

# Monitoreo y Análisis de Redes



Este documento contiene información que es propiedad de MIC LTDA y es considerada confidencial. La información es suministrada exclusivamente para estudio de El Cliente en su proceso de evaluación. Al recibir este documento El Cliente está de acuerdo en mantener la confidencialidad de su contenido, permitiendo el acceso al mismo solo a personas de la organización que tengan responsabilidad en el citado proceso de evaluación. Igualmente, EL Cliente se compromete a no copiar, reproducir ni distribuir copia alguna, en parte o en todo dicha información sin la previa autorización escrita de MIC LTDA.

# Contenido

[Introducción](#)

[Entendimiento de la Necesidad](#)

[Monitoreo y Análisis de Redes – Solución Propuesta](#)

[Descripción del Servicio](#)

[Hardware](#)

[Componentes](#)

[Módulo de Análisis de Tráfico LAN](#)

[Módulo para Auditoría de Servicios](#)

[Módulo para seguimiento de uso y consumos](#)

[Módulo de Análisis de Tráfico en Consola](#)

[Actividades que cubre el servicio](#)

[Descripciones](#)

[Gestión de Niveles de Servicio](#)

[Alcances](#)

[Entregables](#)

[Licenciamiento](#)

[Forma de Pago](#)

[Tiempo de Entrega](#)

[Validez de la Oferta](#)

[Salvedades](#)

## **Introducción** [\(Inicio\)](#)

Las plataformas abiertas se vienen utilizando en grandes proyectos dentro de las empresas, como una alternativa de fácil implementación, económica y eficiente para soportar redes y aplicaciones.

Los grandes fabricantes de equipos como IBM, Compaq, Dell y Hewlett-Packard ofrecen equipos y soporte en plataformas abiertas. De la misma forma, las empresas de software más grandes como Oracle y SAP han portado sus productos y están siendo usados en las empresas para soportar las aplicaciones críticas del negocio, dice Dan Kuznetsky un analista de IDC Corporation.

La mayoría de los usuarios confirman que las plataformas abiertas ofrecen ventajas sobre los productos propietarios. Resultado de ello, es que Apache, servidor web libre, es el más usado en Internet, con el 75% de todos los servidores que existen en la red de redes.

## **Entendimiento de la necesidad** [\(Inicio\)](#)

Nuestro cliente necesita un sistema fiable para monitorear y auditar los servicios que se prestan sobre la red de comunicaciones para obtener indicadores de gestión que le permitan calificar el desempeño de los medios y los equipos.

# Monitoreo y Análisis de Redes

## Solución Propuesta [\(Inicio\)](#)

### Descripción del Servicio [\(Inicio\)](#)

NMS es un conjunto de herramientas seleccionadas con base en criterios suficientes y reales para suplir las necesidades de administración de redes en las compañías, es el resultado de investigar los requerimientos más comunes y no satisfechos plenamente por software comercial costoso e inalcanzable en muchos casos

NMS se instala sobre plataforma Linux por tanto no necesita licencia de sistema operativo ni licencias de bases de datos, los requerimientos de hardware son mínimos comparado con otros productos comerciales:

### Hardware [\(Inicio\)](#)

- Procesador pentium IV 2.2 Ghz
- 512 Memoria RAM
- 40 GB de espacio en Disco Duro
- Una o varias interfaces de red 10/100 (Todas pueden ser monitoreadas)

### Componentes [\(Inicio\)](#)

El programa está compuesto por cuatro módulos, a tres de ellos se accede a través de una consola web y un módulo en formato texto sobre la consola del servidor para obtener información instantánea.

- **Módulo de Análisis de tráfico LAN [\(Inicio\)](#)**  
El módulo de red LAN es una potente herramienta que supera cualquier expectativa frente a la recopilación en línea de información acerca de lo que sucede en la red LAN, útil para encontrar problemas de varios tipos, como por ejemplo exceso de broadcast, virus de multidifusión, equipos con problemas en la NIC. Su información es una buena guía para aplicar segmentación.

