UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

# MONITOREO DE LOS SERVICIOS DE INTERNET PARA EL ASEGURAMIENTO DE LA CALIDAD

T E S I S

PARA OBTENER EL GRADO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

CARLOS ALBERTO MÁRQUEZ OROZCO

DIRECTOR: MSC. MARCO ANTONIO VIGUERAS VILLASEÑOR.

CIUDAD UNIVERSITARIA, MÉXICO, D.F. 2004

**CONTENIDO** **Página**

# Índice de Figuras

## Abstract

This document shows an analysis of Internet Services in Mexico that will help to estimate the Quality of Service (QoS) that the final user is receiving.

The monitoring of the sites was done by Firehunter platform of Agilent Technologies. It was done thanks to the donation of this software by this company to Universidad Nacional Autónoma de México and this software is being used in the Engineering School Laboratories of this Institution.

The monitoring consisted on sixteen sites divided into four categories: universities, government, browsers and commercial sites.

The selection of these sites was done through the information given by one of the most important Internet Service providers in Mexico, who provides a DNS server list of the most visited sites during April in 2004.

This monitoring consisted on adding a HTTP server for each one of the selected sites an added it to a Firehunter model. The result measurements were:

- Availability
- Total Response Time
- Test completed
- DNS Time
- TCP Connect Time
- Redirect Time
- Server Response Time
- Data Transfer Time
- Data Transfer Rate

The most significative results were presented in the availability and Response Time regarding Service Level Agreements (SLA) used in a standard world.

In this thesis we can see a detailed monitoring of each one of the sites as well as the results obtained graphically, so this will help to have a general overview of the actual conditions of Internet services in Mexico.

# CAPÍTULO I
# Introducción

## I.1 Planteamiento

Debido al auge que ha tenido en los últimos años Internet y al creciente uso de los servicios del mismo, los proveedores de servicios de Internet (ISPs) se ven en la necesidad de mejorar su servicio, para ello, es necesario monitorear continuamente que dichos servicios se den con una calidad adecuada y que satisfagan las necesidades de los usuarios, desde acceso personal hasta aplicaciones avanzadas para empresas.
Internet se ha convertido en elemento de comunicación esencial, y como herramienta que facilita las transacciones entre empresas, es el elemento base de los nuevos modelos de negocios.

El acceso a Internet se está convirtiendo en una cuestión fundamental en cualquier entorno profesional de nuestra economía. Es cada vez más importante, por lo tanto, disponer de un servicio de acceso a la red de calidad. Es difícil evaluar la calidad que nos proporciona nuestro proveedor ISP (Internet Service Provider) debido a los numerosos factores que intervienen en la prestación del servicio. Sin embargo, sí se puede hacer un análisis comparativo que nos permita evaluar el servicio que recibimos de un proveedor frente a otro en algunos entornos específicos.

Cada vez más ISPs están buscando herramientas que provean datos basados en el usuario y el uso que se les da, con el fin de servir mejor a sus usuarios y aprovechar plenamente el valor de sus inversiones en redes.

# Capitulo I

El objetivo preciso de elaborar el proyecto de tesis, es lograr estimar la calidad de servicio (QoS) de los servicios de Internet, monitoreando algunos de ellos para encontrar niveles de servicio adecuados que satisfagan las necesidades de los usuarios; aportando información relevante para lograrla, mediante gráficos, establecer niveles de servicio, notificaciones vía mail, alarmas en pantalla, apoyándonos en una metodología eficiente para estimar dicha calidad, utilizando una herramienta que nos auxiliará en el monitoreo de los servicios.

Existen varias interfaces que ayudan a monitorear los servicios de Internet, en este caso se escogió Firehunter de Agilent Technologies, una herramienta que cuenta con muchas ventajas en comparación con sus similares (Tivoli, Atentus, entre otros). Muchas empresas dejan la responsabilidad de la calidad a Firehunter de Agilent.

El Sistema de Monitoreo de Servicio Internet, se puede definir en forma general, como un sistema de registro, recepción, almacenamiento y procesamiento de información. Este sistema busca responder a la necesidad de contar con información sobre los servicios de Internet, para lo cual recoge los datos necesarios que dan cuenta de la calidad y uso de Internet, en forma transparente y automática.

Con los datos, se puede generar una gran cantidad de información útil para determinar, principalmente, la calidad de servicio de Internet entregado por el ISP, pero además es muy importante considerar los siguientes factores que intervienen en la calidad.

**1. Disponibilidad**. Se refiere al nivel de disponibilidad del servicio y de Internet. Considera los intentos que deben realizar los usuarios antes de lograr conectarse; de las veces que se conectan, ¿qué tantas veces logran acceder a Internet sin problemas (sitios nacionales e internacionales)?.

**2. Conectividad.** Se refiere a la frecuencia y tiempo de conexión a Internet en los establecimientos. Considera la velocidad con la que logra conectarse un usuario al ISP y la velocidad de conexión con sitios nacionales e internacionales.

**3. Confiabilidad.** Se refiere a las expectativas temporales de mantener activa una conexión. Es decir, una vez que un usuario logra conectarse, ¿puede confiar que seguirá conectado

todo el tiempo que estime necesario, o sufrirá cortes inesperados?, ¿existe pérdida de información en las transmisiones?.

## I.2 Objetivos

- Desarrollar una metodología adecuada, logrando estimar la QoS (Calidad de Servicio) de los servicios de Internet, para que dichos servicios lleguen al usuario final con una calidad aceptable.

- Estimar QoS de los servicios de Internet, haciendo un monitoreo en tiempo real de los servicios que prestan los ISPs como son: HTTP, tiempo de DNS, disponibilidad, tiempo total de respuesta, entre otros.

- Ofrecer resultados que permitan mejorar la satisfacción del usuario, entregando los servicios de Internet con mayor calidad, fijando niveles de servicio adecuados para cumplir con lo requerido por el usuario.

- Ofrecer parámetros que permitan detectar, aislar y corregir errores rápidamente, utilizando umbrales basados en los requerimientos de los usuarios.

## I.3 Justificación

Internet se ha convertido en uno de los canales más importantes para acceder a la información o a los servicios de una empresa; además de una presentación agradable y unos contenidos adecuados, la calidad de servicio (QoS) de un sitio en la red es un aspecto cada vez tomado más en cuenta por el usuario.

Esta calidad de servicio puede ser analizada desde dos enfoques:

- Un *enfoque cualitativo,* que engloba desde el diseño de la página, pasando por la facilidad de navegación hasta el uso (localización de los servicios relevantes, complejidad a la hora de realizar una operación, etc.).

- Un *enfoque cuantitativo*, que incluiría todas las variables susceptibles a ser medidas detalladamente: los tiempos de las distintas fases para la conexión, la disponibilidad del servicio (entendida como el porcentaje de conexiones con éxito frente a las fallidas), la capacidad de acceso a páginas, el tiempo necesario para realizar una transacción.

Un servicio es rápido, ágil y de calidad si lo es más que el de la competencia. Por ello, el seguimiento periódico de los servicios en sitios Web, debe desarrollarse de manera comparativa.

El presente trabajo de investigación, nos aporta la solución para el análisis de la calidad de servicio de los sitios Web, desde un punto de vista cuantitativo, utilizando herramientas que soportan todos los tipos de medidas relevantes relacionados con la conexión y el acceso a los servicios Web que deseamos monitorear.

Las medidas se realizan mediante accesos permanentes con una periodicidad configurable de acuerdo a las necesidades de cada usuario. Haciendo un análisis estadístico de los datos.

Estos datos pueden mostrarse de forma sencilla, se pueden obtener gráficas de tiempos de respuesta, disponibilidad, etc.

En la recomendación E-800 de la ITU (Internacional Telecommunication Union)[1] se define la QoS como "el efecto colectivo del rendimiento de un servicio que determine el grado de satisfacción del usuario de dicho servicio". Es decir, a la hora de introducir el concepto de QoS se debe reflejar el punto de vista del usuario del servicio, ya que la QoS es claramente una propiedad orientada al usuario del servicio.

En términos cualitativos la calidad está directamente relacionada con la respuesta percibida por los usuarios finales cuando acceden a la red y por el grado de satisfacción de los mismos; mientras que en términos cuantitativos se refleja en una serie de parámetros que se pueden medir y ajustar convenientemente para proporcionar un grado de servicio satisfactorio.

Normalmente se habla de QoS como si se tratase de un dato conocido o, por lo menos, de fácil obtención; sin embargo en muchos casos tiene significados diferentes, para los distintos actores. Básicamente QoS tiene cuatro variantes [1]:

- QoS que el usuario desea
- QoS que el proveedor ofrece
- QoS que el proveedor consigue realmente
- QoS que el Usuario percibe finalmente

En cualquiera de ellas existen parámetros conocidos susceptibles a ser monitoreados.

Es necesario no solo disponer de herramientas que nos faciliten la obtención de medidas para estimar la calidad de servicio, sino también encontrar una metodología adecuada que nos ayude a interpretar los resultados de forma correcta, del análisis de la información de las medidas realizadas, se pueden detectar problemas y proceder a su solución.

[1] www.qos.unam.mx

El objetivo final debe ser proporcionar la calidad de servicio a sus usuarios en función de sus necesidades.

Para evaluar la calidad de servicio de los proveedores en el acceso a Internet, es necesario desarrollar un método de pruebas que se base en tres pilares fundamentalmente [2]:

**Objetividad:** Evitar las decisiones que pueden ser parciales. Algunos análisis se restringen a medir parámetros específicos que favorecen a unos ISPs frente a otros.

**Intensidad de las Pruebas:** Establecer un mecanismo de pruebas estadísticamente suficiente, para sacar conclusiones comparativas en diferentes franjas horarias y con diferentes destinos.

**Fiabilidad:** Hacer pruebas automatizadas utilizando métodos y herramientas que estén específicamente diseñadas para realizar medidas de calidad de servicio adecuadas para ello.

## I.4 Alcances

El monitorear los servicios de Internet que prestan los ISPs, tiene como finalidad el estimar la calidad de servicio que está recibiendo el usuario final.
Las necesidades de los usuarios de Internet han cambiado, ahora éstas se centran en tres aspectos principalmente, un buen servicio de atención al usuario, una buena comunicación punto a punto y un buen precio.

Los usuarios de Internet empiezan a ser concientes de la importancia que tiene el saber elegir adecuadamente a su proveedor de servicios de Internet, ya no solo se fijan en el precio, sino también importa el servicio que obtienen y la capacidad de conectividad que se vea reflejada en la reducción de tiempos de acceso a los servicios de usuario finales.

Por ello es necesario el contar con herramientas que nos ayuden a monitorear los servicios de Internet, para lograr estimar la calidad con que están llegando al usuario final como lo es Firehunter de Agilent.

Como el universo de Internet es muy amplio y debido a que sería imposible abarcarlo; en el presente trabajo se plantea monitorear las páginas más visitadas en Internet, que son las que están expuestas a sufrir de tráfico intenso en la red además de que son un blanco muy buscado por los diferentes tipos de intrusos, debido a que éstos buscan dañar las páginas más solicitadas por los usuarios para lograr hacerse de fama.

Estas son algunas de las razones del porqué muchas veces este tipo de páginas brinda un servicio de poca calidad; por esto, necesitan estar constantemente monitoreadas para lograr una calidad de servicio adecuada y satisfacer los niveles de servicio acordados con el usuario. Esto nos podrá dar un panorama más amplio de cómo mejorar los servicios de Internet y entregarlos con calidad aceptable.

## I.5 Estructura del Documento

En el capítulo uno se plantean los objetivos fundamentales que tiene el presente trabajo de tesis, fijando metas a cumplir y esbozando la justificación adecuada para cada uno de los objetivos planteados. Todo esto con el fin de alcanzar las metas planteadas.

En el capítulo dos se fundamentan los conocimientos teóricos necesarios para entender el funcionamiento actual de los servicios de Internet que prestan los ISPs, desde los principios de las redes de comunicaciones de datos, pasando por las topologías, protocolos, arquitecturas y modelos utilizados en las redes de datos actuales, hasta llegar a una breve explicación de los principales servicios de Internet.

El capítulo tres muestra la importancia de la seguridad en redes y plantea la estrecha relación que existe entre ésta y la calidad de servicio (QoS). Así como los principales tipos de ataques y las estrategias a seguir para los diferentes tipos de violaciones a la seguridad.

La calidad de servicio es punto principal del presente trabajo de investigación. En el capítulo cuatro se amplía más este concepto, desde una definición general de calidad, hasta llegar a la definición de aseguramiento de la calidad para concluir en la satisfacción del usuario final.

El capítulo cinco plantea la necesidad de monitorear los servicios de Internet para estimar la calidad con que están llegando al usuario final. En dicho capítulo, se hace mención de la plataforma utilizada para éste monitoreo, ampliando su funcionamiento en el apéndice B de este mismo trabajo.

También se muestran los resultados obtenidos al monitorear dieciséis páginas de Internet divididas en cuatro categorías, sometidas todas éstas al mismo número de pruebas, arrojando resultados de forma gráfica que ayudan a estimar la calidad de servicio que está recibiendo el usuario final.

En el último capítulo del presente trabajo, se exponen las conclusiones a las que se llegaron después de analizar los resultados obtenidos en el capítulo anterior, haciendo una comparación entre los objetivos trazados en el capítulo uno y los resultados reales.

# CAPÍTULO II
# Antecedentes Teóricos

## II.1 Redes de Comunicaciones de Datos

El constante desarrollo de la computación y su integración con las telecomunicaciones han propiciado el desarrollo de nuevas formas de comunicación como lo son las *Redes de Comunicaciones de Datos*. El desarrollo de estas redes, trajo como consecuencia el establecer una conexión entre ellas, hasta llegar a lo que hoy conocemos como la red de redes, *Internet;* gracias a Internet, una computadora puede compartir información y recursos con otra situada en regiones distantes del planeta.

Una Red de Datos es un conjunto de computadoras, conectadas entre sí con el fin de compartir sus recursos (por ejemplo, impresoras) e información. La conexión puede ser directa, es decir por cable o inalámbrica.

Según el espacio que abarquen o la distancia a la que se encuentren las computadoras que integran la red, suele distinguirse entre LAN por sus siglas en inglés (Local Area Network), que significa, Red de Área Local y WAN (Wide Area Network) Red de Área Amplia. No existen límites claros entre un tamaño de red y otro, y de hecho hay autores como Hahn, que en su libro, *Internet Manual de Referencia* [5] distingue un tamaño intermedio (MAN, Metropolitan Area Network).

El crecimiento de las redes locales en los ochenta, hizo que cambiara nuestra forma de comunicarnos con las computadoras y la forma en que las computadoras se comunican entre sí.

La importancia de las redes locales reside en principio, a que se pueden conectar un número pequeño de computadoras, y que puede ser ampliado, a medida de que crezcan las necesidades.

La comunicación entre dos computadoras puede efectuarse mediante tres tipos de conexión [1]:

1. ***Conexión directa****:* Este tipo de conexión se le conoce como transferencia de datos on–line. Las informaciones digitales codificadas fluyen directamente desde una computadora hacia otra, sin ser transferidas a ningún soporte intermedio. Los datos pueden viajar a través de una interfaz serie o paralelo, formada simplemente por una conexión física adecuada, como por ejemplo un cable.
2. ***Conexión a media distancia****:* Es conocida como conexión off-line. La información digital codificada se graba en un soporte magnético y se envía al centro de proceso de datos, donde será tratada por una unidad central u host.
3. ***Conexión a gran distancia***: Con redes de transferencia de datos, de interfaces serie y módems se consigue transferencia de información a grandes distancias.

## II.1.1 Evolución de las redes de Datos

Recientemente para dar solución a la necesidad de hacer más eficiente el uso de los recursos de cómputo en las organizaciones surgen las redes de computadoras.

Estas surgen a partir de la necesidad que se tenía de compartir recursos distribuidos, dichas redes se convirtieron en el vehículo que permitió el intercambio de información.

Una red de computadoras es la interconexión física y lógica entre puntos terminales llamados nodos de la red, cuyo objetivo es compartir recursos e intercambiar información, el

enlace de las máquinas se realiza primero a través de un enlace físico y posteriormente a través de un medio llamado protocolo, que más adelante mencionaremos [2].

***Clasificación de las Redes***

Una clasificación de las redes, se puede hacer de acuerdo a su tamaño físico, y en este caso tenemos tres categorías:

***LAN***

Las redes cuyas comunicaciones están limitadas en un área geográfica determinada, generalmente un edificio u oficina, recibe el nombre de red de área local (LAN), se puede decir que su extensión puede darse hasta 1km o contener menos de 1000 nodos. [1]
Puede ser desde dos computadoras, hasta cientos de ellas. Todas se conectan entre sí por varios medios y topologías.

La LAN es un sistema de comunicaciones de alta velocidad que conecta microcomputadoras o PC's y/o periféricos que se encuentran cercanos.
Una LAN consta de hardware y software de red, que sirve para conectar las computadoras que están aisladas. Una LAN brinda la posibilidad de que computadoras compartan entre ellas, programas, información y recursos; como unidades de disco, archivos, impresoras, etc.

*Características de las LAN:* El radio que abarca es poco, por ejemplo edificios o campus universitarios, un complejo industrial, etc. Utilizan un medio privado de comunicación. La velocidad de transmisión es de varios millones de bps. Las velocidades habituales van desde 4Mbits en redes Token Ring hasta grandes velocidades como en las redes Gigabit Ethernet. Puede atender a cientos de dispositivos muy distintos entre sí como por ejemplo: impresoras, computadoras, discos, teléfonos, módems, etc.

[1] Redes de Area Local (LAN) Autor: Neil Jenkins. Ed. Prentice Hall 1998.

***MAN***

Se le conocen como redes de área metropolitana por sus siglas en inglés (Metropolitan Area Network); son redes de computadoras de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Es una red compuesta por varias redes LAN interconectadas y se encuentran en un área geográfica amplia. Estas LANs que componen la WAN, se encuentran interconectadas por medio de líneas de teléfono, fibra óptica, o por enlaces aéreos como satélites [7].

***WAN***

Las redes que se extienden a lo largo de un país, continente o bien en el mundo entero. Reciben el nombre de redes de área amplia (WAN). Entre las WANs más grandes se encuentran: La de AT&T, Novell y Microsoft por mencionar algunas.

Las WAN tienen un tamaño superior a las redes MAN, consisten en una colección de host o de redes LANs conectadas por una subred. Esta subred esta formada por una serie de líneas de transmisión interconectadas por medio de ruteadores. Su tamaño puede ser desde 10,000 Km. en adelante y su ejemplo más claro es Internet "la red de redes" [7].

## II.1.2 Beneficios de las Redes Locales

El tener la posibilidad de conectar un cierto número de computadoras entre sí, a través de algún medio de transmisión, trae consigo múltiples beneficios como los que a continuación se mencionan.

- La información de cualquier red es un recurso corporativo, es decir, todos hacen uso de la información y la utilizan, acorde al nivel de acceso permitido, se emplea para un fin productivo dentro de una organización.
- Por otro lado si miramos a nuestro alrededor todas las aplicaciones que utilizamos a diario para la realización de nuestro trabajo y el correcto funcionamiento y operación de la organización depende 100% de las comunicaciones.
- Otro punto, las comunicaciones, se han convertido en este siglo en una herramienta fundamental para las Industrias y empresas internacionales, cada día, las transacciones de operaciones son mayores y requieren de mayor agilidad y confiabilidad. La comodidad de realizar múltiples aplicaciones dentro de la empresa o del hogar en aras de buscar objetivos muy particulares de estos segmentos, ha dado pie a que las comunicaciones evolucionen vertiginosamente y que dependamos más de éstas.
- Integración de varios puntos en un mismo enlace.
- Posibilidad de Crecimiento hacia otros puntos para integración en la misma red.
- Una LAN da la posibilidad de que las computadoras compartan entre ellas programas, información, recursos entre otros. La máquina conectada (PC) cambia continuamente, así que permite que sea innovador este proceso y que se incremente sus recursos y capacidades.
- Otro de los beneficios que trae consigo el conectar las máquinas en red, y uno en el que las empresas ponen más cuidado y del cual están más preocupados, es el económico, el poder conectar sus computadoras en red permite compartir los recursos y evita gastos excesivos en hardware adicional como impresoras, plotters, etc.

## II.2 Topologías

Se llama topología de una Red al patrón de conexión entre sus nodos, es decir, a la forma en que están interconectados los distintos nodos que la forman. Los Criterios a la hora de elegir

una topología, en general, buscan elegir los caminos más simples entre un nodo y los demás. Otro criterio determinante es la tolerancia a fallos o facilidad de localización de éstos. También tenemos que tener en cuenta la facilidad de instalación y reconfiguración de la Red.

Hay tres clases generales de topología utilizadas en Redes de Area Local: **Topología tipo Bus, Topología tipo Anillo y la Topología Estrella**. A partir de ellas derivan otras que reciben nombres distintos dependiendo de las técnicas que se utilicen para acceder a la red o para aumentar su tamaño como la malla, árbol, etc.

***Topología Bus***

En una topología de bus, cada computadora esta conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de la misma. El cable puede ir por el piso, por las paredes, por el techo o puede ser una combinación de los anteriores, siempre y cuando el cable sea un segmento continuo.

La topología bus tiene todos sus nodos conectados a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada nodo esta conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable puede hacer que más de un nodo quede desconectado.

Una Red en forma de Bus es un camino de comunicación bidireccional con puntos de terminación bien definidos. Cuando un nodo trasmite, la señal se propaga a ambos lados del emisor hacia todos los nodos conectados al Bus hasta llegar a las terminaciones del mismo. Así, cuando un nodo trasmite su mensaje alcanza a todos los nodos, por esto el Bus recibe el nombre de canal de difusión.

Otra propiedad interesante es que el Bus actúa como medio pasivo y por lo tanto, en caso de extender la longitud de la red, el mensaje no debe ser regenerado por repetidores (los cuales deben ser muy fiables para mantener el funcionamiento de la red). El fallo de cualquier nodo no impide que la red siga funcionando normalmente, lo que permite añadir o quitar nodos a la red sin interrumpir su funcionamiento [3].

La figura 2.1 muestra una arquitectura clásica de una topología de Red del tipo Bus.

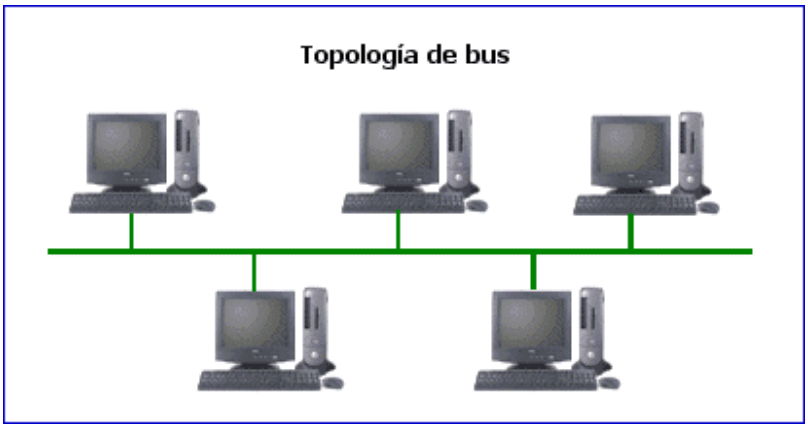


**Fig. 2.1** Diagrama de una Topología Bus.

### *Topología Anillo*

Una topología de anillo consta de varios nodos unidos formando un círculo lógico (Fig.2.2)

Los mensajes se mueven de nodo a nodo en una sola dirección. Algunas redes de anillo pueden enviar mensajes en forma bidireccional, no obstante, solo son capaces de enviar mensajes en una dirección cada vez. La topología de anillo permite verificar si se ha recibido un mensaje. Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo esta conectado solamente con dos nodos adyacentes.

Los dispositivos se conectan directamente entre sí por medio de cables. Para que la información pueda circular, cada estación debe trasferir la información a la estación adyacente.

Dependiendo del control de acceso al medio, se dan nombres distintos a esta topología: Bucle; se utiliza para designar aquellos anillos en los que el control de acceso está centralizado (una de las estaciones se encarga de controlar el acceso a la red). Anillo; se utiliza cuando el control de acceso está distribuido por toda la red. Como las características de uno y otro tipo de la red son prácticamente las mismas, se utiliza el término anillo para las dos.

En cuanto a fiabilidad, presenta características similares al Bus: la avería de una estación puede aislarse fácilmente, pero una avería en el cable inutiliza la red. Sin embargo, un problema de este tipo es más fácil de localizar, ya que el cable se encuentra físicamente dividido por las estaciones. Las redes de éste tipo, a menudo, se conectan formando topologías físicas distintas al anillo, pero conservando la estructura lógica (camino lógico unidireccional) de éste.

El protocolo de acceso al medio debe incluir mecanismos para retirar el paquete de datos de la red una vez llegado a su destino. Resumiendo, una topología en anillo no es excesivamente difícil de instalar, aunque gaste más cable que un Bus. La combinación estrella/anillo puede proporcionar una topología muy fiable sin el costo exagerado de cable como estrella pura [3].


**Fig. 2.2** Diagrama de una Topología Anillo

***Topología Estrella***

Uno de los tipos más antiguos de topologías de redes es la estrella. La cual utiliza el mismo método de envió y recepción de mensajes que el sistema telefónico, ya que todos los mensajes de una red LAN con topología en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, el cual controla el flujo de datos.

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 (Fig. 2.3). La ventaja principal es que permite que todos los nodos se comuniquen entre sí, pero existe una gran desventaja, y esta es, que si el nodo central falla, toda la red se desconecta.

Una forma de evitar un solo controlador central y además aumentar el límite de conexión de nodos, así como una mejor adaptación al entorno, sería utilizar una topología en estrella distribuida. Este tipo de topología está basada en la topología en estrella pero distribuyendo los nodos en varios controladores centrales. El inconveniente de este tipo de topología es que aumenta el número de puntos de mantenimiento [3].

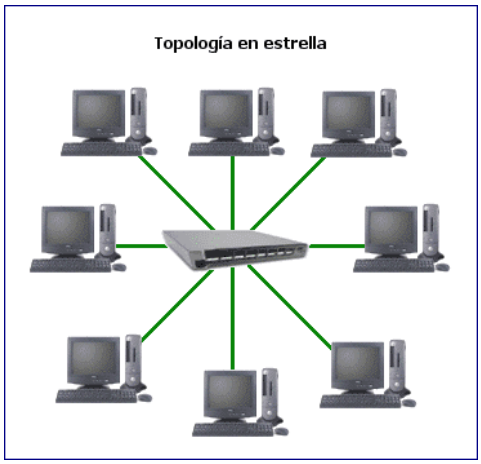


**Fig. 2.3** Diagrama de una Topología Estrella

### *Topología Malla*

En una topología de malla completa cada nodo se enlaza directamente con los demás nodos (Fig.2.4). Las ventajas son, que como todos se conectan físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar, la información puede circular por cualquiera de los demás enlaces hasta llegar al destino. Además esta topología, permite que la información circule por varias rutas a través de la red.

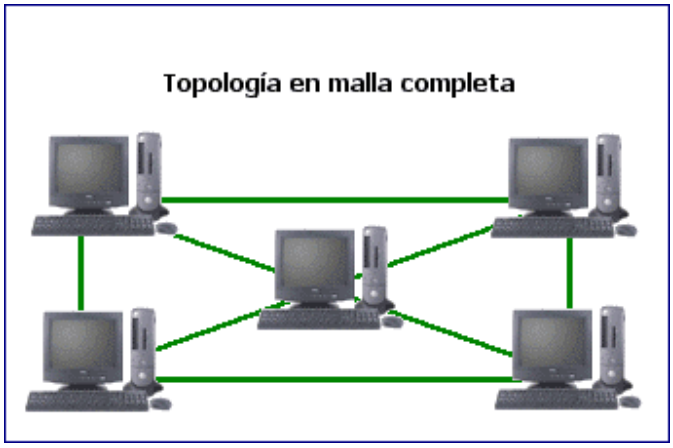


**Fig. 2.4** Topología en Malla

La desventaja principal es que esta topología funciona con una cantidad reducida 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 [3].

## II.3 Modelo OSI

Cuando las empresas intentaron comunicar redes situadas en lugares diferentes, cada una con una implementación particular, se dieron cuenta de que necesitaban salir de los sistemas de networking propietarios, optando por una arquitectura de red con un modelo común que hiciera posible interconectar varias redes sin problemas.

Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto y por lo tanto, elaboraron el modelo de referencia OSI.

OSI es un modelo de referencia de siete capas para asegurar la interconexión de “sistemas abiertos”. Fue definido por ISO (Internacional Standards Organization) en 1984. El modelo OSI (Open Systems Interconection) mostrado en la figura 2.5, describe las tareas que los “sistemas abiertos” deben realizar en términos de siete capas y especifica la funcionalidad de cada una. Sin embargo OSI no especifica como deben ser implantadas todas estas funcionalidades [1].

El modelo OSI describe el uso de los datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el más conocido y usado para describir los entornos de red.


**Fig. 2.5** Modelo OSI.

Como lo muestra la figura 2.5, las capas del modelo OSI están numeradas de abajo hacia arriba. Las funciones más básicas, como el poner los bits de datos en el cable de la red se encuentran en las primeras capas, mientras las funciones que atienden los detalles de las aplicaciones del usuario están en las últimas capas del modelo OSI.

En el modelo de referencia OSI, cada una de las capas ilustra una función de red particular. La división de la red en siete capas presenta las siguientes ventajas:

1. Divide la comunicación de red en partes más pequeñas y sencillas.
2. Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
3. Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida. Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
4. Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Una analogía del sistema de capas puede ser la forma en que una carta es enviada desde el emisor hasta el destinatario. En este proceso intervienen una serie de entidades o capas (carteros, oficinas postales, medios de transporte, etc.), cada una de las cuales realiza una

serie de funciones específicas, necesarias para el funcionamiento de las demás y para la entrega efectiva de la carta.

Podemos decir que este modelo incorpora dos formas de comunicación: Horizontal y Vertical. Cada capa del modelo se comunica con tres capas más, la inmediata superior, la inmediata inferior y la capa al mismo nivel en el otro equipo, como lo muestra la figura2.6. Aunque esto no sucede realmente así, en el modelo OSI el propósito de cada capa es proveer los servicios para la siguiente capa superior, resguardando la capa de los detalles de como los servicios son implementados realmente.

Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra computadora, cuando realmente cada capa se comunica sólo con las capas adyacentes de la misma computadora.

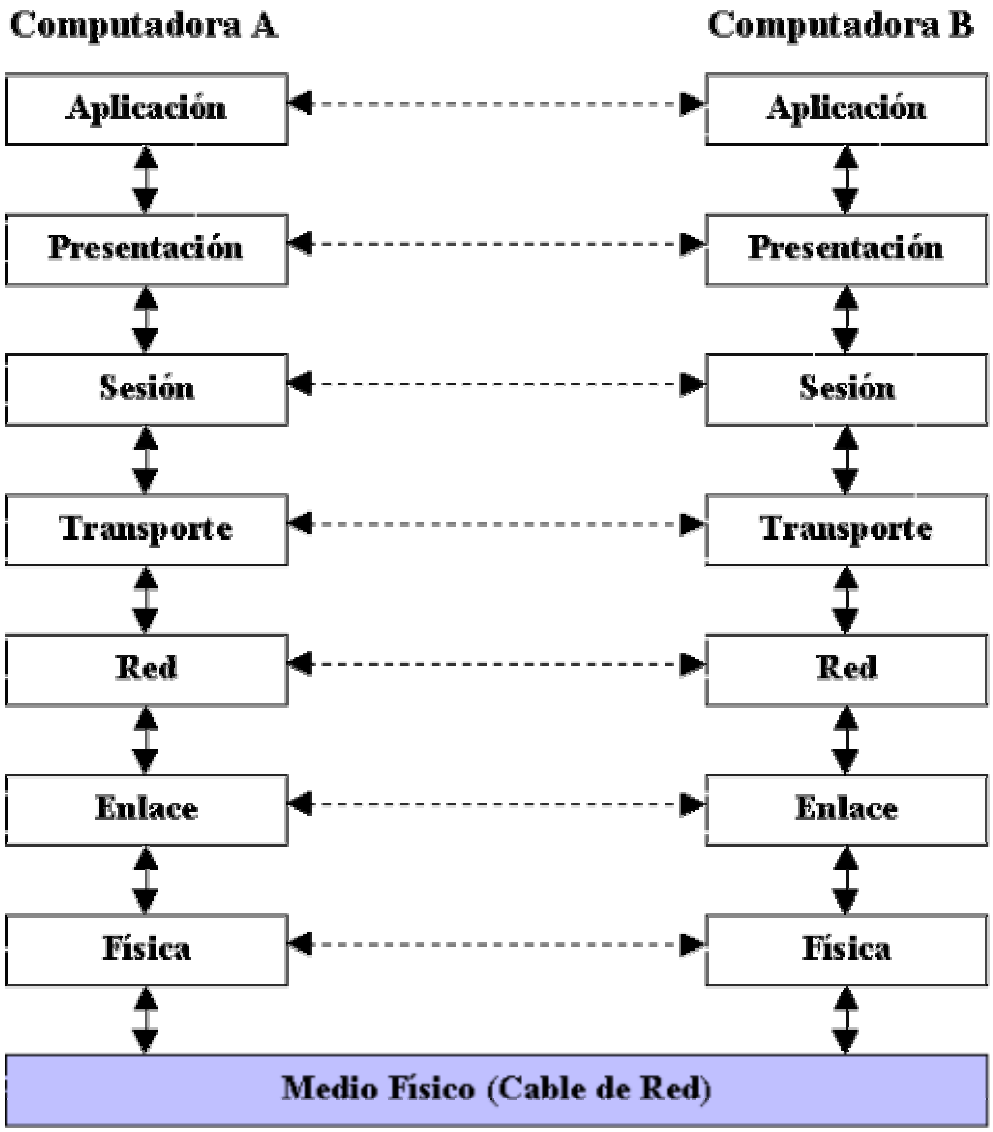


**Fig. 2.6** Comunicación entre capas del modelo OSI

***Capas del Modelo OSI***

*Física:*

La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.

La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son transmitidos [3].

Sus principales funciones las podemos resumir en:

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar voltajes y pulsos eléctricos.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

Esta capa solamente reconoce bits individuales.

*Enlace de Datos:*

La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico.

Se ocupa del direccionamiento físico, la topología de red, el acceso a la misma, la notificación de errores, la formación y entrega ordenada de datos y control de flujo.

Su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo, realizando para ello las siguientes funciones:

- Establecer los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.
- Agregar una secuencia especial de bits al principio y al final de los paquetes de datos, estructurando este flujo bajo un formato predefinido, denominado trama, que suele ser de unos cientos de bytes.
- Sincronizar el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan CRC (Códigos Cíclicos Redundantes) y envío de acuses de recibo positivo y negativo, y para evitar tramas repetidas se usan números de secuencia en ellas.
- Controlar la congestión de la red.
- Regular la velocidad de tráfico de datos.
- Controlar el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.
- Encargarse del acceso de los datos al medio (soportes físicos de la red).

*Red:*

La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de la mejor ruta para la comunicación entre máquinas que pueden estar ubicadas en redes geográficamente distintas.

Es la responsable de las funciones de conmutación y enrutamiento de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red, con objeto de determinar la ruta más adecuada.

Sus principales funciones son:

- Dividir los mensajes de la capa de transporte (segmentos) en unidades más complejas, denominadas *paquetes*, a los que asigna las direcciones lógicas de los host que se están comunicando.
- Conocer la topología de la red y manejar el caso en que la máquina origen y la máquina destino estén en redes distintas.
- Encaminar la información a través de la red en base a las direcciones del paquete, determinando los métodos de conmutación y enrutamiento a través de dispositivos intermedios (routers).
- Enviar los paquetes de nodo a nodo usando un circuito virtual o datagramas[2].
- Ensamblar los paquetes en el host destino.

En esta capa es donde trabajan los routers, dispositivos encargados de encaminar o dirigir los paquetes de datos desde el host origen hasta el host destino a través de la mejor ruta posible entre ellos.

*Transporte:*

La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión.

Para ello, divide los datos originados en el host emisor en unidades apropiadas, denominadas *segmentos*, que vuelve a reensamblar en el sistema del host receptor.

Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones de usuario, las tres capas inferiores se encargan del transporte de datos. Además, la capa de transporte es la primera que se comunica directamente con su capa par de destino, ya que la comunicación de las capas anteriores es de tipo máquina a máquina.

[2] Es una forma de mandar información por la que las partes del mensaje se envían de manera aleatoria y la máquina receptora tiene la tarea de poner las partes del mensaje recibidas en el orden correcto. – Diccionario de términos Computacionales-.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísle las capas superiores de los detalles del mismo, encargándose de conseguir una transferencia de datos segura y económica; y un transporte confiable de datos entre los nodos de la red.

Para ello, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales[3] proporcionando un servicio confiable mediante el uso de sistemas de detección y recuperación de errores de transporte.

Podemos resumir las funciones de la capa de transporte en los siguientes puntos:

- Controlar la interacción entre procesos-usuarios en las máquinas que se comunican.
- Incluir controles de integración entre usuarios de la red para prevenir pérdidas o doble procesamiento de transmisiones.
- Controlar el flujo de transacciones y el direccionamiento de procesos de máquina a procesos de usuario.
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- Aceptar los datos del nivel de sesión, fragmentándolos en unidades más pequeñas aptas para el transporte confiable, llamadas segmentos, que pasa luego a la capa de red para su envío.
- Realizar funciones de control y numeración de las unidades de información (los segmentos).
- Reensamblar los mensajes en el host destino, a partir de los segmentos que lo forman.
- Garantizar la transferencia de información a través de la red.

[3] Se conocen con el nombre de circuitos virtuales a las conexiones que se establecen dentro de una red. En ellos no existe la necesidad de tener que elegir una ruta nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico de datos posterior.- Diccionario de términos computacionales-.

*Sesión:*

La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación de dos host que se están comunicando por red organicen y sincronicen su diálogo y procedan al intercambio de datos.

Sus principales funciones son:

- Establecer, administrar y finalizar las sesiones entre dos hosts (máquinas en red) que se están comunicando.
- Si por algún motivo una sesión falla por cualquier causa ajena al usuario, restaurar la sesión a partir de un punto seguro y sin pérdida de datos o, si esto no es posible, terminar la sesión de una manera ordenada, checando y recuperando todas sus funciones, evitando así problemas en sistemas transaccionales.
- Sincronizar el diálogo entre las capas de presentación de los dos hosts y administrar su intercambio de datos, estableciendo las reglas o protocolos para el dialogo entre máquinas, regulando quien habla y por cuanto tiempo.
- Conseguir una transferencia de datos eficiente y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- Manejar *tokens*. Los tokens son objetos abstractos y únicos que se usan para controlar las acciones de los participantes en la comunicación, base de ciertos tipos de redes, como Token Ring o FDDI.
- Hacer *checkpoints,* que son puntos de recuerdo en la transferencia de datos, necesarios para la correcta recuperación de sesiones perdidas.

*Presentación:*

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo.

Su tarea principal es aislar a las capas inferiores del formato de los datos de las aplicaciones específicas, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red, entendible por todos los sistemas y apto para ser enviado por red.

Es también la responsable de la obtención y la liberalización de la conexión de sesión cuando existan varias alternativas disponibles.

Para cumplir estas funciones, la capa de presentación realiza las siguientes operaciones:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.
- Definir la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, definir el orden de transmisión y la estructura de los registros.
- Definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc).
- Dar formato a la información para visualizarla o imprimirla. Comprimir los datos si es necesario.
- Aplicar a los datos procesos criptográficos cuando sea necesario.

*Aplicación:*

La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de más alto nivel, proporcionando soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

Los procesos de las aplicaciones se comunican entre sí por medio de entidades de aplicación propias, estando éstas controladas por protocolos específicos de la capa de aplicación, que a su vez utilizan los servicios de la capa de presentación, situada inmediatamente debajo en el modelo.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores web, etc.).

La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

## II.4 Protocolos de Comunicación

Los protocolos son como reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadoras conectadas en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma, por tal sentido, el protocolo TCP/IP fue creado para las comunicaciones en Internet, para que cualquier computadora se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación.

### II.4.1 Introducción

Un protocolo de red es como un lenguaje para la comunicación de información. Son las reglas y procedimientos que se utilizan en una red para comunicarse entre los nodos que tienen acceso al sistema de cable (Fig. 2.7). Los protocolos gobiernan dos niveles de comunicaciones:

- Los protocolos de alto nivel: Estos definen la forma en que se comunican las aplicaciones.
- Los protocolos de bajo nivel: Estos definen la forma en que se transmiten las señales por cable.

