UVAQ
UNIVERSIDAD VASCO DE QUIROGA
Repositorio Digital Institucional

REPOSITORIO ACADÉMICO DIGITAL INSTITUCIONAL

(Windows 2000 Server): orientado a seguridad y recursos compartidos: alto nivel

Autor: Josué M. Gómez Zavala

Tesina presentada para obtener el título de:
Lic. En Sistemas Computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarra

Este documento está disponible para su consulta en el Repositorio Académico Digital Institucional de la Universidad Vasco de Quiroga, cuyo objetivo es integrar organizar, almacenar, preservar y difundir en formato digital la producción intelectual resultante de la actividad académica, científica e investigadora de los diferentes campus de la universidad, para beneficio de la comunidad universitaria.

Esta iniciativa está a cargo del Centro de Información y Documentación "Dr. Silvio Zavala" que lleva adelante las tareas de gestión y coordinación para la concreción de los objetivos planteados.

Esta Tesis se publica bajo licencia Creative Commons de tipo "Reconocimiento-NoComercial-SinObraDerivada", se permite su consulta siempre y cuando se mantenga el reconocimiento de sus autores, no se haga uso comercial de las obras derivadas.

Esta obra está bajo una licencia de Creative Commons Reconocimiento-NoComercial-SinObraDerivada 3.0 Unported.

UNIVERSIDAD VASCO DE QUIROGA

(Windows 2000 Server) Orientado A Seguridad Y Recursos Compartidos: Alto Nivel

Tesina

Que Para Obtener El Titulo De:
Licenciado En Sistemas Computarizados

Escuela De Sistemas Computarizados
No. De Acuerdo 952006 Clave 16psu0014q

Presenta:
Josué M. Gómez Zavala

Asesor De Tesina:
M.A. Ing. Sergio Francisco Barraza Ibarra

MORELIA, MICH. AGOSTO 2004.

UVAQ
UNIVERSIDAD VASCO DE QUIROGA
Centro de Información y Documentación "Dr. Silvio Zavala"
Campus Santa María

Indice

Capitulo I.....01

Seguridad Informática.....01

Introducción.....01

Antecedentes De La Seguridad Informática.....02

Propósito General.....03

Beneficios Específicos. 03

A Quién Va Dirigido.....03

Capitulo II.....04

Análisis De Riesgos.....04

Que Debemos Proteger Del Sistema.....04

De Que Hay Que Proteger Al Sistema.....06

Cómo Nos Debemos Proteger.....06

Identificación De Recursos.....08

Identificación De Amenazas.....09

Medidas De Protección.....11

Estrategias De Respuesta.....13

Outsourcing.....15

El `Área De Seguridad'.....18

Capitulo III.....22

Protocolos.....22

La Función De Los Protocolos.....22

Cómo Funcionan Los Protocolos.....23

El Equipo Origen.....23

El Equipo De Destino.....23

Protocolos Encaminables.....24

Protocolos En Una Arquitectura Multinivel.....24

Jerarquías De Protocolos.....25

Capitulo IV.....27

El Modelo De Referencia OSI.....27

Una Arquitectura Por Niveles.....28

Relaciones Entre Los Niveles Del Modelo Osi.....28

El Estándar Ieee 802.X.....30

El Modelo Del Proyecto 802.....30

Mejoras Sobre El Modelo Osi.....31

Subnivel De Control De Enlace Lógico (Llc) 33

Subnivel De Control De Acceso Al Medio (Mac) 33

Capitulo V.....34

Protocolo TCP/IP.....34

Estándares TCP/IP.....35

Tcp/Ip Y El Modelo Osi.....36

Capitulo VI.....37

Topologías De Red.....37

Descripción De Topología.....37

Principales Modelos De Topologías.....38

Topología De Bus.....38

Topología De Anillo.....39

Topología De Anillo Doble.....40

Topología En Estrella.....40

Topología En Estrella Extendida.....41

Topología En Árbol.....41

Topología En Malla Completa.....42

Topología De Red Celular.....43

Topología Irregular.....43

Capitulo VII.....44

Windows 2000 Server.....44

Recomendación De Instalar Windows 2000 Server.....44

Instalación De Windows 2000 Server.....45

Características Principales.....45

Rendimiento Superior.....46

Requisitos Del Sistema.....46

Requisitos Mínimos Para Obtener Un Rendimiento Adecuado.....47

Planificación De Las Particiones.....47

Recogida De Información De La Red.....49

Instalación Desde Windows 95/98 Ó Windows NT.....50

Instalación Desde Un Sistema Con Ms-Dos.....51

Instalación Desde Los Discos De Inicio De Instalación De Windows 2000 Ó Desde El Cdrom.....52

Fase Del Programa De Instalación En Modo Texto.....52

Capitulo VIII.....54

Seguridad 2000 Server.....**54**

Kerberos.....54

Lo Básico.....54

Arquitectura De Kerberos.....56

Autenticación.....57

Login.....58

Obtención De Tickets.....59

Petición De Servicio.....59

Problemas De Kerberos.....59

Capitulo IX.....62

Active Directory.....62

Sitios Y Servicios De Active Directory.....62

Conceptos Fundamentales De Active Directory.....63

Estructura Lógica.....66

Creación Del Dominio Raíz (1)..... 71

Creación De Un Nuevo Árbol En Bosque Existente (2) 71

Creación De Un Subdominio (3) 71

Agregar Un Controlador De Dominio En Un Dominio Existente (4) 71

Remoción De Active Directory.....72

Estructura Física.....72

Conclusiones.....74

Glosario.....76

Bibliografía.....77

Capítulo I

Seguridad Informática

Introducción

Finales 1988 muy poca gente tomaba en serio el tema de la seguridad en redes de computadores de propósito general. Mientras que por una parte Internet iba creciendo exponencialmente con redes importantes que se adherían a ella, como BITNET o HEPNET, por otra el auge de la informática de consumo (hasta la década de los ochenta muy poca gente se podía permitir un ordenador y un módem en casa) unido a factores menos técnicos (como la película *Juegos de Guerra*, de 1983) iba produciendo un aumento espectacular en el número de piratas informáticos.

22 de noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso *worm* o gusano de Internet. Miles de ordenadores conectados a la red se vieron inutilizados durante días, y las pérdidas se estiman en millones de dólares. Desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos. Poco después de este incidente, y a la vista de los potenciales peligros que podía entrañar un fallo o un ataque a los sistemas informáticos estadounidenses (en general, a los sistemas de cualquier país) la agencia DARPA creó el CERT un grupo formado en su mayor parte por voluntarios cualificados de la comunidad informática, cuyo objetivo principal es facilitar una respuesta rápida a los problemas de seguridad que afecten a *hosts* de Internet.

Han pasado más de diez años desde la creación del primer CERT, y cada día se hace patente la preocupación por los temas relativos a la seguridad en la red y sus equipos, y también se hace patente la necesidad de esta seguridad.

Hoy en día cualquier aprendiz de pirata puede conectarse a un servidor *web*, descargar un par de programas y ejecutarlos contra un servidor desprotegido... con un poco de mala suerte, esa misma persona puede conseguir un control total sobre un servidor Windows 2000 de varios millones de pesos, probablemente desde su PC con Windows 98 y sin saber nada sobre Windows 2000.

Antecedentes De La Seguridad Informática

Los centros de cómputo han evolucionado desde aquellos cuya infraestructura se asociaba con la instalación de un equipo central, el cual requería de condiciones muy específicas de ambiente, ubicación y mantenimiento, hasta aquellos equipos de cómputo personal, que de acuerdo a su operación y comunicación entre sí, requieren formas específicas de seguridad.

Los primeros equipos, dadas sus características tecnológicas y proceso centralizado de la información, destinaban una parte importante del proyecto de instalación a cubrir lo referente a seguridad de las instalaciones y de la información, así como al establecimiento de un programa de contingencias que permitiera dar continuidad al servicio que se prestaba.

Actualmente se ha generalizado el uso de los equipos de cómputo personales y departamentales (servidores), así como la integración de éstos en redes, que facilitan la consulta e intercambio de información y que por sus características no requieren de instalaciones tan específicas en lo que se refiere a condiciones de clima principalmente pero, por el contrario, son más vulnerables por tener diversos puntos de acceso.

Aunado a ello, la creciente utilización de estos equipos, el incremento de la cultura informática en los usuarios, así como la ampliación y aumento de las unidades administrativas abocadas a actividades informáticas y la facilidad para su acceso y uso, hacen ineludible la implantación de medidas de seguridad, las cuales deben garantizar, en la medida de lo posible, que la infraestructura informática y la información tengan siempre la disponibilidad necesaria.

Propósito General.

Los sistemas informáticos son ya una parte muy importante de un gran número de empresas, y ésta crece cada día. Por esto se tienen que proteger los sistemas delante de las amenazas a las que están expuestos, amenazas que cambian con el tiempo. La seguridad informática es clave tanto para el buen funcionamiento de las empresas, como para la confianza en los sistemas informáticos de los que operan. Son necesarios profesionales capaces de evaluar la seguridad de estos sistemas, de gestionarla, de actualizarla; esta seguridad debe tener en cuenta por parte de todos los que actúan, y se tienen que conocer las herramientas de seguridad necesarias.

Con este Trabajo de Investigación en Seguridad Informática quiero dar una visión global de cómo mejorar la seguridad en los sistemas informáticos, de aplicaciones existentes con este objetivo, y pretende que estos conocimientos sean directamente aplicables en el entorno de trabajo de los asistentes.

Beneficios Específicos.

- Evaluar y mejorar la seguridad del entorno de sistemas informáticos
- Obtener una visión completa y actual de los mecanismos de seguridad informática
- Identificar y dimensionar amenazas a los sistemas informáticos
- Hacer prácticas de configuración y administración de mecanismos de seguridad

A Quien Va Dirigido.

- Administradores de seguridad de sistemas informáticos
- Evaluadores de seguridad de sistemas informáticos
- Administradores de sistemas
- Empresas que quieran crear su propio equipo de respuesta a incidentes
- Titulados en Informática que quieran especializarse en seguridad

Capitulo II

Análisis De Riesgos

En un entorno informático existen una serie de recursos (humanos, técnicos, de infraestructura...) que están expuestos a diferentes tipos de riesgos: los `normales', aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a parte de una organización o a toda la misma, como la inestabilidad política en un país o una región sensible a terremotos. Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que denominamos un **análisis de riesgos**, término que hace referencia al proceso necesario para responder a tres cuestiones básicas sobre nuestra seguridad:

Qué Debemos Proteger Del Sistema

Los tres elementos principales a proteger en cualquier sistema informático son el *software*, el *hardware* y los datos.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

Contra cualquiera de los tres elementos descritos anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como **interrupción** si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una **interceptación** si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una **modificación** si además de conseguir el acceso consigue modificar el objeto; algunos autores consideran un caso especial de la modificación: la **destrucción**, entendiéndola como una

modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una **fabricación** si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el `fabricado'. En la **figura A** se muestran estos tipos de ataque de una forma gráfica.

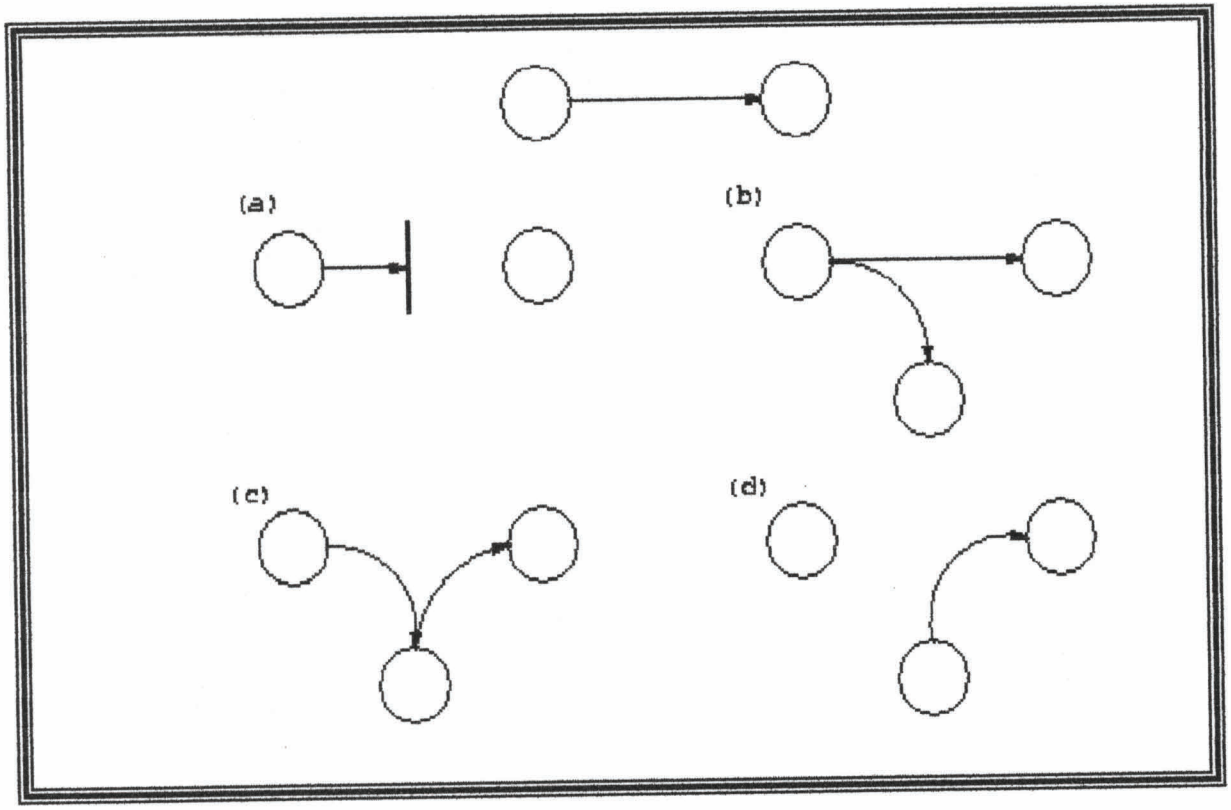


FIGURA A: FLUJO NORMAL ENTRE EMISOR Y RECEPTOR: (a) INTERRUPTOR , (b) INTERCEPTACIÒN, (c) MODIFICACION Y (d) FABRICACIÒN

De Que Hay Que Proteger Al Sistema

En la gran mayoría de publicaciones relativas a la seguridad informática en general, y especialmente en las relativas a seguridad en W2KServer, tarde o temprano se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. Con frecuencia, especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad, se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático. Pero en este trabajo es preferible hablar de `elementos' y no de personas: aunque a veces lo olvidemos, nuestro sistema puede verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo programas, catástrofes naturales o, por qué no, fuerzas extraterrestres; si un usuario pierde un trabajo importante a causa de un ataque, poco le importará que haya sido un intruso, un gusano, un simple error del administrador, o un *alien* que haya abducido un disco duro...

Cómo Nos Debemos Proteger

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar nuestra visión de la seguridad, hemos de hablar de las formas de protección de nuestros sistemas. Cuando hayamos completado este punto, habremos presentado a grandes rasgos los diferentes puntos a tratar en este proyecto.

Para proteger nuestro sistema hemos de realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad se les denomina **mecanismos de seguridad**; son la parte más visible de nuestro sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación. Los mecanismos **de prevención** son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema W2KServer en la red. Por mecanismos **de detección** se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoria como *Tripwire*. Finalmente, los mecanismos **de recuperación** son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el *hardware* adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado **mecanismos de análisis forense**, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

Parece claro que, aunque los tres tipos de mecanismos son importantes para la seguridad de nuestro sistema, hemos de enfatizar en el uso de mecanismos de prevención y de detección; la máxima popular '*más vale prevenir que curar*' se puede aplicar a la seguridad informática: para nosotros, evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y menos comprometedor para el sistema que restaurar el estado tras una penetración de la máquina. Es más, si consiguiéramos un sistema sin vulnerabilidades y cuya política de seguridad se implementara mediante mecanismos de prevención de una forma completa, no necesitaríamos mecanismos de detección o recuperación. Aunque esto es imposible de conseguir en la práctica, será en los mecanismos de detección, y sobre todo en los de prevención, en los que centraremos nuestro trabajo.

