



Descripción del Servicio



CLIENTES MIC

SERVICIO DE DIAGNOSTICO Y ANALISIS DE TRAFICO LAN

Este documento contiene información que es propiedad de TSP 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 TSP.

Confidencial

2005

1. INTRODUCCION

Entregar información que facilite la toma de decisiones a partir del conocimiento real del comportamiento de la tecnología en la red de comunicaciones del **CLIENTE**.

2. ENTENDIMIENTO DE LA NECESIDAD

Las redes de comunicaciones han facilitado y mejorado notoriamente la forma de trabajar de las empresas, ha brindado velocidad en su operación y continuamente una mejor atención al cliente final.

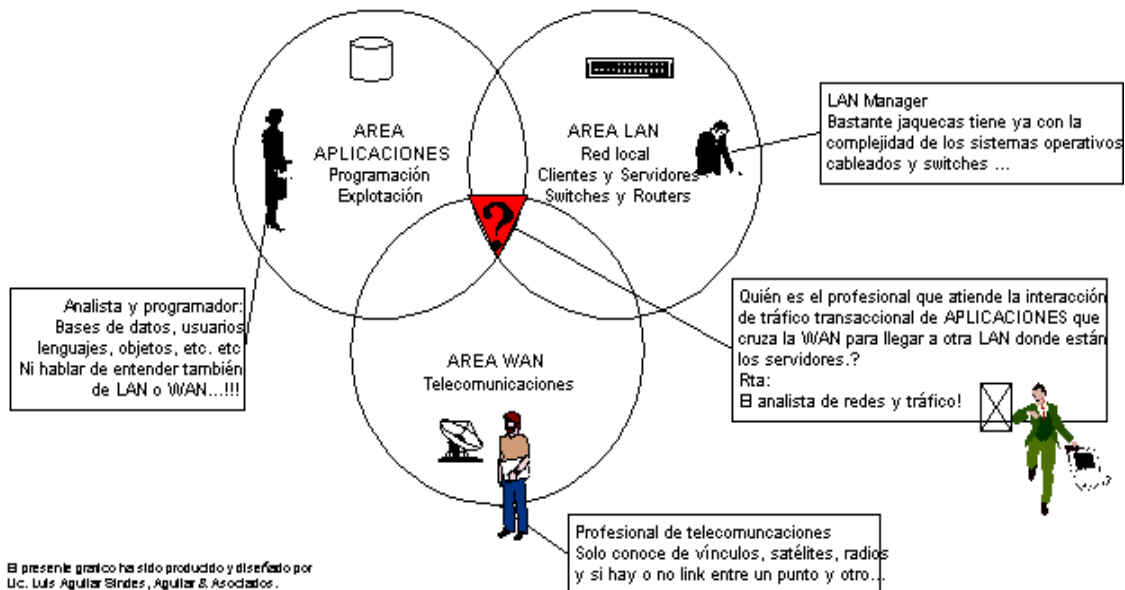
La reducción de costos en la operación diaria, también ha obligado a las compañías a buscar soluciones más económicas que aprovechen el 100% de la inversión que poseen en Tecnologías de la Información TI y todo soportado por la red de datos en continuo crecimiento generando en muchos casos la sobrecarga de las redes en detrimento de las aplicaciones.

Aparentes bajas de rendimiento en los servidores, desconexión continua de las estaciones de trabajo, caídas frecuentes de los canales de comunicación son tan solo algunos ejemplos que viven las empresas en la actualidad; tal vez el problema más serio sea el desconocimiento de las causas de dichos problemas o contar con herramientas o servicios especializados para diagnosticarlos.

El análisis de red debe hacerse continuamente, con medios propios o contratando servicios, la decisión de hacerlo debería darse mínimo cada vez que se intente iniciar un nuevo servicio sobre la red para evitar complicaciones con los usuarios, conflicto entre las aplicaciones actuales, con el proveedor y finalmente con usuarios y clientes de la organización.

