



UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

**AUDITORÍA DE LA RED INFORMÁTICA DE LA UNIVERSIDAD
DE QUINTANA ROO: VALORAR LOS PROCESOS, SERVICIOS Y
NIVELES DE SEGURIDAD DE LOS SERVIDORES Y
PRINCIPALES DISPOSITIVOS DE COMUNICACIONES**

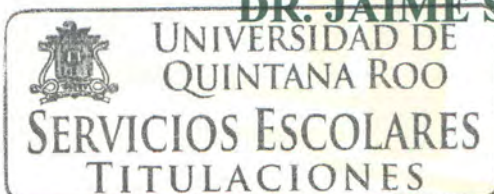
**TESIS
PARA OBTENER EL GRADO DE
INGENIERA EN REDES**

**PRESENTA
KARLIBETH ELIODORO HERNÁNDEZ**



**DIRECTOR DE TESIS
MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE**

**ASESORES
MTI VLADIMIR VENIAMIN CABAÑAS VICTORIA
LIC. LUIS FERNANDO MIS RAMÍREZ
MSI. LAURA YÉSICA DÁVALOS CASTILLA
DR. JAIME SILVERIO ORTEGÓN AGUILAR**



CHETUMAL QUINTANA ROO, MÉXICO, MARZO DE 2015



UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

**TRABAJO DE TESIS ELABORADO BAJO SUPERVISIÓN DEL
COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO
PARCIAL PARA OBTENER EL GRADO DE:**

INGENIERA EN REDES

COMITÉ DE TRABAJO DE TESIS



DIRECTOR:

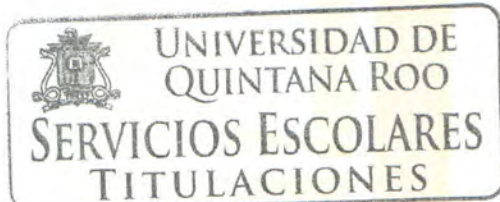

MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

ASESOR:


MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESOR:


LIC. LUIS FERNANDO MIS RAMÍREZ



CHETUMAL, QUINTANA ROO, MÉXICO

Agradecimientos

Este proyecto de tesis es la culminación de un anhelo que no hubiera podido realizar sin la ayuda del ser más poderoso del Universo y el que me dio la oportunidad de nacer y existir: Dios, Él ha estado en cada éxito y derrota y sin duda me ha permitido tener la bendición de culminar con mi carrera.

A mi mamá Elizabeth Hernández Muñoz, por ser la mujer más inteligente, fuerte y trabajadora, por apoyarme y cuidarme desde que nací, y por no dejarme sola nunca.

A mi papá Carlos Daniel Eliodoro Dzib porque durante todos estos años tuve su completo apoyo, ayuda y comprensión, y sin duda ha sido un ejemplo de vida profesional.

A mi papá José Un Itzincab por cuidarme y ayudarme prácticamente desde niña.

A mi hermana Esther por sus consejos y ayuda cuando más lo necesite, a mi niña Paulette y a mis abuelitos Rosa y Gaspar, por enseñarme, cuidarme y darme tanto amor, y porque aún lo siguen haciendo.

Y Finalmente, pero no menos importante al Maestro Rubén Gonzalez Elixavide, ya que con sus enseñanzas y consejos, me hizo ser una mejor alumna, persona y ahora una profesionalista.

Dedicatoria

Este trabajo está dedicado a Dios, a mis padres Elizabeth Hernández y Carlos Eliodoro, y a mi motor de vida a Carlos R. Ojeda Eliodoro.

“Porque Jehová da la sabiduría, y de su boca viene el conocimiento y la inteligencia”
Proverbios 2:6.

Resumen

La Universidad de Quintana Roo -UQROO, es la principal universidad pública del Estado de Quintana Roo, conformada por las unidades académicas en Chetumal, Cozumel y Playa del Carmen. La Universidad ha crecido y con ello ha requerido de una mayor infraestructura informática que dé soporte a los servicios que brinda a sus usuarios. El Departamento de Cómputo y Telemática –DCT de la Universidad ha sido el encargado de la administración de esta infraestructura informática y gestión de distintos servicios para las áreas académicas, de investigación y administrativas:

- Servicios de comunicación y colaboración
- Desarrollo Web
- Videoconferencias
- Redes y telecomunicaciones
- Soporte técnico
- Coordinación¹.

Con la necesidad de incorporar mejoras o resolver puntos críticos, es importante conocer previamente el estado actual de la red, sobre todo en el ámbito de administración, control, calidad y seguridad.

Esta supervisión o revisión de la arquitectura de red, requiere de la aplicación de una Auditoría que permita obtener un Informe actual de los componentes y comportamiento de la red, ya que los cambios que ocurren con el tiempo influirán en el rendimiento y la seguridad de la misma.

Esta Auditoría de red implica la revisión específica y especializada que se realiza al sistema de red considerando en la evaluación el tipo de redes, arquitectura, topología, protocolos de comunicación, conexiones, accesos, privilegios,

¹ <http://ti.uqroo.mx/organizacion/>

administración y demás aspectos que repercuten en instalación, administración, funcionamiento, y aprovechamiento de la misma.

Para hacer posible una auditoría de red, es necesario la utilización de metodologías, herramientas, técnicas de recopilación y sobre de todo, el uso de buenas prácticas con las que se obtenga un marco referencial para futuras mejoras o simplemente el buen uso y aprovechamiento de los recursos de red. Para esto existen modelos de referencia que permiten la planificación de una Auditoría tales como ITIL y COBIT, que plantean los procesos de control empleados al momento de evaluar las TIC².

² TIC, Tecnologías de la Información y la Comunicación. Son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Fuente: <http://www.serviciostic.com/las-tic/definicion-de-tic.html>

Tabla de contenido

CAPÍTULO I Introducción	1
1.1 Introducción	2
1.2 Justificación	4
1.3 Objetivo	5
1.4 Alcance	6
1.5 Metodología	7
CAPÍTULO II Marco Contextual.....	8
2.1 Marco Contextual.....	9
CAPÍTULO III Marco Conceptual.....	10
3.1 Marco Conceptual.....	11
3.1.1 Concepto General de Auditoría.....	11
3.1.2 Concepto de Redes de datos.....	13
3.1.3 Diseño de Redes de datos	18
3.1.4 Auditoría de Redes	35
3.1.5 Legislación, mejores prácticas y técnicas de Auditoría Informática	39
CAPÍTULO IV Metodología Propuesta	46
4.1 Metodología para la Auditoría de Red	47
CAPÍTULO V Desarrollo.....	56
5.1 Introducción	57
5.2 Desarrollo de la Auditoría de Red	58
5.2.1 Planeación de Auditoría	58
5.2.2 Ejecución de la Auditoría.....	64
5.2.3 Dictamen de la Auditoría.....	85
Resultados obtenidos y recomendaciones	86
Resultados obtenidos.....	87
Recomendaciones	94
Conclusiones	96
Conclusiones	97
Trabajos a futuro	100
Anexos.....	101
Anexo A:	102
Instalación de Axence netTools.....	102

Anexo B:	109
Instalación y configuración de OpManager	109
Anexo C:	118
Instalación y configuración de WhatsUp Gold	118
Anexo D:	127
Informe Final	127
Presentación.....	128
Formato de Situaciones Encontradas - Relevantes.....	129
Bibliografía	130
Bibliografía	131

