Uno de los pilares básicos en el desarrollo y expansión de la auditoría en redes telemáticas ha sido la concienciación en los riesgos intrínsecos de las actividades informáticas y telemáticas junto con la necesidad de garantizar las inversiones realizadas por parte de las organizaciones empresariales y gubernamentales en las materias de TIC (Tecnologías de la Información y Comunicación).

AUDITORÍAS EN REDES TELEMÁTICAS

Enrique de Miguel Ambite.
Ingeniero de Núcleo de Red en Telefónica Móviles España

Se puede definir la auditoría en redes telemáticas como el conjunto de técnicas y procedimientos de gestión, destinados al análisis y control de los sistemas que componen dicha red. Los sistemas que forman parte de una red telemática son básicamente: nodos de red —subdivididos en nodos de acceso, nodos del núcleo y nodos de servicios—, sistemas operativos y software básico, metodologías y lenguajes para el desarrollo software, software de uso específico y sistemas de información (nodos de almacenamiento masivo y bases de datos).

En muchas ocasiones, los beneficios de una entidad empresarial no son susceptibles de incremento mediante el aumento de ingresos, sino por la reducción de los costes

El objetivo fundamental de una auditoría es la obtención de un juicio objetivo, independiente y desinteresado. En el caso concreto de la auditoría de redes telemáticas es preciso el conocimiento detallado y preciso de las necesidades de la empresa u organización cubiertas por la red objeto de auditoría.

La seguridad en el procesamiento de la información, comunicaciones en redes de área local (LAN) y en redes de área extensa (WAN) y en la transmisión de datos, es una premisa imprescindible en la mayoría de las entidades, que avala las inversiones realizadas de recursos tanto humanos como materiales. En muchas ocasiones, los beneficios de una entidad empresarial no son susceptibles de incremento mediante el aumento de ingresos, sino por la reducción de los costes. Y es precisamente en este aspecto donde la auditoría actúa como elemento sinérgico del sistema de control interno de la entidad. En la actualidad no es concebible el desarrollo de la gestión empresarial sin la existencia de los procedimientos y las herramientas de control correspondientes. En multitud de empresas y organismos, la auditoría convencional referida a aspectos económicos-financieros está siendo acompañada y en cierto modo, complementada por una auditoría en las redes telemáticas. No mucho tiempo atrás, una empresa con una organización ejemplar en cuanto a división y competencias podía estar cometiendo errores inadvertidos en su sector de comunicaciones e informático, proporcionando debilidades a corto y medio plazo extensibles al resto de los ámbitos de la empresa, mediante un *efecto mariposa* o *efecto dominó.*

COMPONENTES DE UNA AUDITORÍA DE RED TELEMÁTICA

Con las actividades de análisis y síntesis que supone una auditoría de red telemática, la empresa u organismo comprobará el estado de su instalación de red, desde los niveles más bajos (componentes electrónicos, lógica digital y sistemas microprogramados) hasta los protocolos empleados por las aplicaciones de usuario de mayor nivel en la arquitectura de red.

La arquitectura de la red telemática se define por la visión de cada uno de los esquemas de cada parte:

• Físico, desde el punto de vista del hardware, mostrando la topología o distribución física de las máquinas que componen la red.

• Lógico, desde la perspectiva de la distribución de los servicios prestados por cada nodo de la red, la clasificación de los distintos tipos de tráfico, la estructura lógica de la red (división en subredes, VLANs, etc.)

• Administrativo, desde la percepción en posesión de los recursos humanos encargados de las tareas relacionadas con la gestión, administración y mantenimiento de la red.

BENEFICIOS DE LAS AUDITORÍAS EN REDES TELEMÁTICAS

• Ayuda a adecuar la disponibilidad y el rendimiento de la red a las necesidades de la empresa.

• Proporciona información que maximiza el retorno de las inversiones o payback en redes telemáticas y TIC (Tecnologías de la Información y Comunicación) de la empresa.

• Aumenta la estabilidad y fiabilidad de la red.

• Reduce el riesgo potencial de las nuevas implantaciones y actualizaciones en la red, tanto en el entorno estrictamente tecnológico como en los procesos empleados.