El análisis a realizar sobre la red del **CLIENTE** permitirá determinar si se presentan o no deficiencias en la red de datos. En caso de encontrar deficiencias se definirán las labores a realizar para reopotencializar la plataforma, orientando todo este esfuerzo mediante un plan corto, mediano y largo plazo.

EL DILEMA PROFESIONAL Y HUMANO: AREA GRIS NO CUBIERTA



¿Porque es necesario el análisis de red?

3. METODOLOGIA

El modelo metodológico utilizado cumple con los lineamientos y parámetros de los sistemas de información.

3.1. PROCEDIMIENTO

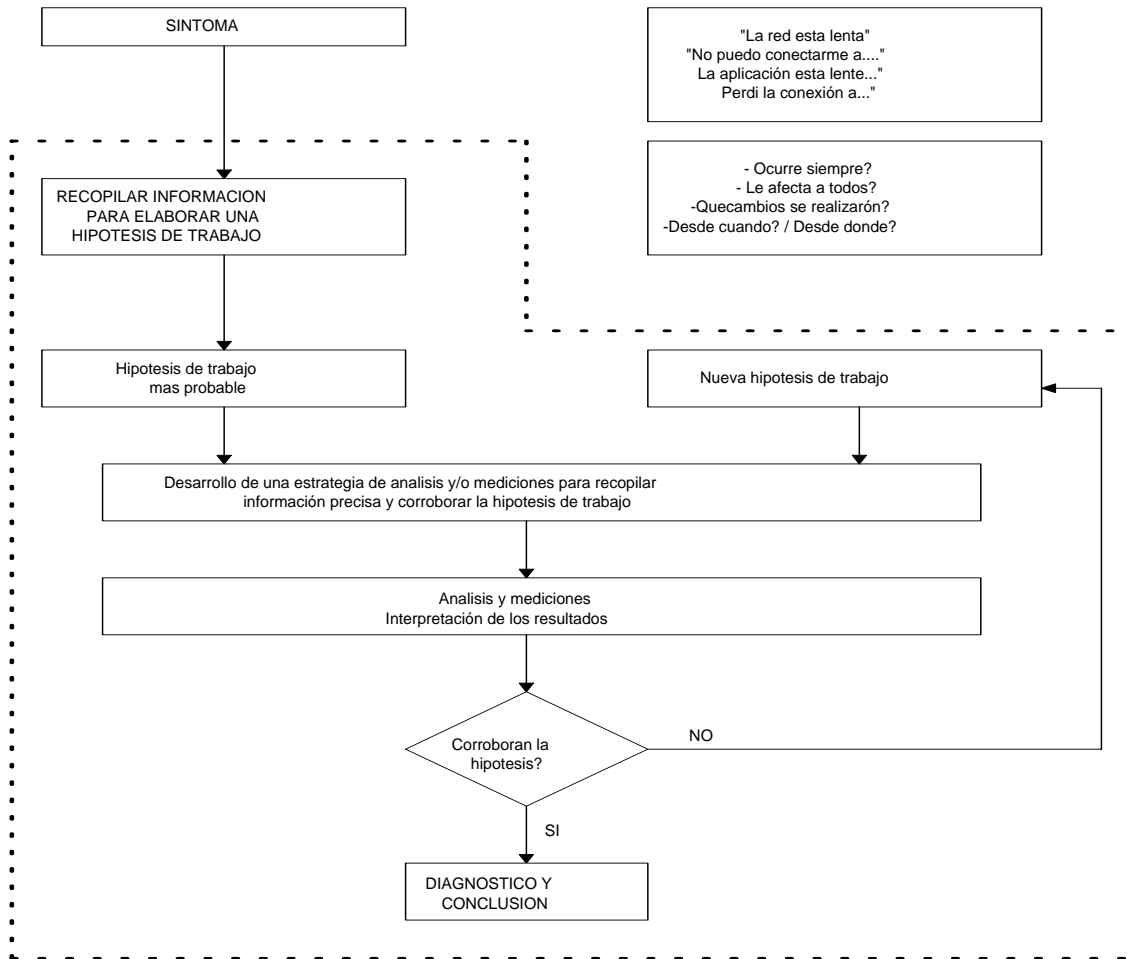


Diagrama bloques del análisis de red

PASOS A DESARROLLAR

- Levantamiento de información
 - ✚ Entrevistas
 - ✚ Recolección de documentación (Diagrama de la distribución física, certificación y documentación de puntos lógicos)
- Mapeo de la red
 - ✚ Descubrimiento de dispositivos en la red
 - ✚ Reconocimiento de equipos interesantes en la red
 - ✚ Detección de sistemas operativos en las maquinas interesantes
 - ✚ Recolección de datos de la red
- Instalación de las herramientas de monitoreo
 - ✚ Puesta en funcionamiento de los indicadores de gestión
 - ✚ Puesta en operación del sistema
- Toma de muestras
- Análisis de red de datos
 - ✚ Caracterización de red
 - ✚ Diagnóstico de tráfico
- Análisis de seguridad (servidores críticos)
 - ✚ Ubicación de equipos y servicios
 - ✚ Ejecución de pruebas de vulnerabilidades
 - ✚ Diagnóstico de vulnerabilidades
- Retroalimentación de información obtenida
 - ✚ Preinforme técnico (presentación de resultados)
 - ✚ Presentación del informe sobre el estado actual de la red
- Informe que resume el estado de los componentes de la red y especialmente el estado de los servicios que presentan fallas