Identificación De Recursos

Debemos identificar todos los recursos cuya integridad pueda ser amenazada de cualquier forma; por ejemplo, Dave Curry en *Site Security Handbook:* define básicamente los siguientes:

- **Hardware**
  Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, ordenadores personales, impresoras, unidades de disco, líneas de comunicación, servidores, *routers*...
- **Software**
  Códigos fuente y objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación...
- **Información**
  En ejecución, almacenada en línea, almacenada fuera de línea, en comunicación, bases de datos...
- **Personas**
  Usuarios, operadores...
- **Accesorios**
  Papel, cintas, tóners...

Aparte del recurso en sí (algo tangible, como un *router*) hemos de considerar la visión intangible de cada uno de estos recursos (por ejemplo la capacidad para seguir trabajando sin ese *router*). Es difícil generar estos aspectos intangibles de los recursos, ya que es algo que va a depender de cada organización, su funcionamiento, sus seguros, sus normas...No obstante, siempre hemos de tener en cuenta algunos aspectos comunes: privacidad de los usuarios, imagen pública de la organización, reputación, satisfacción del personal y de los clientes - en el caso de una universidad, de los alumnos -, capacidad de procesamiento ante un fallo...

Con los recursos correctamente identificados se ha de generar una lista final, que ya incluirá todo lo que necesitamos proteger en nuestra organización.

Identificación De Amenazas

Una vez que conocemos los recursos que debemos proteger es la hora de identificar las vulnerabilidades y amenazas que se ciernen contra ellos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

- **Desastres del entorno.**

Dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones...), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

- **Amenazas en el sistema.**

Bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y su *software* que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad...

- **Amenazas en la red.**

Cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, intranets o la propia Internet, y esta interconexión acarrea nuevas - y peligrosas - amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de Internet, o a instalar sistemas de autenticación de usuarios remotos que necesitan acceder a ciertos recursos internos a la organización (como un investigador que conecta desde su casa a través de un módem).

Algo importante a la hora de analizar las amenazas a las que se enfrentan nuestros sistemas es analizar los potenciales tipos de atacantes que pueden intentar violar nuestra seguridad. Es algo normal que a la hora de hablar de atacantes todo el mundo piense en *crackers*, en piratas informáticos mal llamados *hackers*. No obstante, esto no es más que el fruto de la repercusión que en todos los medios tienen estos individuos y sus acciones; en realidad, la inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada. En organismos de I+D estos atacantes suelen ser los propios estudiantes (rara vez el personal), así como piratas externos a la entidad que aprovechan la habitualmente mala protección de los sistemas universitarios para acceder a ellos y conseguir así cierto *status* social dentro de un grupo de piratas. Los conocimientos de estas personas en materias de sistemas operativos, redes o seguridad informática suelen ser muy limitados, y sus actividades no suelen entrañar muchos riesgos a no ser que se utilicen nuestros equipos para atacar a otras organizaciones, en cuyo caso a los posibles problemas legales hay que sumar la mala imagen que nuestras organizaciones adquieren.

No siempre hemos de contemplar a las amenazas como actos intencionados contra nuestro sistema: muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que derrama una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el

borrado accidental de datos o los errores de programación; decir *`no lo hice a propósito'* no ayuda nada en estos casos. Por supuesto, tampoco tenemos que reducirnos a los accesos no autorizados al sistema: un usuario de nuestras máquinas puede intentar conseguir privilegios que no le corresponden, una persona externa a la organización puede lanzar un ataque de negación de servicio contra la misma sin necesidad de conocer ni siquiera un *login* y una contraseña, etc.

Medidas De Protección

Tras identificar todos los recursos que deseamos proteger, así como las posibles vulnerabilidades y amenazas a que nos exponemos y los potenciales atacantes que pueden intentar violar nuestra seguridad, hemos de estudiar cómo proteger nuestros sistemas, sin ofrecer aún implementaciones concretas para protegerlos (esto ya no serían políticas sino mecanismos). Esto implica en primer lugar cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en nuestra organización, aunque por desgracia en muchos lugares no se suelen registrar los incidentes acaecidos. En este caso, y también a la hora de evaluar los daños sobre recursos intangibles, existen diversas aproximaciones como el método Delphi, que básicamente consiste en preguntar a una serie de especialistas de la organización sobre el daño y las pérdidas que cierto problema puede causar; no obstante, la experiencia del administrador en materias de seguridad suele tener aquí la última palabra a la hora de evaluar los impactos de cada amenaza.

La clasificación de riesgos de cara a estudiar medidas de protección suele realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; se trata principalmente de no gastar más dinero en una implementación para proteger un recurso de lo que vale dicho recurso o de lo que nos costaría recuperarnos de un daño en él o de su pérdida total. Por ejemplo, podemos seguir un análisis similar en algunos aspectos al problema de la mochila: llamamos al riesgo de perder un recurso *i* (a la probabilidad de que se produzca un ataque), y le

asignamos un valor de 0 a 10 (valores más altos implican más probabilidad); de la misma forma, definimos también de 0 a 10 la importancia de cada recurso, siendo 10 la importancia más alta. La evaluación del riesgo es entonces el producto de ambos valores, llamado peso o riesgo evaluado de un recurso, y medido en dinero perdido por unidad de tiempo (generalmente, por año): De esta forma podemos utilizar hojas de trabajo en las que, para cada recurso, se muestre su nombre y el número asignado, así como los tres valores anteriores. Evidentemente, los recursos que presenten un riesgo evaluado mayor serán los que más medidas de protección deben poseer, ya que esto significa que es probable que sean atacados, y que además el ataque puede causar pérdidas importantes. Es especialmente importante un grupo de riesgos denominados *inaceptables*, aquellos cuyo peso supera un cierto umbral; se trata de problemas que no nos podemos permitir en nuestros sistemas, por lo que su prevención es crucial para que todo funcione correctamente.

Una vez que conocemos el riesgo evaluado de cada recurso es necesario efectuar lo que se llama el análisis de costos y beneficios. Básicamente consiste en comparar el costo asociado a cada problema (calculado anteriormente,) con el costo de prevenir dicho problema. El cálculo de este último no suele ser complejo si conocemos las posibles medidas de prevención que tenemos a nuestra disposición: por ejemplo, para saber lo que nos cuesta prevenir los efectos de un incendio en la sala de operaciones, no tenemos más que consultar los precios de sistemas de extinción de fuego, o para saber lo que nos cuesta proteger nuestra red sólo hemos de ver los precios de productos como *routers* que bloqueen paquetes o cortafuegos completos. No sólo hemos de tener en cuenta el costo de cierta protección, sino también lo que nos puede suponer su implementación y su mantenimiento; en muchos casos existen soluciones gratuitas para prevenir ciertas amenazas, pero estas soluciones tienen un coste asociado relativo a la dificultad de hacerlas funcionar correctamente de una forma continúa en el tiempo, por ejemplo dedicando a un empleado a su implementación y mantenimiento.

Cuando ya hemos realizado este análisis no tenemos más que presentar nuestras cuentas a los responsables de la organización (o adecuarlas al presupuesto que un departamento destina a materias de seguridad), siempre teniendo en cuenta que el gasto de proteger un recurso ante una amenaza ha

de ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad. Hemos de tener siempre presente que los riesgos se pueden minimizar, pero **nunca** eliminarlos completamente, por lo que será recomendable planificar no sólo la prevención ante de un problema sino también la recuperación si el mismo se produce; se suele hablar de medidas **proactivas** (aquellas que se toman para prevenir un problema) y medidas **reactivas** (aquellas que se toman cuando el daño se produce, para minimizar sus efectos).

Estrategias De Respuesta

Qué hacer cuando nuestra política de seguridad ha sido violada? La respuesta a esta pregunta depende completamente del tipo de violación que se haya producido, de su gravedad, de quién la haya provocado, de su intención...Si se trata de accidentes o de problemas poco importantes suele ser suficiente con una reprimenda verbal o una advertencia; si ha sido un hecho provocado, quizás es conveniente emprender acciones algo más convincentes, como la clausura de las cuentas de forma temporal o pequeñas sanciones administrativas. En el caso de problemas graves que hayan sido intencionados interesará emprender acciones más duras, como cargos legales o sanciones administrativas firmes (por ejemplo, la expulsión de una organización).

Una gran limitación que nos va a afectar mucho es la situación de la persona o personas causantes de la violación con respecto a la organización que la ha sufrido. En estos casos se suele diferenciar entre usuarios internos o locales, que son aquellos pertenecientes a la propia organización, y externos, los que no están relacionados directamente con la misma; las diferencias entre ellos son los límites de red, los administrativos, los legales o los políticos. Evidentemente es mucho más fácil buscar responsabilidades ante una violación de la seguridad entre los usuarios internos, ya sea contra la propia organización o contra otra, pero utilizando los recursos de la nuestra; cuando estos casos se dan en redes de I+D, generalmente ni siquiera es necesario llevar el caso ante la justicia, basta con la aplicación de ciertas normas sobre el usuario problemático (desde una sanción hasta la expulsión o despido de la organización).

Existen dos estrategias de respuesta ante un incidente de seguridad

- **Proteger y proceder.**
- **Perseguir y procesar.**

La primera de estas estrategias, proteger y proceder, se suele aplicar cuando la organización es muy vulnerable o el nivel de los atacantes es elevado; la filosofía es proteger de manera inmediata la red y los sistemas y restaurar su estado normal, de forma que los usuarios puedan seguir trabajando normalmente. Seguramente será necesario interferir de forma activa las acciones del intruso para evitar más accesos, y analizar el daño causado. La principal desventaja de esta estrategia es que el atacante se da cuenta rápidamente de que ha sido descubierto, y puede emprender acciones para ser identificado, lo que incluso conduce al borrado de *logs* o de sistemas de ficheros completos; incluso puede cambiar su estrategia de ataque a un nuevo método, y seguir comprometiendo al sistema. Sin embargo, esta estrategia también presenta una parte positiva: el bajo nivel de conocimientos de los atacantes en sistemas habituales hace que en muchas ocasiones se limiten a abandonar su ataque y dedicarse a probar suerte con otros sistemas menos protegidos en otras organizaciones.

La segunda estrategia de respuesta, perseguir y procesar, adopta la filosofía de permitir al atacante proseguir sus actividades, pero de forma controlada y observada por los administradores, de la forma más discreta posible. Con esto, se intentan guardar pruebas para ser utilizadas en la segunda parte de la estrategia, la de acusación y procesamiento del atacante (ya sea ante la justicia o ante los responsables de la organización, si se trata de usuarios internos). Evidentemente corremos el peligro de que el intruso descubra su monitorización y destruya completamente el sistema, así como que nuestros resultados no se tengan en cuenta ante un tribunal debido a las artimañas legales que algunos abogados aprovechan; la parte positiva de esta estrategia es, aparte de la recolección de pruebas, que permite a los responsables conocer las actividades del atacante, qué vulnerabilidades de nuestra organización ha aprovechado para atacarla, cómo se comporta una vez dentro, etc. De esta forma podemos aprovechar el ataque para reforzar los puntos débiles de nuestros sistemas.

A nadie se le escapan los enormes peligros que entraña el permitir a un atacante proseguir con sus actividades dentro de las máquinas; por muy controladas que estén, en cualquier momento casi nada puede evitar que la persona se sienta vigilada, se ponga nerviosa y destruya completamente nuestros datos. Una forma de monitorizar sus actividades sin comprometer excesivamente nuestra integridad es mediante un proceso denominado *jailing* o encarcelamiento: la idea es construir un sistema que simule al real, pero donde no se encuentren datos importantes, y que permita observar al atacante sin poner en peligro los sistemas reales. Para ello se utiliza una máquina, denominada **sistema de sacrificio**, que es donde el atacante realmente trabaja, y un segundo sistema, denominado **de observación**, conectado al anterior y que permite analizar todo lo que esa persona está llevando a cabo. De esta forma conseguimos que el atacante piense que su intrusión ha tenido éxito y continúe con ella mientras lo monitorizamos y recopilamos pruebas para presentar en una posible demanda o acusación. Si deseamos construir una cárcel es necesario que dispongamos de unos conocimientos medios o elevados de programación de sistemas; utilidades como chroot() nos pueden ser de gran ayuda, así como *software* de simulación como *Deception Tookit (DTK)*, que simula el éxito de un ataque ante el pirata que lo lanza, pero que realmente nos está informando del intento de violación producido.

Sin importar la estrategia adoptada ante un ataque, siempre es recomendable ponerse en contacto con entidades externas a nuestra organización, incluyendo por ejemplo fuerzas de seguridad, gabinetes jurídicos o equipos de expertos en seguridad informática.

Outsourcing

Cada vez es más habitual que las empresas contraten los servicios de seguridad de una compañía externa, especializada en la materia, y que permita olvidarse - relativamente, como veremos después - al personal de esa empresa de los aspectos técnicos y organizativos de la seguridad, para poder centrarse así en su línea de negocio correspondiente; esta política es lo que se conoce como *outsourcing* y se intenta traducir por `externalización', aplicado en nuestro caso a la seguridad corporativa. A los que somos puramente técnicos muchas veces se nos olvida que la seguridad en sí misma no es ningún fin, sino una herramienta al servicio de los negocios, y por tanto nuestros esfuerzos

han de ir orientados a proteger el `patrimonio' (humano, tecnológico, económico...) de quien contrata nuestros servicios: al director de una gran firma probablemente le importe muy poco que hayamos implantado en sus instalaciones el mejor cortafuegos del mercado junto a un fabuloso sistema distribuido de detección de intrusos si después un atacante puede entrar con toda facilidad en la sala de máquinas y robar varias cintas de *backup* con toda la información crítica de esa compañía; y si esto sucede, simplemente hemos hecho mal nuestro trabajo.

Por qué va a querer una empresa determinada que personas ajenas a la misma gestionen su seguridad? Al fin y al cabo, este manual habla de la protección de muchos activos de la compañía, y encomendar esa tarea tan crítica a un tercero, de quien en principio - ni en final - no tenemos porqué confiar, no parece a primera vista una buena idea...Existen diferentes motivos para llegar a externalizar nuestra seguridad; por un lado, como hemos comentado, un *outsourcing* permite a la empresa que lo contrata despreocuparse relativamente de su seguridad para centrarse en sus líneas de negocio. Además, al contratar a personal especializado - al menos en principio - en la seguridad se consigue - también en principio - un nivel mayor de protección, tanto por el factor humano (el contratado ha de tener gente con un alto nivel en diferentes materias de seguridad para poder ofrecer correctamente sus servicios) como técnico (dispondrá también de productos y sistemas más específicos, algo de lo que probablemente el contratante no puede disponer tan fácilmente). Teóricamente, estamos reduciendo riesgos a la vez que reducimos costes, por lo que parece que nos encontramos ante la panacea de la seguridad.