• Aumenta la satisfacción de los clientes al alcanzar mayores cotas de rendimiento y disponibilidad de la red. Entendiendo el concepto de cliente, en su definición más amplia, que abarca al *cliente interno*, los usuarios directos de la red (empleados de la entidad u organización) —y al *cliente externo*, aquel que solicita un servicio telemático y es la fuente principal de ingresos.

¿CUÁLES SON LOS CONCEPTOS CLAVES EN LA AUDITORÍA DE UNA RED TELEMÁTICA?

Finalidad y utilidad. Estos dos conceptos serán el referente para diferenciar los distintos tipos de auditoría que se pueden plantear en una red telemática.

TIPOS DE AUDITORÍAS DE REDES TELEMÁTICAS

Existen diversos tipos de auditorías de redes debido fundamentalmente al grado de escalabilidad y personalización obtenidos. De forma sintética, se puede hablar de tres tipos básicos de auditorías en redes, que pueden ser complementadas mediante auditorías *ad-hoc*.

Auditoría de la Arquitectura de Redes

La *finalidad* principal de este tipo de auditoría es la obtención de un mapa básico de topología de red como punto de partida del diseño del entorno de red en su conjunto. Por otro lado, la *utilidad* de este tipo de auditorías es la generación de recomendaciones para las áreas susceptibles de cambio y/o actualización de la empresa u organización, evitando los puntos potenciales de criticidad y fallo en la red auditada.

La primera fase de una auditoría de la arquitectura de redes es la *recopilación de información* sobre necesidades empresariales o corporativistas y de datos técnicos sobre los equipos de red activos. Mediante un proceso específico de entrevistas al equipo de recursos humanos dedicado a la gestión-administración, provisión y mantenimiento de la red, se identifican las necesidades empresariales relacionadas con la red. Además, se recolecta la información pertinente sobre los procesos aplicativos que se ejecutan en la red y los planes de crecimiento futuro. Para la recogida de datos técnicos sobre los equipos activos de la red, se utilizan herramientas software y hardware de red seguras.

La utilidad de esta auditoría se desglosa en el informe que incluye la siguiente información:

• Un listado de los equipos activos en la red WAN/LAN.

• Un mapa de la topología de red física.

• Un resumen analítico de ingeniería donde se destacan los puntos potenciales de fallo y/o mejora de la red telemática auditada.

Auditoría de Rendimiento de Redes

La *finalidad* principal de este tipo de auditoría es proporcionar datos del rendimiento, siendo la *utilidad* de la misma la generación de recomendaciones en forma de informes que ayuden a determinar las mejoras que precisa la red telemática para garantizar las necesidades de los usuarios de los aplicativos, tanto en el presente como en el futuro. Se debe contar con un mapa de la topología de red, como punto de partida para la primera de las fases de este tipo de auditoría, *el análisis del rendimiento.* Como resultado, se obtendrá principalmente una solución ERP (Enterprise Resource Planning o Planificación de Recursos Empresariales). Un *ERP* es un software de gestión integral de empresa cuyas características fundamentales son:

• Resuelve todas las necesidades de flujos de información dentro de la organización.

• La aplicación posee naturaleza estándar, con la disponibilidad de un entorno propio de desarrollo a disposición de la empresa, facilitando las adaptaciones necesarias en el sistema de gestión para responder a los cambios de su entorno.

La siguiente fase de la auditoría, es la *Evaluación de planes de crecimiento futuro de la red* y/o planes de cambios necesarios en el entorno de aplicaciones críticas de la empresa. A continuación, se elige el momento más adecuado para realizar *la recopilación de datos del rendimiento de la red*, mediante la implantación de herramientas que recojan datos de rendimiento de la red a través de los siguientes *ítems:*

• Uso comparativo.

• Salud de la red en aspectos globales.

• Análisis de errores.

• Determinación de los diez principales emisores de tráfico en la red.

• Determinación de los diez principales receptores de tráfico en la red.

• Distribución y uso de los protocolos de comunicaciones.