 - ✚ Reportes obtenidos durante el análisis
 - ✚ Gráficas que describen el comportamiento de la red
 - ✚ Muestras de tráfico

- ✚ Matriz de hallazgos y recomendaciones de seguridad lógica
- ✚ Conclusiones y recomendaciones

Esta metodología, es parte de la estrategia de desarrollo a seguir para obtener la reorganización, afinamiento y repotencialización de la red.

3.2. ENTREGABLES

El cliente recibirá los siguientes documentos:

- ⊕ Copia de las actas de reunión (si el trabajo lo amerita)
- ⊕ Documento final que incluye:
 - ▶ Análisis y diagnóstico de la red Lan
 - ▶ Caracterización de la red
 - ▶ Gráficas del comportamiento diario de tráfico y del funcionamiento de la red
- ⊕ Análisis de vulnerabilidad en servidores
 - ▶ Matriz de hallazgos
 - ▶ Recomendaciones
 - ✚ Seguridad
 - ✚ Gestión
 - ✚ Eficiencia
 - ✚ Conclusiones
- ⊕ Documento de acciones a tomar
 - ▶ Modelo para lograr los objetivos propuestos
 - ▶ Recomendaciones
 - ✚ Seguridad
 - ✚ Networking
 - ✚ Conectividad

- ✱ Switch
- ✱ Segmentación
- ⊕ Recomendaciones para el manejo de algunas aplicaciones
- ⊖ Correo electrónico, acceso a Internet
 - ▶ Proxy, firewall, detector de intrusos, antivirus, etc.
 - ✱ Seguridad Gráficas y estadísticas del comportamiento de la red.
 - ✱ Matriz de hallazgos y recomendaciones en seguridad de los servidores.

3.3. HERRAMIENTAS UTILIZADAS

Para el desarrollo del análisis y su afinamiento es necesario contar con herramientas especializadas para tal fin, teniendo en cuenta lo anterior **T.S.P.** provee los siguientes equipos:

Equipo con Hardware (tarjetas de red Ethernet / Token Rin) y Software (Herramientas de gestión, análisis de redes y seguridad).