Dentro de su menú de opciones se encuentra información clasificada de la siguiente manera:

- Protocolos sobre la red a nivel de MAC
- Protocolos sobre la red a nivel de TCP/UDP
- Total de tráfico clasificado por:
  - Enviado o recibido
  - Host origen
  - Protocolo
  - Ancho de banda utilizado
  - Horario
  - Estadísticas
    - Tráfico multicast
    - Tráfico
    - Host sobre la red con selección de ordenamiento
    - Carga de la red con reporte acumulativo, por horas, días, semanas, meses y años
- Estadísticas de tráfico IP
  - Local a Local
  - Remoto a local
  - Local a remoto
  - Remoto a remoto
  - Matrix de tráfico entre hosts
- Estadísticas de protocolos IP
  - Distribución de protocolos

- Uso. (Permite observar quien ofrece el servicio y quien lo accede)
- Sesiones. (Permite ver como se suceden las conexiones IP entre hosts)
- Routers. (Capturar equipos que ofrecen salida a otras redes)

Las figuras 1,2,3 y 4 muestran algunos de los tópicos más importantes:

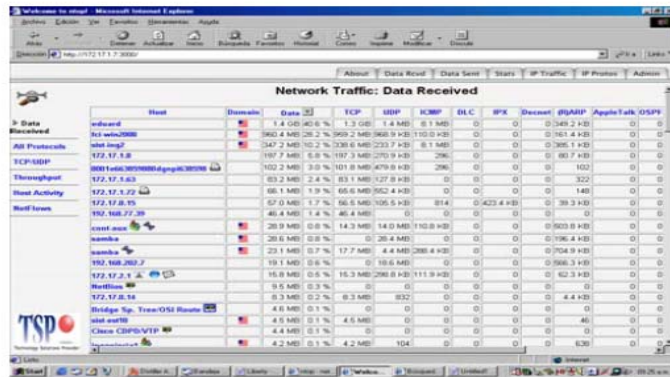


Figura 1

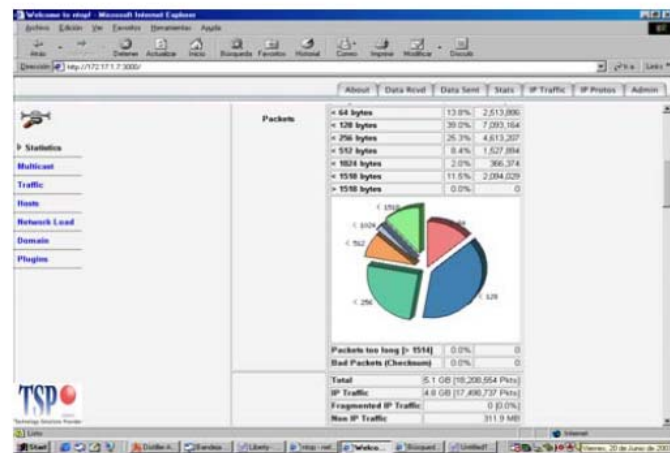


Figura 2

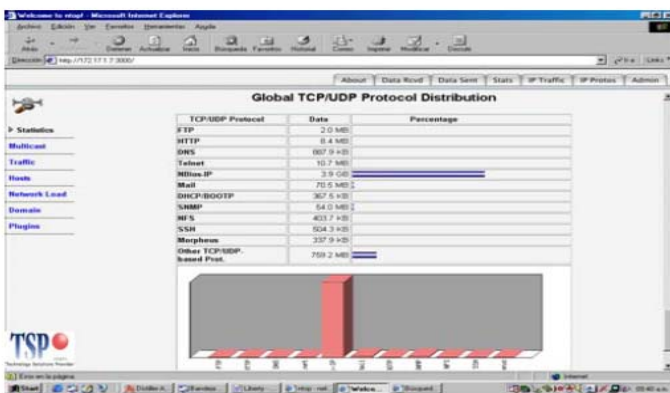


Figura 3

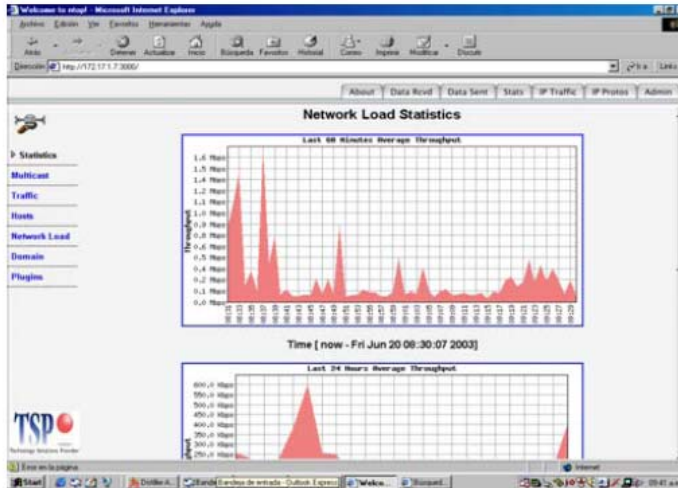


Figura 4

- **Módulo para auditoria de servicios** [\(Inicio\)](#)

Es una plataforma robusta de gestión que usa SNMP y scripts de consulta al protocolo IP lo cual la hace muy flexible, está orientada a obtener y acumular información sobre el estado de los servicios durante todo el tiempo, éste módulo es útil para llevar a cabo auditorias específicas de elementos tales como los enrutadores y sus interfaces lógicas que son configuradas para subir un canal WAN ó servicios de red locales o remotos como SMTP, POP3, HTTP, Proxy, etc. cualquier aplicación IP puede ser monitoreada. La plataforma en su versión actual puede monitorear hasta 5000 elementos distintos.

