UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación de políticas, configuraciones, aplicaciones y administración para la seguridad informática de la empresa

Informe de trabajo profesional
que para optar por el título de
Ingeniero en Computación
Presenta:

Salvador Nieves Padilla

Asesora: M.C. Ma. Jaquelina López Barrientos

AGRADECIMIENTOS

El presente informe es resultado de un gran esfuerzo en el cual directa e indirectamente participaron muchas personas que son muy importantes para mí, participando de muchas formas y donde lo más importante fue su apoyo incondicional.
Agradezco a mi asesora M.C. Ma Jaquelina López Barrientos por haber confiado en mí, por toda la paciencia, la dirección y guía a lo largo de este proyecto. A M. C. Alejandro Velázquez Mena por los consejos y correcciones así como su apoyo para el desarrollo de este informe.
A todos aquellos profesores que a lo largo de toda mi carrera me enseñaron grandes cosas e hicieron posible que lograra la conclusión de este proyecto.

Gracias a toda mi familia que ha sido un pilar muy importante en mi vida, a mis padres y a mi hermana que siempre me han impulsado para cumplir cada una de las metas obtenidas y siempre he contado con ellos para todo, lo que he deseado y realizado siempre me han apoyado incondicionalmente.

A mi novia Fernanda por todo su apoyo, comprensión y aliento a lo largo de este proceso, porque fue más fácil concluir este proyecto gracias a tu ayuda y al tiempo que dedicaste en apoyarme, por los ánimos que me das día a día.

A mis tíos y primos por sus enseñanzas y su apoyo. A Hugo del Castillo por todo su apoyo y correcciones a lo largo de este proyecto, por su paciencia y todos sus consejos.

Agradezco también a todos mis amigos que siempre he contado con su apoyo, que han estado conmigo ya a través de un largo camino, que de una u otra forma su apoyo ha sido muy importante para lograr lo que me he propuesto, gracias por su amistad, Hugo, Luis, Cesar, Raymundo, Humberto, Miguel, Adrián, Arturo, Raul, Hugo DC.

A Yahir y Luis que recorrimos juntos el camino a lo largo de la carrera de ingeniería, que me enseñaron grandes cosas y compartimos muchas más. A toda la comunidad universitaria tanto compañeros y maestros que forman parte de todo el recorrido.

Gracias a Ariel Iturbe por ser un excelente maestro ahora en el ámbito laboral, por compartirme mucho de su amplio conocimiento y también gracias por todo el apoyo a Jorge Luis Perez .

Muchas gracias a todos.

ÍNDICE

INTRODUCCIÓN

Concluidos mis estudios profesionales de nivel licenciatura en 2009, después de una serie de entrevistas y negociaciones, ingreso el 26 de marzo de 2010 al Área de Sistemas con la responsabilidad de la administración y seguridad de los sistemas informáticos de la empresa Tecnología Especializada Asociada de México S.A., compañía dedicada a la integración de soluciones de tecnologías de la información y comunicaciones, que de acuerdo al Plan Nacional de Desarrollo 2007-2012, por el número de empleados y el rango de ventas anuales promedio, entre otros factores, establece que es considerada una Gran Empresa.

El Área de Sistemas en la que laboro se encuentra integrada por 3 ingenieros más que cumplen actividades de soporte, programación, administración de los sistemas de comunicaciones y queda a mi cargo la administración de los sistemas de información.

Al ingresar a dicha área inicia mi capacitación y actualización sobre la estructura de la empresa, tanto en sus recursos humanos como tecnológicos, con lo cual dentro de las primeras semanas llevo a cabo mi integración al personal y comienzo a adquirir el conocimiento del diseño y el cómo se encuentran estructurados los sistemas con los que cuenta la organización, conociendo que desde TEAM México se lleva a cabo la administración de las sucursales que se encuentran a lo largo de la República y una más dentro del Distrito Federal.

Una vez al tanto, me es asignada la labor de desarrollar esquemas y guías sobre el estado en el que se encuentra la infraestructura de servidores de correo, aplicaciones, demos, virtualización, telecomunicaciones y su relación entre sí, los cuales serán mostrados posteriormente.

Con el conocimiento de todos los aspectos y teniendo una perspectiva clara, el siguiente paso fue desarrollar el estatus en el que la empresa se encontraba con respecto a su seguridad, el resguardo de sus activos y todo aquello que tenga que ver con la protección de la información sensible que dentro de la empresa se considera importante. En el presente Informe de Actividades Profesionales presento el proyecto correspondiente a la Implementación de políticas, configuraciones, aplicaciones y administración para la seguridad informática de la empresa, actividad que está a mi cargo.

Importancia de la seguridad informática en la empresa

Comprender que las Tecnologías de la Información (TI) ya no son solamente una base o el soporte para los negocios sino una forma de generarlos, esta nueva perspectiva está haciendo que las organizaciones cambien su forma de ver la tecnología y la aprovechen de distintas maneras.

Una vez identificado el gran avance que son y lo que se puede crear por estos medios, también se puede observar que su mala administración puede tener consecuencias muy adversas a como fue planeado.

Las nuevas posibilidades conllevan riesgos muy importantes que deben tenerse en cuenta, muchas veces las empresas se enfocan simplemente en las tecnologías pero su administración y protección se dejan a un lado mientras se proporcione la labor para la que fueron creados o adquiridos, pero no se identifica lo importante y lo sensible que es su resguardo.

Para una empresa, en cualquier ámbito en el que se encuentre, el resguardo de su información es vital para la continuidad de su negocio, pero muchas veces no se está consciente de ello ni de los riesgos que corre su información. Por obvias razones, el impacto financiero y mercadológico de este tipo de cuestiones es muy alto.

Los riesgos y amenazas que se derivan del uso de la tecnología y de las redes que la intercomunican, ha provocado que la seguridad de la información se haya incrementado hasta alcanzar posicionarse como prioridad para la mayoría de las grandes empresas importantes del mundo, pero a nivel nacional estas cuestiones son más complejas ya que se tiene que concientizar a los directivos de que su información es muy valiosa y requiere de la protección necesaria.

Hace más de una década que los ataques informáticos están presentes y son una gran problemática para todos los ámbitos: el gobierno, la industria y la educación, entre otros. Es bien sabido que, año con año, ataques a la seguridad crean grandes pérdidas de dinero al Estado y a las empresas, razón por la cual es imprescindible hacerles ver a los responsables de la dirección la importancia de contar no sólo con el aseguramiento de bienes físicos sino también de la información que la empresa maneja, y dejar claro que existen diversas formas de realizarlo para asegurar la continuidad del negocio.

Aunque la industria y empresas en México recién empiezan a valorar lo que la implementación de técnicas y sistemas para el aseguramiento de la información puede hacer por su empresa, muchas grandes compañías comienzan a comprender que invertir en estas cuestiones es muy importante.

Un estudio realizado en enero de 2010 por la Australian Information Security Association, señala que tan sólo en ese mes más de 75,000 equipos habían sido hackeados en más de 2500 compañías alrededor del mundo por lo cual es muy importante hacerle ver a las empresas que la seguridad informática no se basa sólo en antivirus y firewalls, éstas son herramientas que ayudan a la protección de la información pero no la aseguran y mucho menos si se hace sin un conocimiento puntual de lo que se quiere resguardar; de manera que saber reconocer que la información es crítica, valiosa e indispensable, ya que es un activo corporativo sensible y debe ser accesible por las personas que lo requieran y estén autorizadas para ello, debido a esto, plantear y generar un modelo de seguridad informática es muy importante para la continuidad del negocio, por lo cual es de vital importancia que nuestra organización esté a la vanguardia de los procesos de cambio, donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental.

Adentrándonos al caso particular, en la empresa TEAM un aspecto muy importante son sus activos, tanto físicos como lógicos, ya que existe información sensible que puede determinar ganar o perder clientes y licitaciones, esto se traduce en grandes cantidades de dinero, además de reputación y otro tipo de pérdidas que pueden generarse.

A continuación se presenta una descripción de la empresa en la que laboro con lo que se pretende adentrarnos en el ámbito en el que se desarrolla y dejar perfectamente plasmado el enfoque del negocio para poder ver con una mejor perspectiva por qué es importante el resguardo de la información en esta empresa.

Base teórica de la Seguridad Informática

A continuación se menciona una serie de aspectos teóricos sobre la seguridad informática con lo que se sentarán las bases para la implementación posterior del proyecto, conceptos que son muy importantes dejarlos bien claros.

La seguridad informática se puede definir como el conjunto de herramientas, procedimientos, técnicas, y reglas que nos ayudan a proteger los sistemas de información y de esa manera poder garantizar los principios de la información.

Dentro de las consideraciones básicas que se deben responder para llevar a cabo un análisis sobre seguridad informática, están los siguientes cuestionamientos.

- ¿Qué es lo que se quiere proteger?
- ¿De qué se quiere proteger?

- ¿Cómo lo vamos a proteger?

El proceso para dar respuesta a estas interrogantes, se lleva desde un panorama general hasta el más particular, de fuera hacia dentro, tomando como base el análisis a la infraestructura actual y al comportamiento del personal de la organización, así como las prácticas que se realizan actualmente con respecto a la seguridad informática, si son buenas pueden adaptarse a los estándares o en su defecto ser erradicadas, para plasmar y dar a conocer una serie de políticas acerca de la seguridad informática a seguir en la empresa Tecnología Especializada Asociada de México.

La identificación correcta y las respuestas acertadas a las preguntas anteriores son de vital importancia para poder llevar a cabo una implementación que de verdad cumpla con los requerimientos necesarios.

Los mecanismos, reglas, normas y buenas prácticas deben de poder garantizar:

- *La disponibilidad de los sistemas de información*. Se refiere a la certeza de que la información pueda ser visible y accesible en el momento en que se necesite y sea requerida, así como, evitar su pérdida o bloqueo, bien sea por ataques, mala administración, etc.

- *La integridad de la información*. Que los datos enviados y recibidos se mantengan de la forma en que fueron creados y que estos no lleguen a ser modificados, alterados o reordenados por un tercero no autorizado.

- *La confidencialidad de la información*. Se refiere a que la información sólo puede ser conocida por las personas autorizadas. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada.

- *No-Repudio*. Permite probar la participación de las partes en una comunicación. Existen dos posibilidades:

    - No repudio en origen: el emisor no puede negar que envió porque el destinatario tiene pruebas del envío.
    - No repudio en destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

- *Autenticación*. Es el proceso de verificación de identidad que prueba que es, quien dice ser ante un sistema.

Estrategias de Seguridad

Para llevar a cabo una implementación con respecto a seguridad informática, contando con un análisis previo se deben plantear una o varias estrategias de seguridad como pueden las siguientes:

- *Seguridad por obscuridad*. Ocultar códigos, procesos, aplicaciones, para que no se tenga la conciencia o conocimiento de ellos.

- *Seguridad por menores privilegios*. Restringir permisos al máximo para sólo poder llevar a cabo las actividades necesarias.

- *Seguridad por punto de ahogo*. Contar y permitir sólo una entrada y una salida para tener control perfecto de las actividades, disposición alineada para monitoreo de un solo canal.

- S*eguridad por postura de falla segura*. Estar conscientes de que las fallas en la seguridad se pueden presentar y contar con una previsión.

- *Seguridad por simplicidad*. Realizar las cosas de forma correcta y simplificada.

- *Seguridad por defensa o fondo*. Implementar una serie de líneas de defensa, con varios esquemas de seguridad.

Conociendo la gama de técnicas que podemos implementar es muy importante saber que una sola técnica no podría proporcionarnos una seguridad adecuada para los diversos tipos de problemas, vulnerabilidades y ataques que pueden presentarse por lo cual las mejores prácticas indican un análisis e implementación de distintas técnicas para un mejor aseguramiento de la seguridad de nuestra información.

Niveles de Seguridad Informática

Existen varios niveles de seguridad informática los cuales se deben analizar para realizar implementaciones de forma adecuada en cada nivel a fin de contar con el aseguramiento de la información. (Véase figura I.1)

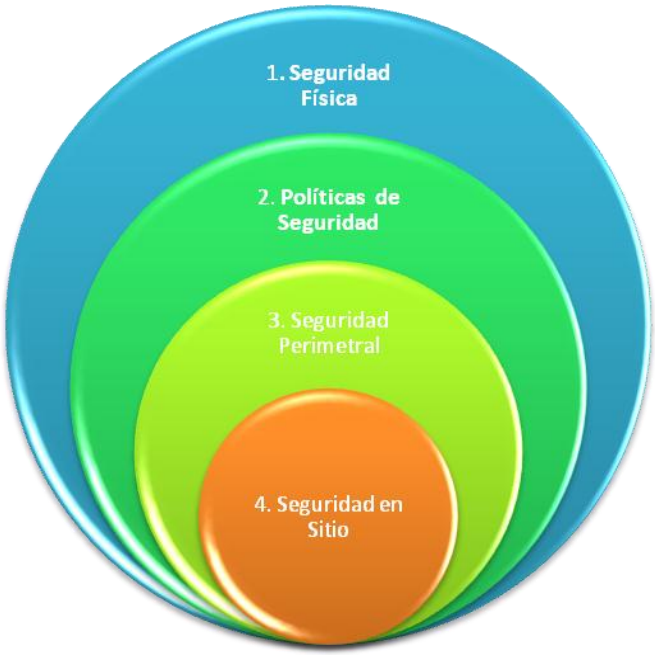


Figura I.1 Niveles de Seguridad Informática

1. Seguridad Física

Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Data Center así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

2. Política de Seguridad

Es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán. Las políticas reflejan una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero ante todo, una política de seguridad es una forma de comunicarse con los usuarios, teniendo en cuenta que la seguridad comienza y termina con personas.

3. Seguridad Perimetral

La seguridad perimetral es un concepto que asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), el principio físico de su forma de percibir las cosas o bien por el sistema de soporte.

4. Seguridad en Sitio

La seguridad en sitio es aquella que se provee en el lugar de acción, donde se desarrolla el centro de los servicios y las aplicaciones, este puede ser en forma física o por medio de herramientas y aplicaciones para el aseguramiento de la información.

Ataques y amenazas a la seguridad corporativa

Como base teórica para poder generar una estrategia adecuada de seguridad informática y poder implementar técnicas que nos permitan resguardar los activos de la organización a continuación se presentan las principales amenazas y ataques conocidos.

Es muy importante explicar lo que es una vulnerabilidad ya que es el medio más importante por el que se lleva a cabo un ataque exitoso. Una vulnerabilidad es un punto del sistema susceptible de ser atacado o de dañar la seguridad del mismo, es decir, representa las debilidades o aspectos susceptibles a ser atacados en un sistema.

Una amenaza representa el tipo de acción, circunstancia, evento, persona o fenómeno que puede ser dañina o provocar una violación a la seguridad.

Un ataque se define como un intento de acceso, o uso desautorizado de un sistema o recurso del mismo, ya sea satisfactorio o no.

De esta forma presento los diversos tipos de amenazas que podemos encontrar, las cuales pueden ser un peligro para la seguridad de nuestra información.

- Humanos

  La amenaza surge por ignorancia en el manejo de la información, descuido, negligencia, inconformidad, entre otras.

  - Ingeniería Social

    Es la manipulación de personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan, de tal forma que revelen datos indispensables que permitan superar las barreras de seguridad.

- Ingeniería Social Inversa

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en la ingeniería social.

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechará esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).

- Robo, Fraude y sabotaje

Por medio de las computadoras dentro de una empresa la información confidencial puede ser extraída de forma no autorizada para la realización de fraudes con fines de lucro, así como sabotaje, uno de los peligros más temidos en los Data Centers, ya que puede realizarse de forma externa e interna.

- Personal Interno

Son amenazas al sistema provenientes del personal desde el propio sistema informático, rara vez son tomadas en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o falta de normas básicas de seguridad; pero también pueden ser intencionales.

- Ex-empleado

Este grupo puede estar especialmente interesado en violar la seguridad de nuestra empresa, sobre todo aquéllos que fueron despedidos y no han quedado conformes; o bien los que renunciaron para pasar a trabajar en la competencia.

Generalmente se trata de personas descontentas con la organización, conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios para causar cualquier tipo de daño.

- Curiosos

Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero sin los conocimientos ni experiencia básicos para considerarlos hackers o crackers.

Generalmente no se trata de ataques dañinos pero afectan el entorno de fiabilidad generado en un sistema.

- Terroristas

  Bajo esta definición se engloba a cualquier persona que ataca el sistema para causar daño de cualquier índole en él.

- Intrusos Remunerados

  Es el grupo de atacantes más peligroso, aunque también el menos habitual, se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar "secretos" (código fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto, etc.) o simplemente para dañar de alguna manera la imagen de la entidad atacada.

  Suele darse sólo en grandes multinacionales donde la competencia puede darse el lujo de hacer un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

- Errores de hardware

Se da la amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

- Errores de la Red

Esta amenaza se presenta cuando la red de comunicación no está disponible para su uso, esto puede ser provocado por un ataque deliberado por parte de un intruso, un error físico o lógico del sistema mismo. Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red y la extracción lógica de información a través de ésta.

- Problemas de tipo lógico

Una amenaza se hace presente cuando un diseño bien elaborado de un mecanismo de seguridad es mal implementado, es decir que no cumple con las especificaciones con las que fue diseñado. La comunicación entre procesos puede resultar una amenaza cuando un intruso utilice una aplicación que permita enviar y recibir información, dándole al intruso elementos para un posible ataque.

Un código malicioso es cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas, esto incluye caballos de Troya, virus, gusanos informáticos, bombas lógicas y otras amenazas programadas.

- Caballo de Troya

  Este tipo de código se presenta escondido en otros programas de aplicación aparentemente inofensivos, para posteriormente activarse de manera discreta cumpliendo su propósito nocivo.

- Virus

  Código malicioso que tiene como principal característica la capacidad de duplicarse o replicarse a sí mismo usando recursos del sistema infectado, propagando la infección rápidamente.

- Gusanos

  Es un programa o cálculo que se puede mover de máquina en máquina, aprovechando los recursos que necesita y se replica a sí mismo cuando es necesario.

- Desastres

Entre los tipos de desastres naturales que amenazan a un sistema de información, tenemos inundaciones, terremotos, incendios, huracanes, tormentas eléctricas, etc. Los cuales provocan cortos circuitos, destrucción total o parcial de los equipos de cómputo, o alteraciones físicas de las localidades, causando que ya no sean apropiadas para albergar un equipo de cómputo.

Por lo tanto es necesario considerar el punto geográfico en el que se llevará a cabo la instalación del equipo de cómputo, centro de servicios de información, centro de cómputo etc. y hacer un estudio que permita determinar las amenazas a las que serían susceptibles a fin de evitar ser víctimas de estas.

Adicionalmente considerar la importancia de un cableado no sólo en la red de datos sino en las redes de energía eléctrica y suministro de agua que de manera indirecta podrían causar algún desastre de este tipo y dañar la información de la organización.

Dentro del flujo normal de la información no debe existir ningún obstáculo para que la información llegue al destinatario.

A continuación se presentan los distintos tipos de ataques que se pueden realizar y que ponen en riesgo nuestra información.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- Interrupción

  Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son: la destrucción de un elemento de hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

- Intercepción

  Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora. Ejemplos de este ataque son el tener acceso a una línea para hacerse con datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

- Modificación

  Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son: el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

- Fabricación

  Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

Asimismo estos ataques se pueden clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques Pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitorea para obtener información que está siendo transmitida. Sus objetivos

son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación puede consistir en:

1. **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitoreados.

2. **Control del volumen de tráfico** intercambiado entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.

3. **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

Ataques Activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como robar la contraseña de acceso a una cuenta.
- **Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, por ejemplo, ingresar dinero repetidas veces en una cuenta dada.**
- **Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".**
- **Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.**

La importancia del personal de la organización en el aseguramiento de la información

En adelante se exponen puntos importantes sobre cómo influyen las personas en la seguridad de la información dentro de la empresa.

Los problemas de seguridad encuentran en la mala administración, errónea implementación y factores tecnológicos, una gran oportunidad para causar graves daños a la organización pero de esta forma también, uno de los grandes problemas que aquejan a las empresas es la falta de cultura informática de las personas que las integran.

El eslabón más débil en la cadena de la seguridad lo constituye el ser humano y no el aspecto tecnológico, lo cual destaca la importancia de tener una cultura de seguridad informática. A todos los usuarios de la organización se les debe divulgar las políticas de seguridad, además de realizar auditorías periódicas para controlar que sean las políticas adecuadas en el momento en que se encuentra la empresa.

Lo que se necesita no es solamente prevenir un ataque a la seguridad, sino ser capaces de detectar y responder a esta agresión mientras ocurre y reaccionar ante la misma, es importante destacar que no existe un control de seguridad único, sino que las empresas deben contar con diversas capas de seguridad en todos los niveles de su información para poder así detectar el problema antes de que llegue a la información crucial.

Según un estudio realizado en agosto de 2010 por la firma de mercadeo inteligente IDC, del 30% al 40% del tráfico de las empresas no está relacionado con el trabajo; en el horario laboral las visitas a los sitios pornográficos, compras en línea, subastas y juegos de azar son muy recurrentes. En definitiva, pornografía, subastas, búsqueda de nuevo empleo, comercio electrónico, banca a distancia, prensa, juegos, correos personales, son los sitios más visitados por todo el personal en la empresa, por lo cual la web, los usuarios y el mal uso de los servicios generan un alto riesgo para la seguridad de la información, de esta forma pueden acceder intrusos o llevarse a cabo ataques en contra de la organización.

Como parte de los servicios que se brindan al personal de TEAM encontramos: correo electrónico, internet, servicio de telefonía, VPN, storage de documentación, aplicaciones y demos, entre otros. A continuación se presenta la forma en que la infraestructura tecnológica está organizada para brindar estos servicios.

Infraestructura de Tecnologías de la Información de la empresa

La estructura de datos y comunicaciones de la empresa se muestra por medio de los siguientes diagramas, esquematizados de la figura I.2 a la I.8 mismas que se encuentran organizadas y distribuidas de la siguiente forma:

Por medio del diagrama que se muestra en la figura I.2, se aprecia cómo se encuentra la configuración de red de la organización, desde la acometida, firewall, servidores, aplicaciones, servicios, distribución de las redes, sistemas de autenticación y de Storage.

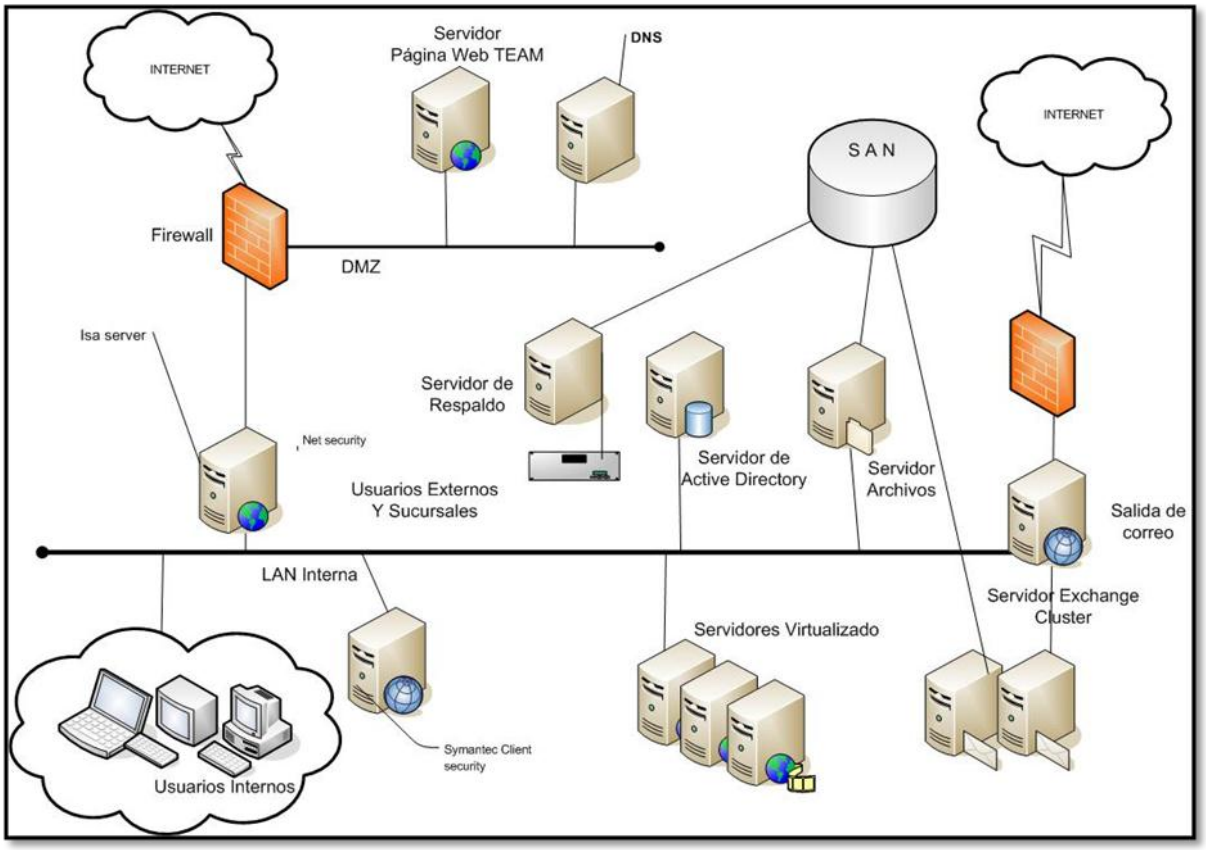


Figura I.2 Esquema general de la red TEAM

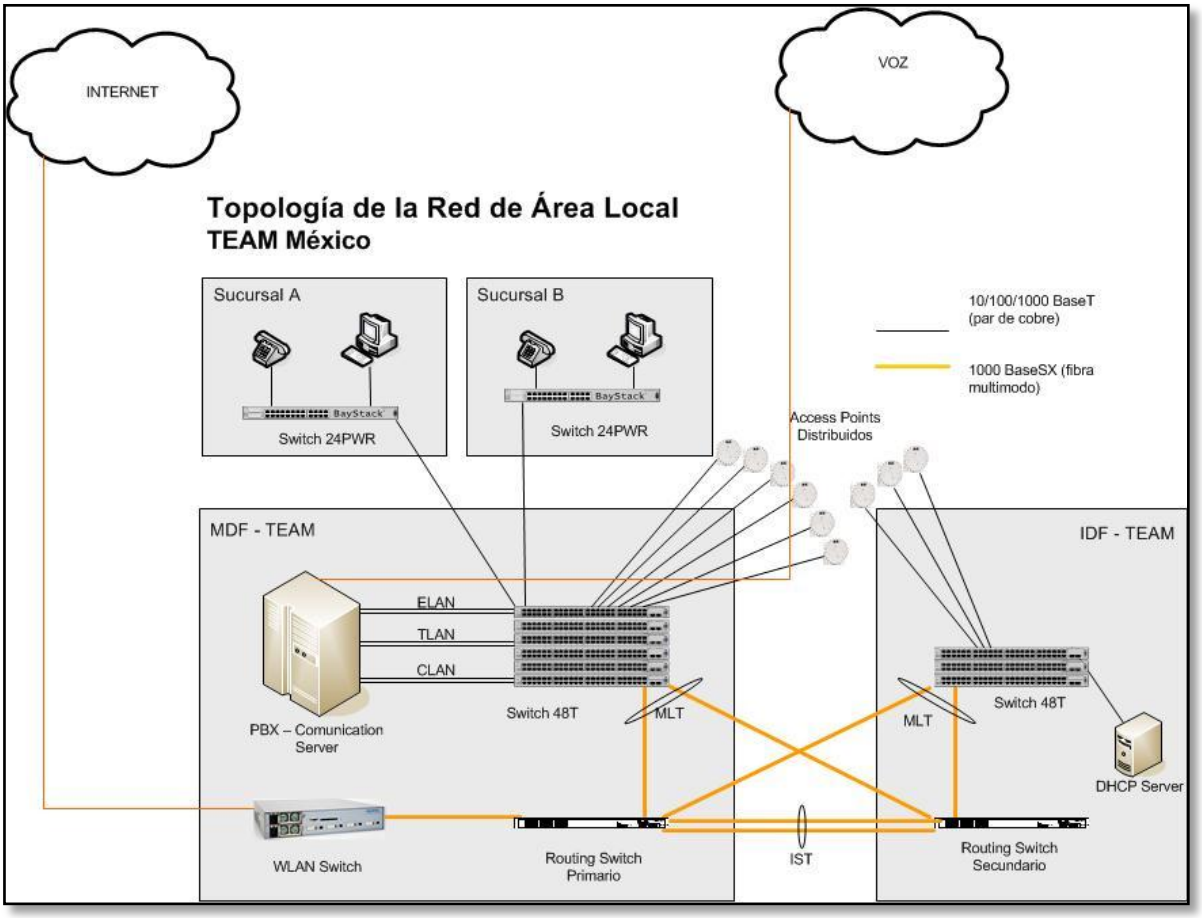


Figura I.3 Red Área Local MDF-IDF TEAM México

Por medio de la figura I.3 se muestra la distribución y configuración de la red de área local en TEAM México a nivel MDF(Instalación Principal de distribución) – IDF(instalación intermedia de distribución),la estructura de cableado, así como las distintas VLANS y cómo se interconecta la matriz con la sucursal A y la sucursal B en el D.F.

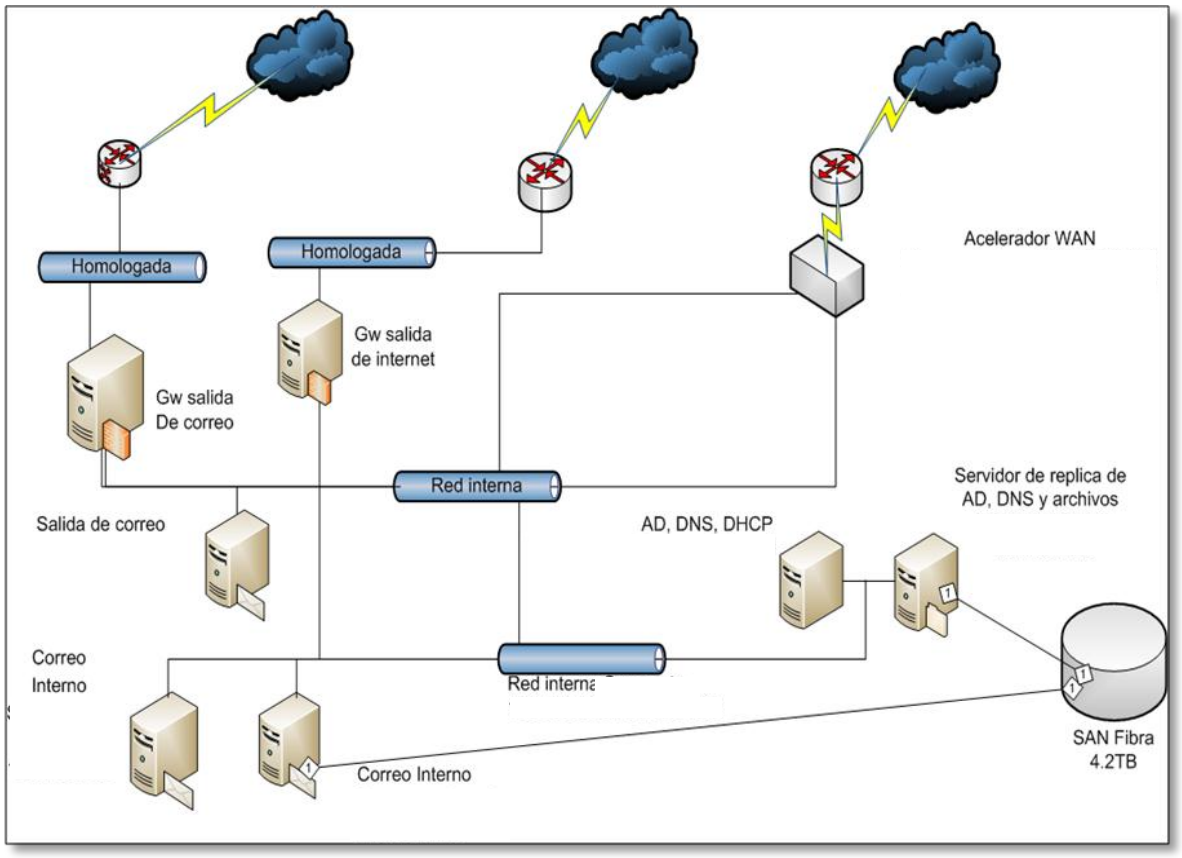


Figura I.4 Esquema General Correo TEAM

En el diagrama de la figura I.4 se observa desde la acometida hacia los routers correspondientes, así como los servidores que dan acceso a la red para dirigirse hacia los servidores de correo de entrada y salida, Back y Front End, así como su interconexión con la SAN y el directorio activo asignado.

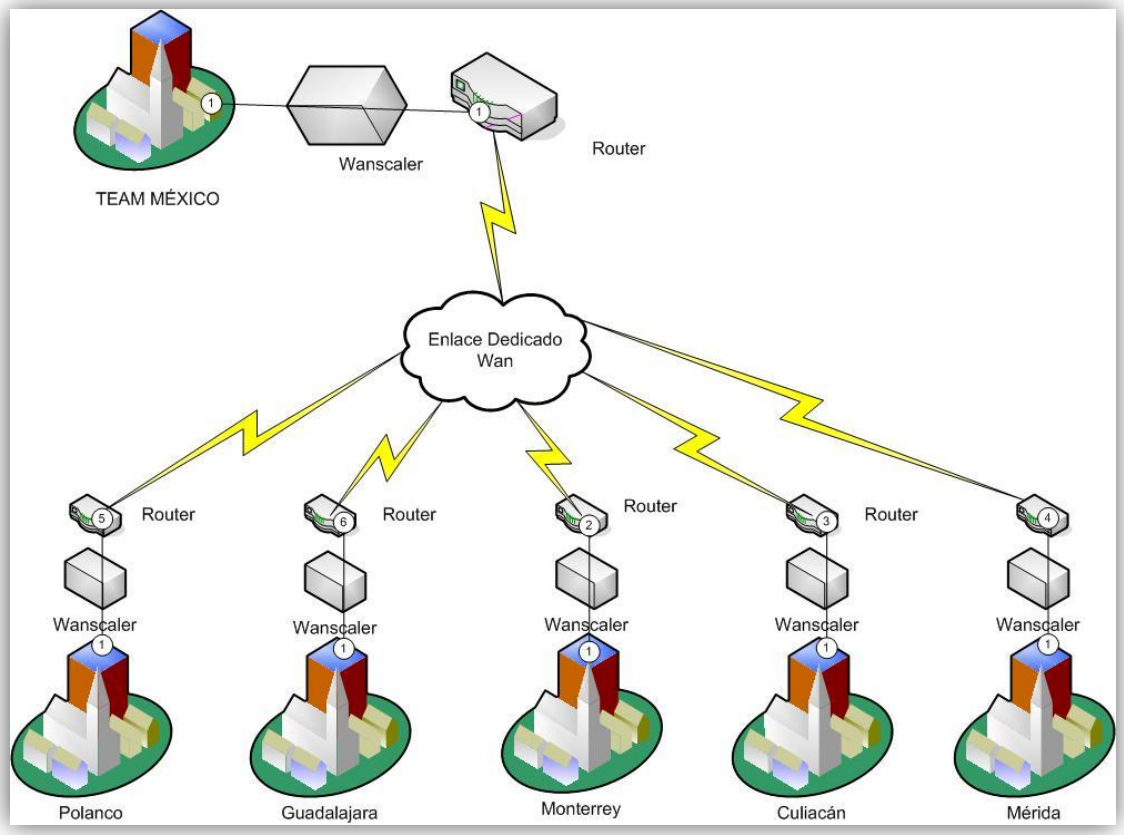


Figura I.5 Esquema WAN TEAM

En el esquema de la figura I.5 se ejemplifica la forma de interconexión WAN de las sucursales, por medio de aceleradores Wanscaler, routers y el enlace dedicado.

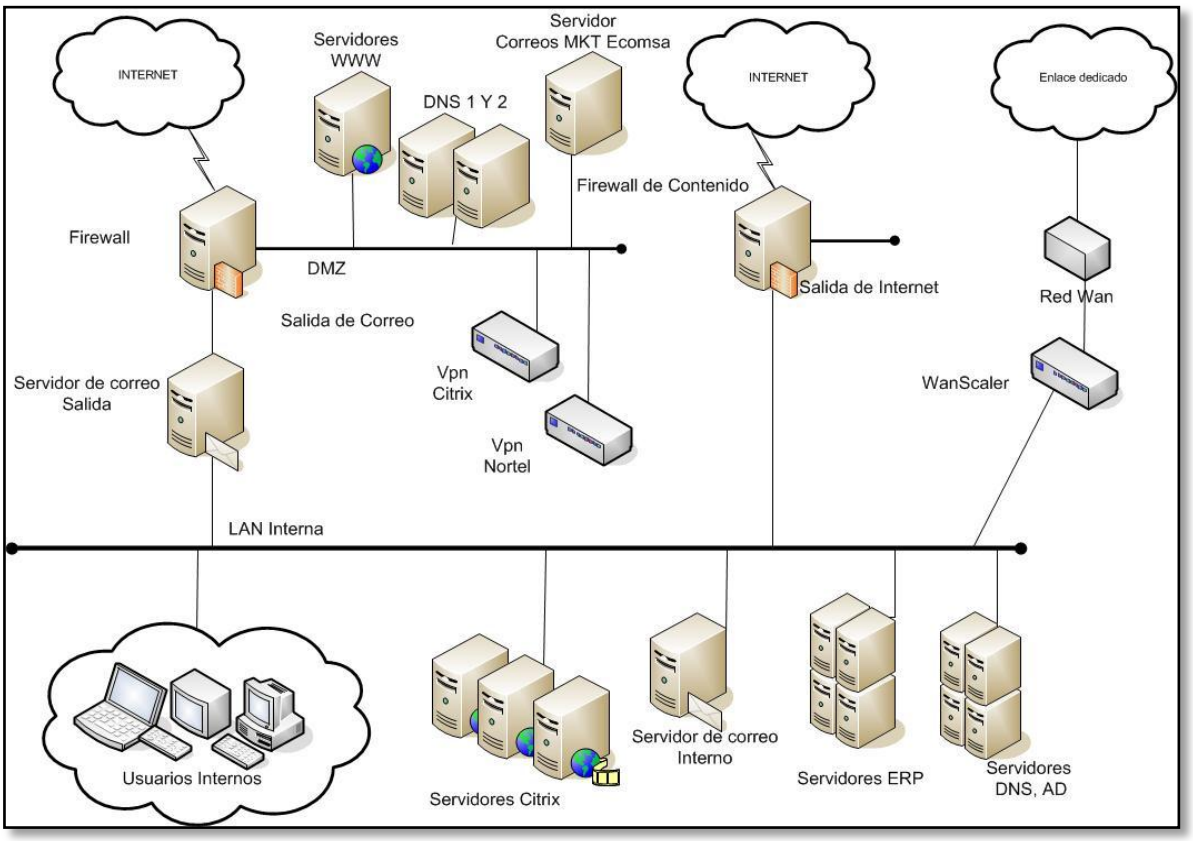


Figura I.6 Esquema VPN TEAM

La figura I.6 muestra la red general, la interconexión y la configuración de las VPN'S con las que se cuentan tanto la de Citrix como la de Nortel, así como la interconexión a la red interna TEAM.

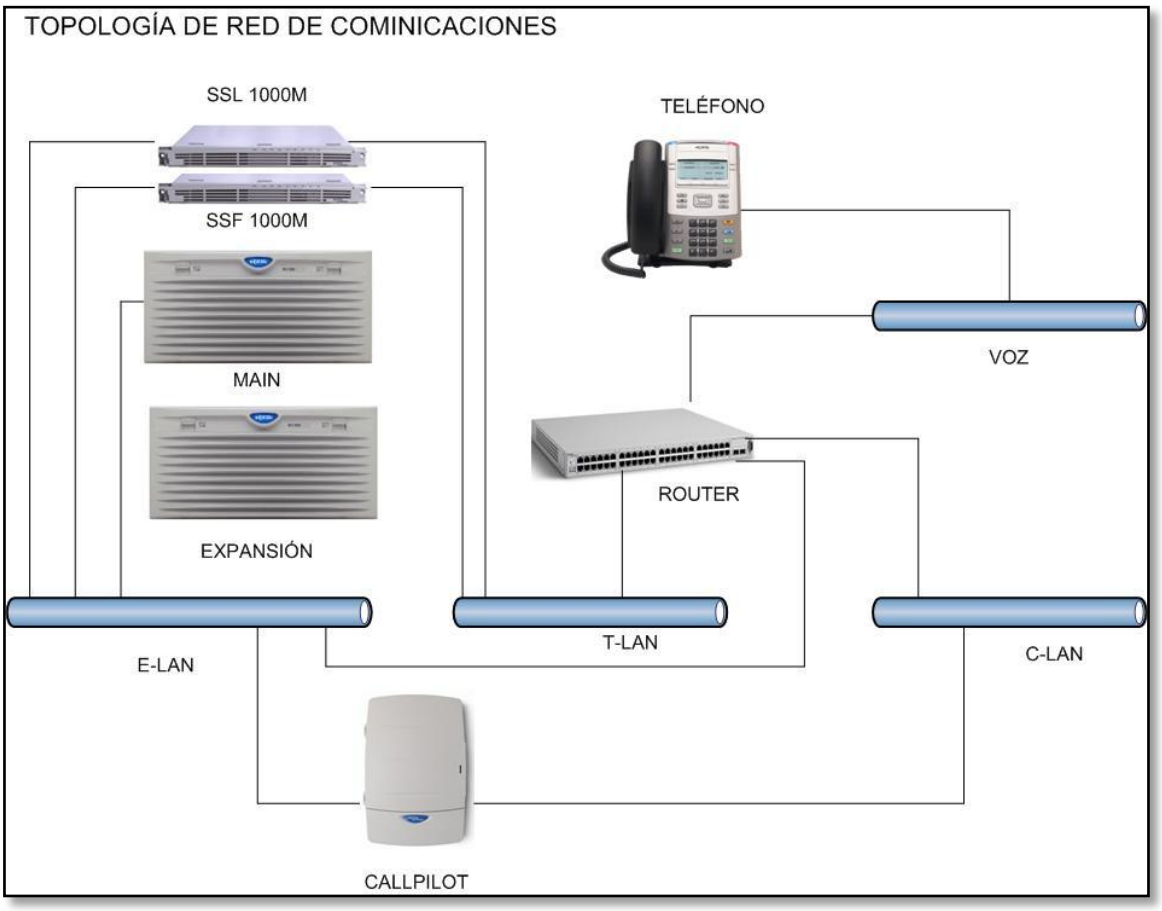


Figura I.7 Esquema General de Comunicaciones

En la figura I.7 se observa la forma en que se compone la infraestructura de comunicaciones basada en un plataforma Nortel, por medio de distintas VLAN'S, conmutadores, routers, buzón de correo y switches hasta llegar a los teléfonos de base o softphones.

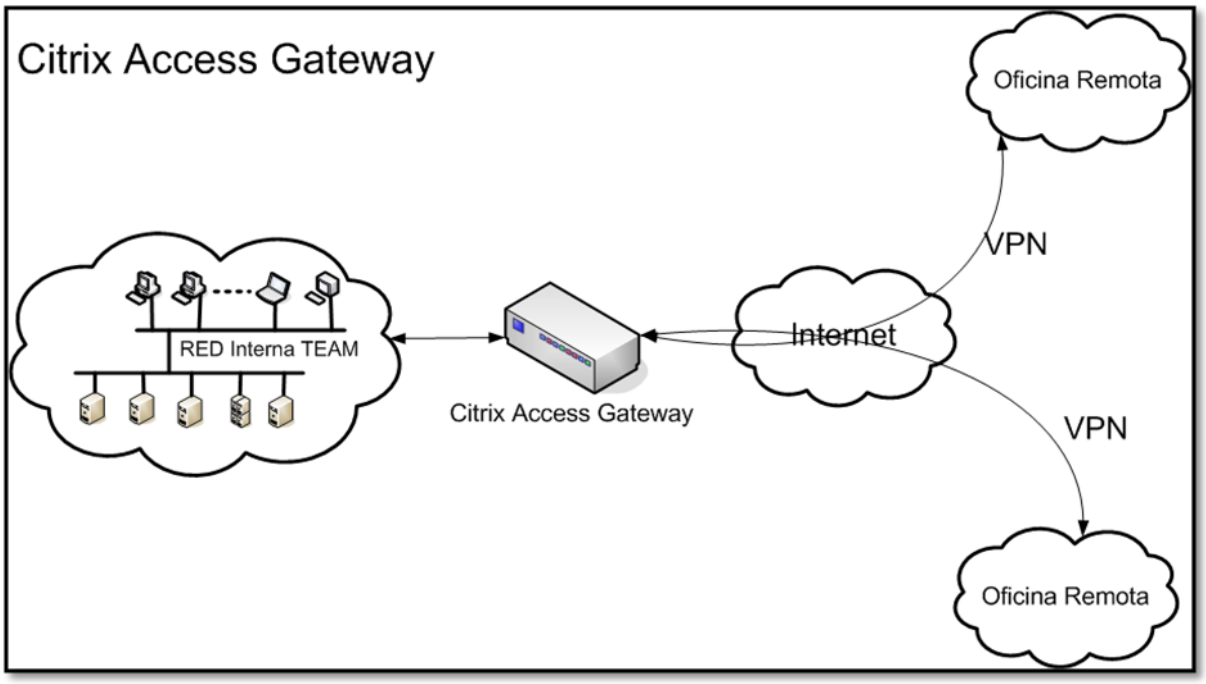


Figura I.8 Esquema Citrix Access Gateway

La figura I.8 mostrada en la parte superior permite observar la interconexión de Citrix Access Gateway con la red interna y su salida vía internet para poder acceder a la red TEAM.

1. TECNOLOGÍA ESPECIALIZADA ASOCIADA DE MÉXICO

La empresa en la que actualmente trabajo está dedicada 100% a las tecnologías de la información y el cómputo, tiene como principal objetivo la integración de soluciones de tecnologías de la información y comunicaciones.

La empresa TEAM fue fundada en 1981, desde entonces integra al mercado de las TIC a través de canales de distribución. Hoy se cuenta con seis oficinas desde la cuales se brinda servicio a todo el país: México Valle, México Polanco, Monterrey, Culiacán, Mérida y Guadalajara.

Actualmente, el core del negocio está basado en la integración y venta de soluciones de plataforma de tecnología de información que permiten atender cualquier requerimiento de distribuidores de hardware, casas de software y desarrolladores e integradores de sistemas que permiten, a su vez, satisfacer las necesidades de los clientes finales.

Estas soluciones están agrupadas, por sus características, en cinco negocios: Infraestructura, Diseño e Impresión, Document Imaging, Comunicaciones y Servicios TIC.

Contamos con alianzas estratégicas con las empresas más destacadas en el mercado de TIC, tales como: HP, HP Índigo, Autodesk, Kodak, Nortel, Oracle, Microsoft, Citrix, Quest, Symantec, Red Hat, Adobe, OCÉ, Corel, Readsoft, Laserfiche, Advantage Security y Dataproducts.

Visión TEAM

Ser el mayorista de elección del canal y de los fabricantes de tecnología de información gracias a que:

- Ofrecemos una integración completa en soluciones e información.
- Gracias a que buscamos la permanencia, desarrollo y evolución de nuestros socios a través de una especialización y enfoque de negocio.
- Gracias a que tenemos una relación íntima de colaboración y aprendizaje mutuo para aumentar el éxito de nuestros negocios.
- Gracias a que hacemos que los negocios sean más fáciles.
- Contamos con capacidades técnicas y financieras para apoyar los negocios del canal y cumplimos con nuestros compromisos de pago con los fabricantes.

Misión TEAM

Nuestra Misión es desarrollar e integrar canales de TI.

Propuesta de Valor

- Desarrollarte en cualquiera de los negocios en que TEAM ha apostado.
- Productos y soluciones que tienen un ciclo de venta corto y que apoyan tu flujo de efectivo.
- Capacitar y entrenar a todo tu personal comercial y técnico.
- Productos de canal cerrado que te permitan competir con menos jugadores.
- Relacionarte con ISV´s con los que puedes generar nuevos negocios.

Recursos Dedicados

- Equipo y software de demostración para ser utilizado en demostraciones ante el usuario final o para la capacitación de los distribuidores.
- Disponibilidad inmediata de productos.

Área de proyectos para el registro y seguimiento de leads de gobierno e iniciativa privada.

Contar con nuestra nueva página Web TEAM, esta gran herramienta de trabajo te facilitará en mucho tus actividades diarias, todos los días en cualquier lugar del mundo y que podrás utilizar para generar negocio debido a su gran contenido estratégico de información.

Soporte Técnico y Comercial

- Nuestras mesas de configuraciones tanto de Servidores como de Seguridad te permitirán responder de manera rápida y eficiente a los requerimientos de tus clientes.
- Técnicos calificados para apoyarte en el proceso de preventa
- Gestionar precios y apoyos para tus proyectos ante los fabricantes correspondientes
- Benchmarks y apoyos en el proceso de pruebas de licitaciones

Generación de Demanda

- Publicar en el portal de TEAM las soluciones y productos que representas
- Utilizar el portal de TEAM para que realices comunicados y promociones exitosas a tus clientes
- Programas comerciales que te permitan atacar con éxito segmentos específicos de mercado
- El área de Servicios Financieros te apoya para otorgarles crédito a tus clientes y puedas realizar tus ventas de una manera más fácil.

Dentro de la empresa Tecnología Especializada Asociada de México S.A de C.V, desempeño un gran número de actividades, siendo mi actividad principal la administración de la infraestructura de TI y comunicaciones, dentro de mis labores se encuentra que la plataforma de correo electrónico, servicios de red, VPN´s, conexiones con sucursales, servicios de telefonía, entro otros, se encuentren y funcionen en óptimas condiciones además del aseguramiento tanto físico como lógico de todos estos servicios y su infraestructura.

Otro de los aspectos a mi cargo es la implementación de nuevas tecnologías y servicios basados en los fabricantes que la organización comercializa, esto con la finalidad de mantener a la vanguardia a la empresa y servir todos estos productos en forma de demostración para que el área comercial cuente con más herramientas y apoyo para poder realizar la venta de productos y la integración de proyectos.

También además de mis tareas en el área técnica, desarrollo labores administrativas dentro de los cuales están la supervisión del pago a los proveedores de servicios al área de TI, aprobar salida de equipo para uso interno, crear planes de trabajo para el área, entre otras actividades de esta índole.

Estas a grandes rasgos son las labores que dentro de esta organización desempeño.

2. Proyectos Realizados

Por medio de este capítulo expongo algunos de mis proyectos realizados previamente en la empresa anterior en la que laboré, IKUSI México, tanto como algunos proyectos llevados a cabo en la empresa Tecnología Asociada de México S.A de C.V anteriores al proyecto de seguridad que implementé y que describo en este Informe.

A continuación se describen algunos de estos proyectos que forman parte de mi experiencia profesional.

2.1 Diseño, implementación y administración de Servidores bajo Windows Server 2003, SQL Server, Active Directory para institución financiera.

Dentro de este desarrollo realicé la implementación de 2 servidores con sistema operativo Windows Server 2003 y los roles de Active Directory, conjuntamente con una base de datos sobre SQL Server, lo que se realizó fue la integración de esta plataforma con un sistema de tarjetas inteligentes para identificación de empleados, horas de llegada, salidas y accesos a distintas zonas de la organización.

Una vez que lo servidores se encontraban funcionando y en sincronía con el sistema de tarjeta inteligentes, de acuerdo con los empleados que ya se encontraban laborando, se dieron de alta dentro de los usuarios en la base de datos y se les asignaron ciertos privilegios conforme la organización lo solicitó.

Cuando todo se encontraba funcionando de forma óptima se realizó la migración a las oficinas del cliente y capacité al encargado en la administración básica del sistema.

2.2 Cálculo y planteamiento de distancias máximas en el diseño de radio enlaces y cableado estructurado

Para la realización de este proyecto relacionado con sistemas de video vigilancia a lo largo del Estado de México, me fue requerido el planteamiento y cálculo de las distancias máximas donde se encontrarían cada radio base para poder brindar el servicio de video vigilancia.

Por medio de software de geo-posicionamiento y utilizando una serie de fórmulas de acuerdo a la frecuencia y estándares utilizados logre determinar cuáles serían los mejores puntos para llevar a cabo la instalación de estas radio bases.

Una vez contando con estos datos la parte de ingeniería se encargó de realizar las instalaciones y pruebas necesarias.

2.3 Implementación y soporte de servidores Linux Red Hat Entreprise con aplicaciones aeroportuarias

Por medio de este proyecto realicé la implementación y soporte de servidores bajo la plataforma Linux Red Hat Enterprise, los cuales tenían que proporcionar servicios que incluían un Sistemas de información al Público (SIP), Megafonía y Sistemas de facturación de vuelos.

Mi trabajo consistía en realizar el levantamiento de los servidores con el sistema operativo antes mencionado y una base de datos Oracle, realizar ciertas configuraciones para que el sistema aeroportuario pudiera ser instalado, después era necesario realizar la instalación paso a paso según lo indica el fabricante.

Una vez instalado el sistema, se migran las configuraciones correspondientes dependiendo el cliente y se hacen algunas configuraciones especiales, teniendo todo esto se realizan pruebas de conexión con los endpoints.

Si lo endpoints respondían y realizaban las tareas para los cuales fueron configurados, se personalizaban algunos elementos que serían visualizados por el cliente y se llevaba a cabo la puesta en marcha en el aeropuerto correspondiente.

Una vez con el sistema instalado y en funcionamiento, hacia entrega de manuales de carga y administración de vuelos, así como la capacitación al área del aeropuerto encargada de estas tareas.

2.4 Diseño y desarrollo de propuestas técnicas para la implantación de Sistemas Aeroportuarios

Dentro del área de consultoría e integración de proyectos, una de mis actividades era la de generar propuestas técnicas especializadas de acuerdo a los requisitos que el área comercial me solicitaba dependiendo de cada cliente y aeropuerto.

Contando con los requerimientos del cliente o la idea básica de este, realizaba la proyección y planteamiento de un sistema integral que cubriera las expectativas del cliente, este era revisado conjuntamente por el cliente y área comercial para acotar los requerimientos, una vez contando con esta retroalimentación realizaba la integración de los sistemas ya con todos los datos obtenidos. Después se le presentaba al cliente un documento con los requerimientos técnicos, planos de ubicaciones, costos, etc.

Si el proyecto se firmaba, mi integración pasaba a las distintas áreas de ingeniería encargadas de la implementación.

2.5 Soporte de servidores Nextiva Verint

Nextiva Verint es un sistema de video vigilancia integral que incluye herramientas de análisis inteligente de video, dentro de este proyecto estaba encargado de dar soporte a este tipo de servidores que corrían bajo un sistema operativo Windows Server 2003, era frecuente que ciertas cámaras por el mal tiempo perdieran la conexión o perdieran la configuración, mi labor en este proyecto era la de administrar este sistema con las peticiones que el cliente realizara en cuestión de configuración, aplicaciones avanzadas que el usuario no tenía acceso así como de asegurar que todas las cámaras estuvieran activas y funcionando a la perfección, estas labores se realizaban en el sitio del cliente debido a las políticas de seguridad establecidas por este.