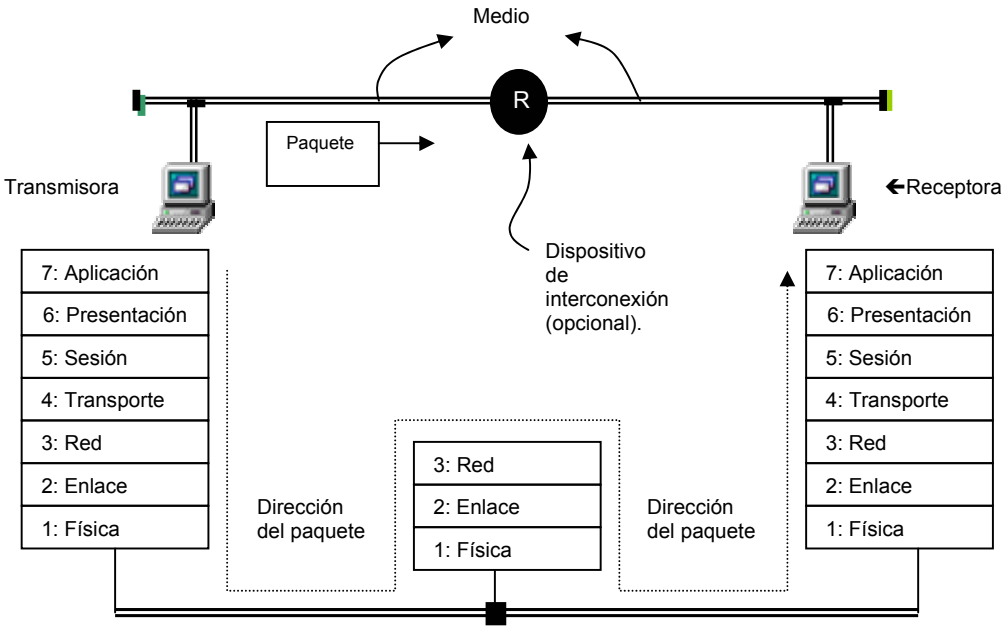


**Fig. 2.7.** Diagrama del proceso de comunicación entre dos computadoras.

Como es frecuente en el caso de las computadoras el constante cambio, también los protocolos están en continuo cambio. Actualmente, los protocolos más comúnmente utilizados en las redes son Ethernet, Token Ring.

Cada uno de estos está diseñado para cierta clase de topología de red y tienen ciertas características estándar.

Ethernet: Actualmente es el protocolo más sencillo y es de bajo costo. Utiliza la topología de "Bus" lineal.

Token Ring: El protocolo de red IBM es el Token ring, el cual se basa en la topología de anillo.

Dos elementos que intervienen en el proceso de comunicación lo forman el paquete de información que la terminal transmisora dirige a la terminal receptora; este paquete contiene entre otras cosas direcciones, información de usuario e información para corrección de errores, requeridos para que alcance a la terminal receptora. Además se encuentra obviamente el protocolo de comunicación.

Los protocolos o normalizaciones son establecidos por organizaciones de reconocimiento mundial, por ejemplo la ISO, IEEE, ANSI, etc. Existen tres tipos de estandarizaciones.

**-** Normas por imposición. Este tipo de normas son impuestas por una organización y debe seguirse en estos terrenos para asegurar comunicación.

**-** Normas por convención. Este tipo de normas son tomadas como tal bajo común acuerdo de distintas organizaciones o grupos de usuarios; éstas fueron tomadas por normas debido a su alto desempeño o que son las únicas en su tipo, sin embargo quien las diseñó no intentaba que fueran una norma impuesta.

## II.4.2 Análisis de Protocolos

Existen muchos protocolos pero a continuación se mencionan los más utilizados.

De todas las arquitecturas de redes sólo sobresalen tres por su valor académico o comercial [5]:

**-** El modelo OSI (Open System Interconection) desarrollado por la ISO.

**-** Los estándares de red IEEE que de hecho esta más orientado al hardware que al software.

**-** La arquitectura TCP/IP originalmente desarrollado por la secretaría de defensa de los Estados Unidos de América junto con algunas universidades importantes.

**Modelo OSI.**

Este conjunto de protocolos está basado en la arquitectura de redes estratificada, en ésta arquitectura el proceso de comunicación se divide en capas y a cada capa le corresponde un protocolo diferente, algunas capas son implementadas en hardware y otras en software y otras en una combinación de las dos.

El protocolo OSI es un protocolo basado en 7 niveles o capas y cada capa como está mencionado anteriormente tiene definido un protocolo; éste protocolo está basado en el supuesto de que una terminal se organiza de tal forma que la comunicación fluye por cada una de las capas, cabe mencionar que la función de cada una de las capas, se mencionó en temas anteriores.

**Estándares de red IEEE.**

Varios comités del IEEE han generado estándares para las topologías de redes y métodos de acceso con fundamento en el conjunto de estándares de capas del modelo OSI. Algunos de los estándares más utilizados son: IEEE 802.3 (El estándar del bus CSMA/CD), el 802.4 (el estándar del bus de señales) y el 802.5 (El estándar Token Ring).

**Arquitectura TCP/IP.**

TCP/IP es un conjunto de protocolos diseñado a finales de los 60's como el fundamento de la red ARPANET que conectaba las computadoras de oficinas gubernamentales y universitarias. Funciona bajo el concepto de cliente-servidor, lo que significa que alguna computadora pide los servicios de otra computadora; la primera es el cliente y la segunda el servidor. ARPANET evolucionó para lo que ahora se conoce como INTERNET y con ello también evolucionó la arquitectura TCP/IP. Sin embargo la organización básica del protocolo sigue siendo la misma. A continuación se amplía un poco más esta arquitectura TCP/IP.

## II.5 Modelo de Referencia TCP/IP

TCP/IP es un conjunto de protocolos, de los cuales el más importante son el IP (protocolo de Internet) y el TCP (protocolo de control de transmisión).

La popularidad de TCP/IP en Internet se debe a que satisfizo una necesidad importante (comunicación de datos a nivel mundial) en el momento oportuno y tenía varias características importantes que permitían satisfacer esta necesidad [8].

## II.5.1 Introducción

TCP/IP es el nombre común de más de 100 protocolos que nos permiten conectar computadoras y redes.

Dentro de Internet la información no se transmite como una cadena continua de caracteres de host [4] a host. Mejor que esto, los datos se transmiten en pequeños "trozos" de información llamados paquetes.

Por ejemplo supongamos que enviamos un correo electrónico muy extenso a un amigo al otro lado del país. TCP dividirá este mensaje en paquetes. Cada paquete se marcara con un número de secuencia y con la dirección del destinatario. Además, TCP inserta determinada información de control de errores.

Estos paquetes se envían a la red, donde el trabajo de IP es transportarlos hasta el host remoto, TCP recibe los paquetes y comprueba si hay errores. Si encuentra algún error, TCP pide que el paquete en cuestión le sea reenviado. Una vez que todos los paquetes se han recibido de forma correcta, TCP utilizará los números de secuencia para reconstruir el mensaje original.

En otras palabras el trabajo de IP es transportar los paquetes de un lugar a otro. El trabajo de TCP es manejar el flujo de datos y asegurarse de que estos son correctos.

Partir los datos en paquetes tiene varios beneficios importantes. Primero, permite utilizar en Internet las mismas líneas de comunicación a varios usuarios diferentes al mismo tiempo. Puesto que los paquetes no tienen que viajar juntos, una línea de comunicación puede transportar tantos tipos de paquetes como ella pueda de un lugar a otro.

[4] Nodo o servidor conectado a Internet.

En su camino, los paquetes son dirigidos de host a host hasta que encuentran su último destino. Esto significa que Internet tiene una gran flexibilidad. Si una conexión en particular esta fuera de servicio, las computadoras que controlan el flujo de datos, pueden encontrar normalmente una ruta alternativa. De hecho es posible, que dentro de una misma transferencia de datos, varios paquetes sigan rutas distintas.

## II.5.2 Niveles de Arquitectura TCP/IP

*Nivel de Acceso a la Red:*

El nivel de acceso a la red es el más bajo (inferior) de la jerarquía TCP/IP. Los protocolos de este nivel proporcionan los medios para que el sistema envíe la información a los otros mecanismos de una red con la que esta conectada directamente. Define como usar la red para transmitir un datagrama IP [4].

A diferencia de los protocolos de niveles más altos, los protocolos de nivel de acceso a la red deben conocer los detalles básicos de la red (su estructura de paquetería, forma de envío, etc.) a fin de formatear correctamente los datos que están siendo transmitidos para cumplir con las necesidades de la red. El nivel de acceso a la red de TCP/IP puede englobar las funciones de los tres niveles más bajos del modelo OSI (Red, Enlace de Datos y Físico). Las funciones que se efectúan en este nivel incluyen el encapsulamiento de los datagramas IP, así como la traducción de direcciones IP a las direcciones físicas usadas por la red. Una de las ventajas de TCP/IP es su esquema de direccionamiento que identifica en forma única a cada anfitrión de Internet.

Las misiones del nivel de acceso a la red son:

- Asignación de direcciones de red únicas.
- Encaminamiento de paquetes.
- Control de gestión.
- Interconexión de subredes distintas.

La figura 2.8 muestra como es que se va haciendo el encapsulamiento de la información en los distintos niveles de la arquitectura TCP/IP.

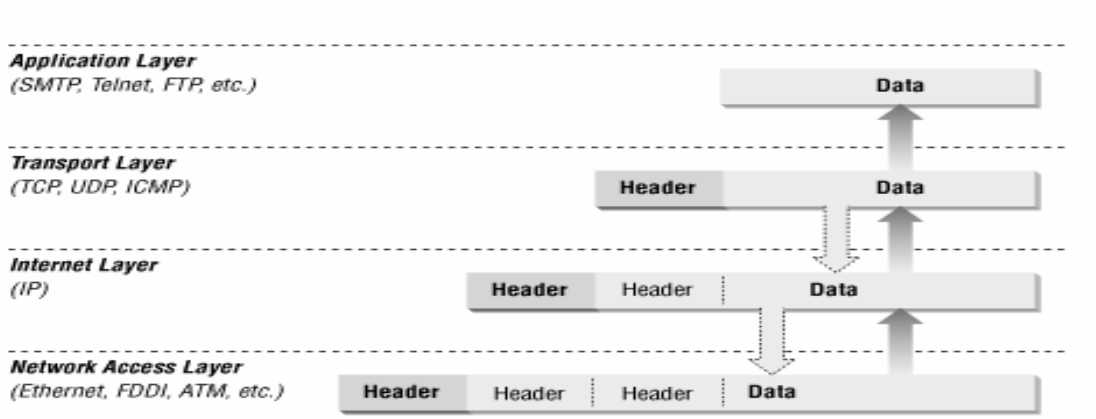


**Fig. 2.8** Encapsulamiento de la Información

*Nivel de Internet:*

El nivel arriba del nivel de acceso a la red en la jerarquía de protocolos es el nivel de Internet. El Protocolo Internet es el alma de TCP/IP y el más importante en el nivel de Internet. IP da el servicio básico de envío de paquetes sobre el cual se construyen las redes TCP/IP. Todos los protocolos por arriba de IP (TCP, UPD) y de bajo de IP (Ethernet, FDDI, ATM y otros), usan a éste para enviar la información. Toda la información TCP/IP fluye a través de IP, hacia dentro y hacia fuera, sin importar su destino final.

IP es el bloque de construcción de Internet. Sus funciones incluyen:

- Definir el datagrama, que es la unidad básica de transmisión de Internet.
- Definir el esquema de direccionamiento de Internet.
- Mover la información entre el nivel de acceso a la red y el nivel de transporte de anfitrión a anfitrión
- Enrutar datagramas hacia anfitriones remotos.
- Realizar la fragmentación y ensamble de los datagramas.

*Nivel de transporte:*

Los dos protocolos más importantes del nivel de transporte son el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagrama de Usuario (UDP).
TCP proporciona servicio de envío de datos confiable con detección y corrección de errores de extremo a extremo. UDP proporciona un servicio de envío de datagramas con menos información de control, sin conexión. Ambos protocolos envían la información entre el nivel de aplicación y el nivel de Internet. Los programadores de aplicaciones pueden elegir el servicio más apropiado para sus aplicaciones específicas.

- La transmisión de datos de nivel de transporte presenta las fases:
  - establecimiento de la conexión
  - intercambio fiable de datos
  - liberación de la conexión.
- La conexión es Full Duplex: Ambos extremos pueden transmitir y recibir simultáneamente.
- La transferencia se apoya en el envío continuo con buffers para almacenamiento de segmentos pendientes.

*Nivel de Aplicación:*

En la parte superior de la arquitectura del protocolo TCP/IP esta el nivel de aplicación. Este nivel incluye todos los procesos que usan los protocolos del nivel de transporte para enviar la información. Hay muchos protocolos de aplicación; la mayoría proporcionan servicios de usuario y siempre se están agregando nuevos servicios a este nivel. Los protocolos de aplicación más ampliamente conocidos y usados son:

Telnet: Protocolo de terminal de red, proporciona acceso remoto a través de la red.

FTP: Se usa para la transferencia interactiva de archivos

SMTP: Protocolo simple de transferencia de correo, envía el correo electrónico.

Aunque los servicios anteriores son de los más usados por los clientes, existen otras aplicaciones TCP/IP usadas comúnmente como:

- Servicio de Nombre de Dominios (DNS), esta aplicación asigna direcciones IP a los nombres asignados a los dispositivos de red.
- Protocolo de Información de Enrutamiento (RIP), el enrutamiento es una parte importante de cómo trabaja TCP/IP. RIP se usa por los mecanismos de la red para intercambiar información de enrutamiento.
- Sistema de Archivos de Red (NFS), este protocolo permite que se compartan archivos entre varios anfitriones de la red.

En la figura 2.9 se muestran los protocolos más utilizados en una arquitectura TCP/IP, seguida de una breve descripción de algunos de ellos.

<table>
<tr><td>HTTP,FTP, SMTP,<br><br>TELNET</td><td>SNMP, X-WINDOWS,<br><br>RPC, NFS</td></tr>
<tr><td>TCP</td><td>UDP</td></tr>
<tr><td colspan="2">IP, ICMP, 802.2, X.25</td></tr>
<tr><td colspan="2">ETHERNET, IEEE 802.2, X.25</td></tr>
</table>

**Fig.2.9** Protocolos más comunes de la Arquitectura TCP/IP

- HTTP (*Hipertext Transfer Protocol*). Es el protocolo encargado de la transferencia de hipertexto.

- *FTP (File Transfer Protocol).* Se utiliza para transferencia de archivos.

- *SMTP (Simple Mail Transfer Protocol).* Es una aplicación para el correo electrónico.

- *TELNET:* Permite la conexión a una aplicación remota desde un proceso o terminal.

- *RPC (Remote Procedure Call).* Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.

- *SNMP (Simple Network Management Protocol).* Se trata de una aplicación para el control de la red.

- *NFS (Network File System).* Permite la utilización de archivos distribuidos por los programas de la red.

- *X-Windows*. Es un protocolo para el manejo de ventanas e interfaces de usuario.

## II.5.3 TCP y UDP

**Protocolo de Control de Transmisión (TCP)** [4]**:** Las aplicaciones que requieren que el protocolo de transporte proporcione un envío confiable de los datos usan el Protocolo de Control de Transmisión (TCP) porque verifica que los datos sean enviados a través de la red de modo acertado y en la secuencia adecuada. TCP es un protocolo confiable, orientado a conexión, de cadena (flujo) de bytes.

TCP brinda confiabilidad con un mecanismo llamado Reconocimiento Positivo con Retransmisión (PAR), dicho de otra manera un sistema que usa PAR envía la información de nuevo a menos que oiga por parte del sistema remoto que llegó bien. La unidad de información intercambiada entre los módulos TCP se llama “segmento”, cada segmento contiene una suma de verificación que usa el receptor para verificar que la información no sufrió daños. Si el segmento de información se recibió sin daños, el receptor envía un reconocimiento positivo al emisor. Si el segmento de información esta dañado, el receptor lo descarta. Después de un lapso apropiado de suspensión, el módulo TCP emisor retransmite cualquier segmento para el cual no haya recibido reconocimiento positivo.

TCP establece una conexión lógica de extremo a extremo entre los dos anfitriones que se comunican. La información de control llamada “negociación” se intercambia entre los dos extremos para establecer un dialogo antes de que se transmitan los datos.

**Protocolo Datagrama de Usuario (UDP)** [4]**:** Los protocolos IP y TCP facilitan las comunicaciones en Internet. Sin embargo, habrá ocasiones en las que se pueda trabajar sin usar el protocolo TCP (ahorrándose así el largo proceso de reordenamiento). Si el mensaje de Internet que enviará cabe en un solo paquete (200 bytes), no hay necesidad de reordenar nada. En este caso no se requiere usar el TCP y en ves de ello puede usarse el UDP.

El Protocolo Datagrama de Usuario ordena las cosas por número de puerto de modo que los mensajes puedan llegar al servicio correcto en el servidor. Sin embargo, los números de puerto UDP no son iguales a los números de puerto TCP. Por ejemplo, TCP 50 no necesariamente llega al mismo servicio que UDP 50, a menos que esto se especifique en el servidor.

UDP realiza un servicio adicional, verifica que los datos en el paquete no se hayan modificado durante su transmisión. A esta verificación se le llama Checksumming. Sin embargo, el problema es que este servicio hace que la velocidad se reduzca, por lo que a menudo las personas lo deshabilitan.

## II.6 Servicios de Internet.

Hay un sinnúmero de servicios estándar de Internet que los usuarios utilizan y que la mayoría de los sitios intenta soportar. Existen razones importantes para utilizar tales servicios; de hecho, sin ellos hay pocas razones para conectarse a Internet. Pero también existen problemas potenciales de calidad con cada uno de ellos.

Cabe mencionar que todos estos servicios trabajan en la capa de aplicación (capa 7) del modelo OSI.

El software que sustenta a Internet proporciona un gran número de servicios técnicos sobre los que todo se construye. La mayoría de estos servicios funcionan ocultos, es decir los usuarios finales no conocen los principios básicos de éstos. A continuación se describen algunos de los principales servicios que proporciona Internet.

## II.6.1 Correo Electrónico

El correo electrónico es uno de los servicios de redes más populares y básicos. Es de riesgo relativamente bajo, pero esto no significa que este libre de riesgos.

El servicio de correo electrónico se ha convertido en un servicio crítico que requiere un alto grado de estabilidad, funcionabilidad, gestión y evolución desde aspectos de seguridad y calidad, hasta nuevos protocolos. [4]

Un usuario de Internet puede enviar y recibir mensajes de cualquier otro usuario de Internet. Más aún, puede enviar mensajes a otros sistemas de correo, como pueden ser CompuServe o MCI Mail que tienen conexiones con Internet.

Sin embargo, correo electrónico no significa solamente mensajes personales. Cualquier cosa que se pueda almacenar en un archivo de texto puede ser enviado por correo electrónico: Programas (fuente) de computadora, anuncios, revistas electrónicas, etc. El sistema de correo electrónico de Internet es la columna vertebral de la red.
El correo electrónico es un gran servicio y el hecho de que sea prácticamente inmediato lo hace destacar entre todos los otros servicios de Internet.

En la práctica los problemas más comunes con el correo electrónico son correos no deseados y personas que confían plenamente en la confidencialidad del sistema de correo electrónico y envía sus datos por medio del correo de Internet.

El Protocolo Simple de Transferencia de Correo (SMTP o Simple Mail Transfer Protocol) es el protocolo estándar de Internet para enviar y recibir correos electrónicos. SMTP en sí no es un problema de seguridad, pero lo pueden ser los servidores SMTP. Un programa que entrega correos a usuarios con frecuencia necesita la capacidad de ejecutarse como cualquier usuario que recibe correos. Esto le da poder amplio y lo hace un blanco tentador para los ataques.

## II.6.2 Word Wide Web

La existencia del Word Wide Web (WWW) es un factor importante detrás del crecimiento explosivo y reciente de Internet. El trafico del WWW en Internet ha crecido a una velocidad explosiva, mucho más rápido que cualquier otro tipo de tráfico (por ejemplo, correo electrónico SMTP, transferencia de archivos FTP, sesiones de terminal remota Telnet, etc.)
El servicio de WWW es una herramienta basada en hipertexto que permite recuperar y mostrar información basada en búsqueda por palabras clave. Lo que hace el servicio de Word Wide Web tan potente es la idea de hipertexto: Datos que contienen enlaces a otros datos.

La ventaja principal de una interfaz gráfica para usuario (GUI) es que las herramientas dentro de ésta son visuales e intuitivas. Además lo que resulta tan poderoso de los servicios de WWW es que se pueden enviar datos al cliente WWW en muchos medios diferentes: texto, texto con colores, imágenes, video, audio e hipertexto.
Los servicios WWW ofrecen, en resumen tres importantes ventajas para los usuarios de Internet [5]:

- ✓ Hacen que las herramientas para navegar en Internet sean sencillas y fáciles de utilizar.
- ✓ Permiten el despliegue de poderosas y coloridas presentaciones multimedia.
- ✓ Se puede acceder a información de todo tipo de servicios, como Gopher[5].

El protocolo para WWW se llama Hipertext Transfer Protocol (protocolo de Transferencia de Hipertexto HTTP). Para entender que es WWW, necesitamos conocer cómo es que funciona el hipertexto.
Hipertexto son datos que contienen ligas a otros datos. En el lenguaje de WWW un documento de hipertexto es algo que contiene datos y, posiblemente, ligas a otros documentos. Cuando seguimos una liga decimos que estamos navegando por la red.

[5] Gopher es una herramienta basada en texto y manejada por menús que sirve para manejar los archivos y directorios a través de Internet [4]

## II.6.3 Telnet y Usenet

### Telnet.

Los programas que proporcionan acceso de terminal remota permiten que utilice un sistema remoto como si su máquina fuera una terminal conectada directamente.
Telnet es el estándar para acceso de terminal remota en Internet. Imita una terminal, no una estación de trabajo gráfica: Proporciona acceso sólo a aplicaciones basadas en caracteres. También brinda acceso remoto a sus usuarios desde cualquier sitio conectado a Internet sin hacer arreglos especiales.

Telnet se consideró en un tiempo un servicio más o menos seguro y de calidad, porque requiere que los usuarios se autentifiquen por ellos mismos. Por desgracia Telnet envía toda su información sin codificar, lo que lo hace muy vulnerable a ataques de espionaje (utilizando analizadores de protocolo) y robo. Por esta razón, ahora Telnet se considera uno de los servicios con menor calidad, debido a su inseguridad cuando se utiliza para entrar a un sitio desde sistemas remotos.

Telnet es seguro solo si su máquina remota y todas las máquinas conectadas a ella son seguras lo cual significa que no es seguro a través de Internet.
Por otro lado, Telnet puede ser muy útil (y muy efectivo, en cuanto a costo) como un mecanismo de acceso remoto si sus usuarios viajan con frecuencia a sitios conectados a Internet. En los lugares donde utilizar un MODEM es costoso, difícil y lento. Usar una conexión a Internet por medio de Telnet puede ser la mejor solución.

Telnet permite que un usuario inicie sesión en otro sistema, como si tuviera una terminal conectada directamente a él. Usamos Telnet como ejemplo porque es muy común y desde el punto de vista del filtrado de paquetes, representativo de muchos otros protocolos, como SMTP.

### Usenet:

Usenet es una gran colección de grupos de discusión en los que participan millones de personas de todo el mundo. Cada grupo de discusión se centra en torno a un tema en particular. Matemáticas, computación, biología, etc. Prácticamente cualquier tema que se pueda pensar tiene su propio grupo de discusión.

En total, Usenet tiene miles de grupos de discusión diferentes. Muchos de estos son de interés regional o local.

Una de las principales preguntas que hace la gente es: ¿Cuánto cuesta utilizar Usenet? La respuesta es que Usenet es gratuito.

Mientras el correo electrónico permite a las personas comunicarse, es más eficaz para que una persona envíe un mensaje a otra, o a una pequeña lista de personas interesadas en un tema específico. Los grupos de noticias son la contraparte en Internet de los foros de discusión y están diseñados para comunicación de muchos a muchos, pero de manera abierta y eficaz, ya que no hay forma fácil de saber sobre todas las listas de distribución de correo y cada receptor tiene su propia copia de cada mensaje.

Los riesgos de las noticias son muy similares a los del correo electrónico: sus usuarios pueden tontamente confiar en la información recibida; pueden divulgar información confidencial; y puede inundarse de mensajes [4].

## II.6.4 Transferencia de Archivos (FTP)

El correo electrónico transfiere datos de un lugar a otro, pero está diseñado para archivos pequeños. Los protocolos para la transferencia de correo electrónico tienen permitido hacer cambios, por ejemplo insertar el signo “<”, pero que no son permitidos para los programas.

Aunque los sistemas de correo electrónico actuales incluyen algoritmos elaborados para tales problemas, estos algoritmos son engorrosos y propensos a errores.

El Protocolo de Transferencia de Archivos (FTP) es el protocolo estándar de Internet para este propósito. En teoría, permitir que sus usuarios obtengan archivos no incrementa más el

riesgo que permitir el correo electrónico; de hecho, algunos sitios ofrecen servicios que permiten que tenga acceso a FTP por medio del correo electrónico [6].
La mayor parte del tráfico en Internet (36%) es de FTP. El correo electrónico representa solo el 6% del tráfico de Internet[6], tal vez porque su uso es más frecuente dentro de las redes locales. Sin embargo, FTP es actualmente el punto fuerte de las herramientas de Internet.
Para conectarse a una computadora remota utilizando FTP el procedimiento es similar al uso de telnet, con excepción de que no se cuenta con todas las herramientas de un shell y el acceso a los grupos de archivos limitado. FTP se usa para transferir archivos de cualquier tipo, por ejemplo de texto o binarios, pues para FTP es realmente lo mismo.
Tampoco son importantes las plataformas en las cuales estén corriendo las dos computadoras.

Una de las razones por las que FTP es uno de los puntos fuertes de Internet es que los clientes de FTP son muy fáciles de obtener para todas las plataformas.
Se puede permitir que los usuarios accedan al sistema mediante le uso de FTP de dos formas: Con una identificación de usuario o como un usuario anónimo. Cuando permite que un usuario entre por FTP a un servidor utilizando su identificación de usuario, se corre el riesgo de que alguien en Internet observe lo que ocurre y pueda de esta forma conocer el nombre de usuario (login) y tener acceso al conjunto de archivos de FTP.
El uso de login anónimo es la forma más segura de dar acceso al servicio de FTP, debido a que puede restringir el acceso de los usuarios al sistema.

## II.6.5 DNS

Como una dirección IP escrita en formato decimal o en formato binario es difícil de recordar, se optó por poder asignar un **nombre de dominio** a cada dirección IP, nombre que fuera más fácil de recordar.

[6]George Eckel, “Construya un Servidor de Internet con Unix” Ed. PHH 1996.

Pero entonces, ¿cómo sabe la computadora a qué IP nos referimos para mandarle los paquetes?. Es aquí donde entran en juego el **Domain Name System** (DNS - Sistema de Nombres de Dominio), que consiste en una serie de tablas en las que se registra la relación IP-nombre de dominio [3].

Inicialmente estas tablas se guardaban en una única computadora central, en un archivo llamado "host.txt", que contenía una tabla de nombres de estructura plana, por lo que cuando otro host cualquiera necesitaba resolver una dirección IP en el nombre de dominio asociado necesitaba consultar a ésta computadora central. Pero a medida que las direcciones IP y sus nombres asociados fueron creciendo el archivo "host.txt" se fue haciendo demasiado grande y complejo, el mantenimiento del mismo se hizo muy complicado.

Por estos motivos se hizo necesario idear e implementar un nuevo sistema de resolución de nombres de dominio que distribuyese el trabajo entre varios servidores especiales, denominados **servidores DNS**, que forman una estructura jerárquica.

Los **Servidores DNS (Name Servers)** son servidores especiales que contestan a las peticiones de los clientes, consultando para ello sus bases de datos de resolución. En caso de no disponer de la equivalencia solicitada por el cliente pueden reenviar la petición a otro servidor DNS.

Cuando la capa IP de un host concreto necesita saber la dirección IP de una serie de paquetes a partir de los nombres de dominio, se establece una conexión UDP (User Datagram Protocol) con el servidor DNS adecuado, que le da la equivalencia necesaria.

Actualmente cada servidor DNS gestiona y actualiza los nombres de host de un dominio o subconjunto de nodos de Internet que son administrados por un organismo (empresa, institución,...). De esta forma, cuando se conecta un nuevo nodo a Internet, su nombre de host es dado de alta en el servidor DNS del dominio al que corresponda.

**Tipos de servidores DNS.**

En función del ámbito de dominios que abarca y de su posición en la jerarquía, los servidores DNS se clasifican en las siguientes categorías [3]:

1. **Servidores DNS primarios** (Primary Name Servers): que almacenan la información de dominios en una base de datos local, siendo los responsables de mantener la información de los dominios actualizada, por lo que cualquier cambio en los datos o cualquier alta o baja de dominio debe ser comunicada a estos servidores.
2. **Servidores DNS secundarios** (Secundary Name Servers): se encuentran por debajo de los anteriores en la jerarquía, por lo que deben obtener de ellos los datos correspondientes a su zona de acción, mediante un proceso de copia denominado "transferencia de zona". Estos servidores actúan además como sistemas de seguridad, al mantener la información de forma redundante, con lo que si un servidor DNS tiene problemas, la información se puede recuperar desde otro. Además, evitan la sobrecarga del servidor principal, distribuyendo el trabajo entre distintos servidores situados estratégicamente, con lo que se gana velocidad en las resoluciones.
3. **Servidores DNS maestros** (Master Name Servers): son los que transfieren las zonas desde los servidores primarios a los servidores secundarios. Puede ser a la vez un servidor primario o secundario de esa zona. Cuando un servidor secundario arranca busca un servidor maestro y le solicita la transferencia de zona, que éste habrá obtenido previamente del servidor primario correspondiente. Con ello se consigue evitar que los servidores secundarios sobrecarguen al servidor primario con transferencias de zona.
4. **Servidores DNS locales** (Caching-Only Servers): servidores que no tienen autoridad sobre ningún dominio, limitándose tan solo a contactar con otros servidores DNS para resolver peticiones de sus clientes a partir de los datos de direcciones almacenados en su memoria caché. Cuando un cliente solicita a

uno de estos servidores la resolución de un nombre de dominio lo primero que hace es consultar su memoria caché. Si encuentra la dirección IP asociada se la devuelve al cliente, y en caso de no encontrarla consulta a otros servidores hasta que la consigue, enviándosela al cliente y anotándola en su caché para próximas peticiones de otros clientes.

## II.6.6 Comercio Electrónico

Con el desarrollo de Internet, paralelamente ha aparecido un nuevo concepto de comercio, al que conocemos como comercio electrónico.

Algunos expertos opinan que en cierta forma, el comercio electrónico comenzó antes de Internet, mediante transacciones comerciales por teléfono y fax, pero el desarrollo de la red global motivó que alcanzara mayor auge, por su masividad y rapidez de operación. Su acepción más general es "acercar el comprador al fabricante por medios electrónicos", lo cual implica eliminación de intermediarios, reducción de costos y una filosofía diferente en la forma de comprar y vender, y lo que es más importante, de obtener información para esas gestiones.

Para especialistas como Juan Fernández, coordinador de la Comisión Nacional de Comercio Electrónico de Cuba, puede definirse como "cualquier forma de transacción de negocios en la cual las partes interactúan electrónicamente en lugar de mediante intercambios materiales o contacto físico directo", y agrega que su esencia se capta mejor si afirmamos que es "uno de los casos poco frecuentes en que se unen las nuevas necesidades con las tecnologías nuevas para revolucionar la forma en que se realizan los negocios." [5]

El Comercio Electrónico, concebido inicialmente como medio complementario de otras formas de comercio, en realidad se está proyectando como una tecnología para el cambio, que por su relación costo-beneficio está al alcance de todas las empresas. En el 2002 había 515 millones de empresas con página Web y para el 2004 se espera que esta cifra aumente considerablemente. Las inversiones de compañías y corporaciones en iniciativas de Internet

sólo EE.UU., que en 2002 totalizaron, con más de 203 mil millones[7]. Las cifras de las compras por comercio electrónico son astronómicas, con pronósticos de 1 billón 318 mil millones de dólares para finales del 2003[8]. Otras firmas, como Forrester Research, dan estimados aún más optimistas: 2 billones 500 mil millones para la misma fecha.

Un estudio elaborado a principios del 2001 por Cisco Systems y la Universidad de Texas expresa que la economía de Internet sólo en Estados Unidos es de tal magnitud, que podría calificarse como una de las mayores del mundo, debido a que actualmente hay más de 900 millones de usuarios de Internet (6).

Existen varios factores que influyen en este tipo de comercio, y que hacen a éste, poco confiable e inseguro y que a continuación se mencionan:

Factores que influyen en el Comercio en Internet

1 - Tangibilidad y Distancia
2 - Confianza y Seguridad
3 - Calidad
4 - "Factor Psicológico" y Costumbres

Cabe aclarar que no están ordenados ni por orden de importancia ni por orden de aparición en Internet.

Estos son solo algunos de los varios factores que intervienen en el comercio electrónico, y que en el presente trabajo nos centraremos principalmente a dos de ellos, el primero es la calidad y el segundo la seguridad y confianza. Son dos factores que están íntimamente

[7] Carrol, Jim y Rick Broadhead. "Selling On-Line), Ed. MacMillan, Toronto, 2000.

[8] Fernández, Juan, Coordinador de la Comisión Nacional de CE de Cuba. Conferencia sobre el Comercio Electrónico en Cuba, Taller Nacional de CE.

relacionados, debido a que si el servicio no se da con calidad, éste va a ser muy inseguro y poco confiable para el usuario.

Todos los servicios que presta Internet son susceptibles a ser blanco fácil de los distintos ataques de seguridad, por ello es necesario conocer los diferentes tipos de ataques, así como las clases de atacantes y las estrategias de seguridad para proteger dichos servicios.

En el siguiente capítulo se muestran algunos tipos de ataques a la seguridad, estrategias de seguridad que podrían ser una solución a los ataques planteados y políticas para la administración de la seguridad que nos lleven a que los servicios de Internet sean de calidad.

# CAPÍTULO III

# Introducción a la Seguridad en Redes y Elementos de Red

## III.1 Importancia de la Seguridad en Redes

Inicialmente Internet nace como una serie de redes que promueven el intercambio de información entre investigadores que colaboran en proyectos conjuntos o comparten resultados usando los recursos de la red. En esta etapa inicial, la información circulaba libremente y no existía una preocupación por la privacidad de los datos ni por ninguna otra problemática de seguridad.

Los protocolos de Internet fueron diseñados de una forma deliberada para que fueran simples y sencillos. El poco esfuerzo necesario para su desarrollo y verificación jugó eficazmente a favor de su implantación generalizada, pero tanto las aplicaciones como los niveles de transporte carecían de mecanismos de seguridad que no tardaron en ser vulnerados.

Recientemente, la conexión a Internet del mundo empresarial ha crecido a un ritmo vertiginoso superior a la difusión de ninguna otra tecnología anteriormente. Esto ha significado que Internet se haya convertido en "la red" por excelencia. Esto es, el medio más popular de interconexión de recursos informáticos.

Se ha incrementado la variedad y cantidad de usuarios que usan la red para fines tan diversos como el aprendizaje, la docencia, la investigación, la búsqueda de información, noticias o, simplemente, el juego. En medio de esta variedad han ido aumentando las acciones poco respetuosas con la privacidad y con la propiedad de recursos y sistemas. *Hackers, Score keepers, Crakers...* y demás familias han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. Es importante recalcar que una componente muy importante para la protección de los sistemas consiste en la atención así como en la vigilancia continua y sistemática por parte de los gestores de la red.

Internet es un avance tecnológico maravilloso que brinda acceso a datos y la habilidad de publicar información en muchas formas. Pero también es un peligro mayor que proporciona la habilidad de contaminar y destruir información.

Al conectarse a Internet se ponen en riesgo tres cosas:

- Los Datos
- Los Recursos
- La Reputación

*Los Datos.*

Los datos tienen tres características que deben protegerse:

- Confidencialidad
- Integridad
- Disponibilidad

En los incidentes de seguridad la detección es difícil. A veces puede tomar mucho tiempo enterarse de que alguien penetró en un sitio. En ocasiones nunca se sabe. Aunque alguien entre pero en realidad no haga nada al sistema o a los datos, se perderá tiempo (horas o días) mientras se verifica que no dañó el sistema.

*Los Recursos:*

Con frecuencia los intrusos dicen que utilizan sólo los excesos de los recursos; por lo tanto, su intrusión no les cuenta nada a sus víctimas. Hay dos problemas con este argumento.

Primero, es imposible que un intruso determine qué recursos se tienen en exceso y utilizar solo esos. Segundo, es un derecho utilizar los recursos propios de la manera que uno quiera.

*La Reputación*

Un intruso en Internet aparece con otra identidad, y esto trae consigo muchas consecuencias. Un sitio con mala reputación, significa que presta un servicio poco seguro y de mala calidad.

## III.1.1 Concepto de Seguridad

La seguridad en redes de computadoras se ha convertido en uno de los problemas más grandes desde la aparición de las redes, y más aún, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este mundo.

Por lo anterior, los ISPs han tenido la necesidad de crear políticas de seguridad consistentes en realizar conexiones seguras, enviar y recibir información encriptada, filtrar accesos e información, entre otros.

La seguridad de las redes suscita cada vez más preocupación, en paralelo al rápido aumento del número de usuarios y del valor de sus transacciones. La seguridad ha cobrado ahora una importancia crítica.

- Las administraciones públicas se han dado cuenta de hasta qué punto la economía y los ciudadanos dependen del funcionamiento eficaz de las redes de comunicación y varias de ellas han comenzado a revisar sus disposiciones en materia de seguridad.

- Es bien conocida la difusión a través de Internet de virus que han causado importantes daños por destrucción de información o negación de acceso a la red.

El interés y la demanda por Internet crece, y el uso de servicios como World Wide Web, Internet Mail, Telnet, el File Transfer Protocol, entre otros, es cada vez más popular. De ahí que es muy importante tener muy claro el concepto de seguridad y de seguridad en redes.

*Seguridad*[1]: Son aquellas cosas que son ciertas, firmes y/o libres de peligro o riesgo. Es el estado de las cosas bajo protección. "un sistema es seguro, si se comporta como los usuarios esperan que lo haga".
La seguridad en redes, es un conjunto de metodologías, documentos, programas y dispositivos físicos encaminados a lograr que los recursos disponibles sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.
Aun cuando todos los componentes de la red (hardware, software y datos) están expuestos a un ataque, los datos y la información, son sujetos principales de la protección.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica.

La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

[1] Construya Firewalls para Internet, Chapman y Zwichy. Ed. Mc. Graw Hill, 1999

## III.1.2 Tipos de Ataques

Hay muchos tipos de ataques contra los sistemas y hay muchas formas de clasificarlos. A continuación dividimos los ataques en tres categorías básicas:

- Intrusión
- Negación del servicio
- Robo de información.

*Intrusión:* Los ataques más comunes a los sistemas son las intrusiones; con ellas las personas pueden utilizar sus computadoras. Los intrusos tienen muchas formas de obtener acceso.

*Negación del servicio:* Un ataque de negación del servicio es el que esta dirigido en su totalidad a evitar que se puedan utilizar sus propias computadoras.

Una "negación de servicio" es caracterizado por un esfuerzo explícito por atacantes para impedirles a los usuarios legítimos de un servicio usar ese servicio. Por ejemplo, un intruso puede acostumbrar su área del ftp anónima como un lugar a guardar copias ilegales de software comercial, consumiendo espacio del disco y generador de tráfico en la red.

*Robo de Información:* Algunos tipos de ataques permiten que el atacante obtenga información sin tener que utilizar directamente las computadoras. Por lo general este tipo de ataques se aprovechan de los servicios de Internet que tienen como fin proporcionar información.

Muchos servicios de Internet están diseñados para usarlos en redes de área local y no tienen el tipo o grado de seguridad que permitirían emplearlos de manera segura a través de Internet.

La mayoría de las personas que roban información intentan tener acceso a las computadoras. Buscan nombres de usuarios y contraseñas, ya que este tipo de información es más fácil de obtener al intervenir la red.

Es importante conocer los ataques pero también los diferentes tipos de personas (atacantes) que llevan a cabo estos ataques y cómo se hacen llamar; a continuación mencionamos algunos de ellos, considerando que son un grupo bastante amplio y que continuamente surgen nuevos grupos.

*Joyriders*

Los Joyriders son personas aburridas que buscan alguna diversión, entran porque piensan que usted puede tener datos interesantes; porque seria divertido utilizar sus computadoras, o porque no tienen nada mejor que hacer. No son activamente maliciosos pero con frecuencia dañan el sistema por ignorancia o porque intentan cubrir su rastro.

*Vándalos.*

Los vándalos quieren causar daños, ya sea porque gozan con destruir cosas, son un gran problema si usted es alguien que el underground de Internet considera como el enemigo (por ejemplo, la compañía de teléfonos o el Gobierno).

*Score keepers*

Son una versión actualizada de la tradición antigua: cobran fama basados en el número y tipos de sistemas a los que han entrado.

*Espías*

El espionaje serio basado en computadoras es poco común, sin embargo es mucho más difícil de detectar que las entradas sin permiso comunes.

*Accidentes*

La mayor parte de los desastres no son causados por mala voluntad, son accidentes o equivocaciones tontas, un estudio reciente indica que el 55% de todos los incidentes que involucran seguridad resultan de usuarios ingenuos o sin entrenamiento que hacen cosas que no debieran[2] .