Desgraciadamente, el mundo real no es tan bonito como lo se puede escribir sobre un papel; el *outsourcing* presenta *a priori* graves inconvenientes, y quizás el más importante sea el que ya hemos adelantado: dejar toda nuestra seguridad en manos de desconocidos, por muy buenas referencias que podamos tener de ellos. Muchas empresas dedicadas a ofrecer servicios de gestión externa de seguridad están formadas por ex-piratas, o cual no deja de ser contradictorio: estamos dejando al cuidado de nuestro rebaño a lobos, o cuanto menos ex-lobos, algo que plantea, o debe plantear, ciertas cuestiones éticas. No voy a expresar de nuevo mi punto de vista (que no deja de ser una mera opinión) acerca de

los piratas, porque creo que ya ha quedado suficientemente claro en diferentes puntos de este documento, así que cada cual actúe como su conciencia o sus directivos le indiquen. Por supuesto, tampoco quiero meter a todo este tipo de compañías en un mismo saco, porque por lógica habrá de todo, ni entrar ahora a discutir acerca de si para saber defender un entorno hay que saber atacarlo, porque una cosa es saber atacar (algo que se puede aprender en sistemas autorizados, o en nuestro propio laboratorio, sin afectar a ningún tercero) y otra defender que sólo un antiguo pirata es capaz de proteger correctamente un sistema.

Aparte de este `ligero' inconveniente del *Outsourcing*, tenemos otros tipos de problemas a tener también en cuenta; uno de ellos es justamente el límite de uno de los beneficios de esta política: ya que la externalización permite a una empresa `despreocuparse' de su seguridad, podemos encontrar el caso - nada extraño - de una excesiva `despreocupación'. Actualmente, el abanico de servicios que ofrece cualquier consultora de seguridad suele abarcar desde auditorias puntuales hasta una delegación total del servicio pasando por todo tipo de soluciones intermedias, y lo que justifica la elección de un modelo u otro es un simple análisis de riesgos: el riesgo de la solución externalizada ha de ser menor que el nivel de riesgo existente si se gestiona la seguridad de forma interna. En cualquier caso, al externalizar se suele introducir una cierta pérdida de control directo sobre algunos recursos de la compañía, y cuando esa pérdida supera un umbral nos encontramos ante un grave problema; en **ningún** caso es recomendable un desentendimiento total de los servicios externalizados, y el contacto e intercambio de información entre las dos organizaciones (la contratante y la contratada) han de ser continuos y fluidos.

Cuanto más alejada de las nuevas tecnologías se encuentre la línea de negocio de una determinada empresa, más recomendable suele ser para la misma adoptar una solución de *outsourcing*; esto es evidente: una empresa frutera, independientemente de lo grande o pequeña que sea, pero perteneciente a un área no relacionada con nuevas tecnologías, rara vez va a disponer de los mismos recursos humanos y técnicos para destinar exclusivamente a seguridad que una empresa de telecomunicaciones o informática. Es habitual - y así debe ser - que el nivel de externalización sea mayor conforme la empresa contratante se aleje del mundo de las nuevas tecnologías, contemplando un

amplio abanico que abarca desde la gestión de elementos concretos de protección (como un *firewall* corporativo) o auditorias y *tests* de penetración puntuales hasta soluciones de externalización total; en cualquier caso, es necesario insistir de nuevo en el error de `despreocuparse' demasiado de la gestión de nuestra seguridad: incluso a esa empresa frutera que acabamos de comentar le interesará, o al menos así debería ser, recibir como poco un informe mensual donde en unas pocas hojas, y sin entrar en aspectos demasiado técnicos, se le mantenga al día de cualquier aspecto relevante que afecte a su seguridad.

Qué áreas de nuestra seguridad conviene externalizar? Evidentemente, no existe una respuesta universal a esta pregunta. Existen áreas que por su delicadez o criticidad no conviene casi nunca dejar en manos de terceros, como es el caso de la realización y verificación de *backups*: todos hemos escuchado historias graciosas - o terribles, según en que lado estemos - relacionadas con errores en las copias de seguridad, como ejecutar la simulación de copia en lugar de una copia real para finalizar más rápidamente el proceso de *backup*. No obstante, elementos importantes pero no críticos *a priori*, como los *tests* de penetración, de visibilidad o las auditorias de vulnerabilidades, que habitualmente se suelen externalizar, ya que incluso existen empresas de seguridad especializadas en este tipo de acciones. Otro ejemplo de área a externalizar puede ser la gestión de los cortafuegos corporativos, trabajo que en demasiadas ocasiones recae sobre el área de Seguridad propia y que como veremos en el próximo punto no debería ser así. En definitiva, no podemos dar un listado donde se indiquen por orden las prioridades de externalización, ya que es algo que depende completamente de cada compañía y entorno; ha de ser el personal de la propia compañía, asesorado por consultores de seguridad y por abogados (recordemos que la LOPD está ahí), quien decida qué y de qué forma gestionar en *Outsourcing*.

El `Área De Seguridad'

Casi cualquier mediana o pequeña empresa posee actualmente lo que se viene a llamar el `Área de Seguridad', formada pocas veces a partir de gente que haya sido incorporada a la plantilla a tal efecto, y muchas a partir del reciclaje de personal de otras áreas de la corporación, típicamente las

de Sistemas o Comunicaciones. En este punto vamos a hablar brevemente de esta área y su posición corporativa, haciendo referencia tanto a sus funciones teóricas como a sus problemas de definición dentro del organigrama de la organización.

Cuál es la función de este área? Realmente, mientras que todo el personal sabe cual es el cometido de la gente de Desarrollo, Sistemas o Bases de Datos, el del área de Seguridad no suele estar definido de una forma clara: al tratarse en muchos casos, como acabamos de comentar, de personal `reciclado' de otras áreas, se trabaja mucho en aspectos de seguridad - para eso se suele crear, evidentemente -, pero también se acaba realizando funciones que corresponden a otras áreas; esto es especialmente preocupante con respecto a Sistemas, ya que en muchas ocasiones el personal de Seguridad trabaja `demasiado cerca' de esta otra área, llegando a realizar tareas puramente relacionadas con Sistemas, como la gestión de los cortafuegos (y no me refiriéndome a la definición de políticas ni nada parecido, sino únicamente al manejo del mismo). Con lo cual se vicia el área de Seguridad centrándose únicamente en aspectos técnicos pero descuidando otros que son iguales o más importantes. Por si esto fuera poco, existe una serie de funciones en conflicto a la hora de gestionar la seguridad corporativa, típicamente la del administrador de seguridad frente a la del administrador de sistemas, de bases de datos, o incluso frente al operador de sistemas y los desarrolladores.

Teóricamente, el área de Seguridad ha de estar correctamente definida y ser independiente de cualquier otra de la compañía, y por supuesto de la dirección de la misma: aunque en la práctica sea casi imposible conseguirlo, no podemos definir una política de obligado cumplimiento para todos los trabajadores excepto para nuestros jefes. Evidentemente, ha de contar con el apoyo total de la dirección de la entidad, que debe estudiar, aprobar y respaldar permanentemente, y de forma anticipada, las decisiones de seguridad que el área decida llevar a cabo (siempre dentro de unos límites, está claro...).

El trabajo del área debe ser más normativo que técnico: no podemos dedicar al personal de la misma a cambiar contraseñas de usuarios o a gestionar (entendido por `manejar') los cortafuegos

corporativos, sino que el área de Seguridad debe definir políticas e implantar mecanismos que obliguen a su cumplimiento, o cuanto menos que avisen a quien corresponda en caso de que una norma no se cumpla. Técnicamente esto no es siempre posible, ya que ni todos los sistemas ni todas las aplicaciones utilizadas tienen porqué ofrecer mecanismos que nos ayuden en nuestra seguridad, pero cuando lo sea es función del área bien su implantación o bien su auditoria (si es implantado por otro área). Si una determinada aplicación no soporta las exigencias definidas en la política de seguridad, pero aún así es imprescindible su uso, el área de Seguridad debe recordar que el cumplimiento de la normativa es igualmente obligatorio; al oír esto, mucha gente puede poner el grito en el cielo: en realidad, si el programa no cumple las especificaciones del área de Seguridad, lo lógico sería prohibir su uso, pero funcionalmente esto no es siempre (realmente, casi nunca) posible: no tenemos más que pensar en una aplicación corporativa que venga gestionando desde hace años las incidencias de la organización, y que evidentemente la dirección no va a sustituir por otra `sólo' por que el área de Seguridad lo indique. Si nuestra política marca que la longitud de clave mínima es de seis caracteres, pero esta aplicación - recordemos, vital para el buen funcionamiento de la organización - acepta contraseñas de cuatro, el usuario **no debe** poner estas claves tan cortas por mucho que la aplicación las acepte; si lo hace está violando la política de seguridad definida, y el hecho de que el programa le deje hacerlo no es ninguna excusa. La política es en este sentido algo similar al código de circulación: no debemos sobrepasar los límites de velocidad, aunque las características mecánicas de nuestro coche nos permitan hacerlo y aunque no siempre tengamos un policía detrás que nos esté vigilando.

Aparte de la definición de políticas y la implantación (o al menos la auditoria) de mecanismos, es tarea del área de Seguridad la realización de análisis de riesgos; aunque el primero sea con diferencia el más costoso, una vez hecho este el resto no suele implicar mucha dificultad. Por supuesto, todo esto ha de ser continuo en el tiempo - para entender porqué, no tenemos más que fijarnos en lo rápido que cambia cualquier aspecto relacionado con las nuevas tecnologías - y permanente realimentado, de forma que la política de seguridad puede modificar el análisis de riesgos y viceversa. Asociados a los riesgos se definen planes de contingencia para recuperar el servicio en caso de que se materialice un problema determinado; esta documentación ha de ser perfectamente conocida por todo el personal al

que involucra, y debe contemplar desde los riesgos más bajos hasta los de nivel más elevado o incluso las catástrofes: qué pasaría si mañana nuestro CPU se incendia o el edificio se derrumba?, cuánto tardaríamos en recuperar el servicio?, sabría cada persona qué hacer en este caso?...

Capitulo III

Protocolos

La Función De Los Protocolos

Los protocolos son reglas y procedimientos para la comunicación. El término «protocolo» se utiliza en distintos contextos. Por ejemplo, los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma forma se aplican las reglas del protocolo al entorno informático. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.

Cuando piense en protocolos de red recuerde estos tres puntos:

Existen muchos protocolos. A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.

Algunos protocolos sólo trabajan en ciertos niveles OSI. El nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red (NIC) y salgan al cable de la red.

Los protocolos también puede trabajar juntos en una jerarquía o conjunto de protocolos. Al igual que una red incorpora funciones a cada uno de los niveles del modelo OSI, distintos protocolos también trabajan juntos a distintos niveles en la jerarquía de protocolos. Los niveles de la jerarquía de protocolos se corresponden con los niveles del modelo OSI. Por ejemplo, el nivel de aplicación del protocolo TCP/IP se corresponde con el nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

Cómo Funcionan Los Protocolos

La operación técnica en la que los datos son transmitidos a través de la red se puede dividir en dos pasos discretos, sistemáticos. A cada paso se realizan ciertas acciones que no se pueden realizar en otro paso. Cada paso incluye sus propias reglas y procedimientos, o protocolo.

Los pasos del protocolo se tienen que llevar a cabo en un orden apropiado y que sea el mismo en cada uno de los equipos de la red. En el equipo origen, estos pasos se tienen que llevar a cabo de arriba hacia abajo. En el equipo de destino, estos pasos se tienen que llevar a cabo de abajo hacia arriba.

El Equipo Origen

Los protocolos en el equipo origen:

1. Se dividen en secciones más pequeñas, denominadas paquetes.
2. Se añade a los paquetes información sobre la dirección, de forma que el equipo de destino pueda determinar si los datos le pertenecen.
3. Prepara los datos para transmitirlos a través de la NIC y enviarlos a través del cable de la red.

El equipo de destino

Los protocolos en el equipo de destino constan de la misma serie de pasos, pero en sentido inverso.

1. Toma los paquetes de datos del cable y los introduce en el equipo a través de la NIC.
2. Extrae de los paquetes de datos toda la información transmitida eliminando la información añadida por el equipo origen.
3. Copia los datos de los paquetes en un búfer para reorganizarlos enviarlos a la aplicación.

Los equipos origen y destino necesitan realizar cada paso de la misma forma para que los datos tengan la misma estructura al recibirse que cuando se enviaron.

Protocolos Encaminables

Hasta mediados de los ochenta, la mayoría de las redes de área local (LAN) estaban aisladas. Una LAN servía a un departamento o a una compañía y rara vez se conectaba a entornos más grandes. Sin embargo, a medida que maduraba la tecnología LAN, y la comunicación de los datos necesitaba la expansión de los negocios, las LAN evolucionaron, haciéndose componentes de redes de comunicaciones más grandes en las que las LAN podían hablar entre sí.

Los datos se envían de una LAN a otra a lo largo de varios caminos disponibles, es decir, se *encaminan*. A los protocolos que permiten la comunicación LAN a LAN se les conoce como *protocolos encaminables*. Debido a que los protocolos encaminables se pueden utilizar para unir varias LAN y crear entornos de red de área extensa, han tomado gran importancia.

Protocolos En Una Arquitectura Multinivel

En una red, tienen que trabajar juntos varios protocolos. Al trabajar juntos, aseguran que los datos se preparan correctamente, se transfieran al destino correspondiente y se reciban de forma apropiada.

El trabajo de los distintos protocolos tiene que estar coordinado de forma que no se produzcan conflictos o se realicen tareas incompletas. Los resultados de esta coordinación se conocen como *trabajo en niveles*.

Jerarquías De Protocolos

Una jerarquía de protocolos es una combinación de protocolos. Cada nivel de la jerarquía especifica un protocolo diferente para la gestión de una función o de un subsistema del proceso de

11000 11000 11000 11000 11000 11000 11000 11000 11000 11000

comunicación. Cada nivel tiene su propio conjunto de reglas. Los protocolos definen las reglas para cada nivel en el modelo OSI:

Nivel de aplicación	Inicia o acepta una petición
Nivel de presentación	Añade información de formato, presentación y cifrado al paquete de datos
Nivel de sesión	Añade información del flujo de tráfico para determinar cuándo se envía el paquete
Nivel de transporte	Añade información para el control de errores
Nivel de red	Se añade información de dirección y secuencia al paquete
Nivel de enlace de datos	Añade información de comprobación de envío y prepara los datos para que vayan a la conexión física
Nivel físico	El paquete se envía como una secuencia de bits

Los niveles inferiores en el modelo OSI especifican cómo pueden conectar los fabricantes sus productos a los productos de otros fabricantes, por ejemplo, utilizando NIC de varios fabricantes en la misma LAN. Cuando utilicen los mismos protocolos, pueden enviar y recibir datos entre sí. Los niveles superiores especifican las reglas para dirigir las sesiones de comunicación (el tiempo en el que dos equipos mantienen una conexión) y la interpretación de aplicaciones. A medida que aumenta el nivel de la jerarquía, aumenta la sofisticación de las tareas asociadas a los protocolos.

La actividad de una red incluye el envío de datos de un equipo a otro. Este proceso complejo se puede dividir en tareas secuénciales discretas. El equipo emisor debe:

1. Reconocer los datos.
2. Dividir los datos en porciones manejables.

3. Añadir información a cada porción de datos para determinar la ubicación de los datos y para identificar al receptor.
4. Añadir información de temporización y verificación de errores.
5. Colocar los datos en la red y enviarlos por su ruta.

El software de cliente de red trabaja a muchos niveles diferentes dentro de los equipos emisores y receptores. Cada uno de estos niveles, o tareas, es gestionado por uno o más protocolos. Estos protocolos, o reglas de comportamiento, son especificaciones estándar para dar formato a los datos y transferirlos. Cuando los equipos emisores y receptores siguen los mismos protocolos se asegura la comunicación. Debido a esta estructura en niveles, a menudo es referido como pila del protocolo.

El modelo de referencia de Interconexión de sistemas abiertos OSI. (Manteniendo estándares, es posible la comunicación hardware-software diversos)

Con el rápido crecimiento del hardware y el software de red, se hizo necesario que los protocolos estándar pudieran permitir la comunicación entre hardware y software de distintos vendedores. Como respuesta, se desarrollaron dos conjuntos primarios de estándares: el modelo OSI y una modificación de ese estándar llamado Project 802.