2.6 Integración y diseño de Data Centers

Desarrollé la planeación e integración de sistemas para Data Center, cuando un integrante del área comercial tenía el requerimiento de un cliente, este pasaba a mi área donde se desarrollaba la propuesta técnica en cuestión de centro de datos, se hacían una serie de revisiones hasta que el cliente firmaba el proyecto o en otro caso se perdía el proyecto.

Una vez que el cliente aceptaba esta integración se pasaba a los especialistas de cada área para llevar a cabo su implementación.

2.7 Presentación, Diseño e Implementación de sistemas Digital Signage

Por medio de este proyecto se creó el área de Digital Signage dentro de la empresa Ikusi México en la que laboraba, por lo cual me tocó desarrollar desde el análisis de las soluciones existentes en el mercado, búsqueda de clientes potenciales, diseño de estrategias y herramientas de ventas para apoyo al área comercial.

Dentro de la parte técnica, una vez ubicadas las que consideramos las mejores soluciones, se desarrollaron Demos conjuntamente con el fabricante para ofrecer la solución que más se adaptara a los clientes y que pudieran costear.

Me encargué de desarrollar las maquetas en el laboratorio de la empresa y conocer todos los aspectos técnicos de cada solución, cuando el área comercial nos entregaba oportunidades, realizaba la propuesta técnica con la solución que más se adaptara a los requerimientos del cliente, la propuesta era revisada hasta lograr concretar el proyecto.

2.8 Desarrollo e integración de propuestas técnicas y económicas para proyectos, involucrando diversas tecnologías

Como consultor integrador, mi labor era la de desarrollar propuestas técnicas y económicas para los distintos proyectos que me eran asignados, los proyectos podían contener un sin número de requerimientos con distintas tecnologías como seguridad física y lógica, video vigilancia, sistemas de despliegue de audio y video, sistemas de control de acceso, hospitalidad, redes, infraestructura, comunicaciones, etc. Conjuntamente con los especialistas de cada tecnología se realizaba la integración del proyecto, se obtenían costos y descuentos, y una serie de puntos extras que eran entregados al cliente.

2.9 Administración de portal web bajo la plataforma DotNetNuke

El objetivo de este proyecto fue la actualización del portal de la organización debido a tenia cerca de 1 año sin contar con nuevo contenido, dentro de este proyecto realicé la programación de nuevos templates, inclusión de nuevas marcas, generación de usuarios, instalación de plug-ins para contar con reportes acerca del tráfico de usuarios, páginas con mayor número de visita y otras cuestiones estadísticas, renovación de logos, creación de nuevas páginas y la integración con el e-commerce.

2.10 Instalación y administración de servidor y portal web bajo la plataforma Joomla

Dentro de este proyecto, se renovó completamente el portal web de la organización, las tareas que desarrollé para este proyecto fueron desde el levantamiento del servidor basado en Linux Cent OS, instalación de todas las herramientas necesarias como son bases de datos, servidor web, servidor ftp, CMS Joomla, además de llevar a cabo un esquema de seguridad bajo el cual estaría el servidor y sus aplicativos.

Una vez contando con el portal activo realicé la puesta a punto, generando usuarios, asignado permisos al servidor para contenido, ftp, entre otros.

3. IMPLEMENTACIÓN DE POLÍTICAS, CONFIGURACIONES, APLICACIONES Y ADMINISTRACIÓN PARA LA SEGURIDAD INFORMÁTICA DE LA EMPRESA

3.1 ANÁLISIS

A continuación presento una breve descripción y llevo a cabo una revisión la cual corresponde al esquema general de seguridad, donde se muestran las implementaciones existentes dentro de la empresa para el aseguramiento de la seguridad informática.

- Seguridad de la información en la red de datos

La forma en que la infraestructura de redes y seguridad está diseñada para brindar los servicios de datos en la organización es la siguiente:

Existe una acometida con 4E1 la cual se distribuye hacia el Firewall principal de tráfico y contenido, el cual cuenta de la acometida con una dirección homologada y entra a la red LAN con una IP interna, con la cual por medio de esta conexión se lleva a cabo la trasferencia de información de una forma protegida. Esta mediación brinda seguridad entre la LAN y el mundo exterior protegiendo, los servicios, aplicaciones e información de la empresa.

- Seguridad del correo principal de la empresa

Para la infraestructura de servicio y seguridad de correo, el diseño está generado de forma que de la acometida de 1E1 accede a un Firewall de tráfico de correo, que recibe una IP homologada y sale a través de una IP interna, el cual se conecta a la LAN de la organización y tiene contacto con el servidor de correo Front-end, encargado de recibir las peticiones y enviárselos a los servidores de correo Back-end los cuales contienen las bases de datos: uno de estos servidores almacena la información en su propio disco y el otro tiene conexión a una SAN. Para brindar una mayor seguridad a la salida y recepción en la nube se cuenta con un servicio de hosteo Message Lab por Symantec el cual brinda protección anti-spam, antivirus, firewall y otros servicios de monitoreo, esto ofrece una mayor confiabilidad, integridad y disponibilidad.

- Políticas de seguridad

No existen políticas escritas, se carece de un documento que contenga reglas, normas bien claras y establecidas, basadas en estándares y perfectamente acotadas a las necesidades de la organización.

Los procedimientos y estrategias de seguridad no se encuentran plasmados en algún documento, se carece de directrices y recomendaciones que orienten en el uso adecuado de las tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresa.

En este sentido, las Políticas de Seguridad Informática, surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos, pues permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

- Firewalls (appliances)

Los firewalls están configurados de forma automática, casi configurados por default o con pocas reglas de administración, lo cual brinda una seguridad casi nula o muy poca a la infraestructura de datos y comunicaciones de la empresa.

Por ser firewalls de tipo appliance tienen grandes atributos los cuales con una correcta administración pueden ser explotados de una mejor forma, en el área de permitir, limitar, cifrar y descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

- Firewall de tráfico y contenido (software)

Firewall de tráfico y contenido no se encuentra en constante monitoreo y actualización, aunque se está administrado se podría sacar mayor provecho de todas sus características y conexiones con otro tipo de software de monitoreo y detección de fallas, a fin de brindar un mejor servicio además de asegurar la protección y mejorar la productividad del personal de la organización.

- Dominio Empresarial

La administración del dominio, dentro del directorio activo la información no se encuentra perfectamente actualizada y algunas cuentas sólo están desactivadas, cuentas de personal que ya no labora en la organización y que podrían hacer mal uso

de sus privilegios. La baja y modificación de las cuentas no se encuentra depurada lo que, en un momento dado, puede ser una amenaza a la integridad de la organización, ya que puede surgir algún ataque por parte de personal que alguna vez laboró dentro de la empresa o pueden ser utilizadas esas cuentas por parte de un externo para por este medio realizar algún ataque dejando rastros mínimos.

- Actualización de parches de seguridad

Existen prácticas de actualización, en la mayoría de los servidores se encuentran bien administradas las actualizaciones, parches de seguridad, etc. Pero por parte de los usuarios no existe la cultura de actualización, así como para cada servidor es muy importante realizar una protección exhaustiva por este medio, también es necesario realizar la correcta actualización de cada una de las aplicaciones de correo y servicio de cada servidor ya que las intrusiones, pérdida o robo también se podrían dar por la mala administración de las aplicaciones que llegan al usuario.

El conocer que existen distintos tipos de parches para preservar y mantener una mayor productividad y seguridad es muy importante para llevar a cabo su implementación.

- Parches de depuración

  El objetivo de este tipo de parches es reparar bugs, o errores de programación que no fueron detectados a tiempo en la etapa de desarrollo. Cuando un programa tiene una alta probabilidad de contener este tipo de errores se le llama versión beta.

- Parches de seguridad

  Este tipo de parches solucionan agujeros de seguridad siempre que es posible, no modifican la funcionalidad del programa. Los parches de seguridad son especialmente frecuentes en aplicaciones que interactúan vía web.

- Parches de actualización

  Consiste en modificar un programa con el objetivo de incorporar metodologías recientes. Por ejemplo, optimizar en tiempo cierto programa, utilizar algoritmos mejorados, añadir funcionalidades, eliminar secciones obsoletas de software, etc.

- Análisis de incidentes e historiales de seguridad

La carencia de un monitoreo de seguridad así como ataques o amenazas detectadas hacen y ponen en gran riesgo a la organización. El perfecto conocimiento del entorno y las amenazas proporcionan mayor certeza acerca de cómo protegernos ante los problemas que pueden acechar a la organización y así plantear e implementar una correcta estrategia de protección.

El análisis de estos historiales también ayudan en caso de alguna falla para llevar a cabo medidas correctivas y realizar análisis forense que nos ayuden a determinar las posibles causar y corregir estos errores, agujeros de seguridad, etc.

- Controles de acceso

Los controles de acceso físico a zonas importantes como los Data Centers de la organización se encuentran muy limitados, aunque la zona es restringida y el personal que tiene acceso es limitado, llegado algún atentado o ataque las posibilidades de irrupción son muy altas, por lo cual no se cuenta con una alta fiabilidad en la parte de la seguridad física para la infraestructura.

- Contraseñas

Las contraseñas de servidores y aplicaciones, son previsibles, con una estructura poco robusta que no cumple estándares, normas o buenas prácticas de generación, además de que estas contraseñas, son muy antiguas y no han sido renovadas. Asimismo el 90% de los servidores de la organización cuenta con una misma contraseña de acceso para su autenticación lo cual trae consigo serios problemas de seguridad ya que una autenticación débil por este medio, crea inconvenientes fáciles de vulnerar.

- Contraseñas de usuario

Las contraseñas de usuarios generadas en toda la organización llevan un patrón al ser creadas, el cual puede ser descifrable de forma sencilla, además de no cumplir con las principales normas conocidas con respecto a la formación de claves robustas.

- Configuración de Servidores

Al realizar el levantamiento de nuevos servidores y generar su configuración, son puestos en operación con una configuración básica de seguridad, con actualizaciones, Service Pack, antivirus y algunos otros pasos a seguir para contar con cierta

seguridad, sin embargo cabe destacar que se trata de una configuración de seguridad estándar, por lo que no se cuenta con un Hardening específico según las aplicaciones, tráfico, o servicios para lo que está destinado.

- Seguridad en los sistemas de telecomunicaciones

El acceso a los sistemas de comunicaciones, switches, conmutador, se encuentra ampliamente desprotegido ya que la mayoría de estos equipos están configurados con claves de acceso con los que fueron creados en el momento de su manufactura y que en el instante que estos salen a producción debieron de haber sido cambiados pero hoy en día aún conservan esta forma de autenticación.

- Seguridad en los sistemas de correo electrónico

La seguridad en los servidores de correos que no son los dominios de correo principales de la empresa, pero que también son muy importantes para la productividad y la forma de operar de la organización se encuentran desprotegidos, se genera mucho Spam y puede ser una fuerte problemática para toda la red ya que por este medio podrían estar accediendo muchos ataques.

- Configuración de cuentas

La mayoría de las cuentas se encuentran configuradas para que no caduquen lo cual genera graves conflictos de seguridad para la organización, además, existiendo una considerable rotación de personal, la seguridad se ve mermada. Éste es un problema grave que se debe resolver de inmediato ya que los ataques internos, como se ha dado a conocer, en muchas ocasiones son una de las grandes amenazas para la seguridad empresarial.

- Configuración WLAN

Dentro de este aspecto se encuentran dos grandes inconvenientes contra la seguridad de la organización, ya que la configuración del acceso a la red vía Wireless está dividida en dos: una para el acceso del personal de la organización el cual autentica a los usuarios por medio de Mac-Address, y otra que es para uso exclusivo de visitantes, el cual se utiliza para cursos a externos, juntas, presentaciones con clientes, canales y foros entre otros. Pero la forma en que ésta se autentica es por medio de usuario y contraseña vía un navegador web, pero la contraseña que se maneja es una muy obvia sin ninguna consideración de las normas para la generación de una contraseña robusta, otro de los problemas que se encuentra en este aspecto, es que la división para visitantes, en este instante cuenta con acceso a toda la red lo

cual genera un alto riesgo de seguridad ya que remotamente se pueden llevar a cabo ataques de forma sencilla siendo muy difícil la identificación de la fuente.

3.2 DISEÑO

A continuación se presenta la forma en que, de acuerdo al análisis previo del estado actual de la seguridad informática de la empresa, Tecnología Especializada Asociada de México, se diseña la estrategia a seguir para realizar la implementación que resguarde los activos lógicos de la empresa de forma que asegure la continuidad del negocio, que dé tranquilidad a los usuarios, pero que no entorpezca la actividad del personal que labora en la organización.

Para llevar a cabo la implementación se hace un esquema de las actividades a realizar, se define de forma breve lo que se llevará a cabo en cada actividad y se clasifican las acciones de acuerdo a los tópicos de análisis, implementación, configuración y administración.

3.2.1 Actividades a realizar para el aseguramiento de la información

1. Generación de Políticas de Seguridad para contraseñas
2. Configuración de Firewalls (appliances)para aplicaciones demo
3. Configuración y administración de Firewall de Contenido (software)
4. Administración de Dominio Empresarial
5. Actualización de Parches de Seguridad
6. Generación y cambio de contraseñas de sistemas de información y comunicaciones
7. Generación y cambio de contraseñas de usuarios
8. Configuración y aseguramiento de servidores
9. Configuración de seguridad de los sistemas de comunicaciones
10. Instalación y configuración de la consola de administración Symantec Endpoint
11. Configuración del servidor de web TEAM dentro de la red Interna
12. Actualización de Mac Address para la autenticación web de la WLAN
13. Actualización de cuentas generadas para VPN Nortel

3.2.2 Definición de las actividades a realizar

1. Generación de Políticas de Seguridad de Contraseñas

Realización de un análisis, generación e implementación de un documento que en términos generales indique lo que está y no permitido, además de plantear la forma en que las contraseñas deben generarse y resguardarse dentro de la organización.

Realizar una serie de normas, reglamentos y protocolos a seguir, donde se definan medidas para proteger la seguridad del sistema y la forma en que los usuarios interactúan con la tecnología, siempre hay que tener en cuenta que la seguridad comienza y termina con el personal de la organización.

Las políticas de seguridad informática sobre contraseñas a implementar deben de cubrir todos los aspectos posibles a resguardar y contar con el conocimiento e interacción del personal de la organización, las políticas estarán realizadas acorde a las necesidades y recursos con los que cuenta la empresa, las normas y protocolos deben ser atemporales y generales pero perfectamente adaptadas a la organización.

Las políticas efectuadas se diseñarán con base en resguardar, brindar y mantener los servicios de seguridad informática: Integridad, Disponibilidad, Privacidad, Control de Acceso, No repudio y Autenticación. Las políticas instauradas serán una definición de lo que se va a proteger, cómo vamos a realizarlo y de que forma el personal de la organización debe interactuar para lograrlo.

2. Configuración de Firewalls (appliances) para aplicaciones demo

Llevar a cabo la configuración de acuerdo a los manuales de implementación para tener conexiones seguras, bloqueo de puertos, redireccionamiento de IP´s y puertos lógicos, control de tráfico, entre otros.

Se encuentran dos firewall de este tipo a lo largo de la organización, uno será configurado para brindar seguridad y redireccionamiento de IP´s a la página web TEAM que es una parte vital para la organización y el otro será utilizado para proteger los aplicativos demos que el equipo comercial utiliza vía remota en presentaciones con clientes.

3. Configuración y administración de Firewall de Contenido (software)

Dentro del servidor de Firewall de contenido, en ésta aplicación realizar configuraciones avanzadas de gestión de contenido, control de tráfico y aplicaciones de entretenimiento que no corresponden a las actividades laborales, así como revisión de los logs de seguridad, intentos de intrusión y balance de actividades. Configurar la entrega de reportes semanales de actividades en la red por parte de los usuarios, en lo que a partir de estos reportes se creen estadísticas de aplicaciones y equipos de mayor riesgo y mal uso de los sistemas.

4. Administración de Dominio Empresarial

Crear una relación del personal actualmente laborando en la empresa, entrar en contacto con los encargados correspondientes en las distintas sucursales para hacer dicha relación, tomar sus datos y puesto en la organización, y a partir de esta información crear la base de usuarios actualizada en el dominio con toda la información fundamental en cada cuenta.

También, en la configuración del Directorio Activo cambiar la característica que indica que las cuentas nunca caducan, lo cual genera un directorio no actualizado y con cuentas de riesgo en el sistema, por este medio es más factible identificar a los integrantes actuales de la empresa.

5. Actualización de Parches de Seguridad

Hacer una recopilación de sistemas operativos, aplicaciones y software implementado y buscar e instalar las actualizaciones más recientes y los parches de seguridad lanzados actualmente, con la finalidad de evitar agujeros de seguridad, vulnerabilidades debido a software desactualizado y bugs en las aplicaciones.

6. Generación y cambio de contraseñas de sistemas de información y comunicaciones

Se generarán nuevas contraseñas para los servidores, appliances y dispositivos de la infraestructura de datos y comunicaciones de la empresa, que cuenten con normas, criterios y buenas prácticas para la creación y establecimiento de contraseñas robustas que dificulten la intrusión y las amenazas de ataques a la organización.

Las contraseñas a los sistemas antes mencionados serán cambiadas trimestralmente para poder así contar con contraseñas actualizadas y evitar que aunque sean robustas puedan llegar a ser conocidas.

7. Generación y cambio de contraseñas de usuarios

Se crearán nuevas contraseñas para todos los usuarios integrantes de la empresa, que cuenten con normas, reglas y buenas prácticas para la creación y establecimiento de contraseñas robustas que dificulten la intrusión y las amenazas de ataques a la organización por medio de la cuenta de algún usuario con accesos diversos.

Las contraseñas para los usuarios serán cambiadas cuatrimestralmente para poder así contar con contraseñas actualizadas y evitar que aunque sean robustas puedan llegar a ser conocidas por personas mal intencionadas.

8. Configuración y aseguramiento de servidores

Realizar un análisis por servidor de las aplicaciones que manejan y los servicios que brindan, así como el sistema operativo que utilizan, con base en esto se realizará el hardening de cada servidor en uso, dependiendo del análisis previamente realizado, y a partir de este punto, cada nuevo servidor implantado en la organización requerirá de este análisis y la realización del hardening correspondiente antes de brindar los servicios para los que fue diseñado.

9. Configuración de seguridad de los sistemas de comunicaciones

Cambiar la configuración de autenticación de acceso remoto y las contraseñas por defecto, de igual forma que en los sistemas de datos por unas más robustas de acuerdo a buenas prácticas y criterios establecidos.

10. Instalación y configuración de la consola de administración Symantec Endpoint

Realizar la instalación de la consola de administración y llevar a cabo una configuración avanzada, de acuerdo a las necesidades de la empresa y de cada área, cuidando el rendimiento de los equipos de cada usuario pero brindándoles una buena seguridad de su información, de esta forma también se limitará el acceso a aplicaciones que merman el desempeño de los equipos y de la red.

11. Configuración del servidor de web TEAM dentro de la red interna

Incluir al servidor web de la compañía dentro de la red interna en lugar de estar en la DMZ y por medio de un Firewall hacer el redireccionamiento de IP´s para proteger el servidor y hacerlo accesible por medio de esté sólo para la visibilidad de las páginas pero sin contar con un acceso a él fuera de la red interna.

12. Actualización de Mac Address para la autenticación web de la WLAN

Hacer una depuración de las Mac Address que alimentan el sistema de autenticación de la WLAN, eliminar todas las cuentas y contando con una nueva base actualizada de usuarios que utilizan la red inalámbrica local y tienen privilegios para hacer uso de la red, se llevará a cabo la inclusión al sistema de la nueva base de Mac Address existentes.

13. Actualización de cuentas generadas para VPN Nortel

Proceder con la eliminación de todas las cuentas actuales de VPN en el sistema y generar con base en una nueva relación de usuarios actualizada tanto de TEAM México como de todas las sucursales, la inserción de las cuentas que realmente deben existir y generar nuevas contraseñas para éstas.

3.2.3 Clasificación de actividades

- **Análisis**

  - Generación de Políticas de Seguridad de contraseñas
  - Análisis, recolección y búsqueda de actualizaciones y de parches de seguridad
  - Análisis de logs de seguridad
  - Análisis para la generación de contraseñas robustas (reglas, criterios, protocolos) de sistemas de información y de comunicaciones.
  - Análisis para generación de contraseñas robustas (reglas, criterios, protocolos) para usuarios de la organización.
  - Análisis de sistema operativo, aplicaciones y servicios brindados por los servidores de la empresa.
  - Análisis de políticas necesarias para el aseguramiento del sistema de correo electrónico

- **Implementación**

  - Implementación de las Políticas de Seguridad de contraseñas generadas
  - Instalación de actualizaciones y parches de seguridad
  - Creación de estadísticas según los logs y los reportes obtenidos.
  - Implantación de nuevas contraseñas en sistemas informáticos y de comunicaciones, según normas y reglas analizadas
  - Institución de nuevas contraseñas para usuarios, según normas y reglas analizadas
  - Aseguramiento de servidores a través de realización de hardening
  - Creación de políticas previo análisis de necesidades para el aseguramiento del sistema de TEAM
  - Instalación de la consola de administración Symantec Endpoint

- **Configuración y administración**

  - Configuración de Firewalls (appliances) para aplicaciones demo
  - Configuración y administración de Firewall de Contenido (software)
  - Administración de Dominio Empresarial
  - Configuración de actualizaciones e instalación de Parches de Seguridad
  - Administración de cambio de contraseñas de sistemas informáticos y de comunicaciones
  - Administración de cambio de contraseñas de usuarios
  - Configuración y aseguramiento de servidores
  - Configuración de la consola de administración Symantec Endpoint
  - Configuración del servidor de web TEAM dentro de la red Interna
  - Actualización de la base de Mac Address para autenticación WLAN
  - Actualización de la base de usuarios de la VPN Nortel

3.3 IMPLEMENTACIÓN

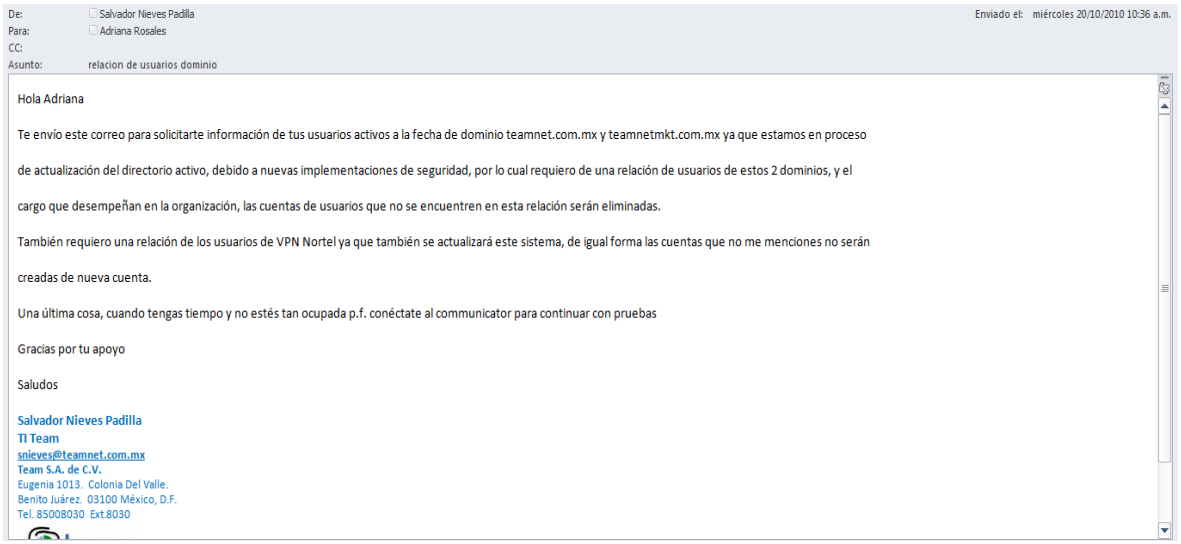
En esta sección se presentan el desarrollo y la ejecución de los aspectos de seguridad estudiados en los puntos anteriores y conforme al diseño se hace la configuración, instalación y administración de las políticas y reglas, software y actualizaciones, entre otros, antes mencionados.

De acuerdo a cada uno de los puntos analizados en donde la organización se encuentra vulnerable, se realizan las implementaciones correctivas, así como también otras implementaciones para contar con una mejora en el aseguramiento de nuestra valiosa información.

3.3.1 Actualización y administración de Dominio Empresarial

Como primer paso para la correcta administración del dominio se lleva a cabo la ubicación de todas las sucursales dentro del directorio, una vez ubicadas, de cada una de las sucursales se toma la relación de usuarios existentes al momento con cuentas activas e inactivas, esta relación es enviada a las sucursales para que con la colaboración del personal de Recursos Humanos y TI, se genere la nueva relación actualizada.

Como estrategia, se toman instantáneas de cada sucursal, sus grupos y sus usuarios, se envía un correo a cada sucursal solicitando la actualización de usuarios. Ver figura 3.1


De: Salvador Nieves Padilla
Para: Adriana Rosales
CC:
Asunto: relacion de usuarios dominio
Enviado el: miércoles 20/10/2010 10:36 a.m.

Hola Adriana

Te envío este correo para solicitarte información de tus usuarios activos a la fecha de dominio teamnet.com.mx y teamnetmkt.com.mx ya que estamos en proceso de actualización del directorio activo, debido a nuevas implementaciones de seguridad, por lo cual requiero de una relación de usuarios de estos 2 dominios, y el cargo que desempeñan en la organización, las cuentas de usuarios que no se encuentren en esta relación serán eliminadas.

También requiero una relación de los usuarios de VPN Nortel ya que también se actualizará este sistema, de igual forma las cuentas que no me menciones no serán creadas de nueva cuenta.

Una última cosa, cuando tengas tiempo y no estés tan ocupada p.f. conéctate al communicator para continuar con pruebas

Gracias por tu apoyo

Saludos

Salvador Nieves Padilla
TI Team
snieves@teamnet.com.mx
Team S.A. de C.V.
Eugenia 1013. Colonia Del Valle.
Benito Juárez. 03100 México, D.F.
Tel. 85008030 Ext.8030

Figura 3.1 Solicitud de relación de usuarios actualizada

Al recibir la relación por parte de cada sucursal, se procede a hacer la actualización dentro del directorio activo y se toma una instantánea fechada para conocer y tener referencia del estado del dominio con la fecha realizada. Ver figuras 3.2 y 3.3.

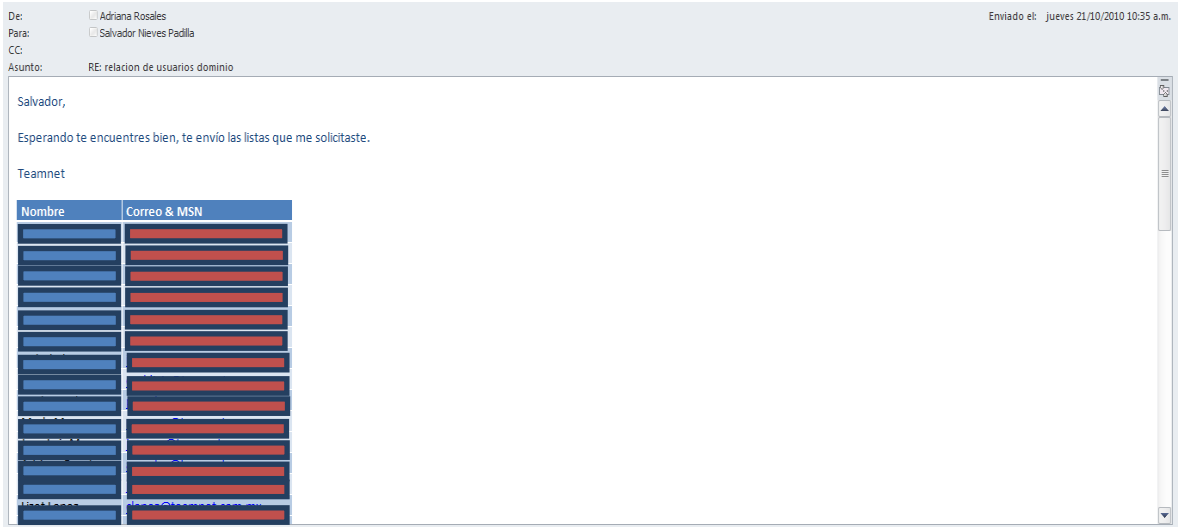


Figura 3.2 Recepción de relación de usuarios actualizada

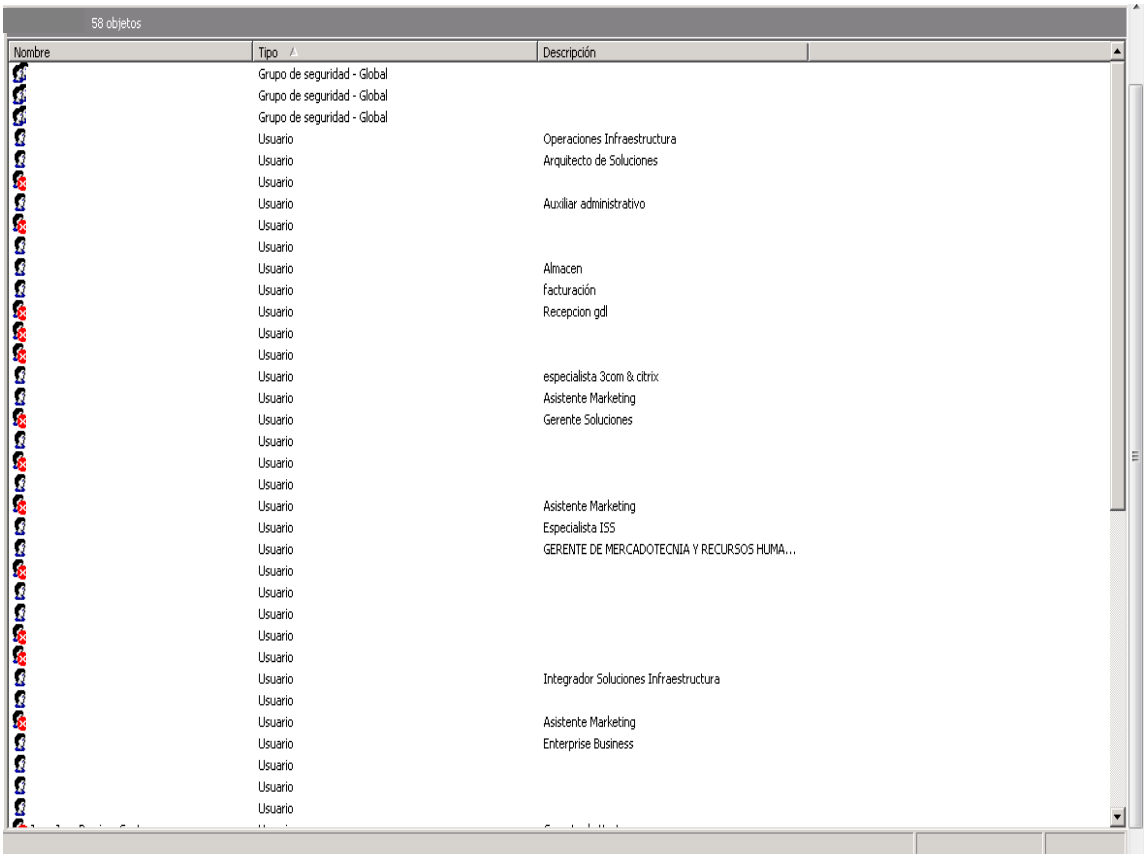


Figura 3.3 Estado del directorio Sucursal C antes de la actualización

Una vez realizada la eliminación de los usuarios inactivos y fuera de la empresa, el estado actual del directorio de dicha sucursal se puede observar en la figura 3.4, que de 58 elementos pasó a ser de 31 lo que indica que existían muchas cuentas que podían resultar una gran vulnerabilidad.

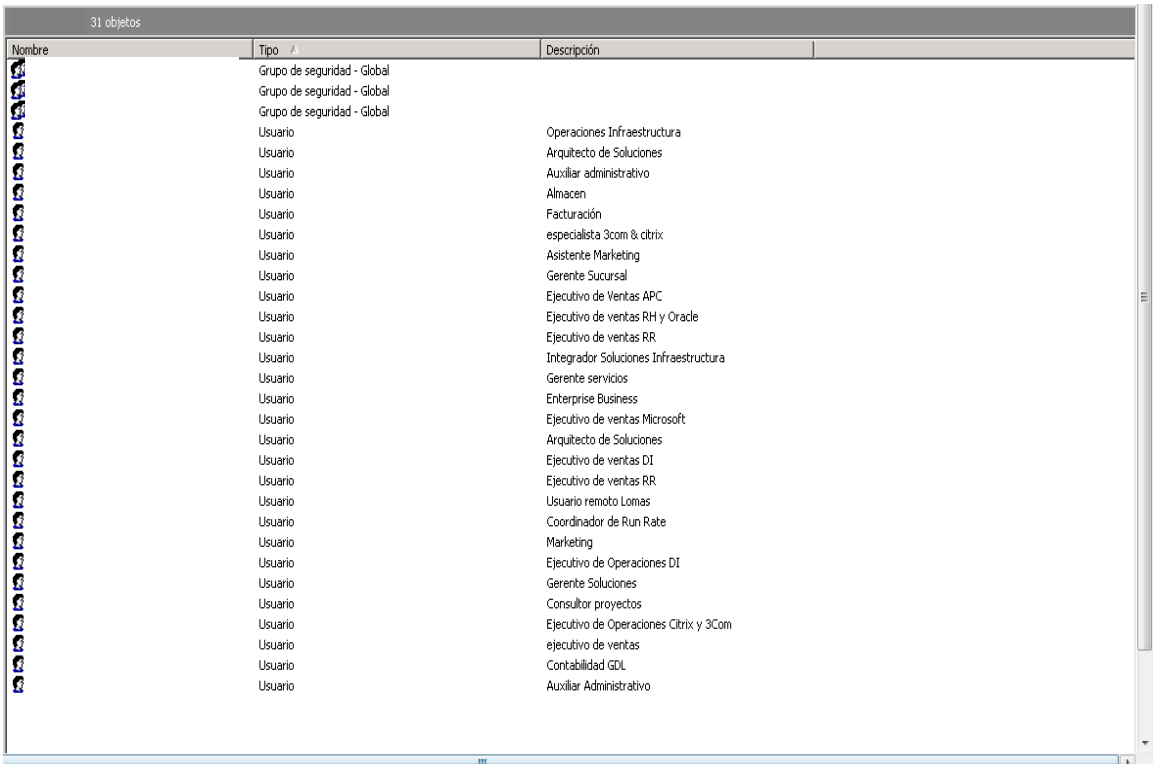


Figura 3.4 Estado del directorio actualizado

De la misma forma se realiza para cada una de las sucursales y para TEAM México, el proceso en esta última toma un poco más de tiempo en su actualización debido al número de integrantes y a que es necesaria la colaboración de otras áreas de la empresa para hacer la correcta eliminación de cuentas, ya que existen cuentas estratégicas que se siguen consultando.

Una vez realizada la actualización y administración del dominio, además de que por este medio se hace menos vulnerable el sistema, de esta forma también se depuró una gran cantidad de espacio en storage gracias a la eliminación de correos asignados a las cuentas que no estaban activas, lo cual optimiza el sistema de correo.

3.3.2 Actualización de cuentas generadas para VPN Nortel

Dentro de esta actualización para las sucursales se sigue la misma temática y pasos que la actualización del directorio activo; se genera una instantánea del estado actual del sistema y a cada sucursal se le es solicitada la información referente a que usuarios mantienen los privilegios de contar con el acceso remoto al sistema por medio de la VPN Nortel.

La diferencia aquí es que toda la base de usuarios en este sistema será dada de baja en día no laboral y restablecida por completo toda la base y sus servicios el lunes siguiente, además, para la actualización de la base de usuarios de la matriz TEAM México, será necesario contar con la relación de usuarios que el gerente de cada área indique que miembros son los que seguirán contando con el acceso a dicho sistema, ya que algunos usuarios sólo fueron autorizados por proyecto o por temporadas.

Contando con la base de usuarios actualizados por medio de una interfaz web accedemos al sistema de administración de la VPN Nortel para realizar la gestión y actualización de cuentas como se muestra a continuación.

Se ingresa al sistema de administración Nortel Networks, para la aplicación Contivity Secure IP Services Gateway, donde se accede a través de la opción Manage Switch. Ver figura 3.5

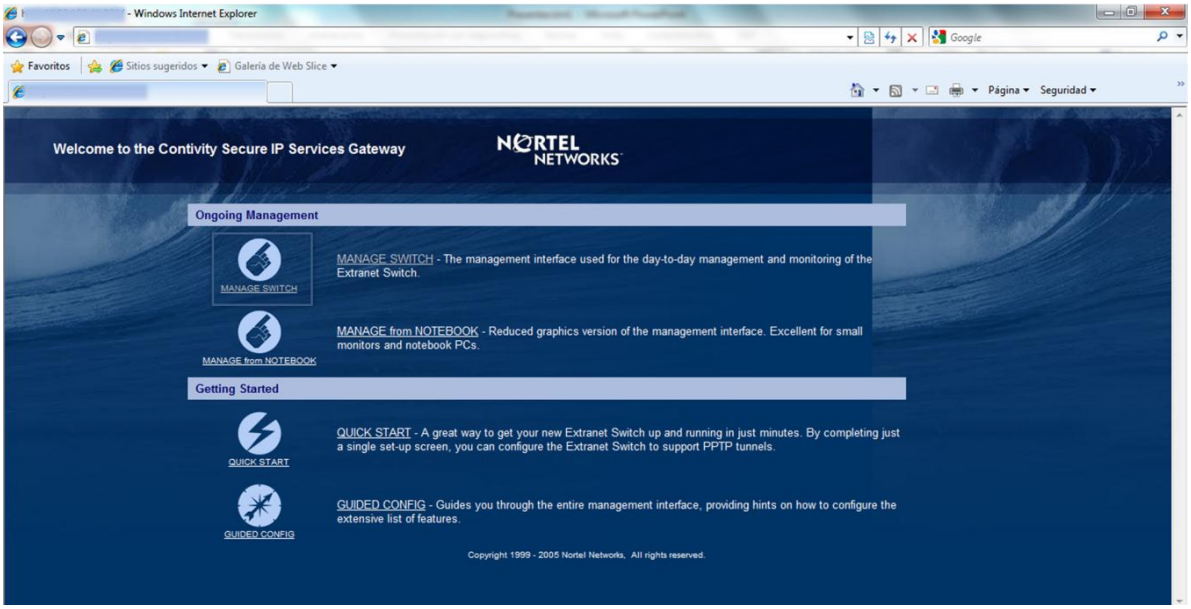


Figura 3.5Acceso a Contivity Secure IP

Se introduce usuario y contraseña para obtener el acceso al sistema de administración.

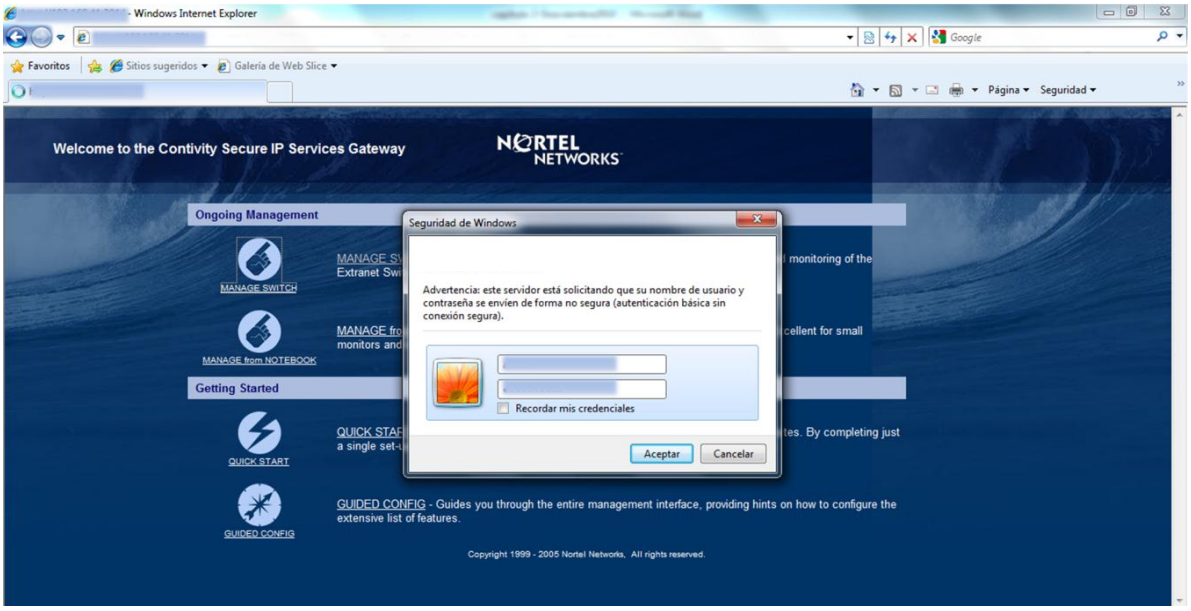


Figura 3.6 Autenticación en el sistema

Esta es la pantalla principal que se muestra al ingresar al sistema y en la parte izquierda se encuentra el menú de operación del sistema.

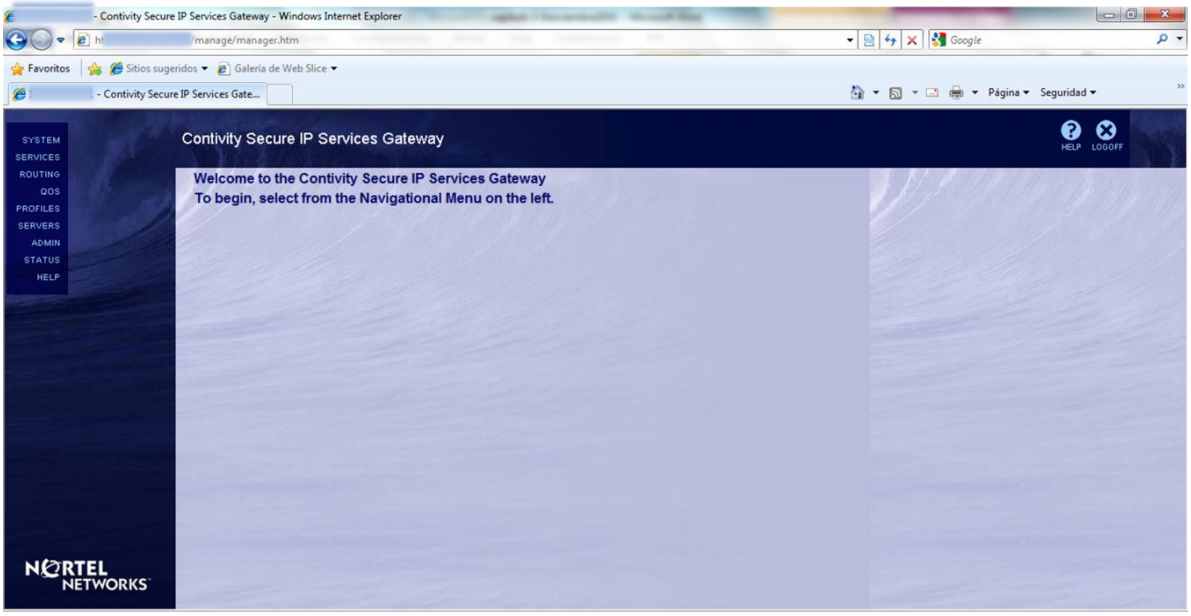


Figura 3.7 Menú Principal

Como siguiente paso para llevar a cabo la administración de usuarios VPN Nortel, dentro de la opción *PROFILES* y dentro de este submenú, elegir la opción *USERS* con lo cual se despliega la pantalla *User Management*.

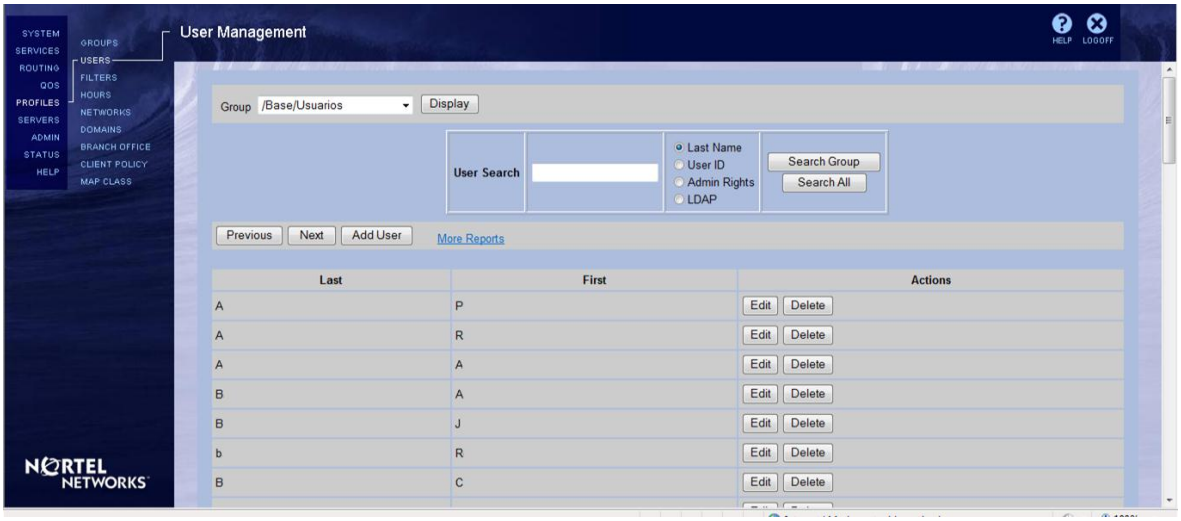


Figura 3.8Administración de Usuarios

Después de contar con la relación de todas las sucursales y de TEAM México actualizadas, corresponde la labor de realizar la baja de las cuentas que ya no deben estar activas, lo cual por medio del botón *Delete* dentro del apartado *Action* es realizado, esto redirige a otra pantalla en donde debo confirmar que estoy seguro de que es el usuario correcto a borrar del sistema.

Figura 3.9 Borrado de cuentas

De esta forma, antes de la actualización se contaba con 62 usuarios registrados en la base, la cual una vez hechos los cambios y bajas necesarios actualmente cuenta con 42 usuarios.

Una vez terminada la actualización se termina la sesión por medio del símbolo *LOGOFF*.

3.3.3 Actualización de la base de Mac Address para autenticación WLAN

Para llevar a cabo la actualización de las Mac Address de las computadoras que se firman a la red TEAM vía inalámbrica a la conexión WLAN TEAM es necesario que por área, según los miembros que la conforman, crear una relación de usuarios que utilizan este servicio ya que una gran parte de usuarios cuenta con PCs que se conectan de forma cableada, y otra cierta cantidad cuenta con laptops que hacen uso de la red inalámbrica, además existe la necesidad de hacer una revisión en cada área con respecto a qué usuarios con dispositivos móviles podrán tener conexión también en estas unidades , ya que en la base actual existen una gran cantidad de macs.

Como primer paso es acudir a cada área de la empresa y verificar qué usuarios se conectan vía inalámbrica, después por medio del comando >ipconfig/all dentro de una consola, estos comandos son debido a que en la empresa se cuenta en su mayoría con sistemas operativos Windows, se determina la dirección mac de cada usuario y se crea la relación, una vez que se cuenta con ella y la de dispositivos móviles como celulares, iPads, entre otros, acudir con cada gerente de área y evaluar quién puede tener acceso en este tipo de dispositivos.

Contando con la relación completa el siguiente paso es realizar la actualización dentro del sistema y ésta se efectúa por medio de una consola a través del comando telnet hacia el dispositivo de administración.

Se ejecuta un telnet dentro de la red hacia el dispositivo. Ver figura 3.10

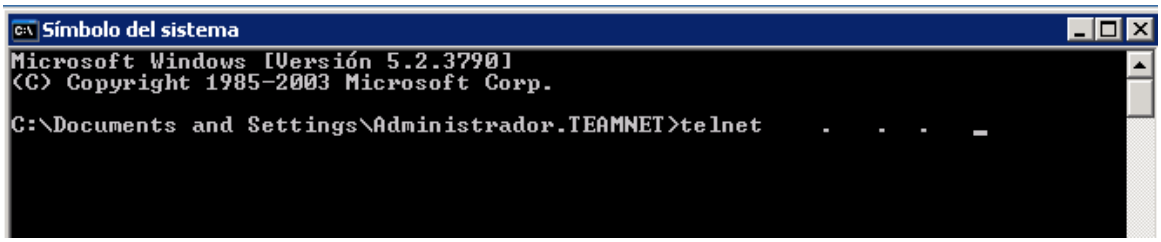


Figura 3.10Conexión al dispositivo

Una vez en el dispositivo es necesario autenticarse de forma correcta para tener acceso a la administración de las Mac Address habilitadas.

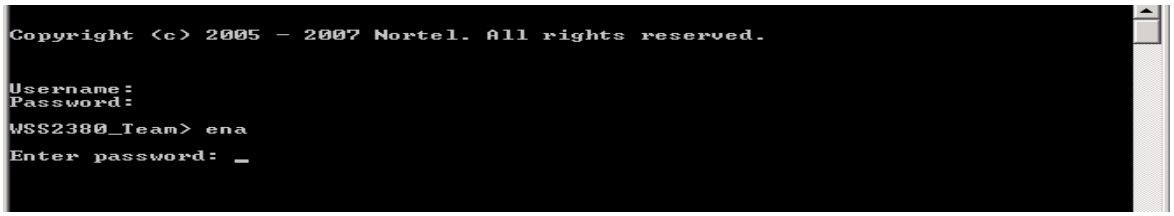


Figura 3.11 Autenticación al sistema

Dentro del sistema se despliega un promt que indica que se ha ingresado correctamente al sistema y podemos comenzar con la administración.

Para visualizar todas las Mac Address dadas de alta se utiliza el comando show aaa, el cual despliega la siguiente información. Ver figura 3.12, 3.13

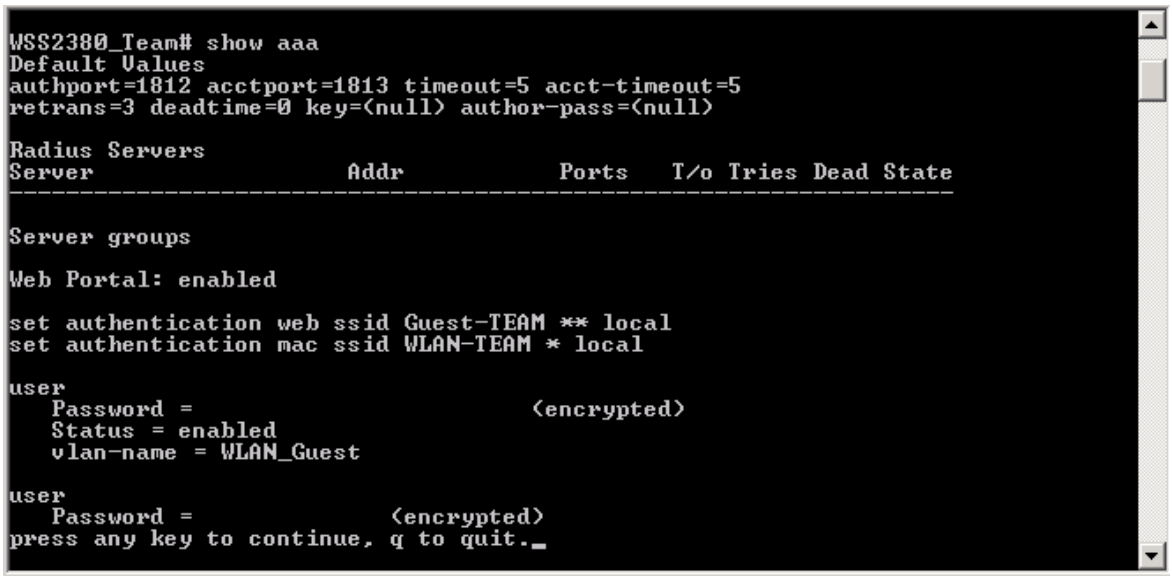


Figura3.12 Comando: show aaa, información de VLAN

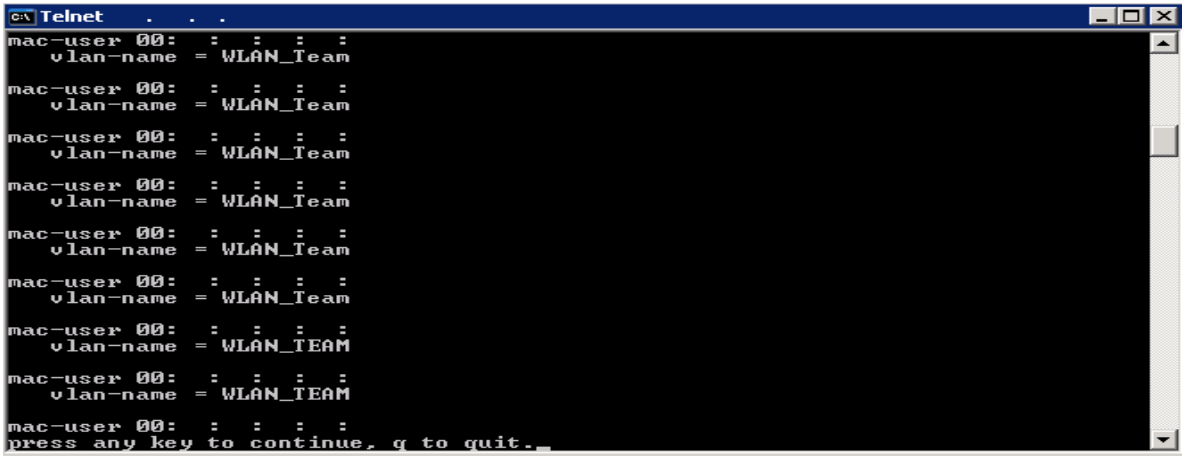


Figura 3.13 Mac Address registradas en el sistema

El estado actual del sistema cuenta con 293 Mac Address registradas.

Para llevar a cabo la depuración del sistema es necesario utilizar el comando

Eliminar MAC Address del sistema
>>Clear mac-user 00:00:00:00:00:00

Eliminar MAC Address de un grupo completo del sistema
>>clear mac-user 01:02:03:04:05:06 grupo

De esta forma se elimina la base de usuarios completa en un día no laboral y de acuerdo a la base de usuarios inalámbricos se dan de alta sólo aquellos que requieren este acceso y que tienen los permisos necesarios para hacerlo.

Una vez realizada el alta de las MAC actualizadas se encuentra que la nueva base de datos de usuarios inalámbricos no rebasa los 80 usuarios.