Finalmente, se realiza el informe ad-hoc a la red auditada, donde se incluye un resumen para la dirección de la empresa u organización, describiendo los resultados de la auditoría de rendimiento y ofreciendo las recomendaciones oportunas de toma de decisiones. Complementariamente, se adjunta el informe resumido de ingeniería que interpreta los datos de rendimiento y proporciona un resumen de referencia del rendimiento del entorno de red en su conjunto, las recomendaciones para mejorar el rendimiento actual en base a las necesidades empresariales, las recomendaciones para prever el crecimiento futuro de la red, datos indicadores de problemas potenciales afectando al tiempo de retorno y tiempo de respuesta de los procesos y un apéndice con todos los datos del rendimiento en formato gráfico. De forma opcional, se suele fijar una reunión-presentación con el equipo directivo, para ofrecer una presentación interactiva de observaciones y recomendaciones relativas al rendimiento del entorno en relación a las necesidades empresariales.

El objetivo fundamental de una auditoría es la obtención de un juicio objetivo, independiente y desinteresado

Auditoría de la Disponibilidad de Redes

La finalidad de esta auditoría es la comprensión profunda de los requerimientos para alcanzar y mantener la disponibilidad y fiabilidad de la red telemática que la empresa u organización precisa. El desarrollo de este tipo de auditoría se basa en una serie de entrevistas a miembros clave de la plantilla de la empresa u organización en sus propias dependencias, que versan sobre los siguientes aspectos:

• Planificación de servicios: objetivos de alta disponibilidad, gestión de niveles y acuerdos de servicios (SLA, Service Level Agreement), aplicaciones y sistemas críticos de la red.

• Estructura de la organización: personal encargado de la red, necesidades de formación y conocimientos específicos, funciones, dependencias y responsabilidades.

• Relaciones con el proveedor: comunicaciones, contratos de soporte y tipos de soporte (presencial, remoto, 24x7, etc.)

• Gestión de cambios: traslados, incorporaciones y cambios; verificación previas de la red antes de actualizar la red y procedimientos de actualización de software.

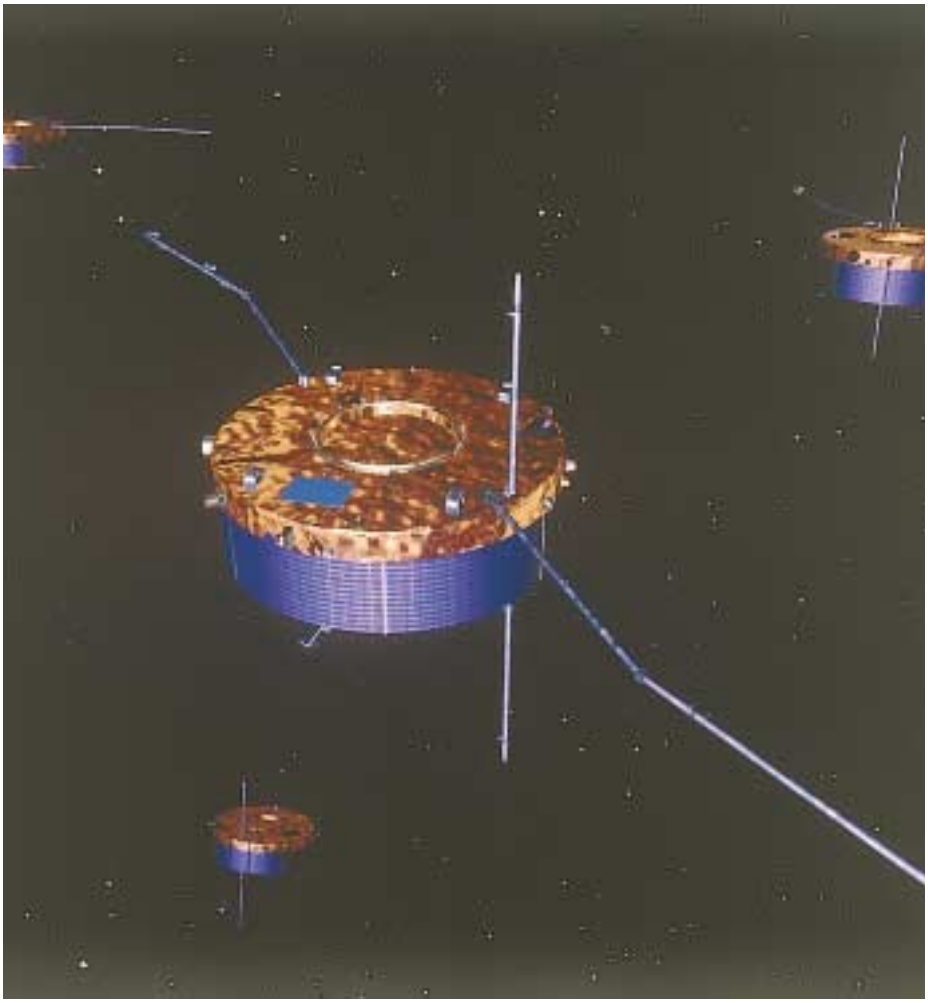
• Gestión de fallos e incidencias: procedimientos de control de incidencias en el servicio, procedimientos de escalado técnico, procedimientos de escalado gerencial, procedimientos de seguimiento y análisis, prevención y estrategias de aislamiento de fallos en la red.