Capitulo IV

El Modelo De Referencia OSI

En 1978, ISO divulgó un conjunto de especificaciones que describían la arquitectura de red para la conexión de dispositivos diferentes. El documento original se aplicó a sistemas que eran abiertos entre sí, debido a que todos ellos podían utilizar los mismos protocolos y estándares para intercambiar información.

En 1984, la ISO presentó una revisión de este modelo y lo llamó modelo de referencia de Interconexión de Sistemas Abiertos (OSI) que se ha convertido en un estándar internacional y se utiliza como guía para las redes.

El modelo OSI es la guía mejor conocida y más ampliamente utilizada para la visualización de entornos de red. Los fabricantes se ajustan al modelo OSI cuando diseñan sus productos para red. Éste ofrece una descripción del funcionamiento conjunto de hardware y software de red por niveles para posibilitar las comunicaciones. El modelo también ayuda a localizar problemas proporcionando un marco de referencia que describe el supuesto funcionamiento de los componentes.

Una Arquitectura Por Niveles

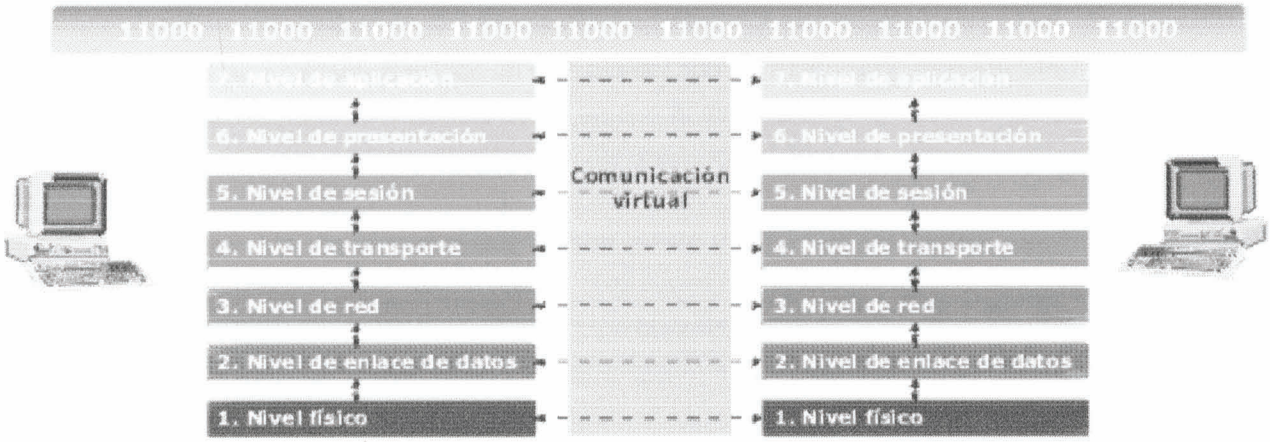
La arquitectura del modelo de referencia OSI divide la comunicación en red en siete niveles. Cada nivel cubre diferentes actividades, equipos o protocolos de red. El modelo OSI define cómo se comunica y trabaja cada nivel con los niveles inmediatamente superior e inferior. Por ejemplo, el nivel de sesión se comunica y trabaja con los niveles de presentación y de transporte.

Cada nivel proporciona algún servicio o acción que prepara los datos para entregarlos a través de la red a otro equipo. Los niveles inferiores (1 y 2) definen el medio físico de la red y las tareas relacionadas, como la colocación de los bits de datos sobre las placas de red NIC y el cable. Los niveles superiores definen la forma en que las aplicaciones acceden a los servicios de comunicación. Cuanto más alto es el nivel, más compleja es su tarea.

Los niveles están separados entre sí por fronteras llamadas interfaces. Todas las demandas se pasan desde un nivel, a través de esta interfaz, hacia el siguiente. Cada nivel se basa en los estándares y actividades del nivel inferior.

Relaciones Entre Los Niveles Del Modelo OSI

Cada nivel proporciona servicios al nivel inmediatamente superior y lo protege de los detalles de implementación de los servicios de los niveles inferiores. Al mismo tiempo, cada nivel parece estar en comunicación directa con su nivel asociado del otro equipo. Esto proporciona una comunicación lógica, o virtual, entre niveles análogos. En realidad, la comunicación real entre niveles adyacentes tiene lugar sólo en un equipo. En cada nivel, el software implementa las funciones de red de acuerdo con un conjunto de protocolos.



Antes de pasar los datos de un nivel a otro, se dividen en paquetes, o unidades de información, que se transmiten como un todo desde un dispositivo a otro sobre una red. La red pasa un paquete de un nivel software a otro en el mismo orden de los niveles. En cada nivel, el software agrega información de formato o direccionamiento al paquete, que es necesaria para la correcta transmisión del paquete a través de la red.

En el extremo receptor, el paquete pasa a través de los niveles en orden inverso. Una utilidad software en cada nivel lee la información del paquete, la elimina y pasa el paquete hacia el siguiente nivel superior. Cuando el paquete alcanza el nivel de aplicación, la información de direccionamiento ha sido eliminada y el paquete se encuentra en su formato original, con lo que es legible por el receptor.

Con la excepción del nivel más bajo del modelo de redes OSI, ningún nivel puede pasar información directamente a su homólogo del otro equipo. En su lugar, la información del equipo emisor debe ir descendiendo por todos los niveles hasta alcanzar el nivel físico. En ese momento, la información se desplaza a través del cable de red hacia el equipo receptor y asciende por sus niveles hasta que alcanza el nivel correspondiente. Por ejemplo, cuando el nivel de red envía información desde el equipo A, la información desciende hacia los niveles de enlace de datos y físico de la parte emisora, atraviesa el cable y asciende los niveles físico y de enlace de datos de la parte receptora hasta su destino final en el nivel de red del equipo B.

En un entorno cliente/servidor, un ejemplo del tipo de información enviada desde el nivel de red de un equipo A, hacia el nivel de red de un equipo B, debería ser una dirección de red, posiblemente con alguna información de verificación de errores agregada al paquete.

La interacción entre niveles adyacentes ocurre a través de una interfaz. La interfaz define los servicios ofrecidos por el nivel inferior para el nivel superior y, lo que es más, define cómo se accede a dichos servicios. Además, cada nivel de un equipo aparenta estar en comunicación directa con el mismo nivel de otro equipo.

El Estándar IEEE 802.X

Los dos niveles inferiores del modelo OSI están relacionados con el hardware: la tarjeta de red y el cableado de la red. Para avanzar más en el refinamiento de los requerimientos de hardware que operan dentro de estos niveles, el Instituto de Ingenieros Eléctricos y Electrónicos IEEE ha desarrollado mejoras específicas para diferentes tarjetas de red y cableado. De forma colectiva, estos refinamientos se conocen como proyecto 802.

El Modelo Del Proyecto 802

Cuando comenzaron a aparecer las primeras redes de área local LAN como herramientas potenciales de empresa a finales de los setenta, el IEEE observó que era necesario definir ciertos estándares para redes de área local. Para conseguir esta tarea, el IEEE emprendió lo que se conoce como proyecto 802, debido al año y al mes de comienzo (febrero de 1980).

Aunque los estándares IEEE 802 publicados realmente son anteriores a los estándares ISO, ambos estaban en desarrollo aproximadamente al mismo tiempo y compartían información que concluyó en la creación de dos modelos compatibles.

El proyecto 802 definió estándares de redes para las componentes físicas de una red (la tarjeta de red y el cableado) que se corresponden con los niveles físicos y de enlace de datos del modelo OSI.

Las Especificaciones 802 Definen Estándares Para:

Tarjetas de red (NIC).
Componentes de redes de área global WAN
Componentes utilizadas para crear redes de cable coaxial y de par trenzado.

Las especificaciones 802 definen la forma en que las tarjetas de red acceden y transfieren datos sobre el medio físico. Éstas incluyen conexión, mantenimiento y desconexión de dispositivos de red.

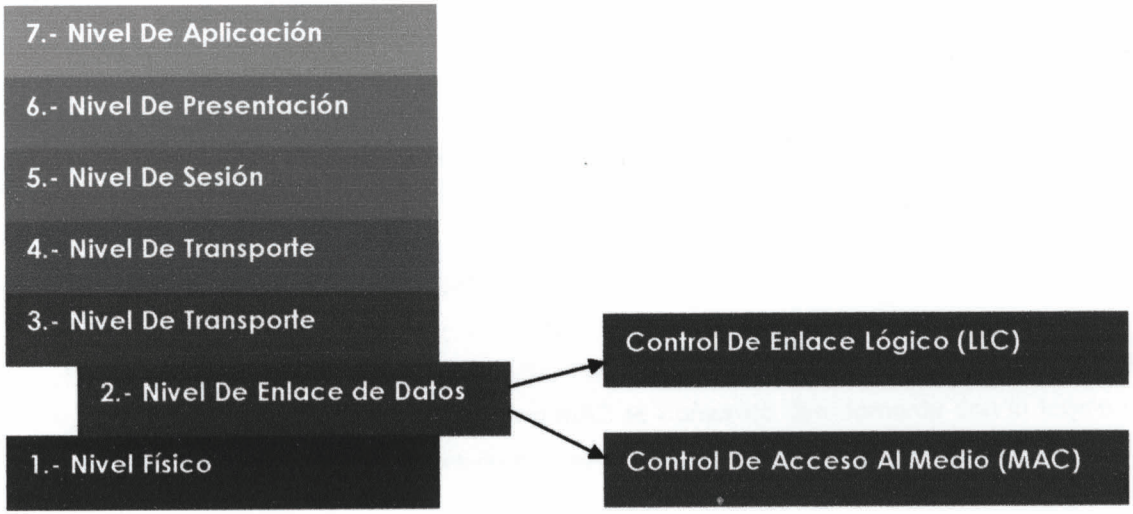
La selección del protocolo a ejecutar en el nivel de enlace de datos es la decisión más importante que se debe tomar cuando se diseña una red de área local (LAN). Este protocolo define la velocidad de la red, el método utilizado para acceder a la red física, los tipos de cables que se pueden utilizar y las tarjetas de red y dispositivos que se instalan.

Mejoras sobre el modelo OSI

Los dos niveles inferiores del modelo OSI, el nivel físico y el nivel de enlace de datos, definen la forma en que múltiples equipos pueden utilizar la red simultáneamente sin que exista interferencia entre ellas.

El proyecto IEEE 802 incorporó las especificaciones a esos dos niveles para crear estándares que tengan definidos los entornos LAN dominantes.

11000 11000 11000 11000 11000 11000 11000 11000 11000 11000



Mientras en las redes de conmutación sólo dos estaciones podían acceder en un momento dado al medio físico, lo que era fácilmente controlable por los protocolos de control de enlace, en las redes de área local (como lo son las redes de difusión) son varias las estaciones que en un momento dado pueden acceder al medio físico en un mismo momento, complicando considerablemente los procedimientos de control de ese proceso Tras la decisión de que se necesitaban más detalles en el nivel de enlace de datos, el comité de estándares 802 dividió el nivel de enlace de datos en dos subniveles:

Control de enlace lógico LLC. Establece y finaliza los enlaces, controla el tráfico de tramas, secuencia las tramas y confirma la recepción de las tramas.

Control de acceso al medio (MAC, *Media Access Control*). Gestiona el acceso al medio, delimita las tramas, comprueba los errores de las tramas y reconoce las direcciones de las tramas.

Subnivel De Control De Enlace Lógico (LLC)

El subnivel LLC gestiona la comunicación de enlace de datos y define el uso de puntos de interfaz lógicos llamados puntos de acceso al servicio SAP. Otros equipos pueden hacer referencia y utilizar los SAP para transferir información desde el subnivel LLC hacia los niveles superiores del modelo OSI. La categoría 802.2 define estos estándares.

Subnivel De Control De Acceso Al Medio (MAC)

El subnivel MAC es el más bajo de los dos subniveles, proporcionando acceso compartido al nivel físico para las tarjetas de red de los equipos. El nivel MAC se comunica directamente con la tarjeta de red y es el responsable del envío de datos libre de errores entre dos equipos de la red.

Capitulo V

Protocolo TCP/IP

El Protocolo de control de transmisión/Protocolo Internet (TCP/IP) es un conjunto de Protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo (formado por elementos diferentes). Además, TCP/IP proporciona un protocolo de red encaminable y permite acceder a Internet y a sus recursos. Debido a su popularidad, TCP/IP se ha convertido en el estándar de hecho en lo que se conoce como *interconexión de redes,* la intercomunicación en una red que está formada por redes más pequeñas.

TCP/IP se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos. La interoperabilidad es la principal ventaja de TCP/IP. La mayoría de las redes permiten TCP/IP como protocolo. TCP/IP también permite el encaminamiento y se suele utilizar como un protocolo de interconexión de redes.

Entre otros protocolos escritos específicamente para el conjunto TCP/IP se incluyen:

SMTP (Protocolo básico de transferencia de correo). Correo electrónico.

FTP (Protocolo de transferencia de archivos). Para la interconexión de archivos entre equipos que ejecutan TCP/IP.

SNMP (Protocolo básico de gestión de red). Para la gestión de redes.

Diseñado para ser encaminable, robusto y funcionalmente eficiente, TCP/IP fue desarrollado por el Departamento de Defensa de Estados Unidos como un conjunto de protocolos para redes de área extensa (WAN). Su propósito era el de mantener enlaces de comunicación entre sitios en el caso de una guerra nuclear. Actualmente, la responsabilidad del desarrollo de TCP/IP reside en la propia comunidad de Internet. La utilización de TCP/IP ofrece varias ventajas:

- **Es un estándar en la industria.** Como un estándar de la industria, es un protocolo abierto. Esto quiere decir que no está controlado por una única compañía, y está menos sujeto a cuestiones de compatibilidad. Es el protocolo, de hecho, de Internet.
- **Contiene un conjunto de utilidades para la conexión de sistemas operativos diferentes.** La conectividad entre un equipo y otro no depende del sistema operativo de red que esté utilizando cada equipo.
- **Utiliza una arquitectura escalable, cliente/servidor.** TCP/IP puede ampliarse (o reducirse) para ajustarse a las necesidades y circunstancias futuras. Utiliza sockets para hacer que el sistema operativo sea algo transparente.

Un socket es un identificador para un servicio concreto en un nodo concreto de la red. El socket consta de una dirección de nodo y de un número de puerto que identifica al servicio.

Históricamente, TCP/IP ha tenido dos grandes inconvenientes: su tamaño y su velocidad. TCP/IP es una jerarquía de protocolos relativamente grandes que puede causar problemas en clientes basados en MS-DOS. En cambio, debido a los requerimientos del sistema (velocidad de procesador y memoria) que imponen los sistemas operativos con interfaz gráfica de usuario (GUI), como Windows NT o Windows 95 y 98, el tamaño no es un problema.

Estándares TCP/IP

Los estándares de TCP/IP se publican en una serie de documentos denominados (RFC); Solicitudes de comentarios. Su objeto principal es proporcionar información o describir el estado de desarrollo. Aunque no se crearon para servir de estándar, muchas RFC han sido aceptadas como estándares.

El desarrollo Internet está basado en el concepto de estándares abiertos. Es decir, cualquiera que lo desee, puede utilizar o participar en el desarrollo de estándares para Internet. La Plataforma de arquitectura Internet (IAB) es el comité responsable para la gestión y publicación de las RFC. La IAB

permite a cualquier persona o a cualquier compañía que envíe o que evalúe una RFC. Esto permite que cualquier sugerencia sea tenida en cuenta para cambiar o crear estándares. Transcurrido un tiempo razonable para permitir la discusión, se crea un nuevo borrador que se convertirá o no en un estándar.