De esta forma queda actualizado y administrado el sistema de autenticación de usuarios de la WLAN TEAM que se encontraba con un alto índice de usuarios que no correspondían o no debían de contar con este acceso.

3.3.4 Generación y cambio de contraseñas de sistemas de información y comunicaciones

Para realizar esta implementación se lleva a cabo la recolección de distintas buenas prácticas, consejos y normas de diferentes asociaciones, grupos, investigaciones universitarias, entre otros documentos, para determinar cuáles serán las normativas a seguir para implementar contraseñas seguras y poder sustentar el por qué es así.

Existen una gran cantidad de ideas y conceptos en cuestión de contraseñas por lo cual expongo algunas de las que me parecieron más interesantes y de la cuales estarán compuestas las normativas y buenas prácticas para generar las contraseñas de los sistemas de información y comunicaciones de la empresa TEAM.

Estas son algunas de las fuentes y un resumen de las características que plantean:

- Consultora Ernst & Young

  Ernst & Young en sus lineamientos básicos de seguridad (Baseline Security Standards BSS) para el área Risk Advisory Services, indica que en el rubro de

contraseñas las características de éstas deben contar con mínimo 8 caracteres de longitud, vigencia máxima de 90 días, hacer uso de letras mayúsculas, minúsculas, símbolos y números. Se debe contar con un bloqueo de cuentas después de cierto número de intentos.

- Unidad Tecnológica Informática
  Sector Educativo

  La longitud mínima se considera de 8 caracteres, utilizando números, letras y símbolos.
  Después de realizados 3 intentos erróneos, congelar la cuenta.
  Contar con un máximo de 120 días de vigencia de la contraseña.
  No se deben utilizar nombres ni teléfonos relacionados al sistema, compañía o usuario al emitir la contraseña.

- Fondo de Cultura Económica

  - La periodicidad de cambio de contraseñas de usuarios es de 45 días, mientras que la de los servidores y otros sistemas de administración es trimestral.
  - La contraseña no debe ser una palabra de diccionario de ningún lenguaje.
  - No está basada en información personal, nombres de familia, etc.

- Artículo: Contraseñas – Kioskea.net

  - La contraseña debe contar con un número igual o mayor a 10 caracteres entre números, símbolos letras, etc.
  - No deben utilizarse palabras de diccionario.
  - Tampoco es recomendable utilizar palabras de diccionario escritas de forma invertida.
  - No deben usarse palabras seguidas de números o entre números.

- Inteco CERT

  Recomienda que un buen método para crear una contraseña sólida es pensar en una frase fácil de memorizar y acortarla aplicando alguna regla sencilla.
  Un ejemplo sería seleccionando la primera letra de cada palabra y convirtiendo algunas de las letras en números que sean por ejemplo, "La seguridad es como una

cadena, es tan fuerte como el eslabón más débil" podría convertirse en "Lsec1cetfceemd".

- Dentro de sus recomendaciones se encuentran
- Mínimo 8 caracteres
- Mezclar letras, números y caracteres especiales
- No debe coincidir con el nombre de usuario o con cualquier otra información personal
- Debe ser diferente para cada cuenta creada
- No utilizar palabras que estén en diccionarios
- Guardar las contraseñas a buen recaudo
- Nunca compartir las contraseñas por Internet, correo electrónico o teléfono

- Georgia Tech Research Institute

  Un artículo publicado por investigadores del Georgia Tech Research Institute señala que debido a los avances en el procesamiento de la información, el avance en la programación de gpu´s más poderosas, es probable que con este poder de procesamiento las contraseñas sean descifradas con mayor facilidad y en menos tiempo.

  El investigador Joshua Davis, cree que la mejor contraseña es una frase completa que incluya números, símbolos y caracteres, se debe cumplir con todo esto, que sea una contraseña larga y compleja, estas 2 condiciones se deben cumplir pero de igual forma debe ser fácil de recordar y menciona que tal vez en este instante o en un momento muy próximo cualquier contraseña de menos de 12 caracteres será muy fácil de descifrar.

  Señala que 12 caracteres con un alto poder de procesamiento tomaría alrededor de 17,134 años para poder ser descifrada, asumiendo que un hacker sea capaz de probar 1 trillón de combinaciones por segundo.

- Artículo: “Cómo escoger buenas contraseñas” por la Universidad de Carnegie Mellon

  Qué no hacer en la creación de una contraseña:

- Elegir contraseñas basadas en información personal, similar al nombre de usuario, o que este estrechamente relacionada al sistema o usuario
- Utilizar palabras de diccionario, de programas de tv, nombres propios, entre otros
- Usar secuencias de números después de la contraseña o cambiar las letras por números como 1 por l de forma secuencial

La mejor forma de escribir contraseñas:

1.- Crear frases que puedan ser fácilmente recordadas por ejemplo:

- I have two kids: Jack and Jill.
- I like to eat Dave & Andy's ice cream.
- No, the capital of Wisconsin isn't Cheeseopolis!

2.- Ahora, tomando la primera letra de cada palabra contando mayúsculas, minúsculas y signos de puntuación, agregando y variando letras por números, obteniendo contraseñas de la siguiente forma.

- Ih2k:JaJ.
- IlteD&A'ic.
- N,tcoWi'C!

De esta forma pueden ser fácilmente recordados y la contraseña es sólida y robusta.

Este artículo nos dice que el mínimo de caracteres aceptable es 8.

Tomando en cuenta todas estas recomendaciones, para la implementación de las nuevas contraseñas en los sistemas de información y comunicaciones de la empresa, ya que la creación está a mi cargo, estas contraseñas como normas, tendrán un mínimo de 12 caracteres y como lo hace la recomendación en el artículo publicado por la Universidad de Carnegie Mellon estarán creadas bajo frases y alternadas con letras (mayúsculas y minúsculas), símbolos, signos de puntuación, y números pero que sean memorizados de forma sencilla, la vigencia será trimestral para cada una de las contraseñas y no deben existir contraseñas repetidas entre cuentas y sistemas, además de no poder alternan o repetir contraseñas por lo menos en 5 periodos de cambio.

Estas contraseñas sólo serán conocidas por mi compañero de soporte y por mí.

Se encontrarán almacenadas en un archivo cifrado para poder contar con mayor seguridad y que sea estrictamente visible sólo por el ingeniero de soporte y por mí.

Para esta sección de implementación sólo se establecen las normas a seguir, el cómo se conforman las contraseñas y su implantación en cada sistema, pero es en la implementación de contraseñas a usuarios donde se establece y se publica una política de contraseñas la cual todos los usuarios sin excepción deben atender.

3.3.5 Generación y cambio de contraseñas de usuarios

Para la generación de las contraseñas de usuarios, aunque es un tópico similar al de la implementación en el punto anterior, se ve afectada por otros factores para su realización, el punto principal de esta implementación es el personal de la organización y el poder crear contraseñas seguras y robustas sin que entorpezcan el continuo desempeño de labores.

De acuerdo con lo analizado y los extractos de normas, consejos y buenas prácticas del punto anterior se expone aquí la política de contraseñas escritas y publicables que los usuarios deben seguir sin excepción para la generación de sus contraseñas, la política de contraseñas de usuarios está conformada como lo muestra el documento que se presenta a continuación.

Políticas de seguridad informática

Contraseñas

Área responsable Gerencia TI		
Liberación xx/xx/2011	Documento Políticas de Contraseñas TEAM México	
Página 1 de 4	Tipo de Documento Políticas de Seguridad Informática	Revisión 01

OBJETIVO:

Establecer normas, recomendaciones y procedimientos para la creación de contraseñas robustas, su protección y la frecuencia de cambio de las mismas dentro de los sistemas y equipos de la organización a fin de evitar o reducir los incidentes de seguridad.

La autenticación por contraseñas es el mecanismo utilizado para evitar el acceso a los sistemas y recursos de personas/programas no autorizadas/os.

ALCANCE:

Esta política aplica a todo el personal que labora, responsable de una cuenta dentro de los sistemas y equipos de TEAM México que requiere alguna forma de autenticación a través de una contraseña, o en caso, de almacenar información sensible(no pública) de la empresa Tecnología Especializada Asociada de México.

BENEFICIOS:

Las políticas y estándares de seguridad de contraseñas establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información de la organización.

Políticas de seguridad informática

Contraseñas

Área responsable Gerencia TI		
Liberación xx/xx/2011	Documento Políticas de Contraseñas TEAM México	
Página 2 de 4	Tipo de Documento Políticas de Seguridad Informática	Revisión 01

POLÍTICA DE CONTRASEÑAS

ASPECTOS GENERALES

1. Todas las contraseñas de inicio de sesión de usuarios, cuentas de aplicación, Acceso a sistemas etc. Deben de cambiarse con una periodicidad de 120 días.

2. Todas las contraseñas de usuarios de TEAM México deben ser parte de un Sistema de autenticación global de administración (Active Directory-Domain Controler).

3. Las cuentas administrativas no pueden ser compartidas, en caso de requerirse que varios usuarios tengan acceso a privilegios administrativos a nivel del sistema, estos serán otorgados a través de un grupo de usuarios administrativos de sistemas.

4. Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificación de usuario y contraseña, necesarios para acceder a la información y a la infraestructura tecnológica de la empresa, por lo cual deberá mantenerlo de forma confidencial.

5. El permiso de acceso a la información que se encuentra en la infraestructura Tecnológica de la organización, debe ser proporcionado por el administrador de la información, con base en el principio de la “necesidad de saber” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

6. Las contraseñas no pueden ser comunicadas a otras personas ya que son intransferibles y personales.

Políticas de seguridad informática

Contraseñas

Área responsable Gerencia TI		
Liberación xx/xx/2011	Documento Políticas de Contraseñas TEAM México	
Página 3 de 4	Tipo de Documento Políticas de Seguridad Informática	Revisión 01

Todas las contraseñas que se manejen dentro de la organización, deben de conformarse con base en los lineamientos descritos a continuación.

NORMAS PARA LA GENERACION DE CONTRASEÑAS:

Para la creación de contraseñas a usar por parte de los usuarios de TEAM México deben contar con las siguientes características:

1. Debe contener caracteres en mayúsculas y minúsculas (por ejemplo: a-z, A-Z)

2. Contener dígitos y caracteres de puntuación así como símbolos especiales (por ejemplo: 0-9, !@#$%^&*()_+|~=\`{}[]:";'<>?,./)

3.Para el establecimiento de una contraseña debe de ser con un mínimo de 10 caracteres

4. La contraseña no debe ser una palabra de diccionario de ningún idioma

5. La contraseña tendrá una vigencia de 120 días

6.No deberá estar basada en información personal, nombres de familia, fechas de cumpleaños, etc.

7. Las contraseñas no deben de ser nunca almacenadas en un equipo de cómputo. Se debe de tratar de crear contraseñas que puedan se recordadas fácilmente. Una forma de hacer esto, es crear una contraseña basado en el nombre de una canción, una afirmación o una frase.

8.No utilizar secuencias de números después de la contraseña o cambiar letras por números como 1 por l de forma secuencial.

Políticas de seguridad informática

Contraseñas

Área responsable Gerencia TI		
Liberación xx/xx/2011	Documento Políticas de Contraseñas TEAM México	
Página 4 de 4	Tipo de Documento Políticas de Seguridad Informática	Revisión 01

Los estándares de protección de las contraseñas para el uso de sistemas dentro De TEAM México son los siguientes:

1. Si algún usuario requiere una contraseña, se debe de referir a este documento y ponerse en contacto con la gerencia de Tecnologías de Información

2. No utilizar las funciones de recordar las contraseñas que poseen algunas aplicaciones (por ejemplo, Outlook, Firefox, Messenger, etc.)

3. No escribir las contraseñas en ningún documento que se encuentre en su lugar de trabajo

4. No almacenar las contraseñas en ninguna computadora (incluyendo agendas personales o dispositivos similares) sin cifrar la información

5. Se deben cambiar las contraseñas en un intervalo de tiempo de cada cuatro meses

6. Si alguna cuenta o contraseña que haga uso de los recursos informáticos de la Organización se tiene la sospecha de haber sido comprometida, reportarlo a la Gerencia de TI para que ésta inicie un proceso de verificación y análisis, Adicionalmente el usuario debe cambiar todas las contraseñas utilizadas en cada uno de los sistemas y equipos de TEAM México.

7. Durante las auditorías de seguridad que realice la gerencia de TI se verificará la Robustez de las contraseñas de los usuarios, en caso de que estas lleguen a ser Comprometidas a través de estas técnicas de auditoría, la contraseña de la cuenta del usuario requerirá ser cambiada.

8. Se utilizará un software de verificación de contraseñas para comprobar la Robustez de las mismas, sino se aprueban la contraseña tendrá que cambiarse.

Dentro de los puntos importantes se consideran 10 caracteres mínimos para los usuarios y 12 para los sistemas, esto para facilitarles recordar sus contraseñas creadas, además de evitar la pérdida de estas y tener que estar restableciendo cuentas por este factor.

Para hacer la comprobación de las contraseñas además de verificar que cuenten con todas las características mencionadas en las políticas como número y tipos de caracteres, que no sean nombres propios, frases seguidas de números, etc. Conjuntamente se realiza una comprobación por medio de la herramienta proporcionada por Microsoft Online Safety para verificar su complejidad, sino alcanza el nivel de bueno o excelente tendrá que generarse una nueva contraseña.

De la misma forma se amplía el tiempo de caducidad de las cuentas a 120 días para los usuarios a diferencia de los sistemas donde es de 90 días de caducidad con la finalidad de que anualmente se renueven 3 veces y sea más fácil para los usuarios llevar a cabo estos cambios.

Las contraseñas se encontrarán almacenadas en un archivo cifrado para contar con mayor seguridad y que sea estrictamente visible sólo por el ingeniero de soporte y por mí.

3.3.6 Configuración de Firewalls (appliances) para aplicaciones demo

Dentro de este punto se realiza la configuración de un Firewall desde cero con las características necesarias para que tenga un tráfico limitado y pueda brindar la seguridad necesaria a los servidores y por lo tanto a sus aplicaciones, con el mismo servicio y accesibilidad de siempre.

Por medio de esta nueva configuración se corrigen problemas como que el tráfico existente a través del firewall no estaba limitado, se contaba con las contraseñas que por default el appliance nos proporciona, se inhabilita la cuenta *admin* que por default está configurada y se limitan los servicios y protocolos.

Para llevar a cabo esta configuración desde cero por medio del display físico del appliance, es necesario realizar un Reinicio de Fábrica, en la figura 3.14 se observa el estado actual, mientras que en la figura 3.15 se ingresa a la opción del Firewall de *Factory Reset* para configurar desde cero el appliance.

Figura 3.14 Firewall en su estado actual

Figura 3.15 Reinicio de Fabrica

Una vez realizado el *Factory Reset*, el appliance, como la opción lo indica, volverá a su estado de fábrica y se inicia la configuración, realiza procesos de copias de arranque y configuración inicial.

Una vez reiniciado el Firewall se configura una IP interna para poder realizar la configuración desde la consola de administración, esta IP se asigna por medio del display del appliance. Ver Figura 3.16, 3.17, 3.18

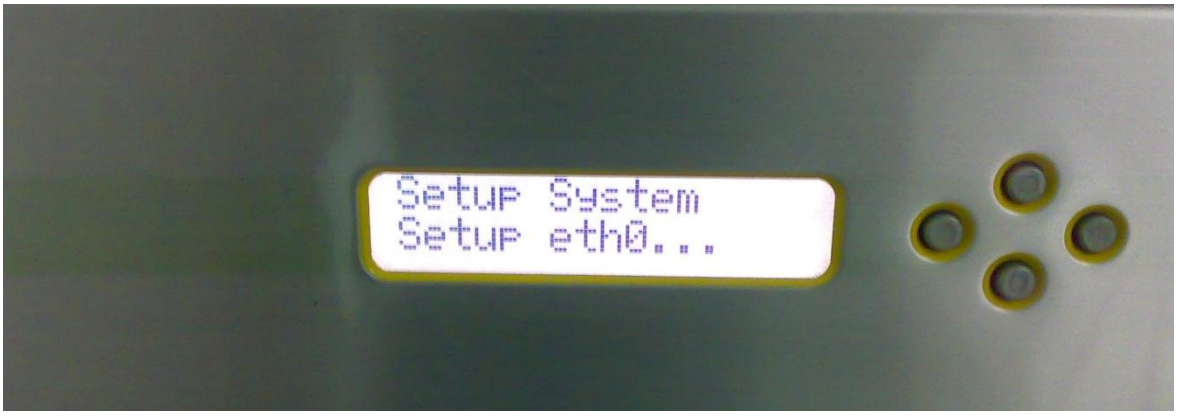


Figura 3.16 Inicio de configuración

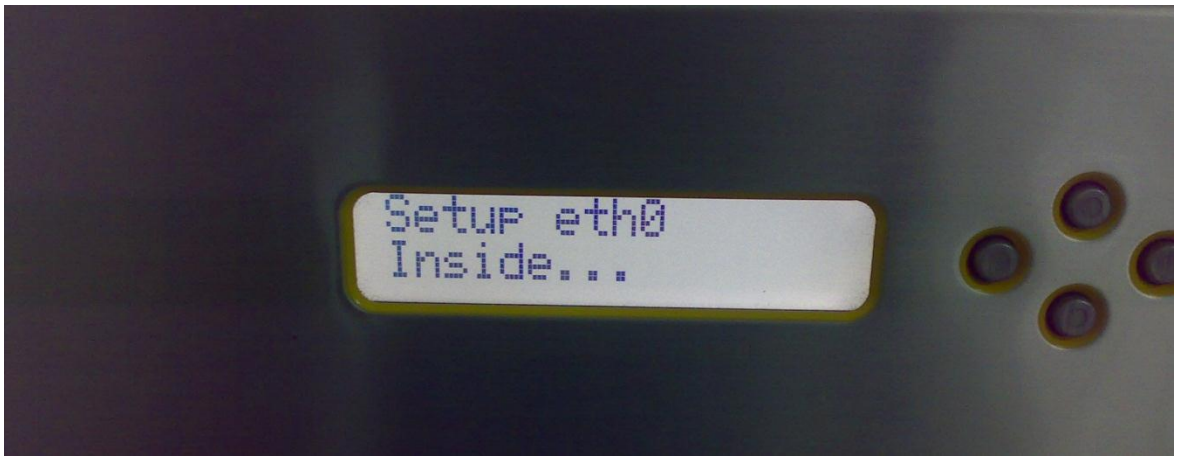


Figura 3.17 Asignación de IP interna

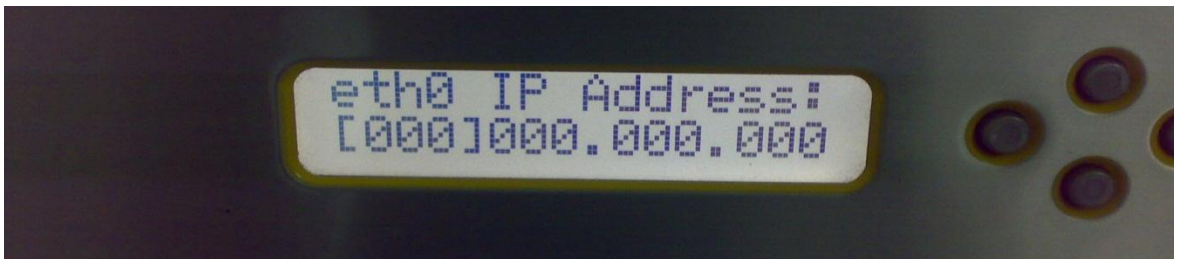


Figura 3.18 Asignación de IP interna

También es necesario asignar una máscara de red como se muestra en la figura 3.19.

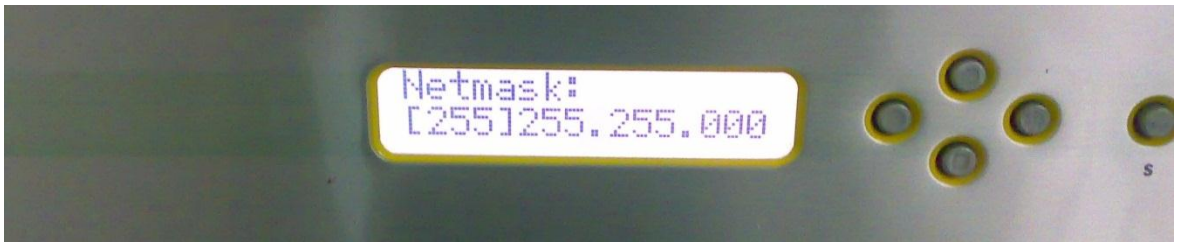


Figura 3.19 Asignación de mascara de red

Una vez hecho esto el sistema se reinicia mostrando una contraseña por default para poder iniciar la configuración y administración del sistema.

Figura 3.20 firewall iniciado

Para iniciar la configuración vía la consola de administración es necesario cambiar dentro de las propiedades de red el Gateway y asignarle la IP interna del Firewall para realizar la comunicación entre el firewall y el equipo con el que se hace la administración.

Después, por medio de un plug-in java se instala la consola, este plug-in los obtenemos al entrar a la dirección IP asignada del firewall por medio de un explorador, la realización se lleva a cabo de forma tradicional, aceptar permisos y directorios de instalación, luego se muestra el siguiente icono de inicio. 

Al iniciar la consola de administración se despliega una pantalla java y muestra una serie de certificados. Ver Figura 3.21

Figura 3.21 inicio de servicios y permisos de la consola de administración

Para ingresar como ya se ha mencionado se realiza la conexión al servidor que es el firewall, se deben ingresar las credenciales siguientes para autenticarse con la cuenta *admin* y la contraseña entregada por default. Ver figura 3.22

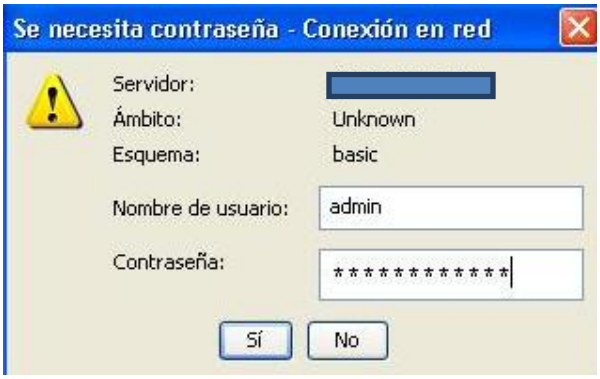


Figura 3.22 Autenticación a la consola de administración

Una vez realizada la autenticación, el sistema despliega la pantalla principal con el estatus de configuración, actualizaciones, licenciamiento, etc. Ver figura 3.23

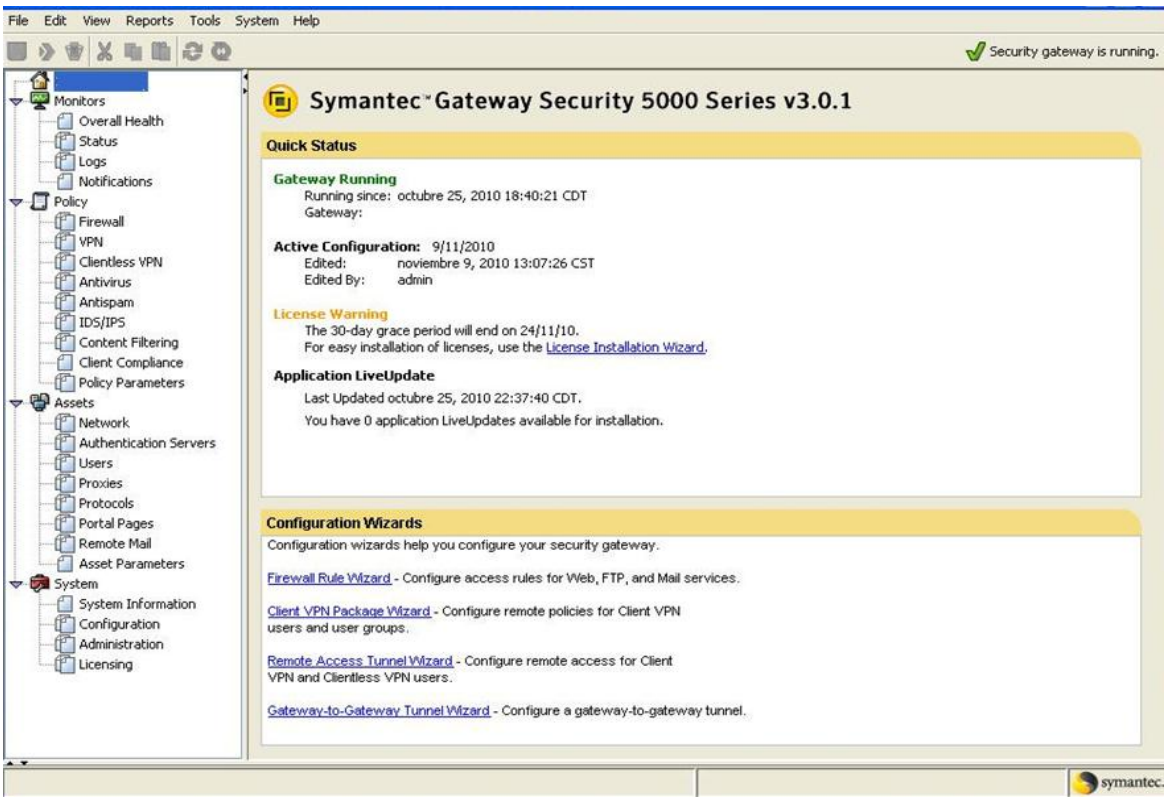


Figura 3.23 Pantalla principal de consola de administración

Como primer paso se configuran una serie de políticas dentro del firewall para que las aplicaciones a proteger y que pasan a través del firewall sean accesibles sin ningún problema y de forma transparente.

De esta forma como en la mayoría de los firewall, se agregan las políticas de origen y destino, el tipo de protocolos accesibles y cómo se comportarán de forma interna hacia el mundo y viceversa. Ver figura 3.24

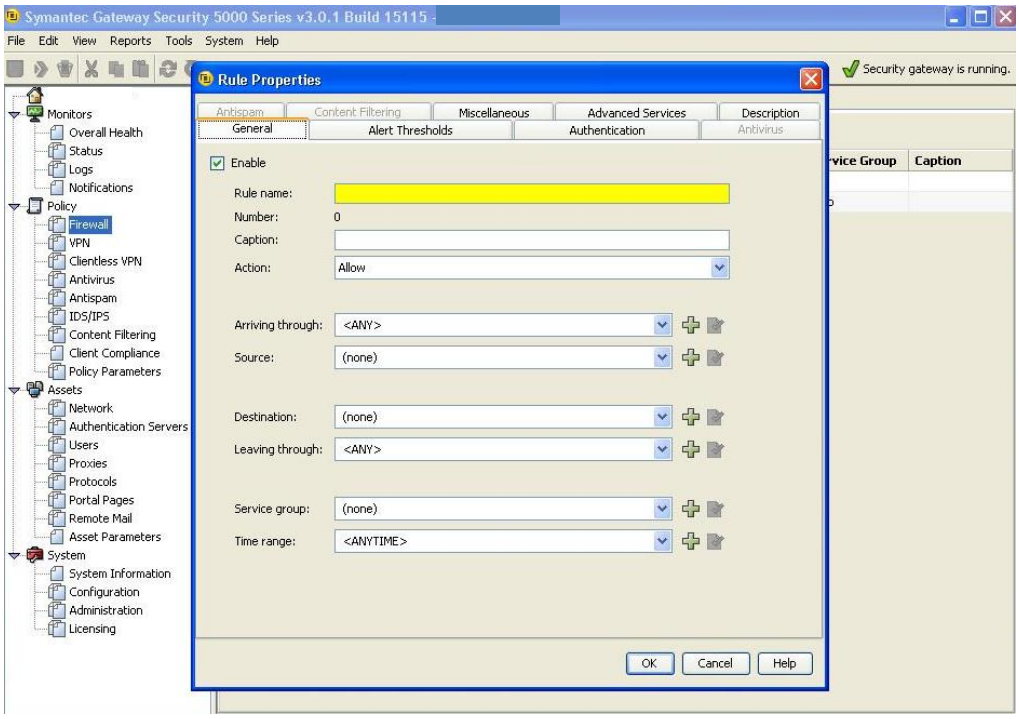


Figura 3.24 Creación de políticas

De esta forma se crean políticas para distintos protocolos de comunicaciones que necesitan para ser accesibles las distintas aplicaciones, estos se generan conforme a requerimiento y no se levanta ningún protocolo adicional que no sea necesario para hacer accesible y funcional estas aplicaciones.

A continuación se observan los protocolos que han sido configurados para su acceso desde la red interna hacia el exterior y viceversa. Ver figura 3.25

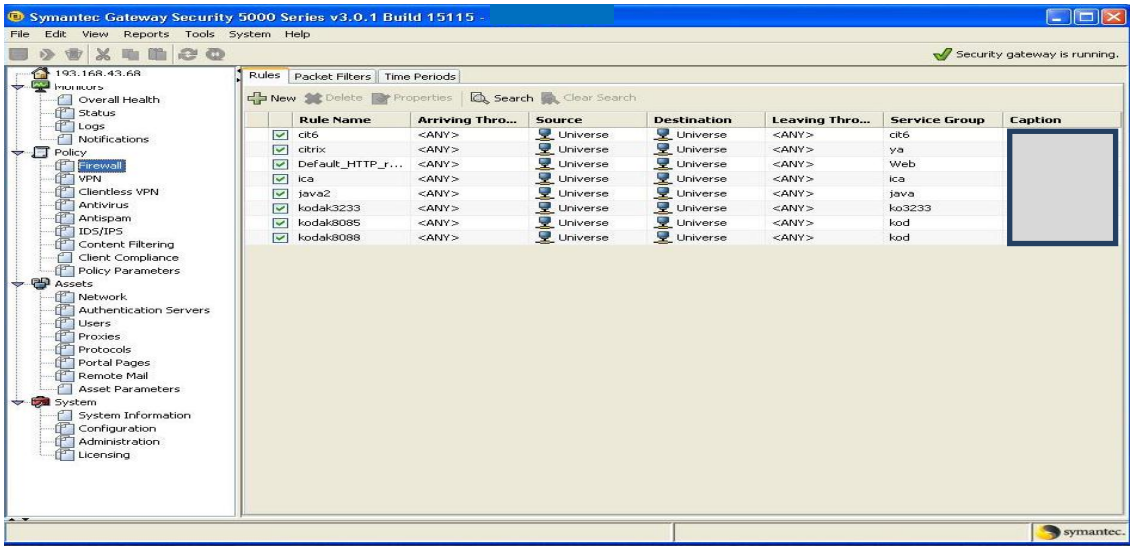


Figura 3.25 Políticas de acceso a las aplicaciones

Una vez contando con los protocolos accesibles es necesario agregar las conexiones de cada aplicación en una interface diferente dentro del firewall, agregamos la IP homologada de cada aplicación para lograr que cuenten con la protección antes generada a través del firewall, por medio de la figura 3.26 podemos observar todas las interfaces generadas.

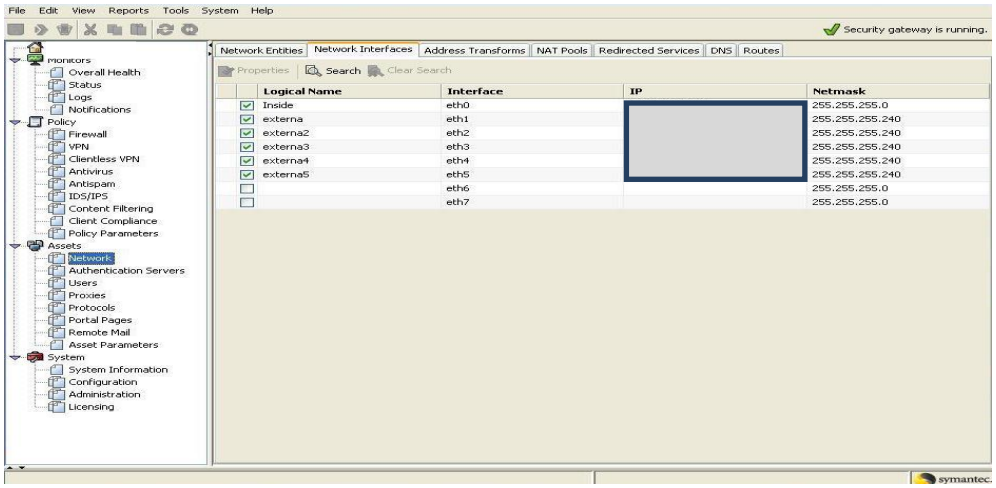


Figura 3.26 Generación de interfaces de aplicaciones

De esta forma se agrega también una IP homologada al Firewall para que tenga comunicación con el exterior y las aplicaciones queden protegidas.

Una vez configuradas todas las interfaces y que las aplicaciones responden desde el mundo exterior, es necesario cambiar las credenciales de autenticación por default de la consola de administración, esto se lleva a cabo inhabilitando la cuenta *admin* que viene por default y creando una nueva con permisos de administración, esta tendrá un nombre no relacionado al sistema. Ver figuras 3.27 y 3.28

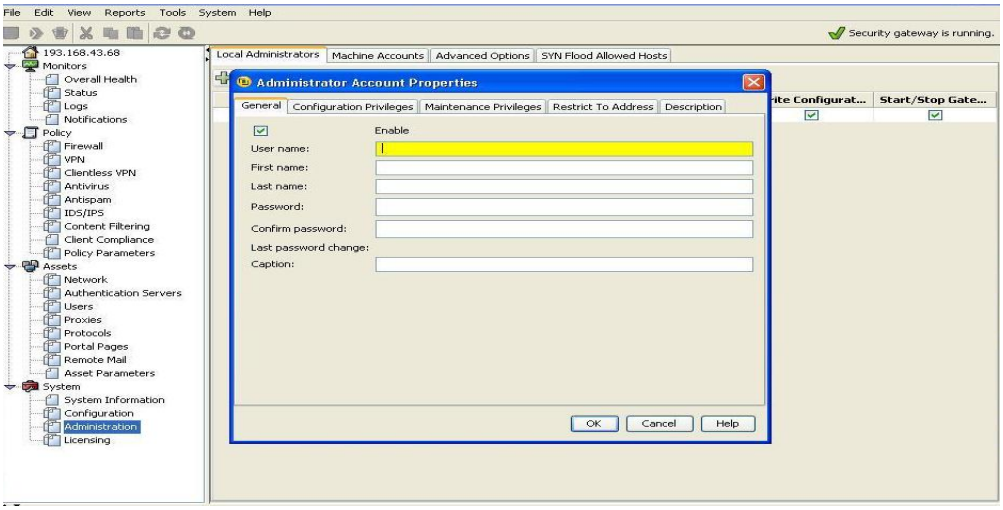


Figura 3.27 Creación de nueva cuenta de administrador

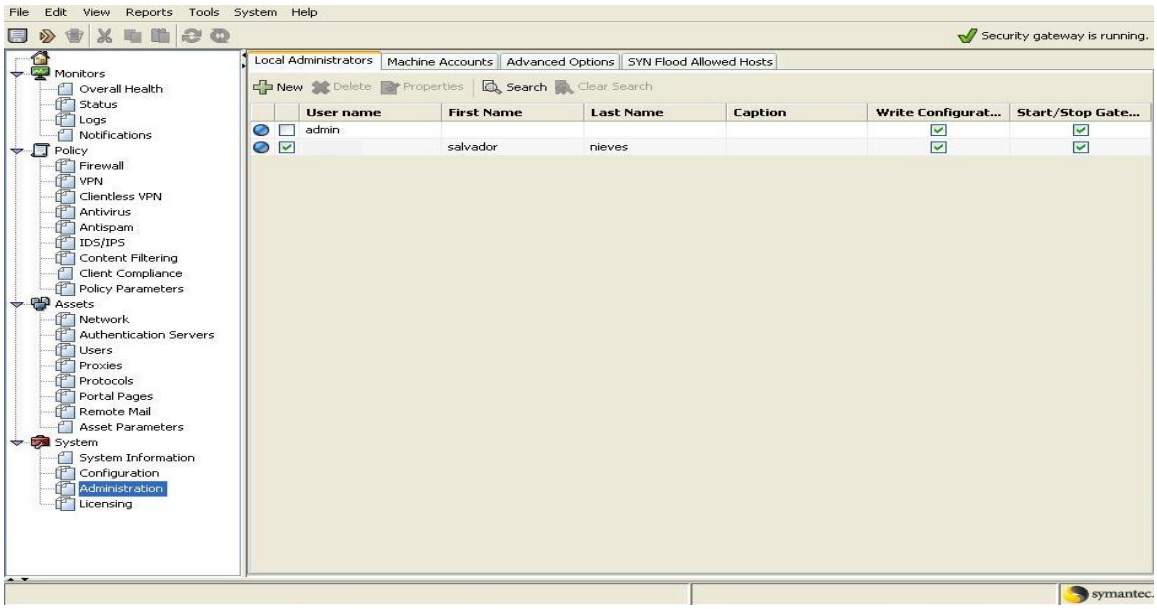


Figura 3.28 Nueva cuenta de administrador

Realizado esto, se reinicia y accede a la consola con la nueva cuenta de usuario y contraseña, así queda deshabilitada la cuenta *admin*, ingresamos a las aplicaciones desde un servidor externo y observamos que sigan accesibles y funcionales, revisados estos puntos concluimos con esta implementación.

Aunque el Firewall tiene una gran cantidad de herramientas para la protección de las aplicaciones y la red, se inició con la configuración y aseguramiento de las aplicaciones demos, dando solo acceso a los protocolos que deben de ser accesibles para poder brindar el servicio y generando las conexiones estrictamente necesarias, así como la realización del cambio de administradores dentro del sistema que era una vulnerabilidad importante con la que se contaba.

3.3.7 Configuración del servidor de web TEAM dentro de la red interna

Dentro de esta implementación se lleva a cabo la configuración de la página web de la organización de forma interna por medio de un redireccionamiento de IP´s y puertos para que de esta forma el servidor se encuentre detrás de un firewall que es el que contiene la IP homologada virtual y hace el redireccionamiento hacia el servidor web TEAM con lo cual se reduce en gran medida las vulnerabilidades y posibles ataques contra el portal de la organización.

Este redireccionamiento se hace dentro de un Firewall muy similar al de la implementación anterior, no existen variaciones en la configuración de estos dispositivos, sus diferencias se encuentran en el número de interfaces con las que cuentan, ya que este dispositivo tiene un menor número de interfaces configurables, y el diseño físico del appliance es más delgado, estas son las únicas diferencias con el Firewall configurado en el punto anterior. Ver figura 3.29

Figura 3.29 Firewall aseguramiento portal web TEAM

Debido a que los firewall se configuran de igual manera, en este punto sólo se describen de manera puntual los pasos a seguir para la configuración del firewall hasta llegar a la configuración del redireccionamiento de IPS y puertos que es donde se describirá de forma más exacta la manera de realizar la inserción de la página web accesible a través del Firewall y contar así con un mejor aseguramiento del portal.

Como se menciona en el punto anterior se inicia con el comando *Factory Reset* dentro del display del appliance esto lleva al dispositivo a su estado de fábrica, el Firewall realiza una configuración inicial, crea un respaldo principal y configura los archivos de inicio.

Una vez que reinicia el dispositivo se configura la IP interna por medio del display, esta IP es por medio de la cual tengo acceso a la consola de administración del appliance.

Una vez configurada la IP interna del dispositivo, dentro del equipo en el que se realiza la conexión al Firewall para llevar a cabo la administración, es necesario en las conexiones de red cambiar el Gateway de la conexión por la IP interna asignada al Firewall.

Por medio del acceso java se inicia la aplicación, me autentico por medio de la cuenta admin y el password asignado por default del appliance, una vez en la consola se realiza la configuración de entrada y salida de protocolos y flujo permitidos.

Teniendo esta configuración agrego la interface del servidor web dentro del Firewall. Ver figura 3.30

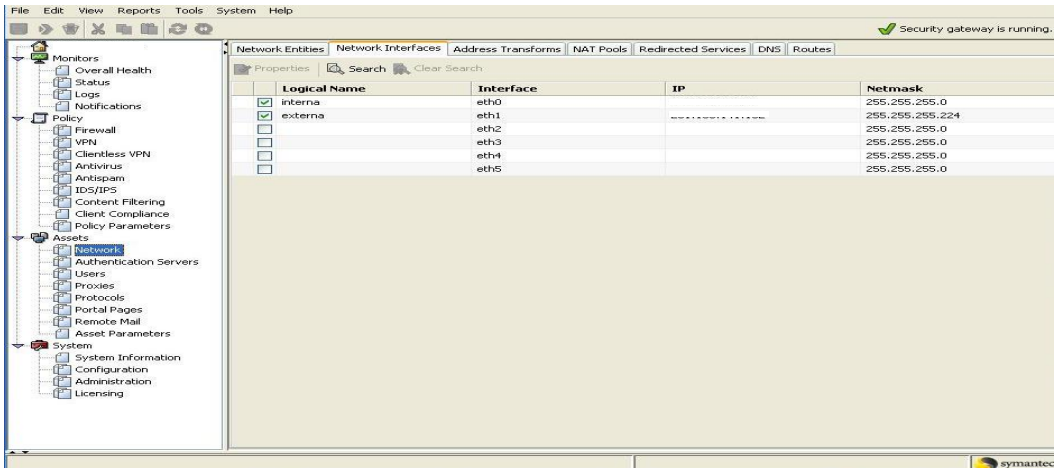


Figura 3.30 Configuración de interfaces

Ahora es necesario que identificada la interfaz se realice el direccionamiento para hacer accesible el servidor web a las peticiones de los usuarios y clientes a través de la red externa.

Esto se realiza por medio de las opciones de red en la pestaña de *Redireccionamiento de servicios*, los datos necesarios para llevar a cabo esta configuración son los protocolos que se habilitarán para el redireccionamiento a través del firewall y que son los servicios que podrán fluir a través del dispositivo de seguridad, otro de los aspectos con los que deben de contar son las IPs con las que se hará el direccionamiento de la IP homologada a la IP interna, la IP homologada que se encuentra almacenada en los DNS tiene que direccionarse hacia la IP interna detrás del firewall y viceversa para poder hacer accesible el portal web al exterior, realizado esto escogemos la interfaz que previamente se había configurado. Ver figura 3.31

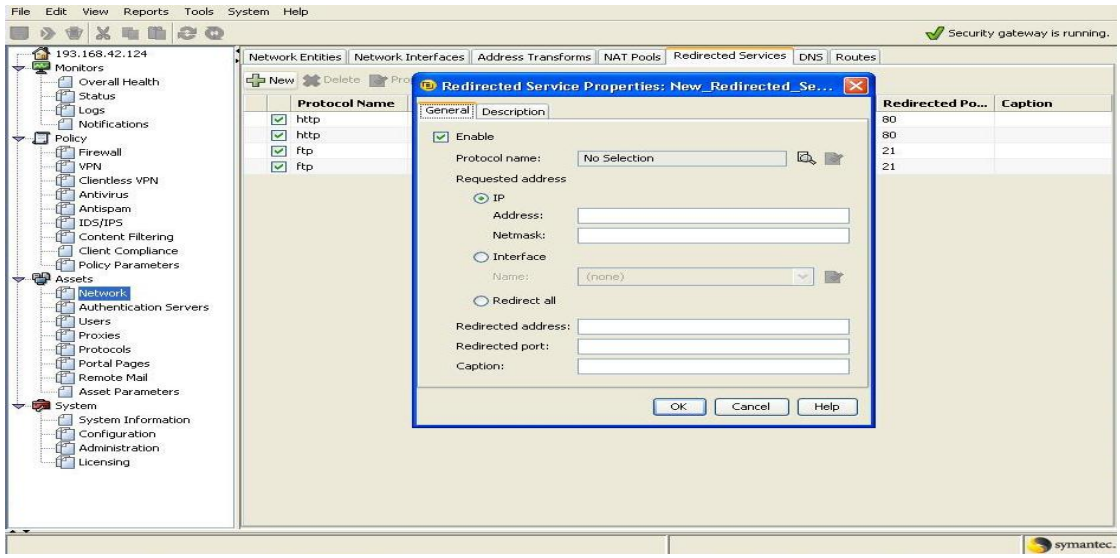


Figura 3.31 Redireccionamiento

Antes de realizar los cambios dentro del Firewall se debe de hacer el cambio de la IP homologada a la IP interna dentro del servidor, de esta forma no se creará un conflicto de IP y una vez realizados los cambios y aplicados dentro del Firewall estará accesible el portal web a través de la IP homologada almacenada en el Firewall el cual aplicará las políticas configuradas. Ver figura 3.32 y 3.33

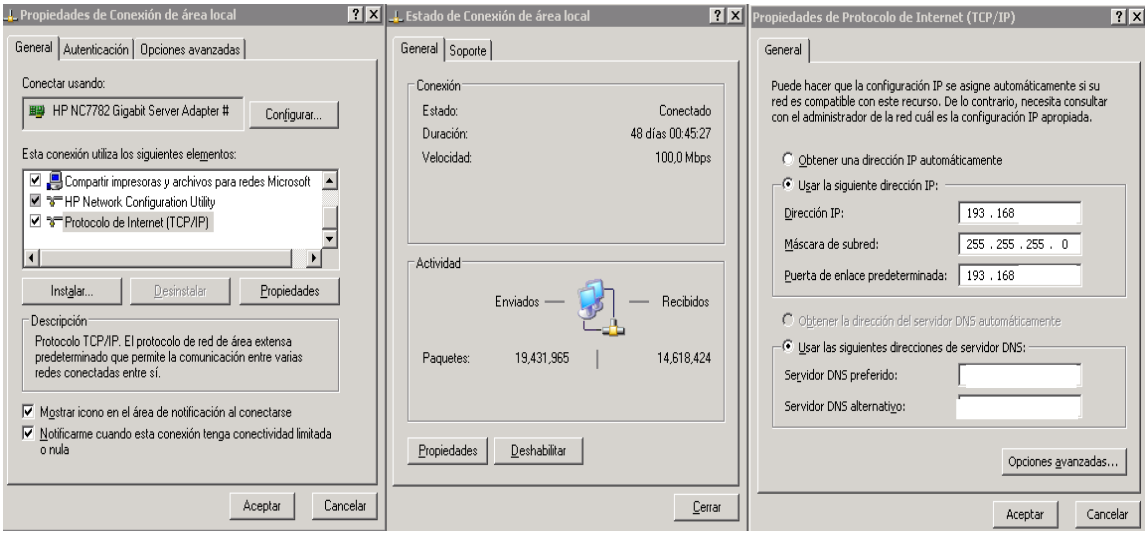


Figura 3.32 Cambio de dirección homologada por una interna

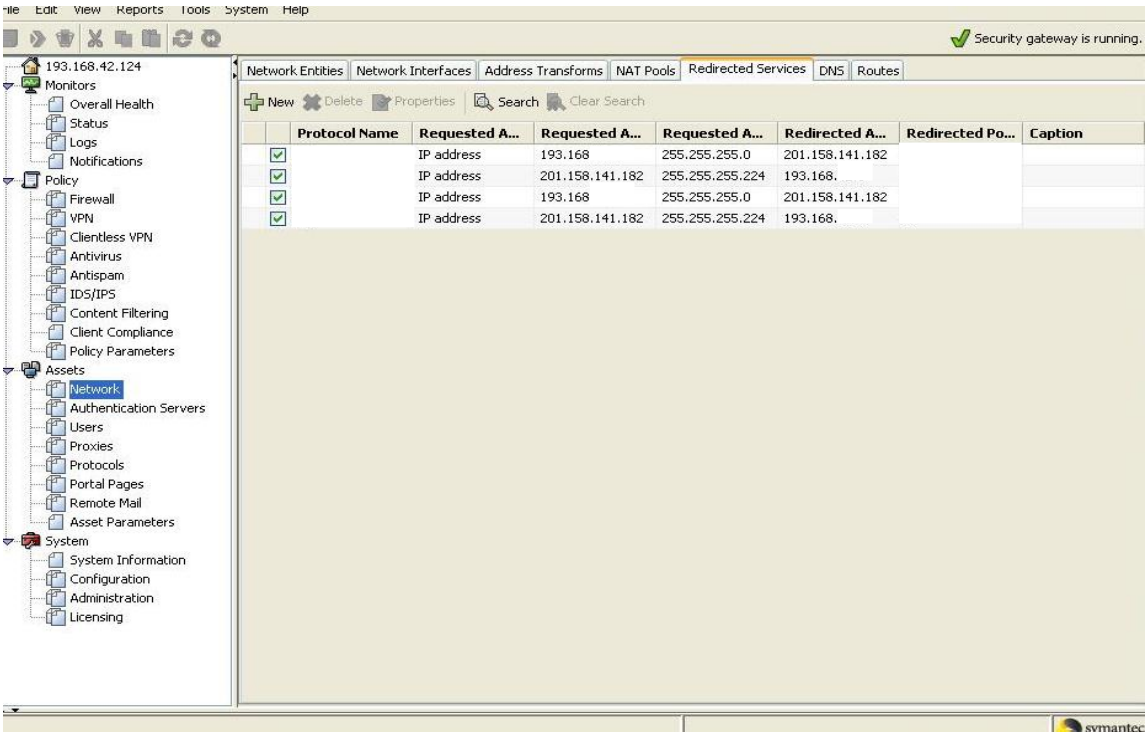


Figura 3.33Redireccionamiento configurado

Una vez realizada la configuración y guardados los cambios se observa que el redireccionamiento es exitoso y podemos ingresar a la página web de la organización. Ver Figura 3.34

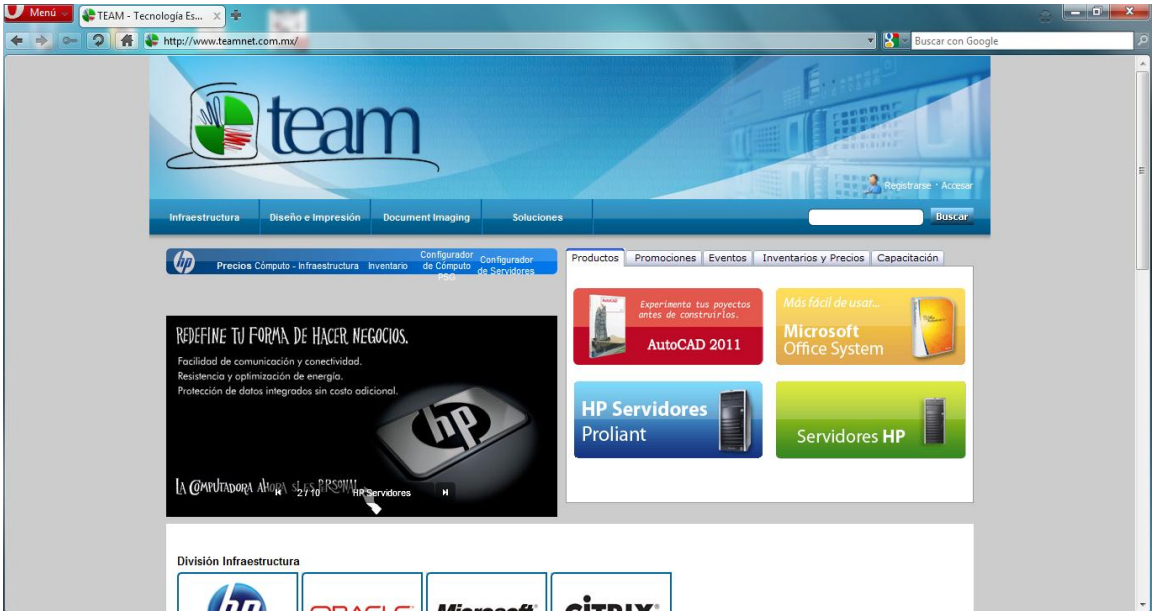


Figura 3.34Redireccionamiento exitoso

3.3.8 Actualización de Parches de Seguridad

Por medio de esta implementación se hace un análisis de las actualizaciones y parches faltantes recientemente dentro de toda la infraestructura de servidores para todas las aplicaciones y servicios importantes de la organización.

Se hace un listado de todos los servidores en producción y sus diferentes sistemas operativos, una vez que se cuenta con esta lista ingreso a cada uno de ellos para llevar a cabo las actualizaciones que se encuentran de forma automática revisando y corriendo la herramienta por medio de Windows Update.

Listado de servidores a actualizar

1.- Servidor de Correo (Front-end)- Windows Server 2003

2.- Servidor de Correo (Back-end)

3.- Servidor de Correo (Back-end 2)

4.- Servidor Controlador de Dominio

5.- Servidor Acceso Citrix

6.- Servidor Hyper-V- Windows Server 2008

7.- Servidor Consola de Antivirus – Windows Server 2003

8.- Servidor Storage – Windows Server 2003

9.- Workstation de Tarificación telefónica – Windows XP

10.- Servidor ERP – Windows server 2003

11.- Servidor Firewall de contenido – Windows Server 2003

12.- Servidor Video vigilancia – Windows Server 2003

13.- Servidor de Correo Marketing – Windows Server 2003

14.- Servidor de Documentación General – Windows Server 2003

15.- Servidor Correo Sucursal – Windows Server 2003

16.- Servidor DNS 1 – Windows Server 2003

17.- Servidor DNS 2 – Windows Server 2003

18.- Servidor Multidominio – Windows Server 2003

19.- Servidor de Correo Ecomsa – Windows Server 2003

20.- Servidor Portal Web Team – Windows Server 2003

21.- Servidor demo Microsoft – Windows Server 2008

22-. Servidor Firewall de contenido alterno – Windows Server 2003

Ahora se ejecuta la herramienta Windows Update en cada uno de los servidores para obtener las actualizaciones a la fecha para cada servidor.