Índice de Figuras

Figura 1 Diseño topología Bus o Lineal	16
Figura 2 Diseño topología estrella.....	16
Figura 3 Topología de anillo	17
Figura 4 Topología de malla	17
Figura 5 Topología de árbol.....	18
Figura 6 Cubo de COBIT. Fuente OGC	43
Figura 7 Marco de COBIT. Fuente OGC	43
Figura 8 Evolución de COBIT. Fuente OGC.....	44
Figura 9 Auditoría de Red. Metodología Propuesta con base en COBIT e ITIL	48
Figura 10 Cubo de COBIT para la Auditoría de Red.....	51
Figura 12 Diagrama Físico de Red UQROO Chetumal	66
Figura 13 Diagrama Lógico de Red UQROO Chetumal.....	70
Figura 14 Inventario de Switches	71
Figura 15 Inventario de Access Point	71
Figura 16 Creación de grupos de dispositivos. WhatsUp Gold	72
Figura 17 Adición de dispositivos WhatsUp Gold	72
Figura 18 Monitoreo de rendimiento de dispositivos.....	73
Figura 19 Top 10. Consumo de memoria en dispositivos de red.....	74
Figura 20 Top 10. Consumo de CPU en dispositivos de red.....	74
Figura 21 Top 10. Capacidad de disco en dispositivos de red.....	75
Figura 22 Top 10, Protocolos en el campus Chetumal.....	76
Figura 23 Top 10 Usuarios-Uso del Protocolo HTTPS.....	77
Figura 24 Reglas QoS en campus Chetumal	78
Figura 25 Consumo de Ancho de banda	79
Figura 26 Monitoreo de Servidores en NetCrunch	80
Figura 27 Ventana de detalles de monitoreo de Servidores.....	80
Figura 28 Servicios de red en Servidores	81
Figura 29 Flujo de tráfico en interfaces de Servidor	81
Figura 30 Consumo de ancho de banda en Servidores.....	82
Figura 31 Gráfica de Consumo de ancho de banda en servidores.....	82
Figura 32 Servicios más solicitados	83
Figura 33 Servicios por tiempo de respuesta.....	83
Figura 34 Rendimiento de Sistema -Switches	88
Figura 35 Uso de disco-Servidores	89
Figura 36 Utilización de CPU-Servidores.....	89
Figura 37 Uso de Memoria-Servidores.....	90
Figura 38 Protocolos de red más consumidos	91
Figura 39 Medición de ancho de banda.....	92
Figura 40 Top 10. Reglas QoS en la UQROO.....	93
Figura 41 Top 10. Reglas QoS en la UQROO_2.....	94
Figura 42 Instalación de netTools_Selección de Idioma	103
Figura 43 Instalación de netTools. Asistente	104
Figura 44 Instalación de netTools. Licencia.....	104

Figura 45 Instalación de netTools. Carpeta de destino.....	105
Figura 46 Instalación de netTools. Acceso directo.....	105
Figura 47 Instalación de netTools. Icono en Escritorio	106
Figura 48 Instalación de netTools. Finalización.....	106
Figura 49 Instalación de netTools. Aviso.....	107
Figura 50 Entorno gráfico de netTools.....	108
Figura 51 Descarga de OpManager.....	110
Figura 52 Instalación de OpManager. Bienvenida	110
Figura 53 Instalación de OpManager. Licencia	111
Figura 54 Instalación de OpManager. Tipo Instalación.....	111
Figura 55 Instalación de OpManager. Lenguaje.....	112
Figura 56 Instalación de OpManager. Selección de Carpeta	112
Figura 57 Instalación de OpManager. Windows NT Service	113
Figura 58 Instalación de OpManager. Accesorios.....	113
Figura 59 Instalación de OpManager. Puerto	114
Figura 60 Instalación de OpManager. Registro Opcional.....	114
Figura 61 Instalación de OpManager. Finalización	115
Figura 62 Instalación de OpManager. Tipo de Servidor.....	115
Figura 63 Instalación de OpManager. Base de datos.....	116
Figura 64 Instalación de OpManager. Inicio de aplicación	116
Figura 65 OpManager. Adición de red	117
Figura 66 OpManager. Adición de red Servidores	117
Figura 67 Inicio de la instalación.	120
Figura 68 Términos y Condiciones.	120
Figura 69 Requerimientos de sistema.....	121
Figura 70 Instalación de SQL.	121
Figura 71 Ruta de Instalación.....	122
Figura 72 Ingreso de Contraseña de Súper Usuario.....	123
Figura 73 Ingreso de Nombre de la Base de Datos.	124
Figura 74 Dirección IP del servidor.....	124
Figura 75 Selección de carpeta contenedora.....	125
Figura 76 Asignación de Puerto de Interfaz Web.....	125
Figura 77 Resumen de Instalación.	126

Índice de tablas

Tabla 1 Normas a utilizar en la Auditoría de red.....	53
Tabla 4 Formato Guía de Evaluación.....	54
Tabla 5 Formato de Inventario.....	55
Tabla 6 Plan de Auditoría	60
Tabla 7 Guía de Evaluación	63
Tabla 9 Adición de Switches a la red UQROO	90
Tabla 10 Adición de APs a la red UQROO.....	91
Tabla 11 Adición de Servidores a la red UQROO.....	91

CAPÍTULO I Introducción

1.1 Introducción

La infraestructura de las Tecnologías de la Información y de las Comunicaciones (TIC), se ha convertido en un activo importante de toda organización, en especial de las Instituciones de Educación Superior donde la red constituye su núcleo. Las redes de comunicaciones, son el sistema a través del cual fluye la información más importante y se da soporte a los servicios³ proporcionados al usuario. Los sistemas que forman parte de una red, son básicamente: sistemas operativos y software básico, software de uso específico y sistemas de información (nodos⁴ de almacenamiento masivo y base de datos) por el lado de la infraestructura física, los componentes son; computadoras, switches⁵, routers⁶, APs⁷, etc.

Muchas empresas, actualmente realizan auditorías de red para verificar el estado de la red y sus componentes, lo anterior con el fin de minimizar el impacto de los cambios, y también para asegurarse de que la red esté estable y segura.

La Dirección de Informática de la Universidad de Quintana Roo, es el área responsable de mantener el correcto funcionamiento de las redes de telecomunicaciones en la Universidad. Ha sido la encargada de la administración de esta infraestructura informática y gestión de distintos servicios.

Tiene la responsabilidad de estar a la vanguardia en las tecnologías de información y telecomunicaciones, para brindar un servicio acorde a las crecientes necesidades de la comunidad universitaria. Con todo esto, es de vital importancia que se evalúen constante y regularmente el estado y funcionamiento de los equipos principales que

³ Servicios de Red. Configuración en una red a través de los dispositivos de comunicación para poder compartir información y recursos. Fuente: <http://xml.cie.unam.mx/xml/Linux/seguridad-2.html>

⁴ Nodo de red: punto de conexión, capaz de crear, recibir o repetir mensajes. Fuente: (Pfaffenberger, 1999)

⁵ Switch. Dispositivo de red encargado del direccionamiento e interconexión de segmentos de red. Opera en la capa de Enlace del modelo OSI. Fuente: <http://definicion.de/switch/>

⁶ Router. Dispositivo de red que se encarga de interconectar redes. Utiliza protocolos de enrutamiento para comunicarse con otros router para saber la ruta más rápida y adecuada para el envío de datos. Opera en la capa de red del modelo OSI. Fuente: <http://www.definicionabc.com/tecnologia/router.php>

⁷ AP. Access Point. Dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. También puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

dan comunicación a todo el campus Chetumal. Con la realización de una Auditoría, se pretende realizar una evaluación de servidores y principales dispositivos de comunicación, esto mediante una metodología basada en buenas prácticas, evaluando y valorando a través de: inventarios, topologías⁸, análisis de protocolos⁹, servicios, rendimiento y seguridad. Todo con el propósito de elaborar un dictamen final que permita brindar un diagnóstico de la red.