Este módulo potencia al administrador de la red para:

- Mapeado: NMS crea un diagrama en dos y tres dimensiones de la red modeladas.
- Monitorización: NMS matricula y monitorea dispositivos críticos, aplicaciones, y la utilización de los recursos.
- Notificación: La notificación de los eventos de inactividad está disponible a través alarmas de sonido, correo electrónico ó buscapersnas, de forma que Ud. sabrá, antes que nadie, si un servidor o servicio críticos quedan inactivos.
- Informes con historiales: NMS provee una suite de reportes en modo gráfico a través del browser con los principales indicadores de gestión de un servicio. Disponibilidad y tiempos de respuesta de los dispositivos y aplicaciones de su red, información útil para exigir niveles de servicio y planificar las capacidades y la administración de recursos.

Los informes gráficos facilitan el seguimiento de los niveles de servicios y le permiten monitorear la calidad proporcionada por sus proveedores de servicios.

- Menú de monitoreo
  - Vista general (Figura 5)
  - Detalle de los servicios (Figura 6)
  - Detalle de los hosts
  - Resumen de las vistas
  - Mapa 2D
  - Mapa 3D (Figura 7)

- Menú de reportes (Por host o servicio)
  - Promedios (Figura 8)
  - Disponibilidad
  - Histograma de alertas
  - Historia de alertas
  - Resumen de alertas
  - Notificaciones
  - Log de eventos (Figura 9)
- Menú de configuración
  - Configuración

Una vez los servicios se han matriculado al sistema, inmediatamente comienza a sensar y a construir la información que puede ser accedida por cada uno de los items del menú.