Los pasos para realizar la actualización por medio de Windows Update son los siguientes:

Podemos realizarlo a través del navegador Internet Explorer, dirigiéndose al menú de *herramientas*, y desplazándonos hasta la parte inferior donde se encuentra la opción de Windows Update.Ver figura 3.35

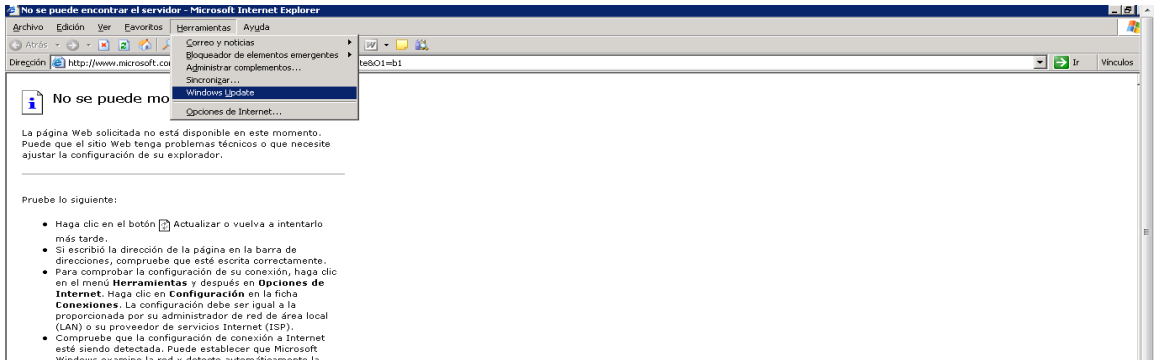


Figura 3.35 Ingresar a Windows Update

Una vez entrando a la aplicación es probable que se requiera instalar un plug-in para llevar a cabo los procesos de diagnóstico y actualización, se acepta la instalación y continúa. Ver figura 3.36

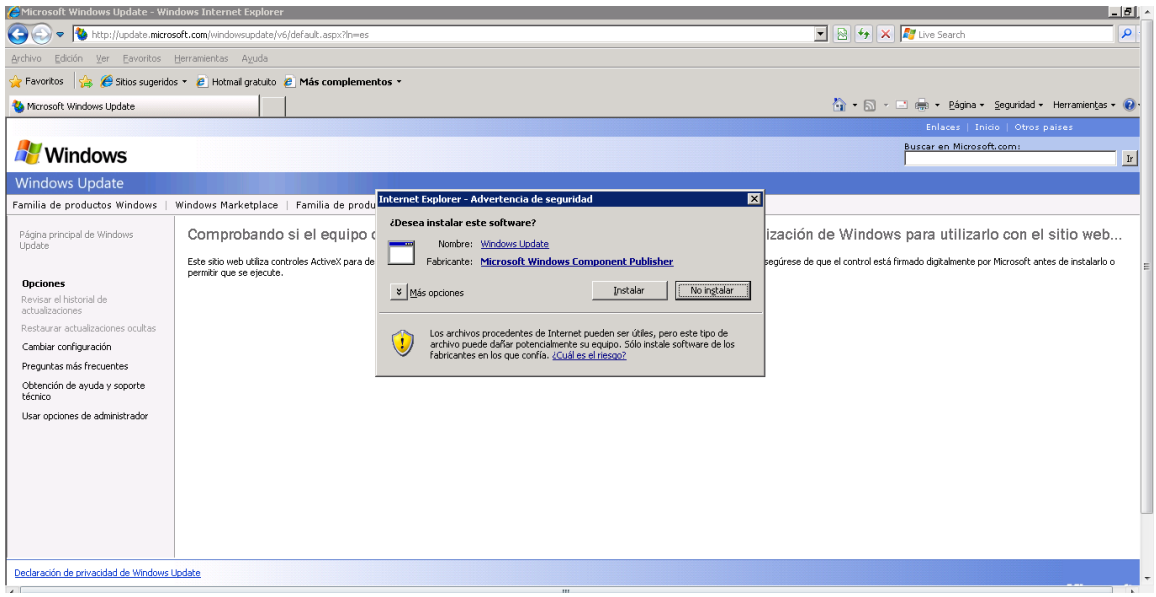


Figura 3.36 Instalación de plug-in

Después de instalado el plug-in se ingresa a la página de bienvenida donde para que se realice un análisis exhaustivo de todas las actualizaciones se selecciona la prueba personalizada. Ver figura 3.37

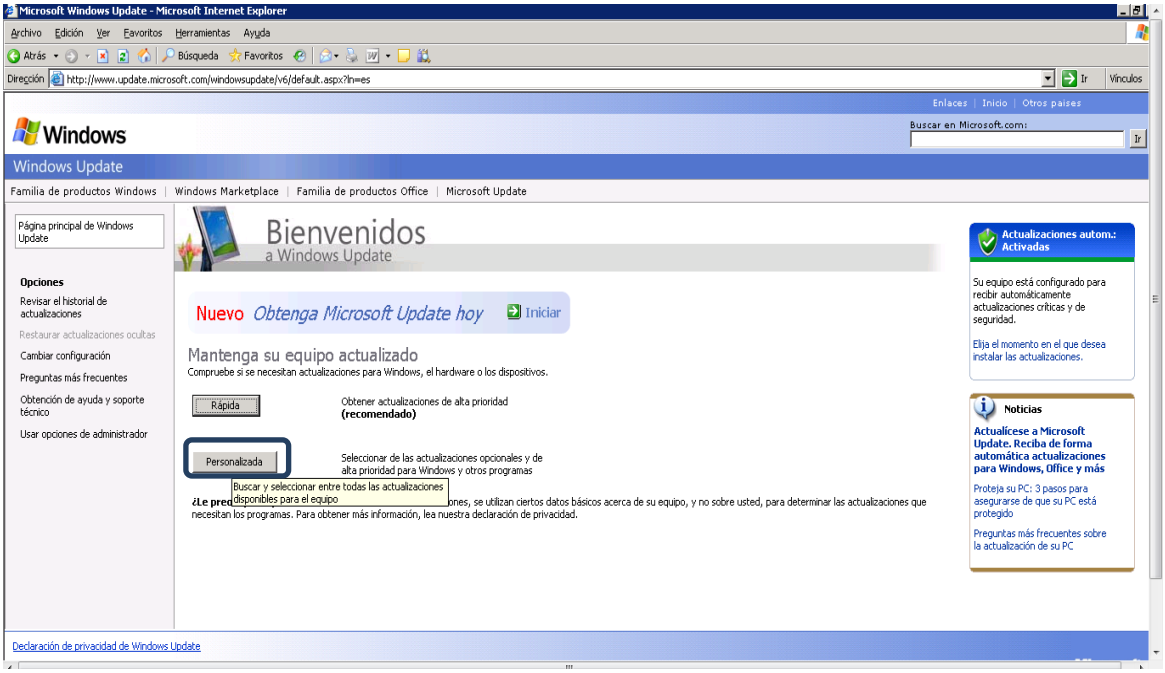


Figura 3.37 Análisis personalizado

Una vez realizado todo esto se muestra un estatus del nivel de actualización del sistema y especifica por categoría cuáles son las actualizaciones críticas a realizar, cuáles son las opcionales y por aplicaciones, a continuación, se muestran algunos resultados obtenidos dentro de los servidores antes mencionados.

En uno de los servidores se encontró una completa desactualización ya que ni siquiera se cuenta con el Service Pack 2 instalado, último pack lanzado por Microsoft para Windows Server 2003, para este servidor las actualizaciones fueron muy amplias lo cual requirió un mucho tiempo de descarga e instalación. Ver figura 3.38

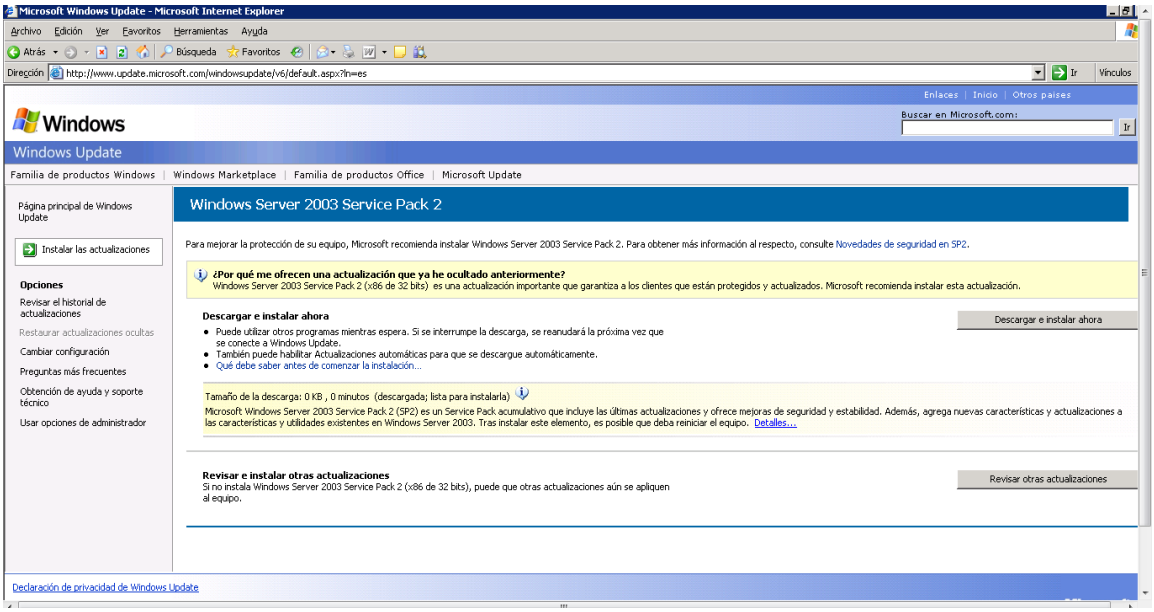


Figura3.38 Windows Server 2003 sin Service Pack 2

Dentro de otro de los servidores de alta prioridad para la empresa lo que se encontró fue una alta desactualización, aunque ya se contaba con el ultimo Service pack, aun así se encontraron más de sesenta actualizaciones críticas y algunas opcionales, también el tiempo de descarga y de instalación para este servidor fue bastante amplio. Ver figura 3.39

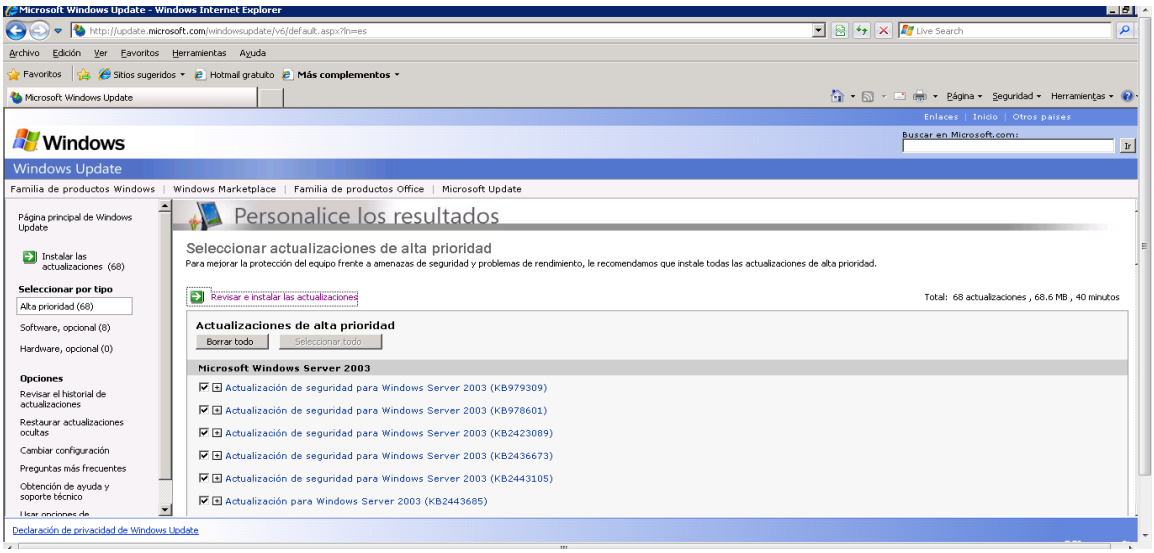


Figura 3.39 Se requerían más de 60 actualizaciones críticas

En otro servidor se encontró que existen 32 actualizaciones críticas y 9 opcionales así como otras tantas por aplicaciones. Ver figura 3.40

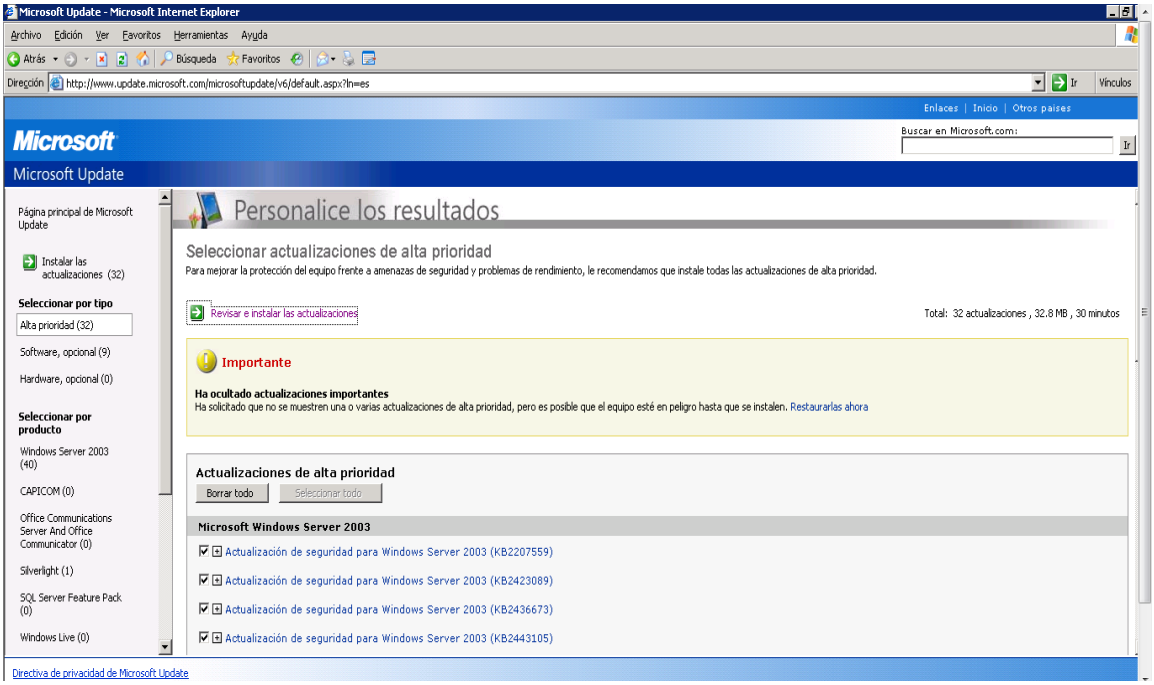


Figura 3.40 Se requieren 32 actualizaciones críticas y muchas por aplicación

Existieron algunos servidores tanto de servicios críticos como demo que no requerían actualizaciones críticas, sólo algunas opcionales o de aplicaciones. Ver figura 3.41

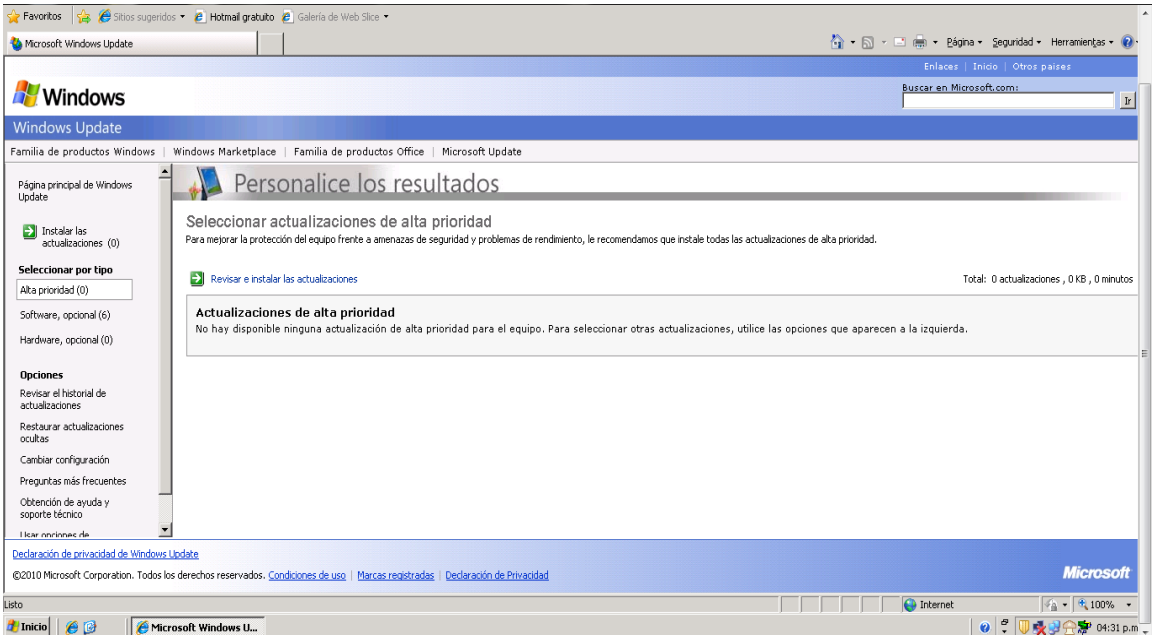


Figura 3.41 Sin actualización críticas sólo opcionales

Al realizar la actualización de todos los servidores por medio de la herramienta Windows Update, se encontró que muchos de los servidores con los que cuenta la infraestructura de Tecnologías de la Información y de las Comunicaciones dentro de la organización se hallaban sumamente desactualizados, lo que proveía grandes vulnerabilidades ya que se encontraron hasta 132 actualizaciones faltantes en ellos y como se comenta, existen algunos que no contaban con el último Service Pack. Se pudo observar es que los últimos servidores lanzados a producción fueron los que requerían menos actualizaciones críticas o ya contaban con todas sus actualización y otros parches de aseguramiento, a diferencia de los servidores más antiguos de la empresa donde se encontraron las mayores vulnerabilidades.

Concluida esta parte de la actividad se lleva a cabo un análisis dentro de los boletines de seguridad de Microsoft de los más recientes bugs e incidentes, por este medio podemos tener datos más detallados acerca de algún problema que se haya suscitado o que pueda llegar a ocurrir.

Dentro del portal de Microsoft Security Bulletin:
http://www.microsoft.com/technet/security/current.aspx

Por medio de este sitio dedicado de Microsoft podemos obtener mucha información de las actualizaciones de seguridad, los agujeros existentes, sistemas afectados y una amplia descripción de los problemas o bugs encontrados.

3.3.9 Instalación y configuración de la consola de administración Symantec Endpoint

En esta actividad de realiza la instalación y configuración de la consola de administración de antivirus para aislar y proteger la red interna y sus servidores de ataques como son virus, gusanos, caballos de Troya, software espía (spyware), adware(software de publicidad no deseada), bots, las amenazas de día cero y los rootkits.

A continuación se presentan características con las que cuenta la aplicación.

Características

- Consola de administración centralizada

Cuenta con un único agente e interfaz integrada para su administración. Permite un método de comunicación y un sistema de entrega de contenidos unificados.

- Brinda una solución de actualización para software y políticas.
- Proporciona informes unificados y centrales.
- Reduce la carga administrativa.

- Control de dispositivos para evitar fuga de datos
- Protección en contra de mp3,USB,etc

- Prevención de intrusos basada en comportamiento
- Inspección de trafico de red, agrega protección basada en vulnerabilidades

- Políticas adaptativas relacionadas con la localización

- Incluye tecnología VxMS(Veritas)

- Certificaciones Virus Bulletin

➢ Análisis proactivo de amenazas

Protección basada en el comportamiento que protege contra las amenazas de día cero. Utilización de tecnología heurística, consiste en un sistema de puntuación con base en comportamientos buenos y malos de las aplicaciones desconocidas, proporciona una detección del software malicioso.

- Detecta los programas maliciosos
- Ayuda a reducir la cantidad de falsos positivos

➢ Detección y eliminación de rootkit

Permite la detección y eliminación de rootkit, integra VxMS (Veritas MappingService) que permite acceder por debajo del sistema operativo para un análisis y una reparación completa.

- Detecta y elimina los rootkits

- Control de las aplicaciones

Permite controlar el acceso a procesos, archivos y carpetas específicos creados por usuarios y otras aplicaciones. Brinda análisis de aplicaciones, control de procesos, control de acceso al registro y archivos, y control de módulos y librerías DLL. Permite restringir ciertas actividades consideradas sospechosas o de alto riesgo.

- Evita que el software malicioso se propague o dañe los endpoints
- Bloquea los endpoints para prevenir la fuga de datos

- Control de dispositivos

Controla periféricos conectados a un equipo y su uso. Bloquea los endpoints para impedir que se conecten las unidades thumbdrive, las grabadoras de CD, las impresoras y otros dispositivos USB.

- Evita que la información confidencial sea extraída o robada de los endpoints (fuga de datos)
- Evita que los virus infecten los endpoints desde los dispositivos periféricos

Arquitectura Consola de Administración

La consola de administración se encuentra dentro de la LAN de la organización. Ver figura 3.42

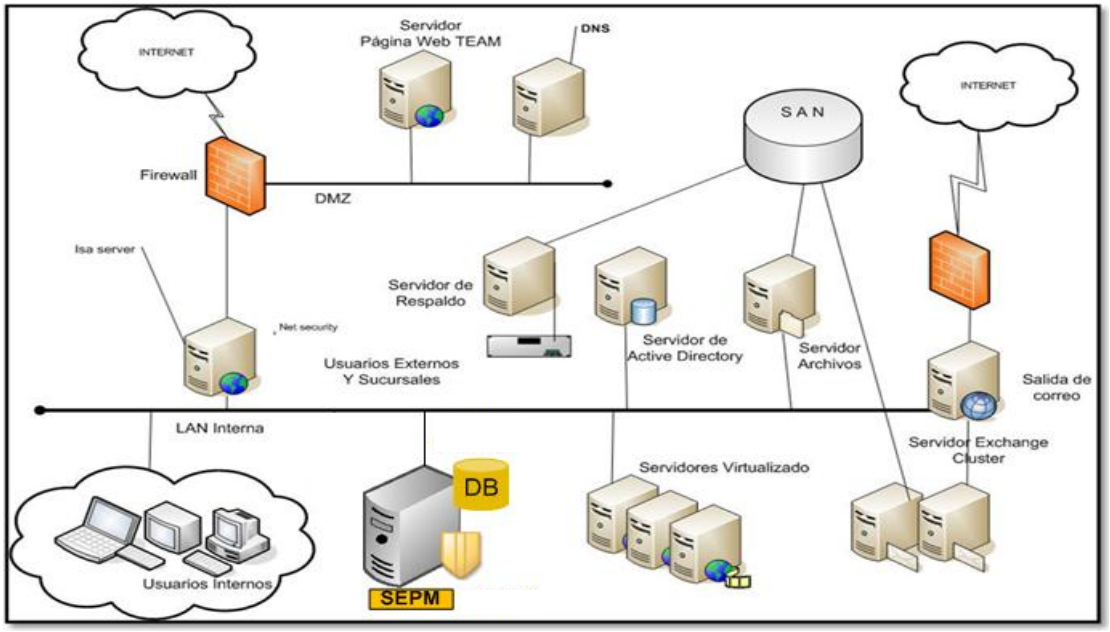


Figura 3.42 Arquitectura de la consola de administración

Para realizar la implementación de la consola de administración y para su configuración se realiza un análisis previo con los siguientes resultados de acuerdo a los requerimientos de la organización.

Políticas	Configuraciones

Grupos	• TEAM
	  • ALMACÉN
	  • CHAMPIONS
	  • MERCADOTECNIA
	  • SERVIDORES
	  • SISTEMAS
	  • VENTAS

Antivirus y Protección Contra Software Espía	• Política, antivirus y contra software espía- Seguridad Elevada • (ALMACÉN, CHAMPIONS , SERVIDORES, SISTEMAS) • Política, antivirus y contra software espía- Alto Rendimiento • (VENTAS, MERCADOTECNIA)
Firewall	• Política de Firewall • (ALMACÉN,CHAMPIONS,DIRECTIVOS,MERCADOTECNIA, SISTEMAS Y VENTAS) • Política de Firewall para Servidores (SERVIDORES)
Prevención de Intrusiones	• Política de Prevención de Intrusiones • (ALMACÉN, CHAMPIONS, MERCADOTECNIA, SISTEMAS Y VENTAS) • Política de Prevención de Intrusiones para Servidores (SERVIDORES)
Control de Aplicaciones y Dispositivos	• Política de Control de Aplicaciones y Dispositivos (SERVIDORES, SISTEMAS) • Política de Control de Aplicaciones y Dispositivos • (ALMACÉN,CHAMPIONS,)
Excepciones Centralizadas	• NINGUNA

Actualizaciones	• Actualizaciones Diarias
	• Estaciones de Trabajo
	  • (13:00 a 14:00)hrs - (ALMACÉN)
	  • (14:00 a 15:00)hrs - (VENTAS/MERCADOTENIA)
	  • (15:00 a 16:00)hrs – (CHAMPIONS/SISTEMAS)
	• Para SERVIDORES
	  • (7:00) (20:00)

Análisis Programado	• Análisis Programado • MARTES - JUEVES • (13:30 a 14:30)hrs - (ALMACÉN)

	• (14:30 a 15:30)hrs - (VENTAS/MERCADOTENIA) • (15:30 a 16:30)hrs – (CHAMPIONS/SISTEMAS) • Para SERVIDORES • DIARIO A LAS SERVIDORES A LAS • (22:00 hrs)
Control de Aplicaciones y de Dispositivos	• Bloqueo de USB(VENTAS, ALMACÉN)
Configuración General (Configuración de Seguridad)	• Solicitar una contraseña para abrir la interfaz del usuario del cliente • Solicitar una contraseña para detener el servicio del cliente • Solicitar una contraseña para importar o exportar una política • Solicitar una contraseña para desinstalar el cliente (**********)

Instalación de Symantec Endpoint Protection 11 Manager

Instalación de Symantec Endpoint Protection Manager con la utilización de la base de datos Sybase.

Pasos Iniciales

- Servidor
- IP estática.
- Instalación de IIS
- Contar con los archivos de instalación los cuales estarán ubicados en el escritorio. Los archivos están en la Media de Instalación o pueden ser descargados de la página *https://fileconnect.symantec.com*, con el número de serie el cual se encuentra en el certificado emitido por Symantec
- Instalar y actualizar el software Symantec Endpoint Protecction
- Asegurarse de que los puertos seleccionados no estén ya en uso en el servidor Symantec Endpoint Protection 11

Pasos para la instalación

1. Se localizan los archivos de instalación de Symantec Endpoint Protection Manager. Ver figura 3.43

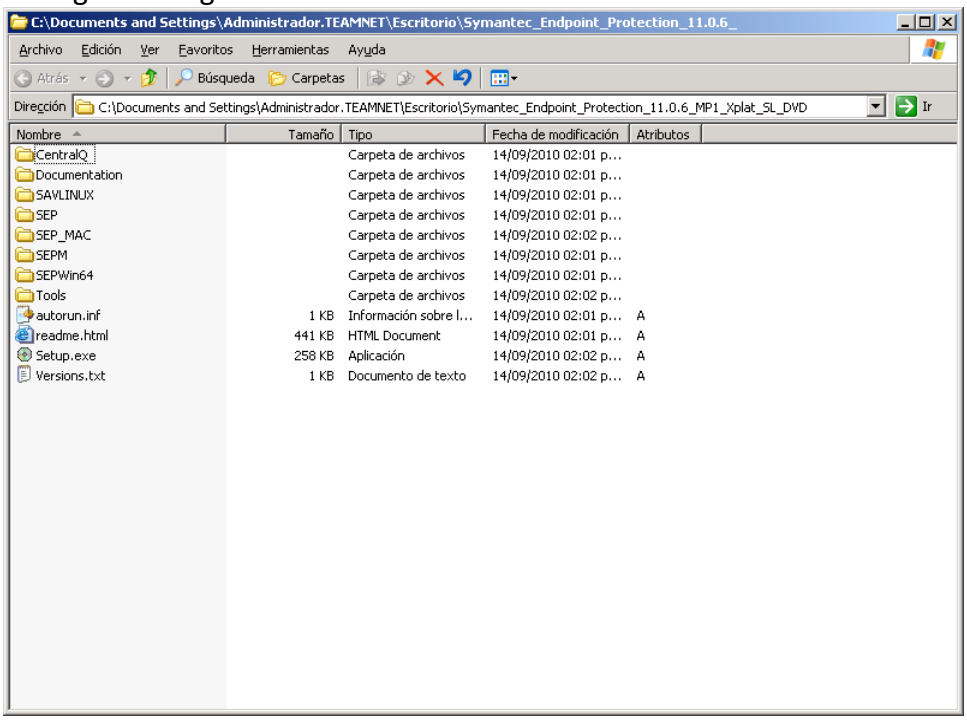


Figura 3.43 Archivos de Instalación

2. Se ejecuta la aplicación Setup.exe.

3. Una vez que se lance el asistente de instalación, haga clic sobre *Instalar Symantec Endpoint Protection Manager* para instalar la consola y el servidor de administración. Ver figura 3.44

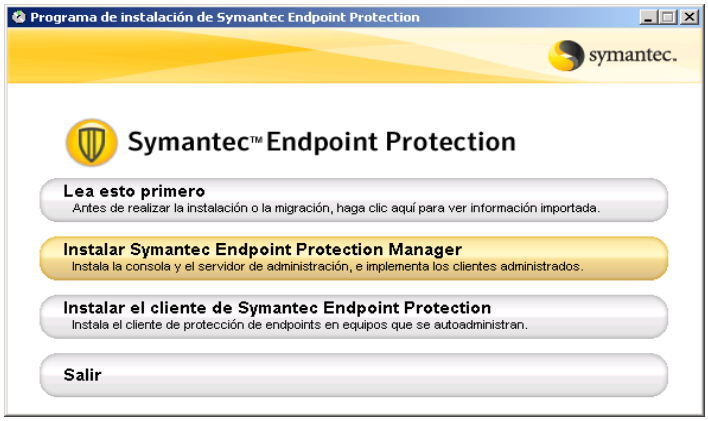


Figura 3.44 Asistente de instalación

4. Cuando aparezca la pantalla *Asistente de instalación de Symantec Endpoint Protection Managar*clic en Siguiente. Ver figura 3.45

Figura 3.45 Asistente de instalación

5. Clic sobre *Acepto los términos del contrato de licencia* y dar *Siguiente*. Ver figura 3.46

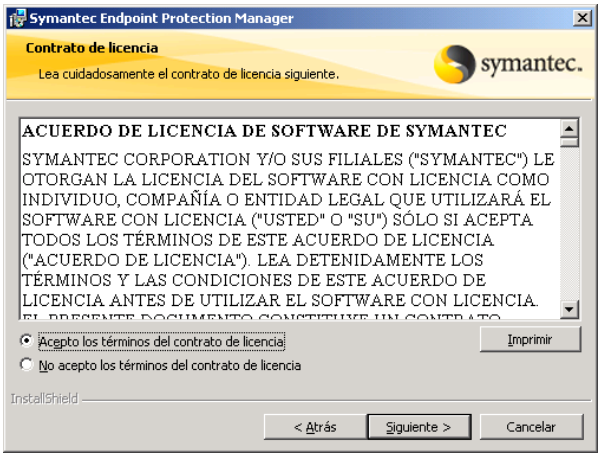


Figura 3.46 Términos de licencia

6. Se indica la ruta de instalación por default (la cual fue consultada con el administrador de sistemas) *C:\Archivos de Programa\Symantec\Symantec Endpoint Protection Manager*, clic en *Siguiente.* Para la implementación en la organización, se utiliza la ruta por default. Ver figura 3.47

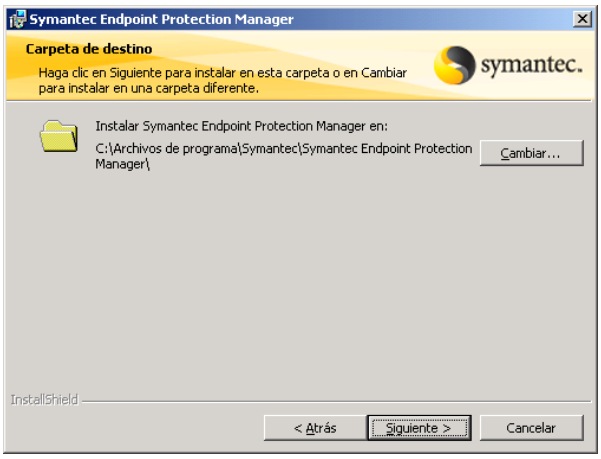


Figura 3.47 Ruta de instalación

7. Se seleccionan las opciones de configuración del sitio Web IIS. Se recomienda por seguridad que Symantec Endpoint Protection Manager utilice su propio sitio web personalizado. Seleccionamos la opción *Crear un sitio web personalizado y el puerto a utilizar [8014].*Ver figura 3.48

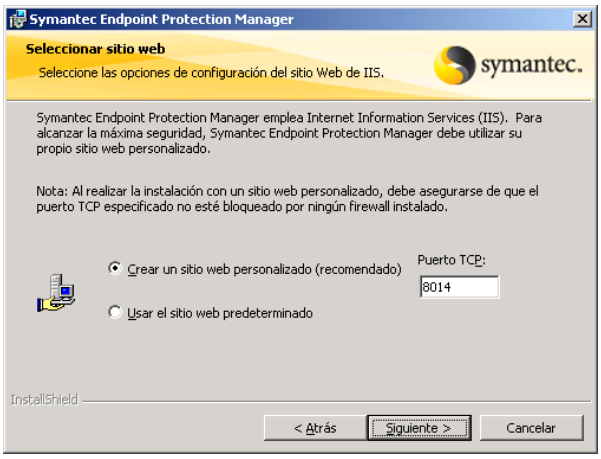


Figura 3.48 Configuración del sitio web IIS

8. Realizados los pasos anteriores se inicia la instalación de Symantec Endpoint Protection Manager, clic *Instalar.* Ver figura 3.49

Figura 3.49 Iniciar instalación

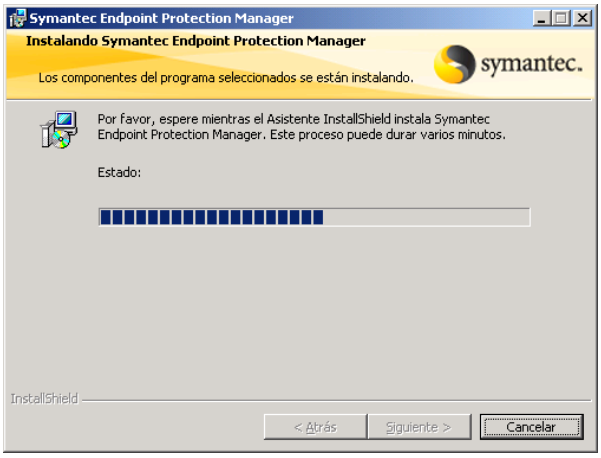


Figura 3.50 Estado de instalación

9. Ahora *Finalizar*.

Figura 3.51 instalación completa

10. Se inicia un asistente de configuración del servidor de administración, para la implementación de TEAM se selecciona el tipo de configuración *Simple*, se administrarán un total de 85 equipos de trabajo utilizando la base de datos Sybase incluida en Symantec Endpoint Protection. Ver figura 3.52

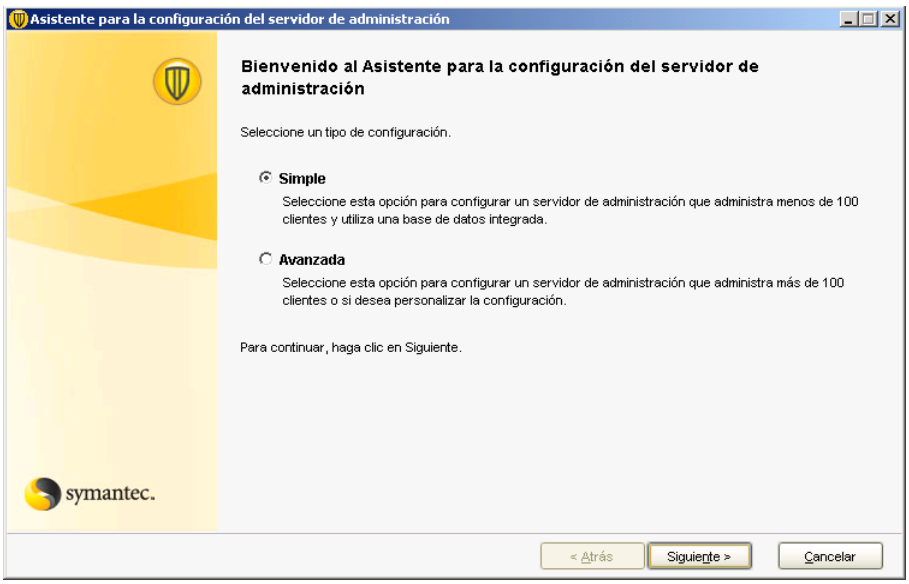


Figura 3.52 Asistente de configuración del servidor de administración

11. Se crea una cuenta de administrador de sistema, ésta permite iniciar sesión en la consola de administración. Ver figura 3.53

Usuario: *****
Contraseña: ********
Dirección de correo electrónico: soporte@teamnet.com.mx

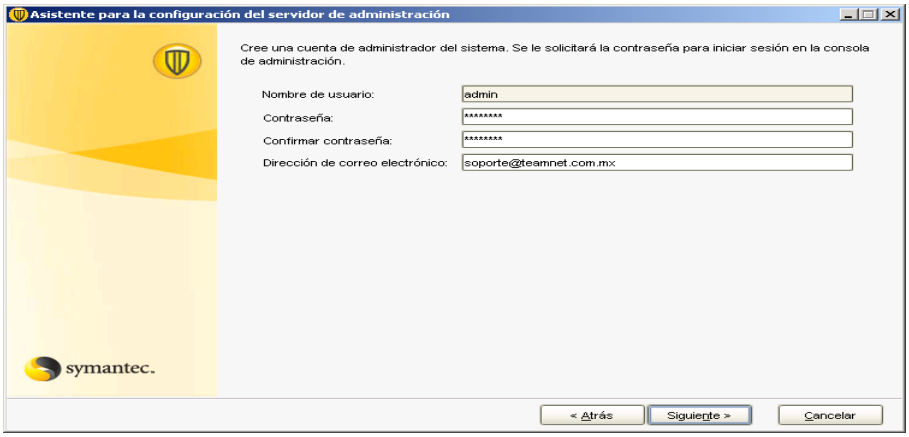


Figura 3.53 configuración de la cuenta de administrador

12. Se activa la casilla “Envío anónimo de información de uso del sistema”, para mejoras de funcionalidad de las soluciones de seguridad para Endpoints. Ver figura 3.54

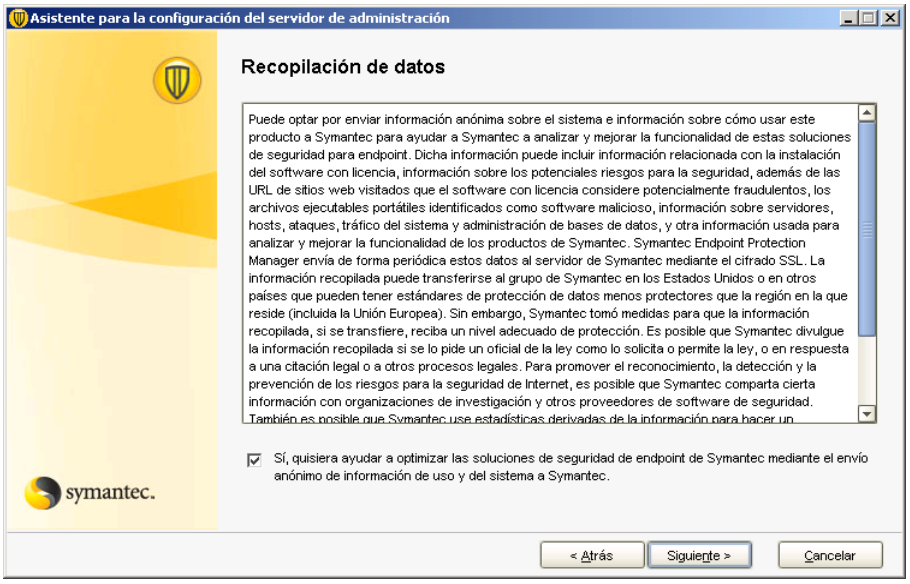


Figura 3.54 Recopilación de datos

13. El asistente envía un resumen de la configuración del servidor de administración. Clic en *Siguiente.* Esperar a que se instale la base de datos.

    Para el caso de TEAM:

    - Nombre del sitio: My sitio
    - Nombre del servidor: *****
    - Puerto del servidor: ****
    - Puerto de acceso remoto: ****
    - Tipo de base de datos: Integrado
    - Nombre de la base de datos: sem5
    - Nombre de usuario: *****

14. Una vez confirmado que se ha configurado perfectamente el servidor de administración, indica si se quiere ejecutar el asistente de migración y distribución ahora, para la implementación indico que *No*, ya que esto realiza la configuración del servidor y las políticas, esto se realiza posteriormente. Ver figura 3.55

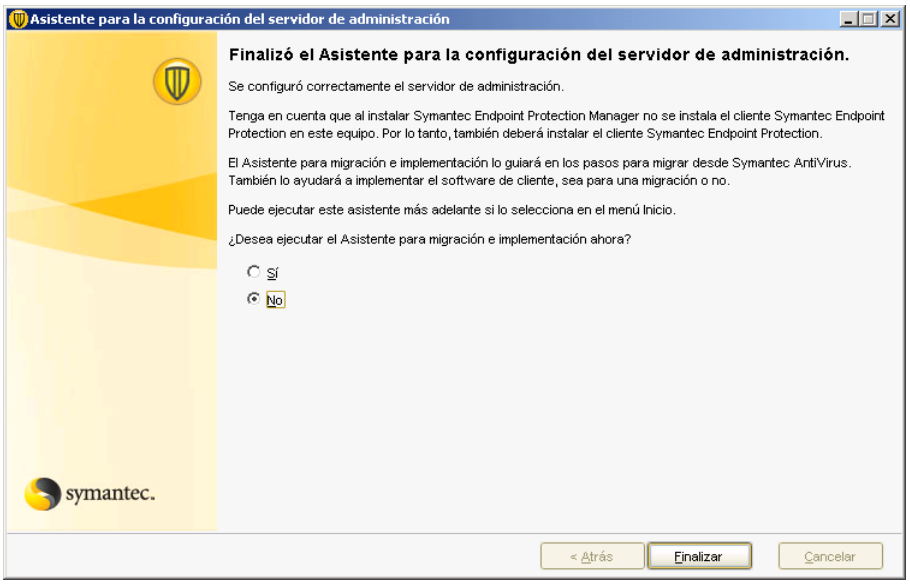


Figura 3.56 Finaliza configuración del servidor de administración

Configuración de Symantec Endpoint Protection Manager

Se realiza la configuración de Symantec Endpoint Protection Manager con la utilización de la base de datos Sybase.

Pasos Iniciales

- Inicio de la Consola de Symantec Endpoint Protection Manager
- Configuración de Usuarios
- Configuración de Políticas (Antivirus y SofwareEspía, Firewall, Prevención de Intrusos, Live Update, Control de Aplicaciones y Dispositivos)

    1. Ir a Inicio > Programas > Symantec Endpoint Protection Manager, dar clic, nos muestra la pantalla de Consola de Symantec Endpoint Protection Manager y nos autenticamos para tener acceso: Ver figura 3.57

        a. Usuario: *****

        b. Contraseña: **********

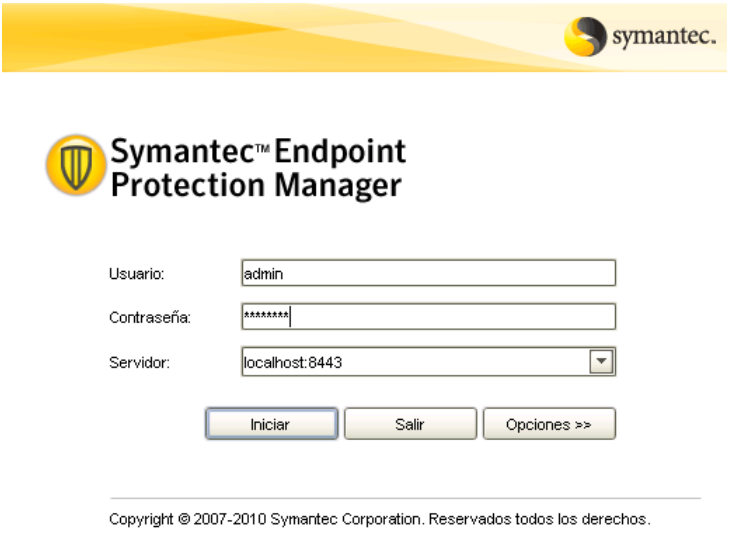


Figura 3.57 Autenticación consola de administración

2. Se puede ingresar a la Consola también por medio del explorador web Internet Explorer, con las siguientes opciones: Ver figura 3.58
    a. Consola Web de Endpoint Protection Manager
    b. Consola de Symantec Protection Manager
    c. Symantec Protection Center

Figura 3.58 Acceso Web

3. Clic en Consola web de Symantec Endpoint Protection Manager, esta es una consola de administración remota. Ver figura 3.59

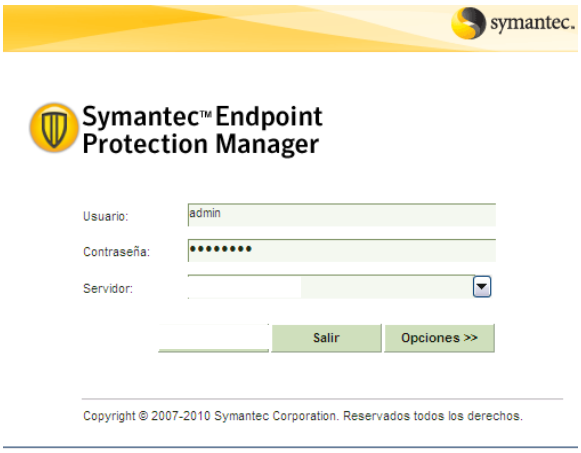


Figura 3.59 Consola de administración remota

4. Al ingresar se observan los menús de Symantec Endpoint Protection Manager (Página Principal, Supervisión, Informes, Políticas, Clientes y Administrador). Ver figura 3.60

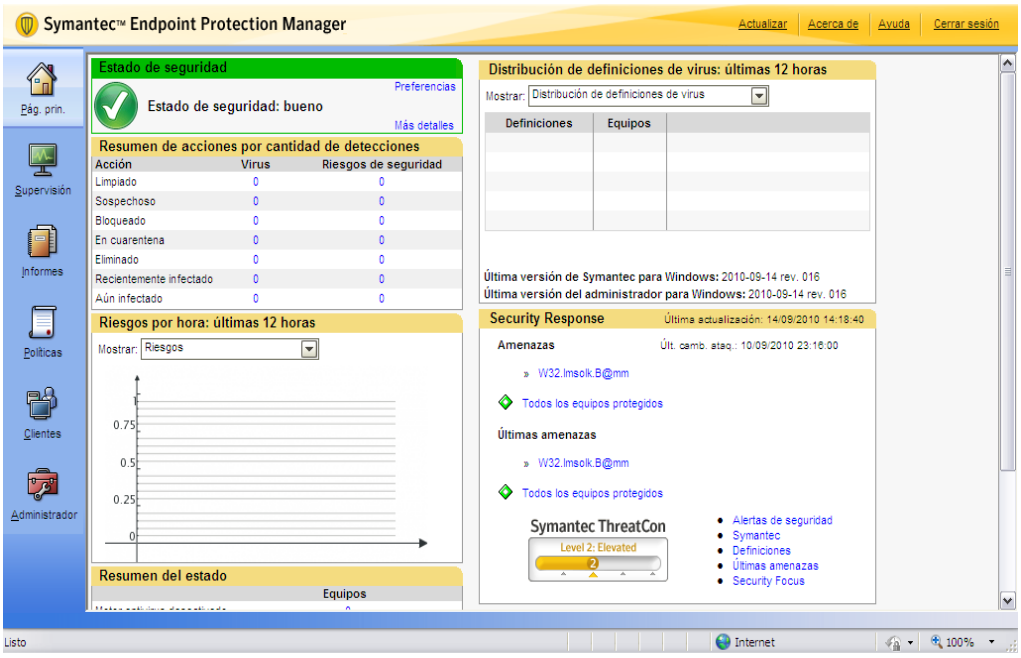


Figura 3.60 Página Principal consola de administración

5. La opción Symantec Protection Center permite acceder a varios productos Symantec y administrarlos, de esta forma se da de alta la consola Symantec de la organización. Ver figura 3.61

Figura 3.61 Symantec Protection Center

6. Por cuestiones de seguridad Symantec Protection Center nos solicita cambiar las credenciales. Ver figura 3.62

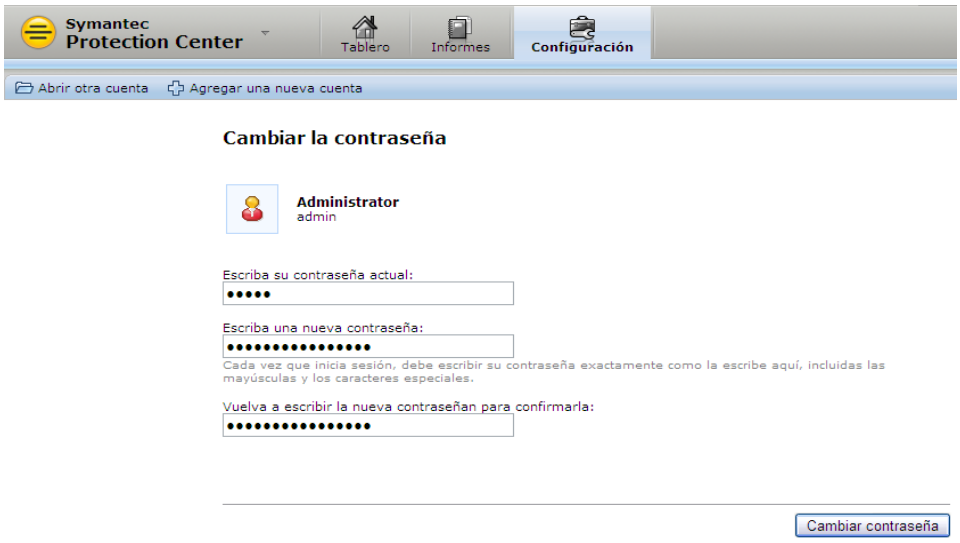


Figura 3.62 Cambio de credenciales de autenticación

7. Se realiza la configuración de nuestro Symantec Protection Center, se agrega el producto a administrar y comprobamos la conexión. Ver figura 3.63

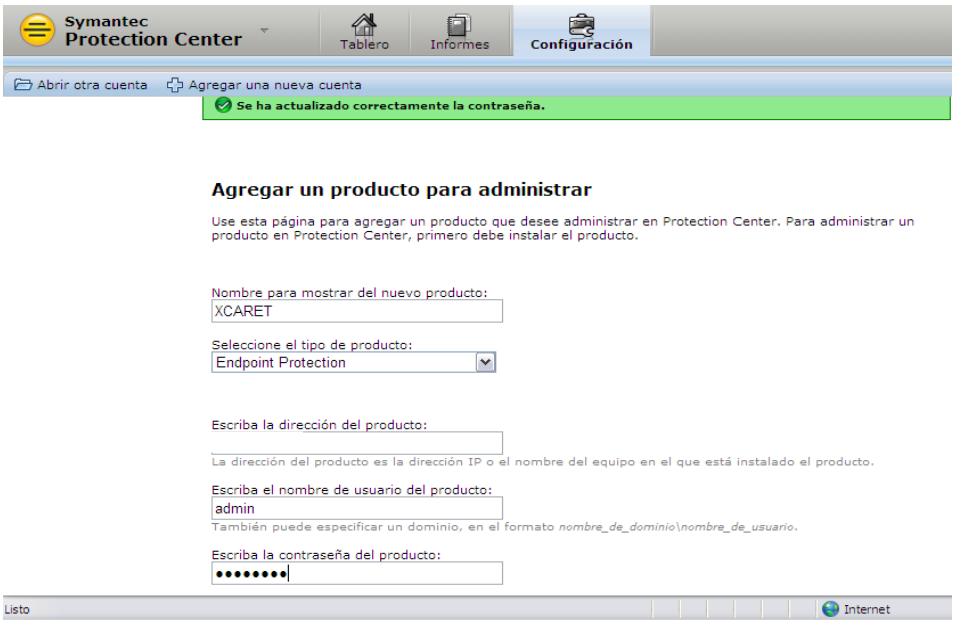


Figura 3.63 Configuración Symantec Protection Center

8. Se finaliza la configuración de nuestro Symantec Protection Center. Ver figura 3.64

Figura 3.64 Symantec Protection Center configurado

9. Continúo con la configuración de la Consola Symantec Endpoint Protection Manager, la cual descargará una aplicación Java. Ver figura 3.65

Figura 3.65 Descarga de aplicación Java

10. Después muestra la verificación de la firma digital de la aplicación, damos clic *Confiar siempre en el contenido de este editor,* damos clic en *Ejecutar*. Ver figura 3.66

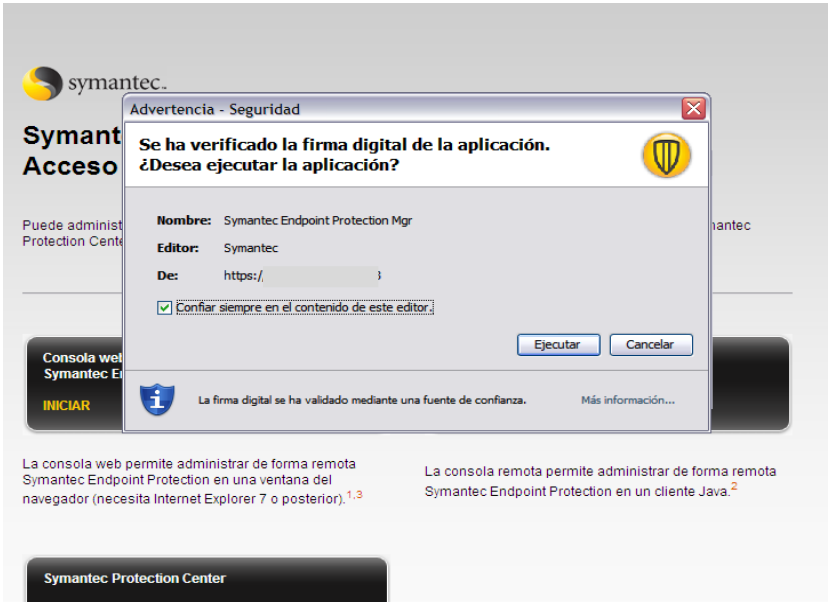


Figura 3.66 Verificación de firma digital

11. Ingresando a la consola de administración de Symantec Endpoint Protection, se realiza la configuración de las directivas y visualización de informes. Accedemos a la consola con las credenciales que fueron configuradas durante la implementación. Ver figura 3.67

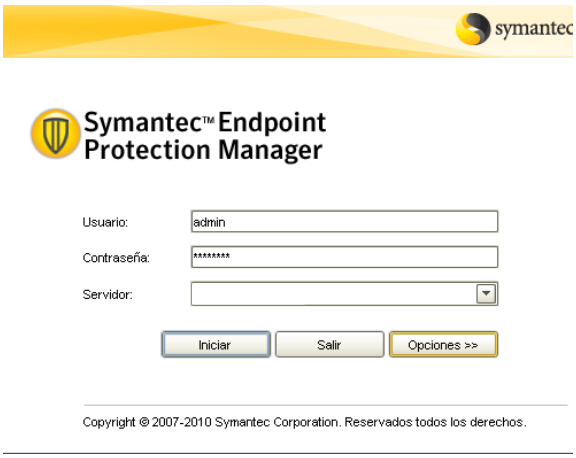


Figura 3.67 Acceso a la consola de administración Symantec Endpoint Protection Manager

12. Pantalla principal de la consola desde la pestaña *Pág. prin*, desde aquí se monitorea el estado de seguridad, cómo las infecciones en puestos y la tarea que se ha realizado en ellos, los riesgos que hemos tenido, si existen equipos sin antivirus o con problemas. Ver figura 3.68

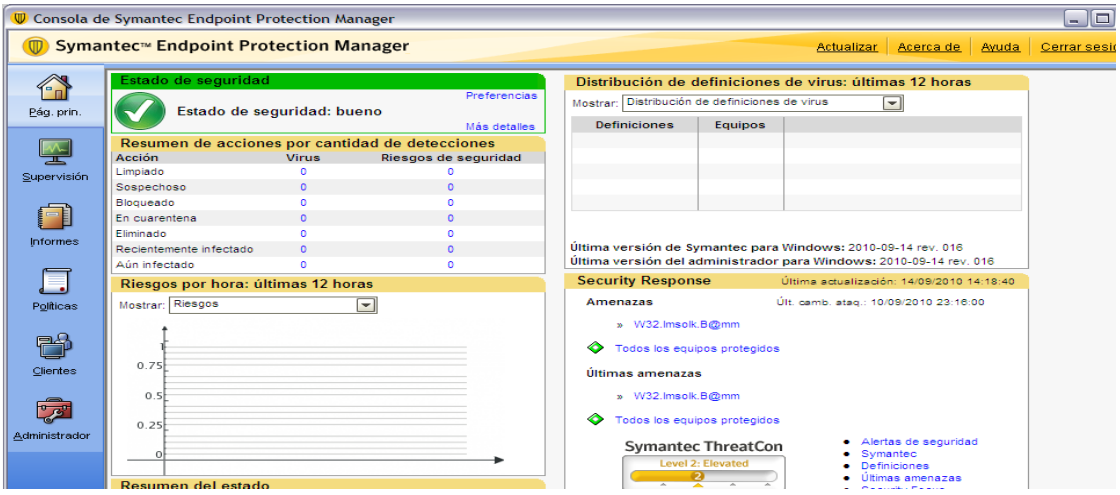


Figura 3.68 Pantalla Principal de administración

13. Como primer paso se crea un grupo para organizar los puestos, desde la pestaña *Clientes* pulsamos en *Agregar Grupo*. Se indica un nombre para el grupo donde se asignarán los puestos de la organización para posteriormente

aplicarles directivas/políticas de antivirus, antispyware, firewall y damos clic en *Aceptar*. Ver figura 3.69

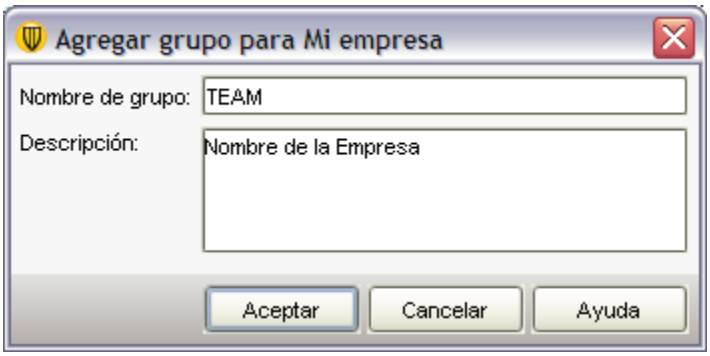


Figura 3.69 Agregar grupo

14. Esta es la estructura jerárquica para la administración de las estaciones de trabajo, equipos y servidores. Ver figura 3.70

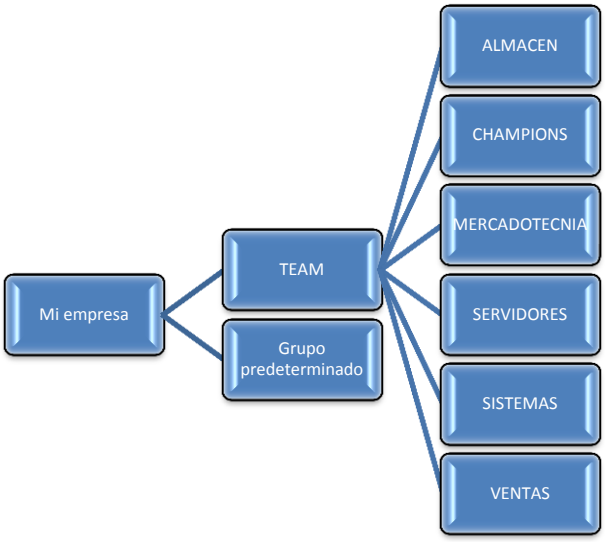


Figura 3.70 Estructura jerárquica de administración

15. En la Pestaña de *Clientes*, se observa el mapa jerárquico de administración. Ver figura 3.71

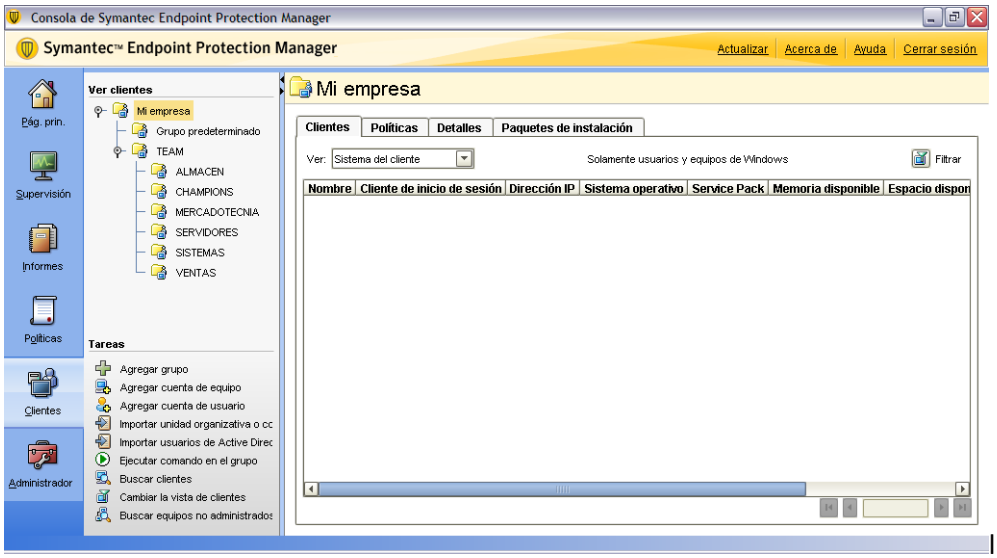


Figura 3.71 Mapa jerárquico de administración

16. En la pestaña *Administrador* se encuentra el dominio que está configurado. Así mismo en la parte de Servidores se observan los servidores del sitio u organización.

