX, (<https://www.microsoft.com/es-es/security/resources/activex-what-is.aspx>).

Active Directory,

(https://es.wikipedia.org/wiki/Active_Directory).

(<https://support.microsoft.com/es-mx/kb/196464/es>)

(<https://technet.microsoft.com/es-es/library/cc163113.aspx>)

(<http://go.microsoft.com/fwlink/?LinkId=15159>)

(<http://www.google.com.mx/url?url=http://download.microsoft.com/download/d/0/5/d05edbea-6dd4-4e77-b16e-0991dad9243e/WindowsServer2003SecurityGuide1.doc&rct=j&frm=1&q=&esrc=s&sa=U&ei=wOGBVYXmL8ipsAXNjKHgBA&ved=0CBkQFjAB&usg=AFQjCNFCHlwHWq4VpZmQIHWyMtzRMtDYLw>).

(<https://technet.microsoft.com/es-es/library/hh147307%28v=ws.10%29.aspx>)

LDAP, (<https://es.wikipedia.org/wiki/LDAP>).

DHCP, (https://es.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)

Directiva de Grupo, ([https://technet.microsoft.com/es-es/library/hh147307\(v=ws.10\).aspx](https://technet.microsoft.com/es-es/library/hh147307(v=ws.10).aspx)).