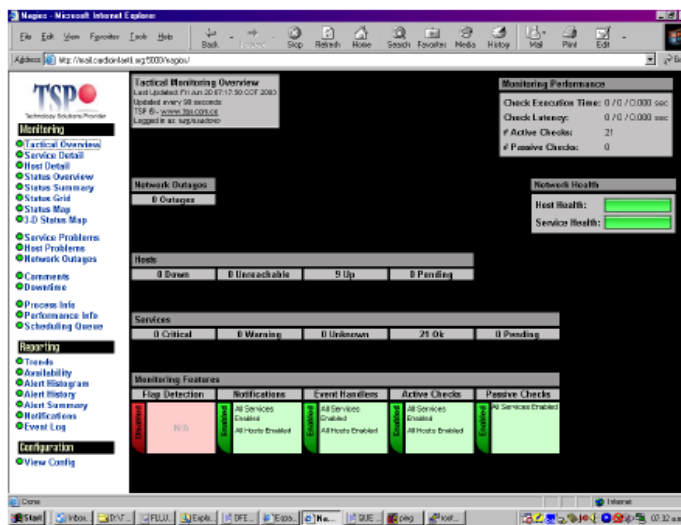


Figura 5

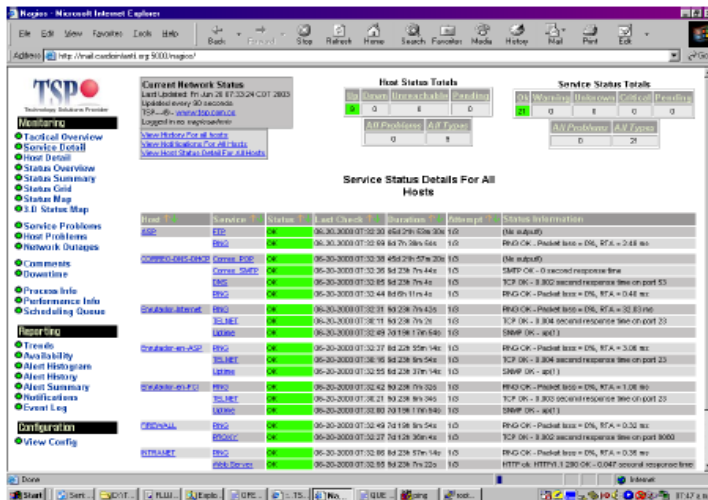


Figura 6



- **Módulo para seguimiento de uso y consumos** [\(Inicio\)](#)  
Su misión es explotar la característica de SNMP que viene con los equipos gestionables, proveer de información continua al administrador del sistema acerca del tráfico sobre los SW y sobre los canales.

Es una herramienta específica y dedicada a dibujar periódicamente los promedios de los totales de tráfico que cursan sobre algún dispositivo específico como:

- Interfaces de canales de comunicaciones sobre enrutadores gestionables.
- Puertos de SW gestionables.
- Puertos de HUBS gestionables.
- Tarjetas de red de servidores o pc's con SNMP activo.

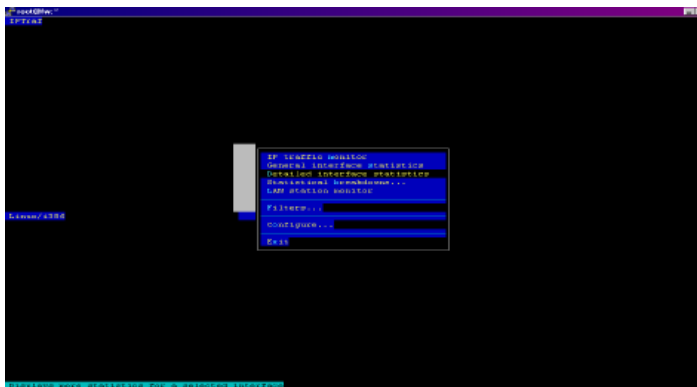
Puede ser extendido a cualquier dispositivo, sistema operativo o aplicación que posea SNMP y pueda ser accedida a través de una comunidad de lectura.

La figura 10 muestra un ejemplo de esta captura y las cuatro vistas que posee, día en intervalos de 5 minutos, semanal, mensual y anual.