17. En la pestaña *Administrador>Paquetes de instalación*, se configuran todos los paquetes de instalación para los clientes TEAM, actualmente se cuenta con los siguientes, mismos que vienen configurados por default para 32 y 64 bits, respectivamente. Ver figura 3.72

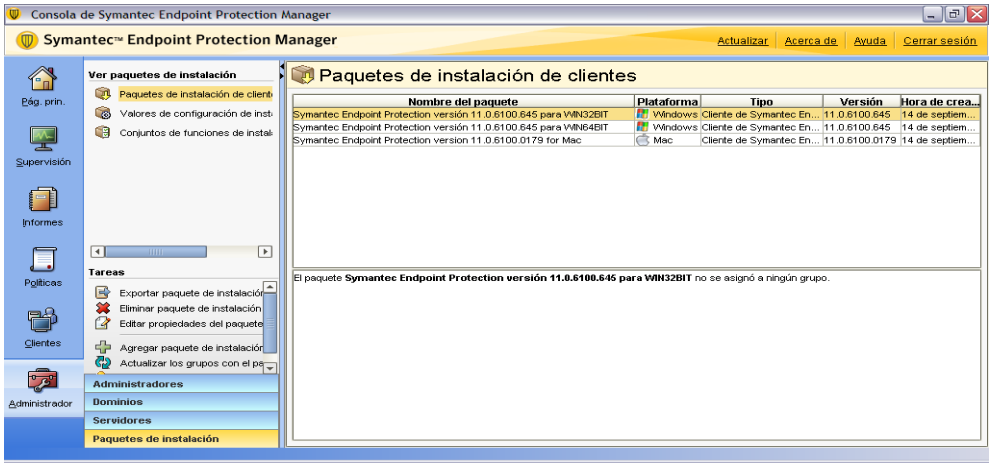


Figura 3.72 Paquetes de instalación de clientes

18. Dentro de *Valores de configuración de instalación de clientes* se crea un nuevo valor con una configuración especial para que la instalación se realice de manera transparente para el usuario final TEAM. Ver figura 3.73

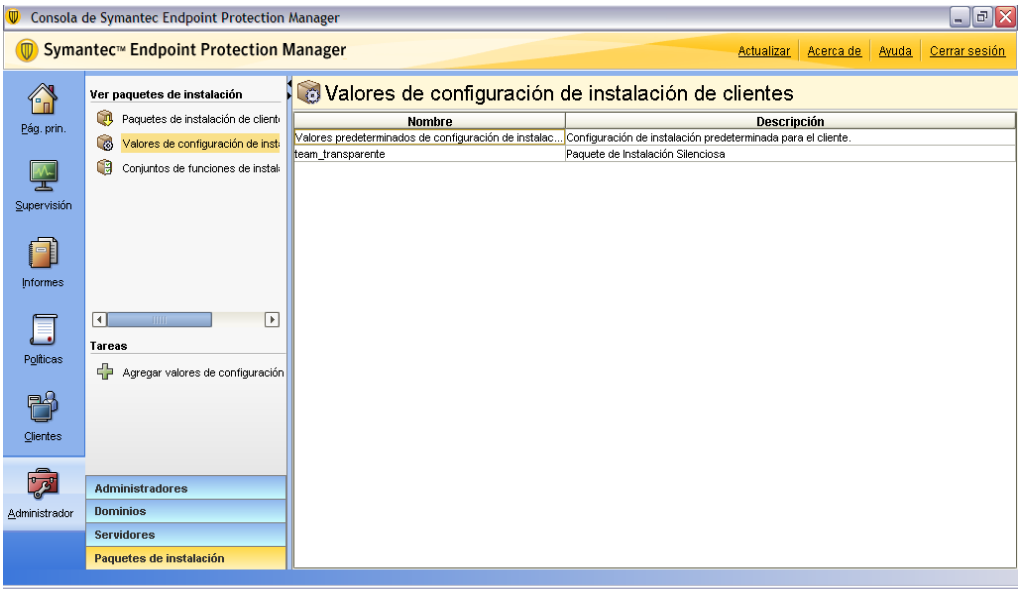


Figura 3.73 Valores de configuración de instalación de clientes

Se editan los valores de configuración para llevar a cabo una instalación transparente por medio de la opción de instalación silenciosa, ver figura 3.74 donde se configuran varios parámetros como:

- No reiniciar después de la instalación
- Ubicación a instalar
- Agregar al menú de inicio

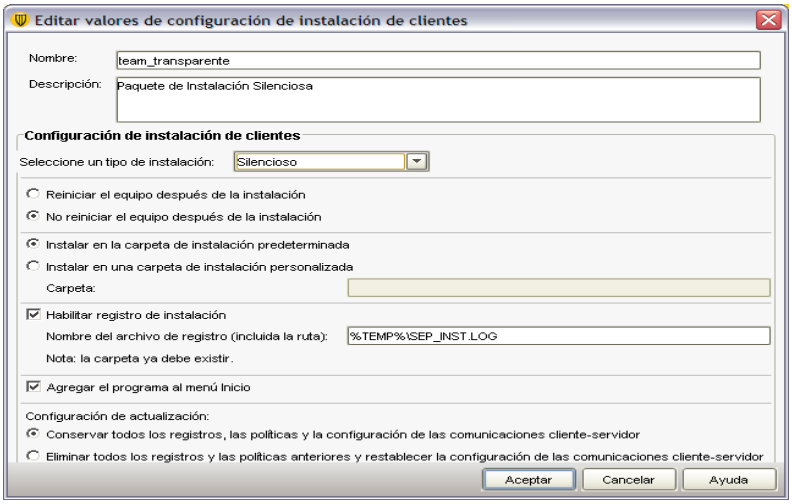


Figura 3.74 Parámetros de instalación

20. Dentro de *Administrador*, en la opción *Conjunto de Funciones de Instalación de Clientes* estas son las características que se instalan en los equipos TEAM cuando se envía la distribución de paquetes. Ver figura 3.75

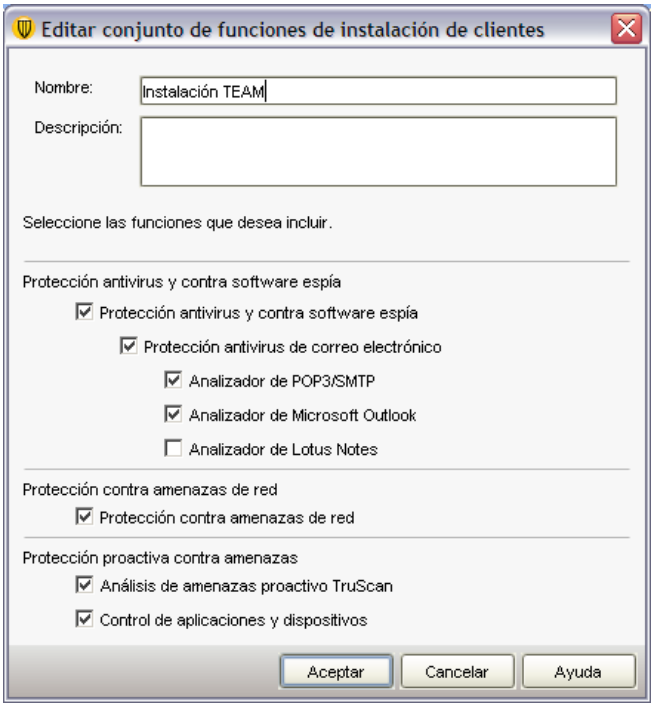


Figura 3.75 Conjunto de funciones de instalación de clientes

Configuración de Políticas Symantec Endpoint Protection Manager

Se realiza la configuración de políticas de Symantec Endpoint Protection Manager.

Pasos Iniciales

- Configuración de Políticas (Antivirus y Software Espía, Firewall, Prevención de Intrusos, Live Update, Control de Aplicaciones y Dispositivos)

Políticas de Antivirus y Protección de Software Espía

1. Para iniciar con la configuración de políticas, nos dirigimos a la sección de Políticas, donde podemos observar todas las opciones de configuración de paquetes que instalemos. Ver figura 3.76

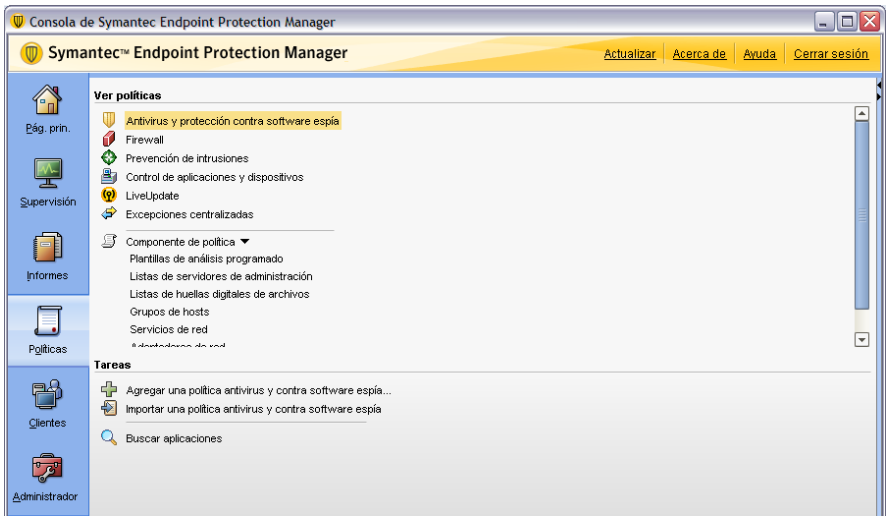


Figura 3.76 Políticas

2. Se inicia por la configuración del *Antivirus y Protección contra software espía*. En la opción *Tareas*, damos clic a la opción *Agregar una política de Antivirus y Protección contra software espía*. Se crea la política Antivirus y Contra Software Espía Servidores. Ver figura 3.77

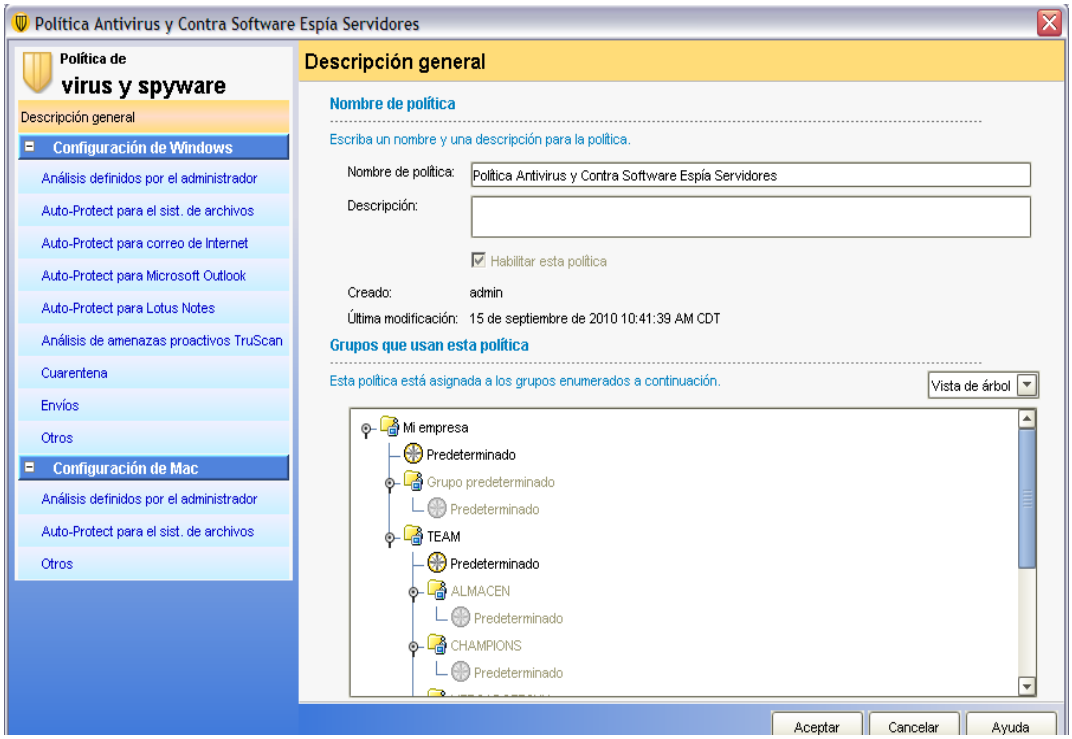


Figura 3.77 Política nueva

3. En la opción *Análisis definidos por el administrador*, se especifica cuándo se realizarán los análisis. (Día, hora, entre otros) Ver figura 3.78

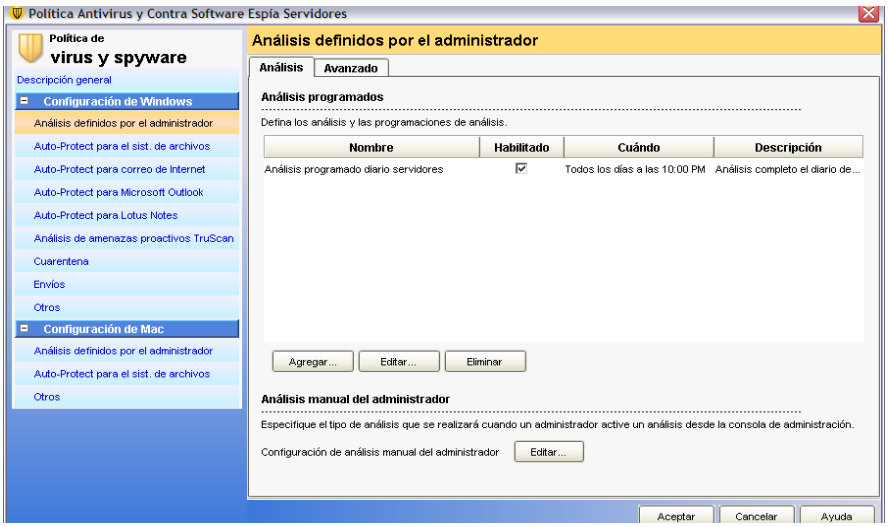


Figura 3.78 Configuración de análisis

4. Se configuran los *Análisis definidos por el administrador*, después en la pestaña de *Agregar*se seleccionan los análisis definidos o creamos un nuevo análisis. Ver figura 3.79

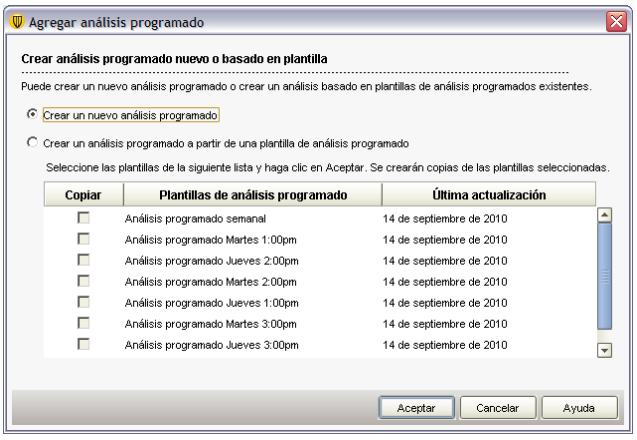


Figura 3.79 Agregar análisis

5. Dentro de la opción *Análisis manual del administrador* se configuran los detalles del análisis, las acciones, el análisis de archivos comprimidos y el ajuste del rendimiento del análisis, esto es sumamente importante debido a que esta sección debe adaptarse de acuerdo a los requerimientos de la empresa, dándole en algunos casos mayor prioridad al performance y optimizando aplicaciones. Ver figura 3.80

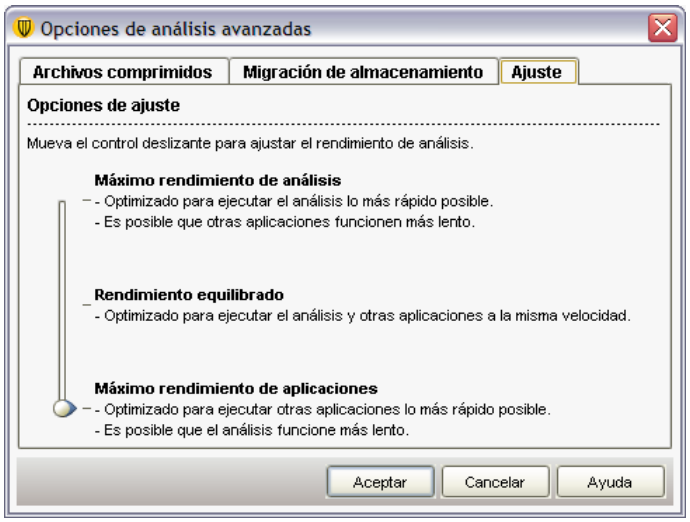


Figura 3.80 Ajuste de rendimiento

6. En la pestaña de *Avanzado* dentro de la opción *Análisis definidos por el administrador* se seleccionan las opciones de los análisis programados, los análisis al iniciar y análisis activados, así como las opciones de progreso de análisis. Ver figura 3.81

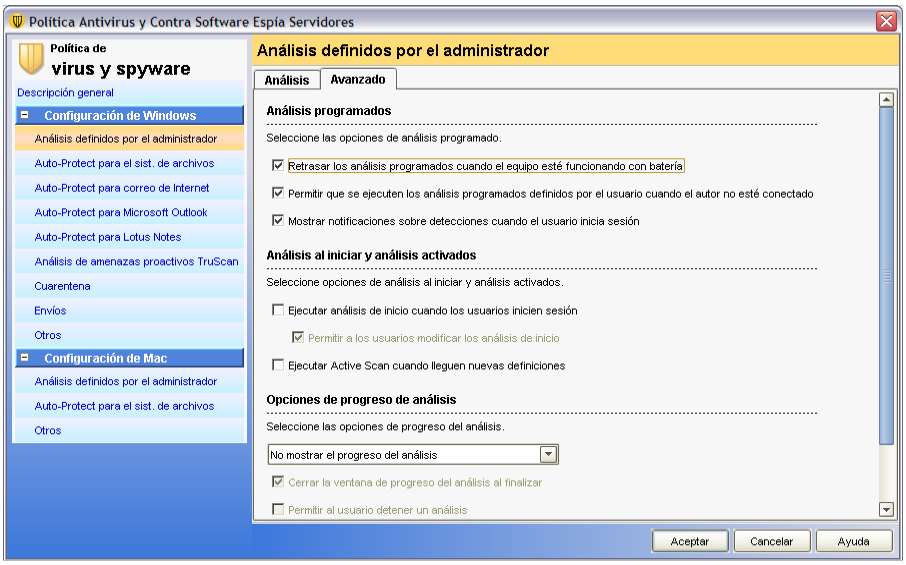


Figura 3.81 Configuración de análisis

7. En la pestaña *Auto-Protect para el sistema de archivos*, el análisis de archivos y procesos, así como las opciones de detección Bloodhound para analizar archivos en busca de comportamiento sospechoso (heurística), también se especifican las opciones de red para analizar archivos en equipos remotos. Para nuestra configuración en la red TEAM, no fue activada por cuestiones de performance. Ver figura 3.82

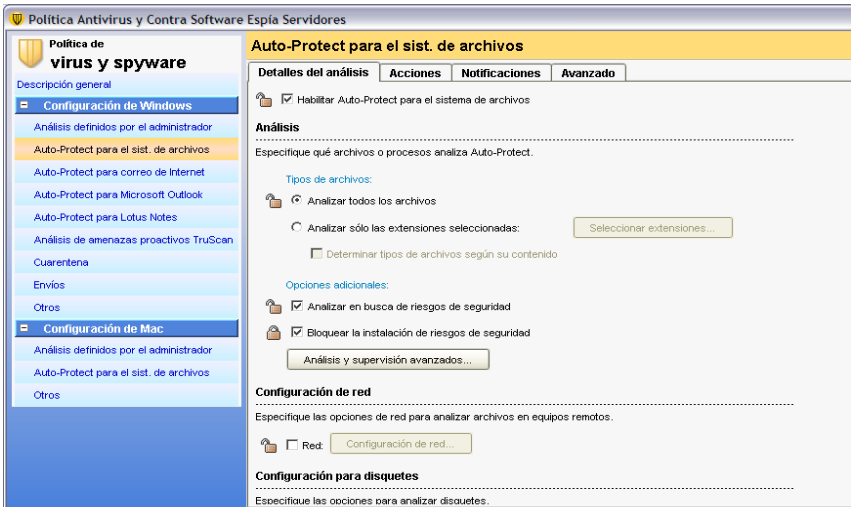


Figura 3.82 configuración Auto-Protect

8. Se activa la opción Auto-Protect para correo y se habilitan los archivos que serán analizados, así como la configuración de conexión de servidores de correo entrante/saliente (POP3/SMTP). Ver figura 3.83

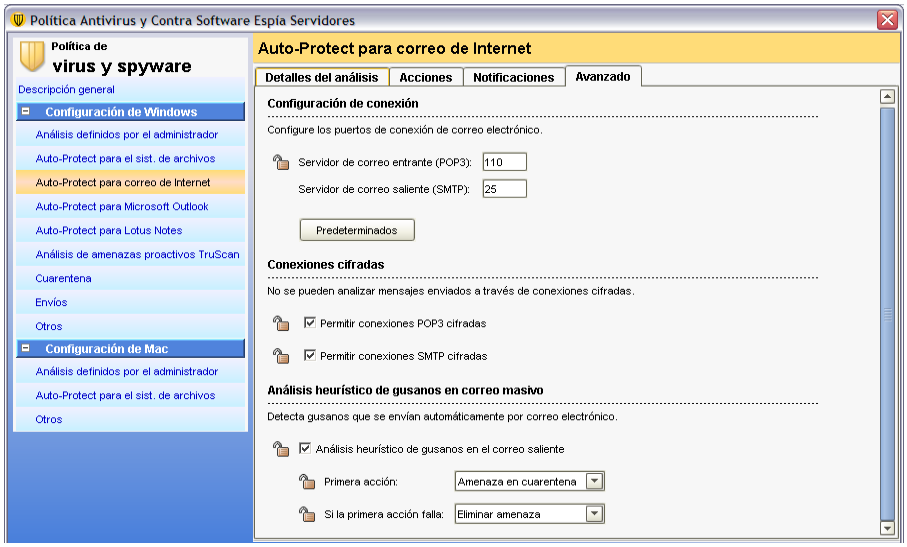


Figura 3.83 Auto-Protect para Correo de Internet

9. Se habilita la opción Auto-Protect para Microsoft Outlook, ya que en TEAM se cuenta con el servicio de correo bajo esta plataforma. Ver figura 3.84

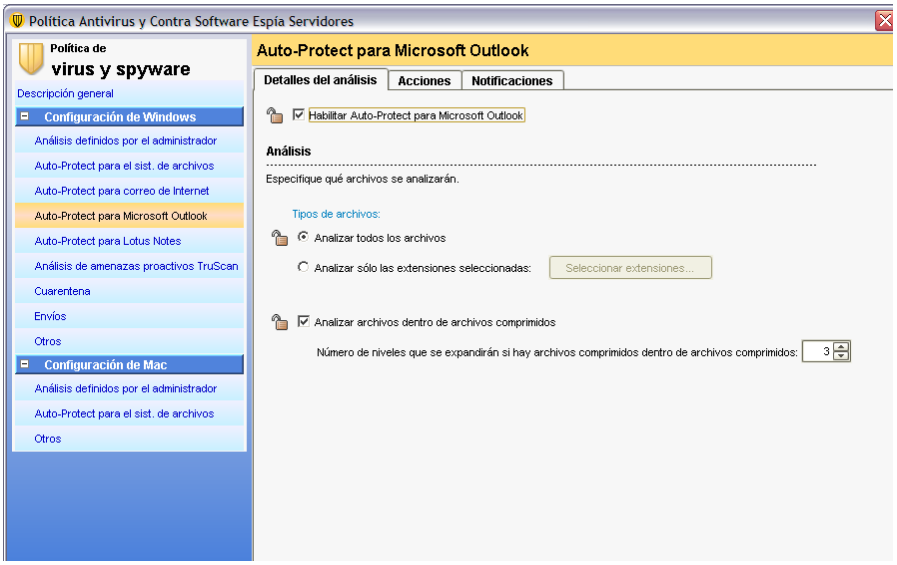


Figura 3.84 Configuración Auto-Protect para MS Outlook

10. La opción de Auto- Protect para Lotus Note queda deshabilitada ya que dentro de la infraestructura de la organización no se trabaja con esta plataforma. Ver figura 3.85

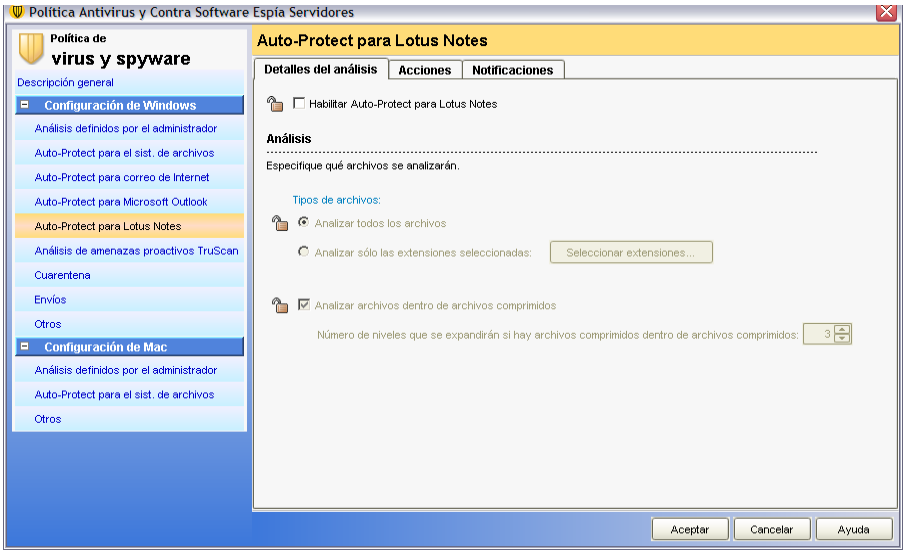


Figura 3.85 Configuración Auto-Protect para Lotus

11. Dentro de la configuración de *Análisis Proactivo* se mantienen las opciones que están asignadas como estándar para la Protección de Troyanos, gusanos, keyloogers, entre otros. Ver figura 3.86

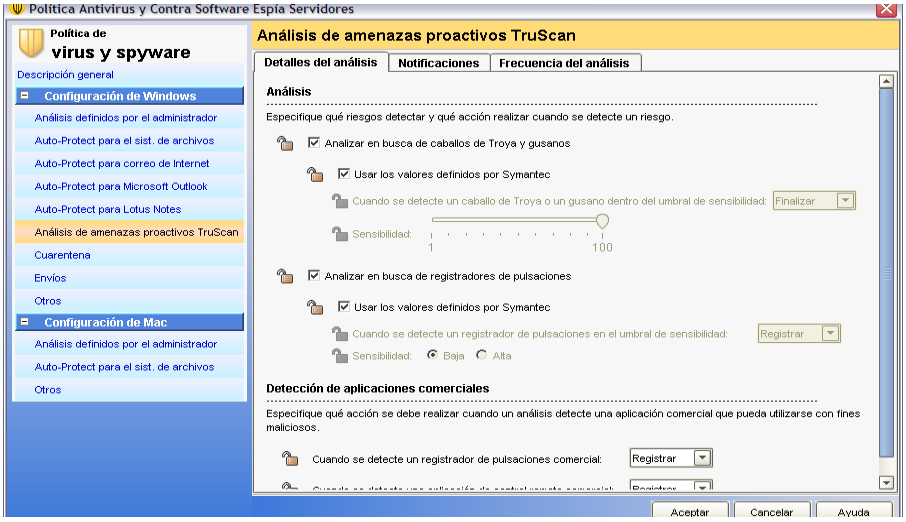


Figura 3.86 Configuración de Análisis de amenazas proactivos TruScan

12. Se configuran las opciones de *Cuarentena* y se establecen los días que permanecerán almacenados los archivos de esta forma. Ver figura 3.87, 3.88

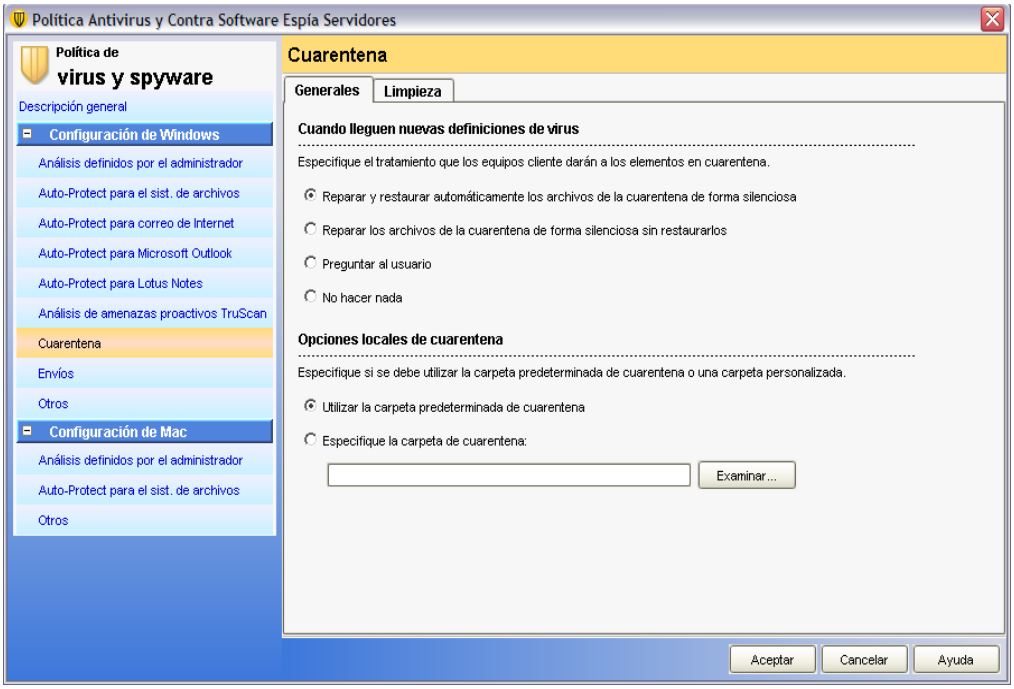


Figura 3.87 Configuración de cuarentena

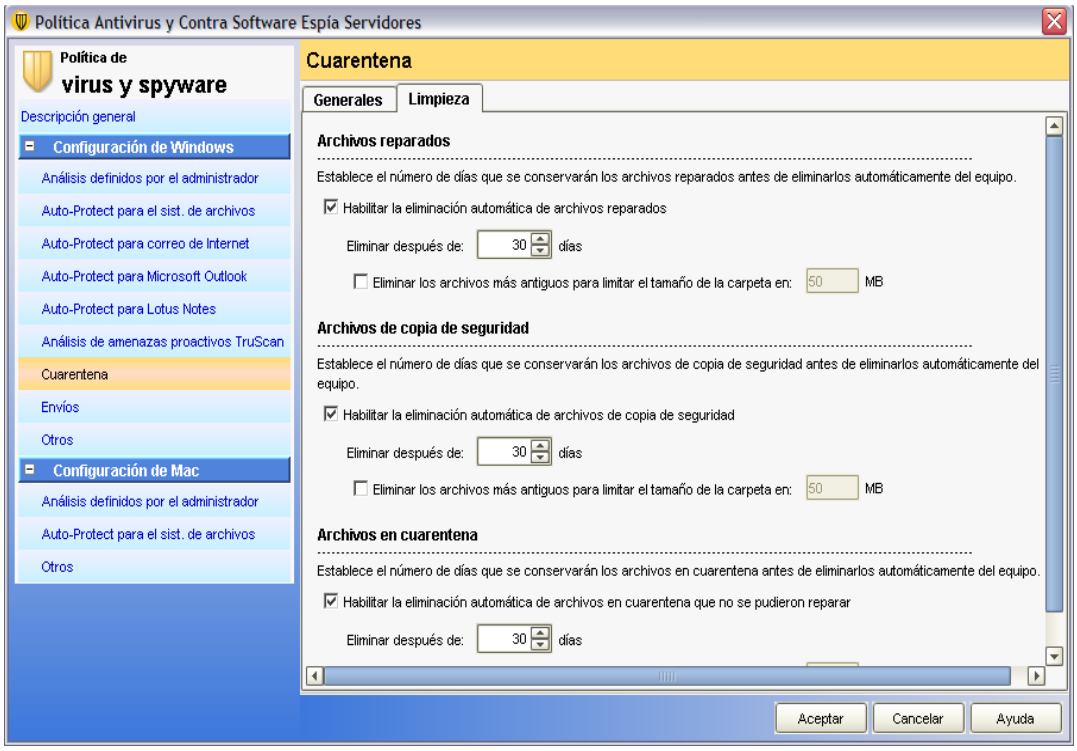


Figura 3.88 Configuración de cuarentena

13. En la configuración de *Envíos*, se especifica que los clientes puedan enviar información a Symantec Security Response acerca de los procesos detectados por los análisis de amenazas proactivos TruScan. Ver figura 3.89

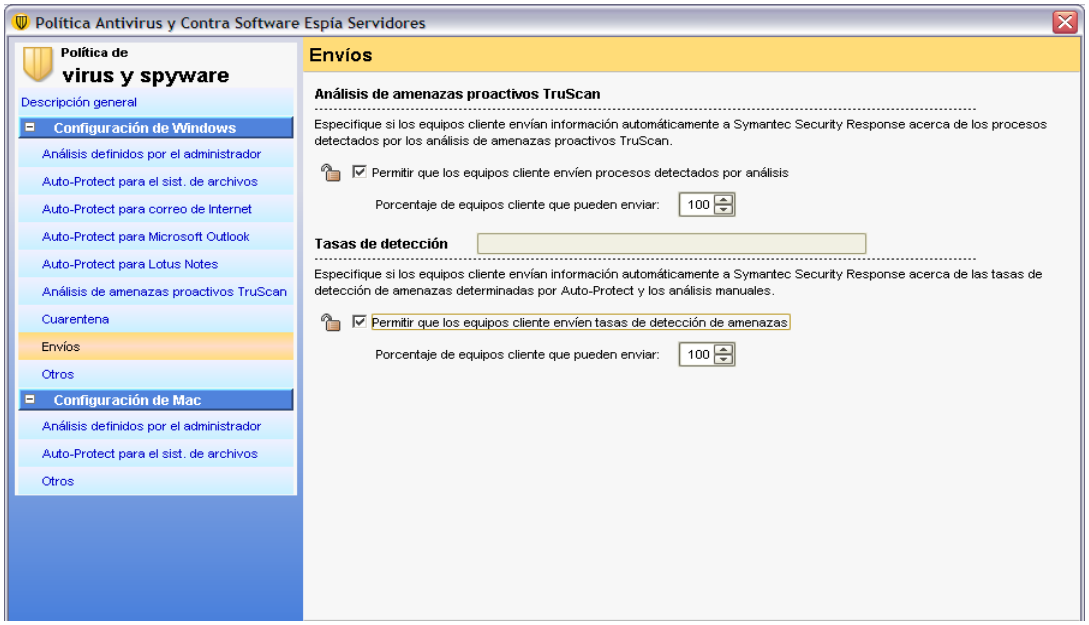


Figura 3.89 Configuración de envíos a Symantec Security Response

14. En la opción *Otros*, se especifica cómo funciona el Centro de seguridad de Windows con Symantec Endpoint Protection. Ver figura 3.90

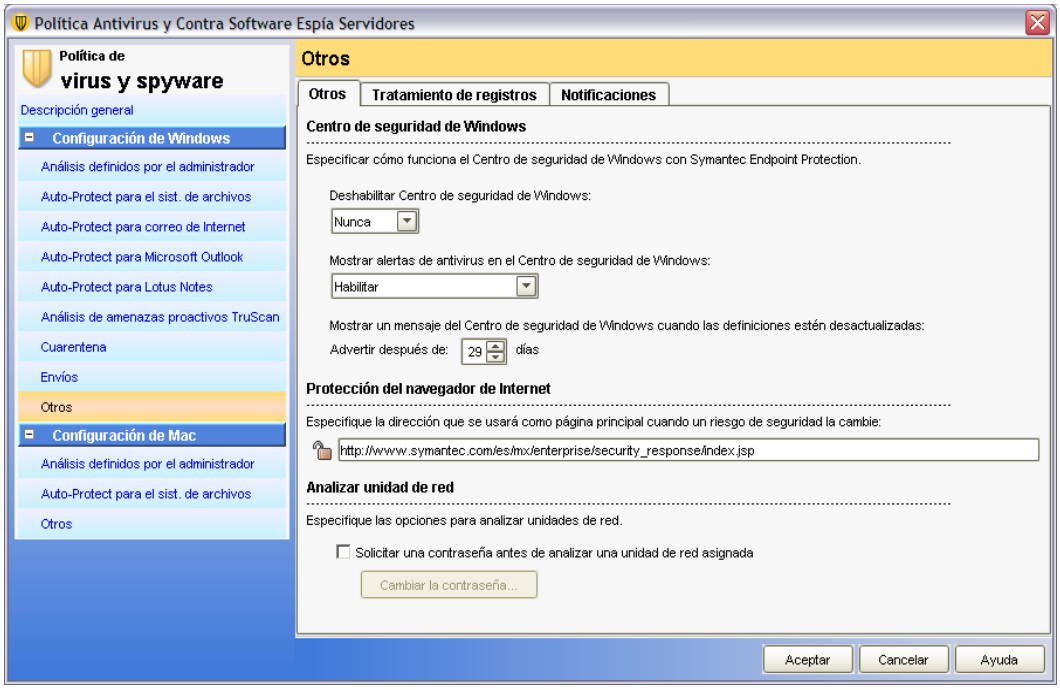


Figura 3.90 configuración del centro de seguridad de Windows

Política de Firewall para Clientes

1. En la opción *Firewall* se realiza la configuración estándar especificada por Symantec. Ver figura 3.91

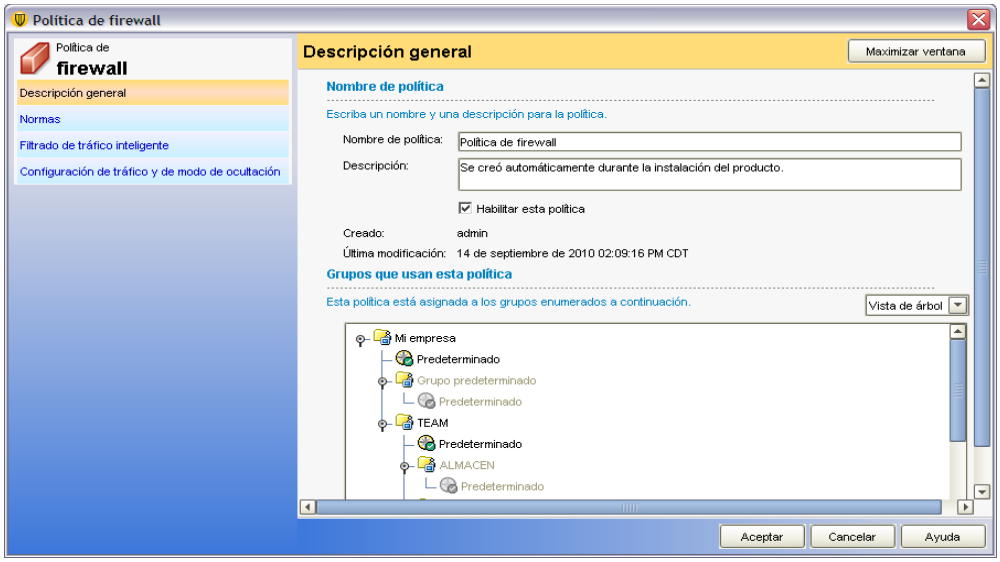


Figura 3.91 Configuración de firewall

2. En la opción de *Normas* se configuran las reglas para permitir y restringir el tráfico en la red. Ver figura 3.92

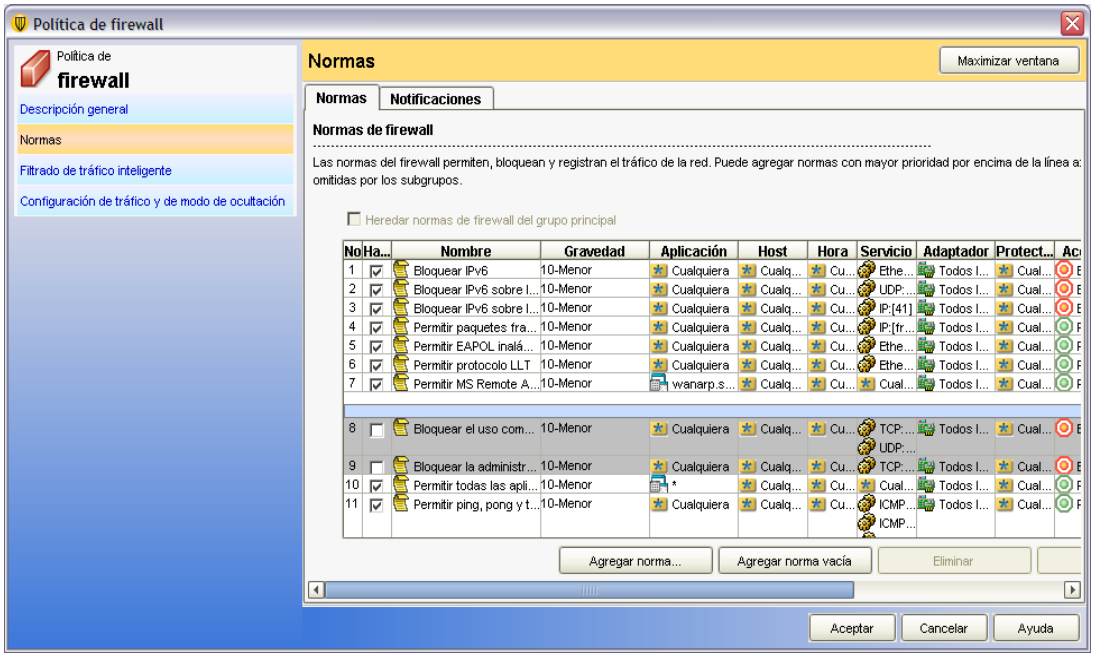


Figura 3.92 Configuración de normas de firewall

3. Dentro del *Filtrado de Tráfico Inteligente* se habilitan las opciones de *Smart DHCP*, *DNS* y *WINS*. Ver figura 3.93

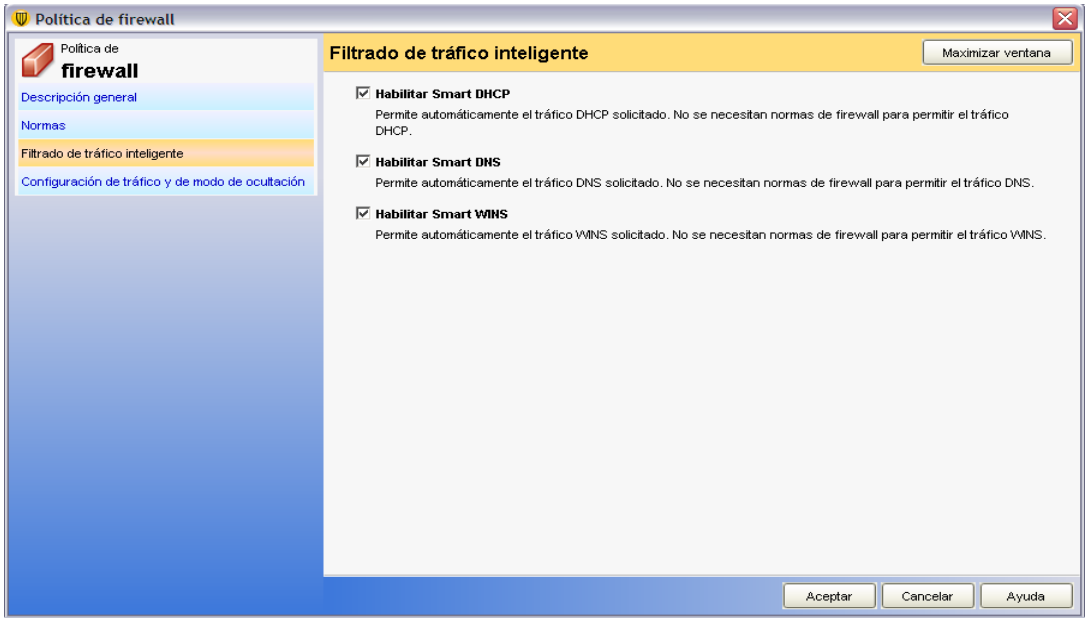


Figura 3.93 Configuración de Filtrado de tráfico inteligente

4. En la opción de *Configuración de tráfico y de modo de ocultación*, se activa la opción *Habilitar normas contra falsificación de MAC*, para bloquear todo el tráfico ARP no esperado. Ver figura3.94

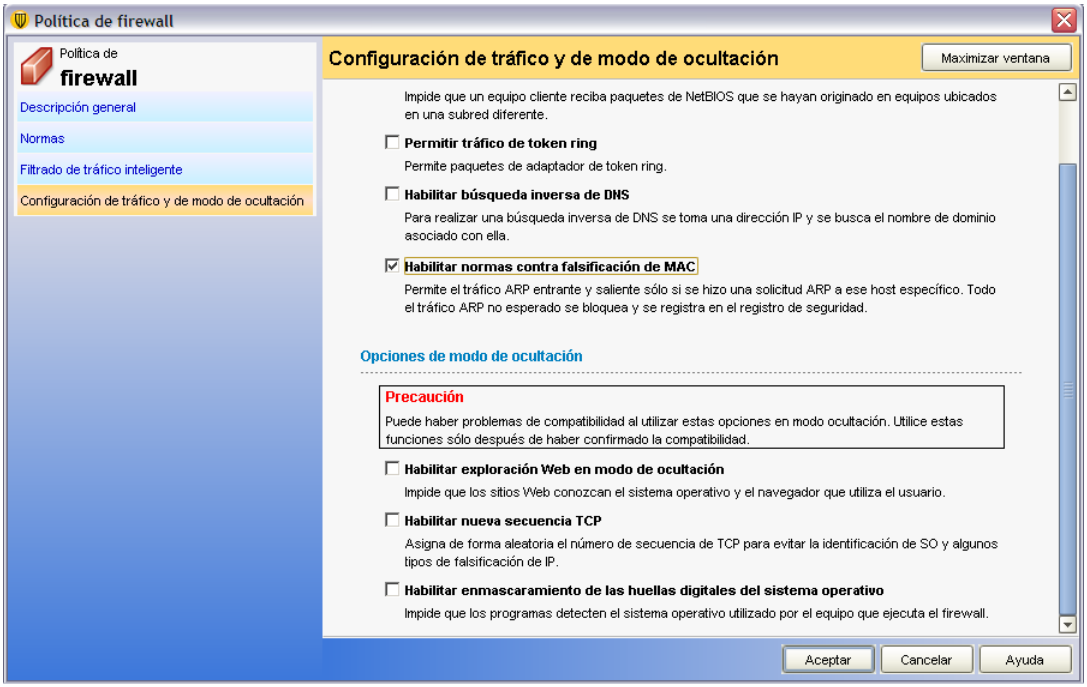


Figura 3.94 Configuración de tráfico y de modo de ocultación

Política de Prevención de Intrusiones

1. Dentro del área de *prevención de intrusiones* se habilitan las opciones para detectar y bloquear ataques. Ver figuras 3.95

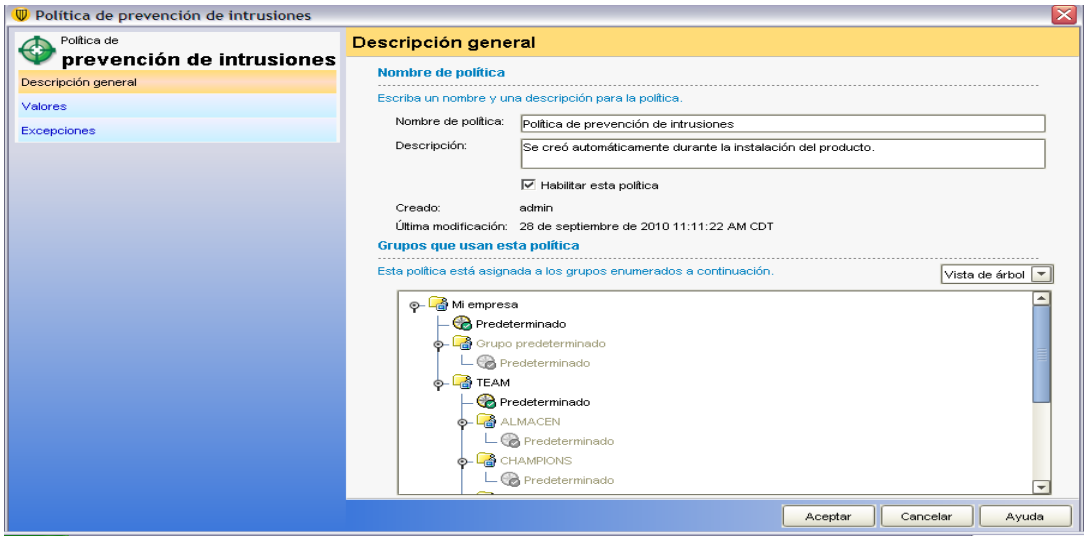


Figura 3.95 Configuración general prevención de intrusiones

2. En las políticas de prevención de intrusiones en la pestaña *valores* se habilitan las opciones de detección y bloqueo de ataques de red, la detección de ataques de negación de servicio y el análisis de puertos. Ver figura3.96