TCP/IP Y El Modelo OSI

El protocolo TCP/IP no se corresponde exactamente con el modelo OSI. En vez de tener siete niveles, sólo utiliza cuatro. Normalmente conocido como *Conjunto de protocolos de Internet*, TCP/IP se divide en estos cuatro niveles:

Nivel de interfaz de red.
Nivel Internet.
Nivel de transporte.
Nivel de aplicación.

Cada uno de estos niveles se corresponde con uno o más niveles del modelo OSI.

Capitulo VI

Topologías De Red

Descripción De Topología

Una topología de red es una representación pictórica de una capa de red. Alguna vez se ha realizado un mapa para decirle a alguien como ir algún lugar, o creado un plano de una casa de tal manera que se pueda conseguir una mejor idea de cómo el espacio es usado.

Hemos visto en el tema sobre el modelo OSI y la arquitectura TCP/IP que las redes de ordenadores surgieron como una necesidad de interconectar los diferentes host de una empresa o institución para poder así compartir recursos y equipos específicos.

Pero los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red.

La disposición de los diferentes componentes de una red se conoce con el nombre de **topología de la red**. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc.

Podemos distinguir tres aspectos diferentes a la hora de considerar una topología:

1. La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (los medios) en la red.
2. La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

3. La topología matemática, mapas de nodos y enlaces, a menudo formando patrones.

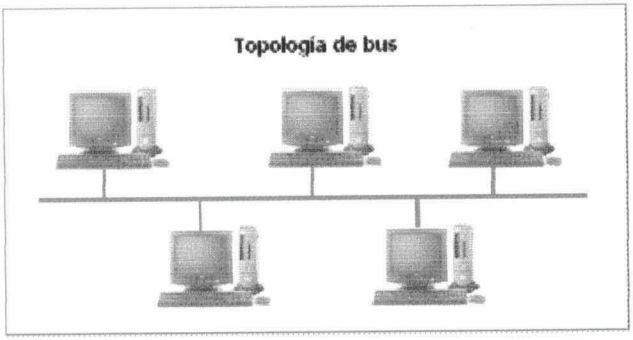
La topología de broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona Ethernet.

En cambio, la transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token significa que puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

Principales Modelos De Topología.

Topología De Bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados.

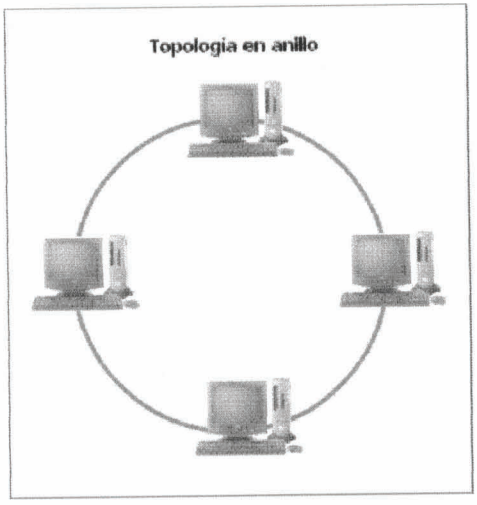


La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden ir segmentando la red en varias partes.

Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

Topología De Anillo

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.



Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

Topología De Anillo Doble

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos.

La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

Topología En Estrella

La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula por la red.

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

Topología En Estrella Extendida

La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs.

La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.

La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

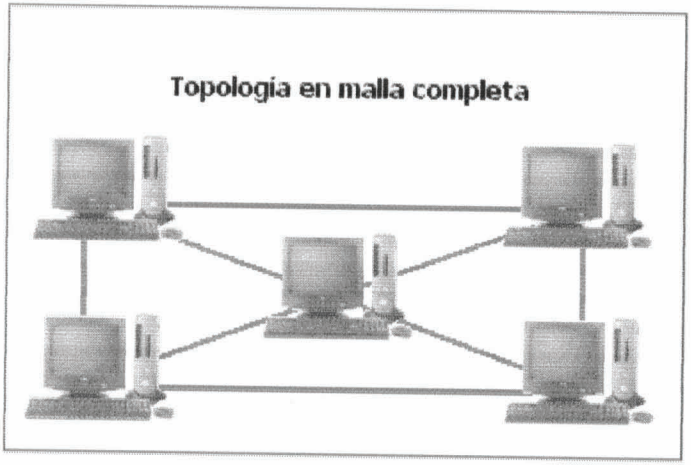
Topología En Árbol

La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

Topología En Malla Completa

En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.



La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

Topología De Red Celular

La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.

La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas.

La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad.

Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

Topología Irregular

En este tipo de topología no existe un patrón obvio de enlaces y nodos. El cableado no sigue un modelo determinado; de los nodos salen cantidades variables de cables. Las redes que se encuentran en las primeras etapas de construcción, o se encuentran mal planificadas, a menudo se conectan de esta manera.

Las topologías LAN más comunes son:

- **Ethernet**: topología de bus lógica y en estrella física o en estrella extendida.
- **Token Ring**: topología de anillo lógica y una topología física en estrella.
- **FDDI**: topología de anillo lógica y topología física de anillo doble.

Capitulo VII

Windows 2000 Server

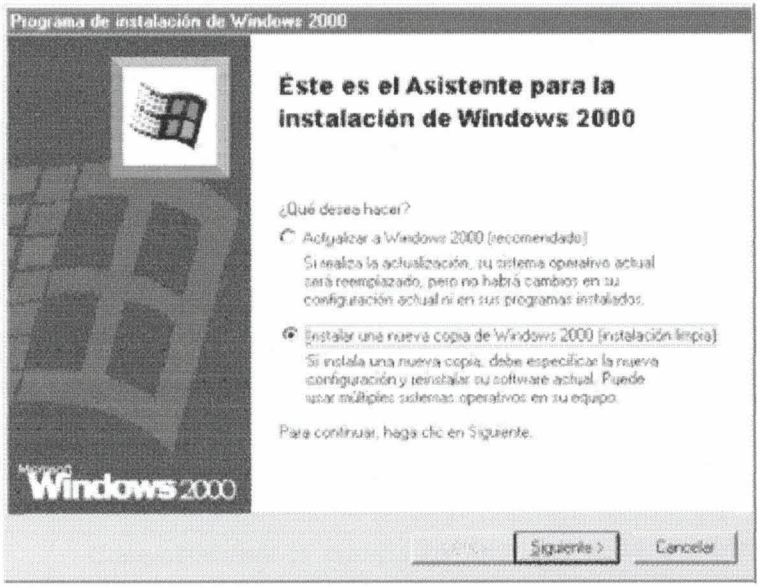
Recomendación De Instalar Windows 2000

Windows 2000 se caracteriza por ser un sistema operativo orientado para empresas y profesionales.

La mayoría de las empresas del mundo y profesionales eligen a Windows 2000 como su sistema operativo de uso diario.

- protección de escritura del modo kernel; y la "pool tagging",
- mínimo el numero de veces que había que reiniciar la maquina (Configuraciones de equipo) de 75 veces para Win9x a 7 veces en plataforma Windows 2000.
- previenen las inestabilidades antes de que lleguen a suceder
- Servicio de instalación contribuye a ello gestionando los componentes compartidos, a comparación de Win95 y 98
- gestionar de forma mas sencilla sus sistemas, empezando porque el laberinto de las DLLs parece resuelto
- permite que las DLLs se instalen en los directorios de sus aplicaciones específicas, y eviten que se eliminen las DLLs compartidas.

Instalación De Windows 2000 Server



La elección de cómo instalar Windows 2000 Server depende de lo que ya hay en el servidor, de dónde se encuentran los archivos de instalación y de cuántas instalaciones haya que hacer. Si se dispone de Windows 95/98 o Windows NT en la máquina, hay que ejecutar la instalación de Windows 2000 de 32 bits desde Windows 95/98 o Windows NT. También se puede iniciar desde el CD-ROM de Windows 2000 o desde el disco de inicio de instalación (o un disco de inicio de MS-DOS con controladores de CD-ROM o de red) y ejecutar el programa de instalación de Windows 2000 de 16 bits. Ambas versiones de la instalación se pueden ejecutar desde la red o se pueden automatizar.

Características Principales

Confiabilidad: Al ser un sistema desarrollado para trabajar junto a empresas y profesionales, Windows 2000 se lo desarrollado dedicando mucho mas tiempo en el TEST.

Seguridad: Es mucho mas seguro ya que esta basado en tecnología NT. Las unidades pueden ser transformadas a particiones de tipo NTFS.

Rendimiento: No recomendamos jugar a los juegos porque mucho no son compatibles, pero en tareas de diseño grafico o como servidor, Windows 2000 es mas superior que sus hermanos Windows 98 o ME. (Recuerda que Windows 98 y ME están orientados a usuarios de hogar)

A prueba de errores: Windows 2000 tiene errores y no lo podemos negar. Encontraremos errores en cualquier sistema operativo, sea Windows, linux o MacOS.
A diferencia de Windows 98 o ME, Windows 2000 presenta muchos menos errores y esto lo hace un sistema altamente estable.

Redes seguras, estables y confiables: Windows 2000 es un sistema altamente usado para cualquier tarea de redes y es por eso que cuenta con cientos de opciones más al configurar una red. Se utiliza para montar servidores o controlar estaciones de trabajo a distancia.

Rendimiento Superior

Compatibilidad: Es compatible con casi todo el hardware existente. Antes de adquirir algún producto deberemos preguntar si este es compatible con Windows 2000. Los diseñadores de Hardware, en su mayoría, realizan controladores para Windows 2000.

Requisitos Del Sistema

Antes de instalar Microsoft Windows 2000 Server hay que verificar que se dispone del hardware adecuado. Esto implica tanto cumplir los requisitos de sistema mínimos (y a ser posible superarlos si se quiere que el servidor realice algún trabajo real) como verificar la lista de hardware compatible HCL de Microsoft para asegurarse de que el equipo y los periféricos son soportados.

Y, antes de comprar hardware para el servidor, hay que comprobar la HCL en la carpeta Support del CD de instalación de Windows 2000. Si el sistema no aparece en la lista, conviene comprobar la HCL en el sitio Web de Microsoft (http://www.microsoft.com/hwtest/hcl/). Si existen controladores actualizados

para el hardware que se va a utilizar, conviene descargarlos y copiarlos a un disquete o disco duro disponible para poder utilizarlos durante la instalación, si es necesario.

Si un componente del sistema no aparece en la HCL se puede visitar el sitio Web del fabricante del dispositivo o contactar con él para ver si hay disponibles controladores actualizados. En general, la regla ha seguir es la siguiente: no utilizar un servidor que no es 100 por 100 compatible.

Requisitos Mínimos Para Obtener Un Rendimiento Adecuado:

- **Intel Pentium 133 a 32 bits:** Uno o más procesadores Intel Pentium II 300 ó más rápidos (o procesadores compatibles; compruébese la HCL).
- **64 Mb de RAM:** 128 Mb de RAM mínimo, 256 Mb o más recomendado.
- **Monitor VGA:** Monitor Súper VGA con resolución de al menos 800 x 600.
- **Teclado y ratón u otro dispositivo señalador:** Cualquier tipo de teclado y ratón u otro dispositivo señalador. (Si el teclado es del tipo PS/2, el ratón debe ser también PS/2 o USB)
- **Partición de 850 Mb con 650 Mb de espacio libre:** 2 Gb de espacio libre en un disco duro Ultra IDE o (preferiblemente) Ultra Wide SCSI con 7200 rpm o más.
- **CD-ROM de inicio 12x:** No se necesita más velocidad para la instalación, aunque tiene que ser compatible con el sistema de inicio *El Torito*.
- **Unidad de disco de 1.44 Mb:** Si se va a realizar la instalación con los cuatro discos de inicio.
- **Uno o más adaptadores de red:** Si se va a realizar la instalación a través de la Red

Planificación De Las Particiones

Lo siguiente es decidir cómo se desea dividir en particiones y configurar las unidades. Microsoft recomienda utilizar el sistema de archivos de NT (NTFS) en todo el sistema, a menos que se necesite mantener la compatibilidad con otro sistema operativo existente en el equipo, algo bastante raro en un servidor. NTFS posee muchas ventajas, incluyendo eficiencia, fiabilidad, seguridad y compresión. Además,

muchas características o servicios de Windows 2000 requieren una partición NTFS. Por ejemplo, para utilizar el servidor como controlador de dominio o servidor de Active Directory debe haber disponible una partición NTFS.

NTFS ha sido siempre superior a la tabla de asignación de archivos (FAT, File Allocation Table) o los sistemas de archivos FAT32, pero tiene un problema en Windows NT. Si, por alguna razón, no se puede iniciar con la unidad de disco de sistema NTFS, la única esperanza de recuperación es realizar una instalación paralela de Windows NT. Windows 2000 viene equipado con una opción de inicio en Modo seguro, al estilo de Windows 95/98, además de un Consola de recuperación especial que permite iniciar con una línea de comandos en un sistema que no inicia y acceder de forma segura a las particiones NTFS.

Se pueden crear hasta cuatro particiones primarias en una unidad de disco, o hasta tres particiones primarias y una partición extendida. Para instalar Windows 2000, se utilizará simplemente, en la mayoría de los casos, una única partición con formato NTFS en la unidad de disco de inicio de aproximadamente 1 ó 2 Gb. Conviene dejar el resto del espacio libre del disco duro sin asignar hasta después de la instalación, cuando se podrán crear particiones adicionales para programas y datos en el espacio sin asignar.

Por regla general, se utilizarán una o más unidades de disco para datos, preferiblemente configuradas con alguna clase de tolerancia a fallos. Si se utiliza una unidad o unidades de disco diferentes para los datos, conviene convertirlas en discos dinámicos y darles formato con el sistema de archivos NTFS. Este enfoque permitirá trabajar de forma sencilla con los volúmenes y almacenar la información de forma segura y eficiente.

Recogida De Información De La Red

Después de determinar cómo se quieren dividir en particiones las unidades de disco, hay que localizar todos los controladores para el hardware. Después, hay que almacenar (o crear) los siguientes parámetros:

- **Nombre en el Sistema de nombres de dominio DNS del equipo:** Este nombre puede contener letras mayúsculas o minúsculas, números y el carácter guión. El nombre DNS del host no debe sobrepasar los 15 caracteres si se pretende que el nombre NetBIOS sea el mismo que el DNS y mantener así la compatibilidad con clientes que no sean Windows 2000.
- **Nombre del dominio o grupo de trabajo al que debe unirse (si se encuentra en una red):** Si se está creando un nuevo dominio Windows 2000, este nombre debería ser compatible con el DNS: por ejemplo, midepartamento.miempresa.com.
- **Dirección IP del equipo:** Esto es necesario a menos que la red disponga de un servidor de Protocolo de Configuración Dinámica de Host.

Si no se dispone de un servidor DHCP y no se asigna una dirección IP al equipo, Windows 2000 asignará al equipo una dirección IP restringida. Esta dirección IP funcionará en una red sencilla con sólo una subred IP, pero no funcionará en redes más complejas, ni funcionará como dirección IP de Internet. Para redes más complejas, conviene instalar un servidor DHCP en la red o asignar las direcciones IP manualmente. Para adquirir una dirección IP de Internet válida es necesario registrar un contexto de direcciones IP en el proveedor de servicios de Internet.

- **Componentes adicionales de Windows 2000 Server**
- **Modo de licencia de clientes y el número de clientes simultáneos (si el modo de licencia es Por servidor)** Windows 2000 Server soporta licencias Por servidor y Por puesto. Si no se está seguro de qué modo de licencia utilizar, es mejor elegir Por servidor. Se puede cambiar de modo Por servidor a Por puesto una vez (sin coste adicional) pero no de modo Por puesto a Por servidor.