⁸ Topología de red. Disposición geométrica de los nodos y los enlaces de cables en una red de área local: Fuente: (Pfaffenberger, 1999)

⁹ Protocolos. Conjunto de reglas para el intercambio de información entre nodos y dispositivos de red. Fuente: <http://definicion.de/protocolo-de-red/>

1.2 Justificación

La red de datos universitaria, se encuentra en constante evolución y crecimiento, tanto en el número de usuarios como en los servicios que soporta. Como parte de la mejora continua, la infraestructura¹⁰ informática debe de ser evaluada de acuerdo a metodologías y estándares internacionales, buscando la calidad en los servicios hacia el usuario final.

La red universitaria ha presentado altibajos en su funcionamiento, por lo que requiere un análisis detallado con resultados que le permita una mejor toma de decisiones en las áreas:

- Planeación
- Seguridad
- Desarrollo
- Integración
- Implementación
- Adopción de nuevas tecnologías
- Escalabilidad de infraestructura y de servicios
- Capacitación
- Procesos administrativos y de gestión

¹⁰ Infraestructura de red. Conjunto de elementos y servicios que posibilita la transmisión de información a través del intercambio de datos en una red informática. Fuente: <http://definicion.de/red-de-datos/>

1.3 Objetivo

General:

Valorar los procesos¹¹, servicios, rendimiento y niveles de seguridad¹² en los servidores y los principales dispositivos de comunicación de la Universidad de Quintana Roo, en el campus Chetumal.

Específicos:

- Determinar los principales dispositivos de comunicaciones a auditar
- Determinar los principales servidores de comunicaciones a auditar
- Realizar un diseño físico de la infraestructura de la red universitaria
- Realizar un diseño lógico de la infraestructura de la red universitaria
- Caracterizar el flujo del tráfico de la red
- Generar un inventario de los principales dispositivos de comunicaciones y servidores existentes
- Generar un reporte del flujo de tráfico en la red
- Generar un reporte de los protocolos activos en la red
- Evaluar los servicios críticos en servidores

¹¹ Procesos. Un proceso es una secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico. Fuente: <http://definicion.mx/proceso/#ixzz3Q8kepdhH>

¹² Niveles de seguridad. Grado de "sensibilidad" que existe en la transmisión de información a través de la red mediante los servidores.

1.4 Alcance

La auditoría de la red del campus Chetumal, permitiría mejorar la toma de decisiones en la creación de políticas de implementación de nuevos dispositivos, procesos y servicios, lo que repercutiría en la mejora de la calidad del servicio brindado.

Los resultados esperados del proyecto son:

- Diseño físico de la infraestructura de la red universitaria
- Diseño lógico de la infraestructura de la red universitaria
- Caracterizar el flujo del tráfico de la red,
- Generar un reporte de los protocolos activos en la red.
- Inventario físico y lógico de los dispositivos de comunicaciones
- Inventario de los servidores existentes.
- Valoración de los procesos de seguridad, gestión y de servicios.

Una vez finalizado este proyecto, serviría de línea base para el análisis de los demás campus, e incluso de cualquier dependencia que cuente con un sistema de red.

1.5 Metodología

Tipo de Investigación

- Exploratoria

Para obtener información estadística de la red, se utilizó software de monitoreo, que permitió examinar los datos y obtener información de importancia para el análisis de la red.

- Cuantitativa

Con la obtención de datos a través del monitoreo de la red universitaria, se pudieron obtener modelos estadísticos y porcentuales, como cantidades definidas de dispositivos o el aprovechamiento de la red en cuanto a consumo de paquetes.

Método de investigación

- Método empírico

Objeto de estudio e investigación

- Red Informática de la Universidad de Quintana Roo, campus Chetumal.

Herramientas utilizadas

- Referencias bibliográficas
- Referencias electrónicas
- Software de Monitoreo:

CAPÍTULO II Marco Contextual

2.1 Marco Contextual

La Universidad de Quintana Roo, es el centro académico en su tipo más joven del país. Su creación responde a un viejo anhelo de los Quintanarroenses de contar con un centro de educación superior para formar profesionales en las áreas sociales, las humanidades, las ciencias básicas y las áreas tecnológicas de mayor demanda y consumo en esta época de alta competitividad.¹³

Debido a que es una de las principales universidades del estado, se ha requerido de una infraestructura informática de red que proporcione los servicios y atención necesaria hacia sus alumnos, docentes y administrativos. Esta infraestructura, está basada en redes de fibra óptica e inalámbrica, dando servicio de voz datos y video tanto al campus Chetumal como a los demás campus.

Debido al creciente aumento tanto en campus, como en usuarios es necesario tener un control de los elementos que componen esta infraestructura de red, en los ámbitos físico y lógico. Una revisión exhaustiva de los dispositivos de red principales, permitirá no sólo obtener datos cuantitativos sino que ofrece a los administradores una serie de información relevante para el mantenimiento y soporte de la misma, y así contar con herramientas que ofrezcan mejoras y soluciones a los posibles problemas que surgen actualmente y a futuro. Una auditoría a la red universitaria, implicará la evaluación del tipo de red, arquitectura, topología, protocolos de comunicación, conexiones, accesos, privilegios, administración y demás aspectos que repercuten en instalación, administración, funcionamiento, y aprovechamiento de la misma, y sobre todo en la seguridad que brinde a todos los campus interconectados.

De esta manera se pretende que al auditar la red universitaria mediante metodologías aceptadas internacionalmente, se tenga un mejor entendimiento del estado de la red y el mejoramiento que se le puede dar a los servicios que esta proporciona.