Figura 10

- **Módulo de análisis de tráfico en consola** [\(Inicio\)](#)  
Es un módulo eficaz para capturar y observar los flujos de tráfico sobre la red de manera inmediata, la figura 12 muestra el menú y la figura 13 muestra un ejemplo del tráfico que cursa sobre una de las interfaces y la caracterización que se le da con sus diferentes propiedades



	Total	Incoming	Outgoing	Dropped
TCP	1244	1244	0	0
UDP	1244	1244	0	0
ICMP	0	0	0	0
Other	0	0	0	0

Total: 1244 packets  
 Incoming: 1244 packets  
 Outgoing: 0 packets  
 Dropped: 0 packets

### Actividades que cubre el servicio [\(Inicio\)](#)

- Consultoría para la implantación del esquema con acceso remoto a través de Internet.
- Matricula inicial de servicios a monitorear.
- Instalación del sistema operativo en la maquina entregada por el cliente: Linux Red Hat e interfaces de red (Aplicación de parches a la fecha de instalación y última versión de kernel)
- Instalación y configuración de los cuatro módulos descritos.

### Descripción [\(Inicio\)](#)

El soporte técnico en informática es un servicio indispensable, el cual se debería contratar por varios motivos. TSP ofrece una amplia variedad de estos servicios, adaptados a distintos tipos de organizaciones y empresas. El soporte técnico es una necesidad que irá creciendo a medida que la empresa esté más sistematizada, para poder explicar mejor que brinda un soporte técnico, se debe entender porque se genera esta necesidad. Para ello se puede apreciar la siguiente lista de requerimientos o incidentes que se pueden presentar:

- **Incidente:** fallos generales del hardware
- **Causa:** El hardware puede fallar por varios motivos, uno de los más comunes es por fallas eléctricas en estos dispositivos, pueden ser cualquier parte de una PC (disco duro, tarjeta de red, procesador, memoria, etc.). En muchos casos es necesario cambiar el dispositivo por uno nuevo lo que conlleva a reconfigurar el hardware en el sistema operativo. Estos defectos casi siempre son insalvables y requieren una atención inmediata.
- **Incidente:** fallos en el sistema operativo y componentes de este
- **Causa:** Si bien Linux es uno de los sistemas operativos mas seguros en el mercado, el cual no requiere tanta atención como otros. Este puede llegar a fallar por varios motivos, unos de los mas comunes es por cortes de luz, lo que genera el mal apagado del equipo y por consiguiente del sistema operativo, ocasionando en el peor de los casos algún tipo de problema en este. Estos incidentes también requieren una atención inmediata.
- **Incidente:** Reestructuración de PCs, impresoras, etc.
- **Causa:** muchas veces en las organizaciones se realizan movimientos de personal o cambios en la planta física lo que ocasiona que se deban reorganizar los equipos informáticos. Durante estas reorganizaciones es conveniente que se supervisen por expertos en el sistema informático, para evitar mayores complicaciones.
- **Incidente:** Nuevos requerimientos informáticos.
- **Causa:** Las organizaciones normalmente crecen en requerimientos informáticos, por varios motivos, algunos de los cuales pueden ser el ingreso de más personal a la empresa,

crecimientos de las bases de datos, nuevos programas informáticos, etc. Todos estos motivos recargan los servidores y estaciones de trabajo de la empresa, lo cual se soluciona optimizando el hardware de estos equipos. En estos casos es necesaria la intervención de especialistas en el sistema operativo para adecuarlo a los nuevos recursos de hardware.

- **Incidente:** Cambio en la operatividad del sistema.
- **Causa:** Muchas veces se deben hacer cambios en la forma en que se organizan los sistemas informáticos, estas reorganizaciones son requeridas muchas veces por causas internas de las empresas, para hacerlas posibles se debe solicitar el servicio de profesionales en sistemas. Se ha visto una lista reducida de algunos posibles problemas en el que las empresas requerirán la intervención de especialistas. Por tal motivo y conociendo que todas no tienen los mismo requerimientos, TSP dispone de la siguiente serie de soportes.

### Descripción del Servicio

MIC LTDA. ofrece dos modalidades de contrato por mantenimiento anual sobre cada uno de los servicios instalados, el cliente elige cual contrato anexa a cada servicio. Estos contratos se firman de común acuerdo y se rigen por el código comercial Colombiano.