Instalación Desde Windows 95/98 Ó Windows NT

Si tenemos instalado Windows 95/98 ó Windows NT, la instalación recopila información y copia los archivos que necesita el equipo para iniciar en el modo de texto de Windows 2000 y después reinicia en modo texto. Se puede entonces (opcionalmente) seleccionar la partición apropiada, después de lo cual se instala Windows 2000 en el disco duro y se pasa al Asistente para instalación de Windows 2000 en modo gráfico, que recopila más información, configura los dispositivos y termina de copiar los archivos. Después de esto, la instalación está completa y el equipo se reinicia en Windows 2000.

1. Insertar el CD-ROM de Windows 2000 y pulsar en Instalar Windows 2000, si está activa la Reproducción automática del CD-ROM

(Notificación automática de inserción). Si no es así, hay que ejecutar winnt32.exe desde la carpeta \i386 del CD-ROM de Windows 2000.

2. Para instalar Windows 2000 Server desde la red, hay que ejecutar el programa winnt32.exe desde la unidad de disco de red que contenga los archivos de instalación de \w2ks y después, proceder con la instalación normalmente.
3. Dependiendo del Sistema Operativo que tengamos y de la Licencia que hayamos adquirido (Actualización o OEM), el sistema activará o desactivará las siguientes opciones, ofreciendo todas las posibilidades de instalación posibles:
    - Actualizar a Windows 2000.
    - Instalar una nueva copia de Windows 2000.
4. Después de elegir la opción deseada pulsamos **Siguiente**.
5. Contrato de Licencia: Se debe leer el contrato de licencia, seguidamente hay que elegir el botón de opción Acepto este contrato y pulsar con el ratón en Siguiente. La instalación muestra la ventana Seleccionar opciones especiales, y que se utiliza para personalizar las opciones de idioma, cambiar cómo copiará la instalación los archivos y activar el uso de utilidades de accesibilidad durante la instalación para usuarios con problemas de visión.

6. Seleccionar opciones especiales: En esta pantalla se pueden configurar las siguientes pociones:
   - **Opciones de Idioma:** Si se desea configurar el sistema operativo Windows 2000 para que utilice conjuntos de caracteres de varios idiomas, hay que pulsar en el botón Opciones de idioma, elegir el idioma principal de la lista desplegable, seleccionar cualquier grupo de idiomas adicionales para los cuales se desea instalar soporte y después pulsar Aceptar
   - **Opciones avanzadas:** Para especificar la carpeta y partición de instalación de Windows 2000, o para decirle a la instalación de Windows 2000 la ubicación de los archivos de instalación, hay que pulsar con el ratón en el botón Opciones avanzadas en la ventana Seleccionar opciones especiales para abrir la ventana Opciones avanzadas.
   - **Opciones de accesibilidad:** Para configurar las opciones de pantalla con configuraciones especiales para disminuidos físicos.
7. Se debe pulsar en **Siguiente** para copiar los archivos de instalación al equipo. Después de que la instalación termine de copiar archivos, se reinicia el equipo y se pasa al modo de texto de Windows 2000 para la parte de la instalación basada en texto.

Instalación Desde Un Sistema Con MS-DOS

Instalación desde un sistema con MS-DOS, la instalación copia los archivos necesarios al disco duro para reiniciar en el modo de texto de Windows 2000 y después lo hace. La instalación realiza el mismo proceso que hubiera realizado si se hubiera iniciado desde un CD-ROM o disco de inicio de instalación de Windows 2000.

Instalación Desde Los Discos De Inicio De Instalación De Windows 2000 Ó Desde El CDROM

Si no se dispone de Windows 95/98 o Windows NT instalado en el servidor, es necesario iniciar el sistema con el CD-ROM de Windows 2000 o los disquetes de inicio de instalación y configuración. (También se puede iniciar con un disco de inicio MS-DOS, pero es mucho más lento.)

Para iniciar desde el CD-ROM de Windows 2000, hay que introducir el CD en la unidad y reiniciar el sistema. Si la instalación no comienza automáticamente, quizás sea necesario configurar el inicio en la BIOS para decirle al sistema que utilice la unidad CD-ROM antes que el disco duro.

Si no es posible iniciar desde el CD-ROM, hay que introducir el Disco de instalación 1 en la disquetera y reiniciar la máquina. Se solicitará el resto de los disquetes de instalación y, entonces, el equipo pasará a la fase en modo texto de la instalación de Windows 2000, como se describe en la siguiente sección.

Fase Del Programa De Instalación En Modo Texto

Cuando se inicia desde el CD-ROM o los disquetes de Windows 2000, o cuando se reinicia la primera vez después de ejecutar la instalación desde MS-DOS, Windows 85/98 o Windows NT, se entra en la fase basada en texto en la cual el programa de instalación copia los archivos necesarios para reiniciar en Windows 2000 para la porción de la instalación basada en GUI. Durante la fase basada en texto de la instalación, hay que seguir los siguientes pasos:

1. La primera pantalla que aparece es la de Instalación de Windows 2000 Server, en la que se presentan tres posibilidades: Instalar Windows 2000, actualizar una instalación previa o salir del programa de instalación. Para continuar con la instalación hay que pulsar **Intro.**
2. Hay que leer el contrato de licencia de Windows 2000 Server. Se puede utilizar la tecla **AV PÁG** para desplazarse hacia abajo, y pulsar después **F8** para continuar. Buscará instalaciones de

Windows 2000 que pueda actualizar y si las encuentra nos pedirá que confirmemos si queremos actualizar o realizar una instalación nueva.

3. En la siguiente pantalla, se pide elegir en qué disco y partición se quiere instalar Windows 2000. Se muestran todas las unidades de disco y particiones reconocidas del sistema, clasificadas por identificador SCSI o IDE y el número de bus. Hay que seleccionar una partición o espacio sin dividir en particiones utilizando las teclas de dirección del teclado. *Si se dispone de una unidad extraíble con capacidad de 829 Mb o más, se puede instalar Windows 2000 en un disco extraíble. Este paso sólo está recomendado para instalaciones paralelas, no para la instalación principal de Windows 2000.*
4. Para borrar la partición seleccionada, hay que pulsar D; para crear una nueva partición, hay que seleccionar algún espacio libre sin dividir en particiones y pulsar c. Si se elige crear una nueva partición, la instalación preguntará si se quiere dar formato a la partición con el sistema de archivos NTFS o FAT. Si se escoge el sistema de archivos FAT en una partición mayor de 2 Gb, la partición se dará formato con el sistema de archivos FAT32.

Al borrar una partición, se borra toda la información que contiene. No se debe borrar una partición a menos que toda su información se encuentre en una copia de seguridad fiable.

5. Cuando se termine de modificar las particiones, hay que seleccionar la partición en la que se desea instalar Windows 2000 y pulsar **Intro**.
6. La instalación pedirá confirmación sobre la elección de la partición y se dará la opción de formatear en FAT o NTFS. Si hubiera una partición formateada previamente, aparecerá una tercera opción que nos permitirá dejar la partición con el mismo sistema de archivos que ya tiene. Seleccionamos la opción correcta y pulsamos **Intro**.
7. La instalación comprueba la ausencia de errores en los discos duros y copia entonces los archivos apropiados en la recién creada carpeta de Windows 2000 (llamada \WINNT de forma predeterminada). Cuando la instalación termina de copiar los archivos, pide que se extraiga cualquier disquete o CD-ROM, y entonces reinicia el sistema e inicia el Asistente para la instalación de Windows 2000.

Capitulo VIII

Seguridad En Windows 2000 Server

Kerberos

En la mitología griega, Kerberos era el perro tricéfalo que custodiaba la entrada al submundo. El último desarrollo de Kerberos es un poco menos feroz que su homólogo mitológico. La definición del protocolo básico usado por Kerberos está recogida en la RFC 1510, fue desarrollado por el MIT en el marco del proyecto Atena y tiene que ver con la autentificación de usuarios. Microsoft ha decidido implementar su propia versión de Kerberos como protocolo de autentificación por omisión para su sistema operativo Windows 2000. En este artículo, abordaremos las características más importantes de la implementación de Kerberos hecha por Microsoft.

Lo Básico

Cuando dos entidades quieren autentificarse una frente a la otra (por ejemplo, un usuario y un servidor), necesitan recurrir a un tercero de confianza para que medie entre ellos. En Windows 2000, el KDC (centro de distribución de claves Kerberos) añade escalabilidad al protocolo Kerberos y sirve de mediador, ya que cada controlador de dominio ejecuta un servicio KDC. La instalación de KDC se realiza durante la instalación del AD (Directorio activo). El AD contiene una copia de las credenciales de usuario (es decir, las contraseñas cifradas de los usuarios) utilizadas por Kerberos en el proceso de autentificación.

Windows 2000 incluye un proveedor de autentificación Kerberos cliente, además del soporte Kerberos para otros tipos de cliente, como Win9x. Si desea que su cliente Win9x utilice Kerberos para llevar a cabo la autentificación, deberá instalar el cliente para los servicios de Directorio. Si, en cambio,

necesita disponer del soporte Kerberos para Windows NT 4.0 Workstation, no tendrá más remedio que migrar a Windows 2000 Professional.

Hasta que se diseñó *Kerberos*, la autenticación en redes de computadores se realizaba principalmente de dos formas: o bien se aplicaba la autenticación por declaración (*Authentication by assertion*), en la que el usuario es libre de indicar el servicio al que desea acceder (por ejemplo, mediante el uso de un cliente determinado), o bien se utilizaban contraseñas para cada servicio de red. Evidentemente el primer modelo proporciona un nivel de seguridad muy bajo, ya que se le otorga demasiado poder al cliente sobre el servidor; el segundo modelo tampoco es muy bueno: por un lado se obliga al usuario a ir tecleando continuamente su clave, de forma que se pierde demasiado tiempo y además la contraseña está viajando continuamente por la red. *Kerberos* trata de mejorar estos esquemas intentando por un lado que un cliente necesite autorización para comunicar con un servidor (y que esa autorización provenga de una máquina confiable), y por otro eliminando la necesidad de demostrar el conocimiento de información privada (la contraseña del usuario) divulgando dicha información.

Kerberos se ha convertido desde entonces en un referente obligatorio a la hora de hablar de seguridad en redes. Se encuentra disponible para la mayoría de sistemas Unix, y viene integrado con OSF/DCE. Está especialmente recomendado para sistemas operativos distribuidos, en los que la autenticación es una pieza fundamental para su funcionamiento: si conseguimos que un servidor logre conocer la identidad de un cliente puede decidir sobre la concesión de un servicio o la asignación de privilegios especiales. Sigue vigente en la actualidad, a pesar del tiempo transcurrido desde su diseño; además fue el pionero de los sistemas de autenticación para sistemas en red, y muchos otros diseñados posteriormente, como *KryptoKnight*, SESAME o *Charon* se basan en mayor o menor medida en *Kerberos*.

El uso de *Kerberos* se produce principalmente en el **login**, en el acceso a otros servidores (por ejemplo, mediante rlogin) y en el acceso a sistemas de ficheros en red como NFS. Una vez que un cliente está autenticado o bien se asume que todos sus mensajes son fiables, o si se desea mayor seguridad se

puede elegir trabajar con mensajes seguros (autenticados) o privados (autenticados y cifrados). **Kerberos** se puede implementar en un servidor que se ejecute en una máquina segura, mediante un conjunto de bibliotecas que utilizan tanto los clientes como las aplicaciones; se trata de un sistema fácilmente escalable y que admite replicación, por lo que se puede utilizar incluso en sistemas de alta disponibilidad.

Arquitectura De Kerberos

Un servidor *Kerberos* se denomina KDC, y provee de dos servicios fundamentales: el de autenticación (AS), y el de *tickets* (TGS) El primero tiene como función autenticar inicialmente a los clientes y proporcionarles un *ticket* para comunicarse con el segundo, el servidor de *tickets*, que proporcionará a los clientes las credenciales necesarias para comunicarse con un servidor final que es quien realmente ofrece un servicio. Además, el servidor posee una base de datos de sus clientes (usuarios o programas) con sus respectivas claves privadas, conocidas únicamente por dicho servidor y por el cliente que al que pertenece.

La arquitectura de *Kerberos* está basada en tres objetos de seguridad: Clave de Sesión, *Ticket* y Autenticador.

- La **clave de sesión** es una clave secreta generada por *Kerberos* y expedida a un cliente para uso con un servidor durante una sesión; no es obligatorio utilizarla en toda la comunicación con el servidor, sólo si el servidor lo requiere (porque los datos son confidenciales) o si el servidor es un servidor de autenticación. Se suele denominar a esta clave, para la comunicación entre un cliente C y un servidor S.
- Las claves de sesión se utilizan para minimizar el uso de las claves secretas de los diferentes agentes: éstas últimas son válidas durante mucho tiempo, por lo que es conveniente para minimizar ataques utilizarlas lo menos posible.
- El **ticket** es un testigo expedido a un cliente del servicio de *tickets* de *Kerberos* para solicitar los servicios de un servidor; garantiza que el cliente ha sido autenticado recientemente. A un *ticket*

de un cliente C para acceder a un servicio S se le denomina. Este *ticket* incluye el nombre del cliente C, para evitar su posible uso por impostores, un periodo de validez y una clave de sesión asociada para uso de cliente y servidor. *Kerberos* siempre proporciona el *ticket* ya cifrado con la clave secreta del servidor al que se le entrega.

- El **autenticador** es un testigo construido por el cliente y enviado a un servidor para probar su identidad y la actualidad de la comunicación; sólo puede ser utilizado una vez. Un autenticador de un cliente C ante un servidor S se denota. Este autenticador contiene, cifrado con la clave de la sesión, el nombre del cliente y un *timestamp*.

Kerberos sigue de cerca el protocolo de Needham y Schroeder con clave secreta, utilizando *timestamps* como pruebas de frescura con dos propósitos: evitar reenvíos de viejos mensajes capturados en la red o la reutilización de viejos *tickets* obtenidos de zonas de memoria del usuario autorizado, y a la vez poder revocar a los usuarios los derechos al cabo de un tiempo.

Autenticación

El protocolo de autenticación de *Kerberos* es un proceso en el que diferentes elementos colaboran para conseguir identificar a un cliente que solicita un servicio ante un servidor que lo ofrece; este proceso se realiza en tres grandes etapas que a continuación se describen. En la tabla se muestran las abreviaturas utilizadas, resumen gráfico de este protocolo.

Tabla: Abreviaturas utilizadas.

C	Cliente que solicita un servicio
S	Servidor que ofrece dicho servicio
A	Servidor de autenticación
T	Servidor de *tickets*

K	Clave secreta del cliente
K	Clave secreta del servidor
K	Clave secreta del servidor de *tickets*
K	Clave de sesión entre el cliente y el servidor de *tickets*
K	Clave de sesión entre cliente y servidor

Login

Inicialmente el cliente C (en este caso el usuario a través del programa login) necesita obtener las credenciales necesarias para acceder a otros servicios. Para ello cuando un usuario conecta a un sistema `kerberizado' teclea en primer lugar su nombre de usuario, de la misma forma que en un sistema habitual; la diferencia está en que el programa login envía el nombre de usuario al servidor de autenticación de *Kerberos* para solicitar un *ticket* que le permita comunicarse posteriormente con el servidor de *tickets*, TGS:

Si el usuario es conocido, el servidor de autenticación retorna un mensaje que contiene una clave para la comunicación con TGS y un *timestamp* cifrado con la clave secreta del cliente, junto un *ticket* para la comunicación con TGS cifrado con la clave secreta de este servidor:

El programa de *login* intentará descifrar, con la clave que el usuario proporciona, y si ésta es correcta podrá obtener y: un cliente sólo podrá descifrar esta parte del mensaje si conoce su clave secreta, (en este caso el *password*). Una vez obtenida, la clave para comunicar al cliente con el servidor de *tickets*, el programa passwd la guarda para una posterior comunicación con el TGS y borra la clave del usuario de memoria, ya que el *ticket* será suficiente para autenticar al cliente; este modelo consigue que **el *password* nunca viaje por la red**

Obtención De Tickets

El cliente ya posee una clave de sesión para comunicarse con el servidor de *tickets* y el *ticket* necesario para hacerlo, cifrado con la clave secreta de este servidor (el cliente **no** puede descifrar este *ticket*). Cuando el cliente necesita acceder a un determinado servicio es necesario que disponga de un *ticket* para hacerlo, por lo que lo solicita al TGS enviándole un autenticador que el propio cliente genera, el *ticket* de T y el nombre del servicio al que desea acceder, S, y un indicador de tiempo: Cuando TGS recibe el *ticket* comprueba su validez y si todo es correcto retorna un mensaje que contiene una clave para comunicación con S y un *timestamp* cifrado con la clave de sesión del par CT, junto a un *ticket* para que el cliente C y el servidor S se puedan comunicar cifrado con la clave secreta del servidor:

C sólo podrá obtener si conoce la clave secreta...