[2] Richard Power, Current and Future Danger, Computer Security Institute

## III.2 Políticas y Administración de Seguridad

Las políticas de seguridad permiten establecer aspectos de seguridad en forma de perfiles que afectan a grupos de usuarios. Una vez definidas las políticas, el administrador sólo tiene que añadir los usuarios a los grupos establecidos con lo que adquieren los perfiles de seguridad. De esta forma la actualización de medidas de seguridad se hace sobre las políticas y no sobre los usuarios directamente.

Otro aspecto a considerar es el de la monitorización y registro de las actividades de los usuarios pudiendo denegar el acceso de los usuarios en función de que intenten realizar actividades para los que no tienen permiso.

- Las políticas de seguridad tienen por objetivo establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de los equipos de cómputo y personas que interactúan haciendo uso de los servicios asociados a ellos.

- Permiten a los usuarios saber qué actitud tener ante un incidente de seguridad a través de normas y procedimientos.

### III.2.1 Organización

- Una forma de disminuir los problemas de seguridad es capacitando a los usuarios para tener mejores prácticas en el manejo de los equipos de cómputo.

- La difusión es parte fundamental en el proceso de mejorar la cultura de seguridad en cómputo.

- Proporcionar asesoría profesional y capacitación a los usuarios.

## III.2.2 Integridad, Autenticación y Cifrado

No existe un mecanismo capaz de proveer todos los servicios de seguridad, ni aquel que ofrezca una seguridad total, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

- *Intercambio de autenticación:*

Corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, en la figura 3.1 A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para burlarlos [1].

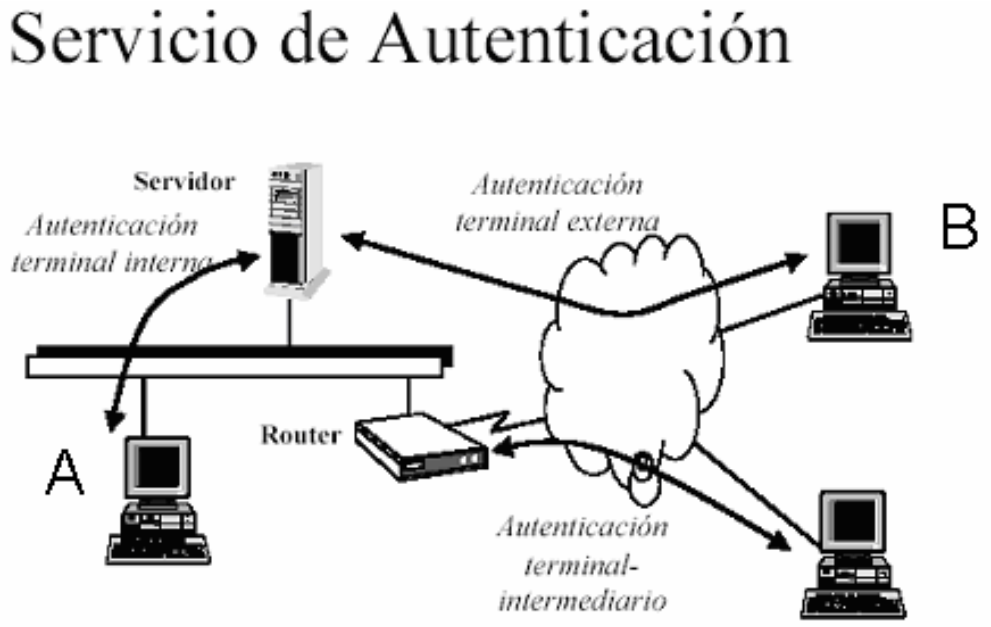


**Fig. 3.1** Diagrama del Proceso de Autenticación

- *Cifrado:*

Garantiza que la información no es comprensible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado [2]. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan sobre flujos continuos de bits. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

- *Integridad de datos:*

Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV) [2].

Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

- *Firma Digital:*

Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos

ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio [2].

- *Control de acceso*:

Es un esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso [3].

- *Tráfico de relleno*:

Consiste en enviar tráfico ilegítimo junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo [2].

- *Control de encaminamiento:*

Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada [2].

- *Unicidad:*

Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas de mensajes [3].

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

## III.2.3 Estrategias de Seguridad

Los clientes escogen una variedad de modelos de seguridad, o medidas que van desde los que no ofrecen ninguna seguridad, pasando por lo que se llama seguridad de ser desconocido y seguridad para anfitrión hasta la seguridad para redes.

*Seguridad a través de ser desconocido.*
Con éste modelo, un sistema es seguro solo porque (supuestamente) nadie sabe de su existencia, contenido o alguna otra cosa, esta medida rara vez funciona mucho tiempo.

*Seguridad para anfitrión.*
Es posible que este método sea el más común, con él se puede reforzar la seguridad de cada máquina anfitrión, lo malo es que este sistema no se puede ampliar a muchas máquinas, implica una cantidad importante de trabajo mantenerlo.

*Seguridad para redes.*
Conforme los ambientes se tornan más grandes y diversos, se vuelve más difícil asegurarlos por lo que se crea el sistema de seguridad de redes, este modelo de seguridad se concentra en controlar el acceso a las redes de distintos anfitriones y los servicios que ofrecen en lugar de asegurarlos uno a uno.

***ESTRATEGIAS DE SEGURIDAD.***

**Menor Privilegio**

- Significa que cualquier objeto (usuario, administrador, programa, sistema o lo que sea) debe tener solo los privilegios que necesita para cumplir con sus tareas asignadas (no mas).

**Defensa a Fondo.**

- No depende solo de un mecanismo de seguridad sin importar cual fuerte parezca; se instalan varios mecanismos que se respalden entre sí. El truco está en hacer que el intento sea demasiado riesgoso o costoso para los atacantes.

**Punto de choque.**

- Obliga a los atacantes a utilizar un canal angosto que es más fácil de monitorear y controlar. Un punto de choque es inservible si hay una manera efectiva de que un atacante lo evite.

**Eslabón más débil.**

- El punto fundamental de seguridad es que la cadena es tan fuerte como su eslabón más débil y se debe concentrar la atención en este punto. Siempre hay un eslabón mas débil el truco consiste en hacer que sea lo suficientemente fuerte y mantenerlo así de acuerdo con el riesgo.

**Postura de falla Segura.**

- En la medida de lo posible los sistemas deben tener una falla segura, es decir si van a fallar deben hacerlo de tal forma que nieguen el acceso a un ataque en lugar de dejarlo entrar.

**Simplicidad.**

- La simplicidad es una estrategia de seguridad por dos razones, primero, mantener las cosas sencillas las hace fáciles de comprender; sino se entiende algo, no se puede saber en realidad si es seguro o no. Segundo, lo complejo proporciona muchos escondites para que se oculten toda clase de cosas.

**Diversificación de defensa.**

- Así como puede obtener seguridad adicional utilizando varios sistemas para dar profundidad a la defensa, también se puede obtener empleando varios tipos de sistemas.

## III.3 Elementos de Red

*Elementos de una Red.*

***1 Servidor***

El servidor es la máquina principal de la red, la que se encarga de administrar los recursos de la red y el flujo de la información. Muchos de los servidores son “dedicados”, es decir, están realizando tareas específicas, por ejemplo, un servidor de impresión solo para imprimir.

***2 Estación de Trabajo***

Es una computadora que se encuentra conectada físicamente al servidor por medio de algún tipo de cable. Muchas veces esta computadora ejecuta su propio sistema operativo.

***3 Sistema Operativo de la Red***

Es el sistema (software) que se encarga de administrar y controlar en forma general la red. Este sistema operativo tiene que ser multiusuario, como por ejemplo: Windows NT, Unix, etc.

***4 Recursos a Compartir***

Al hablar de los recursos a compartir, estamos hablando de todos aquellos dispositivos de Hardware que tiene un alto costo y que son de alta tecnología. En estos casos los más comunes son las impresoras, en sus diferentes tipos.

***5 Hardware de Red***

Son aquellos dispositivos que se utilizan para interconectar a los componentes de la red, que son básicamente:

*Tarjeta de Red:* Esta se instala dentro de la máquina que se encontrará en la red. Cada tarjeta de red determina el protocolo de comunicación y forma de interconexión de acuerdo a la tecnología en la cual se encuentre fabricada, como lo muestra la figura 3.2

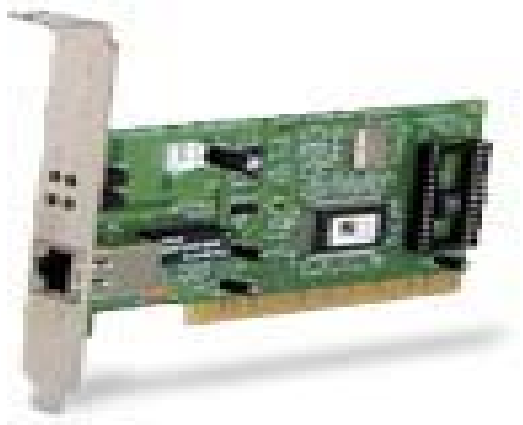

**Fig. 3.2** Tarjeta de Red 3Com 10 / 100

*Concentrador:* Un concentrador proporciona almacenamiento y reexpedición de las transmisiones, permitiendo tomar información de entrada de la que es capaz de procesar y enviar a la salida.

*Switch:* Un switch ocupa el mismo lugar de un Hub o de un concentrador de red. A diferencia de los hubs, los switches examinan cada paquete y lo procesan mejor que un simple repetidor que envía la señal a todos los puertos. La figura 3.3 muestra un Switch 3Com de 32 puertos.

**Fig. 3.3** Switch 10 / 100 MBPS de 32 puertos.

*Hub:*

Es un punto central de conexión para las computadoras de la red. Pueden conectarse varios hubs entre sí para que se puedan conectar más computadoras a la red. El Hub es un dispositivo que brinda la facilidad de asistencia remota de la red, realiza una detección y resolución sencilla de problemas.

En el Hub el tráfico se propaga a través de todos los segmentos, es por eso que se relaciona con una red Ethernet, ya que el hub puede funcionar como el bus principal.

Una limitación importante que se debe de tomar en cuenta al diseñar una red es el número de hubs que pueden ser conectados entre sí. Por cada dos nodos cualesquiera conectados a una red, deben existir más de 4 hubs entre ellos. Existen muchos tipos y modelos de hubs en el mercado, la Fig. 3.4 muestra un tipo de ellos.

**Fig. 3.4** Hub Cisco 8 puertos 10/100

*Bridge:*

Un Bridge es un dispositivo que conecta dos redes LAN separadas para crear lo que aparenta ser una sola red LAN. Los puertos revisan la dirección asociada con cada paquete de información. Luego, si la dirección es la correspondiente al otro segmento de red, el Bridge reconoce que la dirección es la correspondiente a un nodo del segmento de red actual.

Los Bridges también suelen emplearse para reducir la cantidad de tráfico de la red. Mediante la división de un solo segmento de red, en dos segmentos y conectándolos por medio de un Bridge. Los Bridges vienen en todas formas y tamaños, en muchos casos un Bridge es un dispositivo similar a una computadora, con conectores a los que se conectan redes separadas. En otros casos un Bridge es de hecho una computadora con un adaptador para cada red que va a conectarse. Un software especial permite el paso de la información adecuadamente a través de los adaptadores de la red de un segmento de red a otro.

*Router:*

Los routers son dispositivos de red que raramente se encuentran aislados entre sí. Al contrario, suelen estar interconectados, formando una especie de “telaraña” que hace posible el tráfico de datos entre redes separadas físicamente.

Tomando como ejemplo la Red de redes, Internet, cuando una computadora envía una serie de paquetes de datos a otra situada en otra ciudad o país, estos son encaminados de router a router a lo largo del camino entre ambas máquinas. Cada paso de un paquete de un router a otro se denomina “salto”, y el principal objetivo de todos y cada uno de los routers que intervienen en la transferencia del paquete es que éste llegue a su destino en el menor

número posible de saltos, por la mejor ruta posible. La figura 3.5 muestra la conexión de dos redes a través de un router [4].

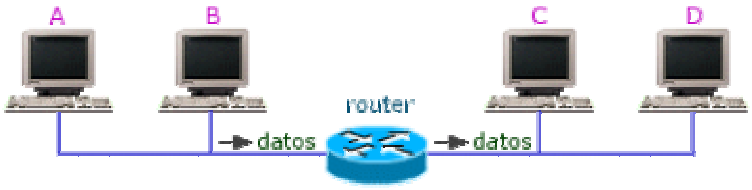


**Fig. 3.5** Conexión de dos redes a través de un Router.

Para poder realizar el menor número de saltos, los routers se comunican constantemente entre sí, informándose de las rutas bloqueadas, de las máquinas intermedias que se encuentran caídas o saturadas de tráfico, aprendiendo con ello cuál es el router idóneo para enviarle los paquetes recibidos.

Si consideramos ahora el caso de un router segmentando una red local (LAN), aunque ahora no debe enviar los paquetes a otro router, sí que tiene que saber por qué puerto debe enviar los datos para que lleguen a la máquina local destino.

Esta habilidad de “saber” a dónde tienen que enviar los paquetes de datos que reciben la consiguen almacenando en su interior una tabla especial, conocida como tabla de ruteo, en la que van anotando las direcciones IP de las máquinas que se comunican con él y el puerto por el que está accesible esa máquina.

Así, cuando a un router llega un paquete, mira en su tabla de ruteo. Si está en ella referenciada la dirección IP de la máquina destino, también lo estará el puerto por el que ésta es accesible, con lo que envía por él el paquete. En caso de no estar la IP en la tabla, manda una petición de respuesta por todos los puertos, preguntando en cuál de ellos se encuentra la máquina destino, y una vez obtenido el puerto de acceso, ingresa la nueva pareja IP/PUERTO en su tabla de ruteo, con lo que los próximos paquetes para esa máquina los enviará directamente.

La seguridad en redes es un punto que se debe cuidar mucho al hablar de calidad de servicio en los servicios de Internet. Como ya lo mencionamos, existen múltiples tipos de ataques a los que están expuestos los servicios de Internet y sería imposible brindar un servicio con calidad, si dicho servicio es inseguro. En pocas palabras, no existe calidad en los servicios de Internet, si estos no tienen estrategias y políticas de seguridad adecuadas.

Aunque en el presente trabajo de tesis no se detalla más en cuanto al concepto de seguridad, es importante conocerlo, debido a que la seguridad juega un papel importante para obtener una calidad de servicio adecuada.

En el siguiente capítulo se ampliará un poco más el concepto de calidad de servicio (QoS) y cuales son los parámetros que la afectan, para así poder estimar la calidad de servicio que esta recibiendo el usuario final y saber si se esta cumpliendo con el SLA (nivel acordado de servicio) establecido entre el cliente y el proveedor, para lograr la satisfacción de cliente.

# CAPÍTULO IV

# Calidad de Servicio (QoS)

## IV.1 Definición de Calidad

La preocupación por la calidad es tan antigua como la sociedad. Sin embargo, en cada momento histórico el concepto de calidad ha sido distinto. Las sociedades y las personas han evolucionado, cada una a su ritmo, y han demandado cosas distintas, con características diferentes. Por ello, la calidad se ha entendido de forma distinta a lo largo de los años, y esto ha conformado las distintas interpretaciones de lo que es o no calidad.
Existen dos conceptos muy importantes en calidad, que son el concepto de aseguramiento de la calidad y el de calidad total, y una conexión muy importante entre ambas, puesto que es difícil llegar a la segunda si los fundamentos de la primera. Más adelante se hablará acerca de estos dos conceptos.

Para el prestador del servicio, calidad es el nivel de satisfacción que quiere proporcionar a sus clientes en todas las prestaciones de servicio que les proporciona.
Para el cliente la calidad es el nivel de satisfacción que le proporciona el servidor o prestador de servicios. Por tanto los clientes son la referencia en cuanto al nivel de servicio que se quiere dar, son los jueces que establecen el nivel de calidad de servicio que realmente esta proporcionando el prestador [1].
El nivel requerido de calidad de servicio hay que alcanzarlo, y una vez alcanzado hay que mantenerlo “en todo momento”.

## IV.2 Concepto de de Calidad de Servicio (QoS)

La calidad de servicio (QoS) puede definirse como el rendimiento de los servicios de Internet observados por el usuario final. Una red debe garantizar que puede ofrecer un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros. En su conjunto, esas condiciones forman un contrato de tráfico entre el usuario y la red.

Las siguientes definiciones son importantes para comprender cuando se habla de calidad de servicio [1]:

1. La clase de servicio (CS) define un conjunto preciso de parámetros cuando se ofrece un servicio.
2. El nivel acordado de servicios (Service Level Agreement: SLA) establece la calidad de servicio pactada mediante un contrato.

El SLA es un convenio entre un cliente y un Proveedor de Servicios el cual establece pautas para la disponibilidad, confiabilidad y seguridad de redes. El proveedor de servicios está a cargo de eliminar la complejidad de servicios.

El concepto de calidad de servicio se originó en las técnicas y estándares de redes, pero también puede extenderse a Internet, las aplicaciones y los servidores de contenido para administrar las clases de servicio a lo largo de todos los recursos de transmisión y procesamiento que forman la infraestructura de Internet.

QoS es el rendimiento de extremo a extremo de los servicios de Internet tal como lo percibe el usuario final. Los parámetros de QoS son: el retardo, la variación del retardo y la pérdida de paquetes. Una red debe garantizar que puede ofrecer un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros.

*Retardo*[1]*:* El retardo es la demora que sufre una unidad de información (en general un paquete) entre origen y destino, este retardo esta formado por una parte fija y una variable:

- La parte fija viene dada por los procesos de empaquetado y desempaquetado, y el retardo de propagación de la señal (que solo es significativo en transmisiones a larga distancia, también típico en las comunicaciones por satélite).
- La parte variable se produce principalmente en las colas de espera de los elementos de encaminamiento. El retardo depende de la carga de la red, por eso, a más carga más retardo.

La pérdida de paquetes se debe principalmente a la congestión de la red, por tanto solo puede disminuirse, si el tráfico total en la red disminuye. Cuando se produce una pérdida es necesario que las fuentes retransmitan lo que se ha perdido y esta retransmisión provoca un aumento en el número de paquetes transmitidos y esto empeora la situación.
El tiempo de respuesta considerado como aceptable para que una página responda es de 10 seg.[2] del cual, algunas páginas rebasan considerablemente.

Para solucionar el problema del retardo, se puede aplicar un mecanismo que consiste en que las fuentes, cuando detectan un nivel de pérdidas excesivo, reducen la velocidad de transmisión y de esta manera disminuyen la congestión. Mientras estamos en una situación de pocas pérdidas, la fuente supone que hay recursos de red disponibles y por ello aumenta su velocidad de transmisión (explota la QoS extra de la red). Este mecanismo es utilizado en el protocolo TCP para evitar la congestión.

Existen diferentes técnicas para la recuperación de los paquetes; como por ejemplo la adaptación del retardo la cual se realiza en el destino; y la adaptación de la velocidad de transmisión que se realiza en la fuente. Simultáneamente pueden usarse diferentes técnicas de recuperación de paquetes.

[1] Definición tomada del glosario de términos computacionales.
[2] http://www.isocmex.org.mx/calidad.html

*Adaptación del retardo:* La adaptación del retardo consiste en cambiar el instante de reproducción de los paquetes. Todos los paquetes que llegan antes de su instante asociado son guardados en un buffer. Si se escogen adecuadamente estos instantes se consigue eliminar la variación del retardo, conocida como jitter, (más adelante hablaremos de esto); dando lugar al flujo original continuo. Estos instantes pueden retrasarse si la QoS de la red empeora (mayor jitter) o adelantarse si mejora (se saca provecho de la QoS extra de la red). Cuando más se reduce la variación del retardo, menos paquetes tardíos (descartados) se producen y por lo tanto se aumenta la fidelidad.

*Adaptación de la Velocidad:* Tal y como se mencionó en la adaptación del retardo; el destino informa a la fuente de la calidad de servicio recibida, y la fuente aumenta o disminuye la velocidad.

Podemos codificar con distintos formatos tanto los flujos de audio (WAV, MPEG audio, ...) como los de vídeo (AVI, MPEG1, ...). Como se puede cambiar la resolución y el número de imágenes por segundo, el flujo puede transmitirse a diferentes velocidades de transmisión. En situaciones de congestión se reduce la velocidad para que los retardos y pérdidas de red disminuyan. De esta manera, y con la aplicación de las técnicas de adaptación de retardo, se consigue un mejor rendimiento de la aplicación. Si la QoS de la red mejora, se aumenta la velocidad de transmisión.

Normalmente una reducción en la velocidad significa una reducción en la calidad por lo que es importante conocer que existe un límite en esta reducción, el cual viene dado por la calidad mínima deseada.

Algunas aplicaciones de tiempo real no pueden construirse con técnicas adaptativas como las anteriores (se llaman rígidas o duras). Se trata de aplicaciones que no toleran las pérdidas ni los cortes, y por ello, no pueden utilizar técnicas de adaptación del retardo. Su implementación es sencilla ya que mantienen fijos los instantes de reproducción. Necesitan que la red asegure la entrega de los paquetes sin pérdidas. Un ejemplo sería una videoconferencia que permitiese a un cirujano ayudar remotamente en una operación.

Algunas aplicaciones que podrían ser adaptativas se construyen rígidas debido a su simplicidad, pero entonces necesitan una mejor QoS de red.

La implementación de Políticas de Calidad de Servicio se puede enfocar en varios puntos según los requerimientos de la red, los principales son:

- Asignar ancho de banda en forma diferenciada
- Evitar y/o administrar la congestión en la red
- Manejar prioridades de acuerdo al tipo de tráfico
- Modelar el tráfico de la red

Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas a medida como son los protocolos de tiempo-real RTP y de reservación RSVP.
Los servicios tradicionales de Internet (SMTP o FTP) disponen de una calidad denominada "*best effort*"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren tiempo-real. Para otros servicios del tipo "*real-time*" (voz y vídeo) se requiere una latencia mínima.

---

*Best-effort.:* Este es un servicio por default que no tiene en cuenta las modificaciones por la QoS. Se trata de una memoria buffer del tipo FIFO (First Input First Output).
*Latencia-Jitter:* Se denomina **latencia** a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete).
Un tiempo de latencia variable se define como **jitter** (fluctuación de retardo) sobre los datos de recepción.
La solución al jitter es guardar los datos en memorias buffer, lo cual introduce un retardo aun mayor.

Las redes pueden introducir retardos, pérdida de paquetes o errores debido a problemas de multiplexaje, conmutación o transmisión en nodos congestionados, impactando entonces la calidad del servicio. Cuando se maneja asignación de recursos de voz, datos y video, las condiciones de la red se tensan al máximo para poder garantizar el desempeño de los servicios múltiples. La calidad de servicio se definió inicialmente en los protocolos de comunicaciones ATM (Asynchronous Transfer Mode) y luego evolucionó al protocolo IP para disponer de las herramientas para manejar la infraestructura de las redes de nueva generación NGN (Next Generation Network).

## IV.3 Aseguramiento y Control de la Calidad

*El aseguramiento de la calidad*

Del control estadístico fueron deduciéndose poco a poco las causas básicas de la no calidad e identificando los puntos de los procesos en los que se producía. La respuesta obligada es el establecimiento de sistemas que garantizasen la calidad evitando los fallos en el momento y lugar adecuado. Comienza el desarrollo de normas cuyo cumplimiento asegura la calidad.

El aseguramiento va más allá de la evaluación como control, ya que implica que la calidad debe ser mantenida a lo largo del proceso. El aseguramiento busca que todo el proceso funcione adecuadamente de manera que los participantes que no cumplen los requisitos sean mínimos en la evaluación final. El control de calidad se refiere a los productos finales, mientras que el aseguramiento se centra en el conjunto del proceso. El aseguramiento, por tanto, implica la gestión de los procesos de definición, diseño y ejecución de un programa para minimizar los rechazos del control de calidad final.

El aseguramiento de la calidad supone el establecimiento de estándares en cada elemento clave.

De los fracasos que se producen en el camino del aseguramiento se llega a dos descubrimientos. El primero es la importancia del factor humano para lograr la calidad, pues las normas cuidadosamente elaboradas que se tratan de aplicar solo tienen éxito si son apoyadas por los que tienen que realizar el trabajo. El segundo es que la calidad técnica que se define desde dentro no tiene ningún valor si no se tiene en cuenta la percepción de los consumidores, usuarios o clientes. La calidad no puede verse desde dentro, sino desde fuera, es decir, la perfección técnica no sirve para nada si no satisface a los consumidores.
Al final de la década de los cincuenta comienza a definirse la calidad (inicialmente por Juran) como "aptitud para el uso", lo que amplia la idea de aseguramiento [2].

*Calidad Total*

En la década de los setenta Deming populariza el concepto de "Calidad Total" que, como él dice, no es un fin en si mismo, sino un método de gestión cuyo objetivo es mejorar la organización, los servicios y la satisfacción del cliente [2]. En esos años se entra en una nueva etapa de la vida económica. Si hasta finales de los años sesenta hay más demanda que oferta, la relación se invierte a lo largo de los setenta y aparece el problema de la competitividad. Hay que ofrecer más, mejor y a menor costo para atraer al cliente. La calidad se convierte en el arma de crecimiento o supervivencia en los últimos años.

La diferencia esencial con otros conceptos de calidad anteriores es que no depende de las especificaciones o del uso sino de la satisfacción del cliente.

## IV.4 Evaluación de la Calidad y Satisfacción del Cliente

Tomando en cuenta las definiciones anteriores de Calidad de Servicio, podemos decir que el mejor juez para evaluar si el servicio proporcionado por el ISP cumple con sus expectativas es el usuario, por ello, es necesario satisfacer sus necesidades. Aunque esto no implique que los servicios prestados sean de una calidad aceptable.

La satisfacción del usuario es uno de los resultados más importantes de prestar servicios de buena calidad. La satisfacción del usuario depende no sólo de la calidad de los servicios sino también de las expectativas del mismo. El usuario está satisfecho cuando los servicios cubren o exceden sus expectativas. Si las expectativas del usuario son bajas o si el usuario tiene acceso limitado a cualquiera de los servicios, puede ser que esté satisfecho con recibir servicios relativamente deficientes.

Cuando el usuario percibe la calidad de manera equivocada, sus expectativas pueden influir en el comportamiento de los prestadores de servicios y, de hecho, reducir la calidad de atención.

La satisfacción del usuario es un indicador importante de la calidad de servicios. No obstante, resulta difícil evaluar la satisfacción del cliente. Los métodos y las medidas para la recolección de datos suelen influir en las respuestas del usuario. Como se mencionó anteriormente, la mayoría de los usuarios afirman estar satisfechos independientemente de la calidad real.

Los ISPs centran su estrategia actual en dos factores difícilmente conciliables: precio y calidad en la mayoría de los sectores y mercados, se puede afirmar que tener precios competitivos es una condición necesaria pero no suficiente para poder tener presencia en el mismo.

Por ello, la calidad se alza cada vez más, como objetivo estratégico para lograr la satisfacción del usuario a través de un monitoreo continuo en tiempo real de los servicios

de Internet, para lograr estimar la calidad con la que están llegando los servicios al usuario final.

Es lógico que las empresas pidan acuerdos específicos sobre el nivel de servicio SLA (service level agreement) antes de confiar sus operaciones a la Internet pública. Buscan calidad de servicio (QoS) desde una perspectiva de usuario final y quieren garantías no sólo de disponibilidad de servicio (base generalizada para los SLAs) sino también de funcionamiento global, incluidos tiempos de acceso y de respuesta de un servicio, velocidad de transferencia de datos, índices de error, pérdida de paquetes, etc.

Para brindar y garantizar estos niveles elevados de QoS, los ISPs han demandado medios para medir y gestionar el funcionamiento de Internet a lo largo de toda la cadena de prestación de servicios, desde la aplicación alojada en la Web hasta la estación de trabajo del cliente.

En el siguiente capítulo se describirá una herramienta que nos ayudará a realizar dichas mediciones, y encontrar una opción para lograr estimar la calidad de servicio que está percibiendo el usuario final.

# CAPÍTULO V

# Desarrollo e Implementación del Sistema

## V.1 Planteamiento

La mayoría de las empresas piden acuerdos específicos sobre el nivel de servicio (SLA service level agreement) antes de confiar sus operaciones a Internet. Buscan alta calidad de servicio (QoS) desde una perspectiva de usuario final y piden garantías no sólo de disponibilidad de servicio sino de funcionamiento global, incluidos tiempos de acceso y de respuesta de un servicio, velocidad de transferencia de datos, índices de error, pérdida de paquetes, etc.

Para brindar y garantizar estos niveles elevados de QoS, los ISPs han demandado medios para medir y gestionar el funcionamiento de Internet a lo largo de toda la cadena de prestación de servicios, desde la aplicación alojada en la Web hasta la estación de trabajo del cliente.

La medición del funcionamiento real del sistema requiere una plataforma de gestión que haga algo más que comprobar la disponibilidad, controlar un elemento o un sistema o gestionar fallos. El sistema debe cumplir todas estas funciones en todo el entorno. Tiene que medir, registrar y comunicar los tiempos reales de la transacción del servicio. Y algo muy importante: tiene que ofrecer una imagen precisa de la calidad del servicio tal como se presenta al usuario final y tal como éste la percibe.

La definición del nivel de servicio es el primer paso para ofrecer una solución efectiva. El proceso debe cumplir los siguientes objetivos:

- Identificar todos los elementos de la cadena existente del servicio de Internet, y presentar cada uno de los servicios.
- Medir el funcionamiento de todos los elementos. Esto implica reunir y correlacionar los datos para dar un panorama general de la salud del servicio; sentar las bases para un comportamiento 'normal' del servicio; establecer umbrales para advertir anticipadamente los problemas del servicio; y llevar una historia de la medición para un análisis y un informe de tendencias.
- Identificar los eslabones más débiles en la cadena de prestación del servicio. Un eslabón débil puede ser un elemento de la red o incluso una aplicación.
- Invertir recursos para reconstruir o reforzar los eslabones débiles.
- Comprobar la nueva cadena de prestación del servicio para evaluar y confirmar las mejoras.
- Seguir el proceso para garantizar una calidad permanente del servicio.

Para cumplir estos objetivos, nos apoyaremos en la plataforma llamada **Firehunter,** para aportar capacidad de gestión de nivel del servicio al entorno de los grandes ISPs. Con la metodología propuesta podemos realizar mediciones en todos los elementos de multiproveedores de Internet (puntos de presencia, redes, servidores y aplicaciones) para captar el estado exacto del funcionamiento de los servicios. También señala, cómo un problema, en uno de los elementos de la cadena de prestaciones influye sobre los demás elementos.

La esencia de la solución de gestión de servicios de Internet es el concepto de modelo de servicio. El modelo de servicio es la capacidad de descubrimiento automatizada que identifica todos los elementos dentro de una cadena de prestación de un servicio, por ejemplo en un servicio de correo electrónico o Web Hosting y en servicios de apoyo como asignación de nombres DNS (Domain Naming Systems) y autenticación. El sistema construye un modelo de servicio descendente que incluye todos los elementos que el ISP escoge gestionar como parte de esa cadena de prestación.

El modelo de servicio ofrece a los ISPs una imagen visual del entorno de servicio. Reúne datos de medición transformándolos en información útil para dar un panorama de la calidad de los servicios. También permite detectar, aislar y resolver los fallos con mayor rapidez.

La capacidad del modelo de servicio es flexible, de modo que los ISPs pueden personalizar los modelos para su propio entorno o conectar nuevos si es necesario. Firehunter incluye modelos para correo electrónico, noticias y servicios de la Web, y se van introduciendo nuevos servicios a medida que los clientes los demandan, como redes virtuales VPN y modelos de e-commerce.

La plataforma de gestión de servicio distribuida trabaja de forma continua para reunir y relacionar nuevas mediciones a lo largo y ancho de múltiples dominios de Internet. El sistema compara los datos nuevos con las bases establecidas, que representan el comportamiento 'normal' de un servicio y con los umbrales definidos por el usuario. Las acciones sólo se desencadenan si el funcionamiento supera estos umbrales. Estas acciones pueden incluir la notificación a los usuarios por correo electrónico o ejecutando automáticamente guiones que enlazan el sistema con clasificadores de problemas u otros sistemas de gestión de la red.

Para resolver el problema de la degradación paulatina de la calidad del servicio a lo largo del tiempo, la metodología propuesta ofrece, tanto umbrales de servicio que advierten precozmente de los niveles en descenso del servicio, como una base de datos del funcionamiento histórico del servicio que pueden analizarse para deducir tendencias.

La capacidad de comunicación de éste sistema de gestión del servicio permite a los ISPs abrir pantallas múltiples y enlazadas que presentan los diferentes parámetros que se rastrean de un extremo a otro de un servicio determinado. Por ejemplo, un gráfico podría presentar la respuesta del servidor de Web, otro el funcionamiento del servicio de nombres (DNS), otro el tiempo de transferencia de los datos, así sucesivamente. Al visualizar los parámetros del funcionamiento, los ISPs tienen una imagen actual del funcionamiento de cada elemento del servicio y una visión global de la calidad del servicio en su conjunto.

Además, esta metodología presenta pantallas de información e informes que son específicos de cada actividad, es decir, enfoques particulares de información del ámbito del servicio a la medida de las necesidades de los operadores que explotan el entorno de servicio, de los planificadores de red y de los gestores de los acuerdos de servicio.

Los Acuerdos de Servicio (SLAs): la información recabada en las mediciones y el control de los servicios de Internet con la metodología propuesta pueden incorporarse a los informes del servicio.
Esto proporciona un conjunto de datos básicos para gestionar los contratos de nivel de servicio SLAs. Los ISPs se quejan porque tienen grandes cantidades de contratos que administrar, lo cual les plantea el desafío de rastrear el funcionamiento del servicio que afecta a esos acuerdos. Con la plataforma seleccionada se pueden introducir los parámetros operativos (medibles) de esos contratos: la disponibilidad de la red o del sistema, el rendimiento y los tiempos de espera y de respuesta del servicio. La metodología propuesta programa las mediciones adecuadas y a continuación mide, registra y comunica los resultados, asociando las mediciones que afectan al servicio con los SLAs específicos.

El sistema permite un control y una información individualizada por cliente, y puede programarse para que emita un aviso si el SLA de un cliente determinado está a punto de ser quebrantado para que el ISP pueda tomar medidas por anticipado.
Las ventajas de la gestión del SLA para los proveedores de servicios de Internet son muchas, entre otras permite:

- Diferenciar servicios.
- Pasar del acceso básico a nuevos servicios empresariales de valor agregado que requieren una elevada calidad de servicio.
- Resolver con más rapidez los problemas de funcionamiento.
- Diferenciar servicios y aumentar la satisfacción del cliente.

Para los clientes de los ISPs, los contratos de nivel de servicio bien gestionados permiten evaluar la calidad del servicio, descargar la gestión del servicio sobre el ISP, entender las garantías y recibir la calidad garantizada a un precio más bajo.

Los datos de consumo brindan información necesaria para trazar el perfil de los clientes potenciales de cada tipo de cuenta, los tipos de servicio que pueden interesarles, cuánto pueden estar dispuestos a pagar y qué recursos de red pueden consumir.

El análisis de los datos de consumo también proporciona información esencial para definir, gestionar y validar los SLAs. Por ejemplo, una representación gráfica de los datos de consumo puede revelar a un ISP que el 90% de los clientes consumidores utilizan menos de 1,9 MB de ancho de banda al día, mientras que el 90% de las empresas clientes utilizan aproximadamente 3,8 MB[1]. El conocimiento de estos umbrales permite al ISP calcular tipos de tarifa basados en límites de consumo y ofrecer la red de acuerdo con ello.

En este caso el ISP también puede establecer disparadores en tiempo real que indiquen cuando un cliente ha sobrepasado los límites de consumo acordados. El conocimiento de este dato hace posible la promoción dinámica de ese cliente a una clase más alta de servicio, una ventaja tanto para el ISP como para el cliente, porque una promoción dinámica de la calidad de servicio QoS permite asegurar que se seguirán respetando los niveles de funcionamiento definidos en el SLA, o sea que el cliente recibirá, siempre un servicio acorde con lo establecido.

## V.2 Diseño del Sistema

Con el crecimiento acelerado y sostenido de Internet se ha producido una proliferación de suministradores de servicios ISPs que ofrecen acceso por teléfono a través de la red telefónica pública, diseñada para tráfico de voz y no de datos. Esta red limitada está siendo

[1] www.firehunter.com

sometida a un gran esfuerzo de tráfico de datos, esfuerzo que se manifiesta en el servicio de Internet con poca calidad.
Con el objeto de estimar la calidad del servicio, el sistema utilizado para el desarrollo de esta tesis cuenta con interfaces de usuario para interactuar con esta plataforma [1].

- Admin Console (Consola de Administración)
- Graphical User Interface (GUI Interfaz Gráfica de Usuario)
- Web-based GUI
- Command Line

## V.3 Pruebas

Con ayuda de todas las herramientas antes mencionadas, se plantea monitorear las páginas más visitadas en México, pues son éstas, las que se encuentran más expuestas a entregar una calidad de servicio deficiente, debido al tráfico constante de información que manejan.

Dichas páginas fueron escogidas de acuerdo al número de visitantes que tuvieron durante el mes de Abril de 2004[2] , y clasificadas en cuatro categorías: Comerciales, Gobierno, Universidades y Buscadores como lo muestra la tabla 5.1.
Esta clasificación se realizo de acuerdo a un listado de las páginas más visitadas, obtenido del DNS de uno de los principales proveedores de Internet en México, al hacer una revisión de todas las páginas, nos dimos cuenta que podíamos agruparlas en las cuatro categorías antes mencionadas, de acuerdo a los servicios que prestan.

Se monitorearon cuatro páginas por cada categoría, para lograr estimar la calidad de servicio que entrega al usuario final cada una de estas categorías y poder así, tener una idea del comportamiento habitual de los servicios de Internet en México.

[2] Información obtenida por importante ISP de México, por medio de los accesos a su DNS

Se eligieron cuatro páginas por categoría debido a que con esto se tendrá un panorama general de cada una de las categorías y poder llegar a resultados más cercanos a la realidad.

La elección de estas cuatro páginas por categoría, se realizó de acuerdo al mayor número de apariciones en cada una de las clasificaciones. Dentro de la clasificación de las universidades cabe destacar la Universidad Nacional Autónoma de México y el sitio del Instituto Politécnico Nacional como las páginas más solicitadas por los usuarios de Internet, aunque muy cerca de ellas se encuentran dos universidades privadas, el Instituto Tecnológico de Estudios Superiores (ITESM)y la Universidad Tecnológica (UNITEC).

Otra categoría que tuvo gran demanda es la de los buscadores, debido a que más del 90% de las visitas de una página Web provienen de los motores de búsqueda, y de esta cifra Google y Yahoo son responsables de más del 75% del tráfico[3], mientras que el resto es repartido entre MSN, Altavista, elsitio y el resto de los buscadores.

Las clasificaciones de gobierno y comerciales están integradas por sitios que aunque no llegan a tener la demanda de los buscadores, el número de visitantes durante el mes de Abril fue significativo, destacando dentro de las páginas comerciales el sitio de Microsoft windowsupdate y en la clasificación de gobierno el portal de la Secretaria de Hacienda y Crédito Público.

Es importante mencionar que el monitoreo de todas las páginas seleccionadas se llevó a cabo dentro de la red de la Universidad Nacional Autónoma de México, específicamente dentro de los laboratorios de Microsoft de la Facultad de Ingeniería. Debido a que el Sistema con el que se monitoreó fue una donación a esta Facultad por parte de la Empresa Agilent Technologies.

[3] www.mastermagazine.info

| Clasificación | Páginas |
|---|---|
| **Comerciales** | http://www.t1msn.com.mx<br>http://www.estafeta.com<br>http://www.windowsupdate.com<br>http://www.symantec.com |
| **Gobierno** | http://www.shcp.gob.mx<br>http://www.segob.gob.mx<br>http://www.sre.gob.mx<br>http://www.sep.gob.mx |
| **Universidades** | http://www.unam.mx<br>http://www.unitec.mx<br>http://www.itesm.mx<br>http://www.ipn.mx |
| **Buscadores** | http://www.google.com<br>http://www.yahoo.com<br>http://www.elsitio.com.mx<br>http://www.altavista.com |

**Fig. 5.1** Clasificación de páginas monitoreadas

La primera clasificación con la que trabajaremos será la de buscadores, pues son estas, las más solicitadas por los clientes y debido a esto, las más expuestas a entregar una calidad deficiente.

Cabe mencionar que el complemento a las gráficas mostradas en este desarrollo, se encuentra contenido en el apéndice A.

Las cuatro páginas que serán monitoreadas se escogieron debido a la alta demanda de visitantes, pues como ya mencionamos el 90% de las visitas a páginas Web depende de esta clasificación y por obvias razones, son los buscadores las páginas más solicitadas por los usuarios.