4. SERVICIOS DE VALOR AGREGADO

T.S.P. realizará como servicio adicional al **CLIENTE** y complementario al análisis de la red Lan, un escaneo de vulnerabilidades sobre los servidores del **CLIENTE**.

5. SERVICIOS ADICIONALES

T.S.P. cuenta con personal capacitado en las diferentes áreas de Networking y comunicaciones, con el fin de poder en un futuro apoyar los requerimientos puntuales del **CLIENTE** en forma local y reduciendo los costos del servicio. Así mismo, se pone a disposición todos los servicios adicionales con que cuenta la compañía (Networking, soluciones a partir del uso de software libre, capacitación, gestión de equipos en comunicaciones y auditoria en seguridad lógica).

6. ASPECTOS LOGISTICOS DEL SERVICIO

6.1 RECURSO HUMANO

Por parte de **T.S.P.**

 Un director de proyecto

 Un ingeniero de campo

Por parte del **CLIENTE.**

El personal que sea designado por el **CLIENTE.** Como recomendación y teniendo en cuenta la especialización del proyecto, deben estar presente el Administrador general del Sistema y un Ingeniero de campo que soporte y conozca las aplicaciones que actualmente funcionan.

Los requerimientos necesarios para el desarrollo de este análisis son:

- ✚ Una dirección IP fija dentro del segmento de red Lan a analizar.
- ✚ Un puesto de trabajo con conexión a red (punto físico).
- ✚ Configuración de SNMP sobre los equipos activos a gestionar (Switch, Bridge, router, etc).
- ✚ Creación de password de usuario con opción de ver configuración de los equipos (Switch, Bridge, router, etc).
- ✚ Autorización para el ingreso a los centros de cómputo y de cableado de los sitios a analizar
- ✚ Autorización para la inspección física de todos los sitios en el punto central para la toma de datos del servidor (es) de acuerdo al tráfico manejado.
- ✚ Conexión con salida a Internet.
- ✚ Asignación de horario para mediciones y conexiones críticas en la red (prueba de vulnerabilidades).

6.2 CRONOGRAMA DE ACTIVIDADES

De acuerdo con las actividades mencionadas, se definirá un cronograma en conjunto con el **CLIENTE**, el cual especificará todas las actividades a desarrollar, los intervalos de tiempo que se otorgarán para definir con un tiempo prudencial, posibles desconexiones del sistema, apagado de servidores, etc.

ACTIVIDAD	DESCRIPCION	DIAS									
		1	2	3	4	5	6	7	8	9	10
ANALISIS DE RED LAN											
1	Levantamiento de información										
1,1	Firma acuerdo de confidencialidad										
1,2	Definición de cronograma de actividades										
1,3	Entevista										
1,4	Solicitud de documentación de red										
1,5	Estudio de sitio (disponibilidad recursos)										
2	Recopilacion en tiempo real										
2,1	Instalación de Indicadores de gestión										
2,2	Reconocimiento lógico de la red										
2,3	Recopilación de tráfico en la red										
2,4	Recopilación SNMP										
2,5	Etical Hacking de la intranet										
3	Análisis de la información										
3,1	Comparación de estadísticas										
3,2	Hallazgos y descubrimientos nuevos										
4	Diagnostico de red										
4,1	Presentación de resultados										
5	Evaluación y recomendaciones										
5,1	Informe Final										

**Cronograma típico para la realización de las actividades descritas*

NOTA:

- El cronograma variará de acuerdo a la dimensión de la red a ser analizada.
- El número de servidores a analizar, depende del tamaño de la red (2% de la red). Servidor adicional se cotizará aparte.

6.3 SERVICIOS COMPLEMENTARIOS

Así mismo, a partir de estas pautas del servicio se pueden ofrecer estudios en casos particulares como:

- ✚ Análisis para el diagnostico de problemas.
- ✚ Detección de fallas puntuales a nivel Lan o Wan.
- ✚ Caracterización de aplicaciones (consumo de canal).