¹³ <http://www.uqroo.mx/nuestra-universidad/identidad-universitaria/historia/>

CAPÍTULO III Marco Conceptual

3.1 Marco Conceptual

3.1.1 Concepto General de Auditoría

Conforme se expandía el comercio en el mundo y aumentaban las operaciones los comerciantes tuvieron la necesidad de establecer mecanismos de registro que les permitieran administrar las actividades mercantiles que realizaban. A la par de estos cambios fue necesario que alguien evaluara que estos registros y resultados fueran correctos, entonces se requirió también de alguien que verificara la veracidad y confiabilidad de esas operaciones. Fue en ese momento que nació el acto de auditar. En un principio se consideró a la auditoría una herramienta específica de la contaduría pública, pero posteriormente se aplicó a otros campos. A pesar de abarcar más espacios, la auditoría se sigue basando en los mismos principios y fundamentos teóricos y prácticos que la rigen como profesión. (Razo, 2002)

Una Auditoría, es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre sus resultados y el cumplimiento de sus operaciones. (Razo, 2002)

1.1 Tipos de Auditoría

- Auditoría por su lugar de aplicación
 - Auditoría externa
 - Auditoría interna

- Auditoría por su área de aplicación
 - Auditoría financiera
 - Auditoría administrativa
 - Auditoría operacional
 - Auditoría integral
 - Auditoría gubernamental

- Auditoría de sistemas (informática)
- Auditoría especializada (Áreas específicas)
 - Auditoría al área médica (evaluación médico-sanitaria)
 - Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
 - Auditoría fiscal
 - Auditoría laboral
 - Auditoría de proyectos de inversión
 - Auditoría a la caja chica o caja mayor (arqueos)
 - Auditoría al manejo de mercancías (inventarios)
 - Auditoría ambiental
 - Auditoría de sistemas
- Auditoría de sistemas computacionales
 - Auditoría informática
 - Auditoría con la computadora
 - Auditoría sin la computadora
 - Auditoría a la gestión informática
 - Auditoría al sistema de cómputo
 - Auditoría alrededor de la computadora
 - Auditoría de la seguridad de sistemas computacionales
 - Auditoría a los sistemas de redes
 - Auditoría integral a los centros de cómputo
 - Auditoría ISO-9000¹⁴ a los sistemas computacionales
 - Auditoría Outsourcing¹⁵
 - Auditoría ergonómica de sistemas computacionales

¹⁴ ISO 9000 es un conjunto de normas sobre calidad y gestión de calidad, establecidas por la Organización Internacional de Normalización (ISO). Fuente: (Pfaffenberger, 1999)

¹⁵ Prestación de servicios, proveedores, soporte y mantenimiento que una empresa brinda a otra en el ámbito de las TIC. Fuente: <http://www.estudiogambier.com.ar/outsourc.html>

3.1.2 Concepto de Redes de datos

Se denomina red de datos, a toda aquella infraestructura tecnológica, que se ha diseñado específicamente para la transmisión de información mediante el intercambio de datos entre dispositivos.

El objetivo de la creación de una red de datos es:

- Compartir recursos, equipos, información y programas que se encuentran localmente o dispersos geográficamente.
- Brindar confiabilidad a la información, disponiendo de alternativas de almacenamiento.
- Obtener una buena relación costo / beneficio
- Transmitir información entre usuarios distantes de la manera más rápida y eficiente posible

Las redes de datos, generalmente se clasifican de acuerdo a la tecnología de conmutación utilizada, tamaño, topología, tecnología de transmisión, transferencia de datos, medio de transmisión y método de acceso al medio. Para cuestiones meramente informativas sólo se desarrollaran los conceptos de las primeras tres clasificaciones: tecnología de conmutación, tamaño y topología. (Andreu, 2011).

2.1 Redes por tipo de Tecnología

Redes conmutadas¹⁶ y no conmutadas

Una red conmutada es un conjunto de nodos interconectados entre sí, a través de medios de transmisión, los cuales realizan una petición de enlace para el envío de datos.

En las redes no conmutadas, los enlaces entre nodos se administran de manera exclusiva, es decir, hay una ruta permanente para el envío de datos de un lado a

¹⁶ Conmutación. Conexión que realizan los diferentes nodos que existen en distintos lugares para lograr conectar a dos usuarios de una red de telecomunicaciones. Fuente: (Herrera, 2003)

otro. Este tipo de enlace es de gran utilidad para usuarios que no pueden aceptar retrasos, o que necesitan enviar/recibir grandes cantidades de información.

Redes de datos con conmutación de circuitos

La conmutación de circuitos, se origina cuando se establece una conexión dedicada entre nodos, durante un tiempo determinado llamado sesión. Las ventajas se notan principalmente en el envío de voz video, ya que asegura la QoS, además de un mínimo retardo y pérdida de información. Por otro, lado las desventajas se revelan en que nunca se utiliza la capacidad máxima del canal para un solo circuito, y que si todos los circuitos están ocupados la comunicación es imposible.

Redes de datos con conmutación de paquetes

En la conmutación por paquetes, el mensaje enviado se fragmenta en paquetes, añadiendo la información de origen y destino y un número de secuencia, al llegar al receptor estos paquetes se ensamblan en el orden de su número de secuencia previamente insertado en el origen. Este tipo de conmutación, mejora la comunicación al tener rutas alternativas de un mismo mensaje.

2.2 Redes por Tamaño

Redes LAN

Red de área Local. Dispositivos interconectados entre sí dentro de un edificio o campo, prevalece aun cuando se trata de varias redes conectadas entre sí, siempre y cuando su área se limite a un solo espacio (un edificio, un salón, una oficina).

Redes MAN

Red de Área Metropolitana. Una red MAN se compone por la interconexión de varias redes LAN que se encuentran a mayores distancias pero sin excederse de 50 Km. Se utilizan para conectar computadoras que se encuentran en distintos edificios pero pertenecen a la misma corporación. Es una red de alta velocidad que se extiende más allá de la cobertura de una LAN.

WAN

Red de Área Amplia. Una red WAN conecta dos o más redes LAN que se encuentran en diferentes ciudades pero dentro del mismo país o continente. Operan dentro de un área geográfica extensa, permitiendo el acceso a otras LAN mediante interfaces seriales. Lo que la diferencia de las demás es que proporciona un medio de transmisión a larga distancia de datos, voz, imágenes y videos.

2.3 Redes por Topología

La topología de red, se refiere a la forma de conexión física de los nodos de red. Estos nodos se conectan entre sí mediante dispositivos de comunicación y conexiones físicas. Al establecer la topología el diseñador de red debe plantear los siguientes objetivos:

- Encontrar una forma económica y rápida de conectar dichos nodos y al mismo tiempo mantener la confiabilidad de la red.
- Evitar los retardos en la transmisión de datos.
- Permitir la escalabilidad de la red.
- Mejorar la gestión de la red.

A continuación se describen algunos tipos de topología:

- **Topología Bus o Lineal:** En esta topología todas las estaciones se conectan a un único canal de comunicación. Tiene como limitación una velocidad máxima de 10 Mbps¹⁷. La información enviada la recibe solo la estación destino. Este tipo de topología es fácil de instalar, y es escalable, además si una estación falla no afecta, por el contrario, si falla el canal que las une la comunicación se acabaría. Otra desventaja es que sólo hay un medio de comunicación en común, por lo que las transmisiones son una a la vez, además existen momentos de colisión al momento de considerar que estación transmitirá, y esto aumenta al añadir más dispositivos.

¹⁷ Mbps. Mega bits por segundo.

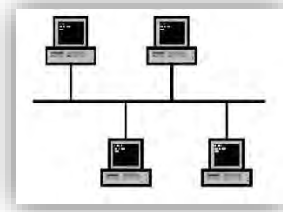


Figura 1 Diseño topología Bus o Lineal

- **Topología Estrella:** La topología de estrella consiste, en conectar todas las estaciones a un dispositivo central (servidor de red, switch, hub, etc.), el cual se encarga de la distribución de la información transmitida entre estas. La velocidad es alta entre estaciones y dispositivo central, pero lenta entre ellas. Igual que en la topología de bus, si falla una estación no afecta la comunicación, pero si falla el dispositivo central se acabaría por completo.