Para ingresar un nuevo servidor de Web, dentro de nuestro modelo de servicio no es necesario conocer su IP, basta con ingresar su URL como lo muestra la Fig. 5.2. y automáticamente formará parte de nuestro modelo de servicio.

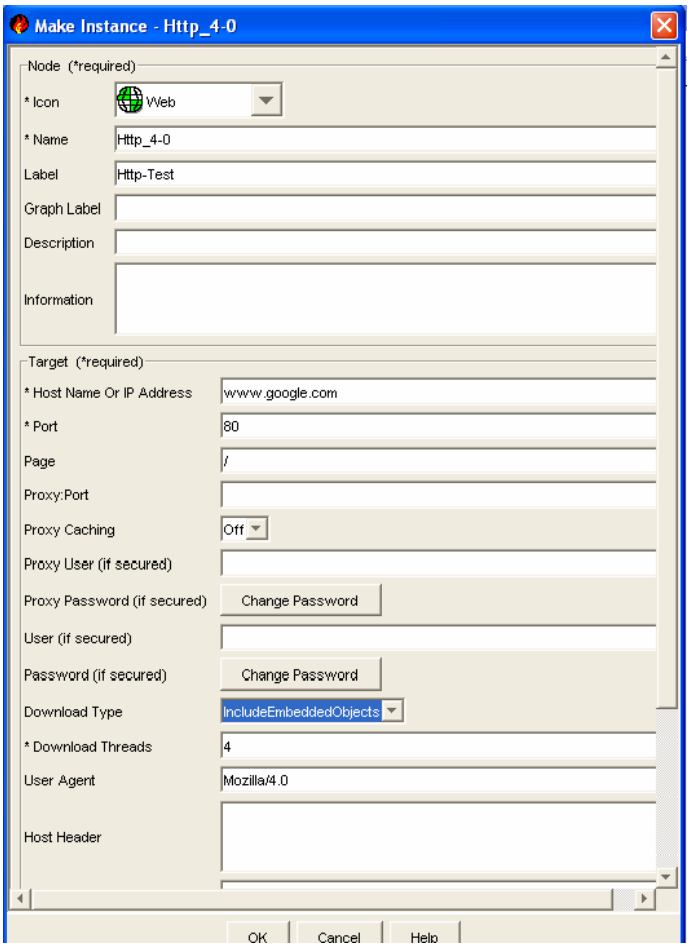


**Fig. 5.2.** Configuración de un nuevo Servidor

Para monitorear las cuatro páginas de buscadores, se agregó un servidor de Web para cada una de ellas y se fijaron los niveles de servicios que se desean cumplir Fig. 5.3, así como el intervalo de tiempo para realizar las mediciones; De acuerdo a las recomendaciones de sitios encargados de monitorear los servicios de Internet, basta con monitorearlos en un rango de 8 a 16 horas al mes[4] para tener un panorama general del estado de los servicios de Internet, como son el tiempo total de respuesta o la disponibilidad, tomando en cuenta estas

[4] www.integracion-de-sistemas.com

recomendaciones, se decidió monitorear por una semana continua dichos servicios tomando mediciones en las horas donde la demanda de estas páginas es mayor.

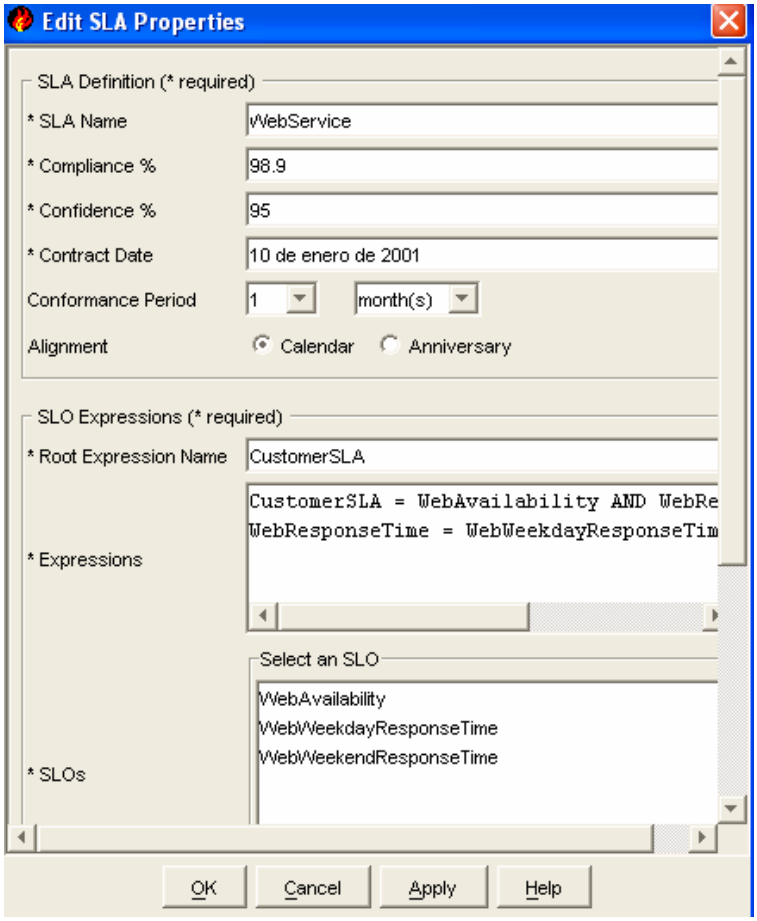


**Fig. 5.3** Configuración del SLA

El monitoreo de las páginas de buscadores, se llevo a cabo tomando mediciones como lo son: Disponibilidad, Tiempo de Respuesta, Prueba Completa, Tiempo DNS, Tiempo de Conexión TCP, Tiempo de Redirecionamiento, Tiempo de Respuesta del Servidor, Tiempo de Transferencia de Datos y Taza de Transferencia de Datos, estas nueve mediciones son cargadas automáticamente al configurar nuestro servidor de Web, pues vienen predefinidas dentro de las pruebas de http, como lo muestra la figura 5.4.

Dichas mediciones, muestran los resultados de forma gráfica, actualizando esta gráfica cada cinco minutos para poder tener una idea del estado actual del sitio de interés.

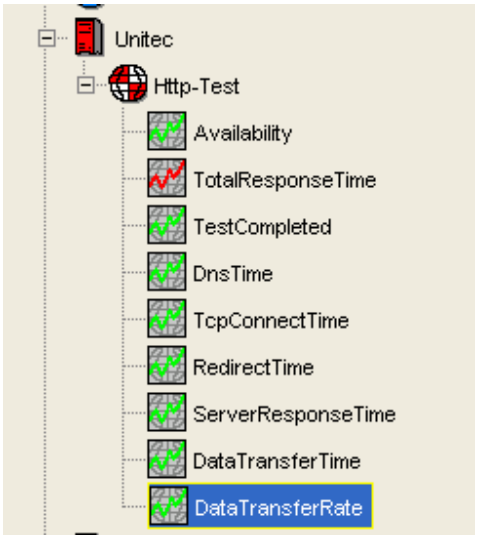


**Fig. 5.4** Mediciones para un Servidor http.

De las nueve mediciones hechas a las páginas de buscadores en el periodo de muestreo solo se rebasaron los límites de disponibilidad y el tiempo total de respuesta.

La primera página monitoreada es google, no solo porque es una de las más populares, sino por que actualmente es la página número uno en cuanto a usuarios de Internet[5].

En 1997 Larry y Sergey (creadores de Google) registraron el dominio 'google.com'. Además, dieron a conocer su tecnología a la 'Office of Technology Licensing' (OTL) google adquiere este peculiar nombre por su parecido a la palabra 'googol', que en inglés es el nombre que se da a la cifra '10 elevado a 100' (un uno seguido de 100 ceros). En los comienzos de Google (en el dominio google.stanford.edu), su diseño era muy austero y limitado para la gran cantidad de páginas hospedadas en el sitio. En Febrero de 1999 responde a 500.000 consultas por día, se trasladan a unas nuevas oficinas en Palo Alto, y firma su primer contrato comercial con RedHat, el cual empieza a suministrar el Sistema Operativo Linux de

[5] www.mastermagazine.info

los servidores de Google[6]. En la actualidad Google es uno de los buscadores más solicitados no solo en México, sino que es líder a nivel mundial.

En las pruebas realizadas google solo presentó pequeños problemas en cuanto a disponibilidad, y en lo que respecta a tiempo de respuesta, esta página muestra un buen tiempo de respuesta, solo por debajo de Altavista.

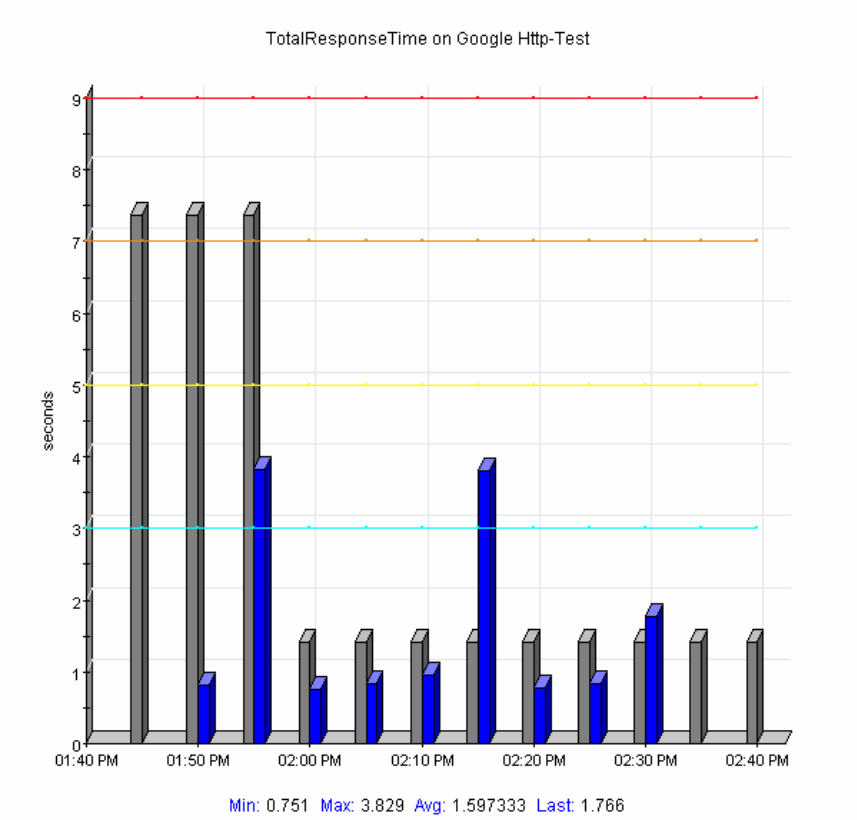


**Fig. 5.5** Gráfica Tiempo de Respuesta de Google.

En promedio, el tiempo mínimo de respuesta de esta página es de tan solo 0.751 seg. Y el máximo es de menos de 4 seg. Como lo muestra la gráfica 5.5. Si consideramos que el tiempo máximo para que responda una página se fijó en 10 seg. podemos decir que esta página no muestra ningún problema en cuanto a tiempo de respuesta.

[6] http://www-diglib.stanford.edu/.

El balance general de google es muy favorable, sus tiempos de respuesta son muy buenos ya que no rebasaron en ningún momento los umbrales establecidos.

La siguiente página monitoreada fue la de Altavista, otra de las páginas con más estabilidad y el record del menor tiempo en responder.
Altavista, que significa "una visión desde las alturas", se vio inspirada por la creación de grandes ideas de un equipo de expertos fascinados con el seguimiento de la información. Durante la primavera de 1995, los científicos del Laboratorio de investigaciones de Digital Equipment Corporation en Palo Alto, California, crearon una forma de almacenar todas las palabras de todas las páginas HTML de Internet en un índice rápido en el que se podían realizar búsquedas. Esto llevó al desarrollo de Altavista, la primera base de datos de texto completo en la que se podían realizar búsquedas en la World Wide Web.

La empresa añadió búsquedas multilingües con compatibilidad para 25 idiomas en 1997; lanzó 20 sitios locales de países entre 1999 y 2001; lanzó compatibilidad con búsqueda de archivos multimedia (audio, video, imágenes) en 1999; fue el primer motor de búsqueda importante que introdujo la búsqueda gratuita de noticias en Internet en 2001; y presentó Altavista Prisma™, su poderosa herramienta de búsqueda asistida, en 2002. Desde abril del 2003, Altavista forma parte de Overture[7].En lo que respecta a la disponibilidad del sitio Altavista, no tuvo ningún contratiempo, la página siempre se mantuvo disponible y trabajando con normalidad Fig. 5.6, manteniéndose por encima del 98.9% establecido en el SLA.

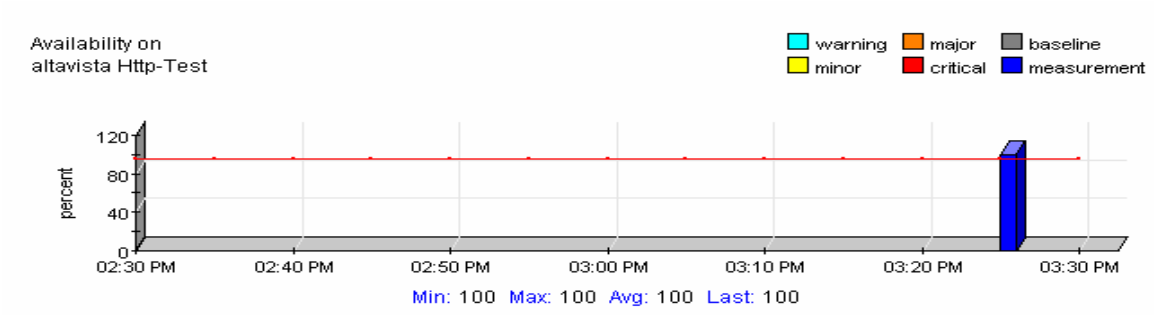


**Fig. 5.6** Gráfica Disponibilidad de Altavista.

[7] http://www.buscadores.ws/ficha_altavista.htm

Una de las explicaciones del porqué este sitio tiene mucho mejor tiempo de respuesta y su disponibilidad es superior a los demás, se debe a que su tasa de transferencia de datos es menor (Fig 5.7), es decir el número de usuarios es menor que el de google, por ejemplo. Debido a esto se encuentra menos expuesta a errores o retrasos por un tráfico excesivo.

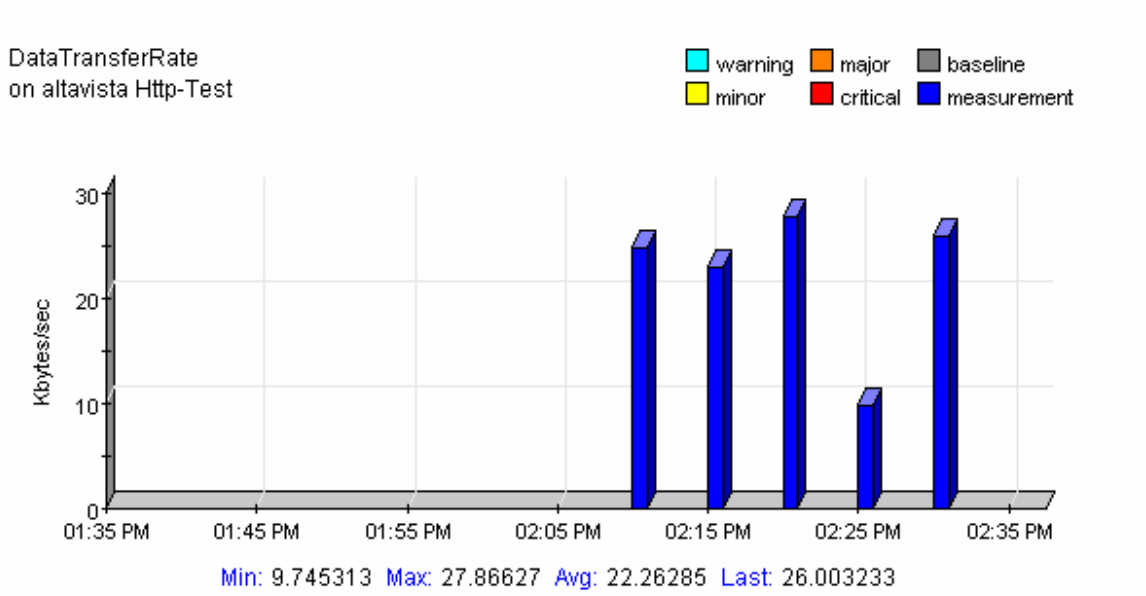


**Fig. 5.7** Gráfica Tasa de Transferencia de Altavista.

Siguiendo con la tasa de transferencia, toca el turno analizar a elsitio, la página con más conflictos de los cuatro buscadores que analizamos, esta página esta establecida en varios países de América como Argentina, Chile, México, Uruguay, Colombia, USA y Brasil cuenta con el algoritmo de búsqueda menos poderoso, por ello, es el menos solicitado y el que mayor conflicto muestra en cuanto a tiempos de respuesta Fig. 5.8. Sus tiempos de respuesta son muy altos, el promedio de respuesta anda por los 10 seg. que es el límite superior permitido, lo que muestra un gran problema, pues llega a tener picos en tiempos de respuesta de hasta 25 seg.

Su tasa de transferencia de datos es muy baja, comparada con los demás buscadores, pues oscila entre los 1- 3 Kilobytes/seg., mientras que google tiene una tasa de 20 hasta 100 Kilobytes/seg. En cuanto a la disponibilidad de esta página, no existe ningún problema pues es del 100% durante el periodo de muestreo.

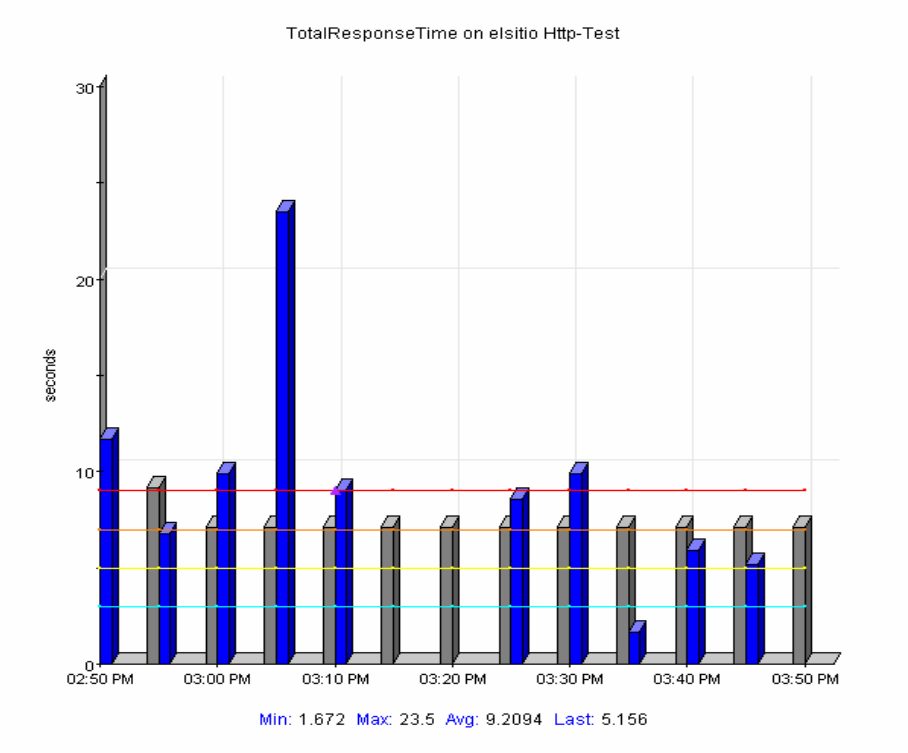


**Fig. 5.8** Gráfica Tiempo Total de Respuesta de elsitio.

Por último, la página propuesta para monitorear fue la de yahoo. El tráfico de Yahoo! sobrepasó las 100.000 visitas por día para fines de 1994, desde un modesto arranque de sólo un par de miles por día al principio del lanzamiento oficial de Yahoo!. Yang y Filo (los creadores) podían tranquilamente afirmar que estaban logrando más actividad en la Web que cualquier otra persona en el mundo y sin marketing. (Un años después, las visitas diarias a la página Web de Yahoo alcanzaron a un millón y a fines de 1998, un notable de 167 millones). Lo que comenzó como un pasatiempo se convirtió en una preocupación. Yang y Filo sabían que no iban a permanecer en Stanford y sabían también que los recursos informáticos de la Universidad de Stanford no estaban equipados para acomodar su servicio[8].

Después de varios años de estar en la Web, Yahoo! Se convirtió en uno de los buscadores favoritos de los mexicanos, y es por ello que es sujeto de ser monitoreada en esta tesis. Yahoo es un sitio, que aunque sus tiempos de respuesta no son tan buenos como los de Altavista o los de google, no rebasó el umbral de los 10seg. Fig. 5.9.

[8] www.yahoo.com

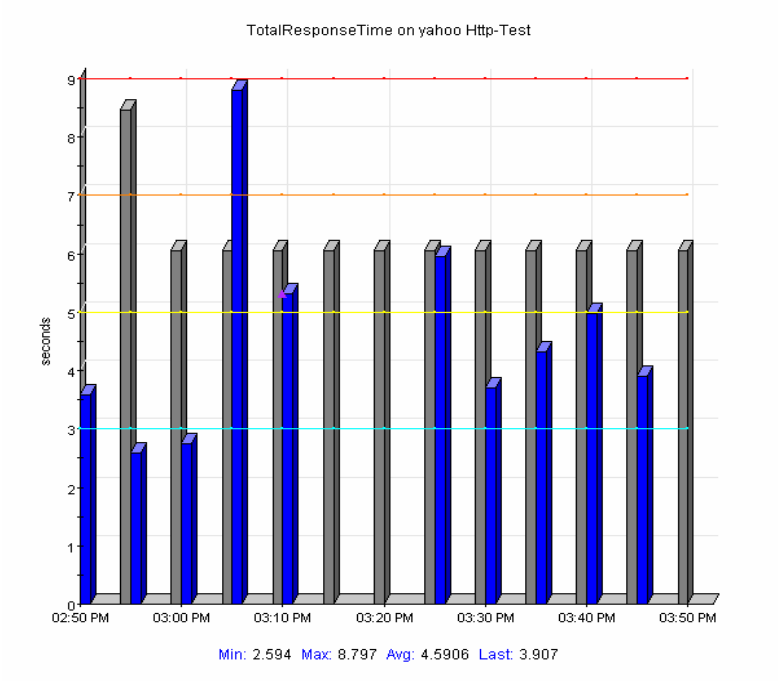


**Fig. 5.9** Gráfica Tiempo Total de Respuesta de Yahoo!.

En cuanto a la disponibilidad este buscador no presentó ningún problema, ya que siempre se mantuvo activa. La tasa de transferencia de datos también era alta, y aunque no se comparaba con la de google, también es una página que tiene mucha actividad.

La segunda clasificación que vamos a analizar es la de Universidades. En este grupo contamos con cuatro de las principales Universidades en México, la Universidad Nacional Autónoma de México (UNAM), El Instituto Politécnico Nacional (IPN), Instituto Tecnológico de Monterrey (ITESM) y la UNITEC.
Cabe mencionar que dentro de estas cuatro páginas más visitadas de universidades se encuentra nuestra máxima casa de estudios, la UNAM, es orgullo y satisfacción monitorear la página de la universidad, para la que fue donado este software.

En el mes de Abril de 1910 Justo Sierra presentó, la Ley Constitutiva de la Escuela Nacional de Altos Estudios, que formaría parte de la Universidad; después, el día 26 del mismo mes, el proyecto para la fundación de la Universidad Nacional.

La nueva institución estaría constituida por las escuelas Nacional Preparatoria, de Jurisprudencia, de Medicina, de Ingenieros, de Bellas Artes. Por fin, después de aprobado el proyecto, el 22 de Septiembre de 1910 tuvo lugar la inauguración solemne de la Universidad Nacional de México[9].

En el año de 1921 surge la iniciativa vasconcelista que más ha perdurado: la ley que establece el escudo y el lema de la institución, “Por mi raza hablará el espíritu”, junto con la imagen del águila y el cóndor que rodean el mapa que representa a la América Latina.

En el Año de 1954 se hizo la entrega formal de la Ciudad Universitaria a la Universidad, un año más tarde la población universitaria era de 36 mil 165 alumnos, de los cuales más de 10 mil eran de primer ingreso.

La Universidad Nacional Autónoma de México representa más del 50% de la Investigación en nuestro país, como muestra, el 5 de Septiembre de 1996 la UNAM se convirtió en la tercera institución del mundo que lanza al espacio su propio satélite, el satélite fue diseñado y construido totalmente por científicos mexicanos de la Máxima Casa de Estudios.

Es por todo esto, que la página de Internet de la UNAM es una de las más visitadas en México, por ello, está expuesta a rebasar los límites permitidos para ofrecer un servicio de calidad.

En cuanto al tiempo de respuesta, las páginas de las universidades no tienen grandes diferencias, pues su tiempo de respuesta es muy similar, solo existen pequeños intervalos de tiempo donde se rebasan los límites establecidos como aceptables Fig. 5.10.

[9] www.unam.mx

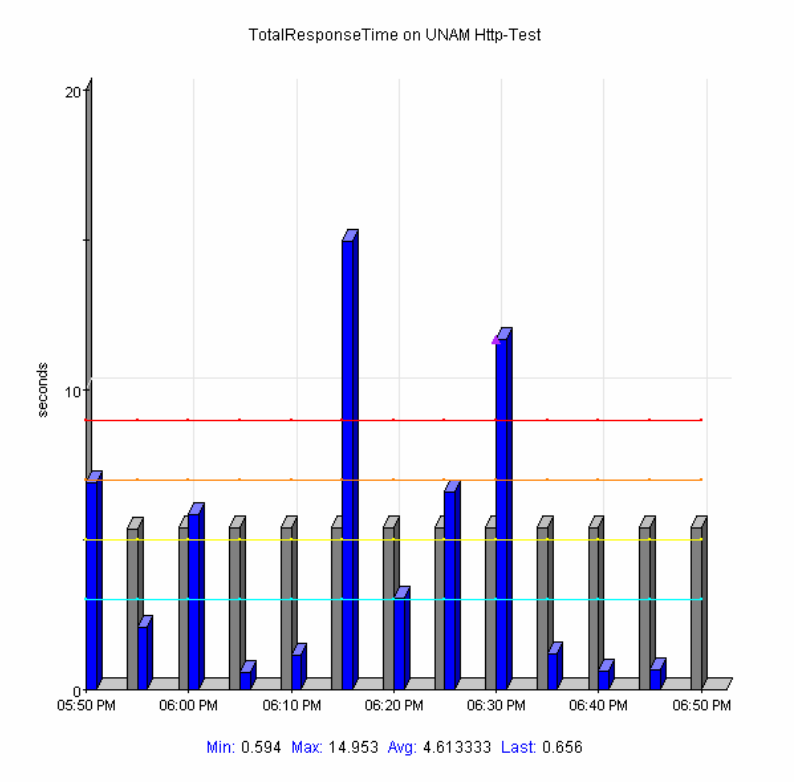


**Fig. 5.10** Gráfica Tiempo Total de Respuesta de la UNAM.

Es importante decir que estos picos se deben a que la página de la UNAM es una de las más solicitadas y es la que tiene mayor tasa de transferencia Fig. 5.11. El promedio de tiempo de respuesta de la UNAM es de 7.7 seg. Aunque no es el mejor tiempo de respuesta, si es un tiempo aceptable, pues no pasa nuestros límites permitidos.

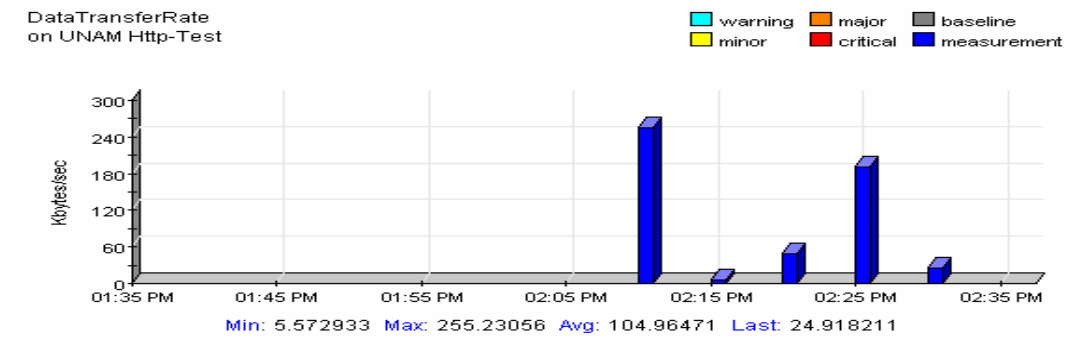


**Fig. 5.11** Gráfica Tasa de transferencia de la UNAM.

De todas las páginas de universidades, la UNAM es la que tiene mayor tasa de transferencia, esto es, la velocidad media con que los datos son transferidos desde la red del ISP al usuario es la mejor de todas las páginas de universidades monitoreadas. Es importante mencionar que como el monitoreo se realizo dentro de la UNAM interviene de manera considerable para que los tiempos de respuesta sean menores y que la tasa de transferencia sea alta, debido a que influye que tan lejano esta el servidor donde se encuentra cargada la página.

Toca el turno de monitorear la página del ITESM, el Instituto Tecnológico de Estudios Superiores de Monterrey fue fundado en el año de 1943 por un grupo de empresarios regiomontanos encabezados por don Eugenio Garza Sada[10].

El Tecnológico de Monterrey tiene como misión, formar personas comprometidas con el desarrollo de su comunidad y que sean competitivas en su área de conocimiento. El Tecnológico también cuenta con una universidad virtual que ofrece sus programas académicos y de educación continua en México y Latinoamérica.

El Instituto Tecnológico de Estudios Superiores de Monterrey es un conjunto de diversas organizaciones y fundaciones nacionales e intencionales. Al monitorear la página del Tecnológico, nos pudimos dar cuanta que su tasa de transferencia es menor (Fig. 5.12) que la página de la UNAM. Este poco tránsito de información hace que la página sea más lenta, y esta expuesta a ofrecer una calidad deficiente.

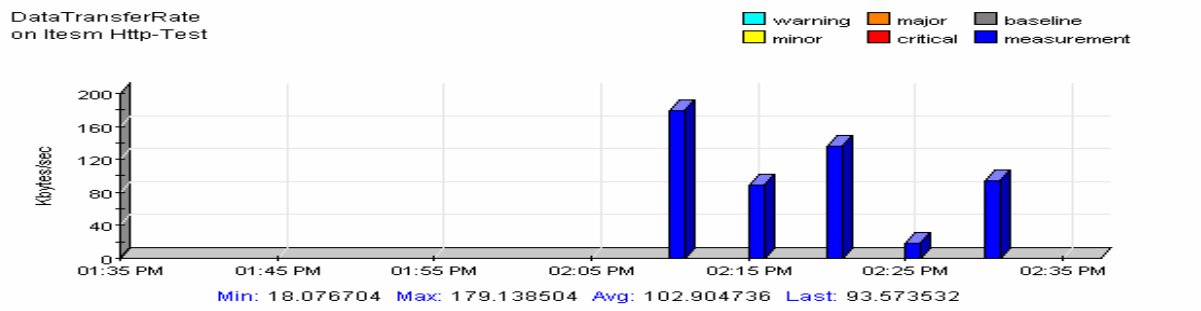


**Fig. 5.12** Gráfica Tasa de transferencia del ITESM.

[10] www.itesm.mx

El promedio de su transferencia de datos anda entre los 98 KiloBytes/seg, y aunque es el segundo en cuanto a tasas de Transferencia, no llega a ser como el de la UNAM. En cuanto a la disponibilidad, fue la única universidad, que tuvo problemas, pues llegaba a estar sin disponibilidad en pocos periodos de tiempo, como lo muestra la Fig. 5.13.

Esta figura muestra en la misma Gráfica, un comparativo entre la disponibilidad y el tiempo total de respuesta, el área marcada con el número 1, muestra la disponibilidad de la página, y en ella podemos ver que dicha página no estuvo disponible a las 12:35.

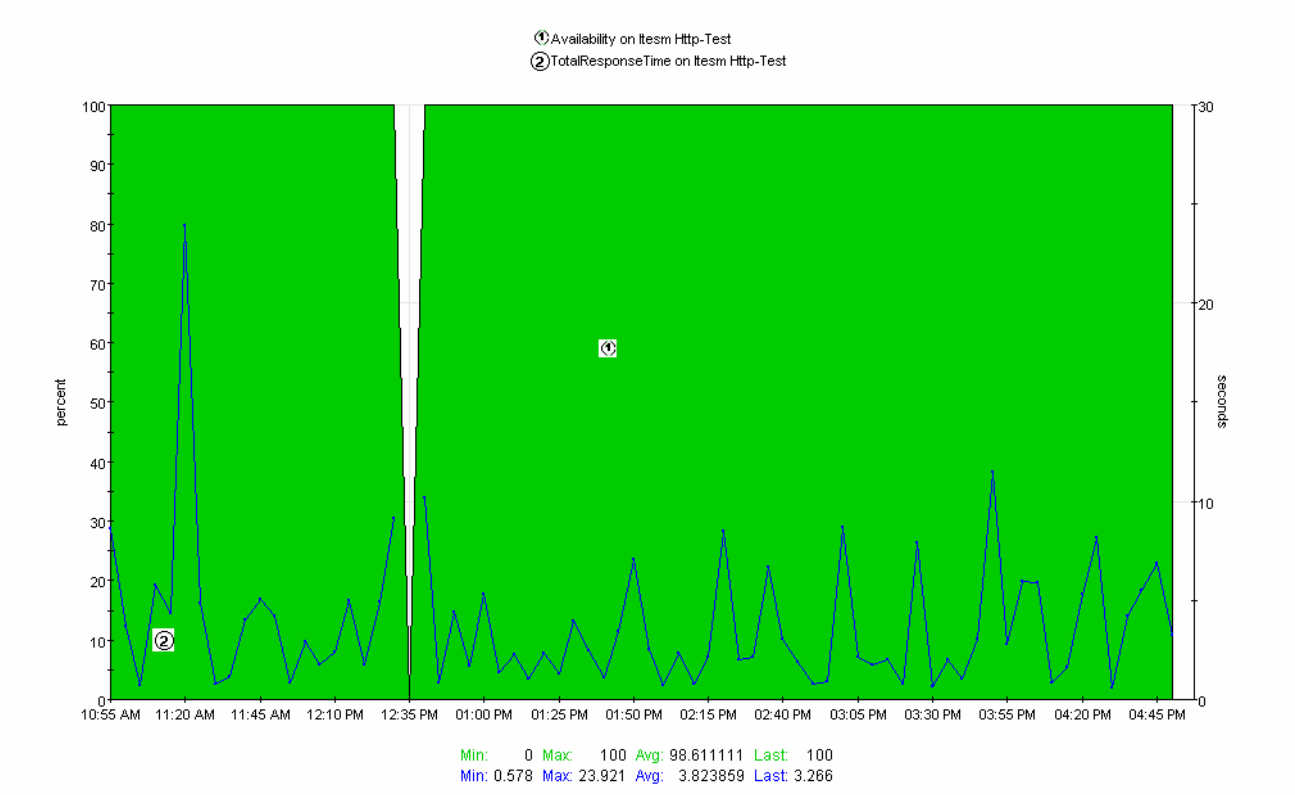


**Fig. 5.13** Gráfica Disponibilidad vs Tiempo de Respuesta del ITESM.

En lo que respecta al tiempo de respuesta, la página muestra un tiempo de respuesta que sobrepasa el limite superior permitido, pues su promedio de tiempo anda por los 12.2 seg.

Este tiempo elevado se debe a que la página muestra muchos gráficos, que aunque son agradables a la vista del usuario, saturan y hacen que el tiempo de respuesta sea mayor.

Otra universidad que fue candidata a ser monitoreada es la del Instituto Politécnico Nacional IPN. El IPN es una institución educativa laica, gratuita de Estado, rectora de la educación tecnológica pública en México, líder en la generación, aplicación, difusión y transferencia del conocimiento científico y tecnológico junto con la UNAM, creada para contribuir al desarrollo económico, social y político de la nación.

El IPN es una institución educativa innovadora, flexible, centrada en el aprendizaje; fortalecida en su carácter rector de la educación pública tecnológica en México; poseedora de personalidad jurídica y patrimonio propios, con capacidad de gobernarse a sí misma; enfocada a la generación y difusión del conocimiento de calidad; caracterizada por procesos de gestión transparentes y eficientes; con reconocimiento social amplio por sus resultados y sus contribuciones al desarrollo nacional; por todo ello, posicionada estratégicamente en los ámbitos nacional e internacional.

Participa en el Sistema Educativo Nacional, comparte recursos intra y extra institucionales, intercambia información y conduce proyectos educativos y de investigación conjuntos, ubicando su operación en rangos de excelencia definidos por indicadores internacionales, constituyéndose en referentes del Sistema Nacional de Educación Científica y Tecnológica. Cuenta con un sistema de educación virtual consolidada, con programas educativos y de formación a lo largo de la vida.

Durante el monitoreo la página del Instituto Politécnico Nacional fue ejemplo en lo que respecta a tiempos de respuesta Fig. 5.14.

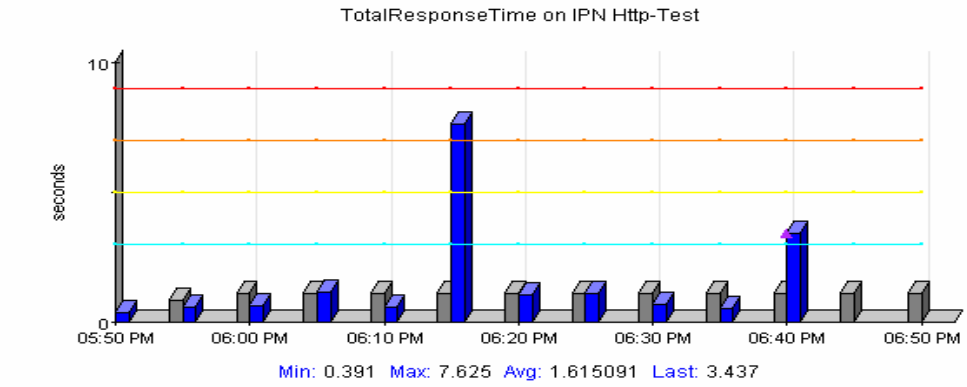


**Fig. 5.14** Gráfica Tiempo de Respuesta de IPN.

Sus tiempos de respuesta son muy bajos, teniendo un tiempo de respuesta mínimo de 0.39seg. y pocas veces, o casi nunca rebaso el límite superior de los 10seg., como lo podemos observar en la Gráfica 5.14.

En cuanto a la disponibilidad, la página siempre se mantuvo disponible, y trabajando adecuadamente, y aunque la tasa de transferencia no se compara con la del ITESM o la de la Universidad Nacional Autónoma de México, podemos decir que tiene una actividad considerable.

La última universidad que se monitoreo es la Universidad Tecnológica de México (UNITEC), esta Universidad tuvo su origen hace 37 años. La primera instalación de la UNITEC, nace en 1966, en Avenida Chapultepec No. 412, en la Ciudad de México, donde sólo se impartían las Licenciaturas en Administración de Empresas y Contaduría Pública.

En el 2001, para promover la visión emprendedora de la Comunidad Universitaria, se inauguró la Incubadora de Empresas en Negocios Electrónicos y Tecnología de Información. La primera en Latinoamérica y un espacio para que alumnos, profesores y empresas desarrollen sus ideas de negocios en proyectos viables y financiables[11].

En abril de 2001, la Federación de Instituciones Mexicanas Particulares de Educación Superior (FIMPES) le otorgo a la Universidad Tecnológica de México el máximo status de calidad, el de Institución Acreditada.

Al monitorear la página de la UNITEC, nos dimos cuanta, que de las universidades, es la que presenta más problemas en cuanto a tiempo de respuesta, pues tiene picos que sobrepasan los 30seg. y para un usuario, es un tiempo excesivo que lo hará cerrar la página y buscar otras opciones. Este problema tiene causas muy similares a las del ITESM, pues se enfocan más en el aspecto estético, y saturan de gráficos y animaciones sus sitos, esto hace que la página tarde mucho más tiempo en responder (Fig. 5.15).