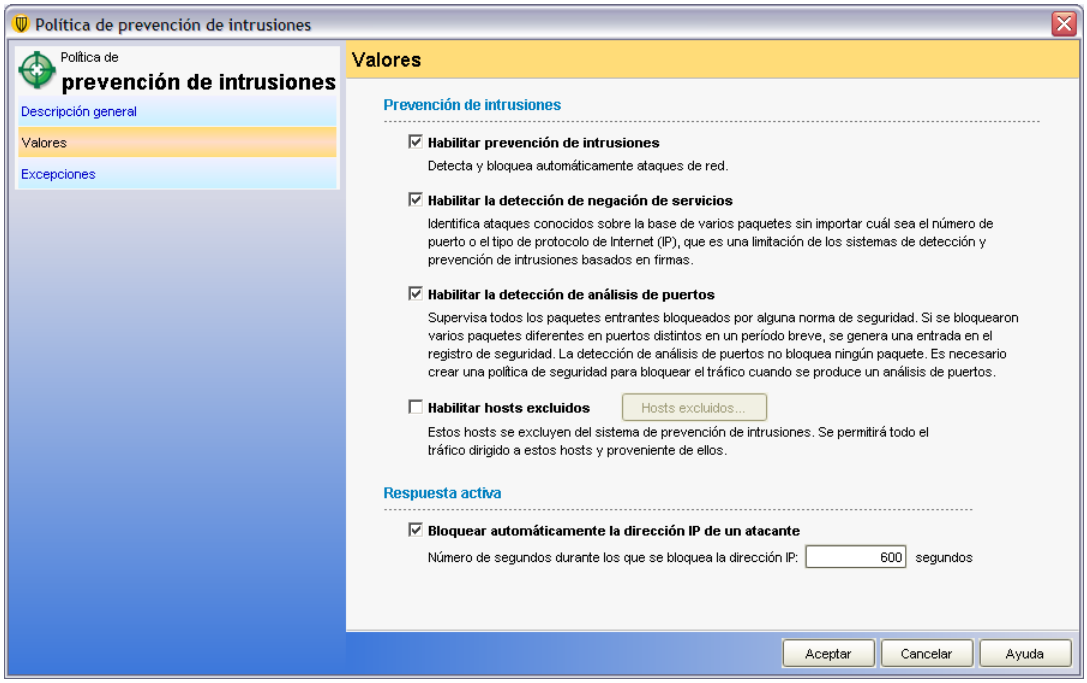


Figura 3.96 Configuración de valores dentro de la prevención de intrusiones

Control de Aplicaciones y Dispositivos

1. En la opción *Control de aplicaciones y dispositivos* por cuestiones de seguridad en la empresa se determina para algunas áreas el bloqueo de USB. Ver figura 3.97, 3.98

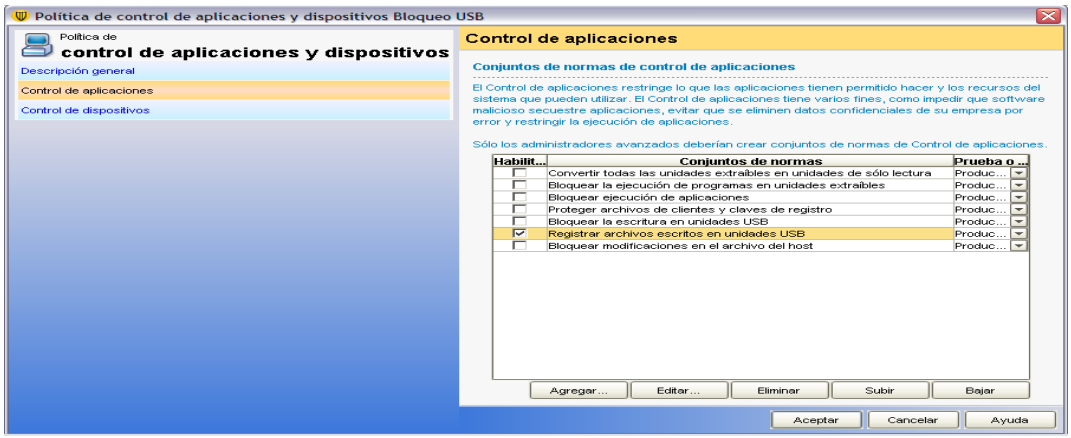


Figura 3.97 Configuración de control de aplicaciones

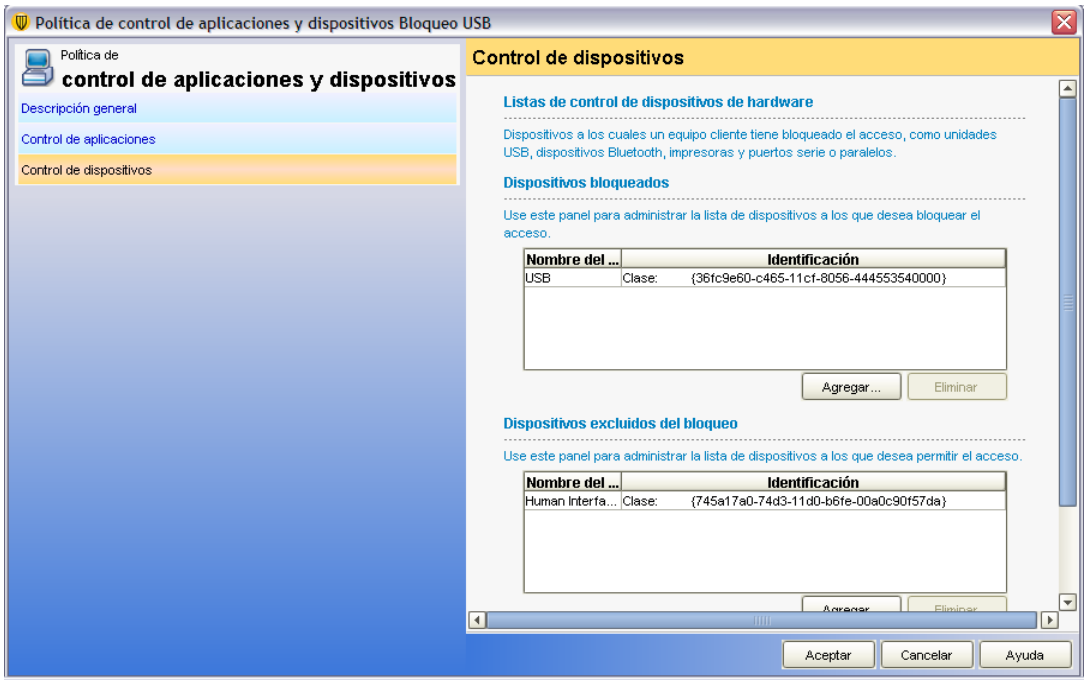


Figura 3.98 Configuración de control de aplicaciones

Configuración Políticas Live Update

1. Las actualizaciones se programan en el horario de comida que es cuando la actividad disminuye (13:00, 14:00 y 15:00), la producción no se ve afectada. Ver figura 3.99 y 3.100

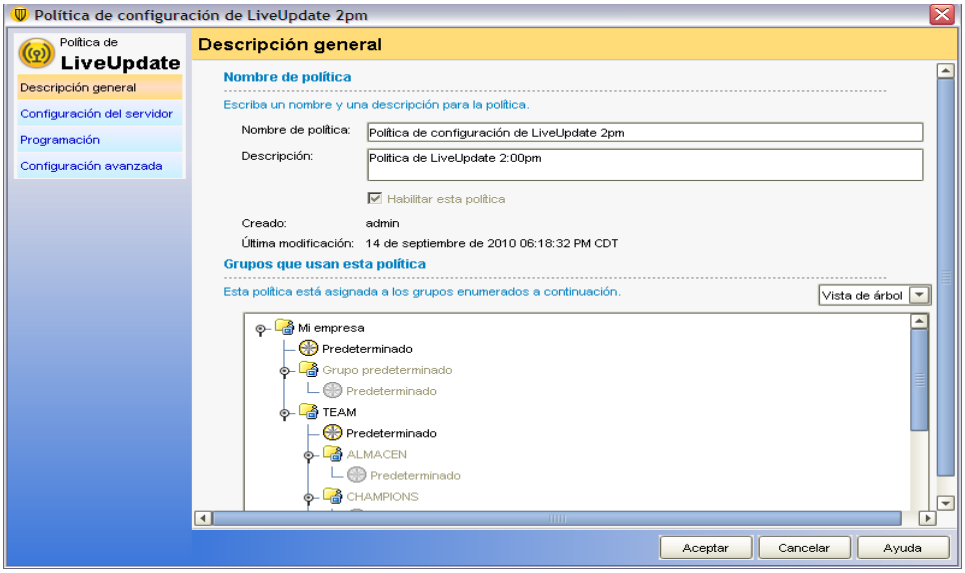


Figura 3.99 Configuración de políticas LiveUpdate

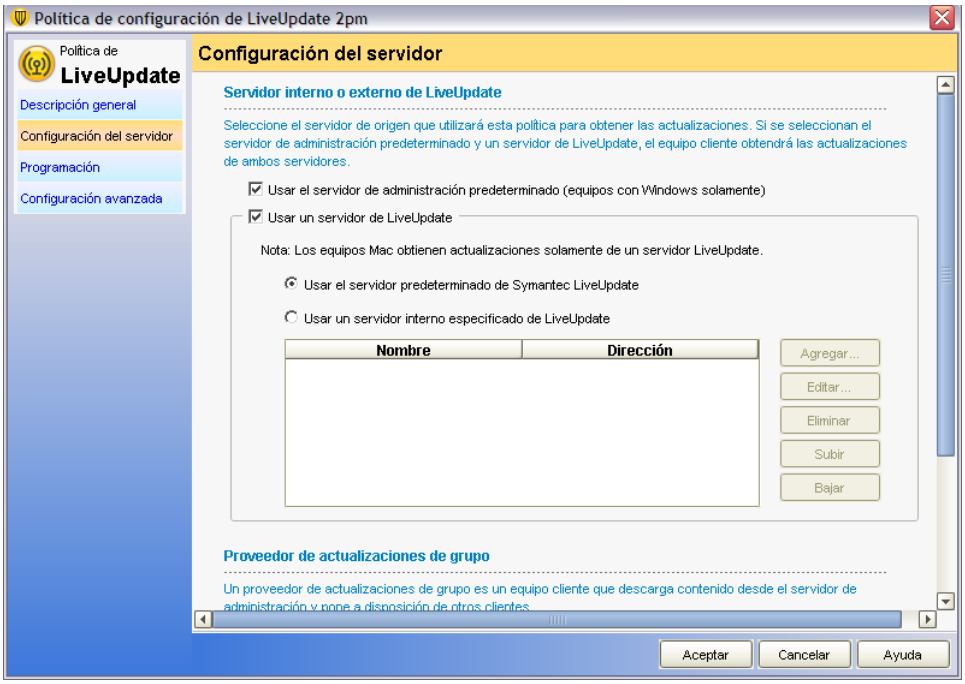


Figura 3.100 Configuración de políticas LiveUpdate

2. Todos los equipos excepto las laptops se actualizan desde la consola. Ver figura 3.101

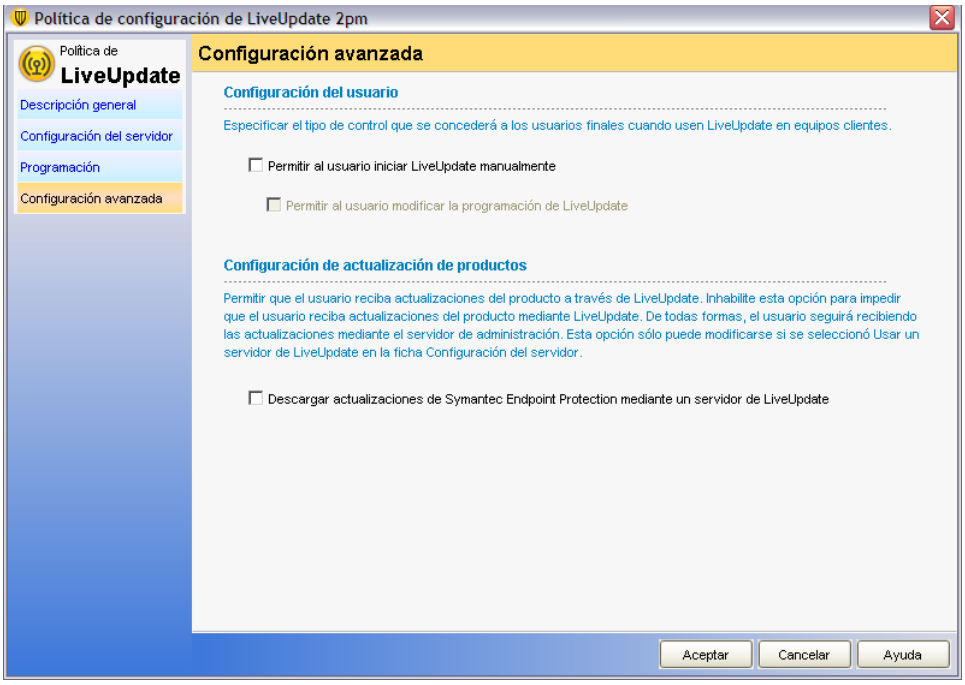


Figura 3.101 Configuración avanzada LiveUpdate

Con esto se finaliza la configuración de la consola de administración y está lista para llevar a cabo la gestión de los equipos de cómputo de la organización de acuerdo a las reglas establecidas.

3.3.10Configuración y administración de Firewall de Contenido (software)

Dentro de esta configuración se realiza la creación de nuevas reglas de filtrado y administración de la red, tanto para servicios como filtrado de contenido, restricciones a usuarios, excepciones, administración del tráfico, creación y análisis de reportes.

Como primer paso para la configuración de un firewall de tipo software como lo es Microsoft ISA Server, debemos de llevar a cabo la creación del tipo de red a proteger y su configuración.

A continuación en la imagen 3.102 podemos observar un esquema general acerca de los pasos a seguir para la configuración, se inicia, como ya se había mencionado, con la configuración de la red y sus atributos.

Figura 3.102 Página principal firewall Microsoft ISA Server

A continuación se realiza la configuración de la red a administrar. Ver figura 3.103

Se asigna un nombre de identificación de la red.

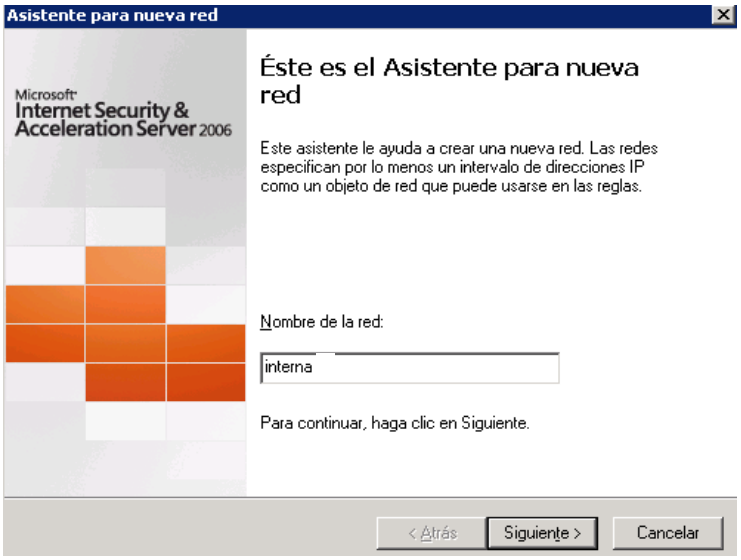


Figura 3.103 Asistente para configuración de red

Después se elige un tipo de configuración para la red, por lo cual de acuerdo a los requerimientos de la organización selecciono la configuración perimetral, la cual contiene servidores publicados en internet. Ver figura 3.104

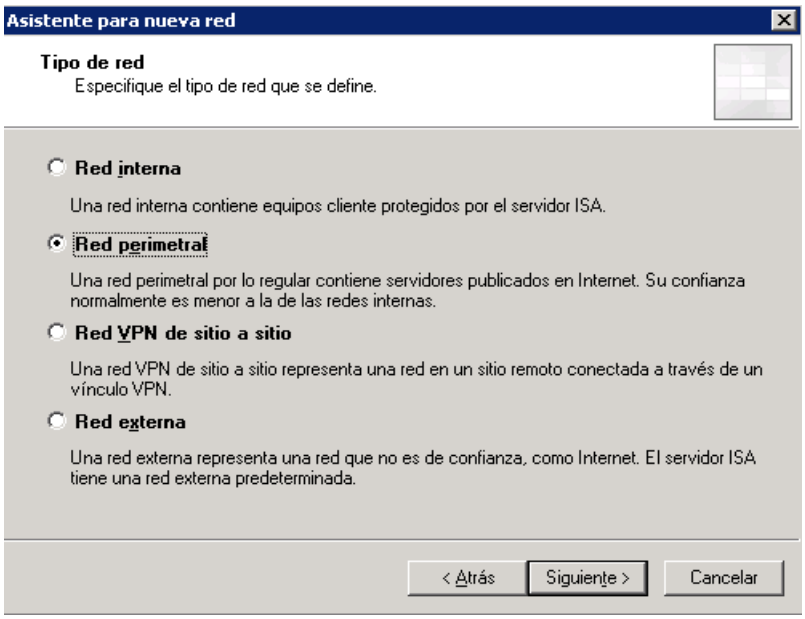


Figura 3.104 Tipo de red

Ahora se configuran los segmentos de red a analizar. Ver figura 3.105

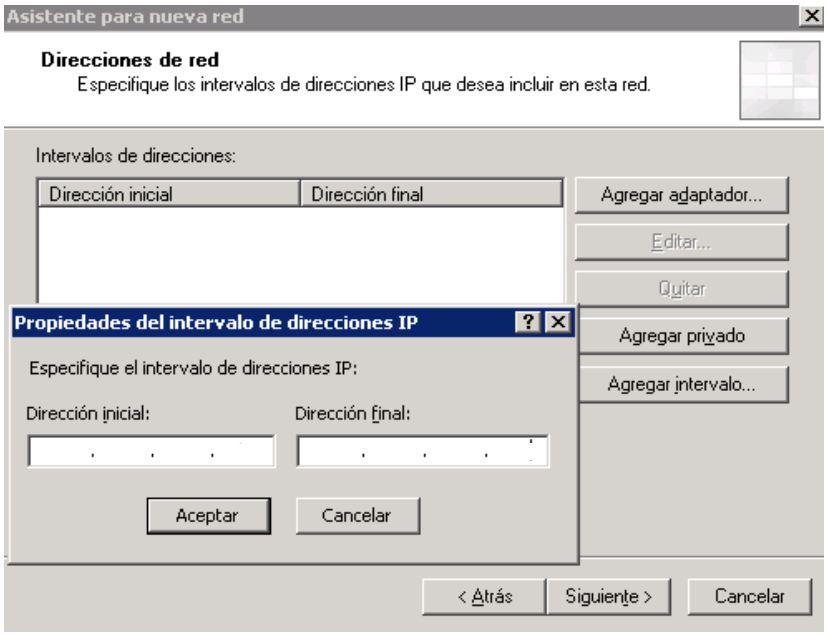


Figura 3.105 Configuración de segmentos de red

Con esto se finaliza la configuración de la parte de red, por medio de esta se asignan los adaptadores y segmentos de red a supervisar y analizar. Ver figura 3.106

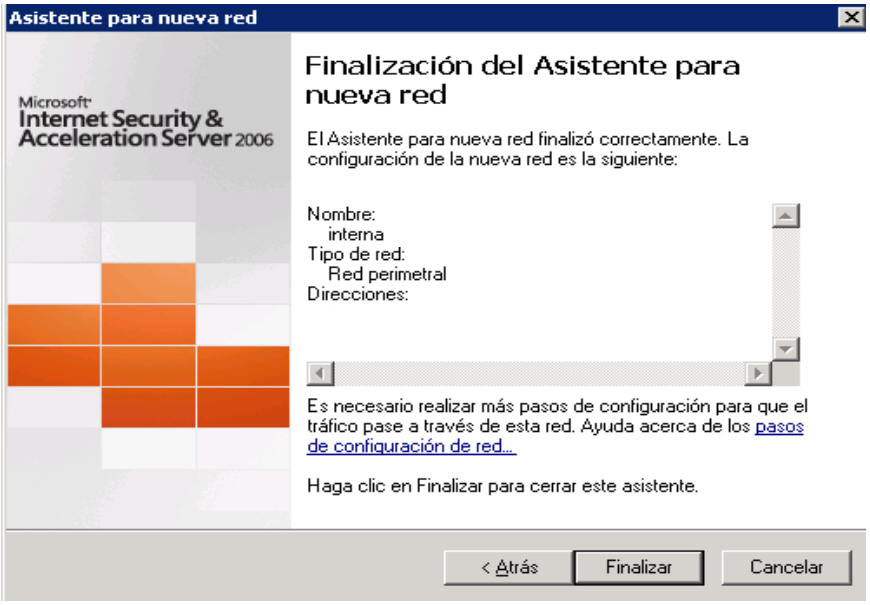


Figura 3.106 Finaliza configuración de red

En la figura 3.107 se observa la configuración establecida para la configuración de red y sus segmentos a analizar.

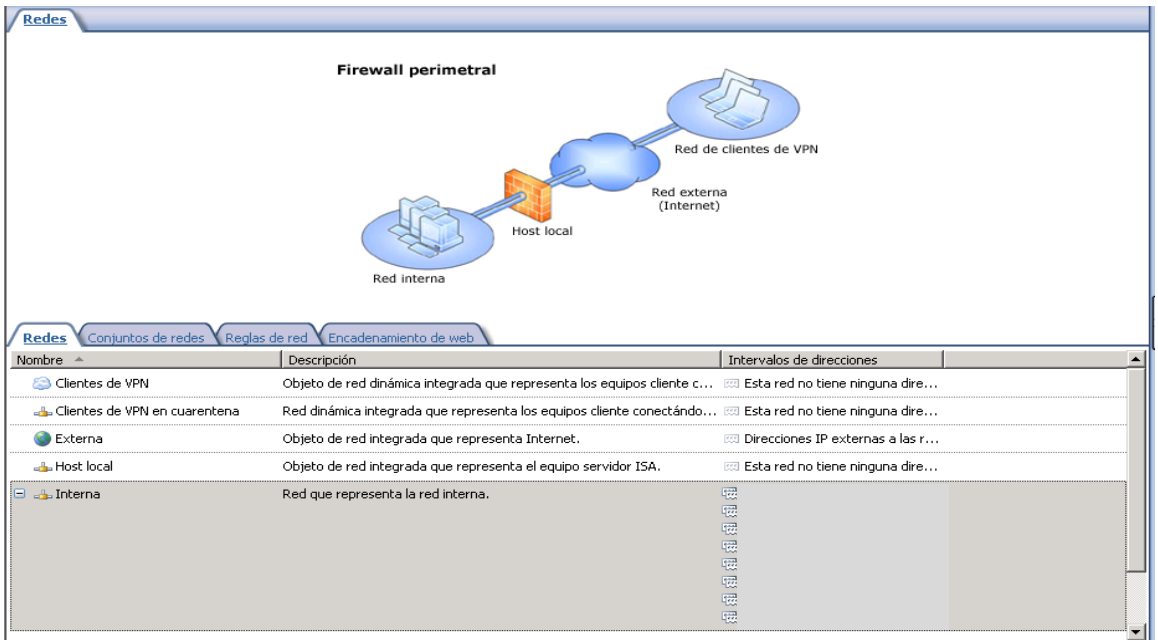


Figura 3.107 Configuración de redes y segmentos

Una vez configurado el esquema de red es necesario llevar a cabo la configuración de las directivas de firewall, es decir, aquellas reglas que se interpretan para dar paso al flujo permitido a través de la red e interpretarán los protocolos, filtros, entre otras cosas que estarán restringidas en la red. Ver figura 3.108

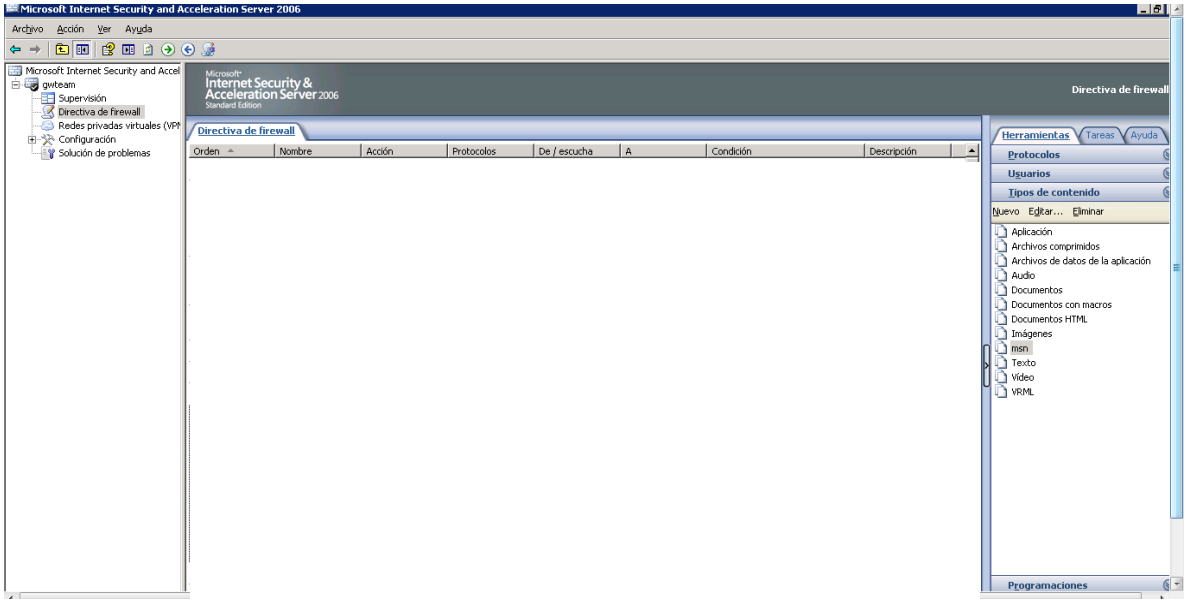


Figura 3.108 Panel de directivas de firewall

A continuación se lleva a cabo la configuración de una directiva la cual asegura que exista el flujo de internet a lo largo de toda la red.

Para la selección *Directivas de Firewall* se elige *Nuevo* y creamos una nueva *Regla de acceso*. Ver figura 3.109

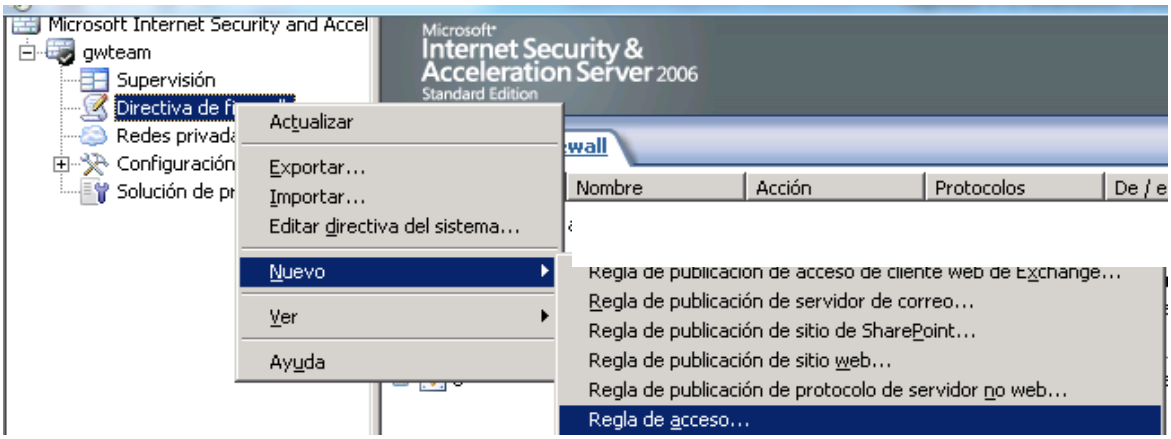


Figura 3.109 Crear nueva regla de acceso

Se selecciona el nombre para la nueva *Regla de acceso*, a esta regla la nombro *salida web* ya que especifica el envío y recepción de todo el tráfico sin restricciones. Ver figura 3.110

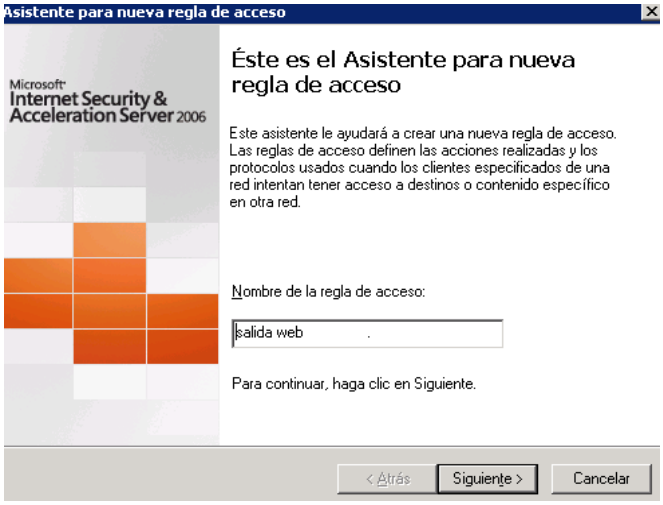


Figura 3.110 Nueva regla de acceso

Ahora se especifica la acción a realizar de acuerdo a las peticiones de los usuarios especificados en los segmentos de red, para esta acción se selecciona permitir ya que dará paso al flujo de información externa hacia la red interna. Ver figura 3.111

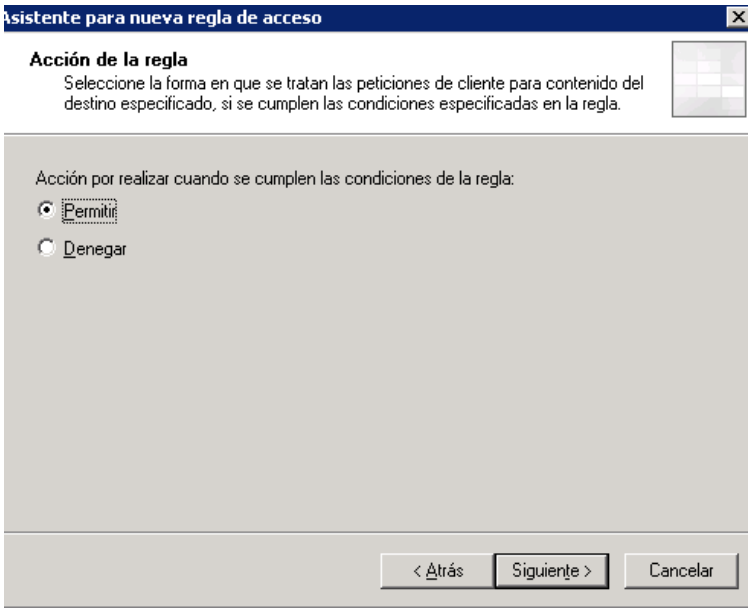


Figura 3.111 Acción especificada a realizar

A continuación se selecciona a que protocolos se aplica esta acción por lo cual como ya se había mencionado esta regla es para permitir todo el flujo de información por lo cual se elige “Todo el tráfico saliente”. Ver figura 3.112

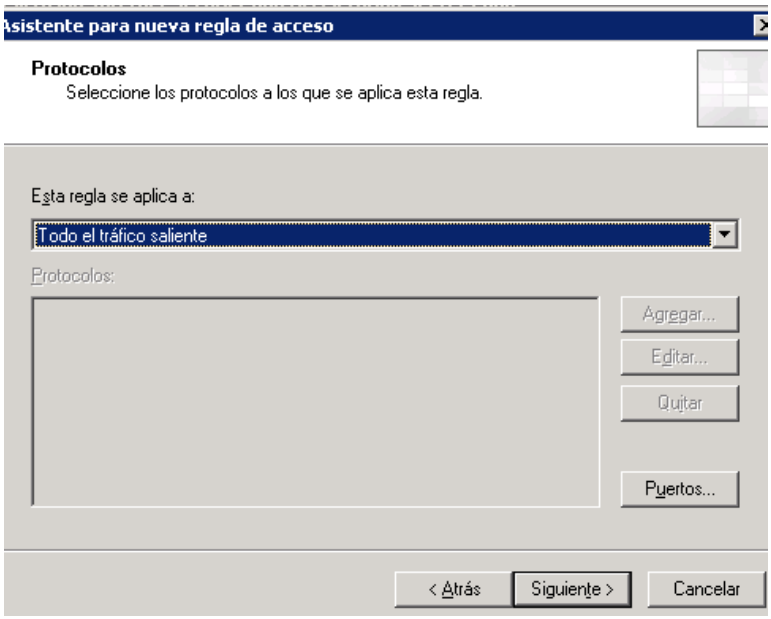


Figura 3.112 Protocolo al que se aplica la acción

Como siguiente paso, de acuerdo a la configuración que se hizo del esquema de red, se selecciona la red de origen, la cual se configuró como *Interna*. Ver figura 3.113

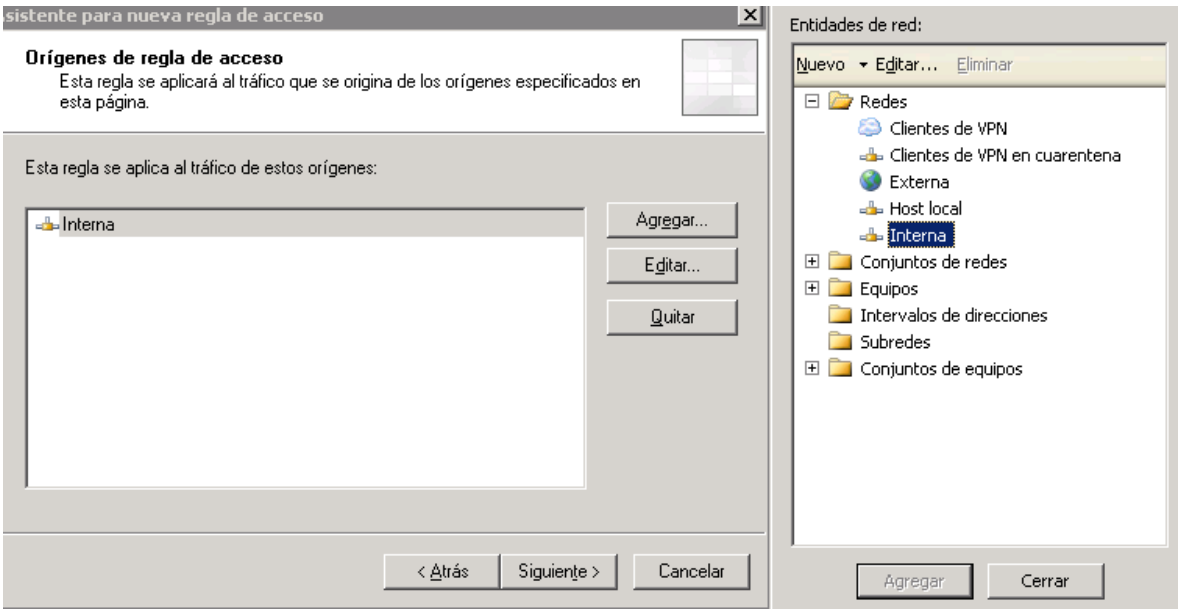


Figura 3.113 Origen del flujo de información

De la misma forma que en el paso anterior se selecciona ahora la red de destino, para la cual se elige la red *Externa* que será la salida al mundo público. Ver figura 3.114

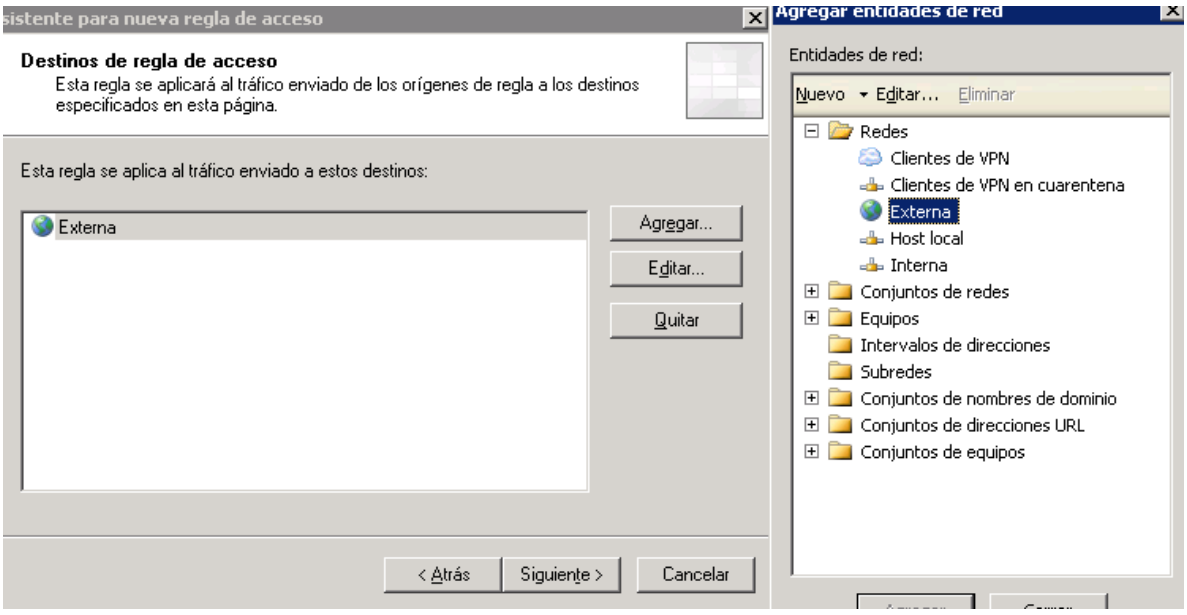


Figura 3.114 Destino del flujo de información

Después se selecciona a qué usuarios dentro de la red asignada se aplica esta regla por lo cual se selecciona *Todos los usuarios.* Ver figura 3.115

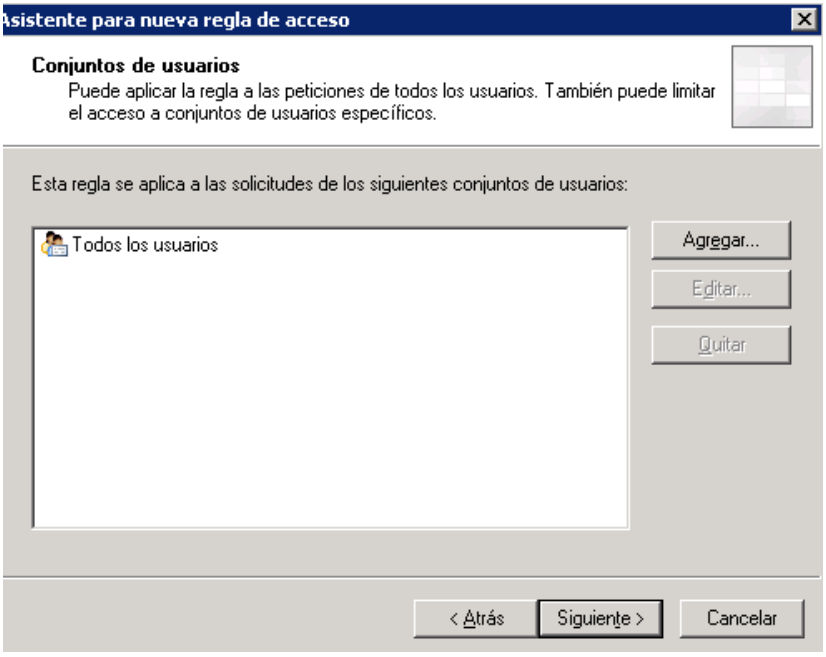
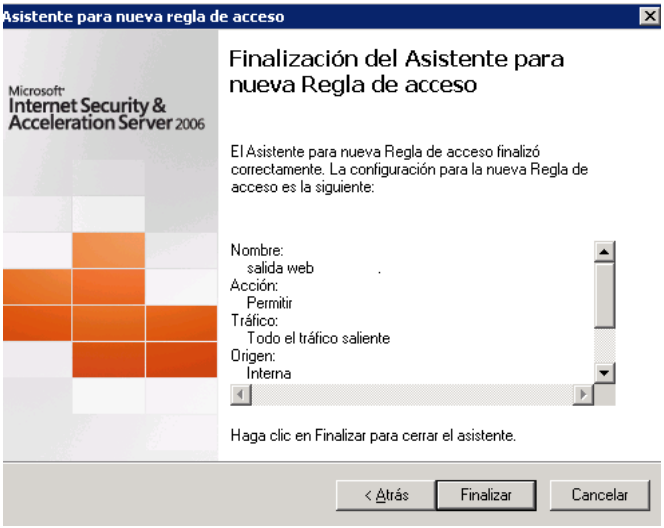


Figura 3.115 La regla aplica a todos los usuarios

Con esto se finaliza la creación de una nueva regla de acceso. Ver figura 3.116



3.116 Regla configurada

Aquí se observa la nueva regla creada, figura 3.117, la cual admite todo el tráfico a través del firewall, a continuación se muestra de manera resumida las opciones de esta regla:

Nombre: salida web
Acción: Permitir
Protocolos: Todo el tráfico saliente
De/escucha: Interna
A: Externa
Condición: Todos los usuarios

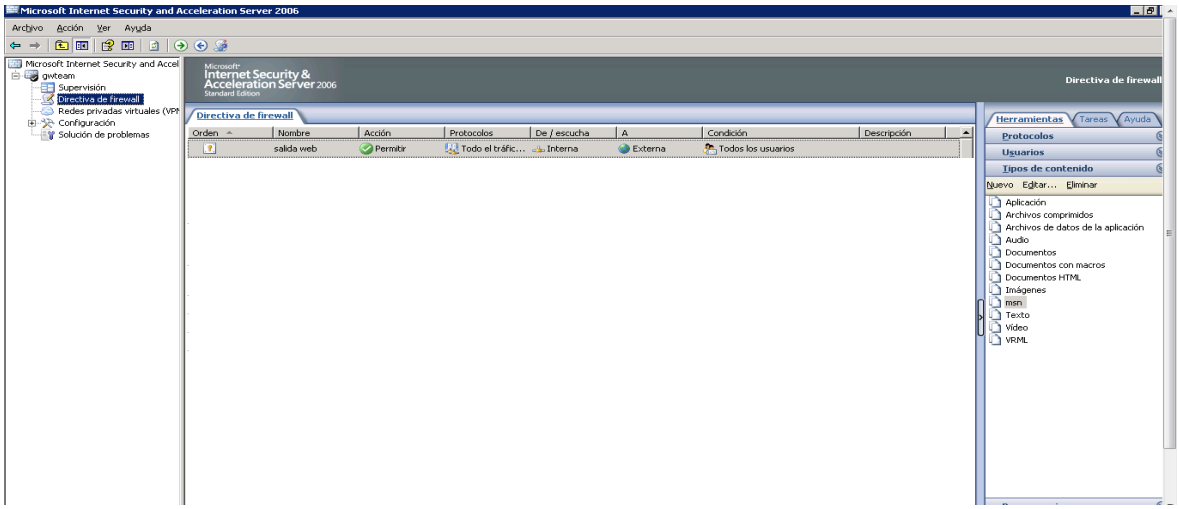


Figura 3.117 Directivas de firewall creadas

Ahora se crean una serie de directivas necesarias para el flujo correcto del tráfico sobre la red, así como filtros web, protocolos y aplicaciones, las cuales describo en su forma resumida y se explica el objetivo de cada nueva regla.

La siguiente regla creada está desarrollada para permitir el flujo de tráfico de los protocolos HTTP y HTTPS tanto dentro de la intranet como hacia la nube, y está configurada de la siguiente forma: Ver figura 3.118

Nombre: red interna
Acción: Permitir
Protocolos: HTTP, HTTPS
De/escucha: Interna
A: Interna, Externa
Condición: Todos los usuarios

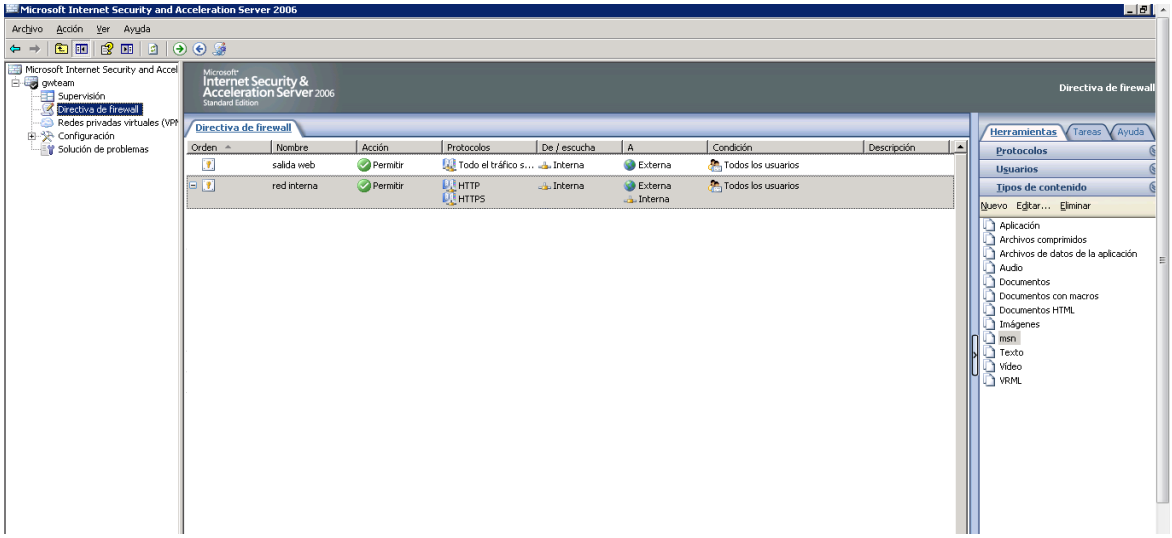


Figura 3.118 Regla de tráfico Http y Https

Las siguientes dos reglas son configuradas para el host, la primera regla me permite como administrador llegar al host por medio de Ping, y el otro servicio me da acceso a la administración remota, estos son los parámetros utilizados para su configuración. Ver figura 3.119

Nombre: Ping RDP
Acción: Permitir
Protocolos: Ping, RDP, Servidor RDP
De/escucha: Interna
A: host local
Condición: Todos los usuarios

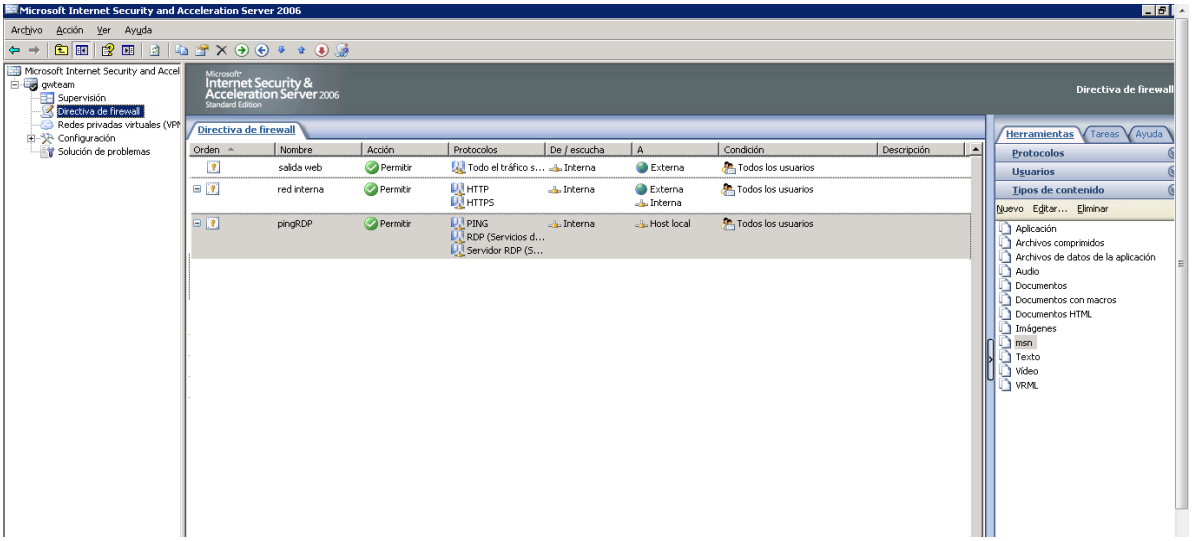


Figura 3.119 Acceso a servicios del host

La siguiente regla permite el acceso del host a internet, lo cual es necesario para realizar actualizaciones y otro tipo de servicios necesarios vía web, estos son los parámetros de configuración para esta regla: Ver figura 3.120

Nombre: host
Acción: Permitir
Protocolos: Todo el tráfico
De/escucha: host local
A: externa
Condición: Todos los usuarios

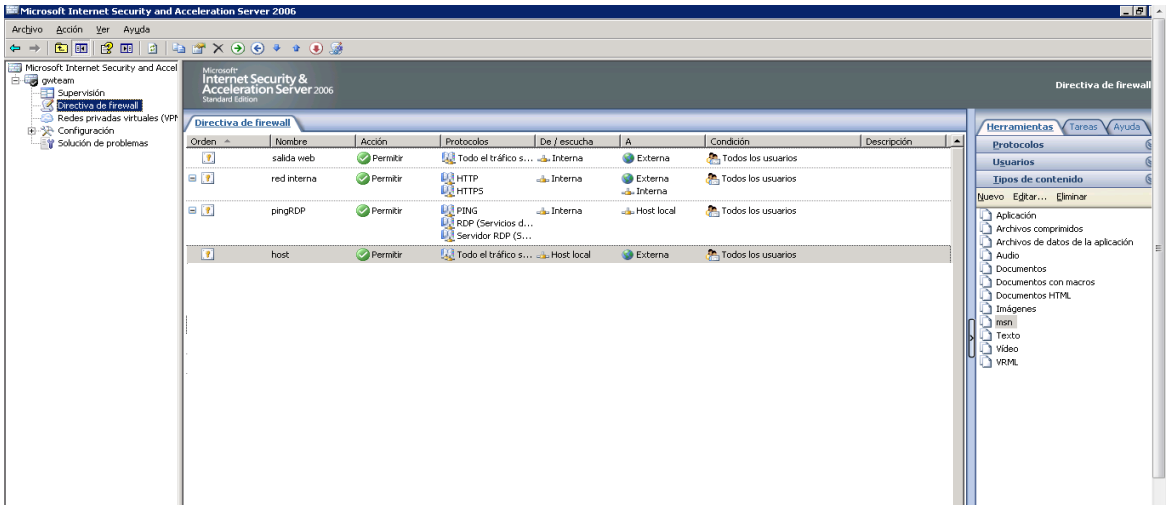


Figura 3.120 Configuración acceso web del host

Por medio de la creación de la siguiente regla descrita, se realiza el bloqueo web de los sitios que no se encuentran autorizados en la organización y se realiza la excepción de algunos equipos por medio de su IP asignada.

Los parámetros para llevar a cabo la configuración son los siguientes: Ver figura 3.121

Nombre: bloqueo web
Acción: denegar
Protocolos: ftp, http, https, servidor https
De/escucha: interna
A: bloqueo1
Condición: Todos los usuarios

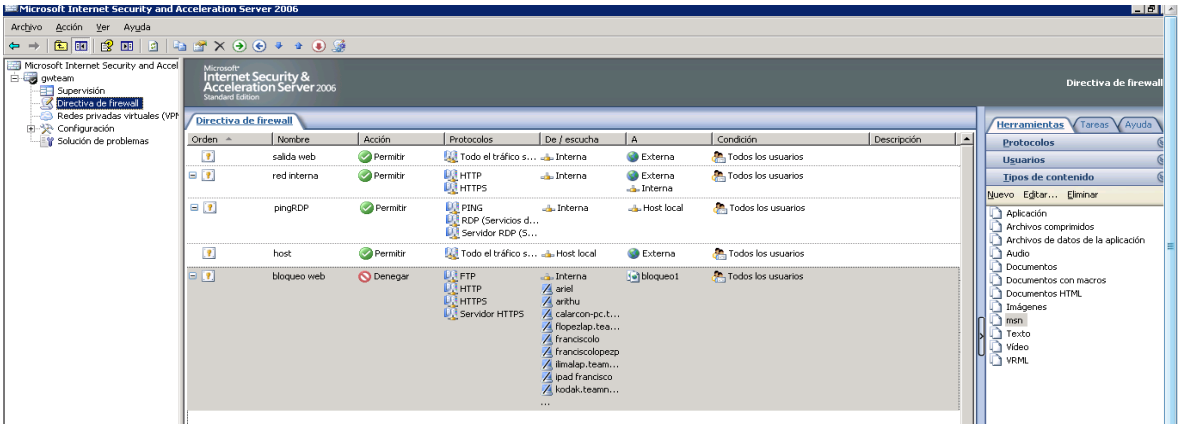


Figura 3.121 Bloqueo web

Para realizar esta regla es necesario crear una lista de bloqueo de URL, la cual se crea dentro de *Herramientas*, se eligen los *Objetos de red* y se despliega la lista, en esta lista se encuentra un apartado nombrado *Conjunto de direcciones URL* el cual por medio de clic derecho se despliega un sub-menú donde se encuentra la opción *Nuevo conjunto de direcciones URL.* Ver figura 3.122

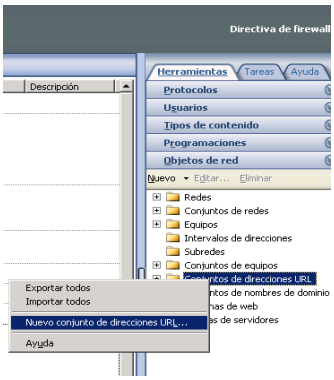


Figura 3.122 Nueva lista de bloqueo URL

Una vez que creamos la nueva lista de direcciones URL, se deben agregar aquellas que se quieran bloquear, para que el bloqueo sea exitoso podemos descargar listas previamente creadas y/o personalizar las propias. Ver figura 3.123

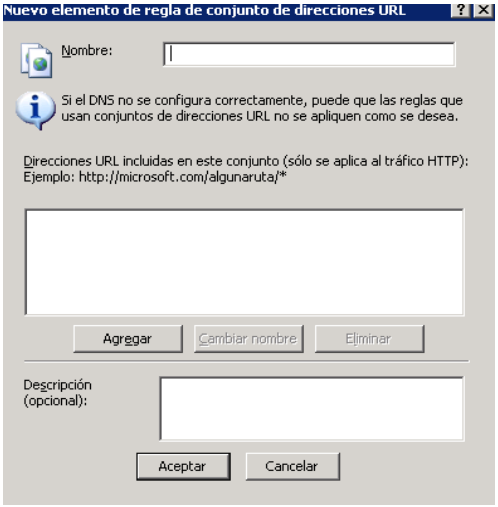


Figura 3.123 Nueva lista de direcciones URL

Una vez generada la nueva lista, se elige un nombre para ésta, se ingresan las direcciones y se agregan las distintas formas por las que se pueda ingresar a una dirección específica a bloquear, en la figura 3.124 se puede observar mi lista de bloqueo generada y con distintas direcciones a denegar el acceso.