Estos contratos buscan que el cliente no se sienta desprotegido por el uso de estas tecnologías y se libera de la carga del soporte de estos servicios a nivel de servidores de tecnología periférica, preocupándose solamente por mantener en operación y soportar las tecnologías centrales del negocio y a sus usuarios finales.

A continuación se describe los dos tipos de servicio:

SERVICIO	CONTRATO TIPO A	CONTRATO TIPO B
Atención a incidentes	Si	Si
Visita técnica preventiva al mes	Si	No
Actualizaciones periódicas	Si	Si
Asistencia telefónica	Si	Si
Asistencia remota vía Internet o RAS	Si	Si
Asistencia técnica presencial	Si	Si
Horarios de atención	5X24	5X8
Tiempo de respuesta	3H	24H
TAC (Ticket de servicio vía Web)	Si	Si
Backup automático diario en TSP	Si	No

### Descripción del Servicio

NMS debe ser acompañado por servicios de mantenimiento de la red y todos sus componentes, esto implica conocimiento y experiencia en el manejo de tecnologías y soluciones para aprovechar de forma real la información que entrega un sistema de gestión como NMS.

MIC LTDA. con su equipo de Ingenieros calificado, brinda este servicio a través de contratos que incluyen diagnóstico permanente, generación de planes de trabajo por medio de una visita semanal de seguimiento y acompañamiento tanto en la presentación de proyectos para mejorar la red como en el desarrollo de aquellos que la impacten directamente.

La red es un sistema compuesto por elementos activos y pasivos, la red parte del cable y termina en el resultado que entrega un sistema de información, involucra muchos elementos que deben ser revisados continuamente para mantener todo en operación con base en un conocimiento pleno de la misma que solo se logra con un equipo de trabajo con el conocimiento necesario para dedicar el tiempo exclusivamente en ello.

El marco de negocios actual exige una respuesta rápida a la evolución del mercado. Su empresa no se puede quedar atrás, necesita una gestión proactiva de la misma. La rápida evolución de las tecnologías de red obliga a considerar los siguientes factores a la hora de mantener una arquitectura competitiva:

Necesidades crecientes de ancho de banda por la aparición de aplicaciones Cliente/Servidor  
Mezcla de contenidos en la transmisión de información: datos, voz, multimedia, vídeo  
Soporte de las nuevas tecnologías de WAN aportadas por los operadores: RDSI, Frame Relay, ATM, xDSL, Servicio IP, etc.

Evolución de los adaptadores de red: Fast Ethernet, Giga Ethernet.  
En este entorno, para crecer, su empresa ha de adaptarse a esta evolución constante que supone necesidades de gestión de red cada vez más complejas y con requerimientos de disponibilidad garantizados.

MIC ofrece este servicio en compañías que han adoptado la solución NMS de MIC o la labor se cumple con las herramientas de gestión que posea el cliente y las recomendadas para cada fin.

Para crecer, su empresa ha de adaptarse a necesidades de gestión de red cada vez más complejas y requerimientos de disponibilidad garantizados.

### **Gestión de niveles de servicio [\(Inicio\)](#)**

Gestión del Servicio REAL ofrecido a los clientes o usuarios del departamento T.I. con un enfoque en:

Medida del servicio REAL, midiendo la salud de la infraestructura informática.

Identificación y análisis del problema, no sólo a través de las alertas generadas por las diferentes infraestructuras, sino identificando el origen y la causa raíz del problema, para su resolución automática o manual, permitiendo conocer el análisis de cómo y porqué ha ocurrido, de forma rápida y evitando que vuelva a ocurrir en el futuro. Esta es la diferencia entre resolver un problema puntual y dejar que vuelva a ocurrir o de resolverlo de forma eficaz y rápida para que no vuelva a suceder. Identificación del Impacto en el servicio y en los negocios, en los procesos a los que da soporte la infraestructura IT.

Visualización de forma clara, sencilla y global, desde cualquier puesto, desde cualquier lugar, del servicio ofrecido al negocio a través de las infraestructuras y procesos informáticos, con su particularización para cada área y persona implicada en el mismo.