[11] www.unitec.mx

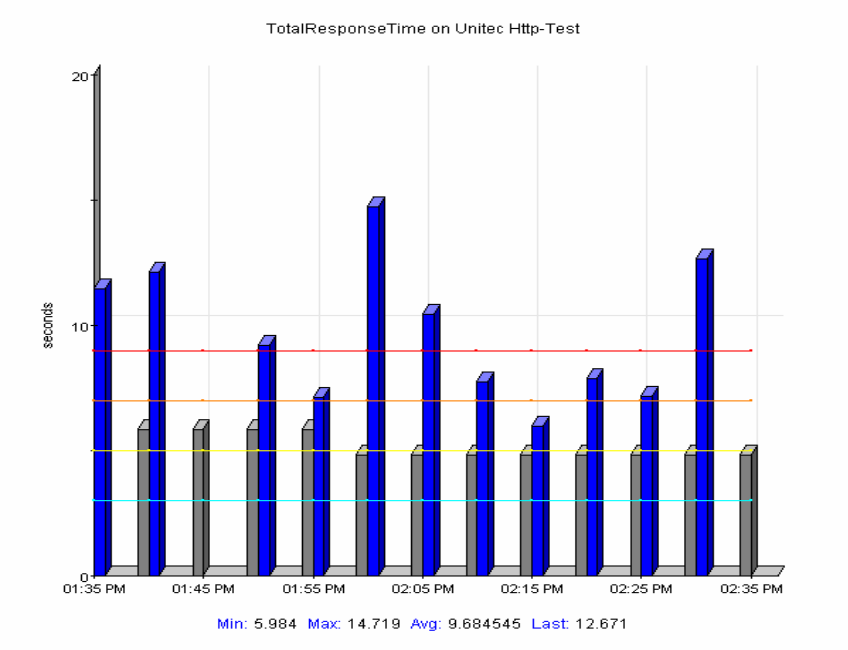


**Fig. 5.15** Gráfica Tiempo de Respuesta de UNITEC.

La disponibilidad de este sitio no presentó ningún contratiempo, pues siempre estuvo disponible. En cuanto a su tasa de transferencia, es la página que menos tráfico presentó, pues su tasa de transferencia oscila entre los 20 y 40 kiloBytes/seg. (Fig. 5.16), que comparado con los 300KiloBytes/seg. de la Universidad Nacional Autónoma de México es mínima.

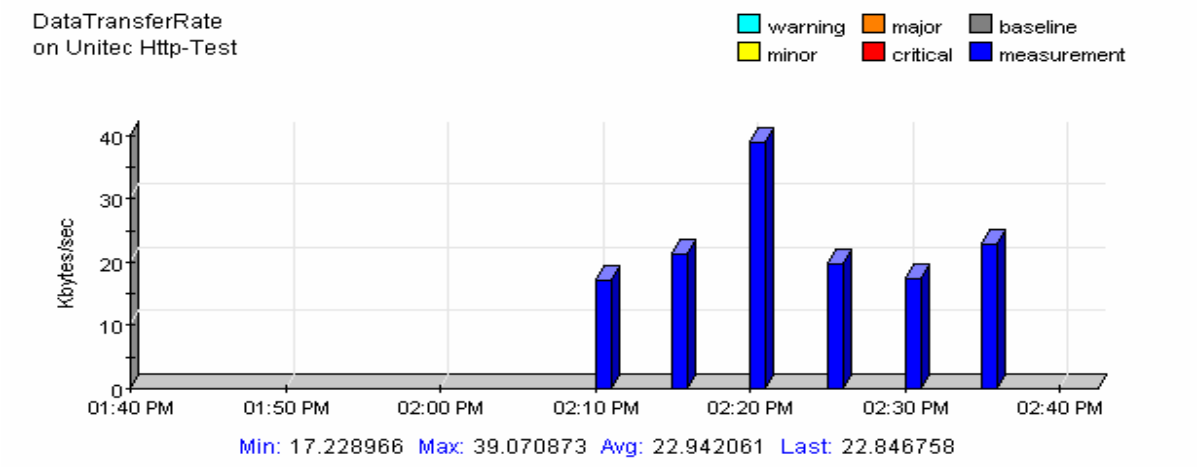


**Fig. 5.16** Gráfica Tasa de Transferencia de UNITEC.

La siguiente clasificación que toca analizar son las páginas del gobierno, entre las que se encuentran: La Secretaria de Hacienda y Crédito Publico (SHCP), la Secretaria de Relaciones Exteriores (SRE), la Secretaria de Gobernación (SEGOB) y por ultimo la Secretaria de Educación Pública (SEP).

Esta selección de las páginas se hizo con el mismo criterio que las anteriores, pues fueron las más visitadas en el mes de Abril del 2004.

La primera página monitoreada fue la Secretaria de Hacienda y Crédito Público. El 27 de mayo de 1852, se publicó el Decreto por el que se modifica la Organización del Ministerio de Hacienda, quedando dividido en seis secciones, siendo una de ellas la de Crédito Público; antecedente que motivó que en 1853 se le denominara por primera vez Secretaría de Hacienda y Crédito Público.

Con las reformas y adiciones a la Ley Orgánica de la Administración Pública Federal del 29 de diciembre de 1982, se le confirieron nuevas atribuciones a la Secretaría de Hacienda y Crédito Público en materia de planeación, coordinación, evaluación y vigilancia del sistema bancario del país, derivadas de la nacionalización bancaria, así como en materia de precios, tarifas y estímulos fiscales.

A fin de fortalecer la cohesión de la política económica y con ello contribuir a la consolidación de la recuperación económica, de la estabilización y del financiamiento del desarrollo, el 21 de febrero de 1992, mediante el Decreto que deroga, reordena y reforma diversas disposiciones de la Ley Orgánica de la Administración Pública Federal, se dispuso la fusión de las Secretarías de Programación y Presupuesto y de Hacienda y Crédito Público. Con esta medida, a la Secretaría de Hacienda y Crédito Público se le confirieron, además de las atribuciones en materia fiscal, financiera y crediticia, las de programación del gasto público, de planeación y de información estadística y geográfica.

Finalmente, el 10 de junio de 1998 se publican en el **Diario Oficial de la Federación** reformas a los Reglamentos Interiores de la Secretaría de Hacienda y Crédito Público y del órgano desconcentrado Servicio de Administración Tributaria, así como un nuevo Acuerdo de

adscripción de unidades administrativas de la Secretaría, efectuándose los siguientes cambios a la estructura orgánica básica de la Secretaría.

Conforme a lo expuesto, la estructura orgánica básica actual de la Secretaría de Hacienda y Crédito Público, queda conformada por: 1 Secretario, 3 Subsecretarios, 1 Procurador Fiscal de la Federación, 1 Tesorero de la Federación, 1 Oficial Mayor, 1 Coordinación General, 37 Direcciones Generales o unidades equivalentes y 2 Órganos Desconcentrados[12].

Al estar monitoreando la página de la SHCP, nos dimos cuenta que los tiempos de respuesta son de los mejores, pues existen grandes diferencias entre las otras páginas de la misma clasificación. Aunque sus tiempos de respuesta no son tan buenos como el de otra clasificación como el de Universidades o el de Buscadores, comparada con las otras páginas del gobierno, sus tiempos son buenos Fig.5.17.

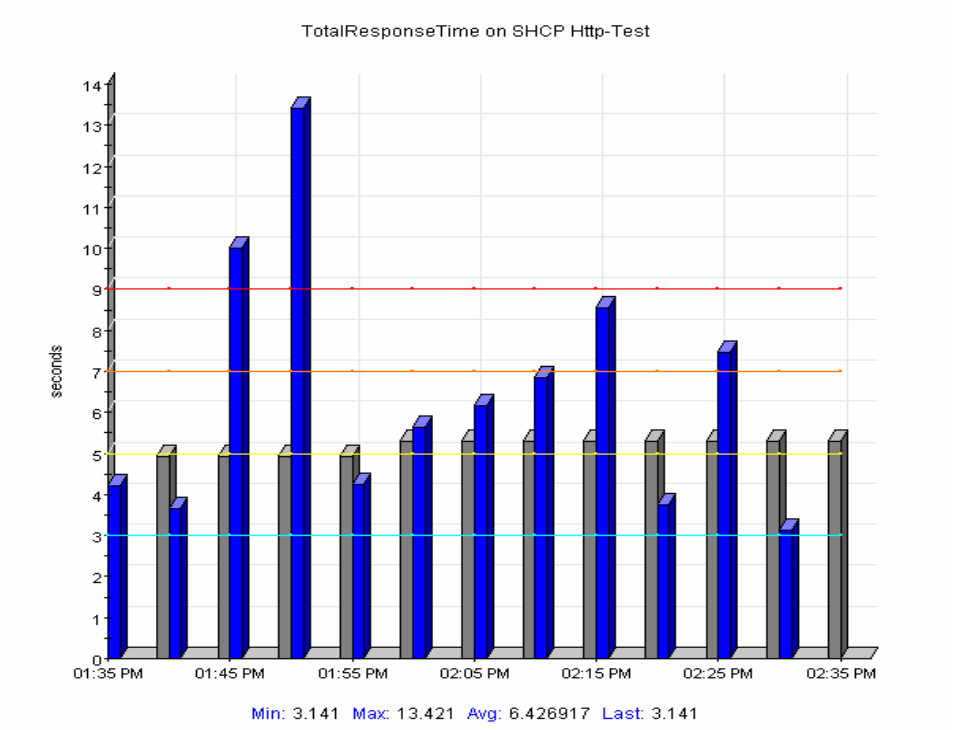


**Fig. 5.17** Gráfica Tiempo de Respuesta de la SHCP.

[12] www.shcp.gob.mx

En la Figura 5.17 nos podemos dar cuenta que el tiempo de respuesta promedio oscila entre los 9 y 10 KiloBytes/seg., es decir están en el límite permitido.

La página de la SHCP nunca tuvo problemas de disponibilidad, y con una tasa de transferencia baja (Fig. 5.18), pues comparativamente con las páginas de las otras clasificaciones como la de universidades o la de buscadores, su actividad es mínima.

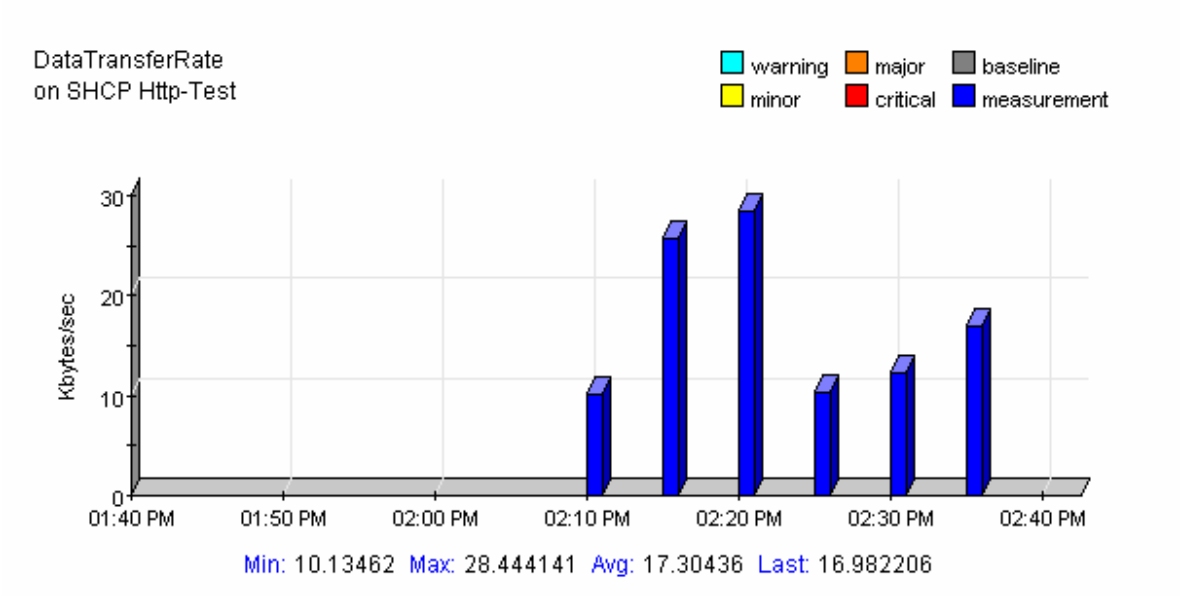


**Fig. 5.18** Gráfica Tasa de Transferencia de Datos de la SHCP.

La Segunda página monitoreada de esta clasificación fue la de la Secretaria de Relaciones Exteriores (SRE). Esta secretaria forma parte de la línea estratégica de "Garantizar un Gobierno de Calidad Total", la Secretaría de Relaciones Exteriores asume el compromiso de implantar, mantener y mejorar Sistemas de Gestión de la Calidad para sus procesos clave, en beneficio de los clientes y usuarios de sus servicios[13].

Procurar la implantación, mantenimiento y mejora de los servicios que presta SRE., en beneficio de los clientes y usuarios de sus servicios.

Al estar monitoreando esta página, nos damos cuenta que cae en serias contradicciones, pues el “gobierno de calidad total” que se promete, al menos en los servicios que presta a

[13] www.sre.gob.mx

través de Internet, no lo es, pues es la página con el peor tiempo de respuesta (Fig. 5.19) de todas las páginas monitoreadas.

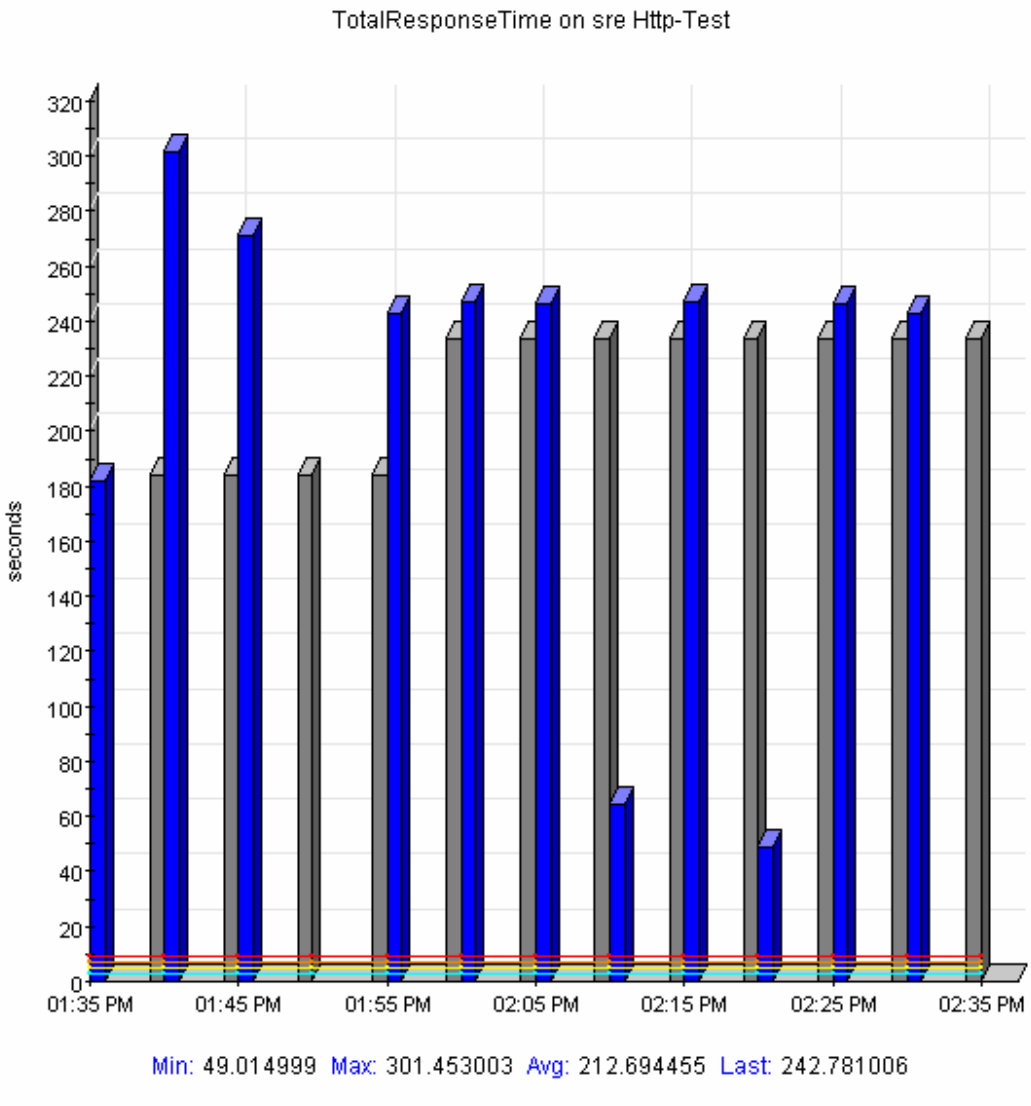


**Fig. 5.19** Gráfica Tiempo de Respuesta de la SRE.

En esta figura podemos ver que los límites permitidos de tiempo de respuesta se ven seriamente rebasados ya que se acordó en el SLA que no debería ser mayor de los 10 seg. y en el grafico se ve claramente que el menor tiempo de respuesta hecho por esta página fue de 49 seg. lo que demuestra que rebasa por casi 5 veces el límite superior permitido.

Es excesivo el tiempo total de respuesta promedio, pues es de 175 seg. Esto se debe a la baja transferencia de Datos (Fig. 5.20), pues no llega ni a 1 KiloByte/seg.

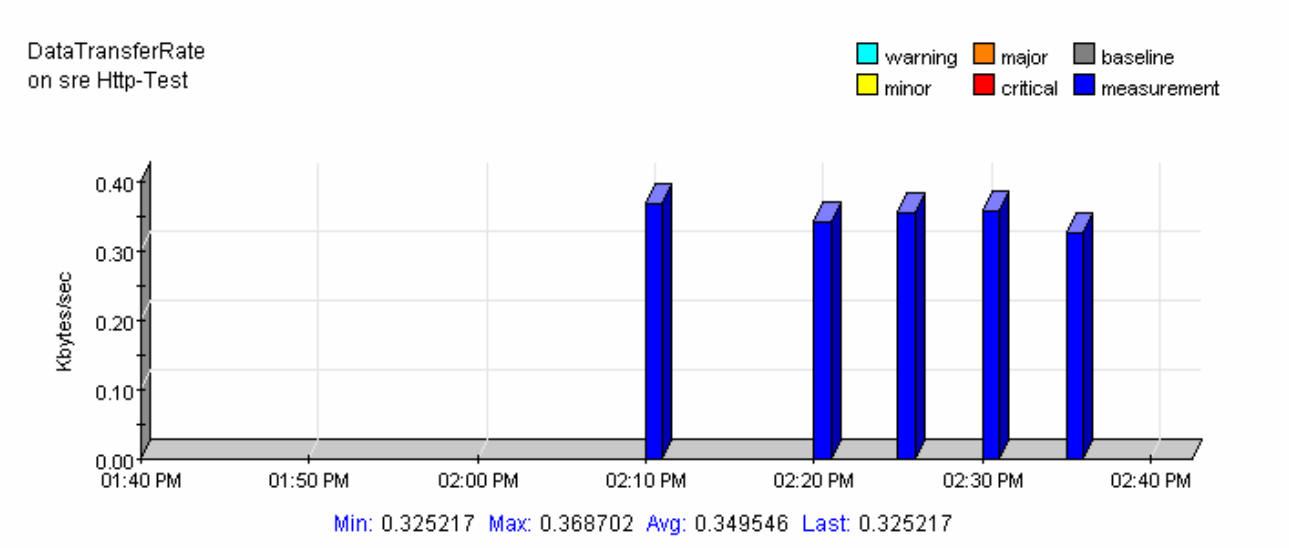


**Fig. 5.20** Gráfica Tasa de Transferencia de Datos de la SRE.

Esta página se encuentra en una grave situación, pues pierde muchos usuarios al ser tan grande su tiempo de respuesta, y tan baja su tasa de transferencia de datos.

De todas las páginas monitoreadas en este trabajo de investigación, la página de la Secretaria de Relaciones Exteriores, es la que nos presenta los peores resultados en: Tiempos Total de Respuesta, Disponibilidad y Tasa de Transferencia de Datos.

La tercera página de Gobierno monitoreada, es la de la Secretaria de Educación Pública, esta secretaria (SEP).

La SEP tiene como propósito esencial crear condiciones que permitan asegurar el acceso de todas las mexicanas y mexicanos a una educación de calidad, en el nivel y modalidad que la requieran y en el lugar donde la demanden.

La página de la SEP, es el espacio principal en Internet que la Secretaría de Educación Pública pone a disposición del público en general, donde se pueden consultar trámites y servicios del Sector Educativo, información sobre la educación en México, secciones

especializadas en la educación básica, media superior y superior, indígena, niños, docentes y tecnológica, calendario escolar, información institucional, así como también provee ligas a sitios afines al tema a nivel mundial[14].

El Portal SEP, cuenta con una gran gama en aspectos de Infraestructura Tecnológica y metodológica, que nos permite ofrecer mayores beneficios en cuanto a estructura de la información, mejores métodos de navegación entre secciones o páginas, destacando la manera sencilla de usar el portal SEP.

El sitio de la SEP es el orgullo de esta clasificación, pues es la mejor en tiempo de respuesta, su promedio de respuesta esta entre los 2 y 2.5 seg. Un excelente tiempo aun comparado con las demás clasificaciones.

Y aunque su Tasa de Transferencia de Datos no es tan alta como el de Google o el de la UNAM, si es buena, su promedio es de 29 KiloByte/seg. Fig. 5.21.

Existe una abismal diferencia entre la página anteriormente monitoreada (SRE) y la página de la Secretaria de Educación Pública. El ejemplo más claro es el tiempo de respuesta, el portal de la SEP compite en tiempo de respuesta con los mejores tiempos de respuesta de las otras clasificaciones, mientras que el sitio de la Secretaria de Relaciones Exteriores el peor tiempo de respuesta de todos los sitios.

Aunque el portal de la Secretaria de Educación Publica también tiene muchos gráficos, que podrían hacer que su tiempo total de respuesta creciera, no es así, es el único sitio de gobierno que se interesa y ocupa por tener una estructura de la información que mejore los métodos de navegación y poder así reducir los tiempos. En cuanto a la disponibilidad, este sitio también es ejemplo a seguir, ya que siempre se mantuvo disponible en el periodo de monitoreo.

[14] www.sep.gob.mx

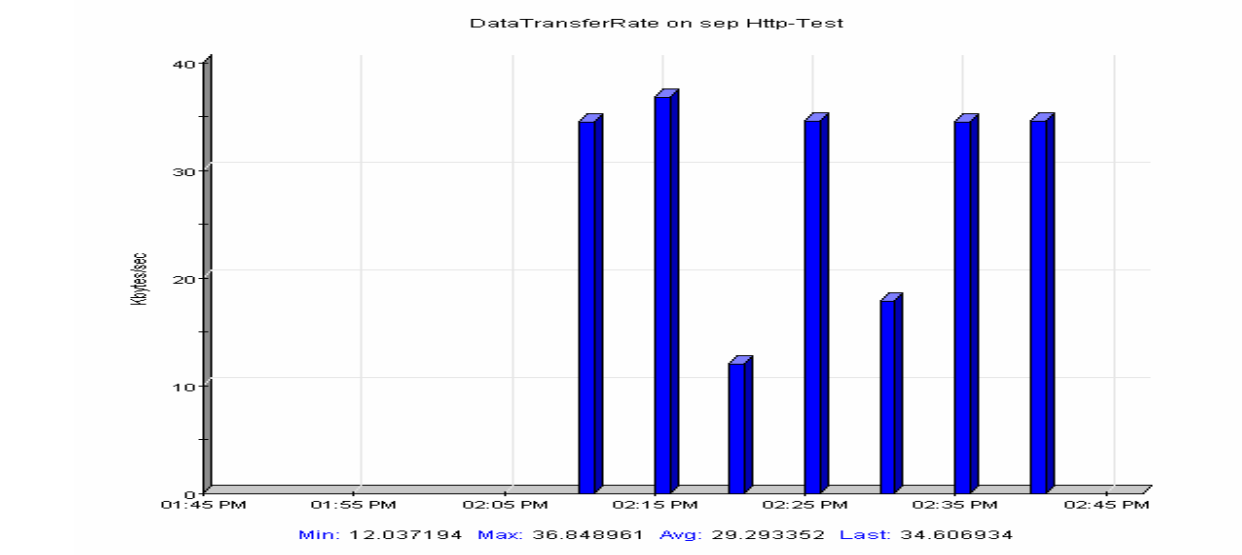


**Fig. 5.21** Gráfica Tasa de Transferencia de Datos de la SEP.

Toca el turno de analizar la página de la Secretaria de Gobernación (SEGOB), desde sus inicios, la Secretaría de Gobernación tiene encomendada la adecuada conducción de la política interna del país que permita a través de programas, acciones y estrategias el desarrollo de una sociedad cada vez más participativa en las acciones del Gobierno para satisfacer sus demandas; permitiendo con ello un crecimiento en ámbito económico, político y social del país.

Es por ello que el Ejecutivo Federal teniendo como responsabilidad la consolidación de un Estado de Derecho que fomente sus bases en los principios de legitimidad y legalidad, ha encomendado a esta Secretaría la elaboración de programas y estrategias que permitan la democratización de la sociedad mediante el diálogo, el consenso y orden, que la Constitución Política de los Estados Unidos Mexicanos emana, fortaleciendo así la soberanía y el régimen federal[15].

El proceso de globalización a nivel mundial en el cual estamos inmersos, obliga a los Gobiernos a crear nuevas formas de organización social para que esta se involucre en el proceso de cambio. De esta manera, corresponde a la Secretaría de Gobernación vigilar que la relación entre el Estado y la sociedad organizada en asociaciones civiles, gremiales,

[15] www.segob.gob.mx

empresariales, comunitarias y de ayuda mutua se realicen apegadas al Estado de Derecho, respetando su integridad y fortaleciendo la separación de los Poderes de la Unión.

Para fortalecer más la relación entre el gobierno y la sociedad, la Secretaria de Gobernación crea el sitio en Internet que es sujeto de monitorearse en este trabajo.

Al estar monitoreando la página nos damos cuenta que el tiempo de respuesta no es tan bueno, rebasa considerablemente los limites permitidos Fig. 5.22.

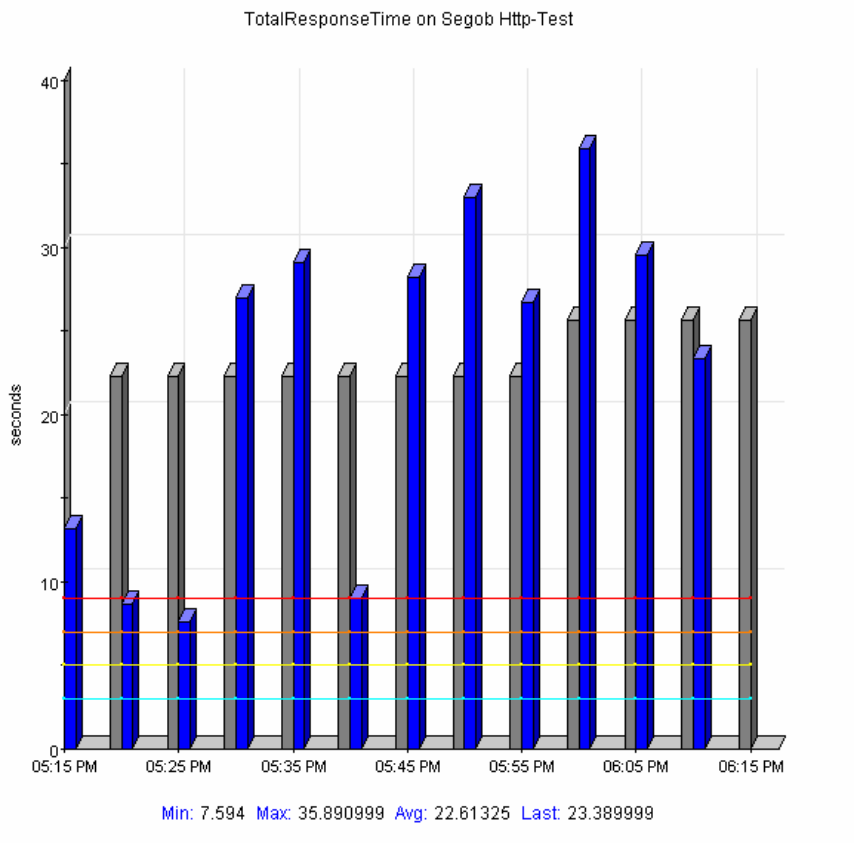


**Fig. 5.22** Gráfica Tiempo Total de Respuesta SEGOB.

Y aunque no llega a ser tan malo como el de la Secretaria de Relaciones Exteriores, su tiempo promedio es de 22.6 seg.

En cuanto a la tasa de transferencia de datos, es muy similar a la de la Secretaria de Educación Pública, su promedio es de 26 KiloBytes/seg. Y solo presentó pequeños problemas de disponibilidad, pues solo por un pequeño periodo de tiempo la página estuvo sin disponibilidad.

Esta fue la última página de la clasificación de Gobierno, y ahora toca el turno a la clasificación de páginas comerciales, esta categoría está formada por la página de la compañía de mensajería estafeta, el sitio de t1msn, el portal de Microsoft, específicamente el de windowsupdate y por último, la página de la compañía Symantec.

La primera página monitoreada es la de Estafeta, Estafeta es la empresa pionera y líder en servicios de mensajería y paquetería en el mercado mexicano desde hace 25 años.

Diariamente distribuye por vía terrestre y aérea alrededor de 100,000 envíos a más de 2,500 poblaciones, mediante 1,500 vehículos, 4 aviones Boeing 737 cargueros, 40 centros operativos, 415 oficinas y una extensa red de concesionarios.

Además, entrega a 200 países en los cinco continentes y ofrece un innovador menú de servicios de importación y exportación a Estados Unidos[16].Cuenta con un equipo de 3,500 personas que utiliza la más avanzada tecnología de comunicación e información con aplicaciones únicas en esta industria a nivel nacional como el rastreo en línea a través de su página.

Dado que estos servicios son muy importantes para los usuarios de Estafeta, es importante que su portal se mantenga en óptimas condiciones de disponibilidad y tiempo total de respuesta, así como una buena tasa de transferencia de datos.

Es por todo esto que el sitio se monitoreo en este trabajo de investigación, arrojando buenos resultados en tiempo de respuesta, aunque esta página presenta una particularidad, en general sus tiempos de respuesta no rebasan el límite permitido de los 10seg., pero cuando llegan a rebasarlo, sus picos de tiempo son altos. Fig. 5.23.

[16] www.estafeta.com

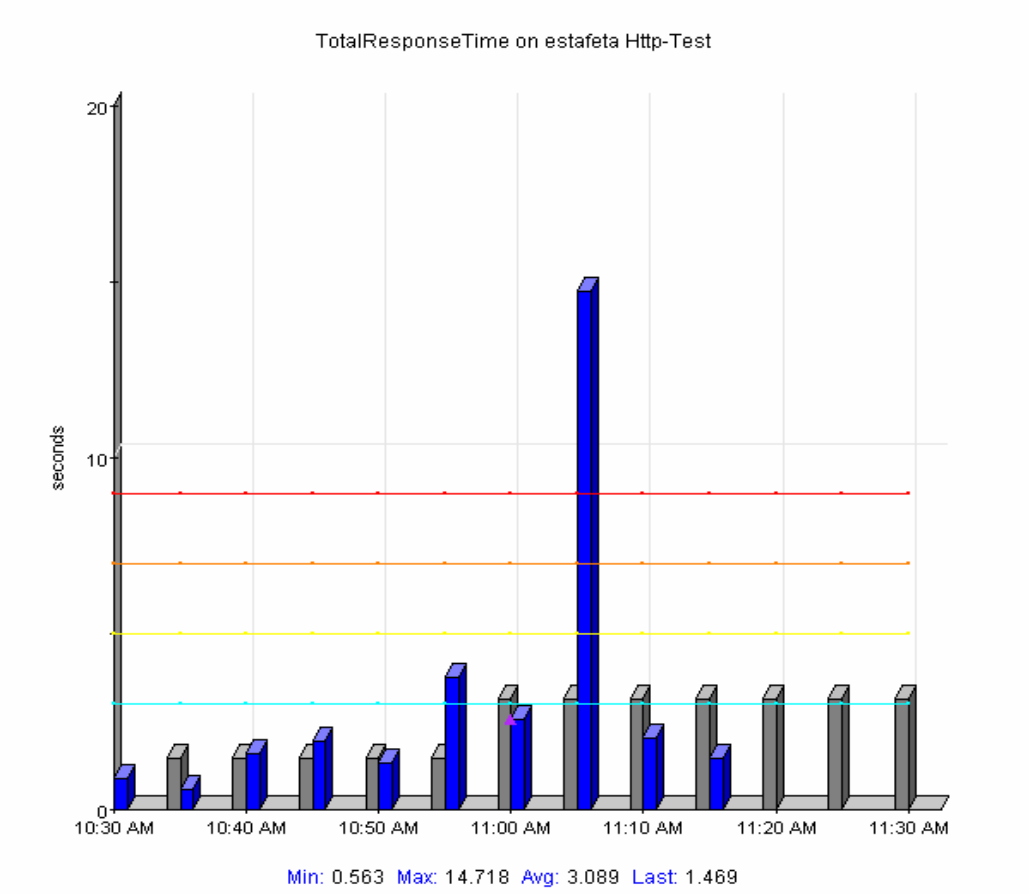


**Fig. 5.23** Gráfica Tiempo Total de Respuesta Estafeta.

Aunque estos picos son esporádicos, debido a que no llegan a afectar el promedio de tiempo de respuesta, que es de 3.08 seg.
La página tiene una alta tasa de transferencia de datos que oscila entre 182 KiloBytes/seg. en promedio, que es una tasa alta comparada con las páginas hasta ahora monitoreadas, la más cercana a esta tasa es la página de la Universidad Nacional Autónoma de México.

En general, la página no presenta problemas graves que pudieran causar un error o que el usuario se desespere y termine por cerrar la página.

La segunda página a monitorear, es la de la compañía Symantec. Symantec fue fundado en 1982. Es el líder global en la seguridad de la información, proporciona una amplia gama de software para aplicaciones y servicios diseñados para ayudar a individuos, negocios

pequeños, mediados, y a las empresas grandes. La marca Norton de Symantec, es líder mundial en soluciones de seguridad, Symantec tiene operaciones en más de 35 países con más de 5.000 empleados[17]. Es por ello, que es uno de los sitios más solicitados por los cibernautas mexicanos. De ahí la importancia que se mantenga en las mejores condiciones y trabajando adecuadamente.

Al monitorear la página arrojo datos importantes en cuanto a tiempo de respuesta Fig.5.24, debido a que presenta resultados muy similares al de la página de Estafeta.

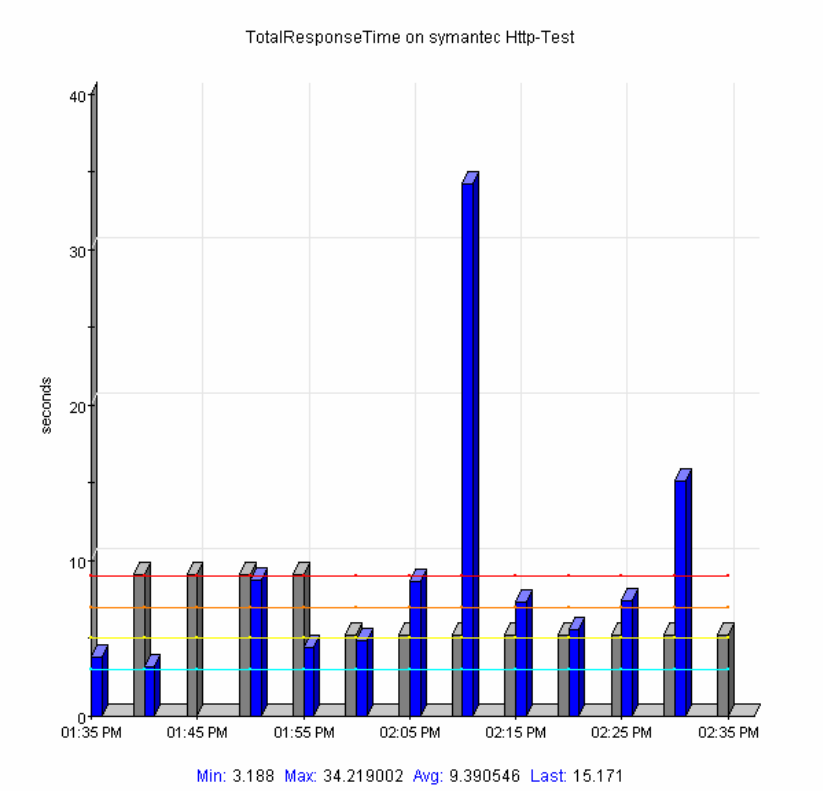


**Fig. 5.24** Gráfica Tiempo Total de Respuesta Symantec.

Su tiempo promedio de respuesta es inferior al límite permitido, pero cuando llega a rebasar este límite, alcanza tiempos de respuesta de hasta 34 seg. Su tasa de Transferencia de Datos, no es tan alta como la de estafeta, pues su rango de transferencia esta entre los 3 – 43 KiloBytes/seg. Fig. 5.25.

[17] www.symantec.com

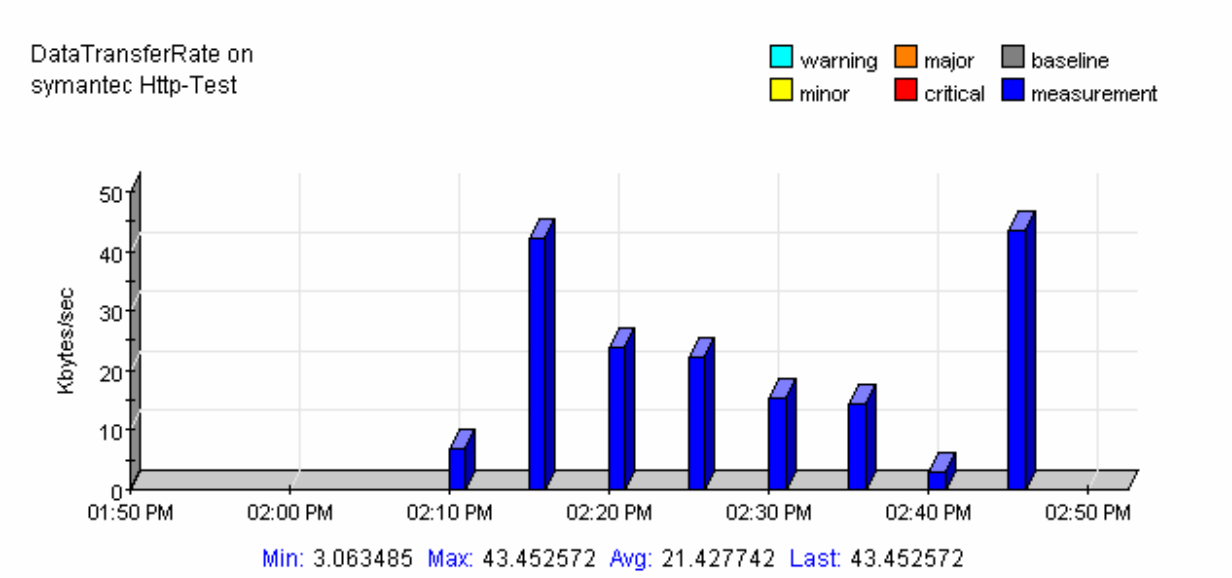


**Fig. 5.25** Gráfica Tasa de Transferencia de Datos Symantec.

En cuanto a la disponibilidad, este portal no presentó ninguna irregularidad, siempre estuvo activo. Con respecto a las otras lecturas tomadas, como lo son el tiempo de DNS o el Tiempo de Transferencia de Datos, no hubo ningún problema, debido a que siempre se mantuvieron dentro de los límites permitidos.

El tercer sitio candidato a monitorearse, es el de t1msn, muy solicitado en México por lo servicios que presta a los usuarios. T1msn es el resultado de la alianza de Microsoft y Telmex lideres en tecnología y comunicaciones.

Actualmente T1mns se encuentra dentro de los portales líderes en México con 7.5 millones de usuarios únicos y más de 651 millones de páginas visitadas en un mes. Datos a Enero 2002[18].

T1msn proporciona la relación más próxima y personal en Internet para consumidores y marcas al ofrecer la más extensa serie de servicios integrados.

Los resultados obtenidos al monitorear, no son tan favorables, debido a que sus tiempos de respuesta son exageradamente excesivos. Fig. 5.26.

[18] www.t1msn.com.mx

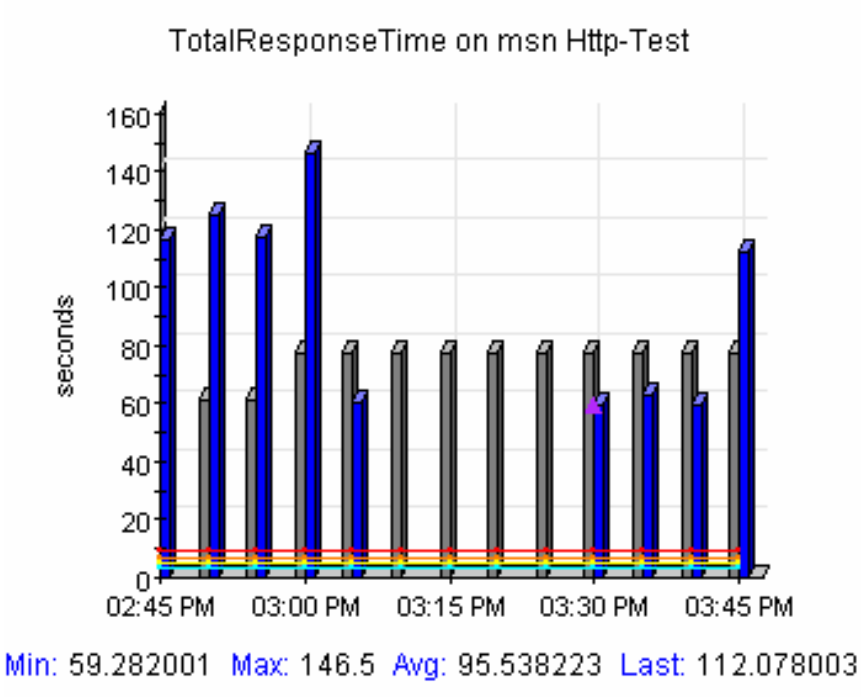


**Fig. 5.26** Gráfica Tiempo Total de Respuesta T1msn.

Su promedio de respuesta es de 95.5seg. esto significa que rebasa por mucho el límite permitido de 10seg. y aunque es una de los sitios más visitados en México, los usuarios deben de esperar por mucho tiempo para que la página cargue en su totalidad. Aparte de presentar dificultades en tiempos de respuesta, T1msn, tiene una tasa de transferencia de datos muy baja. Fig. 5.27.