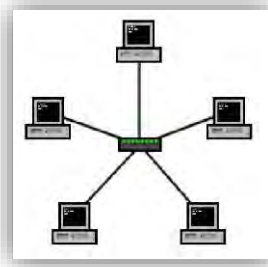


Figura 2 Diseño topología estrella

- **Topología de anillo:** En la topología de anillo, todas las estaciones están conectadas entre sí formando un anillo. La información transmitida pasa por todas las estaciones hasta llegar a su lugar de destino, lo que implica una baja velocidad. Si una estación falla no perjudica la comunicación, pero si falla el enlace dejaría bloqueada la red en su totalidad.

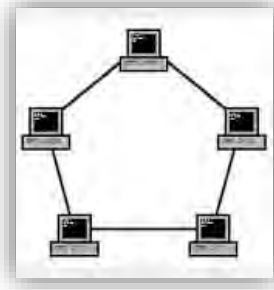


Figura 3 Topología de anillo

- **Topología Malla**

En esta topología, todas las computadoras están conectadas entre sí. Esta configuración proporciona redundancia al haber un respaldo de enlace en caso de falla, por otro lado es costosa al existir estos “dobles enlaces”.

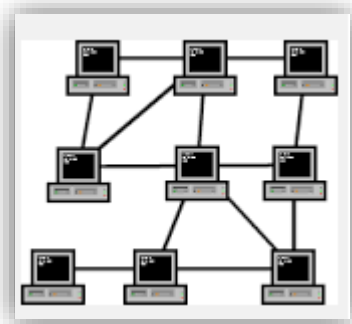


Figura 4 Topología de malla

- **Topología de Árbol**

La topología de árbol combina las características de una topología bus y estrella. Consiste en un grupo de subredes en escala conectadas a un bus central. La ventaja recae en la facilidad de crecimiento, por otro lado es más difícil su configuración, y en caso de que falle del segmento principal todos los demás se vendrían abajo.

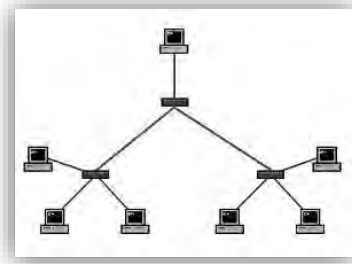


Figura 5 Topología de árbol

3.1.3 Diseño de Redes de datos

Durante los últimos años, han surgido nuevas metas y preocupaciones para los diseñadores de red. Estas son algunas:

- La necesidad de apoyar a usuarios móviles y remotos.
- Una mayor seguridad de red.
- Una mayor necesidad de redes gestionables y dispuestas a cambios.
- Aprovechamiento de las redes inalámbricas
- Nuevos diseño de red y herramientas de gestión
- La redundancia de red
- La modularidad en el diseño de redes
- El soporte de tráfico de voz y datos

3.1 Metodología *Top-Down*

La metodología de Diseño Red *Top-Down*, nos muestra un método clásico para el diseño de red que sigue siendo relevante hoy en día. Se centra en el análisis de requisitos antes de la selección de los componentes de red. Se puede aplicar a redes de todo tipo, incluidas las redes de 10-Mbps, Ethernet¹⁸ o *Token Ring*¹⁹, así

¹⁸ Ethernet. Estándar de red que define las características del cableado o tipo de conexión de las redes, además de brindar los formatos necesarios para las tramas de datos de cada nivel. Fuente: <http://www.mastermagazine.info/termino/4930.php#ixzz3K6clldwb>

¹⁹ Token Ring. En redes de área local, arquitectura que combina el paso de token con una topología híbrida de anillo/estrella. Fuente: (Pffaffenberger, 1999)

como las redes con Gigabit Ethernet²⁰, red óptica síncrona (SONET)²¹ y redes inalámbricas.

El Diseño de red *Top-Down*, es una metodología que comienza por las capas superiores del modelo OSI²². Se centra en las aplicaciones, sesiones y transporte de datos antes de la selección de routers, switches y los medios de comunicación que operan en las capas inferiores. Este método es también iterativo. Primero se obtiene una visión general de las necesidades de un cliente. Más tarde se examinan los protocolos, requisitos de escalabilidad, preferencias de tecnología, y así sucesivamente. Con esta metodología, se contempla que el diseño lógico y físico pueda cambiar a medida que se recopila más información.

Análisis de Requerimientos

Identificando los objetivos y necesidades del cliente.

Analizar las necesidades del cliente, comprende la identificación de los objetivos y las restricciones que deberá tener el diseño de la red. Como paso fundamental, es importante determinar quién o quienes tienen la autoridad de aceptar o rechazar una propuesta de diseño de red.

Análisis de las metas técnicas

Conocer las metas técnicas del cliente, sirve para conocer el alcance en el diseño de red; ya sea al momento de crear uno nuevo o actualizar el existente, y así poder recomendar las tecnologías que cumplan con sus requerimientos.

²⁰ Gigabit Ethernet. Tecnología de transmisión basado en el formato de trama Ethernet y el protocolo utilizado en redes de área local (LAN), proporciona una velocidad de datos de 1 mil millones de bits por segundo (un gigabit). Fuente: <http://searchnetworking.techtarget.com/definition/Gigabit-Ethernet>

²¹ SONET *Synchronous Optical Network* (SONET) es un estándar para el transporte de telecomunicaciones en redes de fibra óptica.

²² OSI. Modelo de interconexión de sistemas abiertos creado por la ISO en 1980. Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones. Fuente: (Pfaffenberger, 1999)

Algunos objetivos técnicos son:

- Escalabilidad: la escalabilidad de una red, se refiere a la facultad de adaptarse a cambios o aumentos en dispositivos, número de usuarios, aplicaciones y conexiones de red. Todo con la finalidad de proponer un mejor alcance.
- Disponibilidad: la disponibilidad en una red, es la cantidad de tiempo que los servicios proporcionados por la red están habilitados para sus usuarios, tiene relación con la estabilidad de la red en cuanto a retardos, la redundancia resistencia y seguridad.
- Rendimiento: El rendimiento de la red, incluye aspectos como, la eficacia, retardo y tiempo de espera en el tráfico de la red. Este punto, es de vital importancia al analizar el estado de red actual, ya se proporciona una visión de cuáles podrían ser los cambios para mejorar el rendimiento.
- Seguridad: la seguridad en un diseño de red, es fundamental ya que implica el hecho de planificar un método de contingencia ante alguna falla o pérdida. También implica analizar cuáles son las vulnerabilidades de la red, y cuáles podrían ser los posibles riesgos, para que en algún momento que se presente un problema se pueda tratar a tiempo sin afectar el funcionamiento de la empresa.
- Administración: la administración en un diseño de red, debe cubrir las necesidades del cliente y como éste quiere que se refleje en la gestión de la misma. Debe entre otros aspectos ser simplificada, para el fácil entendimiento y uso por los administradores de red.
Según la terminología ISO²³, la meta de los administradores de red debe considerar los siguientes puntos:
 - Análisis de tráfico para la optimización de la red de acuerdo a los niveles de servicio.
 - Descubrimiento, aislamiento y corrección de fallas.

²³ ISO. Organización Mundial de la Normalización. Organismo encargado de promover el desarrollo de normas internacionales de comunicación, comercio y fabricación para todas las ramas industriales. Fuente: (Pfaffenberger, 1999)

- Identificación y recolección de información de los dispositivos de comunicación.
- Supervisión de la seguridad y políticas de protección, autenticación y cifrado.