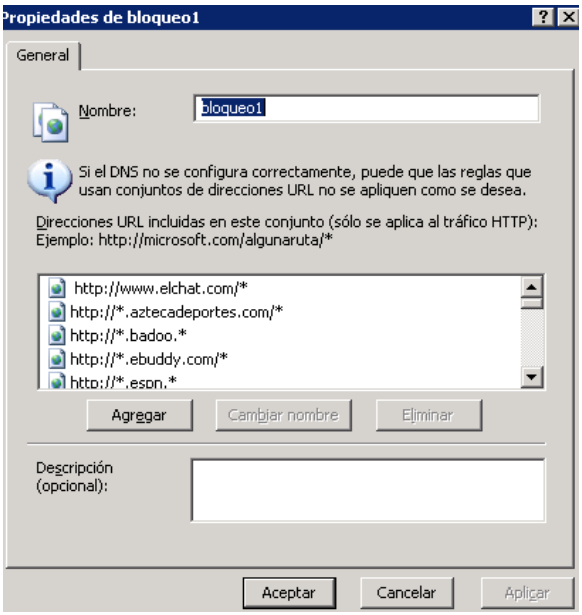


Figura 3.124 Mi lista de bloqueo

A continuación se presenta la forma en que se realizan las excepciones para los distintos equipos de dirección que están exentos de este bloqueo web, de igual forma en el menú *Herramientas* dentro del elemento *Equipos*, dando clic derecho se despliega un submenú donde elegimos *Nuevo equipo*. Ver figura 3.125

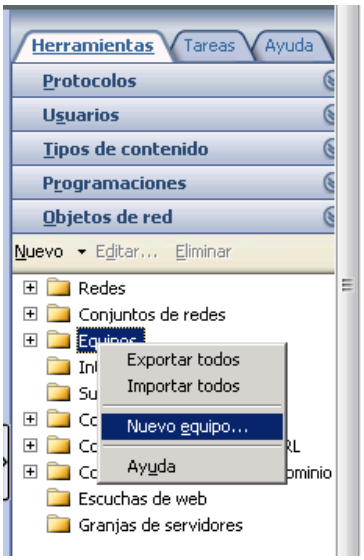


Figura 3.125 Equipo nuevo

Una vez que elegimos esta opción se despliega una ventana para agregar el nuevo equipo dado por su IP asignada dentro de nuestra red. Ver figura 3.126

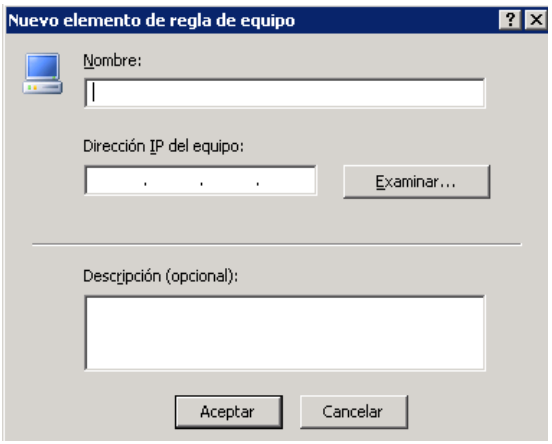


Figura 3.126 Asignar nuevo elemento de equipo

De esta forma se dan de alta y se ingresan los nuevos equipos que quedarán exentos de esta regla.

Generación de Reportes

Por medio de los reportes generados se puede obtener información muy valiosa para la correcta administración de la red, dentro de los parámetros que muestran estos reportes se encuentran:

- Protocolos más solicitados, estos pueden ser Http, Https, TCP, DNS, SMTP, entre otros
- Tráfico por protocolo, tráfico de los protocolos antes mencionados
- Usuarios más frecuentes, los usuarios que generaron la mayor cantidad de tráfico
- Tráfico generado por usuarios
- Sitios web más frecuentes, los sitios que generaron mayores solicitudes
- Tráfico por sitios web
- Rendimiento de la caché del Firewall
- Cantidad de tráfico reportado por fecha y hora
- Tráfico por día
- Tráfico por hora del día
- Exploradores web más utilizados
- Sistemas operativos utilizados
- Errores de autorización
- Paquetes perdidos

A continuación describo la forma en que se realiza la generación de reportes.

Como primer paso dentro del área del panel menú principal, ver figura 3.127, que se encuentra ubicado en la columna izquierda se ubican las opciones:

- Supervisión
- Directiva de firewall
- Redes virtuales privadas
- Configuración
- Solución de problemas

Figura 3.127 Menú de *Supervisión*

Dentro de este menú se selecciona la opción *Supervisión* la cual despliega en el panel central 8 pestañas, dentro de la cual se encuentra *Informes,* que se selecciona para llevar a cabo la visualización y generación de reportes. Ver figura 3.128

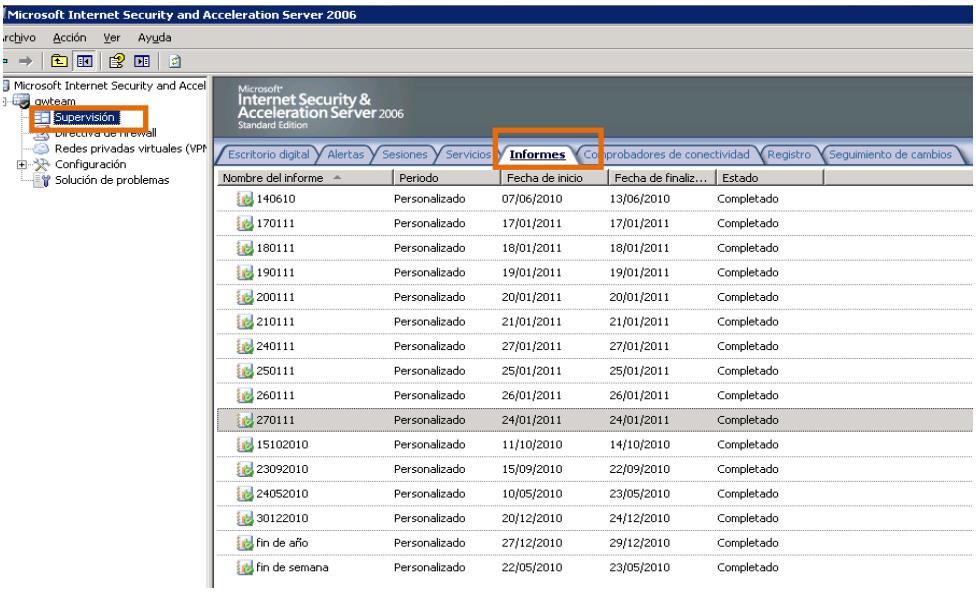


Figura 3.128 Informes

Una vez que se ha ingresado a la sección de *Informes*, en la columna derecha, se despliega un submenú con las pestañas, *Tareas* y *Ayuda*, donde se selecciona, *Generar un nuevo informe.* Ver figura 3.129

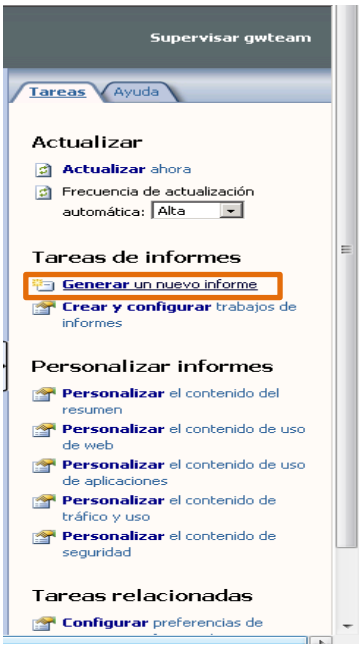


Figura 3.129 Generar un nuevo informe

Para generar un nuevo reporte se cuenta con un asistente para su creación, como primer paso se debe nombrar al informe que queremos generar, de esta forma por convención los nombro por su fecha de creación. Ver figura 3.130

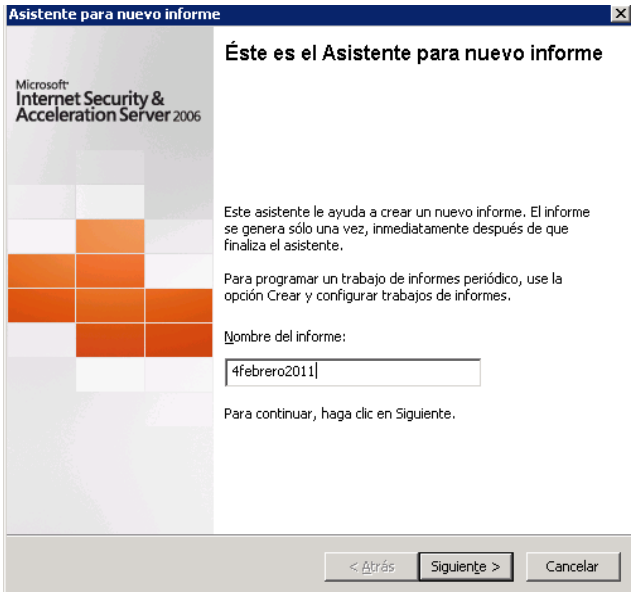


Figura 3.130 Nombre del informe

Después se selecciona el *Contenido del informe*, dentro del cual elijo todos los parámetros para obtener la mayor información que los reportes puedan obtener. Ver figura 3.131

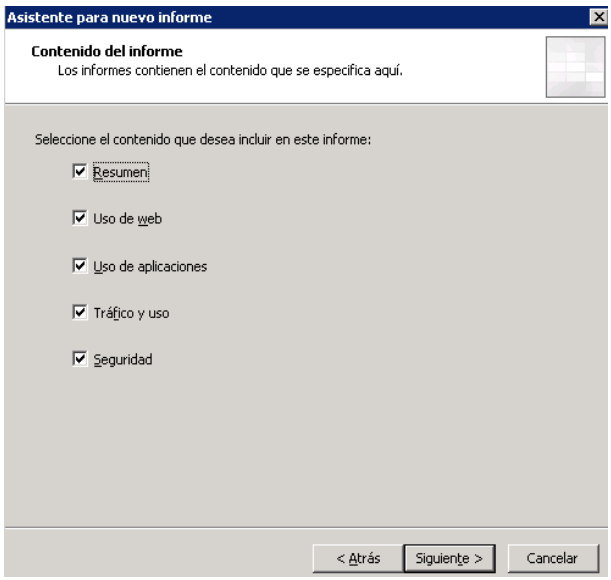


Figura 3.131 Contenido del informe

Como siguiente paso se selecciona el rango de fechas de las cuales queremos obtener el reporte. Ver figura 3.132

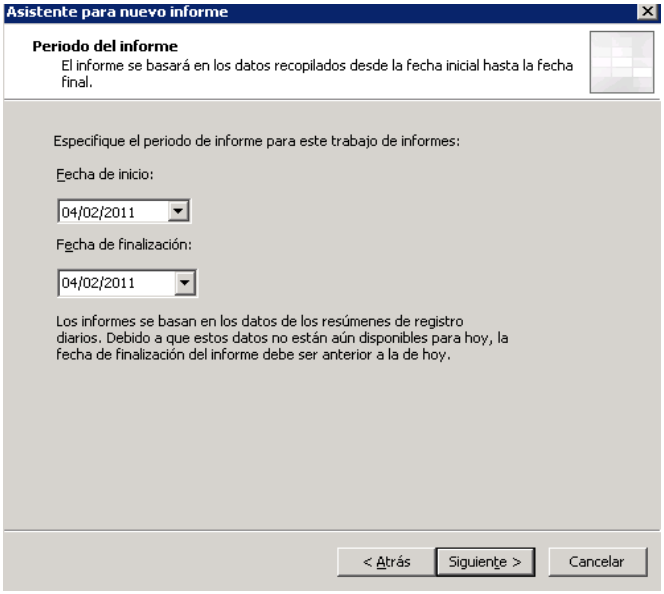
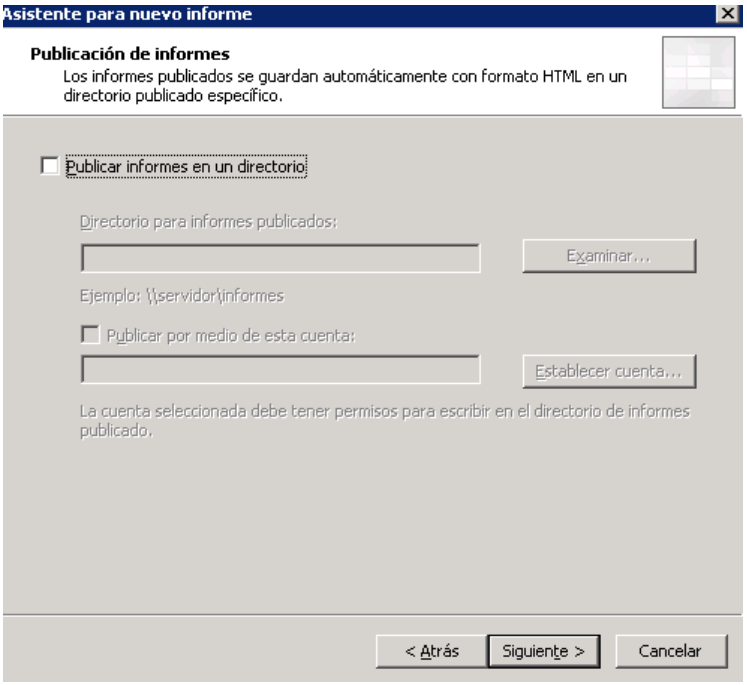


Figura 3.132 Periodo del informe

El siguiente paso, si se cuenta con un directorio específico para almacenar los reportes, es asignar el directorio donde estará alojado el informe, si no es así se consulta bajo un explorador web y solo se da clic en siguiente. Ver figura 3.133



3.133 Publicación de informes

Dentro de la siguiente ventana del asistente para la generación de reportes, se muestra la opción *Enviar una notificación por correo electrónico cuando finalice un informe*, decido omitir esta función y se da clic en siguiente inmediatamente. Ver figura 3.134

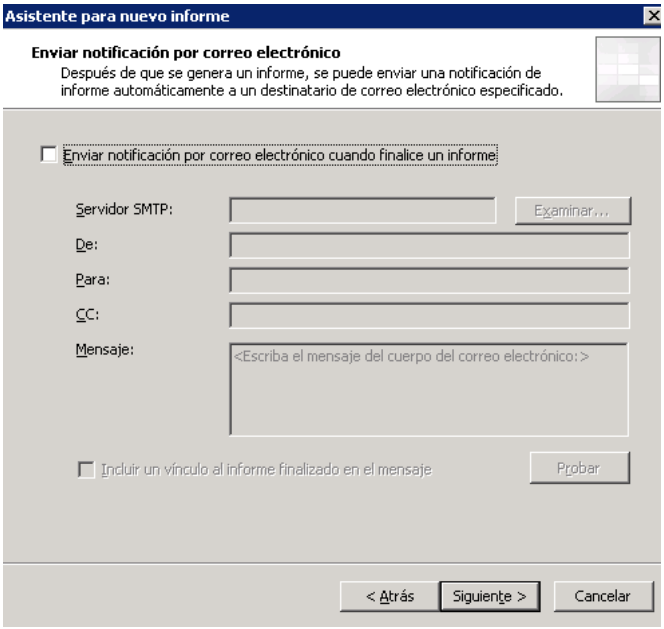


Figura 3.134 Notificación de reporte

De esta forma se finaliza el asistente para la creación de informes y se muestra la ventana de finalización y resumen de las opciones elegidas. Ver figura 3.135

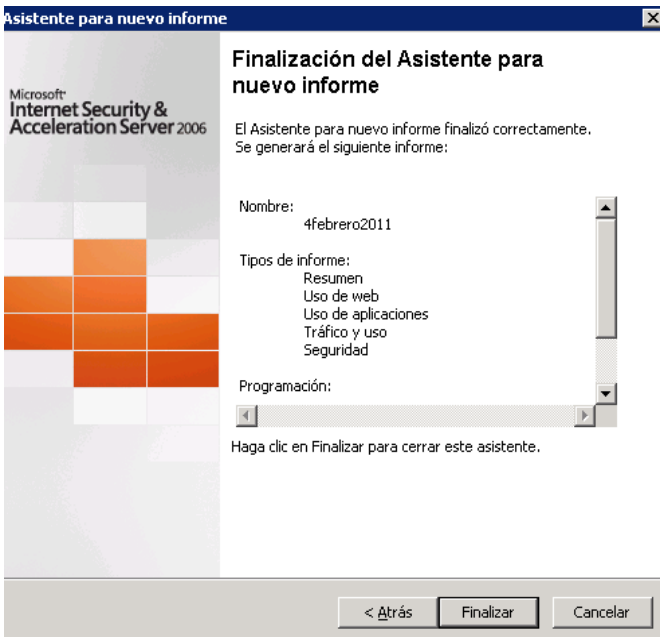
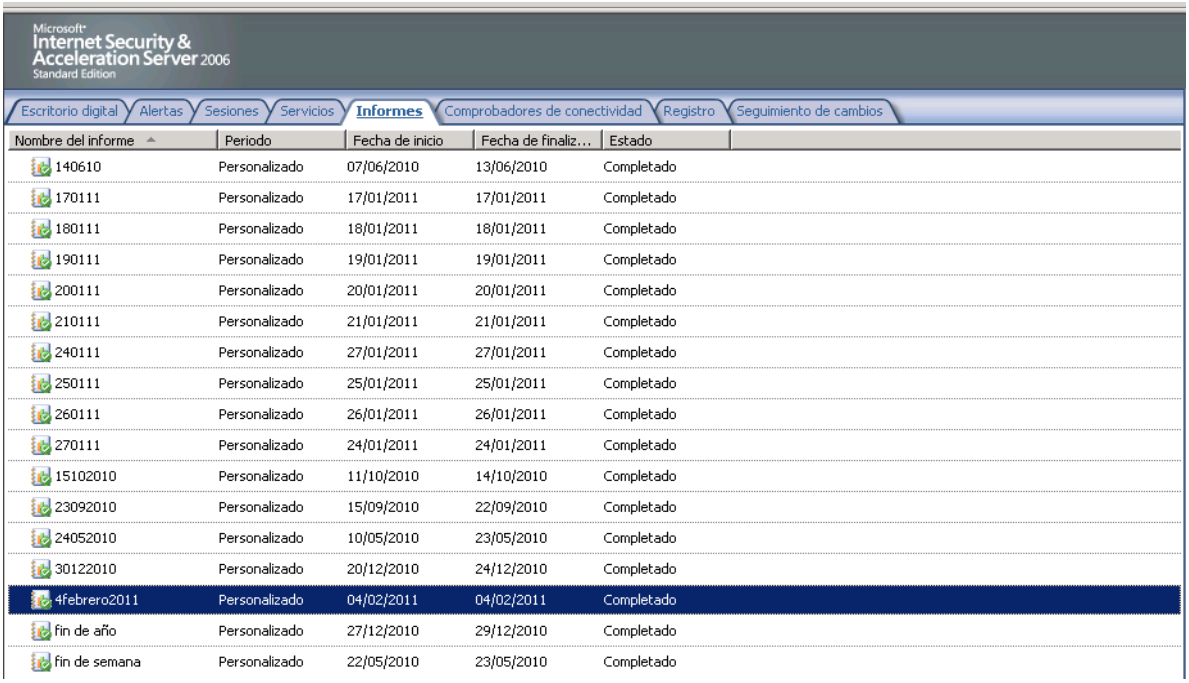


Figura 3.135 Finalización del asistente para la creación de reportes

El reporte configurado tarda unos instantes en generarse y después aparece en el panel central de informes con el nombre que le se le asignó. Ver figura 3.136



Nombre del informe	Periodo	Fecha de inicio	Fecha de finaliz...	Estado
140610	Personalizado	07/06/2010	13/06/2010	Completado
170111	Personalizado	17/01/2011	17/01/2011	Completado
180111	Personalizado	18/01/2011	18/01/2011	Completado
190111	Personalizado	19/01/2011	19/01/2011	Completado
200111	Personalizado	20/01/2011	20/01/2011	Completado
210111	Personalizado	21/01/2011	21/01/2011	Completado
240111	Personalizado	27/01/2011	27/01/2011	Completado
250111	Personalizado	25/01/2011	25/01/2011	Completado
260111	Personalizado	26/01/2011	26/01/2011	Completado
270111	Personalizado	24/01/2011	24/01/2011	Completado
15102010	Personalizado	11/10/2010	14/10/2010	Completado
23092010	Personalizado	15/09/2010	22/09/2010	Completado
24052010	Personalizado	10/05/2010	23/05/2010	Completado
30122010	Personalizado	20/12/2010	24/12/2010	Completado
4febrero2011	Personalizado	04/02/2011	04/02/2011	Completado
fin de año	Personalizado	27/12/2010	29/12/2010	Completado
fin de semana	Personalizado	22/05/2010	23/05/2010	Completado

Figura 3.136 Reporte generado

Dando doble clic sobre el nombre asignado para el reporte, se despliega el informe por medio de un explorador web, el cual se observa de la siguiente forma. Ver figura 3.137

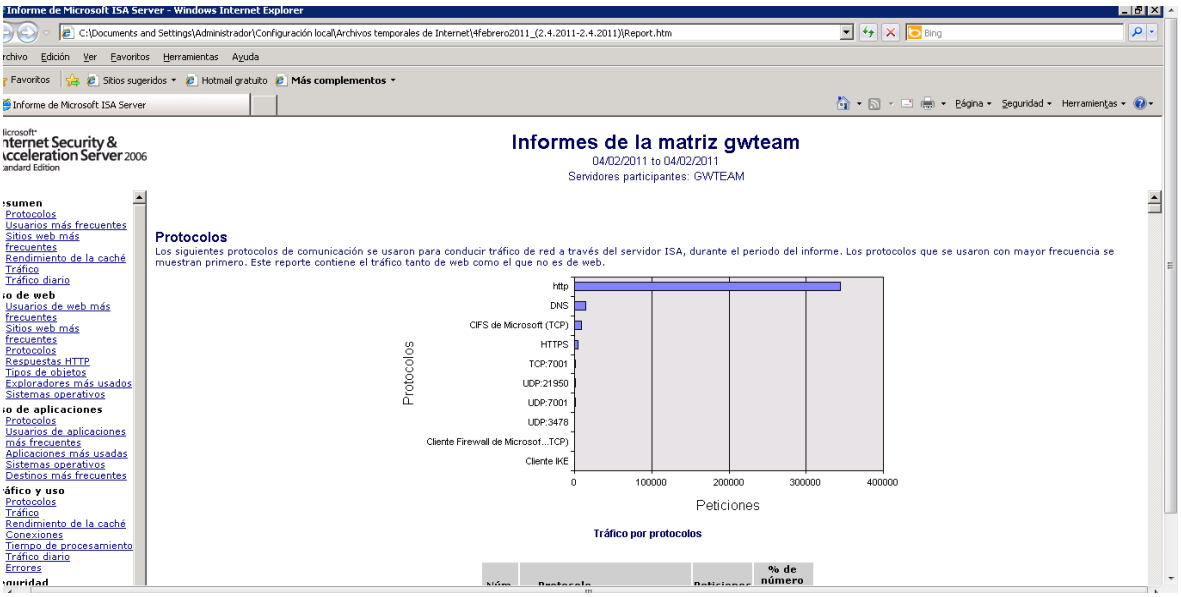


Figura 3.137 Reporte generado

De esta forma se cuenta con reportes de la fecha que se requiera y por este medio se pueden hacer análisis del rendimiento de la red y de sus usuarios.

Así se ha concluido la configuración del firewall por software Microsoft ISA Server, teniendo controlado el flujo de tráfico y se ha realizado el filtrado de páginas web en la organización lo cual podría provocar accesos a sitios no deseados o que impacten en el rendimiento de la red.

3.3.11 Configuración y aseguramiento de servidores

Esta configuración es importante, ya que dentro de los servidores se encuentran alojados la mayoría de los servicios que el área de TI proporciona a la organización, así que el asegurar su correcto funcionamiento y total disponibilidad es una de las tareas diarias que está a mi cargo.

A través de esta implementación se realiza la configuración de servicios, herramientas, protocolos, entre otros, que son indispensables para que los servidores puedan realizar la tarea para las cuales fueron creados.

Para esta implementación se instala la herramienta de seguridad que Windows Server incorpora en su sistema operativo.

Esta herramienta se instala de la siguiente forma:

Dentro de inicio, se selecciona panel de control y después se ingresa a *Agregar o quitar programas*, una vez dentro de esta ventana, en el panel izquierdo se selecciona *Agregar o quitar componentes de Windows*. Ver Figura3.138

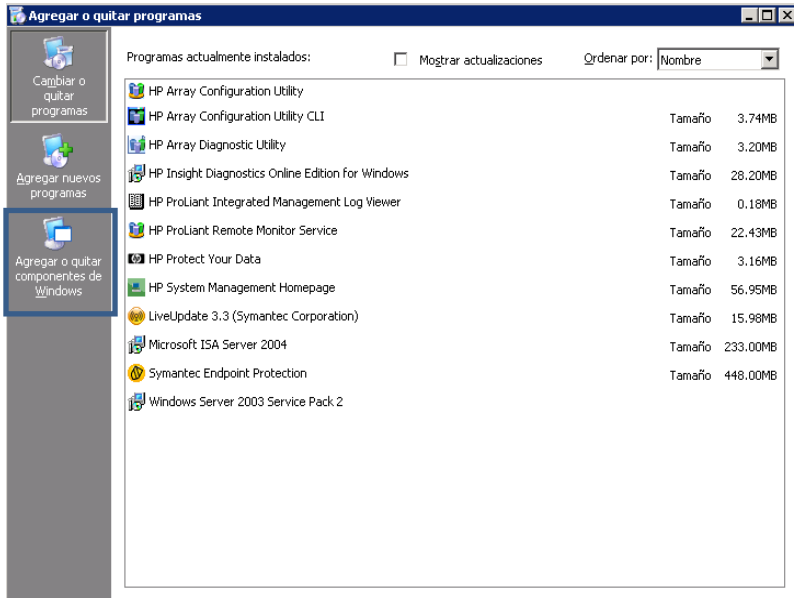


Figura 3.138 Agregar o quitar componentes de Windows

Al seleccionar esta opción se despliega una nueva ventana con un asistente para componentes de Windows, para instalar la herramienta de seguridad, se selecciona la casilla que indica *"Asistente para configuración de seguridad"* y se da clic en siguiente. Ver figura 3.139

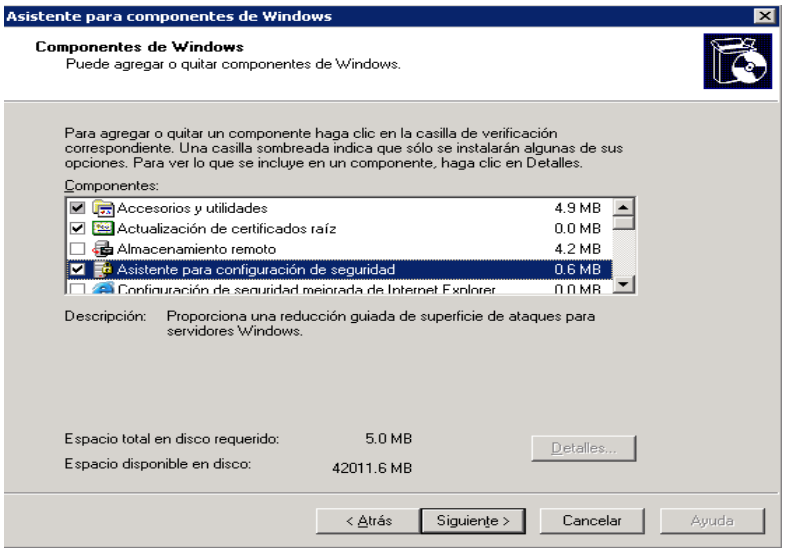


Figura 3.139 Asistente para configuración de seguridad

Se comienza la instalación la cual tarda unos minutos, al concluir el proceso se da clic en el botón de *finalizar* y ahora dentro de las *Herramientas administrativas* se encuentra instalada la aplicación *Asistente para configuración de seguridad*, se busca la herramienta y se accede a ella. Ver figura 3.140

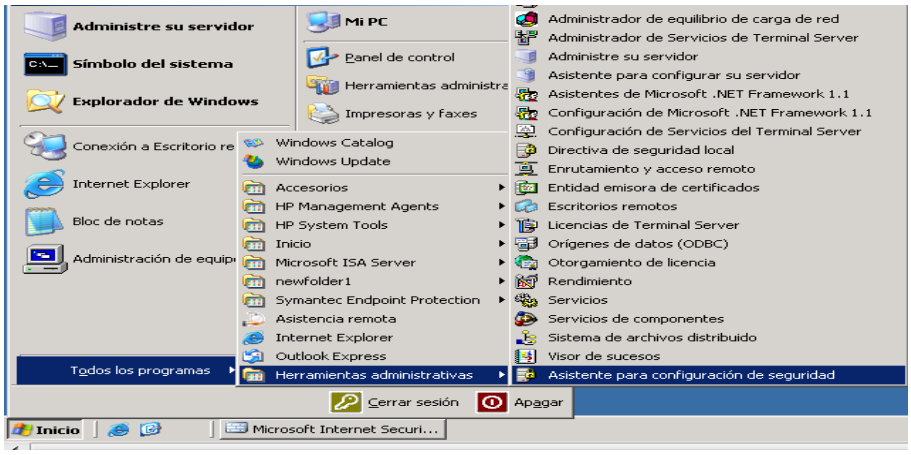


Figura 3.140 Ingresar al Asistente de configuración de seguridad

Se inicia el *Asistente para la configuración*, y como se indica, de acuerdo a los servicios y aplicativos brindados por cada servidor, se ponen en marcha, para que el asistente detecte los puertos en uso. Ver figura 3.141

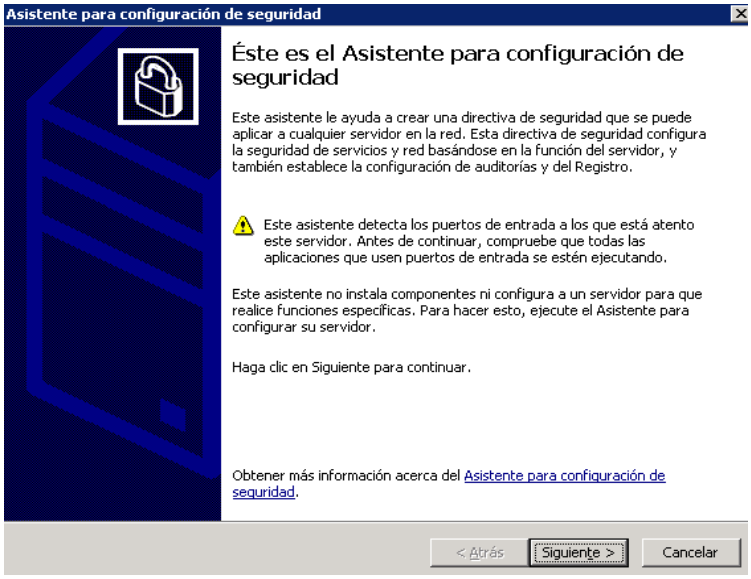


Figura 3.141 Inicio de Asistente

Dentro del siguiente paso se crea una nueva directiva de seguridad y se da clic en *siguiente*. Ver figura 3.142

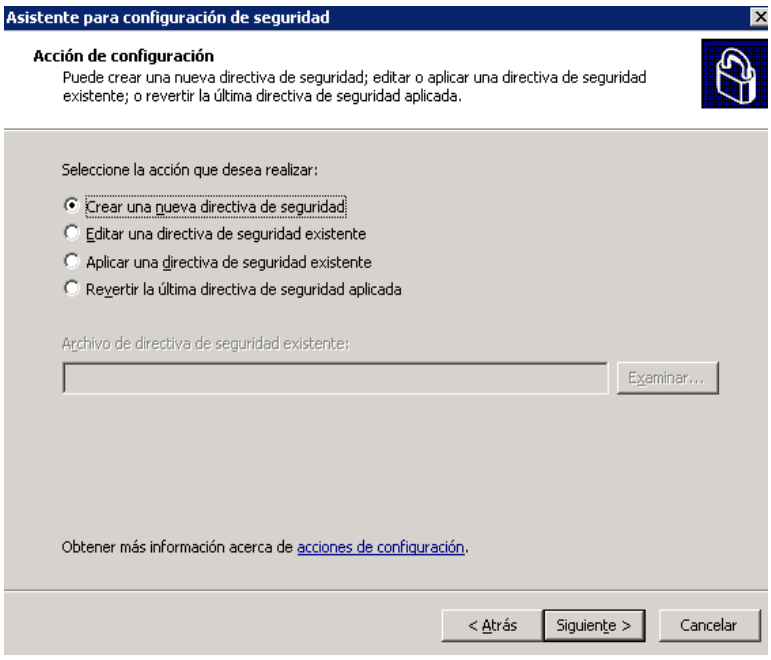


Figura 3.142 Creación de nueva directiva de seguridad

Como siguiente paso se selecciona un servidor de línea de base para esta directiva de seguridad, por lo cual se elige el mismo servidor local y continuamos. Ver figura 3.143

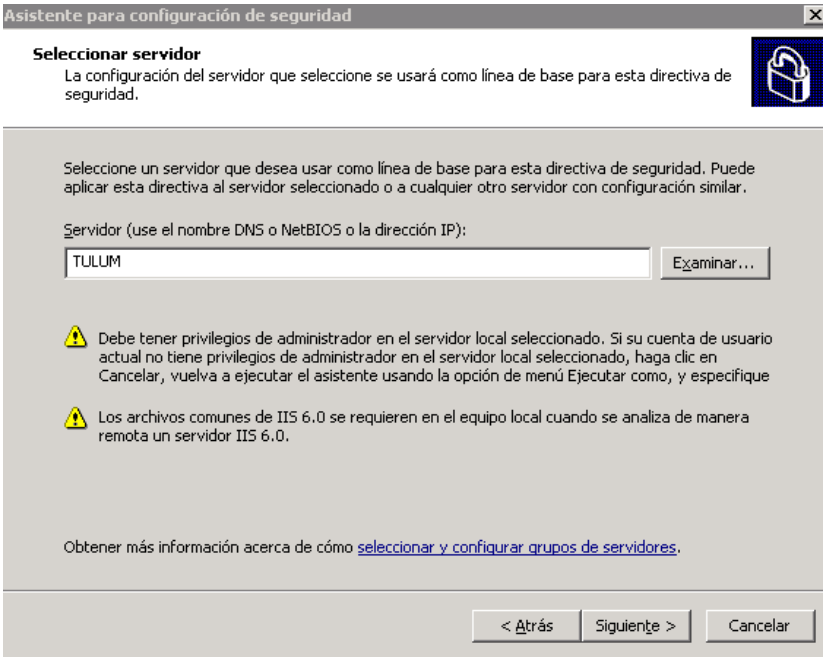


Figura 3.143 Servidor de línea de base

Después se inicia un proceso de configuración, al finalizar muestra una ventana donde se continúa con el *Asistente de configuración*, en esta sección se configuran los servicios basados en las funciones del servidor, es importante realizar correctamente esta sección ya que de no ser así podemos deshabilitar servicios necesarios para alguna aplicación. Ver figura 3.144

Figura 3.144 Configuración de servicios

Debido a que un servidor puede realizar diversas funciones y entregar distintas aplicaciones es necesario que se seleccionen las funciones instaladas para determinar el nivel de restricciones, de esta forma, en cada casilla, según las funciones, selecciono las funciones convenientes. Ver figura 3.145

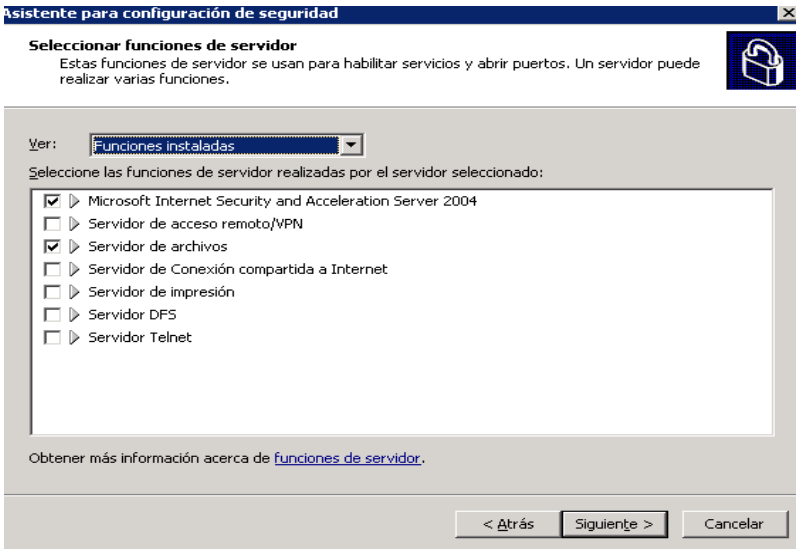


Figura 3.145 Selección de funciones

Como siguiente paso se seleccionan las características de clientes, las cuales son utilizadas para habilitar servicios de acuerdo a las aplicaciones o funciones para las que esté destinado el servidor, tomando en cuenta las herramientas de monitoreo que se usan en este servidor se seleccionan las características de cliente. Ver figura 3.146

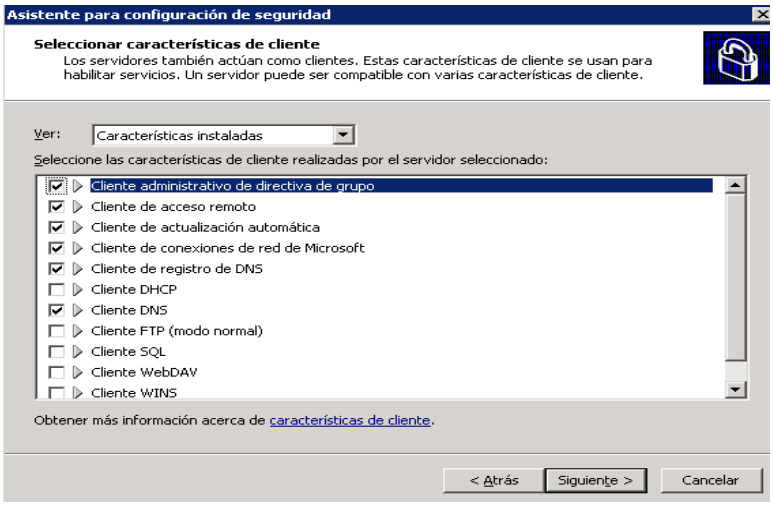


Figura 3.146 Selección de características de cliente

En la siguiente ventana del asistente se deben configurar las opciones de administración, que son las que se utilizan para habilitar servicios y abrir puertos con relación a las herramientas de administración que sean requeridas y utilizadas. Ver figura 3.147

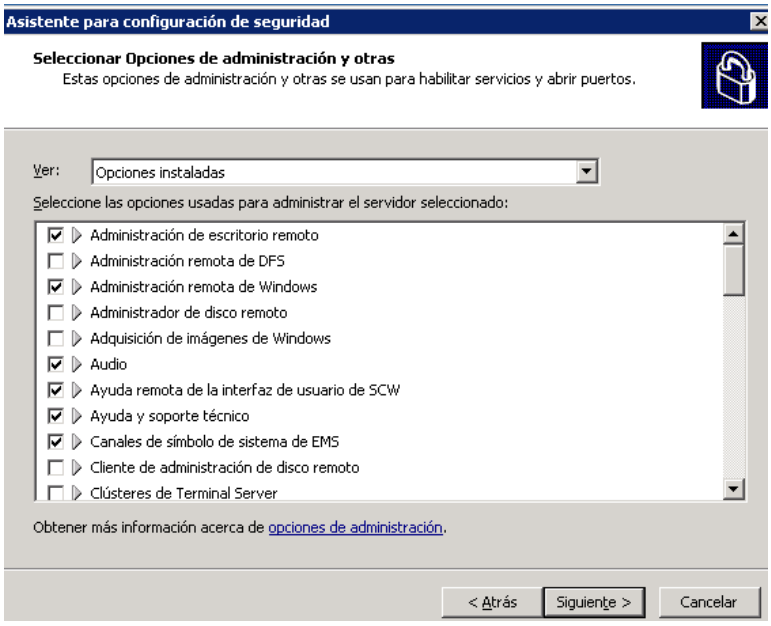


Figura 3.147 Configuración de opciones de administración

En el paso siguiente del asistente se seleccionan servicios adicionales los cuales fueron instalados por medio de aplicaciones externas como son antivirus, herramientas y otros sistemas de administración. Ver figura 3.148

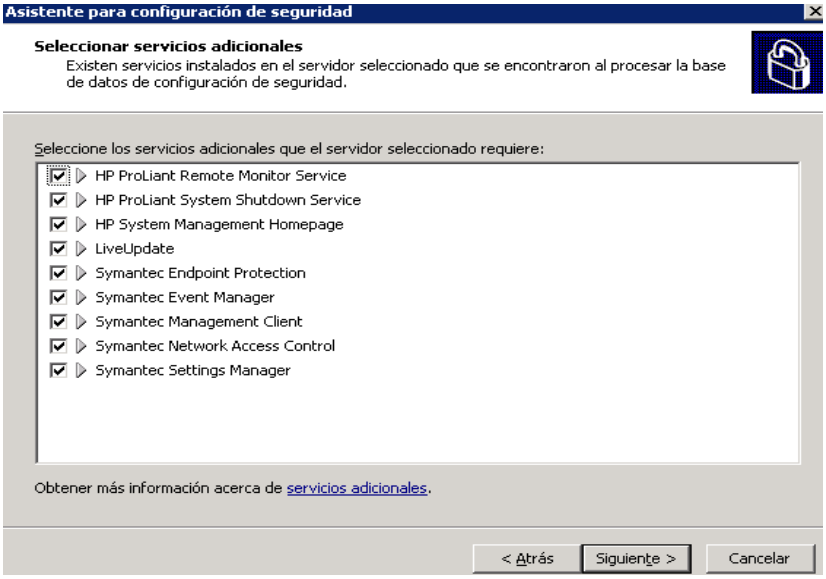


Figura 3.148 Configuración de servicios adicionales

Debido a que esta directiva de seguridad también puede ser aplicada en otros servidores, se debe asignar la forma en que se va a actuar en otros servidores si se implementa la misma directiva, se pueden deshabilitar los nuevos servicios encontrados o se pueden conservar, por ello decido elegir *No cambiar el modo de inicio del servicio*. Ver figura 3.149

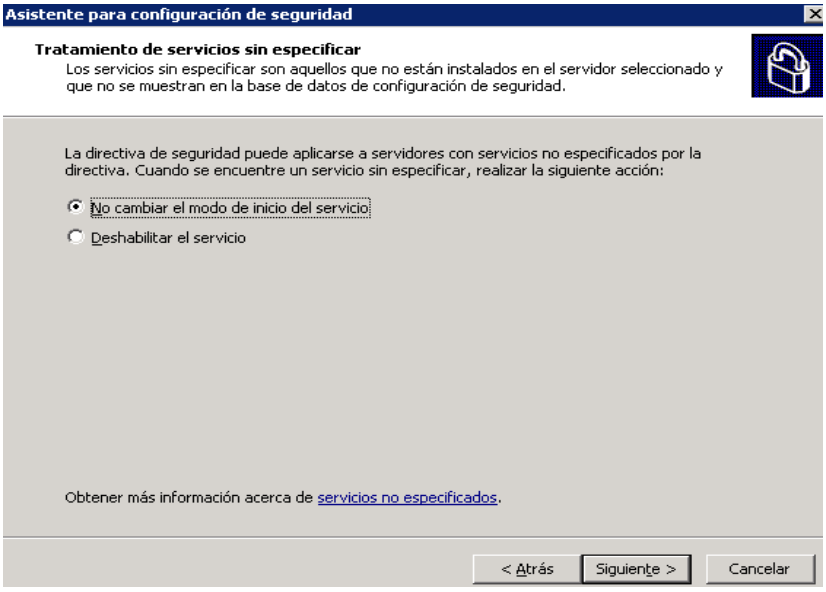


Figura 3.149 Configuración de servicios sin especificar

Una vez realizada esta configuración se muestra una ventana resumen donde se observan todos los cambios en los servicios, en su forma de inicio actual y la asignada por directiva de seguridad creada, si todas las configuraciones realizadas son las correctas de acuerdo al servicio y su aplicación se da clic en siguiente. Figura 3.150

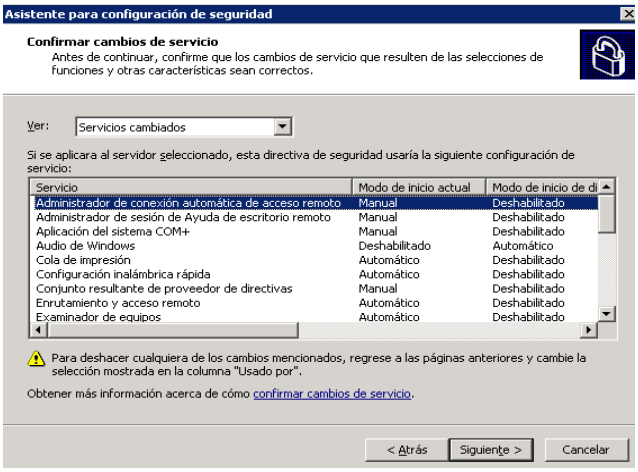


Figura 3.150 Resumen de configuración

Al finalizar esta parte, se inicia otra sección donde se configuran los puertos de entrada por medio del firewall de Windows y las aplicaciones configuradas. Ver figura 3.151

Figura 3.151 Configuración de puertos de entrada

Debido a que donde se lleva a cabo esta configuración es un servidor Firewall de contenido Microsoft ISA Server el asistente no realiza esta configuración, por lo cual se da clic en siguiente. Ver figura 3.152

Figura 3.152 Función Microsoft ISA Server

El siguiente paso del asistente es la configuración de los protocolos de comunicación entre el servidor, sus clientes y otros equipos. Ver figura 3.153

Figura 3.153 Configuración de protocolos

La siguiente configuración que se realiza es la de políticas mínimas de los clientes para poder obtener los servicios y comunicación con el servidor, además de habilitar las firmas digitales. Ver figura 3.154

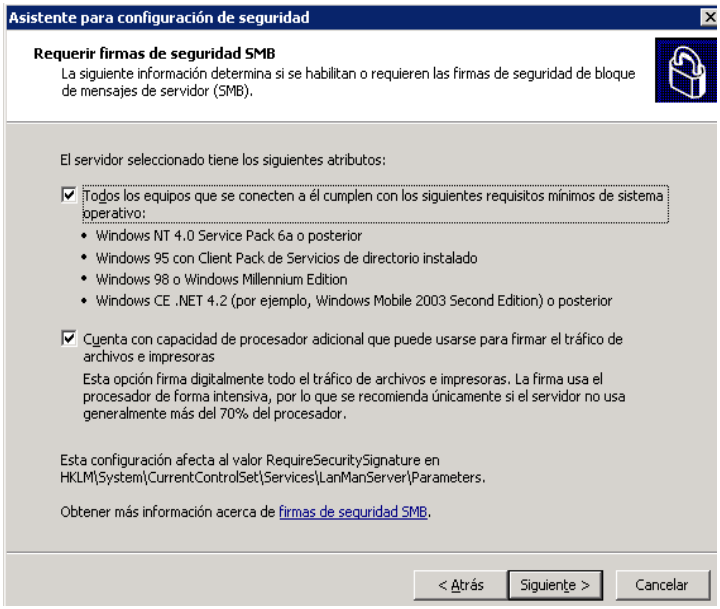


Figura 3.154 Configuración de firmas digital

Ahora se configura la forma en que los clientes se autentican, debido a que el servidor se encuentra en una plataforma de dominio se selecciona la opción *Cuentas de dominio.* Ver figura 3.155

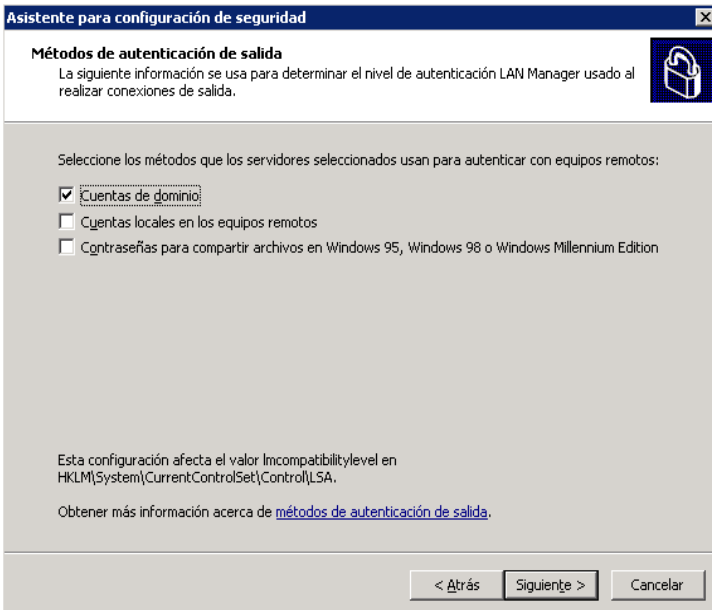


Figura 3.155 Configuración método de autenticación

Dentro del paso siguiente se configura el nivel de autenticación LAN Manager donde se selecciona la opción de *Windows NT 4 o sistemas posteriores* y se da clic en *siguiente*. Ver figura 3.156

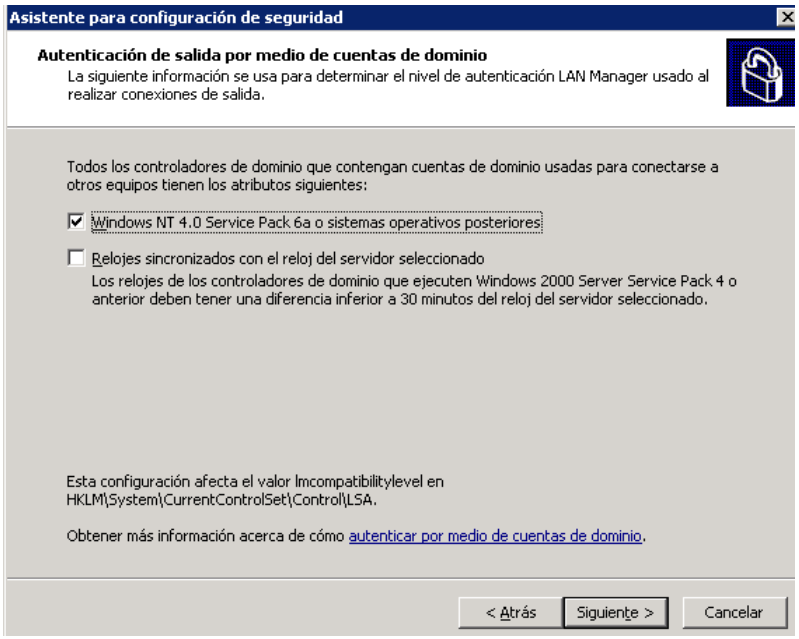


Figura 3.156 Configuración de autenticación LAN Manager

De igual forma para concluir esta sección y habilitar los cambios realizados se muestra el resumen de la configuración, si es la configuración que se requiere, se aplica *siguiente*. Ver figura 3.157

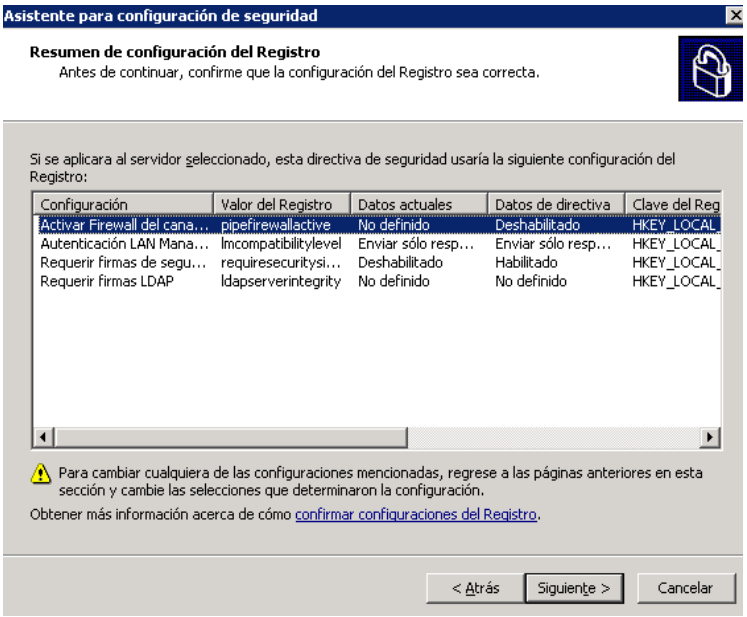


Figura 3.157 Resumen de configuración

Dentro de la siguiente sección se configuran las directivas de auditorías, que indican los sucesos correctos y erróneos que se registran. Ver figura 3.158

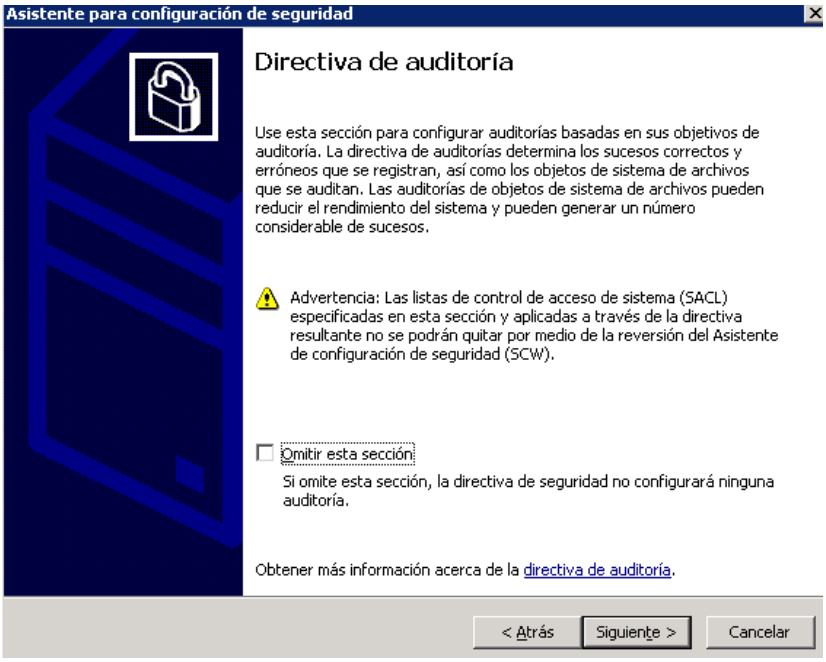


Figura 3.158 Directiva de auditoría

Como siguiente paso se asigna el objetivo de dicha directiva de auditoría, se selecciona la opción de *Auditar actividades correctas*, que permite reconstruir sucesos, determinar el autor de determinados cambios y mantiene un rendimiento alto del sistema. Ver figura 3.159