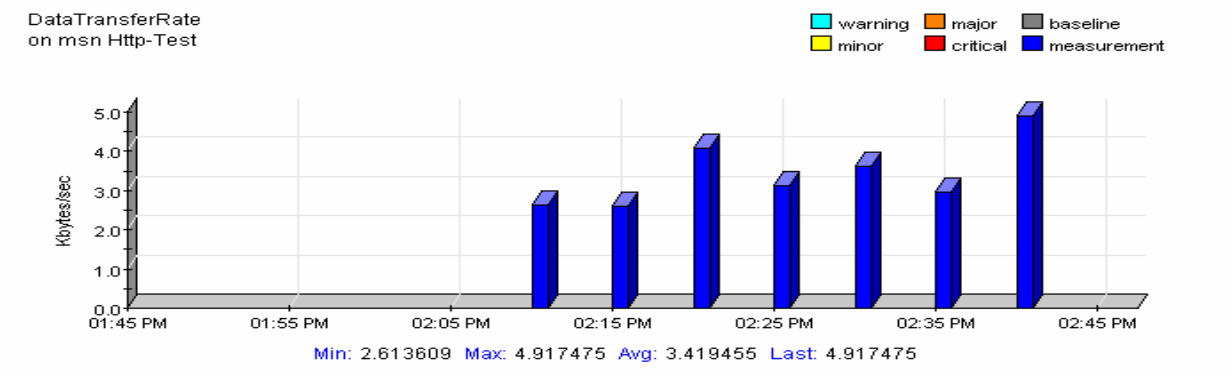


**Fig. 5.27** Gráfica Tasa de Transferencia de Datos T1msn.

Tiene un promedio de transferencia de datos de 3.4 KiloBytes/seg., que para la demanda que tiene esta página en México es muy bajo, razón por la cual tiene problemas en tiempo de respuesta. La última página que fue elegida para ser monitoreada en el presente trabajo, fue la de Windows Update, sitio que pertenece a la compañía Microsoft, y que todos los usuarios de Windows alguna vez hemos utilizado. Microsoft Windows Update es un sitio Web interactivo que ofrece una forma consistente de mantenerse al día con las últimas mejoras de seguridad, rendimiento y funciones adecuadas para su equipo Windows. Windows Update funciona con Windows NT® 4.0, Windows 98, Windows Me, Windows 2000, Windows XP y Windows Server™ 2003.

Windows Update permite revisar, seleccionar e instalar todas las últimas ampliaciones, mejoras, actualizaciones de seguridad y controladores para su equipo, en el momento de su elección. Las actualizaciones automáticas son parte de un servicio proporcionado por Microsoft que entrega automáticamente actualizaciones críticas a su sistema operativo Windows, para solucionar aspectos que pueden hacer vulnerable a su equipo ante ataques de virus o gusanos. La ventaja principal de utilizar Actualizaciones automáticas es que las actualizaciones de seguridad más críticas para su equipo se descargan e instalan automáticamente, a través de una página cuyo tiempo de respuesta Fig. 5.28 es de los mejores de todas las páginas monitoreadas.

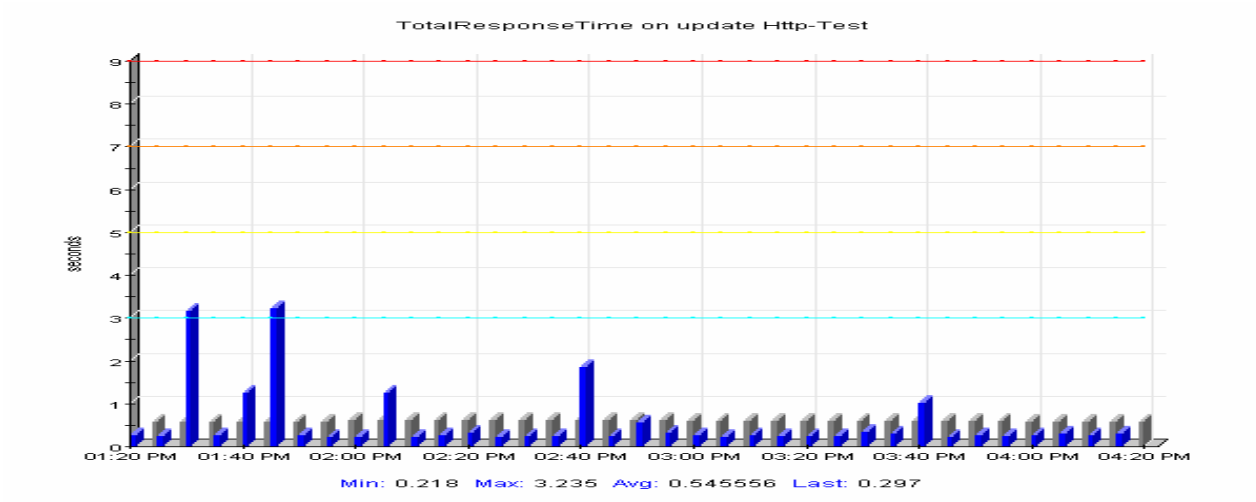


**Fig. 5.28** Gráfica Tiempo Total de Respuesta Windows Update.

Durante todo el periodo de muestreo, la página se mantuvo con excelentes tiempos de respuesta, obteniendo un tiempo promedio de 0.54 seg. considerado de los mejores tiempos de las 16 páginas monitoreadas.

Su tasa de transferencia de datos, no es muy alta Fig. 5.29 pero si constante. De esto nos dimos cuenta porque en un periodo de monitoreo largo de tiempo se mantuvo constante, alrededor de los 20 KiloBytes/seg.

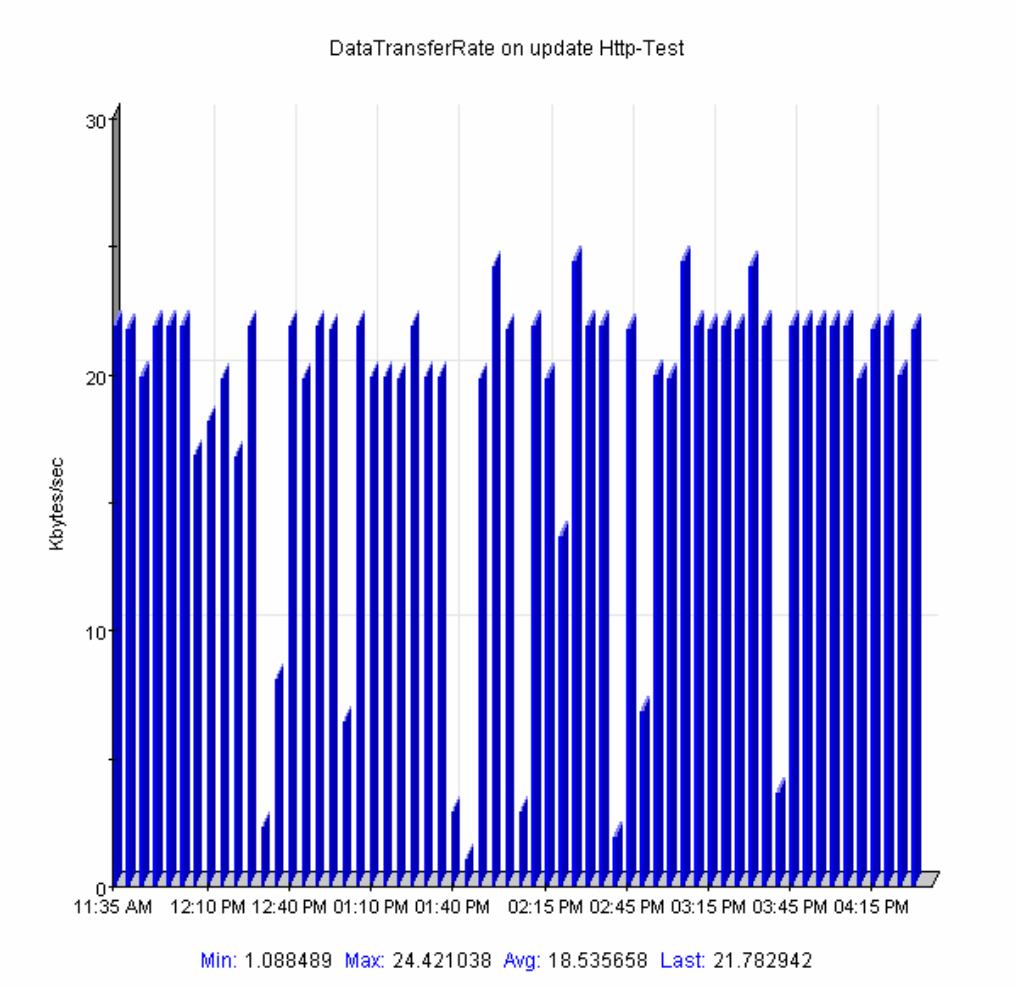


**Fig. 5.29** Gráfica Tasa de Transferencia de Datos Windows Update.

Haciendo una balance general de los resultados obtenidos al monitorear las 16 páginas de las cuatro categorías, nos damos cuenta que los servicios de Internet tienen grandes contrastes, debido a que hay páginas que presentan buenos tiempos de respuesta y una disponibilidad del 100% como el portal de Microsoft o el sitio de la SEP, mientras que existen otros sitio que tienen grandes carencias en cuanto al tiempo de respuesta y pequeñas caídas en cuanto a la disponibilidad como la página de la Secretaria de Relaciones Exteriores. Dichos contrastes se deben a varios factores como lo son: el tráfico en la red, la distancia entre el servidor, entre otros.

En el siguiente capítulo se abordaran las conclusiones a las que se han llegado basándonos en los resultados obtenidos al monitorear las páginas seleccionadas. Dichas conclusiones nos ayudaran a tener un panorama general de la calidad de los servicios de Internet que están recibiendo los usuarios finales y poder así diferenciar entre cual es la calidad que percibe el usuario y cual es realmente la calidad que recibe.

# CAPÍTULO VI
# Conclusiones

## Conclusiones

El trabajo de Tesis muestra los resultados obtenidos al monitorear dieciséis páginas de Internet, clasificadas en cuatro categorías: Gobierno, Comerciales, Universidades y Buscadores.

Se escogieron estas páginas, en base al número de usuarios que tuvieron durante el mes de Abril del presente año. Estos datos se obtuvieron de los servidores de DNS de uno de los principales proveedores de Internet en México.

Todas las páginas se sometieron al mismo número de pruebas, dentro de las que se encontraban:

- Disponibilidad
- Tiempo de Respuesta
- Prueba Completa
- Tiempo DNS
- Tiempo de Conexión TCP
- Tiempo de Redireccionamiento
- Tiempo de Respuesta del Servidor
- Tiempo de Transferencia de Datos
- Tasa de Transferencia de Datos

De todas estas pruebas a las que se sometieron todas las páginas, solo se presentaron problemas en tres de ellas que fueron: la disponibilidad, el tiempo de respuesta y la tasa de transferencia de datos. En todas las demás no se presentó ningún problema, ya que todas se mantuvieron dentro de los límites acordados (ver Apéndice A).

Durante el desarrollo de la Tesis se ideo una metodología adecuada, para lograr estimar la Calidad de Servicio (QoS) de los Servicios de Internet, para que los ISP tengan un panorama más amplio de cuales son sus carencias y poder así corregirlas, para entregar un servicio de calidad al usuario final.

Se logró estimar la Calidad de Servicio de los Servicios de Internet, haciendo un monitoreo en tiempo real para cada una de las páginas de las cuatro categorías: Gobierno, Buscadores, Comerciales y Universidades. Se obtuvieron resultados muy importantes, estos resultados se presentaron de forma gráfica debido a que es la forma más fácil de interpretarlos. Por ejemplo, podemos entregar reportes en forma gráfica, donde en una sola gráfica se muestre el comparativo de todas las páginas comerciales en cuanto a tiempo de respuesta y disponibilidad.

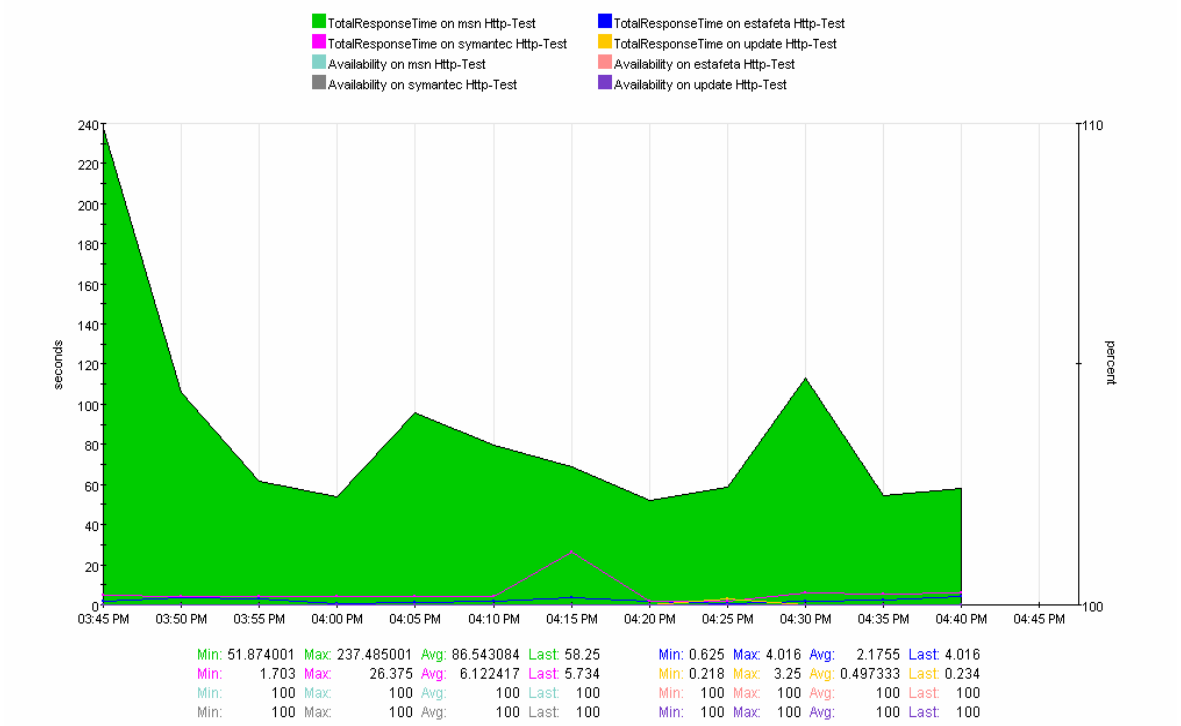


**Fig. 6.1** Gráfica Comparativa Tiempo de Respuesta vs Disponibilidad páginas comerciales.

Este tipo de gráficas facilita la comprensión y comparación de los resultados obtenidos al monitorear las páginas.

El tiempo total de respuesta es uno de los puntos que la mayoría de las páginas pone especial atención, debido a que cada vez que se abre una página Web, solo se dispone de segundos para llenar la pantalla de contenido atractivo al usuario. Si no se consigue, se traduce en pérdida de usuarios. De ahí la importancia de este trabajo, ya que brinda la oportunidad tanto a los ISP como a los usuarios de saber, cómo realmente están llegando los servicios de Internet al usuario final.

Otro punto que observamos al monitorear es variabilidad de la tasa de transferencia. Este parámetro corresponde a la velocidad media con que los datos son transferidos desde la red del ISP al usuario conectado a éste, durante periodos de tiempo determinados. En la tasa de transferencia intervienen muchas variables, es así como un sitio Web hospedado en un servidor de gran capacidad podrá ser accesado sin dificultad por usuarios de distintos lugares del mundo. Por el contrario, si se accede a un sitio Web hospedado en un servidor de bajo desempeño (o en un servidor "lejano"), la velocidad del acceso a los datos se verá decrementada notoriamente.

En otras palabras, la responsabilidad del ISP es proveer acceso a Internet, una vez allí, el usuario deberá competir con los demás navegantes por el recurso al que esta accesando. Esto significa que una buena y objetiva medición de calidad de la transferencia de datos debe considerar la tabulación de sitios Web "cercanos", por ejemplo sitios nacionales de reconocida disponibilidad.

La disponibilidad, es una de las lecturas que presentó pequeñas deficiencias en páginas como la del Instituto Tecnológico de Estudios Superiores, aunque los periodos de tiempo que no estaba disponible eran cortos, el error es muy notorio. Por lo que debe de existir especial cuidado y mantener las páginas disponibles al 100%.

El trabajo realizado ofrece la opción de entregar reportes semanales de las lecturas tomadas, como el que se muestra en la figura 6.2 que representa la disponibilidad de las universidades a lo largo de una semana.

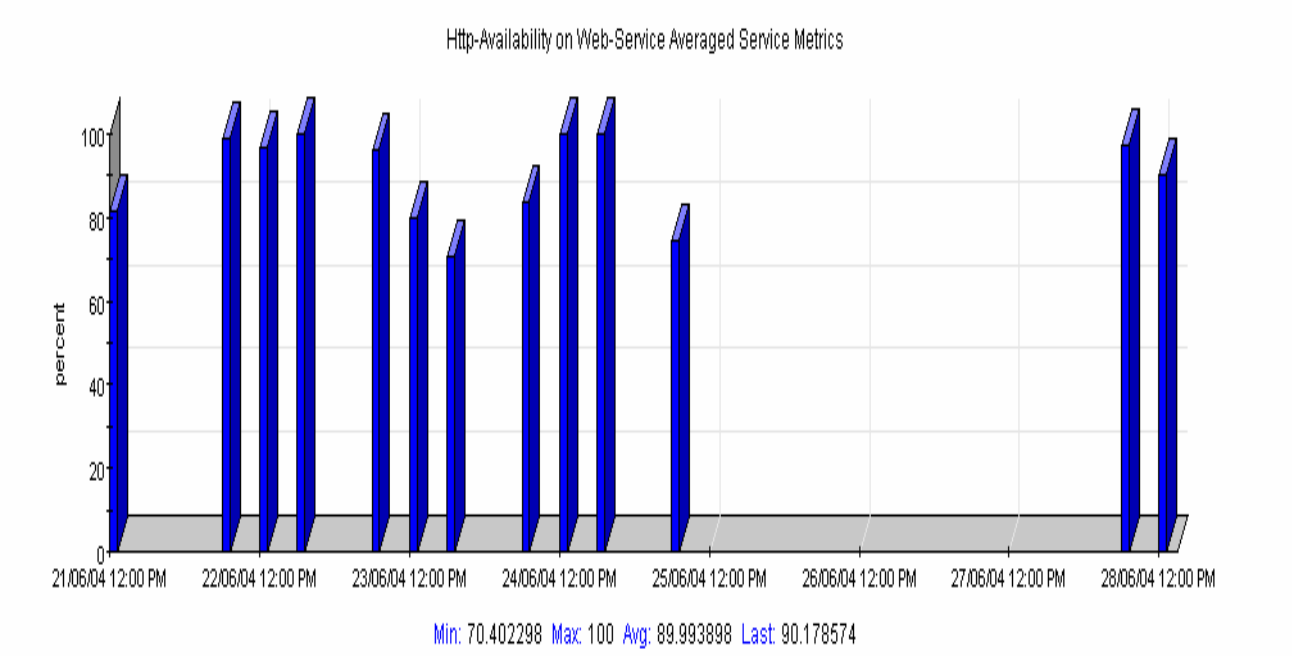


**Fig. 6.2** Gráfica Informe semanal de Disponibilidad Universidades.

En la actualidad el uso masivo de Internet dejó de ser una promesa, nos enfrentamos a una gran demanda de esta tecnología de información en todos los rubros de la actividad humana. Sin embargo, ésta tecnología no se encuentra exenta de problemas. La congestión y la nula diferenciación entre los servicios generan decepción entre los usuarios.

Los usuarios de Internet deben reducir sus altas expectativas de eficiencia, por la falta de infraestructura adecuada para concretarla, o bien, por desconocer las verdaderas capacidades del servicio. Esto se debe a que actualmente, la infraestructura que se esta utilizando para transportar datos, fue diseñada para voz. Aunque en la actualidad, se están

intercambiando los papeles, con la utilización de tecnologías como Voz sobre IP (VoIP), que es exactamente lo contrario, es utilizar una red de datos para transportar voz.

Algunas recomendaciones para hacer los servicios de Internet más eficientes pueden ser: El hacer un diseño adecuado de la página Web, debido a que gran número de los sitios en Internet se centran en hacer un sitio atractivo a la vista y descuidan los tiempos de respuesta. Otra alternativa es utilizar plataformas que permitan monitorear el desempeño real de los servicios de Internet como la empleada en este trabajo.

En cuanto a la metodología, algunas modificaciones que podríamos hacer sería: Una selección más amplia de las páginas monitoreadas, esto es, no solo considerar las páginas de un mes, ya que podrían arrojar resultados erróneos, debido a que en ese mes pudo haber existido alguna promoción, concurso u oferta que haga más atractivo visitar la página durante dicho mes.

Otro cambio en la metodología sería el extender el periodo de monitoreo, ya que esto nos arrojaría datosmás cercanos a la realidad. Además de dar una visión más amplia del estado actual de los servicios de Internet, y tener argumentos para formar criterios acerca de la calidad de dichos servicios.

En el ambiente de empresas proveedoras de servicio de Internet (ISP), la calidad constituye un mecanismo de competitividad que puede hacer la diferencia entre diversos ISPs.

Aunque el monitoreo de las páginas se hizo mediante una red cableada las nuevas tecnologías tienden a las redes inalámbricas por sus grandes beneficios como movilidad, simplicidad de diseño, entre otros, no obstante estas redes ofrecen menor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps, frente a los 100 Mbps que puede alcanzar una red cableada. Por otra parte hay que tener en cuenta la tasa de error debida a las interferencias, que puede alcanzar hasta 6 órdenes de magnitud de diferencia[1]. Estamos hablando de un bit erróneo por cada 10,000 bits, o lo que es lo mismo, de cada Megabit transmitido, 1Kbit será erróneo.

[1] http://www.80211-planet.com/

Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.

Como trabajo futuro se espera explotar aun más la plataforma utilizada en el presente trabajo de investigación y no solo centrarse a servidores de HTTP, sino ampliarlos a servidores de FTP, servidores de mail, Telnet, entre otros, debido a que esta plataforma tiene la capacidad de soportar dichos servicios.