Graficando la red existente

Analizar la red actual, consiste en la ejecución de un software de mapeado/monitoreo de red que nos permita visualizar las conexiones, dispositivos, y direccionamiento existentes.

1. Desarrollo de un mapa de red

Saber cómo está estructurada la red, nos permite saber cómo está compuesta, cómo se comporta el flujo de tráfico y el nivel de rendimiento. Es el punto de partida.

2. Herramientas para el desarrollo de un mapa de red

Para el desarrollo del mapa de red existente es importante utilizar ciertas herramientas para:

Monitoreo de red:

- *Cisco Works*
- *WhatsUp Gold*
- *HP OpenView*
- *LANSurveyor*
- Capsa
- Nagios
- Nmap
- Otros

Diseño de diagramas de red:

- Visio
- *Edraw*

- Otros

3. Caracterizando la topología lógica de red

La topología lógica de una red, nos permite identificar si una arquitectura de red es plana o jerárquica, estructurada o no, en capas o no. También nos dice, cuál es su forma de conexión (estrella, anillo, etc.). Nos muestra cuanto es su nivel de complejidad, el estado de convergencia, enrutamiento, cableado y redundancia. Una vez analizado la arquitectura lógica, es fácil identificar si la red es capaz de actualizarse, de soportar cambios sin afectar su rendimiento.

Direccionamiento y Nombramiento

El esquema de direccionamiento y nombres, es muy importante al caracterizar la infraestructura lógica de una red. Un buen esquema de direccionamiento puede influenciar en la habilidad de adaptar el nuevo diseño de red a los objetivos del cliente.

Cableado y medios de enlace

Determinar la tecnología de capa de enlace que está en uso, permite saber qué tipo de medios se está utilizando, su capacidad y aprovechamiento.

4. Comprobación del funcionamiento de la red (línea base)

Al estudiar el estado de la red, se crea una línea base para poder medir y comparar el rendimiento actual con el esperado en el nuevo diseño. Al capturar el tráfico de una red, se pueden identificar que protocolos y servicios realmente están en función.

Línea Base para Rendimiento

El desarrollo de un línea base para el rendimiento, tiene como principal paso seleccionar la cantidad de tiempo en el que se hará el análisis de tráfico. Es fundamental delimitar por cuánto tiempo se estudiará el comportamiento, mientras más sea el tiempo, más exactos son los resultados. Además del tiempo, es importante delimitar en qué momento se realizará el estudio, por lo general se recomienda durante los períodos de carga de tráfico normal.

Análisis de la Disponibilidad

Para medir la disponibilidad de red, es importante comparar el tiempo en el que la red trabaja normalmente, cuando falla y el tiempo que lleva reparar tal falla. En entrevista con el administrador de red se puede preguntar sobre las causas de los periodos de falla e inactividad.

Analizando el uso de la red

El uso de red, se mide por la cantidad de ancho de banda que se consume en un período determinado, normalmente especificado en porcentaje. Una parte de este análisis es el consumo por protocolo.

Analizando la eficiencia de la red

La utilización de ancho de banda, se optimiza para que haya eficacia cuando las aplicaciones y protocolos están configurados para enviar grandes cantidades de datos por trama. El aumento de la Unidad Máxima de Trasmisión (MTU)²⁴ en interfaces del router también mejora la eficacia. Todo este procedimiento, requiere del análisis por medio de un analizador de protocolos para medir el tamaño de los paquetes que circulan en la red.

Analizando el retardo y tiempo de respuesta

Para verificar que el rendimiento del nuevo diseño de red se encuentra dentro las exigencias del cliente, es fundamental medir el tiempo de respuesta entre dispositivos de red antes y después de que el diseño sea implantado. Mediante un analizador de protocolos, se mide la cantidad de tiempo entre paquetes, obteniendo un estado del tiempo de respuesta en contraste con las capas de enlace de datos, transporte y aplicación.

Verificar el estado de Routers, Switches y Firewalls

Al analizar el estado de los dispositivos de comunicación es importante conocer su estructura y como obtener información de él, algunas características importantes para analizar son:

- Proveedor

²⁴ MTU. Maximum Transfer Unit. Unidad Máxima de Transferencia. El paquete más grnde que puede transmitirse en una red de conmutación de paquetes Fuente: (Pfaffenberger, 1999)

- Memoria
- Utilización de CPU²⁵
- Número de paquetes procesados/perdidos
- Estado de *buffer*²⁶
- Conexiones.

Caracterizando el tráfico de Red

1. Caracterización del flujo de tráfico

La caracterización de flujo de tráfico, implica identificar la fuente y destino de tráfico de red, el análisis de la dirección y la simetría de los datos que viajan entre estos dos puntos.

2. Caracterización de la carga de tráfico

Antes de seleccionar la topología y tecnologías usadas en una red, es importante conocer la carga de tráfico que se espera que soporten estas. Para evitar los cuellos de botella, se investigan los patrones de uso de aplicaciones, los tiempos muertos entre paquetes y sesiones, tamaños de trama, y otras características de comportamiento de tráfico.

3. Caracterización de la Calidad de Servicio

Al analizar las necesidades de la red en cuanto al tráfico y la disponibilidad, más allá del flujo y carga, es importante saber si una aplicación es flexible o no a la demora. En el caso importante de envío de voz y video, no se puede comparar con el envío de datos simples, ya que la primera requiere un ancho de banda mayor. La calidad de servicio hace mención a esto, de las aplicaciones que en ciertas circunstancias requieren más capacidad para asegurar su entrega.

²⁵ CPU Central Processing Unit, que en español significa Unidad Central de Procesamiento. Dispositivo encargado de procesar datos e interpretar instrucciones en el uso de información y aplicaciones. Fuente: <http://definicion.mx/cpu>

²⁶ Buffer. Espacio de memoria en un disco o instrumento digital, reservado para el almacenamiento temporal de información digital mientras espera ser procesada. Fuente: (Pfaffenberger, 1999)

3.2 Diseño Lógico

Diseño de una topología de Red

Una topología de red, nos indica el direccionamiento, los segmentos de red, el tamaño, los puntos de interconexión y la distribución de usuarios. El diseño de una topología de red, es el primer paso para el diseño lógico de una red basada en la metodología *Top-Down*. Dependiendo del diseño de la topología lógica, serán las características de escalabilidad y adaptabilidad que tendrá el diseño de red.

Diseño de Red Jerárquica

Un diseño de red jerárquico, implica la división de la red lógica y los dispositivos de comunicación en 3 capas:

- Capa Núcleo: Esta es la capa principal, ya que aquí se encuentran los routers y switches de alta velocidad, los cuales necesitan de la mayor disponibilidad, rendimiento y redundancia ya que a través de ello se realizan las transacciones de datos y comunicación
- Capa de Distribución: Aquí se encuentran routers o switches mediante los cuales se crean las políticas, el control de acceso a los recursos y el control del tráfico
- Capa de Acceso: Aquí se encuentran los switches que dan acceso a los usuarios finales y puntos inalámbricos en los diferentes segmentos de red.

Motivo para usar un modelo de red jerárquico

- Una metodología de red jerárquica, permite diseñar una topología modular que limita el número de routers que se comunican.
- Minimiza los gastos ya que se incorporan sólo los dispositivos apropiados para cada capa.
- Un mejor aprovechamiento del ancho de banda ya que se planifica la capacidad máxima en cada capa

- Mejor administración de dispositivos.
- Es más fácil identificar y aislar fallas.
- Adaptabilidad a los cambios.