Petición De Servicio

Tras obtener el *ticket* para comunicarse con S el cliente ya está preparado para solicitar el servicio; para ello presenta la credencial autenticada ante el servidor final, que es quien va a prestar el servicio. C se comporta de la misma forma que cuando solicitó un *ticket* a T: envía a S el autenticador recién generado, el *ticket* y una petición que puede ir cifrada si el servidor lo requiere, aunque no es necesario:

El servidor envía entonces al cliente la prueba de actualidad cifrada con la clave secreta de la sesión:

Sólo S pudo obtener y por tanto enviar este mensaje.

Problemas De Kerberos

A la vista de todo lo comentado en los puntos anteriores puede darnos la impresión de que *Kerberos* es la panacea de los sistemas de autenticación. Sin embargo, y aunque se trate de un sistema robusto, no está exento de ciertos problemas, tanto de seguridad como de implementación, que han hecho que este sistema no esté todo lo extendido que debería.

Uno de los principales problemas de *Kerberos* es que cualquier programa que lo utilice ha de ser modificado para poder funcionar correctamente, siguiendo un proceso denominado `kerberización'. Esto implica obviamente que se ha de disponer del código fuente de cada aplicación que se desee kerberizar, y también supone una inversión de tiempo considerable para algunas aplicaciones más o menos complejas que no todas las organizaciones se pueden permitir.

El problema anterior es simplemente de implementación; no afecta para nada a la seguridad - o inseguridad - del protocolo. Un problema que sí está relacionado con la seguridad de *Kerberos* es la gran centralización que presenta el sistema. Para un correcto funcionamiento se ha de disponer en todo momento del servidor *Kerberos*, de forma que si la máquina que lo alberga falla, la red se convierte en inutilizable; obviamente esto es una contradicción con lo que nos dice la teoría de sistemas distribuidos, donde se recalca el uso de la distribución para mantener la disponibilidad del sistema, intentado que si un equipo falla el resto pueda seguir funcionando, si no a pleno rendimiento, al menos correctamente. Por si esto no fuera suficiente, otro ejemplo de la centralización de *Kerberos* reside en el hecho de que casi toda la seguridad reside en el servidor que mantiene la base de datos de claves, de forma que si éste se ve comprometido, la red entera está amenazada.

Otro potencial problema de seguridad es el uso de *timestamps* como pruebas de frescura en *Kerberos*. Esto obliga a que todas las máquinas que ejecutan servicios autenticados mantengan sus relojes mínimamente sincronizados (con desfases máximos de pocos minutos), con todo lo que esto implica. Además ese tiempo global ha de ser accesible a todas las estaciones; aunque en el diseño no se asume que todas mantengan la hora exacta, sí que se les obliga a mantenerse dentro de los márgenes si desean solicitar *tickets*, para lo que se necesitan servidores de tiempo con los que los clientes puedan sincronizar periódicamente sus relojes, por ejemplo cada vez que arrancan.

Todos estos problemas, y algunos más que se han ido solucionando en diferentes versiones del sistema, han propiciado que el uso de *Kerberos* no esté muy extendido; en la mayoría de redes es

suficiente con un protocolo de comunicación cifrado para mantener una mínima seguridad, de forma que el complejo modelo de *Kerberos* se ve sustituido a ese efecto por programas tan simples y transparentes como SSH

Capitulo IX

Active Directory

Sitios Y Servicios De Active Directory

Sitios y servicios de Active Directory es un complemento de MMC que se utiliza para crear y administrar los sitios que constituyen una red de Microsoft Windows 2000 y para establecer vínculos entre los sitios. Un sitio se define como un grupo de equipos de una o varias subredes de protocolo de Internet (IP) que están bien conectadas. Una subred es una red que forma parte de otra red de mayor tamaño.

Bien conectadas significa que los sistemas comparten un transporte de red que proporciona comunicaciones de bajo coste y gran velocidad entre las máquinas y, generalmente, hace referencia a sistemas de una misma ubicación que están conectados mediante LAN. Los sistemas que no están bien conectados son los que utilizan comunicaciones relativamente lentas y caras. Active Directory consta de uno o varios sitios, pero los sitios no forman parte de los espacios de nombres con los que se trabaja al crear la jerarquía de Active Directory.

Los sitios no aparecen como objetos en el espacio de nombres de Active Directory; se hallan apartados completamente de la jerarquía de bosques, árboles y dominios. Un sitio puede contener objetos de diferentes dominios, y los objetos de un dominio pueden estar repartidos entre sitios diferentes. La razón fundamental para dividir la red de una empresa en varios sitios es aprovechar las comunicaciones eficientes entre los sistemas bien conectados y regular el tráfico con las conexiones más lentas y caras. Más concretamente, Active Directory utiliza los sitios durante la autenticación y la réplica.

Autentificación: Cuando un usuario inicia una sesión en la red desde una estación de trabajo, el sistema lo autentifica siempre que sea posible con un controlador de dominio ubicado en el mismo sitio. Esto acelera el proceso de autentificación y ayuda a reducir el tráfico WAN.

Réplica: Las actividades de réplica de los controladores de dominios que deben atravesar los límites de los sitios están sometidas a condiciones especiales debido a la necesidad de utilizar las conexiones WAN.

Los sitios de Active Directory están asociados a subredes IP concretas utilizadas por la red. Durante el proceso de autentificación, la estación de trabajo transmite información acerca de la subred en la que reside. Los controladores de dominios utilizan esta información para hallar los servidores de Active Directory de la misma subred que la estación de trabajo.

El uso de sitios durante la réplica es algo más complejo. Cuando dos controladores de dominios se hallan en el mismo sitio, la réplica se realiza con toda la velocidad de la LAN, generalmente, de 10 a 100 Mbps. Por otro lado, es probable que dos controladores de dominios situados en edificios o en ciudades diferentes estén conectados mediante tecnología WAN, que es mucho más lenta y, también, mucho más cara que la tecnología LAN. Por tanto, maximizar la eficacia de las comunicaciones entre los sitios suele ser cuestión del momento y de la frecuencia de las réplicas que utilizan los vínculos WAN.

Conceptos Fundamentales De Active Directory

Dada la gran importancia que ha producido la incorporación de Windows 2000 y Active Directory, y los grandes cambios que tiene respecto de sus versiones anteriores es de fundamental importancia comprender este servicio de directorio. De por sí, puede llegar a ser más complejo para los que conocemos la versión anterior, porque traemos incorporados ciertos conceptos que no siempre se mantienen.

La apuesta fundamental de Microsoft fue desprenderse de la interfaz NetBIOS que viene desde los "antiguos sistemas", aunque la sigue teniendo por razones de compatibilidad. En el caso de una red homogénea Windows 2000 y sin aplicaciones que la utilicen es posible directamente deshabilitar **NetBIOS sobre TCP/IP**, con lo cual bajaremos una parte sustancial del tráfico de red, y aliviaremos a algunos administradores.

Pero ¿cuál es el inconveniente de NetBIOS? El tema a tener en consideración es que NetBIOS es utilizado por todos los sistemas operativos Windows anteriores a Windows 2000, como mecanismo de encontrar los servicios en la red, como única alternativa. Y el espacio de direccionamiento NetBIOS es plano. Esto significa que cada servicio en la red es identificado por un nombre de hasta 16 caracteres (aunque se pueden especificar sólo 15), donde no es posible establecer sistemas jerárquicos. Esto trae aparejados dificultades en la administración de redes a medida que son más grandes.

Pero ya existía un sistema jerárquico de nombres, ampliamente aceptado, probado, normalizado: el espacio de nombres de DNS ¡la solución! La forma en que Windows 2000 encuentra los servicios de red es a través del espacio de nombres de DNS.

Esta estructura jerárquica plantea un campo de muchas más posibilidades en ambientes grandes y tiene las ventajas de ser un standard, pero también tiene algunos inconvenientes: en una estructura jerárquica hay nodos que dependen de un nivel superior, lo cual en algún momento puede presentar poca flexibilidad, como por ejemplo que el espacio **debe construirse de arriba hacia abajo**.

Active Directory es el servicio de directorios de Windows 2000, así que primero que nada definiremos muy sintéticamente la funcionalidad de un servicio de directorio: Permite organizar, administrar y controlar desde un punto los recursos de red. Además permite que los usuarios tengan un único inicio de sesión, a partir de lo cual pueden acceder a los recursos a los que está autorizado. Tengamos en cuenta que estamos tomando la definición de recurso de red en su acepción más amplia, esto es, no sólo carpetas y archivos, sino que los equipos, los servicios del directorio y los servicios de red están incluidos.

La menor unidad constructiva para poder utilizar Active Directory es el Dominio, que podemos definir de varias formas, entre ellas: un conjunto arbitrario de recursos de red bajo una administración común, tal que se cumpla:

- **Límite de administración:** Los administradores sólo tendrán poder de administración dentro de él

- **Límite de seguridad:** Los administradores definirán los requerimientos de seguridad en sus dominio
- **Límite de replicación:** La información sensitiva de los recursos de red no se replicará fuera de sus límites

Para crear un dominio, los requisitos básicos son tener instalado un Windows 2000, en cualquiera de sus 3 versiones de Server (Server, Advanced Server o Datacenter Server), protocolo de red TCP/IP instalado y configurado manualmente (no obtención automática de dirección IP). Hay además un tercer requisito que es la presencia de un servidor de nombres DNS instalado y configurado en la red, pero podemos hacer que el sistema se encargue de instalarlo y configurarlo adecuadamente, preguntándonos sólo si queremos que lo instale y configure. Además debemos disponer más de 250MB de espacio libre en disco y por lo menos una partición debe estar formateada en NTFS, no necesariamente donde está instalado el sistema operativo.

Una vez que tenemos el Server instalado con los requisitos anteriores, debemos ejecutar DCPROMO.EXE. Este asistente se encargará de instalar Active Directory, transformando un Server en Controlador de Dominio. Si lo ejecutamos sobre un Controlador de Dominio, lo volverá a Server.

En este caso Server se refiere a un Server miembro de dominio o a un Server en grupo de trabajo Es altamente recomendable que por cada domino existan por lo menos 2 Controladores de Dominio, ya que esto nos provee balance de carga y sobre todo tolerancia a fallas. Las funciones fundamentales de los Controladores de Dominio son proveer la validación de los usuarios y equipos; y la replicación de la información del directorio a otros Controladores de Dominio del mismo dominio.

De todas formas antes de ejecutar DCPROMO.EXE debemos tener en claro, si es necesario un único dominio, o si por el contrario necesitaremos una jerarquía de dominios. En general y lo recomendado para la mayoría de los casos es utilizar un único dominio, ya que esto disminuye los costos, facilita la administración y provee un sistema jerárquico interno que no dificultará la administración como era el caso de Windows NT 4.0, donde el administrador debía lidiar con un listado "plano" de todos los usuarios. Los motivos que pueden justificar la necesidad de más de un dominio son: diferentes Directivas

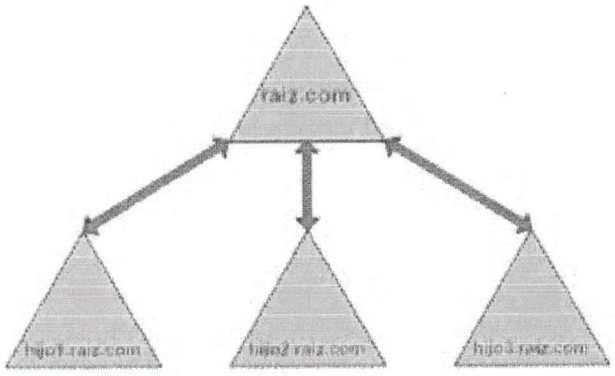
de Grupo (Group Policies) para cuentas, disminución de tráfico sobre enlaces WAN y algunas consideraciones de administración descentralizada.

Entre los elementos que deberemos diseñar y tener en claro desde el principio son las estructuras Lógica y Física. Esta última es novedad total en Windows 2000, ya que las versiones previas no soportan ningún tipo de diseño físico de estructura.

Estructura Lógica

El caso más sencillo de estructura lógica es si hemos determinado que un único dominio cumple con nuestras necesidades. Pero como hemos visto, en algunos casos esto no va a ser posible. Si debemos instalar varios dominios, éstos se pueden agrupar en estructuras jerárquicas denominadas árboles (Trees)

Para poder construir un árbol (Tree) debemos comenzar por crear el primer dominio en la estructura, raiz.com en este caso. A partir de lo cual podemos crear los subdominios, hijoN.raiz.com en este caso.



Pero demos una definición más precisa de un árbol de dominios: es un conjunto jerárquico de dominios que comparten:

- Relaciones de confianza, creadas automáticamente con el dominio superior, de tipo bidireccional (A –> B y B –> A) y transitiva (A –> B –> C por lo tanto A –> C)
- Espacio contiguo de nombres. Cada subdominio debe incluir el nombre del dominio del cual "cuelga", salvo el primero. No hay un límite teórico en cuanto a la cantidad de subdominios que puede tener cada uno, ni en cuanto a los niveles de hijos de cada uno
- Comparten la **Configuración** y el **Esquema**
- Comparten la información en el **Catálogo Global** (Global Catalog)

La Configuración es una partición del Active Directory, donde está almacenada la configuración común de todos los dominios como pueden ser los nombres y la ubicación de cada uno de ellos, relaciones de confianza, etc.

El Esquema, es la definición formal de los atributos y clases de objetos que forman el directorio. Una de las novedades más importantes de Windows 2000, es la posibilidad de crear nuevas clases de objetos o modificar clases existentes para adaptarlo a necesidades propias de la empresa.

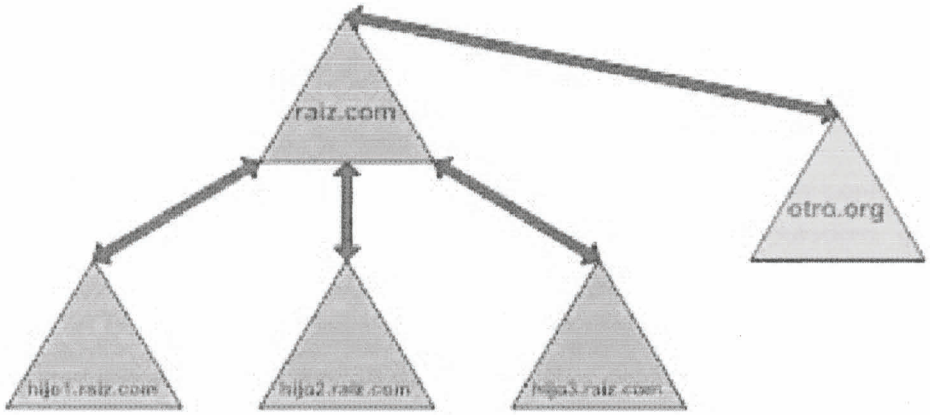
El Catálogo Global es un rol adicional que cumplen uno o más Controladores de Dominio en la estructura. Por omisión existe sólo uno pero un administrador puede (y debería) nombrar a por lo menos otro Controlador de Dominio. Los Controladores de Dominio nombrados Catálogo Global, reciben una réplica parcial, de todos los objetos del directorio. Se utilizan durante el inicio de sesión y cuando se hacen búsquedas de objetos en todo el directorio

Detalles importantes a tener en cuenta, es que esta estructura se crea "de arriba hacia abajo", es decir, primero debemos crear el dominio raíz del árbol, a partir de cuyo establecimiento se pueden crear los que "cuelgan" del mismo. Además el dominio raíz tiene características particulares que no tiene ningún otro dominio, entre otras, el dominio raíz tiene el grupo con privilegios para modificar el esquema,

y es el único dominio que tiene un grupo capaz de efectuar configuraciones que afectan a todo el directorio.