### **Alcances [\(Inicio\)](#)**

MIC se compromete a través de una visita semanal de 4 horas a realizar una revisión de la red y sus componentes a través de varias herramientas continuas de gestión que se instalan en un equipo del cliente como parte del servicio.

MIC Se compromete a realizar un Análisis de tráfico sobre la red LAN cada 6 meses.

Finalmente MIC se compromete a ejecutar herramientas puntuales para descubrir posibles causas de error o simplemente adelantarse a los hechos que se puedan presentar a futuro como consecuencia de algún elemento en mal estado.

Dentro de esta área se ejecutan las siguientes labores:

**Administración de las Fallas:** Consiste en determinar lo más rápido posible el punto de la red donde se presenta una falla para que sea corregida, ya sea a través de la administración remota, o del personal de servicio que acude al lugar donde se presenta la falla.

**Administración del Rendimiento:** Interpretación de el monitoreo de la red detectando sobrecargas o cargas bajas que afectan el buen funcionamiento del sistema, así como el análisis de áreas donde el tráfico tiende a aumentar. El Nivel de Servicio que se ofrece a los Usuarios es de una gran capacidad de respuesta, no solo en caso de fallas que se presenta el sistema, sino en la posibilidad de prevenirlas, además de administrar el rendimiento y configuración de la red.

**Administración de la Configuración:** Se ofrece al cliente la información detallada de todos los elementos de conectividad activos que conforman su red.

### **Entregables [\(Inicio\)](#)**

Informe mensual con estadísticas de rendimiento de servicios en la red local y los canales de ASP e Internet con el siguiente contenido.

- OBJETIVO
- INFORMACIÓN ACERCA DEL TRAFICO SOBRE LA RED
- Trafico sobre puertos del SW
- TOP 10 Equipos que más envían información actualmente.
- TOP 10 Equipos que más reciben información actualmente.
- Equipos con otros protocolos
- CARACTERÍSTICAS GENERALES DE FUNCIONAMIENTO DE LA RED LAN
- CARACTERÍSTICAS ESPECIALES DE INTERNET
- CARACTERÍSTICAS GENERALES DE FUNCIONAMIENTO DE LOS CANALES WAN (ASP – INTERNET)
- ASP
- Internet
- ESTADÍSTICAS DE SERVICIOS
- Servidor ASP
- Enrutador ASP en Integrar
- Enrutador ASP en FCI
- Firewall
- Correo
- Gestión
- Intranet
- LISTA DE SERVICIOS EFECTUADOS POR TSP
- Informe semestral con los resultados del Análisis de tráfico sobre la red LAN.

**Licenciamiento** [\(Inicio\)](#)

GPL - GNU

**Forma de Pago** [\(Inicio\)](#)

- **Instalaciones**  
50% anticipo a la firma del contrato.  
50% contraentrega a la firma del acta de recibido.
- **Contratos de Mantenimiento o Soporte**  
Factura mensual anticipada

**Tiempo de Entrega** [\(Inicio\)](#)

15 días para todo el proceso de consultaría e instalación

**Validez de la Oferta** [\(Inicio\)](#)

30 días a partir del recibo de este documento

**Salvedades** [\(Inicio\)](#)

- MIC. realizará los trabajos en la ciudad de Bogotá, desplazamiento o viáticos a otras ciudades correrán por cuenta del CLIENTE.
- MIC. no realizará gestiones que correspondan a las actividades propias del CLIENTE en el desarrollo del proyecto, como:
- Tramites ante entidades privadas o gubernamentales para la instalación o adquisición de elementos tangibles o intangibles que se requieran para la ejecución de este proyecto diferente a los que genere la contratación del servicio de instalación física de los equipos.
- Asignación de recurso humano para labores que no estén contempladas y comprometan de mejor forma al personal del CLIENTE.
- Actividades contractuales que se deriven por incumplimiento de alguna de las partes que se involucren en este proyecto y estén contempladas en las cláusulas acordadas entre el CLIENTE y el proveedor.
- MIC. no asumirá gastos ocasionados por tiempo e incumplimiento del cliente.