Verificando la aplicación correcta del diseño de red jerárquico.

Para saber si se aplicó la metodología de diseño de red jerárquico, es indispensable poner a prueba la red y comprobar que se pueden realizar las siguientes acciones sin ninguna dificultad:

- Añadir nuevos edificios y enlaces WAN.
- Cuando nuevas condiciones solo causan un cambio local en los dispositivos directamente relacionados.
- Duplicar o triplicar el tamaño de la red sin modificar el diseño principal.
- Fácil corrección de problemas.

Diseño de red redundante.

Una topología de red redundante, implica mantener la disponibilidad de la misma a través de la duplicación de componentes como dispositivos y enlaces, con el fin de mantener la comunicación a pesar de fallas. Esta redundancia, puede aplicarse a redes simples o a las capas de un modelo de red jerárquico. Antes de aplicar un diseño redundante, es importante conocer las necesidades del cliente ya que tal diseño implica un costo elevado tanto en la incorporación como en el mantenimiento. El diseño de red redundante hace uso de:

- Rutas de respaldo
- Balanceo de cargas

Diseño de red Modular

El diseño de una red, implica la formación de distintas áreas y módulos, los cuales tienen un enfoque particular en los servicios y soluciones que soportan,

relacionados con la jerarquía y la redundancia, sin dejar a un lado el diseño general de la red.

- Modelo de red Empresarial: Este modelo se aplica a grandes empresas y consta de 3 áreas principales:
 - Campus de la empresa: en esta área se incluyen los módulos requeridos para una red con alta disponibilidad, escalabilidad y flexibilidad. Un área robusta que puede funcionar independiente de la red.
 - Borde la empresa: Esta área es la encargada de la conectividad entre los módulos y rutas entre campus. Incluye todos los elementos de red para la comunicación entre el campus y sitios remotos.
 - Proveedor de servicios de borde: Estos solo se activan para trabajar con otras redes mediante diferentes tecnologías WAN e ISPs²⁷.

Diseño de red de Campus

El diseño de red de campus se compone de un modelo jerárquico y modular, el cual tiene dominio en los siguientes puntos:

- Ancho de banda
- *Broadcast*
- Redundancia
- Servidores espejo
- Selección de rutas de comunicación
- Disponibilidad
- Rendimiento

El manejo de la red, es importante en este diseño ya que se, por ejemplo, el *backbone* debe proporcionar acceso a dispositivos que soporten monitoreo, solución de problemas, seguridad, etc.

²⁷ ISP. *Internet Service Provider*. Proveedor de Servicios de Internet. Empresa que brinda cuentas y conexión a Internet a individuos y empresas. Fuente: (Pfaffenberger, 1999)

Según este modelo se deben incluir los siguientes módulos dentro de un campus:

- Módulo de infraestructura
- Módulo de administración de la red
- Módulo de servidores
- Módulo de distribución de borde

Diseño de Red segura

Un diseño de red seguro, implica conocer cuáles serán los dispositivos más importantes y así saber cuáles serán los objetivos a implantar.

Un *Firewall*, es un dispositivo que permite o deniega la transmisión de datos de una red a otra. Un firewall puede ser un router con ACLs configuradas, un dispositivo físico o una aplicación corriendo en un sistema. La colocación del firewall debe ser en un lugar donde tenga que pasar el tráfico entrante y saliente, por lo general en el límite de la red e Internet. Para grandes empresas se recomienda la utilización de un firewall dedicado.

Diseño de un esquema de direccionamiento y nombres

Para un buen funcionamiento de la red, es indispensable el uso de un esquema de direccionamiento IP y nombres, sin este vendrán problemas como:

- Falta de direcciones
- Desperdicio de direcciones
- Direcciones y nombres duplicados
- Nombres difíciles de manejar

Este esquema se basará en políticas y procedimientos.

Para asignar direcciones IP

- La asignación de direcciones de red, debe ser previamente planeadas y documentadas
- Debe basarse en un modelo estructurado y jerárquico
- Planee el crecimiento de la empresa, por lo tanto de las direcciones.
- Basarse en la red física
- Usar la asignación automática de direcciones para usuarios finales
- Usar direcciones privadas cuando se requiera.

Usando un modelo de direccionamiento jerárquico

El diseño jerárquico en el direccionamiento al igual que en el diseño lógico de la red, permite una mayor manejabilidad de la red además de una optimización, solución de fallas, escalabilidad, estabilidad.

En un router, por ejemplo, permite la sumarización al poder agregar más redes a la tabla de enrutamiento, esta características permite un mayor rendimiento y escalabilidad. Un direccionamiento jerárquico también facilita el uso de VLSM.

Diseño de un modelo de Nombres

Un modelo de nombres, también refuerza el rendimiento y disponibilidad de la red, además de facilitar el direccionamiento de red. Los nombres son asignados a diferentes recursos: computadoras, switches, routers, impresoras. Las características que deben tener los nombres son:

- Cortos
- Fáciles de identificar (de acuerdo al tipo de recurso o función del mismo)
- Distinto
- Evitar caracteres especiales, guiones, etc.
- Puede incluir un número

Siguiendo la línea de un modelo jerárquico, se puede mencionar el uso del servicio de DNS²⁸, el cual está formado de una base de datos distribuida que proporciona un sistema de nombramiento jerárquico.

Selección de Switches y Routers

La selección de switches y routers, depende entre otros puntos de cubrir ciertos requerimientos de conmutación y enrutamiento de acuerdo al diseño de la topología de red. Estos puntos son:

- Características del tráfico de red
- Ancho de banda, memoria y uso de CPU
- Capacidad de cambio
- Capacidad de certificar rutas alternativas por razones de seguridad.

Al seleccionar por ejemplo que switches utilizar es importante saber si soportan ciertas características como STP²⁹ o VLANs³⁰, el caso de los routers es fundamental conocer qué tipo de dispositivos se utilizarán y que protocolo de enrutamiento correrán, ya que dependiendo del protocolo usado serán la eficiencia del dispositivo. Los protocolos de enrutamiento se diferencian en su escalabilidad y rendimiento

Estrategias de seguridad de red

Las estrategias de seguridad en un diseño de red lógica, implica la necesidad de proteger cada uno de los componentes. De acuerdo a la metodología *Top-Down*, estas estrategias se concentran en la planificación y desarrollo de políticas antes que la selección de productos de seguridad.

²⁸ DNS *Domain Name System*. Programa que corre en un sistema de computación conectado a Internet, y proporciona una traducción automática entre nombres de dominio y las direcciones IP correspondientes. Fuente: (Pfaffenberger, 1999)

²⁹ STP. *Spanning Tree Protocol*. Protocolo de red que opera en la capa 2 del modelo OSI (enlace de datos), su función es gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes. Fuente: librosnetworking

³⁰ VLAN. *Virtual Local Area Network*. LAN virtual. Configuración de diferentes segmentos virtuales en un mismo switch, para disminuir los dominios de broadcast. (Pfaffenberger, 1999)

Aquí el punto no es sólo crear las estrategias sino tener una técnica apropiada para aplicarlas. Estos son los pasos para desarrollar las estrategias de seguridad:

1. Identifique los activos de red
2. Analice los riesgos de seguridad
3. Analice los requerimientos de seguridad y restricciones
4. Desarrolle un plan de seguridad
5. Defina políticas de seguridad
6. Desarrolle un procedimiento para aplicar las políticas de seguridad
7. Desarrolle una estrategia de realización técnica
8. Consiga la compra
9. Entrene a usuarios, personal técnico y gerente (s)
10. Ponga en práctica la estrategia técnica y los procedimientos de seguridad
11. Pruebe la seguridad y actualice la estrategia en caso de falla
12. Mantenga la seguridad programando auditorías independientes y periódicas.