# Gráficos Páginas de buscadores

## Altavista

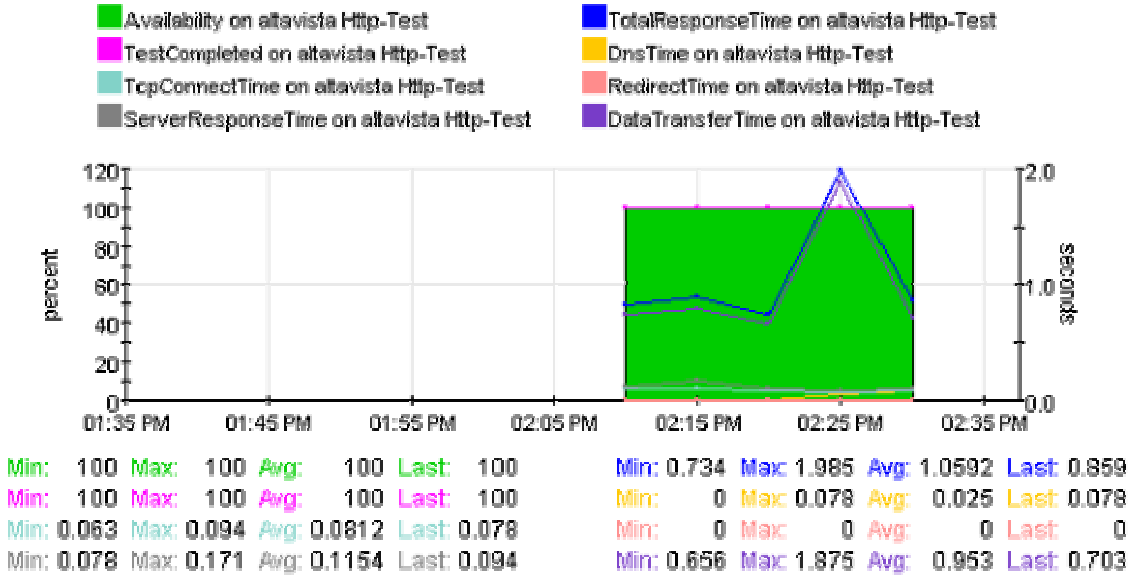


**Fig. A.1** Gráfica Comparativa Altavista.

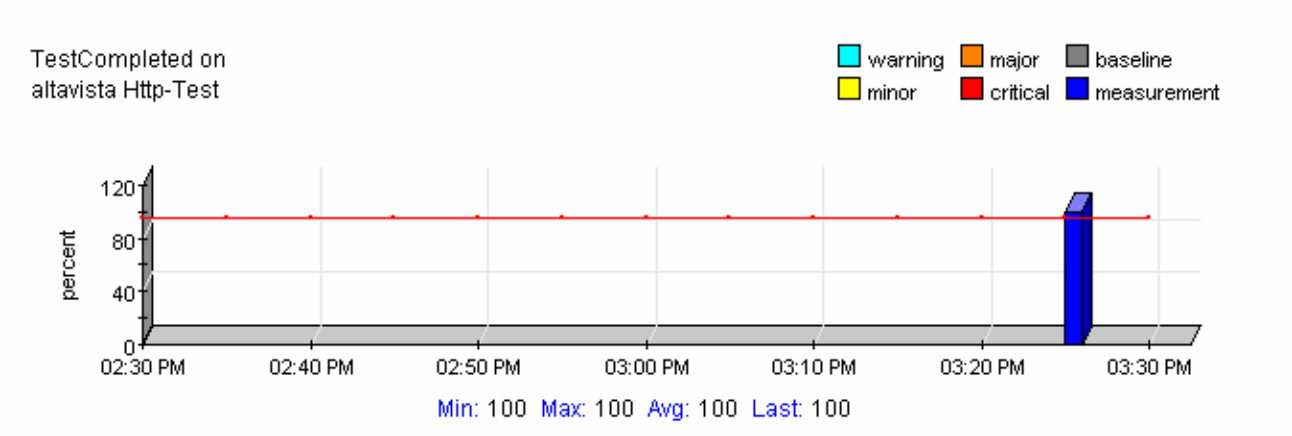


**Fig. A.2** Gráfica Prueba Completada Altavista.

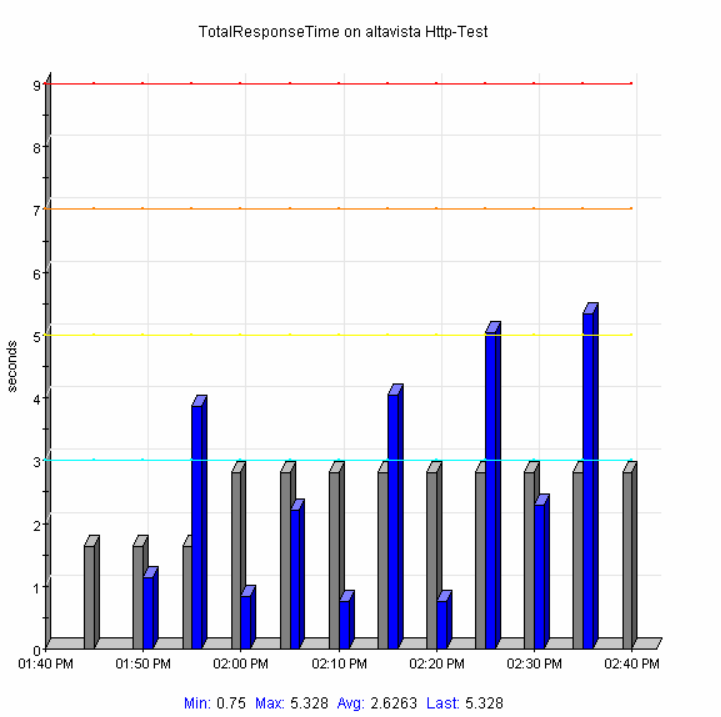


**Fig. A.3** Gráfica Tiempo Total de Respuesta de Altavista.

## elSitio.

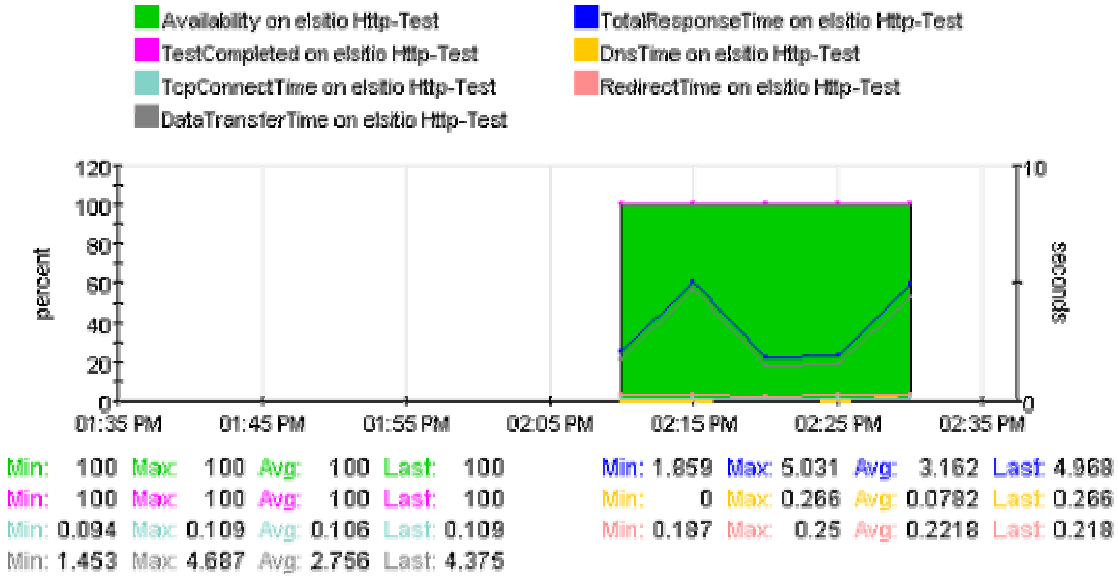


**Fig. A.4** Gráfica Comparativa elSitio.

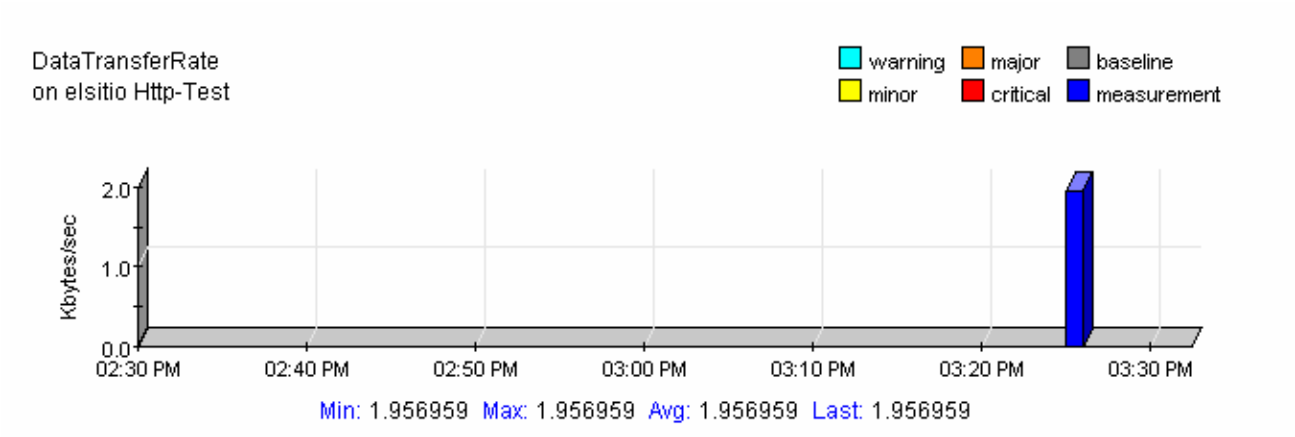


**Fig. A.5** Gráfica Tasa de transferencia de datos elSitio.

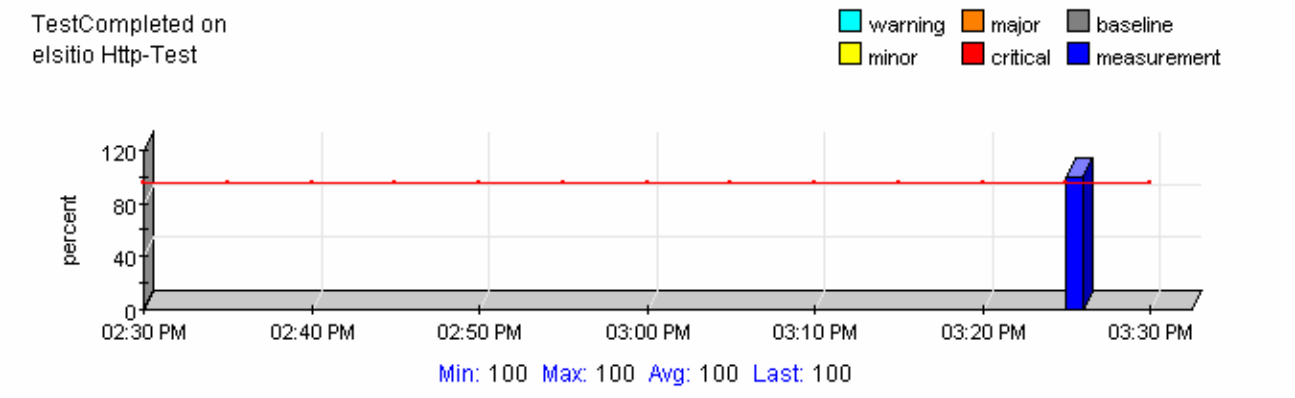


**Fig. A.6** Gráfica Prueba completada elSitio.

## Google.

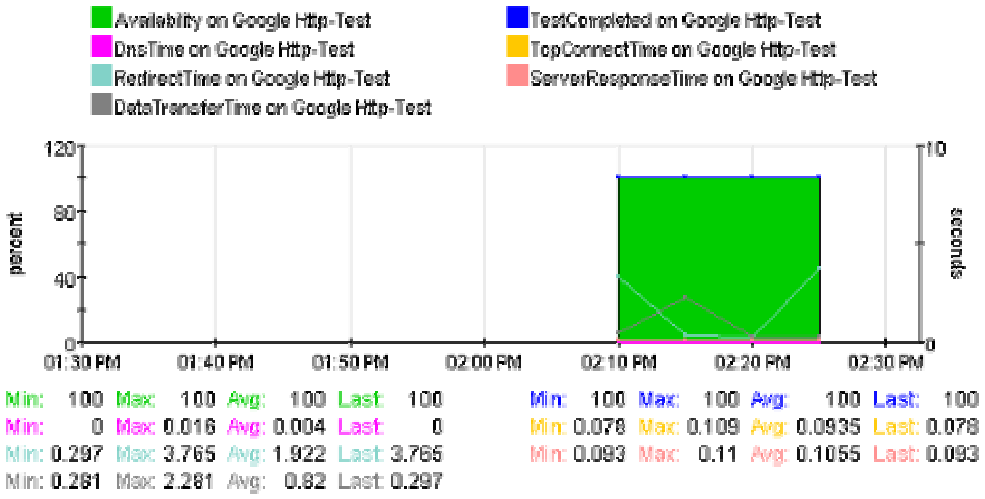


**Fig. A.7** Gráfica Comparativa Google.

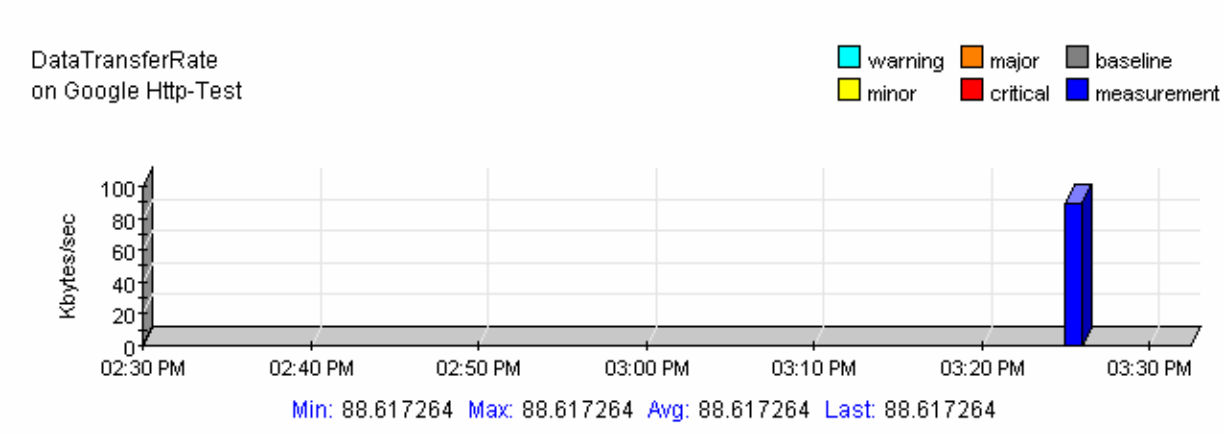


**Fig. A.8** Gráfica Tasa de Transferencia de datos Google.

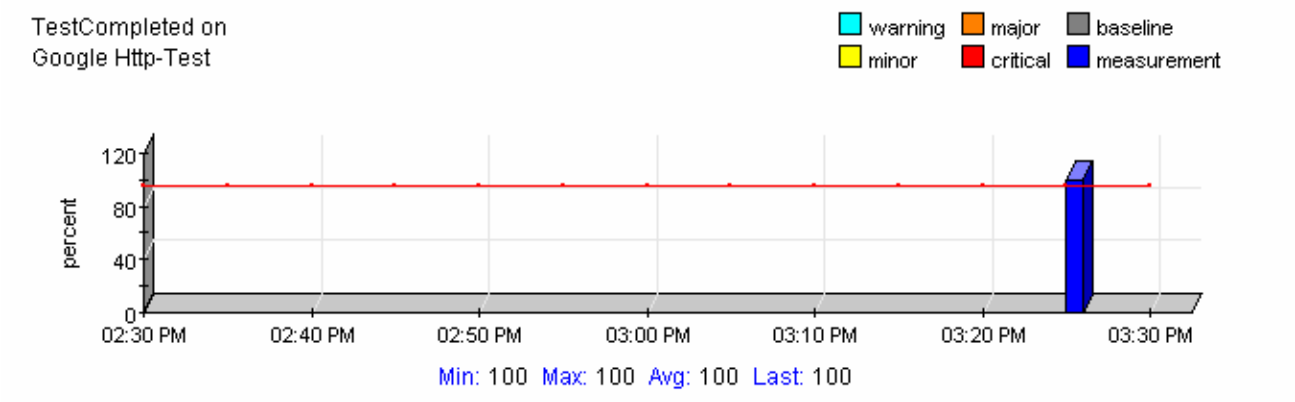


**Fig. A.9** Gráfica Prueba Completada Google.

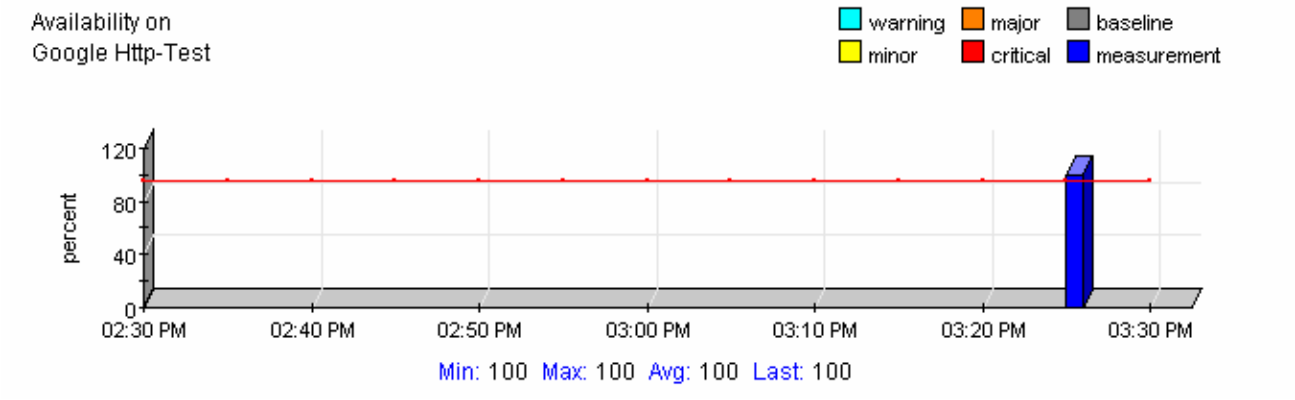


**Fig. A.10** Gráfica Disponibilidad Google.

**Yahoo.**

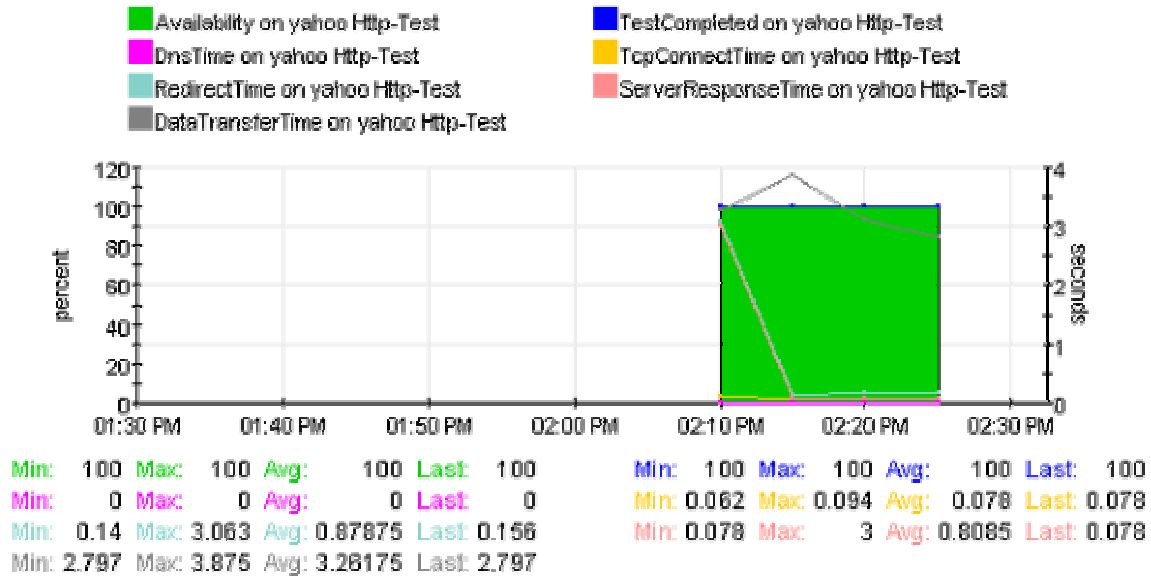


**Fig. A.11** Gráfica Comparativa Yahoo.

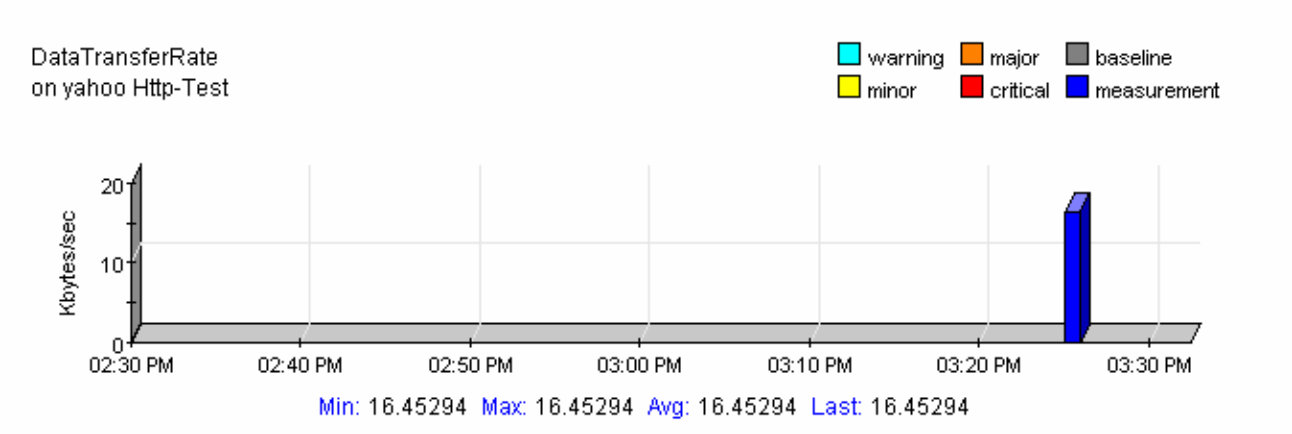


**Fig. A.12** Gráfica Tasa de transferencia de datos Yahoo.

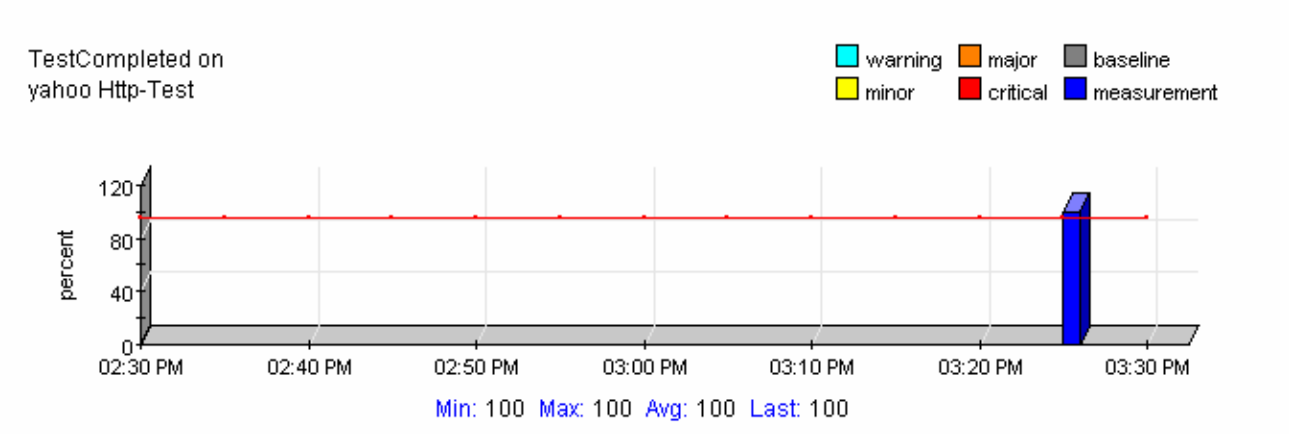


**Fig. A.13** Gráfica Prueba completada Yahoo.

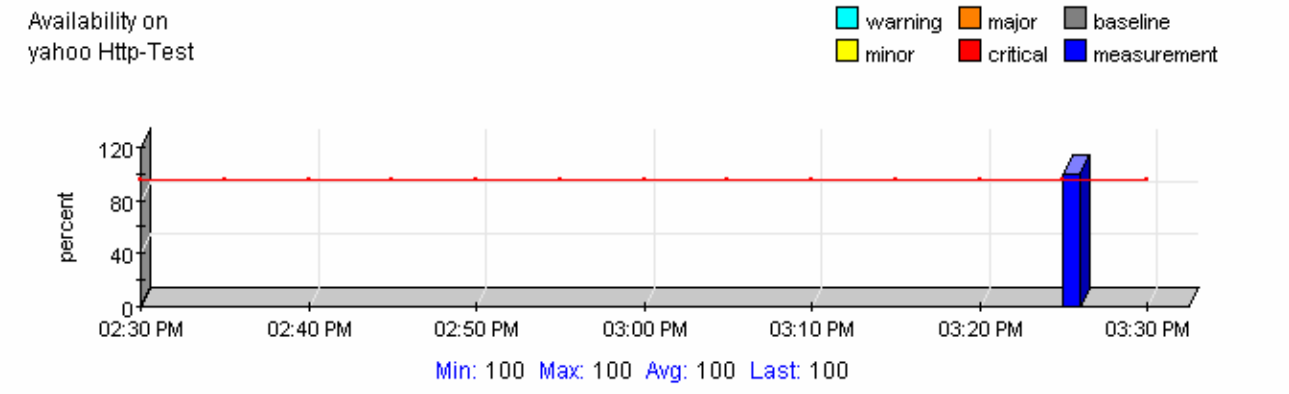


**Fig. A.14** Gráfica Disponibilidad Yahoo.

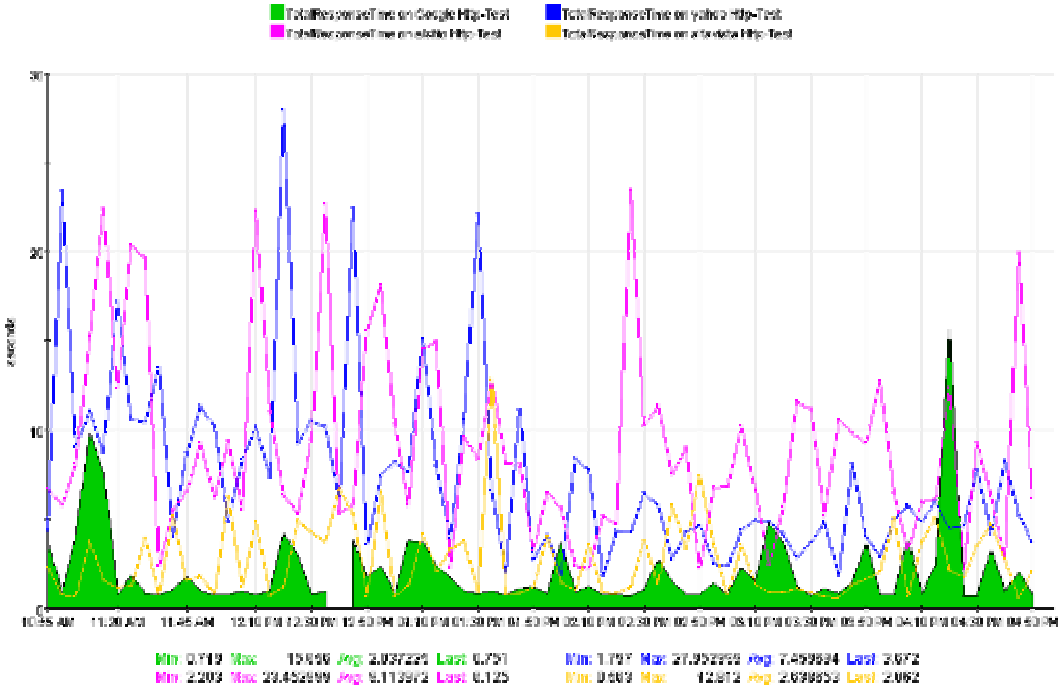

**Fig. A.15** Gráfica Comparativa Tiempos de Respuesta páginas de Buscadores.

## Gráficos Páginas Comerciales

## Estafeta.

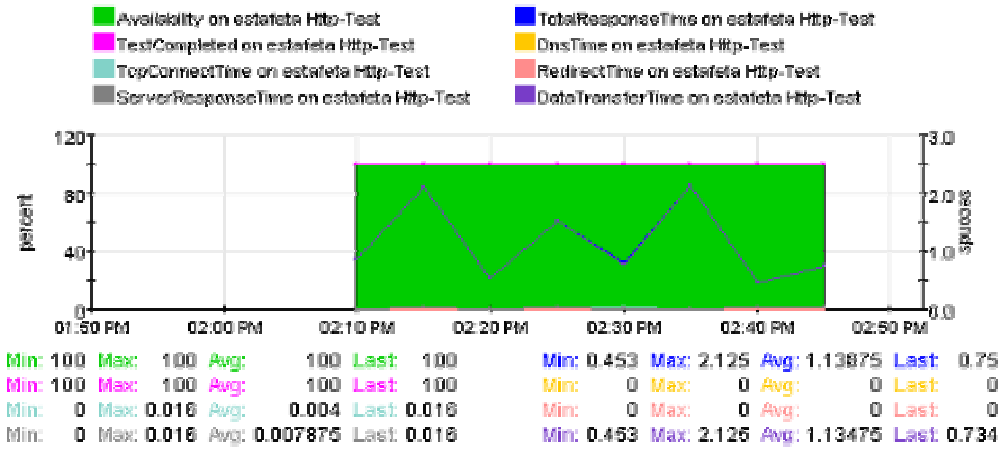


**Fig. A.16** Gráfica Comparativa Estafeta.

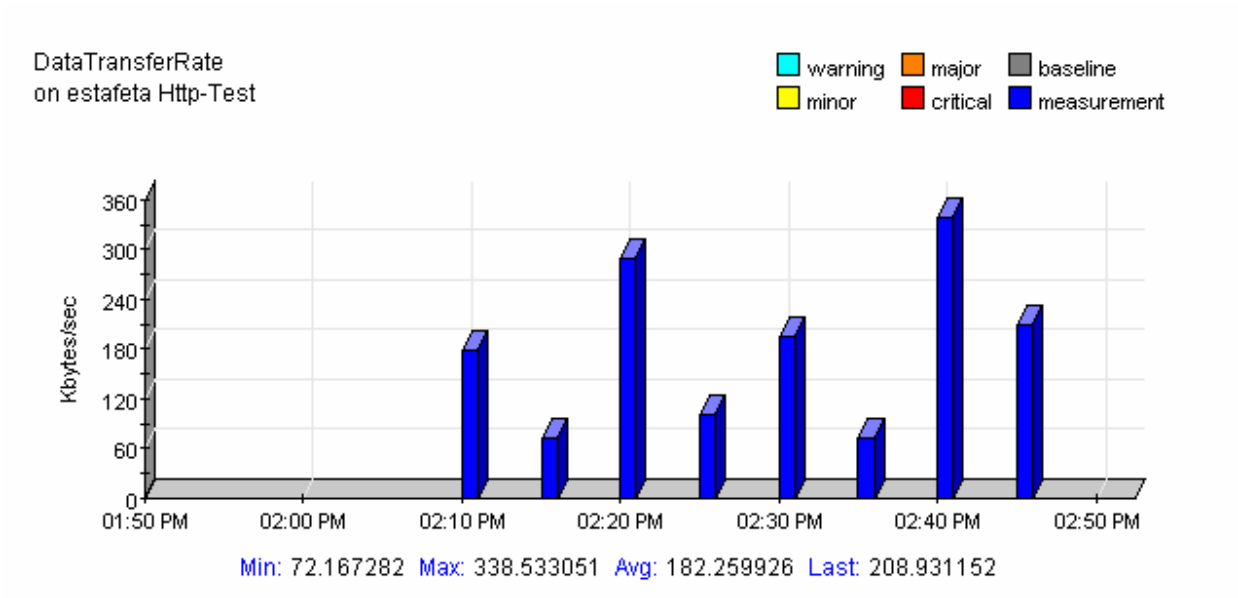


**Fig. A.17** Gráfica Tasa de Transferencia de datos Estafeta.

## T1msn.

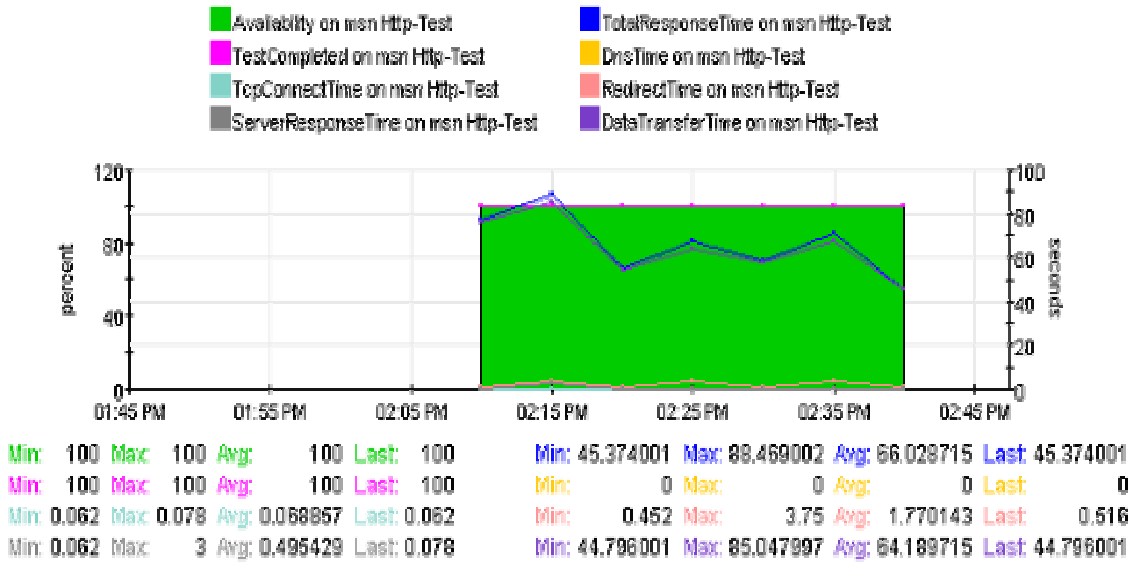


**Fig. A.18** Gráfica Comparativa t1msn.

## Symantec.

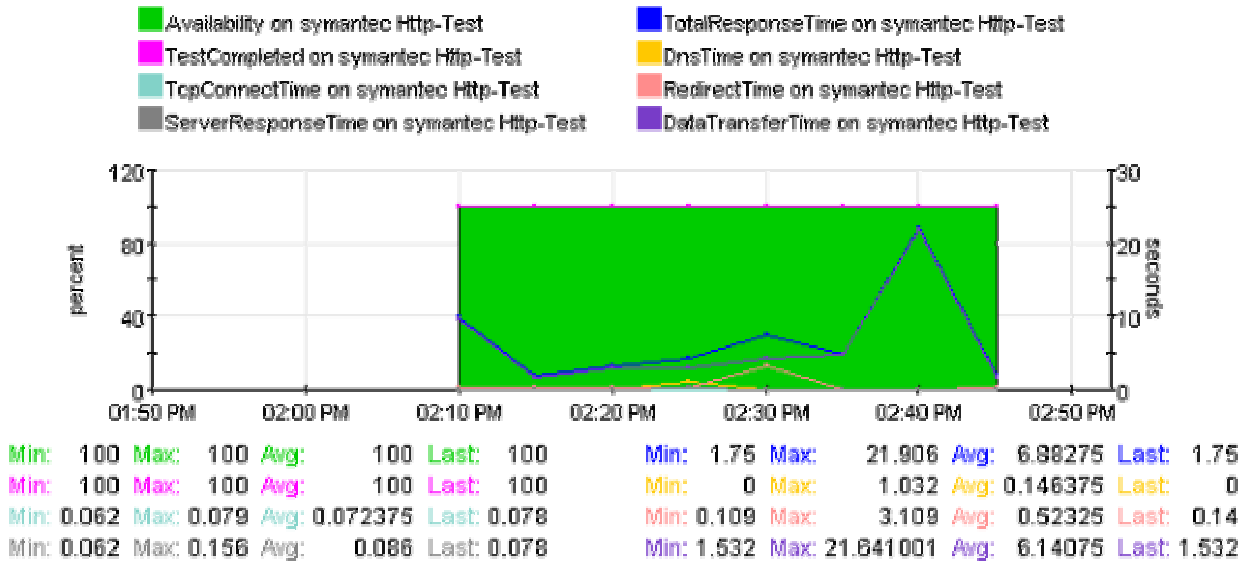


**Fig. A.19** Gráfica Comparativa Symantec.

## WindowsupDate.

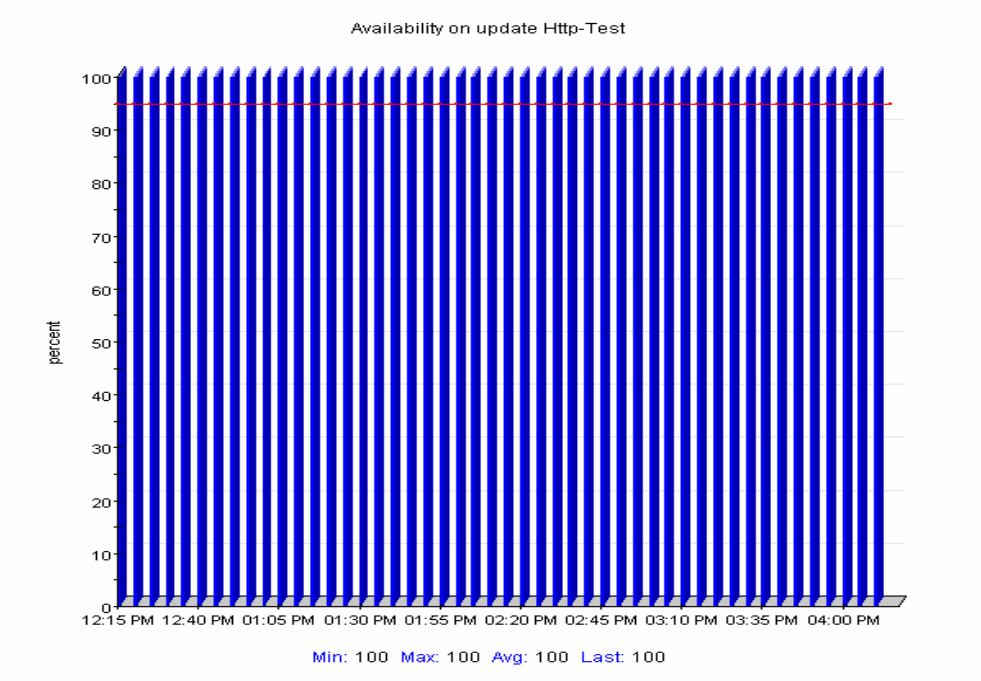


**Fig. A.20** Gráfica Disponibilidad WindowsupDate.

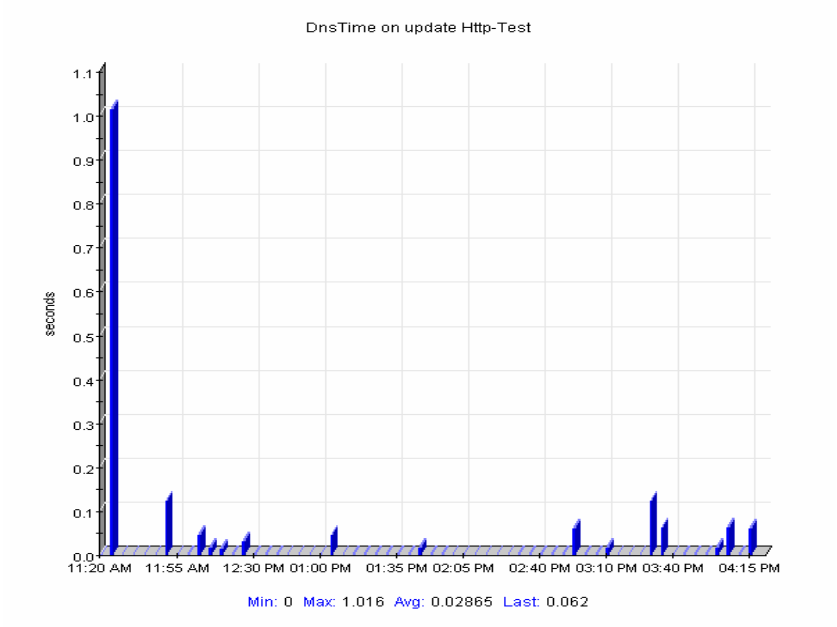


**Fig. A.21** Gráfica Tiempo de DNS WindowsupDate.

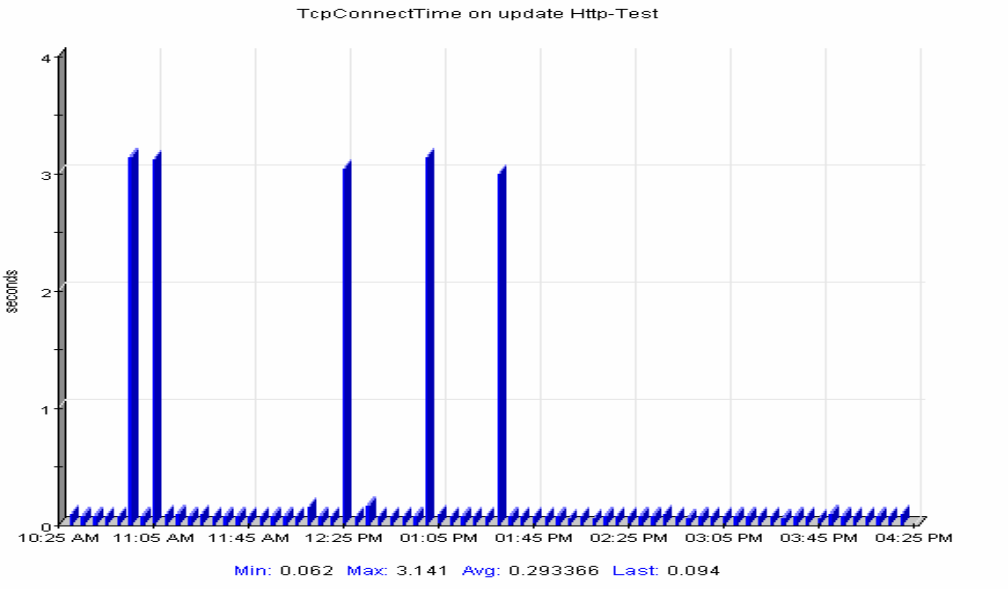


**Fig. A.22** Gráfica Tiempo de conexión TCP WindowsupDate.

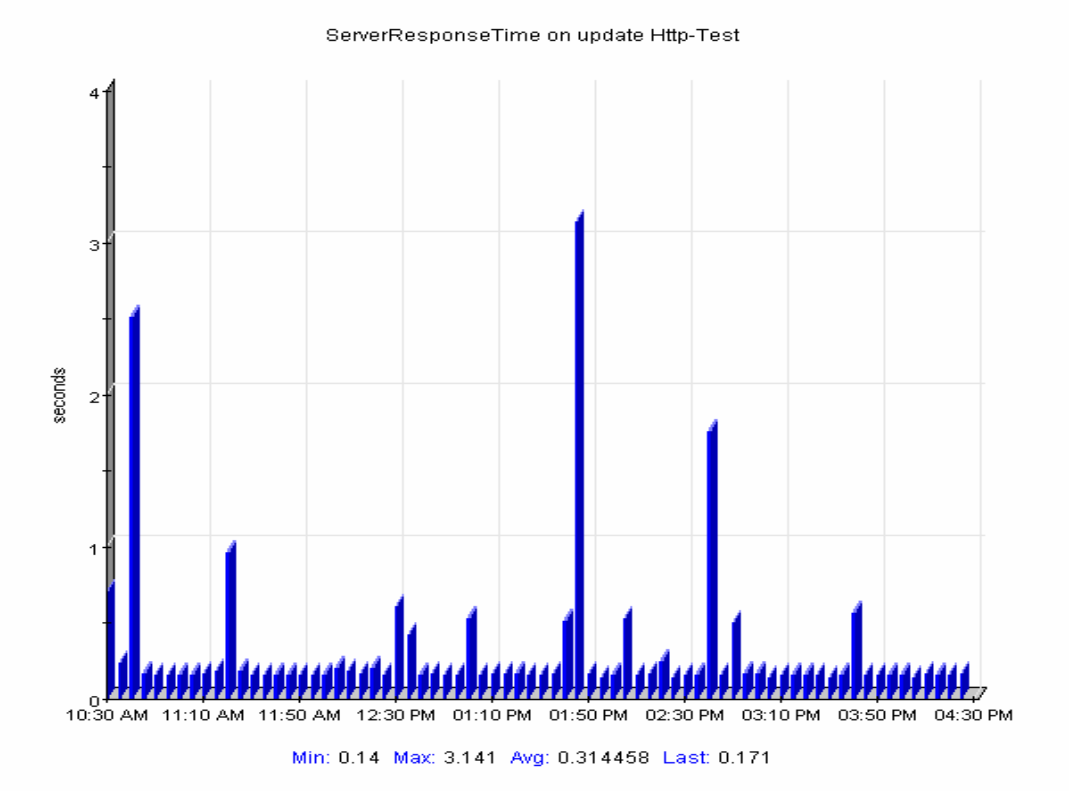


**Fig. A.23** Gráfica Tiempo de respuesta del servidor WindowsupDate.

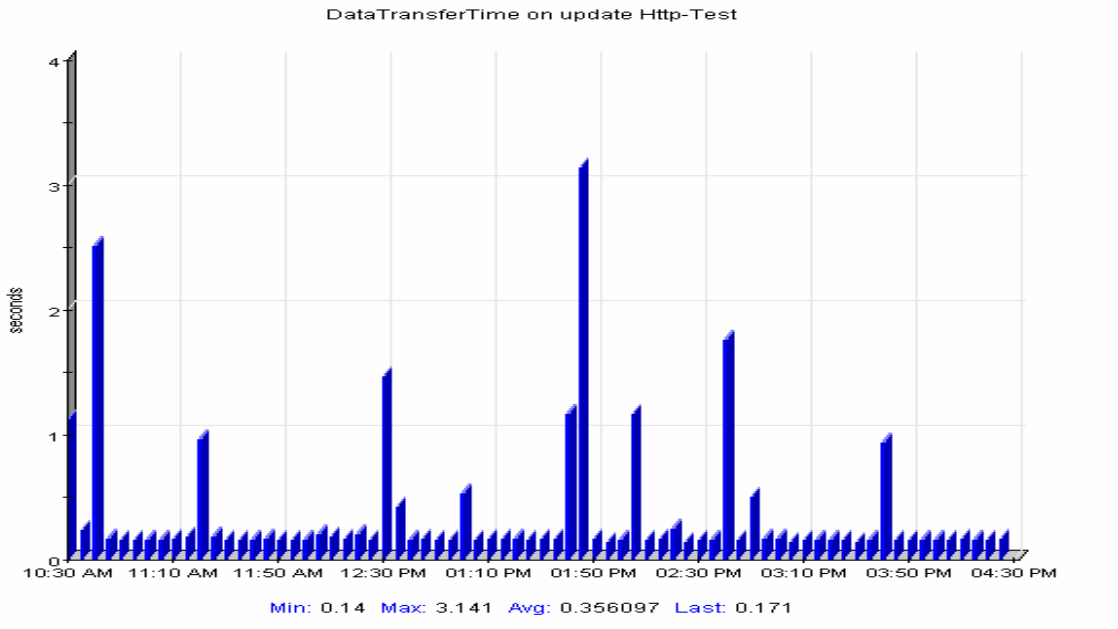


**Fig. A.24** Gráfica Tiempo de transferencia de datos WindowsupDate.

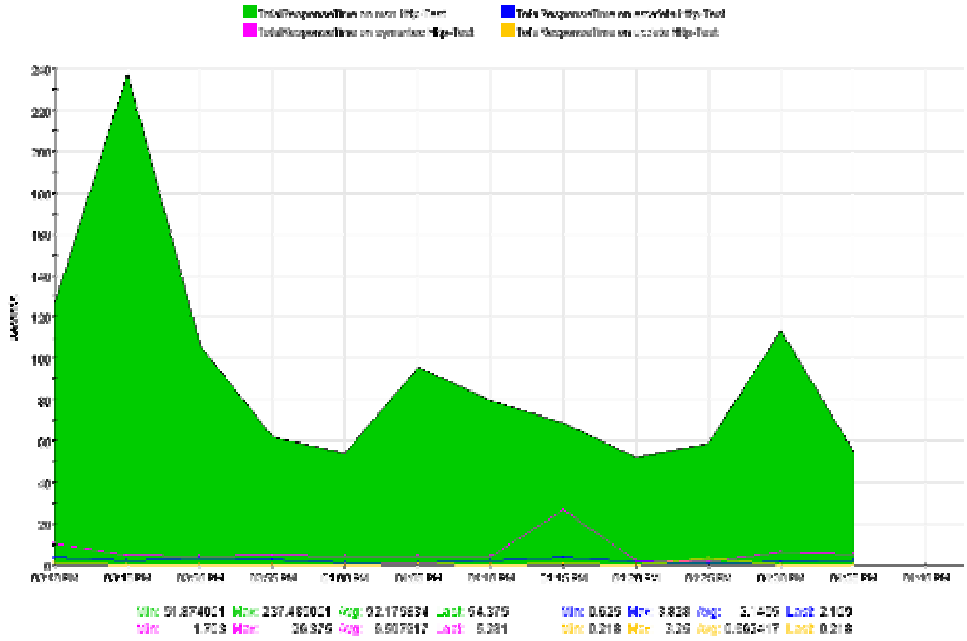

**Fig. A.25** Gráfica Comparativa Tiempos de Respuesta páginas Comerciales.

## Gráficos Páginas de Universidades

### ITESM.

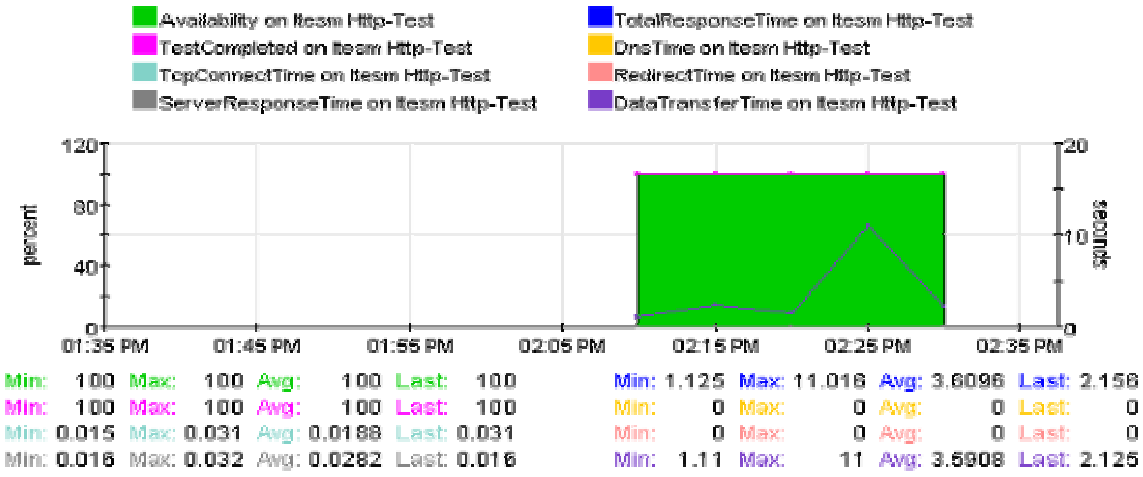


**Fig. A.26** Gráfica Comparativa ITESM.

## UNAM.

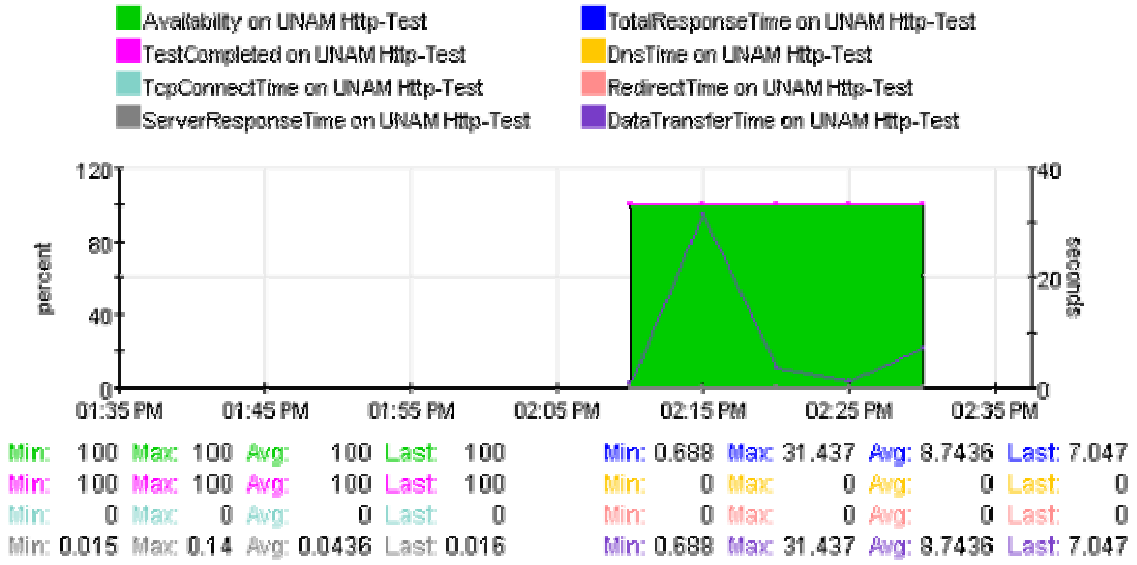


**Fig. A.27** Gráfica Comparativa UNAM.

## UNITEC.

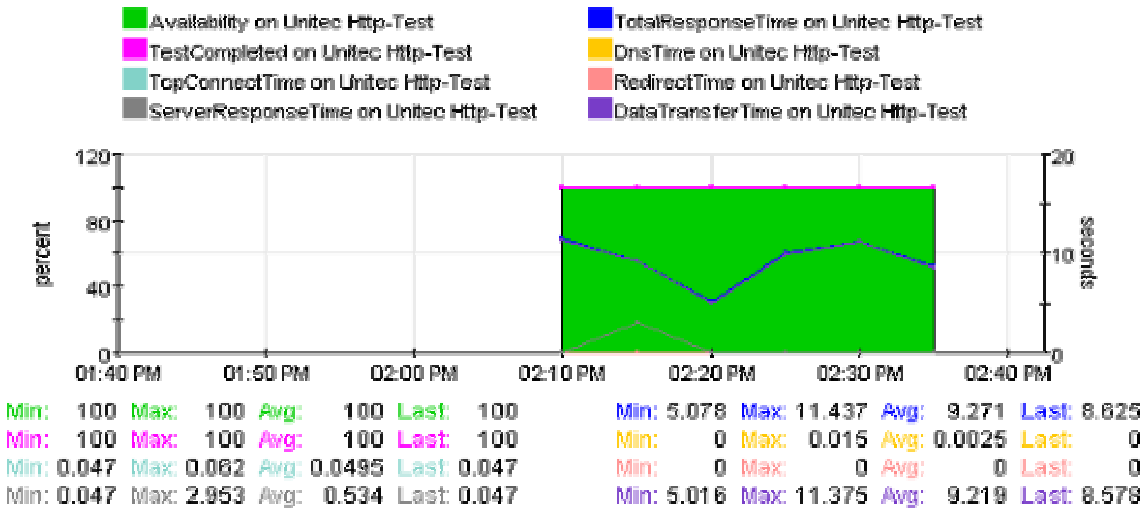


**Fig. A.28** Gráfica Comparativa UNITEC.

**IPN.**

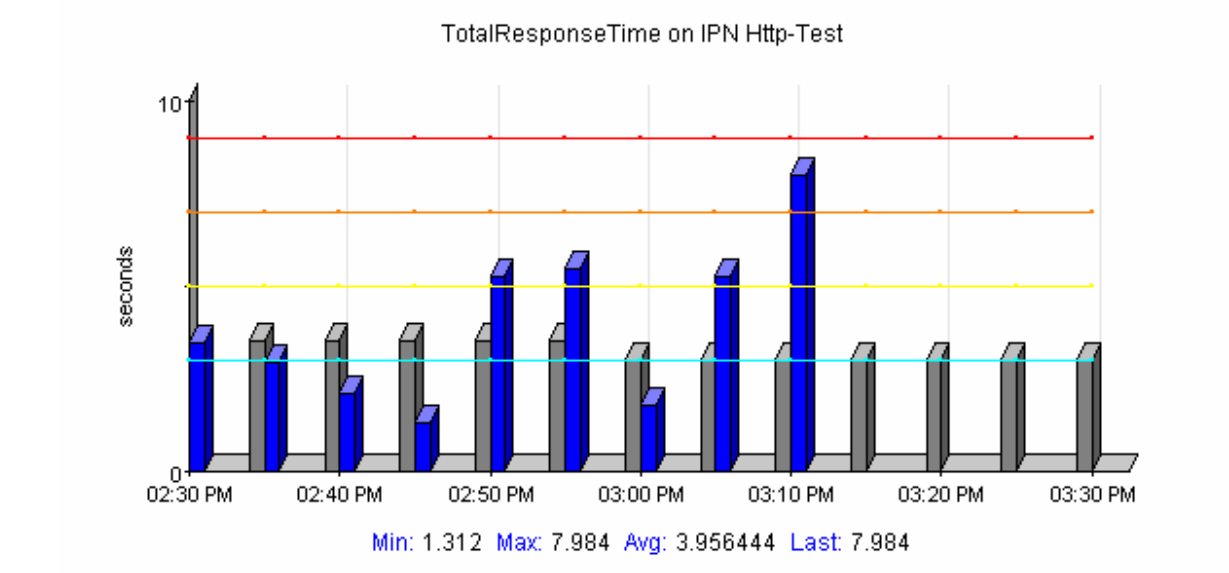


**Fig. A.29** Gráfica Tiempo de respuesta IPN.

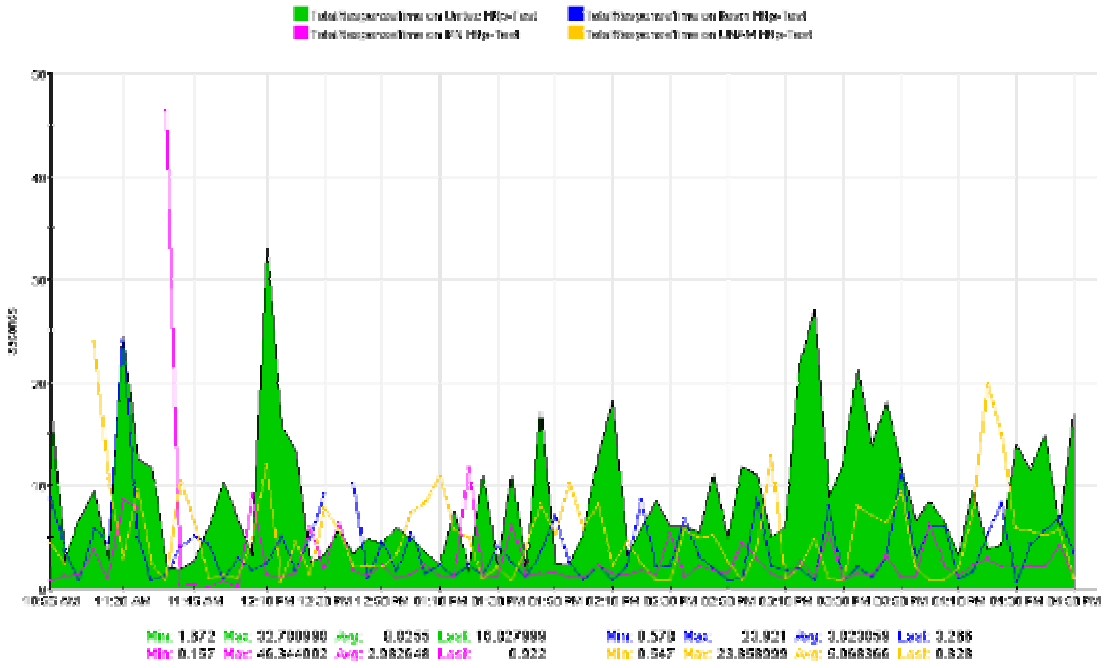

**Fig. A.30** Gráfica Comparativa Tiempos de Respuesta páginas de Universidades.

## Gráficos Páginas de Gobierno.

### SEGOB.

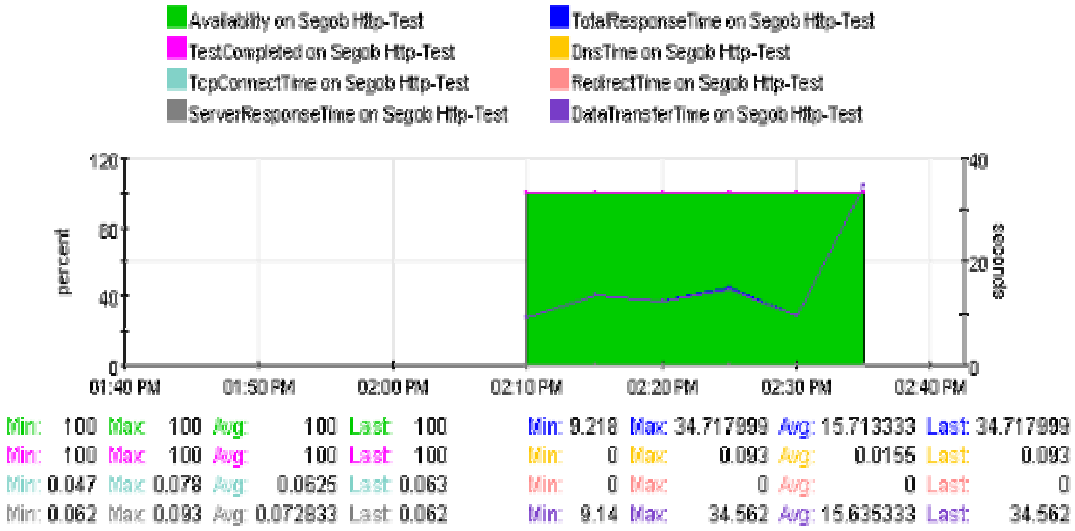


**Fig. A.31** Gráfica Comparativa SEGOB.

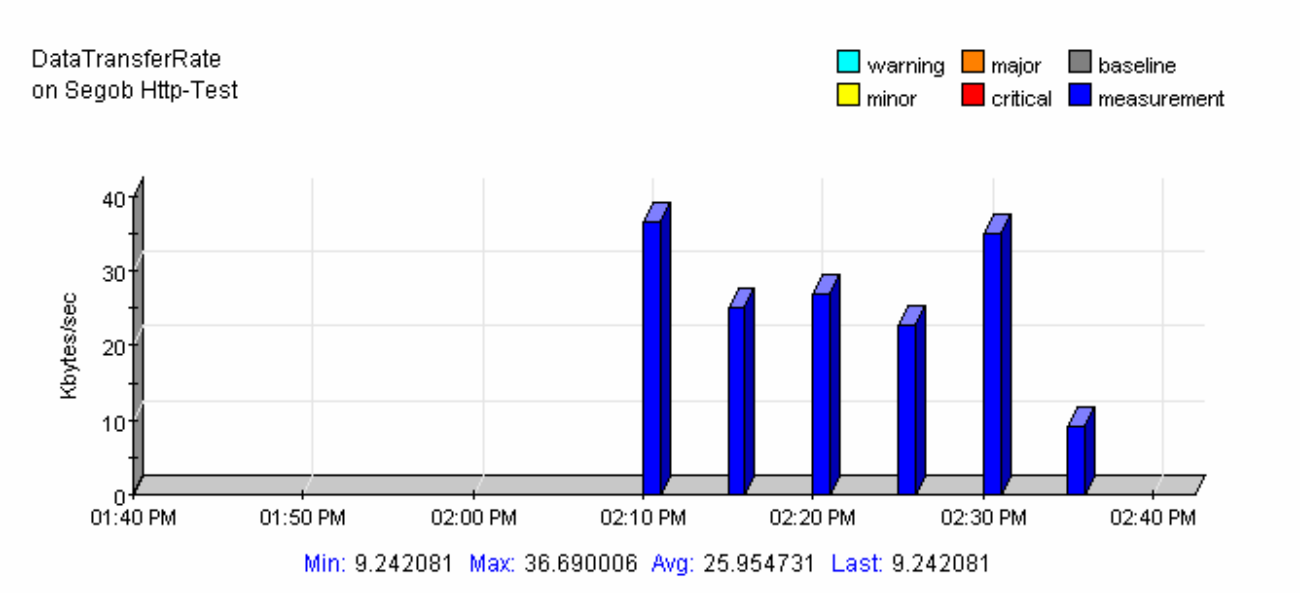


**Fig. A.32** Gráfica Tasa de transferencia de datos SEGOB.

## SHCP.

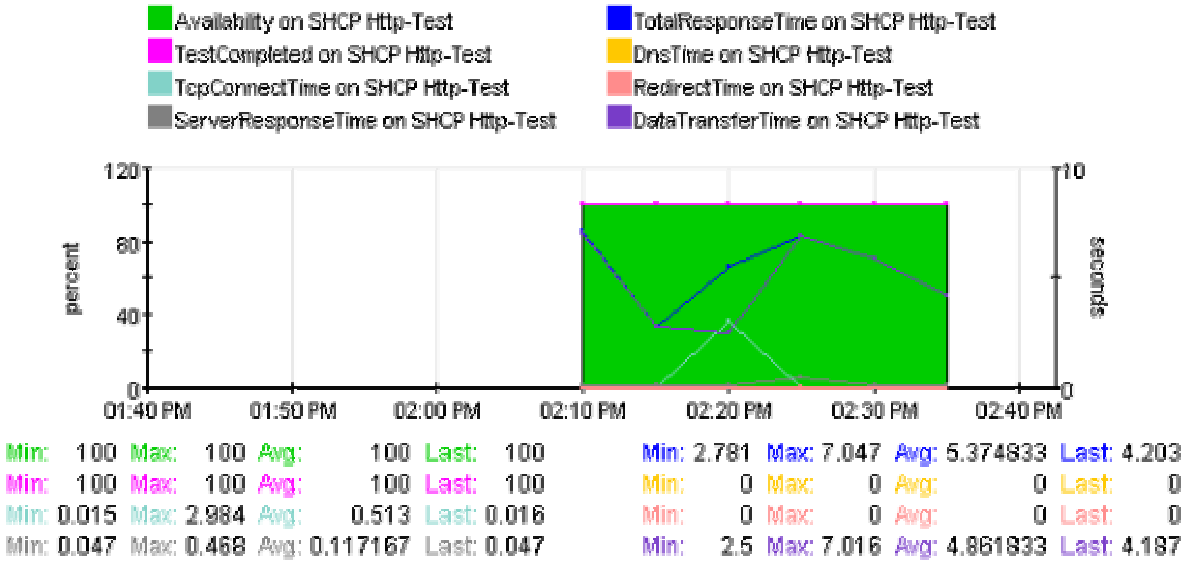


**Fig. A.33** Gráfica Comparativa SHCP.

## SRE.

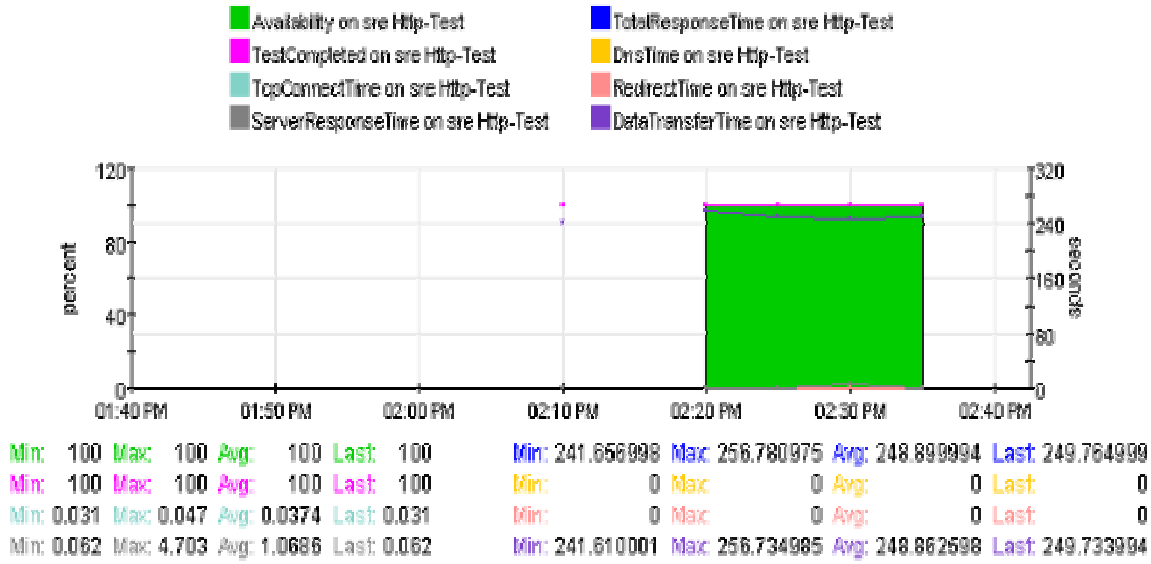


**Fig. A.34** Gráfica Comparativa SRE.

## SEP.


**Fig. A.35** Gráfica Disponibilidad SEP.

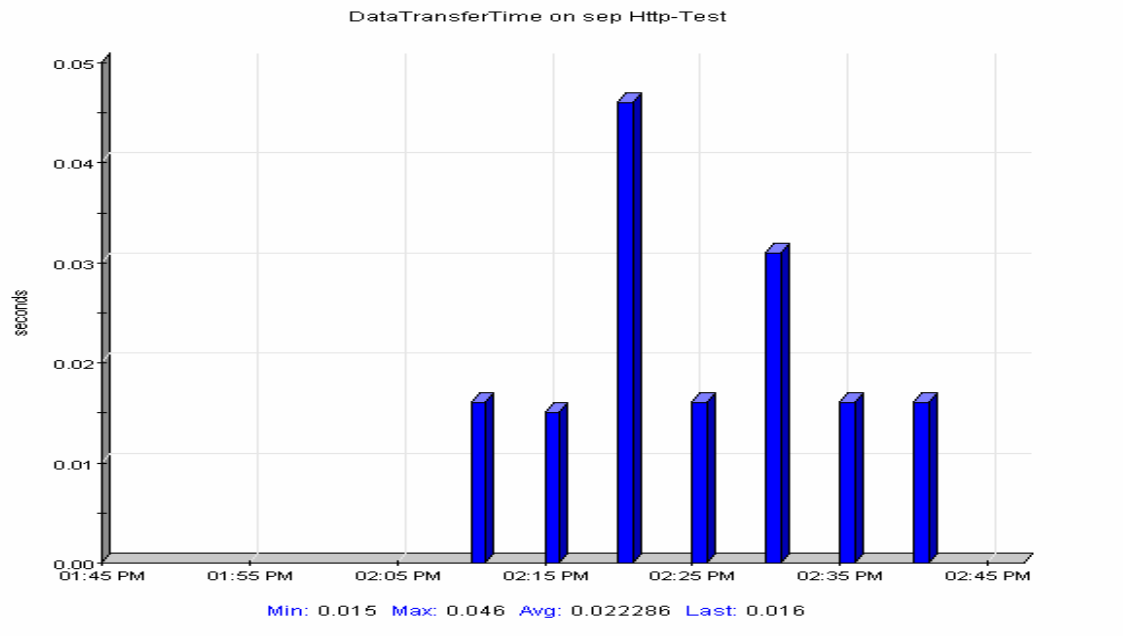


**Fig. A.36** Gráfica Tiempo de transferencia de datos SEP.

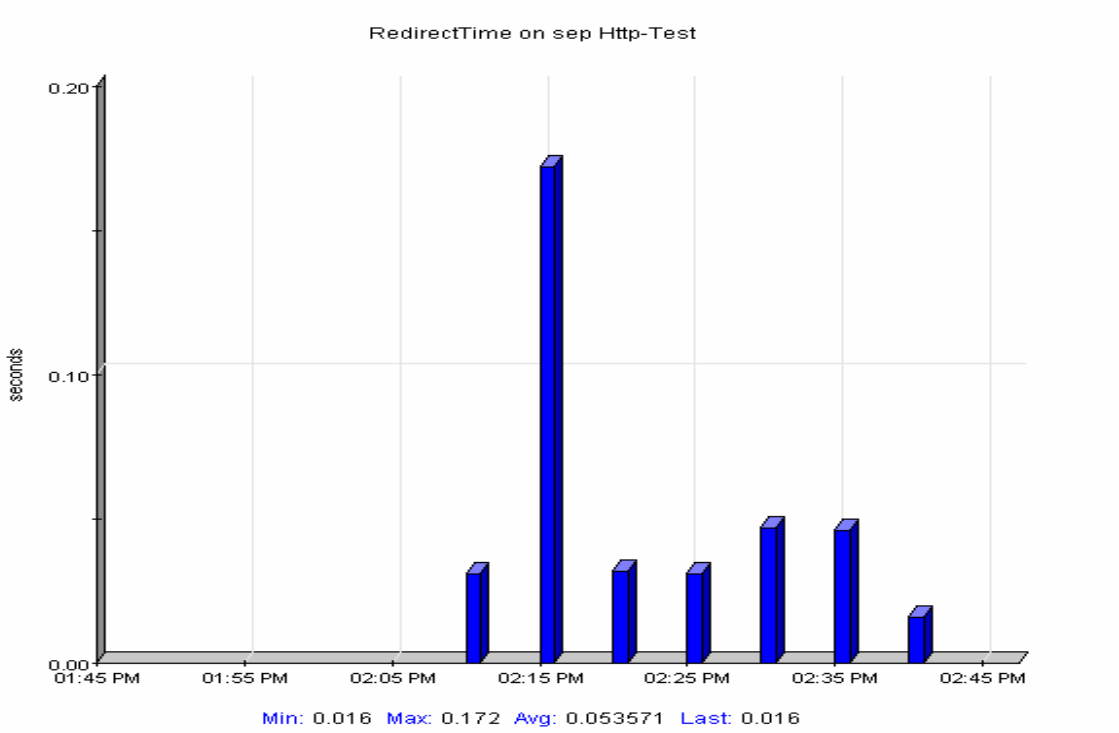


**Fig. A.37** Gráfica Tiempo de redireccionamiento SEP.

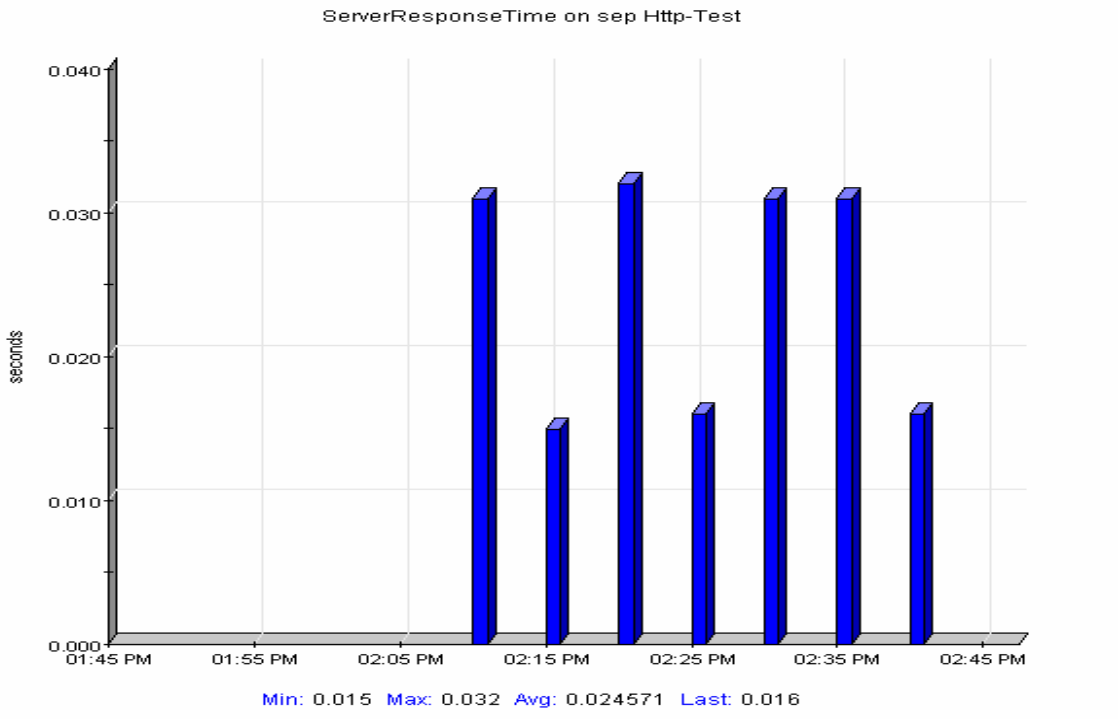


**Fig. A.38** Gráfica Tiempo de respuesta del servidor SEP.

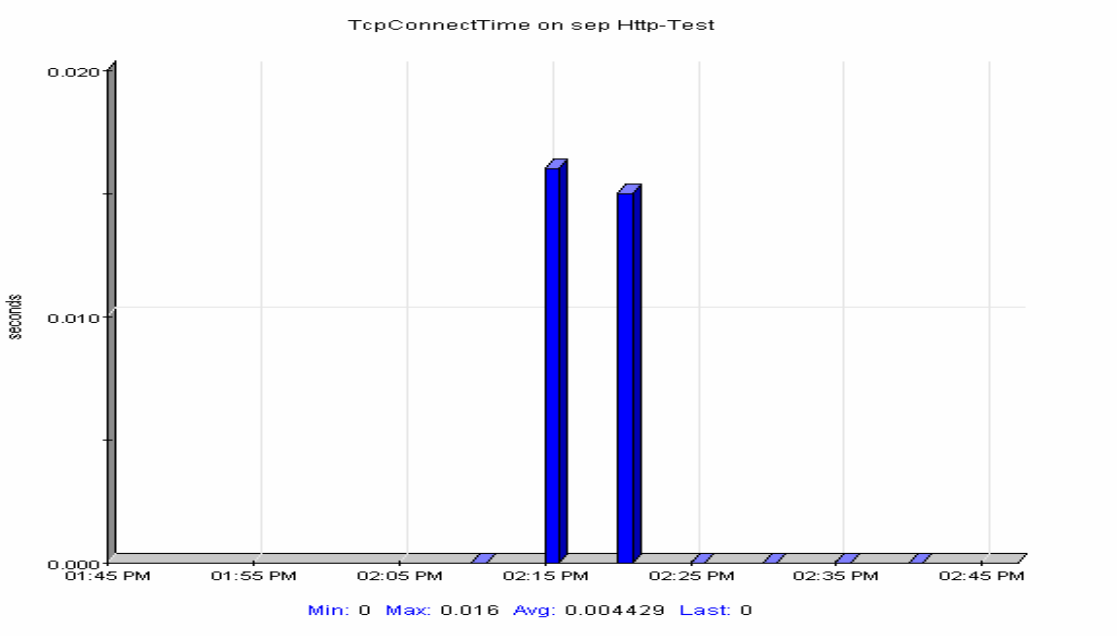


**Fig. A.39** Gráfica Tiempo de conexión TCP SEP.

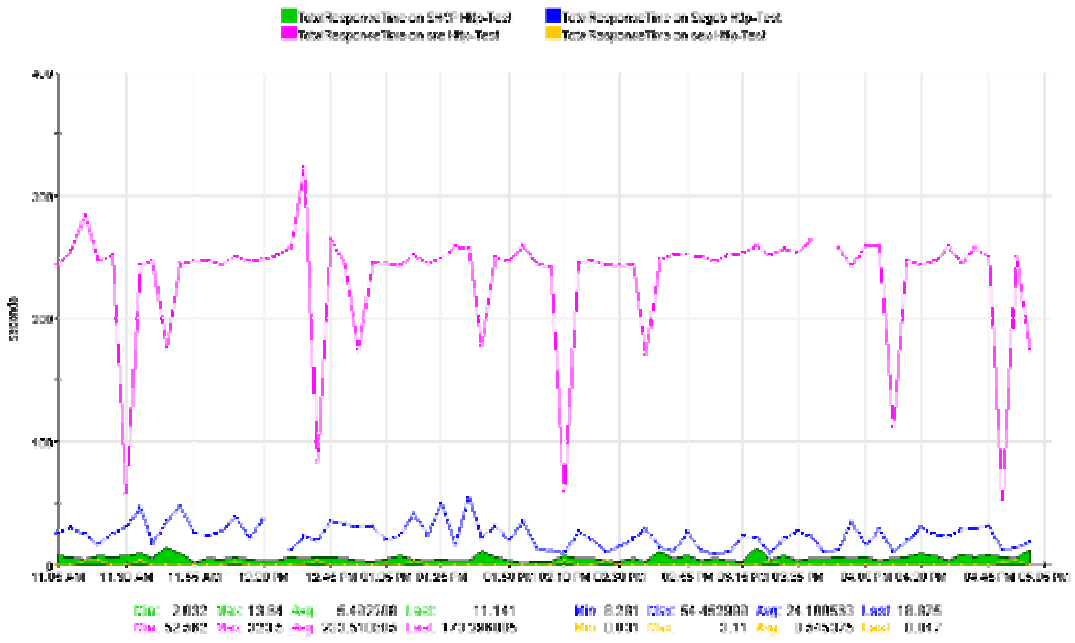

**Fig. A.40** Gráfica Comparativa Tiempos de Respuesta páginas de Gobierno.

## Funcionamiento

***Consola de Administración:***

La consola de administración es donde se construye y maneja el modelo de servicios, si entendemos que el modelo de servicio es el que proporciona una vista dinámica y gráfica del ambiente de servicio.

Además, la consola de administración muestra los servicios y facilita el manejo y la configuración de éstos, de acuerdo al modelo de servicio establecido.

La ventana de la consola de administración está dividida en dos partes, la parte derecha muestra la vista de plantillas, mientras que en la parte izquierda están los servicios, como lo ilustra la figura B.1.

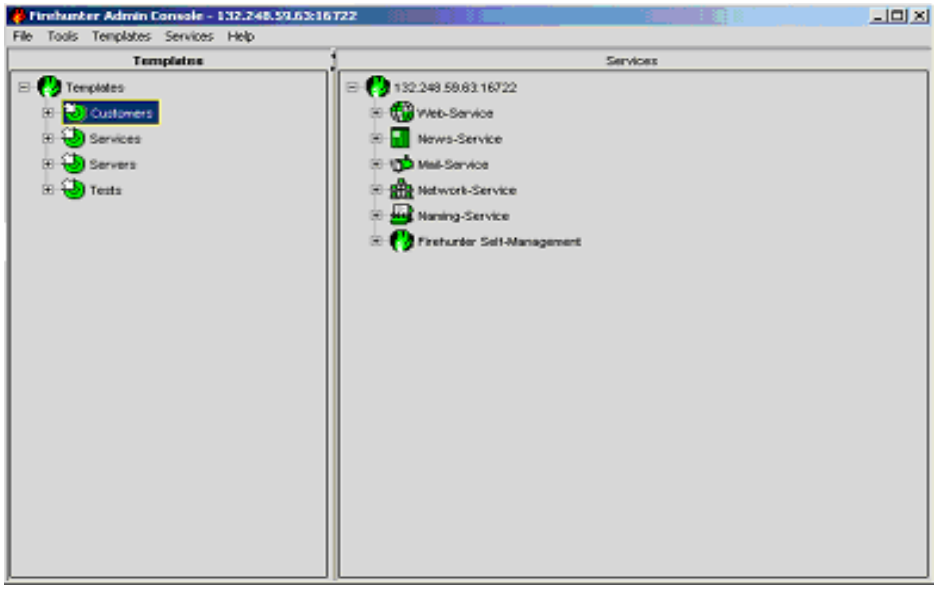


**Fig. B.1.** Consola de Administración.

***Interfaz Gráfica de Usuario:***

La Interfaz Gráfica de Usuario (GUI) permite monitorear fácilmente el estado de los servicios por medio de gráficos, eventos e informes de acuerdo a lo establecido en los niveles de servicio. A través de la GUI se puede ver el ambiente de nuestro modelo de servicio en tiempo real, la ventana principal de la GUI (figura B.2) contiene cuatro etiquetas, que se pueden configurar para que se despliegue cualquier combinación de éstas.

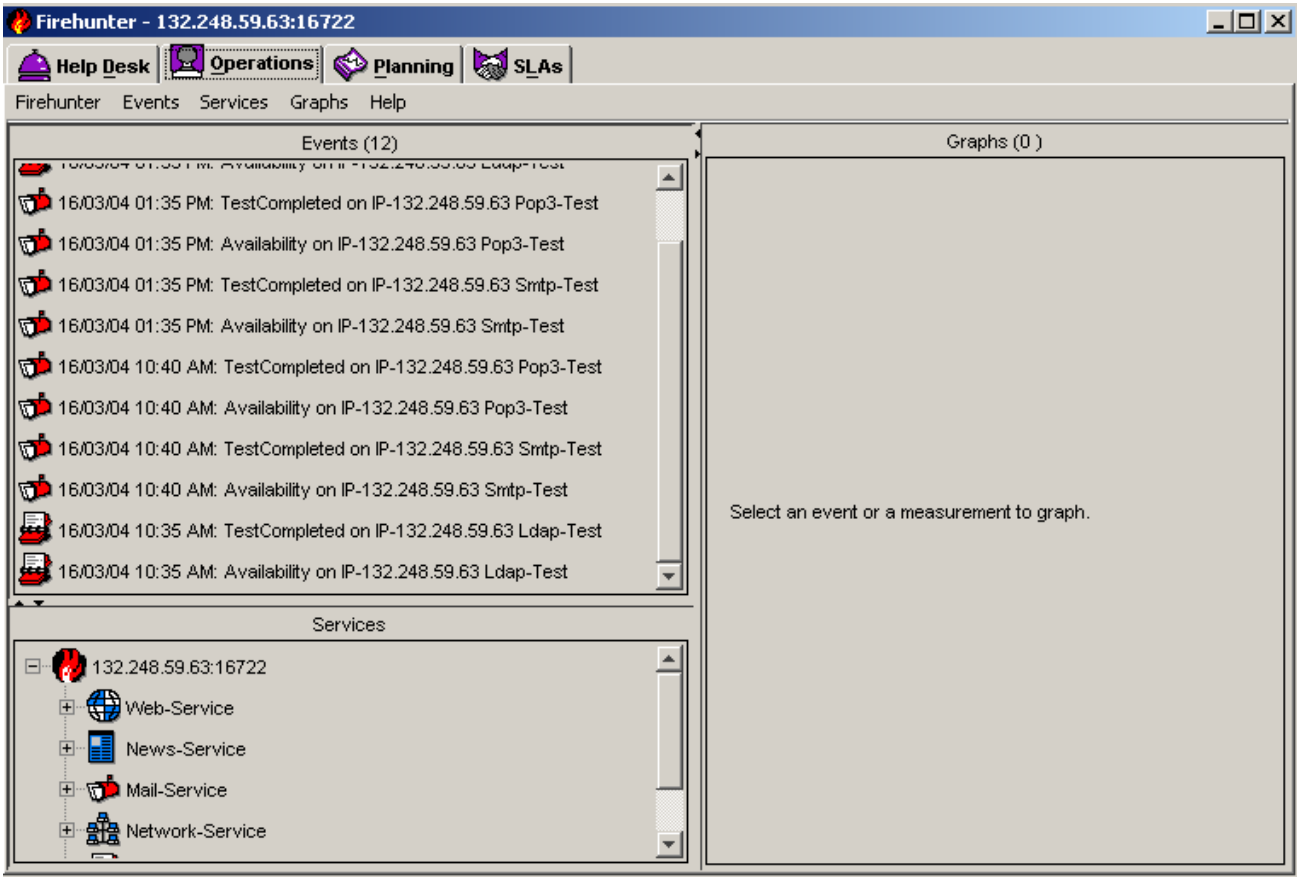


**Fig. B.2.** Interfaz Gráfica de Usuario.

La etiqueta de ayuda de escritorio permite ver rápidamente información sobre los servicios específicos, cada uno de los servicios es representado por un icono, el color del icono permite ver de manera fácil el estado del servicio.

Mientras que la pestaña de *operations* nos despliega la información en tres vistas, la vista de eventos muestra los valores que han cruzado los límites acordados, la vista de servicios despliega el modelo de servicio que se configuró en la consola de administración, y en la vista de gráficos se muestran gráficamente los valores específicos contra el tiempo.