• Entorno físico: seguridad física, consideraciones ambientales, estrategia de cableado estructural y etiquetado, accesos a los emplazamientos a mantenedores y suministradores.

• Planificación de contingencias: copias de seguridad y respaldo, recuperación proactivas y reactivas de la información.

• Seguridad: revisión de reglas en firewalls, políticas y procedimientos, acceso remoto, autentificación de métodos y políticas de intranet y extranet.

Para concluir, se planifica una presentación con el personal directivo y



con personal clave encargado de la red, donde se realiza una comparación entre los objetivos empresariales con estrategias de operaciones TIC y sus planes de implantación, indicando las vulnerabilidades y debilidades en la disponibilidad de la red, obstáculos y factores críticos.

HERRAMIENTAS SOFTWARE UTILIZADAS

Las principales herramientas de software libre empleadas en las auditorías de redes telemáticas son las siguientes:

1. Para el análisis de red:

• *Scotty:* herramienta de monitorización de agentes que incluye capacidades de gestión de dispositivos SNMP. Está implementado en Tcl/Tk con extensiones propias, e incluye un navegador de MIBs.

• *Tcpdump:* herramienta de adquisición y análisis de tráfico. Es una fuente de la librería Libpcap.

• *Ethereal:* herramienta de adquisición y análisis de tráfico con un entorno gráfico de alto nivel. Se pueden realizar distintos tipos de filtrado de la información capturada.

• *Mrtg:* herramienta con interfaz WWW que permite una lectura en tiempo real de estadísticas de distintos elementos, entre otros, dispositivos SNMP. Es una de las herramientas más conocidas para monitorización de tráfico, y una de las más extendidas.

• *Cheops:* herramienta sustitutiva de *scotty* para la gestión de elementos de red, todavía no incluye soporte de SNMP pero es tremendamente gráfica e intuitiva.

• *Mon:* se trata de una herramienta integrada para la gestión de red, soportando múltiples sistemas en los que, a través de agentes, se pueden monitorizar las aplicaciones de éstos y su rendimiento. Tiene soporte de SNMP y ofrece la posibilidad de definir muchos niveles de alertas, desde correo electrónico a notificaciones con voz en tiempo real.

• *Iptraf:* es un monitor de red a nivel IP. Permite la obtención del ancho de banda consumido, monitorizar todas las conexiones relativas a una máquina, comprobación de *checksums errors* y detectar ciertas operaciones no permitidas por parte de los usuarios.

2. Para la realización de gráficos y esquemas:

• *Tkined:* es la interfaz gráfica de la herramienta *scotty.*

• *ArgoUML:* software que facilita la comunicación entre desarrolladores, clientes, analistas y demás personas que intervienen en un proyecto utilizando un lenguaje gráfico denominado UML. En el caso de esta utilidad de modelado, el escogido ha sido Java.

• *Xfig:* herramienta de dibujo vectorial en 2D.

Aumenta la satisfacción de los clientes al alcanzar mayores cotas de rendimiento y disponibilidad de la red