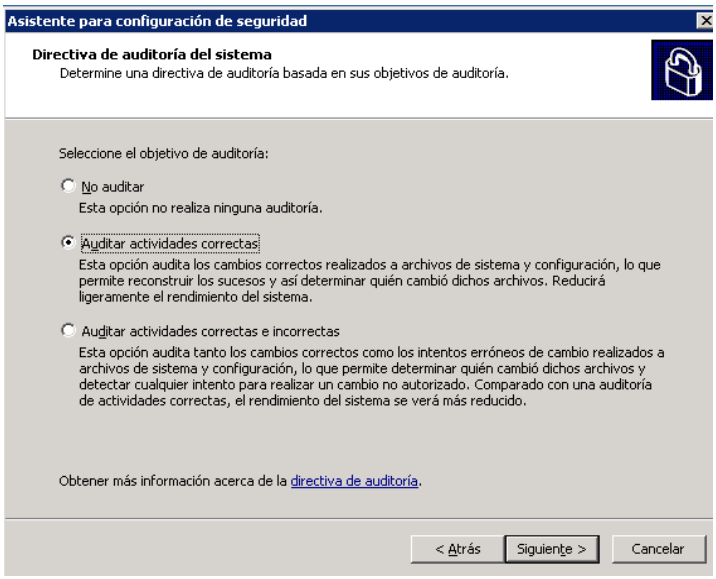


Figura 3.159 Directiva de auditoría

A continuación muestra un resumen de las opciones elegidas, si esto es correcto se da clic en *Siguiente* para continuar. Ver figura 3.160

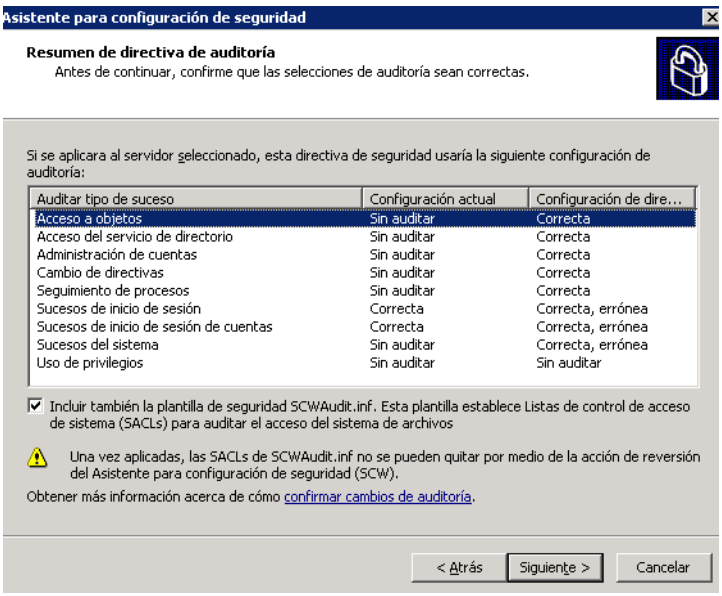


Figura 3.160 Resumen de auditorías

En la sección siguiente se configuran las opciones de almacenamiento de la nueva directiva de seguridad creada. Ver figura 3.161

Figura 3.161 Guardar directiva de seguridad

El siguiente paso de esta sección es asignar un nombre y directorio para la directiva de seguridad creada. Ver figura 3.162

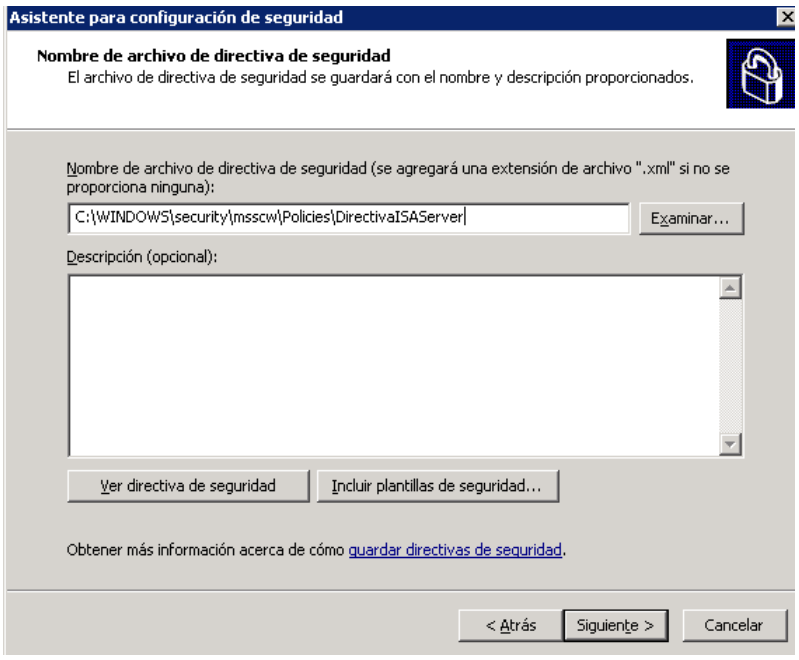


Figura 3.162 Asignación de nombre de directiva

En la siguiente ventana se muestra la opción de aplicar la directiva en ese instante o guardarla para ser aplicada más tarde, en esta opción elijo *Aplicar ahora.* Ver figura 3.163

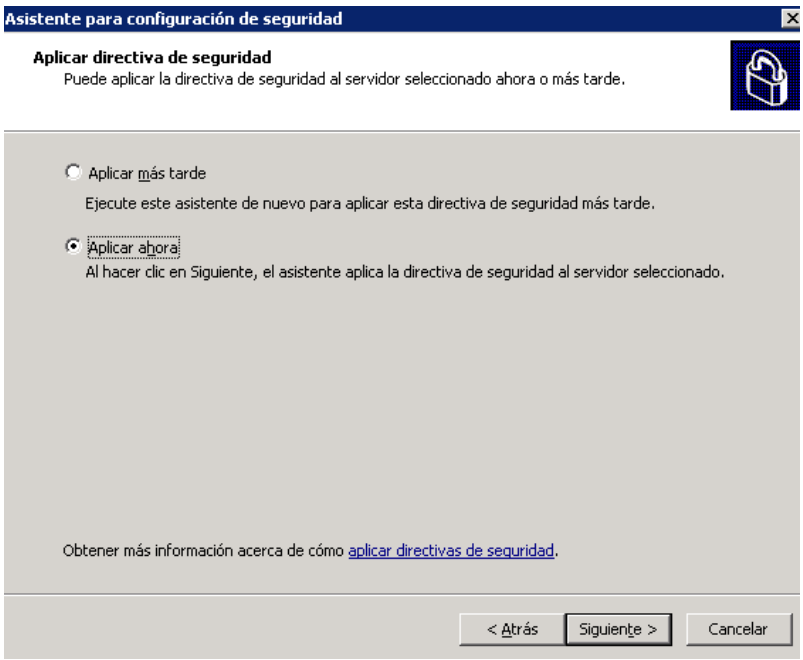


Figura 3.163 Aplicar directiva de seguridad

El proceso de aplicación de directiva inicia, el cual tarda unos minutos y al finalizar se da clic en *Siguiente*. Ver figura 3.164

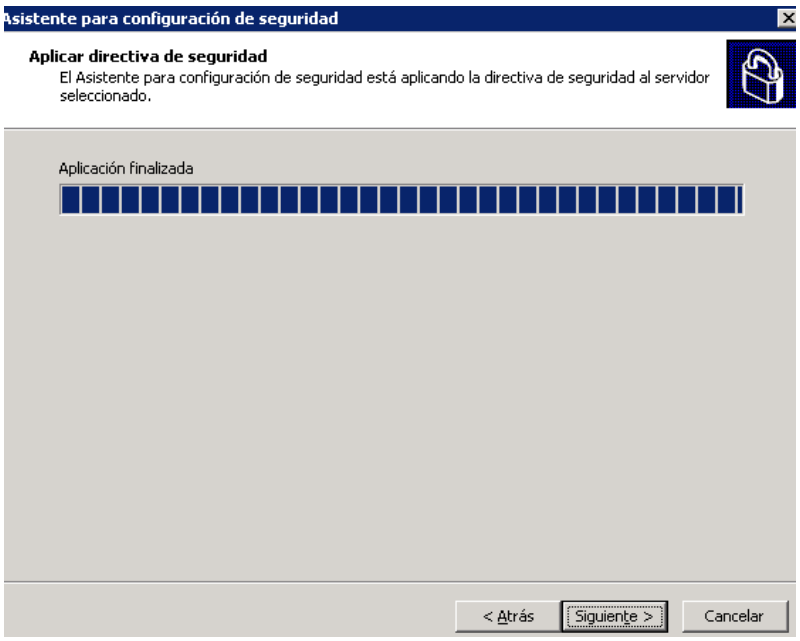


Figura 3.164 Aplicación de directiva de seguridad

Con esto se concluye la creación y aplicación de una directiva de seguridad para el aseguramiento de un servidor con sistema operativo Windows Server 2003. Ver figura 3.165

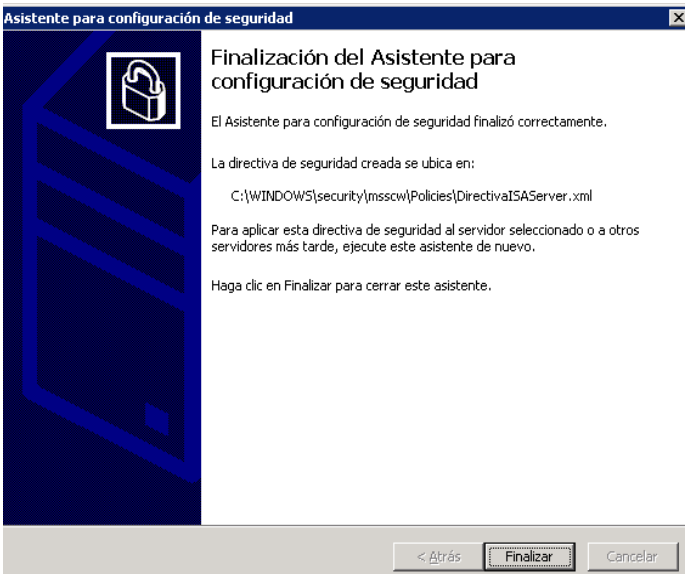


Figura 3.165 Finalización del Asistente para creación de directiva

Por medio de esta implementación se acotaron los servicios, funciones, aplicaciones, protocolos y puertos para brindar los servicios para los que fue creado el servidor pero limitando muchos sectores que pudieran ser una puerta para ataques o posibles problemas en el futuro.

4. RESULTADOS

En este capítulo se exponen los resultados obtenidos y su análisis a través de las implementaciones especificadas dentro del diseño del proyecto, realizadas anteriormente y de las cuales se desglosa lo siguiente.

Dentro de las implementaciones realizadas de administración de aplicaciones y sistemas, encontré que existía un alto nivel de desactualización y una falta de orden en los procesos que día a día se realizan dentro de cada una de las actividades para las cuales se llevó a cabo acciones de administración.

Al realizar la administración de dominio de la organización pude observar que se encontraba completamente desactualizada la base de altas y bajas de usuarios, así como cuentas clave que no pueden ser borradas pero que debían encontrarse deshabilitadas y sólo ser accesibles en el momento en que se requiera cierto tipo de información, estas cuentas con información sensible y con contraseñas sencillas se encontraban activas, con la correcta administración y actualización del dominio se redujo en un 40% el número de cuentas habilitadas y las inactivas se encuentran alrededor de las cinco cuentas, por medio de esta implementación se puede decir que se acota el número de accesos a los servicios e información de la organización, además se implementó para cada cuenta una cierta descripción del usuario y su labor en la empresa para facilitar las tareas de administración, lo cual a resultado de mucha ayuda para ubicar de mejor manera usuarios, restricciones, privilegios, entre otros elementos.

Otro de los desarrollos donde la administración fue fundamental es la administración de la VPN Contivity de Nortel Networks. Dentro de la organización se cuenta con dos tipos de VPN, una de ellas es la administrada por un Access Gateway de Citrix que se encuentra ligada al directorio activo de la organización, por lo tanto cualquier cambio en el dominio se verá reflejado en la autenticación de esta VPN, por lo cual una vez realizada la administración y actualización del dominio, la administración de la VPN Citrix queda actualizada, la administración y autenticación de la VPN Nortel se lleva de forma separada a la infraestructura de dominio por lo que se tuvo que hacer una actualización y administración de VPN´s que debían de encontrarse activas, dentro de esta implementación se observó que existían un gran número de cuentas demos, proyectos de mucho tiempo atrás, consultores, entre otros, personal de la organización con privilegios limitados, que no deberían de contar con este tipo de recursos, debido a que en

sucursales existe una gran rotación de personal, había muchas cuentas de nivel gerencial que estaban activas, cuando las personas tenían un largo tiempo de no laborar en la organización. Al realizar la depuración y dar acceso sólo a aquellos que estuvieran autorizados, los cuales son directivos y gerentes, la base de usuarios se redujo en un 60%, esto muestra que existía un gran índice de cuentas que no debían permanecer.

La correcta administración y actualización de la base de Mac Address permitió dentro de la organización tener un mejor control de quién ingresa a los recursos de red y quién tiene acceso a cierto tipo de información. Con esta implementación se logró disminuir en un 70% el número de equipos que podían obtener acceso a la red vía autenticación Mac Address, además de que cada uno de los usuarios que ahora tiene acceso a la WLAN TEAM, ya sea en sus equipos portátiles y/o móviles, pasaron por un filtro de autorización de acuerdo a cada área ya sea por un directivo o un elemento de la gerencia, con esto se limita el acceso a dispositivos que no sean estrictamente utilizados con la finalidad de desempeñar una actividad para las labores diarias de la empresa.

Dentro de la implementación de la actualización de parches de seguridad para los servidores activos de la organización, encontré que un gran número de estos no habían sido aplicados, entre mayor es el tiempo que tiene el servidor en activo, se encontró un mayor número de parches y actualizaciones faltantes, en algunos servidores no se contaba con el Service Pack más reciente y/o contaban con una infinidad de parches críticos que era de alta prioridad que fueran instalados; los servidores más recientes incorporados a la infraestructura de la organización se encontraban casi en su totalidad actualizados, sólo con algunas pequeñas actualizaciones no críticas a instalar. Esta implementación brinda una mayor protección por medio del sistema operativo a los servidores de los que depende la infraestructura de la empresa, entre más desactualizado se encuentre un sistemas y carezca de los parches más recientes, muchos problemas y agujeros podrán explotarse de forma sencilla, más si estos problemas se encuentran expuestos de mucho tiempo atrás y no han sido resueltos de forma inmediata, por lo ello la actualización constante de los sistemas es una buena práctica que debe ser desarrollada día a día para la mejora de la disponibilidad de nuestros servicios expuestos a través de estos servidores.

Dentro de las prácticas que se venían aplicando en el área, consistía en un sistema de contraseñas básico y débil lo que hacía, tanto a los equipos como a los elementos de la infraestructura, un blanco sencillo de ataques o intrusiones, ahora con la implementación de normas y buenas prácticas establecidas en el documento de políticas de seguridad informática referente a contraseñas, los usuarios pueden proponer sus propias contraseñas con lo cual es más fácil el poder recordarlas y evitar tener que restablecerlas de forma continua, estas contraseñas son establecidas siempre y cuando cumplan con las

características expuestas en el documento antes mencionado y obteniendo un nivel de bueno a excelente dentro de la herramienta de pruebas de complejidad de contraseñas proporcionada por Microsoft, una vez aprobadas por estos dos filtros son establecidas y sólo el usuario, mi compañero de soporte y yo, conocemos la contraseña, de esta forma no se ha reportado ningún incidente de intrusión, comportamiento extraño o suspicacias de intrusión en los equipos de la organización como había llegado a acontecer en algunas ocasiones desde que me encuentro en la empresa.

Continuando con las implementaciones de seguridad para los servidores de la infraestructura que son una de las piezas claves para proveer servicios y aplicaciones a la organización, se realizó la configuración de la herramienta de aseguramiento para los servidores con Windows Server 2003, con ella se logró acotar los servicios, puertos y protocolos de los servidores de acuerdo a las aplicaciones con las que cuenta cada uno y a los servicios que provee a la organización, con lo cual se reducen las probabilidades y los caminos para realizar ataques o intrusiones dentro de los servidores que administro. Los servicios, puertos y protocolos están reducidos simplemente a los necesarios para que los servidores cumplan las funciones para las cuales fueron implementados, ésta acción, entre otras, mejora la seguridad en torno a los servidores de la organización.

Dentro de las actividades de configuración se realizaron tareas de aseguramiento y administración de los firewalls de tipo appliance y por software, además de la protección del portal web de la organización a través de uno de estos dispositivos, por medio de las implementaciones se logró que aplicaciones demo para el área técnica y comercial se encontraran en la nube, disminuyendo los riesgos de seguridad. La página principal de TEAM México se puso bajo resguardo detrás de uno de estos firewall siendo redireccionada a través de éste, acotando sus accesos, lo cual hasta el momento, ha dado una alta disponibilidad e integridad en los datos que se manejan y de acuerdo a los logs del dispositivo de firewall, se han bloqueado ataques dirigidos hacia el portal web.

Una de las actividades que llevó más tiempo en su realización fue la implementación de la consola de administración de antivirus, ya que para llegar a la instalación y configuración de esta aplicación primero tuvo que realizarse un diseño apropiado con distintos factores como: listado de equipos y su rendimiento, sistemas operativos, personal con ciertos privilegios o restricciones, restricciones por áreas, exclusiones de acuerdo a puesto en la organización, análisis de horarios de actualizaciones para que el rendimiento de la red no se vea afectado, entre otros, que ayudaron a determinar la configuración y la forma en que sería administrada la consola.

Una vez implementada la consola de administración de antivirus, como era su propósito, es más sencilla la administración de los clientes en cuanto a la aplicación de antivirus,

protección y generación de políticas, de acuerdo a los grupos establecidos, ahora cada vez que se incorpora un nuevo equipo a la organización es muy sencillo asignarle una configuración de políticas y realizar una instalación transparente de la aplicación en el cliente, además se logró de buena forma optimizar la red a través de las actualizaciones programadas de la aplicación, ya que se definieron horarios donde el tráfico es bajo y se determinaron distintos horarios para los grupos y áreas para tener un mejor desempeño de la red.

Una vez concluidas todas estas implementaciones de seguridad informática, ya sea por medio de nuevas instalaciones, configuraciones, nuevas formas de administrar o actualizaciones de aplicaciones y parches, todo esto en conjunto le ha dado a la organización una estructura de seguridad informática a partir de la cual desarrollarse y crecer. Dichas implementaciones sientan las bases para poder contar con una empresa más sana en cuestión de nuevos procesos y poder brindar así servicios más confiables, siempre disponibles y con mejor tiempo de respuesta.

Estas implementaciones serán la base para formar una estructura más sólida en cuanto a la seguridad informática se refiere, a partir de lo desarrollado se buscarán implantar nuevas políticas hacia usuarios y mejorar las existentes, para el segundo semestre de este año se tiene planeada una reestructuración importante por medio de hardware y software HP Networking con un firewall especializado y un dispositivo IPS, lo cual hará más confiable la red de la organización, antes de su implementación se buscará la realización de mi certificación en la instalación, configuración y administración de estos dispositivos. Se planea también la renovación de la infraestructura de Switches por una totalmente nueva que traerá consigo una nueva configuración en cuanto a la red, su distribución y proporción de acuerdo al crecimiento que la organización ha tenido a lo largo estos años.

De esta forma se concluye el Informe de Actividades de acuerdo a las implementaciones de seguridad informática realizadas dentro de la empresa, Tecnología Especializada Asociada de México, quedando a mi cargo los aspectos relacionados con la administración de la infraestructura y el aseguramiento de la información.

CONCLUSIONES

Dentro de esta sección se presentan las conclusiones que obtuve de la realización del proyecto anteriormente elaborado.

Por medio de este proyecto aunque ya contaba con conocimientos y algo de experiencia tanto en el área de seguridad informática así como en implementaciones en el sector privado, llevar a cabo este proyecto tuvo consigo un gran esfuerzo tanto técnico como en las relaciones laborales, ya que como he venido mencionando uno de los pilares más importantes para el rendimiento óptimo de una infraestructura de TI y comunicaciones, son los usuarios y sus buenas practicas, pero comúnmente estas buenas prácticas son desconocidas por los usuarios o son pasadas por alto, lo cual como administrador de TI dificulta el trabajo y la convivencia con los usuarios.

Un aspecto muy importante es hacerle ver a los usuarios que todas estas normas, estándares y buenas prácticas son para su beneficio y el mejoramiento del desempeño laboral, para así brindarles más y mejores herramientas y hacer más eficientes las labores de su día a día dentro de la organización y lo último que se quiere es obstaculizarlos en su trabajo.

Existieron personas muy renuentes a realizar el cambio de contraseñas ya que todo el tiempo que venían laborando en la empresa habían contado con una misma, también hubo descontento entre el personal que de acuerdo a sus gerentes no deberían contar con accesos a la VPN de la organización y otros servicios los cuales les fueron restringidos, debido a este tipo de cuestiones fueron algo complicadas estas implementaciones para las cuales se requería de la interacción con los usuarios.

Otro tópico que debo mencionar es acerca de la importancia que la dirección le da a la seguridad de su información, dentro de la empresa en la que laboró aunque se encuentra dentro del rubro de la comercialización e integración de TICS, aun así es complicado concientizar a la dirección de que la inversión en seguridad informática es muy importante para el aseguramiento de la información valiosa y el óptimo desempeño de los servicios que se brindan a los usuarios, por lo cual pienso que en otro tipo de organizaciones con giros distintos a la tecnología, este aspecto se complica todavía más y los recursos destinados a la seguridad son escasos, incrementándose así los costos de implementación o recuperación cuando llega a presentarse un incidente grave, ya que esto se realiza bajo

presión, sin tiempo de análisis y se optan por alternativas apresuradas, de este modo una correcta planeación y prevención es la mejor forma de implementar una buena estructura de seguridad. Aunque día a día se desarrollan nuevos virus y formas de ataques, contando con una estructura de seguridad bien definida podemos acotar los accesos y/o vulnerabilidades y así poder reaccionar de una forma más rápida y mejor ante los problemas que lleguen a presentarse.

Por otra parte a través de las implementaciones me pude dar cuenta que la parte técnica y la puesta en marcha es la pieza cúspide de un proyecto, pero lo que va a ser la guía para una implementación exitosa siempre serán las bases, como un exhaustivo análisis y una correcta planeación, tratando de abarcar todos los aspectos que intervienen, teniendo en cuenta estos aspectos el correcto funcionamiento y exitosa implementación estará casi asegurada, aunque este ciclo de análisis y planeación se prolongue, a la larga reducirá los tiempos en modificaciones o factores que no fueron tomados en cuenta.

Para la realización del proyecto fue indispensable de un completo análisis de la estructura de la empresa en sus diversas áreas, ya que muchas políticas no se pueden aplicar de igual forma debido a la información que se maneja y a las actividades que desempeñan, por lo cual una regla no se puede aplicar de la misma forma para todos, existen muchas excepciones que se deben tomar en cuenta para no obstaculizar a los usuarios en el intento de brindarles mejores servicios, por lo cual el conocimiento de las actividades de cada área y su interacción con otras fue indispensable para desarrollar implementaciones y políticas que se adaptaran a cada una de estas.

Dentro de lo que pude observar a lo largo del proyecto, es que aunque las metodologías e implementaciones de seguridad informática no son algo nuevo y los que estamos involucrados en el área de las TI vemos todos los días información nueva relacionada con seguridad, implementaciones más avanzadas, nuevos estudios, etc. Para muchos usuarios parecería como un mito, donde por medio de un antivirus están completamente protegidos de absolutamente todo, o donde en algunos otros, la desinformación es más elevada que prefieren aumentar el rendimiento de sus equipos por mínimo que sea, evitando la instalación de este tipo de herramientas, por lo cual el concientizar a las personas, de nueva cuenta es un punto primordial, además de que aquellas implementaciones que se realicen de nada servirán si el usuario da la llave de entrada a los intrusos.

Un aspecto peculiar e importante al cual me enfrente desarrollando estas implementaciones dentro de la empresa, lo cual tienen sus pros y sus contras, es que toda la infraestructura de TI se debe de basar en las soluciones que la organización comercializa, debido a la imagen que se proyecta ante los clientes, por lo cual esto acota

las implementaciones a tecnologías que en la organización se manejan, aunque esto facilita la adquisición de soluciones que de otra forma seria complicada contar con ellas por sus elevados costos, también se cuenta con restricciones para implementar soluciones de software libre o appliences de otras marcas.

Al llevar a cabo este proyecto me di cuenta que una solución no solo es buena o protege más que otra, debido al número de procesos que realiza o al elevado costo que esta tenga, hay que tener un completo análisis de lo que se va a proteger y de las acciones que se quieren realizar, si solo se implementan soluciones o herramientas sin conocimiento o análisis previo, estas no servirán de nada y la finalidad para la cual fue implementada no se cumplirá, en cambio sí tenemos plena conciencia de la bondades que brinda la herramienta y contamos con un análisis de lo queremos obtener de ella, la buena configuración y administración lograrán que la implementación sea exitosa y brindará los servicios para las cuales fue adquirida y/o desarrollada.

Como antes mencioné, las políticas, reglas y buenas prácticas deben ser adaptativas, lo que para una organización puede ser excelente, para otra puede no tener efecto alguno, por lo cual este tipo de cuestiones deben de desarrollarse a la medida, tomando en cuenta cada aspecto, cada rol, la cultura en general de los usuarios, partir de esto, determinar cómo serán implantadas ciertas normas, más importante será que estas se lleven a cabo en los términos establecidos pero brindándoles a los usuarios una satisfacción en donde ellos las adopten y no se les forcé o sea una obligación.

Gracias a este proyecto tuve la oportunidad de aplicar todos los conocimientos teóricos adquiridos con anterioridad, realizar implementaciones en un ambiente real, en producción, donde cada cosa que se realiza, cada cambio, tiene un efecto determinante en el desarrollo de la organización y donde el margen para errores es muy escaso, en el cual las cosas que se planean de una forma u otra se tienen que concretar, no se pueden quedar sin concluir, no solo los conocimientos en el aspecto técnico son importantes, también el trato con las personas, el hacer suyas las implementaciones, las políticas, las reglas y los privilegios, que el usuario le dé la importancia que requiere a su información y a los servicios que se le brindan. Por medio de este proyecto conocí muchas tecnologías, muchas soluciones. A través de los desarrollos ejecutados en esta empresa, aplique mis conocimientos de una forma tangible, que se viera reflejada en el desempeño diario de las actividades, en el que cada movimiento afecta el flujo en que la organización avanza, la importancia de las tecnologías y los servicios que brinda el área de TI pueden mejorar u obstaculizar todos los esfuerzos que se generan a través de los personas que en la organización laboran.

De esta forma me parece que este proyecto tiene un gran impacto para la organización Tecnología Especializa Asociada de México, debido a que en cuestiones de seguridad se encontraba muy elemental, casi nula, con implementaciones por default, contraseñas inseguras, etc. Pero tampoco quiere decir que con esto la organización se encuentra totalmente protegida y esté libre de ataques, esta implementación sienta las bases de una seguridad más robusta y procesos más ordenados a través de los cuales partir y seguir implementando, innovando y desarrollando, conforme la empresa siga creciendo, crear mejores procesos de aseguramiento, más exactos y precisos en donde los engranes fluyan de forma natural y la seguridad informática sea el día a día de la administración, dirección, así como de los usuarios.

Esta implementación me abrió un nuevo panorama en cuanto a soluciones existentes, tecnologías libres y propietarias de seguridad, protocolos y nuevos avances en esta área de conocimiento.

GLOSARIO

Acometida.- lugar por donde la línea de conducción se enlaza con la red principal.

Active Directory-Directorio Activo (AD).- es un componente central de la plataforma Windows que proporciona los medios para gestionar las identidades y relaciones que organizan los entornos de red.

Activos.- conjunto de bienes y derechos de los que es titular la empresa.

Activos lógicos.- conjunto de conocimiento o cúmulo de información y datos empresariales.

Adware.- contracción de las palabras Advertising Software. Se denomina adware al software que muestra publicidad, empleando cualquier tipo de medio: Pop-Up, Banners, cambios en la página de inicio o de búsqueda del navegador, etc.

Agujeros de seguridad.- falla en la seguridad de una aplicación, sistema informático o sitio web, que permiten ser explotado por una persona no autorizada. Los agujeros son considerados bugs de programación.

Amenazas de día cero.- amenazas a vulnerabilidades que los productores de software todavía no han tenido tiempo de remendar en sus programas.

Análisis de tráfico.- análisis del flujo de información y datos que atraviesa por una red determinada.

Análisis forense.- uso de principios y métodos científicos, aplicados sobre evidencia obtenida de fuentes digitales, con el fin de facilitar la reconstrucción de eventos.

Antivirus.- aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en sistemas informáticos.

Appliance.- dispositivo que combina hardware y software instalado para realizar tareas específicas.

ARP-Address Resolution Protocol.- Protocolo de Resolución de Dirección. Protocolo que emplea una computadora para correlacionar una dirección IP con una dirección de hardware.

Ataques informáticos.-intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red.

Australian Information Security Association.- asociación dedicada a la investigación, desarrollo, promoción, entre otras cosas de la seguridad informática.

Benchmarks.- punto de referencia estándar reconocido de excelencia contra el cual los procesos son medidos y comparados**.**

Bienes físicos.- son todos aquellos bienes tangibles, es decir, que se pueden tocar y ocupan un espacio. Por tanto, la inversión es tangible.

Boletín de seguridad.- forma de difundir actualizaciones, parches y mejoras en la seguridad de forma regular o periódica.

Bots.- es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario.

Bugs.- también conocidos como *holes* o agujeros. Defecto en un software o un hardware que no ha sido descubierto por los creadores o diseñadores de los mismos.

Cabeceras de paquetes.-contiene la dirección del equipo de origen y destino o el identificador del Circuito Virtual.

Cableado estructurado.- estándares y normativas para el diseño y tendido del cableado a lo largo de un inmueble.

Caché.- componente que almacena datos para que los futuros requerimientos a esos datos puedan ser servidos más rápidamente, generalmente son datos temporales.

Canal cerrado.-canal de distribución con ciertos candados como certificaciones y capital de canal.

Canales.- canales de distribución para hacer llegar al cliente final los productos con los que se cuenta.

Código fuente.- texto escrito en un lenguaje de programación específico y que puede ser leído por un programador. Debe traducirse a lenguaje máquina para que pueda ser ejecutado por la computadora o a bytecode para que pueda ser ejecutado por un intérprete.

Conmutador.- se encarga de establecer un enlace físico o un enlace lógico entre los terminales.

Core.- aplicación o dispositivo principal.

Corto circuito.- conexión accidental de dos conductores de distinta fase, o de éstos con el neutrón.

Crackers.- es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

Data center.- es una instalación empleada para albergar los sistemas de información y sus componentes asociados, como las telecomunicaciones y los sistemas de almacenamiento.

Datos.- un dato se define como la unidad mínima de información o bit, puede ser un carácter, una palabra, etc**.**

Database(DB).- es una colección de información organizada de forma que un programa informático pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico.

Demos.- es una aplicación o sistema, que sirve para mostrar cómo es y cómo funciona, pudiendo conocer el mismo.

Destinatario.- persona a quien va dirigida o destinada alguna cosa.

Dhcp-Dynamic Host Configuration Protocol.- el protocolo de configuración dinámica de host DHCP, es un estándar IP diseñado para simplificar la administración de la configuración IP del host. El estándar DHCP permite el uso de servidores DHCP para administrar la asignación dinámica a los clientes DHCP de la red, de direcciones IP y otros detalles de configuración relacionados.

Display.- monitor, pantalla, forma en que se muestra algo.

Dmz.- es una red que se encuentra expuesta a las conexiones entrantes de Internet, y por ello queda recluida en un segmento de red cuyo tráfico saliente se encuentra lo más restringido posible.

Dns.- es una abreviatura para Sistema de nombres de dominio, Domain Name System, un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP.

Domain Controller-Controladora de dominio.- es una entidad administrativa, esto es, no es un equipo en concreto, sino un conjunto de equipos agrupados que se rigen a unas reglas de seguridad y autenticación comunes.

E1.- equivale a 2048 kilobits o 256 kilobytes. Contar una trama E1 significa contar con un servicio de 30 líneas telefónicas digitales para comunicaciones.

Emisor.- es aquel objeto que codifica el mensaje y lo transmite por medio de un canal o medio hasta un receptor.

Endpoints.- punto final, cliente final.

Enlace dedicado.- es una conexión directa desde un punto, hasta la central o hasta un backbone de internet, esto garantiza un enlace más confiable.

Equipo de cómputo.- es una máquina electrónica que permite el procesamiento de datos.

ERP-Enterprise Resource Planning.- sistemas de planeación de los recursos de la empresa de forma integral.

Firewall.- herramienta de seguridad que controla el tráfico de entrada/salida de una red.

Firma digital.- es el resultado de un procedimiento realizado con una clave numérica llamada clave privada la cual es creada por un algoritmo de generación de claves el cual se encarga de generar junto con la clave privada una segunda clave denominada clave pública que funciona como complemento de esta clave privada. La clave privada debe permanecer bajo el exclusivo control de su propietario siendo este el único capaz de tener acceso a ella, esta característica es lo que permite que una firma digital identifique en forma unívoca al firmante, la clave pública por otra parte es la que permite verificar a un tercero el origen de la firma y la no alteración del mensaje.

FTP-File Transfer Protocol.- el protocolo de intercambio de archivos.

Gateway.- es una puerta de enlace, acceso, pasarela. Es un nodo en una red informática que sirve de punto de acceso a otra red.

Hacker.- el término hacker, se utiliza para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal sin intentar causar daños.

Hardening.- se le llama así al aseguramiento por medio de herramientas, bloqueo de puertos, limitación de aplicación, entre otros, para asegurar un servidor en este caso.

Hardware.- cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora.

Heurística.- es la capacidad que ostenta un sistema determinado para realizar de manera inmediata innovaciones positivas para sí mismo y sus propósitos.

Host.- es un sistema que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde residen servicios.

Http-Hyper Text Transfer Protocol.- (Protocolo de transferencia de hipertexto) es el método más común de intercambio de información en World Wide Web, el método mediante el cual se transfieren las páginas web a un equipo de cómputo.

Https-Hypertext Transfer Protocol Secure.- es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en WWW, generalmente para transacciones de pagos o cada vez que se intercambie información sensible.

IIS.-Internet Information Services.- es un conjunto de servicios para servidores usando Microsoft Windows. Es especialmente usado en servidores web.

Intranet.- red entre computadoras montada para el uso exclusivo dentro de una empresa u hogar. Se trata de una red privada que puede o no tener acceso a Internet.

IP homologada.- es aquella IP pública que puede ser visible y accedida a través del mundo exterior.

Java.- es un lenguaje de programación por objetos creado por Sun Microsystems, Inc. que permite crear programas que funcionan en cualquier tipo de ordenador y sistema operativo.

Keyloogers.- programa informático que registra todas las pulsaciones que se realizan sobre un teclado para ser guardadas en un archivo o para ser enviadas por internet. El fin de un keylogger puede ser malicioso porque quien lo instala puede hacerlo de forma oculta y logrará así saber todo lo que se escribe sobre el teclado.

LAN-Local Area Network.-Red de Área Local conexión de múltiples computadoras dentro de un edificio, de manera que pueden compartir información, aplicaciones y dispositivos periféricos.

Leads.- adelantar o tomar la delantera.

Live update.- aplicativo para llevar a cabo actualizaciones.

Mac Address.- identificador de 48 bits que se corresponde de forma única con una interfaz de red.

MAN-Metropolitan Area Network.- Red de Área Metropolitana. Red de alta velocidad que cubre un área geográfica extensa. Es una evolución del concepto de LAN (red de área local), pues involucra un área mucho más grande como puede ser un área metropolitana.

Mesa de configuraciones.- equipo de ayuda para realizar configuraciones con respecto a servidores, redes, entre otros.

Mp3.- es el nombre de la extensión de archivo y también el nombre del tipo de archivo para MPEG, capa audio 3.

Navegador web.- aplicación que sirve para acceder a la WWW (World Wide Web) y navegar por ella a través de los enlaces o URL. Generalmente estos programas no sólo traen la utilidad de navegar por la WWW, sino que pueden también administrar correo, grupos de noticias, ingresar al servicio de FTP, etc.

Nube.- es un paradigma que permite ofrecer servicios de computación a través de Internet. La "nube" es una metáfora de Internet.

Ping-Packet Internet Groper.- Rastreador de Paquetes Internet. Programa que es empleado para verificar si un host o servidor está disponible (conectado, en funcionamiento o activo).Para comprobarlo envía paquetes de datos, si el servidor remoto responde significa que está activo.

Piratas informáticos.- aquellos hackers que emplean sus conocimientos con fines ilegales, inmorales o con fines de lucro.

Plug in.- programa que puede anexarse a otro para aumentar su funcionalidad. Es un módulo aparte que se incluye opcionalmente en una aplicación.

Políticas de seguridad informática.- plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad.

POP3-Post Office Protocol 3.- Protocolo 3 de Correo. Es un protocolo estándar para recibir mensajes de correo electrónico. Los mensajes son enviados a un servidor, son almacenados por el servidor pop3. Cuando el usuario se conecta al mismo (sabiendo la dirección POP3, el nombre de usuario y la contraseña), puede descargar los archivos.

Portal web.- sitio web que, por su gran cantidad de información, enlaces y servicios, puede satisfacer las necesidades de cualquier usuario. En general los portales ofrecen servicios como: directorios, servicio de provisión de correo electrónico, buscador para su sitio, noticias generales, chats, grupos de noticias, etc.

Puertos lógicos.- son aquellos usados como medio de comunicación de datos a través de las redes**.**

RDP-Remote Desktop Protocol.- protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre una terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en la terminal mediante el ratón o teclado).

Red.-sistema de comunicación entre computadoras que permite la transmisión de datos de un equipo a otro, con lo que se lleva a cabo entre ellos un intercambio de todo tipo de información y de recursos.

Rootkit.- es una colección de herramientas que permiten a un hacker crear backdoors en un sistema, recolectando información sobre otros sistemas en la red.

Router.- dispositivo de hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. El router toma decisiones (basado en diversos parámetros) con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.

SAN-Storage Area Network.- Red de Área de Almacenamiento, es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

Service Pack.- agrupación de actualizaciones, reparaciones y ampliaciones para una aplicación o sistema operativo específico, contenido en un solo paquete ejecutable.

Servicio de hosteo.- servicio que ofrecen algunas compañías en Internet que consiste en ceder un espacio en sus servidores para subir alojar servicios para que pueda ser accedido en todo momento de forma online.

Servidor de correo.-tipo de servidor que almacena, envía, recibe, encamina y realiza operaciones relacionadas a los correos electrónicos de sus clientes de red.

Servidores.- son proveedores de servicios, incluyendo la WWW (las páginas web), FTP, correo electrónico, los grupos de noticias, etc.

Sistema operativo.- sistema tipo software que controla la computadora y administra los servicios y sus funciones como así también la ejecución de otros programas compatibles con éste. Permite controlar las asignaciones de memoria, ordenar las solicitudes al sistema, controlar los dispositivos de entrada y salida, facilitar la conexión a redes y el manejo de archivos.

SMTP-Protocolo simple de transferencia de correo.-está diseñado para transferir correo confiable y eficaz. Se utiliza ampliamente en instalaciones gubernamentales y educación y también es el estándar utilizado por Internet para la transferencia de correo.

Softphone.- combinación de Software y de Telephone, es un software que hace una simulación de teléfono convencional por computadora. Es decir, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales. Un Softphone es parte de un entorno Voz sobre IP y puede estar basado en el estándar SIP/H.323 o ser privativo.

Software.- es todo programa o aplicación programada para realizar tareas específicas. El software se ejecuta dentro del hardware.

Spam.- es todo aquel correo electrónico que contiene publicidad que no ha sido solicitada por el propietario de la cuenta de e-mail.

Spyware.- software espía, cualquier aplicación informática que recolecta información valiosa de la computadora desde donde está operando. Es un tipo de malware que por lo general se introduce y opera en las PCs sin que el usuario lo advierta.

Storage.- es todo aquel sistema de almacenamiento de información.

Switch.- dispositivo que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI. Un conmutador interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro.

TCP-Protocolo de Control de Transmisión/Protocolo de Internet.-sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red.

Tecnologías de la Información (TI).- es un amplio concepto que abarca todo lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de la información. El concepto se emplea para englobar cualquier tecnología que permite administrar y comunicar información.

TIC.- las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.

URL-Uniform Resource Locator.- Localizador Uniforme de Recursos. Forma de organizar la información en la web. Una URL es una dirección que permite acceder a un archivo o recurso como ser páginas html, php, asp, o archivos gif, jpg, etc. Se trata de una cadena de caracteres que identifica cada recurso disponible en la WWW.

USB-Universal Serial Bus.-puerto de gran velocidad para comunicar computadoras y periféricos. Soporta plug&play y conexión en caliente (hot plugging). Soporta transferencias de 12 Mbps. Un sólo puerto USB permite ser usado para conectar más de 127 dispositivos periféricos como ratones, módems, teclados, impresoras, etc.

Versión beta.- tipo de versión de una aplicación que se encuentra en estado de prueba. Generalmente se identifica con una "b".

Virtualización.- es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución.

VLAN-Virtual LAN.- es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local.

VPN-Red Privada Virtual.- conecta los componentes de una red sobre otra red. VPN logra este objetivo mediante la conexión de los usuarios de distintas redes a través de un túnel que se construye sobre internet o sobre cualquier red pública.

WAN-Wide Area Network.- Red de Área Extensa, es una red de computadoras de gran tamaño, generalmente dispersa en un área metropolitana, a lo largo de un país o incluso a nivel mundial.

Web.- medio de comunicación de texto, gráficos y otros objetos multimedia a través de Internet, es decir, la web es un sistema de hipertexto que utiliza Internet como su mecanismo de transporte.

Windows update.- sistema de actualizaciones utilizada en los sistemas operativos diseñado por Microsoft.

Wins-Servicio de nombres Internet de Windows.- proporciona una base de datos distribuida en la que se registran y consultan asignaciones dinámicas de nombres NetBIOS para los equipos y grupos usados en la red. WINS asigna direcciones IP a los nombres NetBIOS y se diseñó para solucionar los problemas que ocasiona la resolución de nombres NetBIOS en entornos con rutas.

Wireless.- tecnología de acceso a internet de forma inalámbrica.

REFERENCIAS

— [3 PÁG.]3COM, "Firewall", http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c02583789/c02583789.pdf [consultado: 15 de marzo de 2011].

— [5 PÁG.]NIEVES, SALVADOR, "Tecnología Especializada Asociada de México", 2011, http://www.teamnet.com.mx [consultado: 15 de marzo de 2011].

— [8 PÁG.]ANTÓN, Enrique, "Seguridad informática: protección de activos lógicos", abril de 2005, http://estrategiafinanciera.wke.es/noticias_base/seccion/en%20profundidad/seguridad-informática-protección-de-activos-lógicos [consultado: 15 de marzo de 2011].

— [8 PÁG.] "Seguridad Informática", http://www.alegsa.com.ar/ [consultado: 15 de marzo de 2011].

— [9 PÁG.]LÓPEZ B., María Jaquelina y Quezada, R. Cintia, *Fundamentos de la seguridad informática*, México: UNAM, Facultad de Ingenieria,2006.

— [10 PÁG.] BORGHELLO, Cristian, " Políticas de Seguridad ", http://www.segu-info.com.ar/politicas [consultado: 15 de marzo de 2011].

— [11 PÁG.] ESCAMILLA, Terry, *Intrusion Detection: Network Security Beyond the Firewall*: Wiley, 1998.

— [17 PÁG.]PC WORLD, "Proteja su PC", http://www.pcwla.com/pcwla2.nsf/articulos/716E2A826D5D0CF0852572B0006D05C2 [consultado: 15 de marzo de 2011].

— [25 PÁG.]MSEXCHANGE, "Articles&Tutorials", http://www.msexchange.org/ [consultado: 15 de marzo de 2011].

— [25 PÁG.]TECHNET, "Exchange ActiveSync",21 de junio de 2007, http://64.4.11.252/es-es/library/aa995986(EXCHG.65).aspx [consultado: 15 de marzo de 2011].

— [25 PÁG.] TECHNET, "Managing Exchange ActiveSync",13 de junio de 2006, http://technet.microsoft.com/en-us/library/bb124396(EXCHG.80).aspx [consultado: 15 de marzo de 2011].

— [28 PÁG.]STEEL, Chad, *Windows Forensics: The Field Guide for Corporate Computer Investigations*: Wiley, 2006.

— [29 PÁG.]CACHE, Johnny, *Hacking Exposed Wireless*: McGraw-Hill Osborne Media, 2007.

— [31 PÁG.]SYMANTEC, *Symantec Enterprise Firewall*, E.U.A: Symantec, 2004.

— [31 PÁG.] COMPLIANCES FORUM, "Password Security Policy", http://www.compliancesforum.com/hipaa-password-security-policy-templates [consultado: 15 de marzo de 2011].

— [32 PÁG.] MICROSOFT, *Planning, Implementing & Maintaining a Microsoft Windows Server 2003 Active Directory Infraestructure*, E.U.A: Microsoft, 2005.

— [32 PÁG.]MICROSOFT, *Planning, Managing & Maintaining a Microsoft Windows Server 2003 Enviroment*, E.U.A: Microsoft, 2005.

— [37 PÁG.] MICROSOFT, "Directorio Activo de Windows Server 2003", 10 de julio de 2007, http://www.microsoft.com/spain/windowsserver2003/technologies/directory/activedirectory /default.aspx [consultado: 15 de marzo de 2011].

— [37 PÁG.]MICROSOFT, "Guía detallada de los datos de usuario y la configuración de usuario", http://www.microsoft.com/latam/technet/productos/windows/windowsserver2003/usrdata. mspx [consultado: 15 de marzo de 2011].

— [37 PÁG.]TECHNET, "Active Directory Domain Services Requirements, Support, and Topologies", http://technet.microsoft.com/en-us/library/gg398760.aspx [consultado: 15 de marzo de 2011].

— [38 PÁG.]MICROSOFT, “Cómo extender un volumen de datos en Windows Server", 26 de marzo de 2010, http://support.microsoft.com/kb/325590/es [consultado: 15 de marzo de 2011].

— [38 PÁG.]MICROSOFT, *Implementing a Microsoft Windows Server 2003 Network Infraestructure*, E.U.A: Microsoft, 2005.

— [38 PÁG.]TECHNET,"Active DirectoryInfrastructureRequirements", 1 de febrero de 2011, http://technet.microsoft.com/en-us/library/gg412955.aspx [consultado: 15 de marzo de 2011].

— [42 PÁG.] BERMUDA, Raffaeu, "configure Exchange 2003", 8 de agosto de 2009 en línea: http://blog.raffaeu.com/archive/2009/08/08/real-guide-configure-exchange-2003-sp2-and-iphone-3.0-os.aspx [consultado: 15 de marzo de 2011].

— [44 PÁG.] TECHNET, "Guía de planeamiento de la seguridad de las cuentas de administrador",25 de mayo de 2005, http://technet.microsoft.com/es-ar/library/dd578410.aspx [consultado: 15

de marzo de 2011].

— [45 PÁG.] MISTRETTA, Mónica, "Llaman expertos a adoptar estándares mínimos de seguridad", 10 de marzo de 2010, http://www.bsecure.com.mx/enlinea/llaman-expertos-a-adoptar-estandares-minimos-de-seguridad/ [consultado: 15 de marzo de 2011].

— [45 PÁG.] KIOSKEA, "Contraseñas", 16 de octubre de 2008, http://es.kioskea.net/contents/attaques/passwd.php3 [consultado: 15 de marzo de 2011].

— [46 PÁG.]SUTTER, John D., "How to create a 'superpassword'", 20 de agosto de 2010, http://edition.cnn.com/2010/TECH/innovation/08/20/super.passwords/index.html?hpt=Mid#fbid=64Raiat-eVj&wom=false [consultado: 15 de marzo de 2011].

— [46 PÁG.] HASSELL, Jonathan,"How to create a 'superpassword'", http://www.searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1294391,00.html [consultado: 15 de marzo de 2011].

— [47 PÁG.] CARNEGIE MELLON, "How to choose good passwords", http://www.cs.cmu.edu/~help/security/choosing_passwords.html [consultado: 15 de marzo de 2011].

— [53 PÁG.]MICROSOFT, "Safety & Security Center", https://www.microsoft.com/security/pc-security/password-checker.aspx?WT.mc_id=Site_Link [consultado: 15 de marzo de 2011].

— [53 PÁG.]SYMANTEC, *Symantec Gateway Security Appliance 5600*, E.U.A: Symantec, 2005.

— [62 PÁG.]AKERMAN, Richard, "Ports for Internet Services", http://www.chebucto.ns.ca/~rakerman/port-table.html [consultado: 15 de marzo de 2011].

— [62 PÁG.]SYMANTEC, *Symantec Virus Protection and Integrated Client Security Solution*, E.U.A: Symantec, 2005.

— [64 PÁG.]SCAMBRAY, Joel, *Windows Server 2003 Hacking Exposed*: UNAM, McGraw-Hill Osborne Media, 2007.

— [65 PÁG.]TECHNET, "Server Hardening for Windows Server 2003 SP2",27 de agosto de 2007, http://social.technet.microsoft.com/Forums/en/winserversecurity/thread/ea93d8e2-cf3a-4a0d-9e6b-784fb0625774 [consultado: 15 de marzo de 2011].

— [66 PÁG.]APPLIED TRUST ENGINEERING, "Windows Server 2003 Hardening Checklist ", 31 de octubre de 2005, http://www.crswann.com/3 NetworkSupport/WindowsServer2003HardeningChecklist%20v21.pdf [consultado: 15 de marzo de 2011].

— [70 PÁG.]MICROSOFT, "Microsoft Security Bulletin Search", http://www.microsoft.com/technet/security/current.aspx [consultado: 15 de marzo de 2011].

— [105 PÁG.]MICROSOFT, *Implementing Microsoft Internet Security & Acceleration Server*, E.U.A: Microsoft, 2005.

— [105 PÁG.] QUINTERO, Fernando, "Servidor ISA Server", marzo de 2009, http://www.slideshare.net/ces1227/manual-de-isa-server [consultado: 15 de marzo de 2011].

— [125 PÁG.]BRAGG, Roberta, *Hardening Windows Systems*: McGraw-Hill Osborne Media, 2004.

— [126 PÁG.] DANSEGLIO, Mike*, Windows Server 2003 Security Cookbook*: UNAM, O'Reilly Media.

— [126 PÁG.]UNIVERSITY OF TEXAS, "Windows 2003 Server Hardening Checklist", 20 de julio de 2009, http://security.utexas.edu/admin/win2003.html#r23 [consultado: 15 de marzo de 2011].

— [126 PÁG.] WINDOWS SECURITY, "Windows Server 2003 Hardening List", 7 de diciembre de 2004, http://www.windowsecurity.com/articles/Windows-Server-2003-Hardening-List-Part1.html [consultado: 15 de marzo de 2011].

— [127 PÁG.] JONES, Don, *Microsoft Windows Administrator's Automation Toolkit*: Microsoft Press, 2005.

— [145 PÁG.] GABILOS,"El Balance. Activo, Patrimonio Neto y Pasivo", http://www.gabilos.com/cursos/curso_de_contabilidad/5_el_balance_activo_y_pasivo.htm [consultado: 15 de marzo de 2011].

— [145 PÁG.] GÓMEZ RUIZ, Santiago, "Controladores de dominio ", febrero de 2007, http://biblioteca.utec.edu.sv/siab/virtual/articulos_soft_libre/controladores_de_dominio.pdf [consultado: 15 de marzo de 2011].

— [145 PÁG.] RODRÍGUEZ, Marcelo, "Automatización de Procesos de Análisis Forense Informático", 24 junio de 2010, http://www.cert.uy/historico/pdf/autoForensic.pdf [consultado: 15 de marzo de 2011].

— [145 PÁG.]"Concepto de acometida", en línea: http://www.wordreference.com/definicion/acometida [consultado: 15 de marzo de 2011].

— [145 PÁG.]"Concepto de adware", en línea: http://www.pergaminovirtual.com.ar/definicion/Adware.html [consultado: 15 de marzo de 2011].

— [146 PÁG.]"Concepto de benchmark", en línea: http://es.mimi.hu/economia/benchmark.html [consultado: 15 de marzo de 2011].

— [146 PÁG.]"Concepto de bot", en línea: http://www.antivirus.interbusca.com/glosario/BOT.html [consultado: 15 de marzo de 2011].

— [146 PÁG.]"Concepto de bug", en línea: http://www.masadelante.com/faqs/bug [consultado: 15 de marzo de 2011].

— [147 PÁG.]SELVI, José, "Concepto DMZ", 23 de Junio de 2009, http://www.securityartwork.es/author/jselvi/ [consultado: 15 de marzo de 2011].

— [147 PÁG.]TECHNET, "Concepto DHCP", http://technet.microsoft.com/es-es/library/cc780906(WS.10).aspx [consultado: 15 de marzo de 2011].

— [147 PÁG.]TECHNET, "Concepto DomainName System",13 de diciembre de 2010, http://technet.microsoft.com/en-us/library/gg398386.aspx [consultado: 15 de marzo de 2011].

— [148 PÁG.]SEGURIDAD PC, " Concepto Hacker", http://www.seguridadpc.net/hackers.htm [consultado: 15 de marzo de 2011].

— [148 PÁG.]MONTAÑO BADILLA, Ricardo, "Sistema ERP", 10 febrero de 2010, http://www.gestiopolis.com/administracion-estrategia/erp-definicion-funcionamiento-ventajas-desventajas.htm [consultado: 15 de marzo de 2011].

— [152 PÁG.] TECHNET, "Concepto SMTP", 30 de abril de 2006, http://support.microsoft.com/kb/87022/es [consultado: 15 de marzo de 2011].