El sistema propuesto monitorea los servicios de Internet de acuerdo a un modelo de servicio, dicho modelo es una estructura de árbol jerárquico, que permite ver las dependencias e interpretar los datos rápidamente, además de contar con ayuda visual, debido a que se puede estimar el estado de un servicio de acuerdo al color del icono que lo representa, esto es, si el icono está en rojo, indica un problema crítico en ese servicio, y en verde indica que todo está trabajando apropiadamente. Pueden existir estados intermedios entre los dos anteriores, que el sistema propuesto también los ilustra de forma visual como lo muestra la figura B.3.

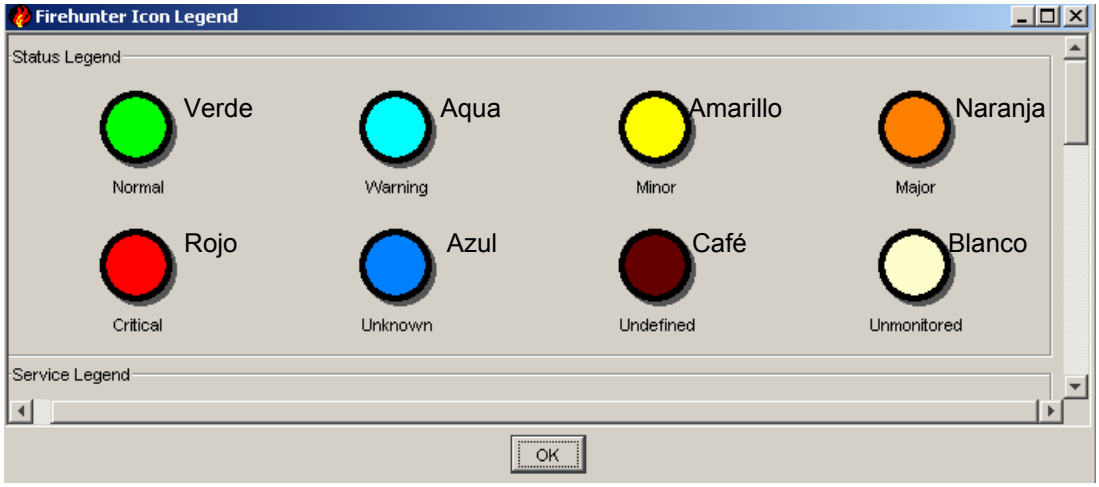


**Fig. B.3.** Código de colores.

El código de colores anterior muestra, que si el icono de un servicio se encuentra de color aqua, se está en alerta, en amarillo indica que el grado de peligrosidad es menor, contrario al naranja que indica un grado de peligrosidad mayor, el icono en color azul indica que el estado es desconocido, el café está indefinido, y el color blanco indica que el servicio no está monitoreado.

La flexibilidad de la estructura del modelo de servicio permite monitorear fácilmente cualquiera de estos, correr pruebas y tomar medidas.

Para ayudar a crear un modelo de servicio, el sistema proporciona plantillas para definir y organizar los clientes, servicios, servidores, componentes de la red, pruebas, etc.

La estructura de dichas plantillas contiene subgrupos predefinidos que incluyen las pruebas y las dimensiones establecidas para los grupos fijados en el modelo de servicio.
Las plantillas de Firehunter se agrupan en cuatro (Fig. B.4.):

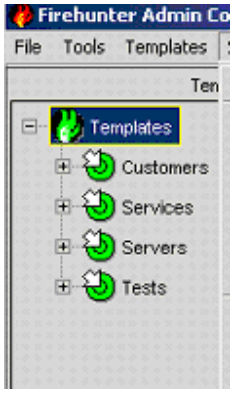


**Fig. B.4.** Plantillas del Modelo de Servicio

- Clientes: Esta plantilla proporciona una estructura que contiene los servicios, los servidores y las pruebas apropiadas para los tipos de clientes que soporta el modelo.

- Servicios: Esta plantilla representa los servicios, contiene una estructura predefinida de los servicios agregados, como FTP, seguridad, servicios de red, etc.

- Servidores: La plantilla de servidores contiene pruebas específicas y mediciones para diferentes tipos de servidores.

- Pruebas: Esta plantilla representa las pruebas de Firehunter que están disponibles.

El modelo de servicio tiene la flexibilidad para organizarlo de varias formas como: por clientes específicos y sus servicios o por servicios específicos y sus servidores.

Firehunter cuenta con detección automatizada de los servicios que se encuentran dentro del rango de direcciones IP establecido (Fig. B.5.). Los servicios detectados son agregados automáticamente al modelo de servicio propuesto.


**Fig. B.5.** Ventana para establecer el rango de direcciones IP.

Para tener un panorama más amplio de los servicios, el software cuenta con dos tipos de pruebas:

- Pruebas activas: Las pruebas activas ayudan a evaluar la calidad de los servicios simulando experiencias de clientes reales. Las pruebas activas generan el tráfico a las redes, servidores y aplicaciones, para evaluar el desempeño durante un uso real.
- Pruebas Pasivas: Las pruebas pasivas proporcionan información sobre el desempeño de la infraestructura, por ejemplo, una prueba pasiva estima el estado de un servidor de acuerdo a su desempeño histórico.

Las pruebas proporcionan datos de las mediciones en un intervalo de tiempo definido, estos datos pueden verse de forma gráfica (Fig. B.6.) a través de la interfaz gráfica de usuario.

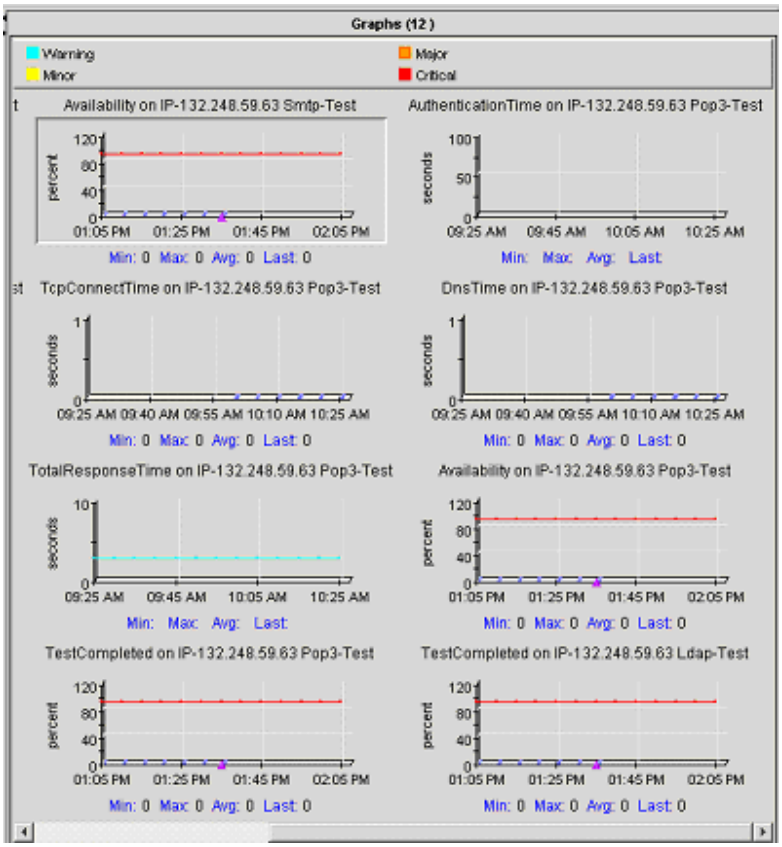


**Fig. B.6.** Gráficos de respuesta (GUI).

Para evitar datos innecesarios que podrían confundir o hacer complicada la toma de decisiones, el software tiene la habilidad de manejar los datos por excepción, sólo se manejan los datos significativos y se notifica cuando ocurre un evento importante, para poder saber cuando existe un problema, se lleva un registro histórico de cómo se comporta cada uno de los servicios y cuándo este servicio rebasa el umbral para asegurar la calidad.

Estos umbrales pueden ser de varios tipos: estáticos, variables, crecientes y decrecientes, a continuación se hace una breve descripción de cada uno de ellos.

**Umbral Estático**: El umbral estático permite definir los límites como un valor fijo, por ejemplo, si nos interesa que el servidor de FTP esté siempre disponible, se configura un umbral estático para que cuando se detecte que la disponibilidad es menor del 100% sea notificado de inmediato.

**Umbral Variable**: Un umbral variable permite definir los límites del umbral, debido a que los valores tomados durante la medición varían considerablemente conforme pasa el tiempo, este tipo de umbral es muy ocupado en los servicios que durante el día su tráfico es constante y que por las noches o fines de semana se ve reducido.

**Umbral Creciente**: La condición del umbral creciente permite definir un límite superior específico para los valores tomados. La violación de este límite ocurre cuando un valor tomado excede el umbral creciente.

**Umbral Decreciente**: El umbral decreciente permite especificar un límite inferior para los valores tomados.

# Referencias

## Capitulo I

[1] www.cisco.com

[2] Calidad de Servicio y Satisfacción del Cliente
Martínez Tur Ed. Paidos.
España 1998. 369 pp.

## Capitulo II

[1] Redes de Área Local (LAN)
Neil Jenkins. Ed. Prentice Hall 1998.

[2] Diccionario de términos Computacionales
Walter Ströbl Ediciones Rioduero
México 1990.

[3] www.htmlweb.net/redes

[4] Construya Firewalls para Internet
Chapman Ed. Mc Graw Hill
México 2001 515pp.

[5] Internet, Manual de Referencia
Harley Hahn Ed. Mc Graw Hill
México 1995 692pp.

[6] Construya un Servidor de Internet con Unix
George Eckel, Prentice Hall
México 1996 325pp.

[7] Redes de Computadoras, Protocolos, normas e Interfaces.
Uyless Black, Ed. Macrobit
España 1990 465pp.

[8] TCP/IP
Pete Loshin Ed. Ap. Professional
USA 1997 408pp

# Capitulo III

[1] http://europa.eu.int/information_society

[2] Construya Firewalls para Internet
Chapman Ed. Mc Graw Hill
México 2001 515pp.

[3] Construya un Servidor de Internet con Unix
George Eckel, Prentice Hall
México 1996 325pp.

[4] www.cisco.com

# Capitulo IV

[1] www.qos.unam.mx

[2] Calidad de Servicio y Satisfacción del Cliente
Martínez Tur Ed. Paidos
España 1998.

# Capitulo V

[1] www.firehunter.com