Esta estructura de árbol seguramente será suficiente para la mayoría de los casos, pero si se diera el caso de no poder mantener la continuidad en el espacio de nombres, como podría ser el caso de la fusión de empresas en donde se desee preservar el nombre de cada una, la solución sería armar un Bosque (Forest).

Un Bosque comparte las mismas características que el Árbol, salvo que el espacio de nombres no es contiguo.



Esta característica, como mencionamos puede ser útil en el caso de la fusión de 2 o más empresas preservando su identidad en el nombre de dominio. Aunque debemos tener en cuenta algo muy importante, se construye igual al árbol, esto es, a partir del dominio raíz es posible crear un Árbol o un Bosque. Pero no se pueden unir 2 Bosques ya establecidos. Hay un único dominio raíz que es el primero

que se instala. Esto podría crear escenarios complejos en el caso de fusión de empresas que ya establecieron sus dominios con Windows 2000. No es imposible, pero se debería llevar a cabo un proceso de reestructuración de dominios que es mucho más complejo. Para estos casos hay herramientas gratis de Microsoft ADMT y pagas de terceros. Es importante que recordemos que cualquiera sea la estructura de dominios que utilicemos, sea Bosque o Árbol, hay un único dominio raíz (el primero creado). En el caso de utilizar un único dominio, éste es el dominio raíz.

Hasta ahora describimos las opciones "hacia fuera" que hacen a la escalabilidad con ambientes de múltiples dominios, pero también tenemos estructura jerárquica "hacia adentro", esto es, dentro de cada dominio.

Al crear un dominio, el sistema crea una serie de contenedores predefinidos, y el administrador puede, y debería, crear una estructura jerárquica que facilite la administración. Esto es debería crear una estructura de contenedores, llamados Unidades Organizativas, que se adapte al entorno de trabajo y administración.

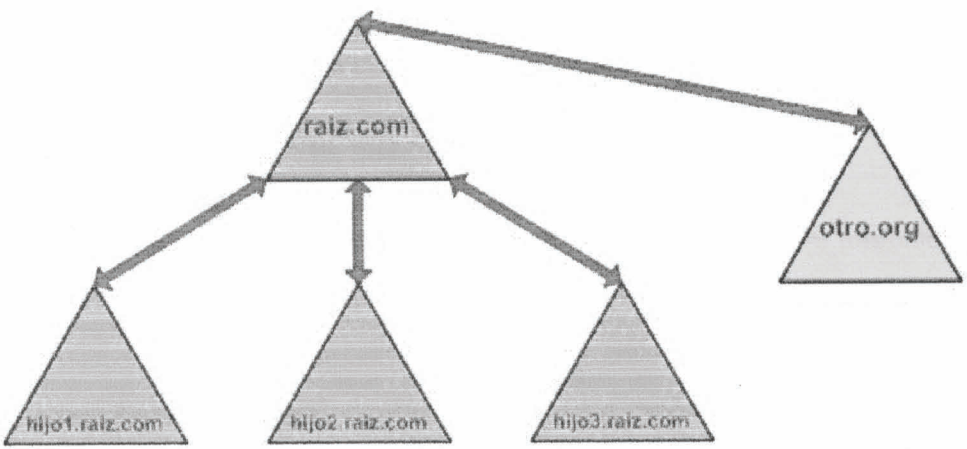
Las Unidades Organizativas son contenedores, es decir, que pueden contener otros objetos, como ser otras Unidades Organizativas, cuentas de Usuario y de Computadora, grupos, carpetas compartidas e impresoras. El concepto de contenedor es diferente del de grupo, ya que este último en realidad no es un contenedor. Un grupo contiene referencias (punteros) al objeto que contiene. En cambio un contenedor realmente lo contiene. Si borramos una Unidad Organizativa también borramos todo lo que contiene.

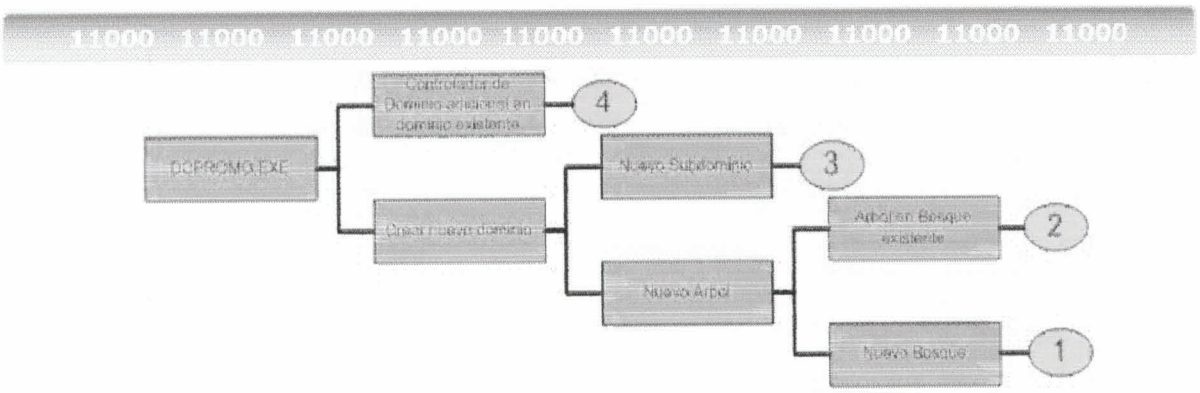
Un tema importante a tener en cuenta es que siempre que creamos un dominio, éste se instala en Modo Mixto ¿Qué significa esto? esto es, que se instala en un modo que es compatible con Controladores de Dominio Windows NT 4.0, lo cual en algunos casos es una ventaja, pero que no permite utilizar la nueva funcionalidad al 100%. El administrador deberá manualmente, cuando sea apropiado, cambiar el dominio a Modo Nativo.

La condición necesaria y suficiente para poder cambiar el dominio a Modo Nativo es que **todos los Controladores de Dominio, en el dominio, deben ser Windows 2000.** No los clientes, que pueden ser Windows en cualquiera de sus versiones.

Mientras el dominio esté en Modo Mixto, no se pueden aprovechar algunas ventajas del nuevo directorio, ya que no se puede replicar a un BDC Windows NT 4.0 elementos que éste no sepa utilizar, como podrían ser los grupos de tipo Universal, relaciones de confianza transitivas, etc.

Volvamos al asistente para instalar el servicio de directorio (DCPROMO.EXE). Este nos dará un cuadro de bienvenida y luego ofrecerá las siguientes alternativas:





Creación Del Dominio Raíz (1)

Es lo primero a crear. Debemos elegir: Crear nuevo dominio, Nuevo árbol, Nuevo Bosque. Para este caso debemos ser administradores del Server donde lo ejecutemos.

Creación De Un Nuevo Árbol En Bosque Existente (2)

Debemos elegir: Crear nuevo dominio, Nuevo Árbol, Árbol en Bosque existente. En este caso además de ser administrador del Server nos pedirá las credenciales de un usuario con poderes sobre todo el Bosque (Enterprise Admins)

Creación de un Subdominio (3)

Debemos elegir: Crear nuevo dominio, Nuevo subdominio. En este caso además de ser administrador del Server nos pedirá las credenciales de un usuario con poderes sobre todo el Bosque (Enterprise Admins)

Agregar Un Controlador De Dominio En Un Dominio Existente (4)

Debemos elegir: Controlador de Dominio en dominio existente. En este caso además de ser administrador del Server nos pedirá las credenciales de un administrador del dominio al cual deseamos agregar el controlador de dominio.

Remoción De Active Directory

Si ejecutáramos DCPROMO.EXE en un Server que ya es controlador de dominio, nos ofrecerá como única opción desinstalar Active Directory de ese Server, pidiéndonos por supuesto las credenciales apropiadas.

Estructura Física

Una de las novedades importantes de Windows 2000 en comparación con Windows NT 4.0 es que ahora el sistema es consciente que existe una infraestructura física de red. Todos los que hemos trabajado en ambiente Windows NT 4.0 en redes medianas o grandes con enlaces WAN en algún momento hemos sentido sus efectos. Cuando un cliente buscaba un servicio de red y había varios Servers que lo proveían, consideraba que el mejor era el que respondía primero, sin importarle cuán lejos estaba.

En cambio a partir de Windows 2000 podemos configurar de acuerdo a la estructura física real de nuestra red, para que los clientes utilicen los Servers que se encuentran más cerca. Por más cerca nos referimos a Servers en la misma LAN y no en redes remotas.

Una de las herramientas administrativas provista al instalar Active Directory, permite crear Sitios, identificar las subredes que están en cada uno, definir los enlaces entre sitios y además podemos definir el protocolo de replicación a utilizar.

Primero debemos definir que es un Sitio, no sólo por que es importante para el diseño físico, sino porque Microsoft en diferentes productos usa distintas definiciones. Se ha comprometido a que toda su línea de productos utilizará la definición de Windows 2000.

Un Sitio es un conjunto de subredes "bien conectadas" ¿qué significa bien conectadas? conectividad permanente, confiable, barata y con suficiente ancho de banda. ¿Doy una definición más práctica? una o más LANs conectadas directamente.

Por eso cuando definimos un Sitio, el paso más importante es definir que subredes IP están en el Sitio. De esa forma cada cliente aprenderá dónde se encuentra y cuando busque servicios los buscará primero en el Sitio propio. El sistema crea un Sitio por omisión que originalmente contiene todas las subredes, y por lo tanto contendrá a todos los Servers y clientes.

Luego deberemos definir los Enlaces que conectan los sitios. Estos deben incluir por lo menos dos sitios y deben reflejar nuestra topología de red. Por ejemplo si cada sucursal está conectada a la oficina central, deberemos definir un sitio para esta oficina central y uno para cada sucursal, a partir de lo cual crearemos los enlaces que unen cada sucursal con la central.

En estos Enlaces podremos definir: la frecuencia de replicación, días y horarios que se puede utilizar, y además un costo, que es un valor de preferencia. Si existieran varios caminos para replicar el sistema elegirá el de menor costo.

En cada enlace podremos definir el protocolo que se utilizará: RPC sobre IP, o SMTP.

Lo importante a tener en cuenta es que al ser el sistema consciente de la estructura física, tratará de aprovecharla al máximo, sea cuando los clientes buscan los servicios de red, como para la replicación de la información entre los controladores de dominio.

Conclusiones

Debido a que en la informática lo elemental es siempre "información" sin descuidar la parte humana, hardware y software, sino mas bien manteniendo una equidad. Me es muy importante participar elaborando este trabajo de investigación en el cual incluyo temas que me servirán para un correcta planeación y estandarización de recursos, con mis principios, dentro de aspectos laborales; Independientemente de los cambios en las versiones de Windows y Aplicaciones robustas que a ellos los complementen.

Este trabajo de investigación me permitió ampliar y reafirmar algunos sectores básicos en la Seguridad de Redes, comenzando por crear una cultura diferente entre los miembros de la red; conocer las limitaciones y responsabilidades para cada usuario, delegando accesos a la información y recursos con un análisis de minimización de errores posibles.

Analizando un aspecto dentro de casi cualquier red en nuestros días es el Internet como un medio electrónico informático que esta muy masificado en nuestros días tanto a nivel mundial como en México en diferentes áreas:

Gobierno
Educación e Investigación
Salud
Comercio / Industria

Esto nos da una idea de cuanta gente puede ocupar nuestros servicios para comunicarse de forma barata, sencilla y la mejor seguridad posible (debido a la gran cantidad preocupantes de ataques) para cada tipo de necesidad que seamos contratados, esto quiere decir que en poco tiempo estaremos abarcando casi cualquier área.

La seguridad es básica, Active Directory me parece una herramienta muy útil ya que permite organizar, administrar y controlar desde un punto de los recursos de cualquier red. Y si a esto le añadimos que puedan los usuarios entrar en dicha red con privilegios específicos, hace a este sistema aun más fuerte, ya que los usuarios solo realizan las actividades a las cuales fueron destinados.

El sistema seria básicamente completo (seguro) trabajando integralmente con cada miembro de la organización e utilizando de manera adecuada cada recurso de nuestro entorno. (Físico o Lógico)

Entonces acabo por resumir:

La seguridad es un proceso, una especificación, no un producto.

Sino se define un estándar de seguridad, se puede estar dando simples "*golpes al aire*"

Glosario

DARPA (DEFENSE ADVANCED RESEARCH PROJECTS AGENCY)

CERT (COMPUTER EMERGENCY RESPONSE TEAM)

DLLS (DYMANIC LINK LIBRARIES)

I+D (UNIVERSIDADES, CENTROS DE INVESTIGACIÓN...)

TCP/IP (TRANSFER COMMUNICATION PROTOCOL / INTERNET PROTOCOL)

LLC (LOGICAL LINK CONTROL).

IEEE (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS)

WAN (WIDE AREA NETWORKS).

HCL (HARDWARE COMPATIBILITY LIST)

DNS (DOMAIN NAME SYSTEM)

ISO (INTERNATIONAL STANDARDS ORGANIZATION)

OSI (OPEN SYSTEM INTERCONNECTION)

MMC (MICROSOFT MANAGEMENT CONSOLE)

ADMT (ACTIVE DIRECTORY MIGRATION TOOL)

NIC (NETWORK INTERFACE CARDS)

M.I.T. (MASSACHUSSETTS INSTITUTE OF TECHNOLOGY)

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL).

RFC (REQUEST FOR COMMENTS)

KDC (KERBEROS KEY DISTRIBUTION CENTER)

AD (ACTIVE DIRECTORY)

OSF/DCE (DISTRIBUTED COMPUTING ENVIRONMENT).

AS (AUTHENTICATION SERVICE)

TGS (TICKET GRANTING SERVICE).

SAP (SAP, SERVICE ACCESS POINTS).

BDC (BACKUP DOMAIN CONTROLLER)

Bibliografía

TCP/IP NETWORK ADMINISTRATION, Craig Hunt, O'Reilly & Associates, 1993.

REDES DE COMPUTADORAS, (3ª edición), Andrew S. Tanenbaum, Prentice-Hall, 1997.

KERBEROS

S.P. Miller, B.C. Neuman, J.I. Schiller, and J.H. Saltzer.

Kerberos Authentication and Authorization System.

In *Project Athena Technical Plan*, chapter E.2.1. Massachusetts Institute of Technology, Diciembre 1987.

MICROSOFT EXCHANGE SERVER 2000 EDICION ESPECIAL

Joshi, Kent; Software Spectrum (Prentice Hall)

REDES CON MICROSOFT TCP IP 3ª

Heywood, Drew (Prentice Hall)

TCP IP

John Ray (Prentice Hall)

S.P. Miller, B.C. Neuman, J.I. Schiller, and J.H. Saltzer.

Kerberos Authentication and Authorization System.

In *Project Athena Technical Plan*, chapter E.2.1. Massachusetts Institute of Technology, Diciembre 1987.

Active directory http://www.mug.org.ar/Infraestructura/ArticInfraestructura