Algunas técnicas de seguridad, pueden venir acompañadas del uso de recursos como *Firewall* o sistemas IDS, los cuales apoyan en el uso de políticas de seguridad en cuanto al tráfico de red y aplicaciones.

Estrategias de Gestión de red

La gestión de la red, es un aspecto importante en el diseño lógico ya que proporcionará la operación, mantenimiento, disponibilidad, rendimiento y objetivos de seguridad de esta. También proporciona apoyo a la hora de analizar el comportamiento y realizar mejoras o solución de fallas.

La ISO define 5 tipos de procesos en la gestión de la red:

- Manejo del rendimiento
- Manejo de fallas
- Manejo de configuración
- Manejo de seguridad

- Manejo de contabilidad

Existen algunas herramientas que permite que la gestión de la red sea más amigable y por consiguiente dinámica. Algunas de ellas son:

- *Cisco NetFlow*
- Nagios
- *WhatsUp Gold*
- *Solar Winds*
- Capsa
- *Wireshark*
- Nmap
- Etc.

3.3 Diseño Físico

El diseño físico de red, implica la selección de la tecnología LAN y WAN para la red y su ubicación y conexión física. Un diseño eficaz de acuerdo a la metodología *Top-Dow*, debe desarrollar primero soluciones del campus, luego del acceso remoto y por último de las conexiones WAN.

Topología del cableado

Diferentes compañías como ATM e IBM han publicado especificaciones del tendido del cableado, sin embargo una generalización puede ser hecha con base en estos dos tipos de esquemas:

1. Cableado centralizado: Un ejemplo es la topología de estrella.
2. Cableado distribuido: Topología de Bus, Anillo y Árbol.

Tipos de cable:

1. Cable de cobre protegido: STP y Coaxial
2. Cable de cobre no protegido: UTP

3. Cable de fibra óptica

Tecnologías LAN

- Ethernet: tecnología perteneciente a la capa física y de enlace de datos, y sirve para la transmisión de tramas en una LAN. Es escalable y existen de diferentes tipos y capacidades como:
 - *Half- Full Duplex*
 - 10 Mbps Ethernet
 - 100 Mbps Ethernet
 - 1000 Mbps Ethernet (1 Gbps)
 - 10 Gbps
 - Metro Ethernet
 - Ethernet de largo alcance (LRE)
 - Cisco *EtherChannel*

Selección de dispositivos

Los criterios generales para seleccionar los dispositivos que comunicarán la red, son los siguientes:

1. Número de puertos
2. Velocidad de procesamiento
3. Cantidad de memoria
4. Cantidad de latencia al transmitir datos
5. Rendimiento en paquetes por segundo
6. Auto detección de velocidad
7. Auto descubrimiento del medio
8. Capacidad del medio (cable)
9. Facilidad de configuración
10. Manejabilidad
11. Costo
12. Soporte de filtros de paquetes y otras medidas de seguridad

13. Características de QoS³¹
14. Disponibilidad en el soporte técnico
15. Calidad de la documentación

En switches:

1. Soporte de STP
2. Soporte de direcciones MAC³² que puede recordar
3. Soporte de seguridad de puerto
4. Soporte de VLANs
5. Cantidad de memoria

Para routers:

1. Protocolos de red soportados
2. Soporte de aplicaciones multicast³³
3. Soporte de compresión
4. Soporte de codificación

Para APs:

1. Velocidad
2. Velocidad de puerto Ethernet
3. Soporte de NAT³⁴ y DHCP³⁵
4. Soporte de VLANs

³¹ QoS. *Quality of Service*. Calidad de Servicio. Es el rendimiento promedio de una red, visto por los usuarios. Algunas características que se miden son: ancho de banda, rendimiento, jitter, retraso en la transmisión, pérdida de paquetes y disponibilidad. Fuente: (Pfaffenberger, 1999)

³² MAC. Dirección de la tarjeta de Red. Es única y sirve para la identificación de dispositivos que se conectan a una red de datos. (Pfaffenberger, 1999)

³³ Multicast. Es el envío de información a múltiples redes de manera simultánea. Fuente:

³⁴ NAT (*Network Address Translation* - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Fuente: (Pfaffenberger, 1999)

³⁵ DHCP. Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host. Protocolo de red que permite asignar direcciones IP a los dispositivos conectados a la red de manera automática. Fuente: (Pfaffenberger, 1999)

5. Soporte EAP³⁶
6. Soporte de WPA³⁷
7. Otros.

3.4 Pruebas y documentación

Una vez terminado el diseño de la red, es importante verificar si el funcionamiento es acorde a los objetivos y requerimientos anteriormente establecidos. Realizando las pruebas pertinentes, se comprobarán que las soluciones desarrolladas cumplen con el rendimiento, disponibilidad, escalabilidad, y sobre todo con la calidad de servicio que el cliente espera.

3.1.4 Auditoría de Redes

Una Auditoría de Red, es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, protocolos de comunicación, conexiones, accesos, privilegios, administración y demás aspectos que repercuten en su instalación, administración, funcionamiento y aprovechamiento. Es también la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red. (Piattini)

La arquitectura de red se compone de cada uno de los siguientes esquemas:

- 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, clasificación de los distintos tipos de tráfico, la estructura lógica de la red (división en subredes, VLANs, etc.)

³⁶ EAP. *Extensible Authentication Protocol*. Es un framework de autenticación usado habitualmente en redes WLAN, utilizando la conexión punto-punto. Fuente: (Pfaffenberger, 1999)

³⁷ WAP. *Wireless Application Protocol*. Protocolo de aplicaciones inalámbricas, es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, p.ej. acceso a servicios de Internet desde un teléfono móvil. Fuente: (Pfaffenberger, 1999)

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

4.1 Tipos de auditoría

Existen diversos tipos de auditorías de redes, debido fundamentalmente al tipo de estudio, alcance u objetivo en específico.

- Auditoría de la arquitectura de redes

La finalidad principal de este tipo de auditorías, 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. La primera fase de una auditoría de la arquitectura de redes, es la recopilación de información sobre las necesidades empresariales y datos técnicos sobre los equipos de red activos. Mediante un proceso específico de entrevistas al equipo de recursos humanos dedicado a la 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 que se ejecutan en la red y los planes de crecimiento futuro. Para la recopilación de datos técnicos sobre los equipos activos de red, se utilizan herramientas software y hardware de monitoreo 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 y lógica.
 - Un resumen analítico de ingeniería donde destacan los puntos potenciales de fallo y/o mejora de la red auditada
- Auditoría de rendimiento de redes

La finalidad principal de este tipo de auditoría, es proporcionar datos del rendimiento, siendo la generación de recomendaciones en forma de reportes las que ayuden a determinar las mejoras que necesita la red para garantizar las necesidades de los usuarios, 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. 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 principales emisores de tráfico en la red.
- Determinación de los principales receptores de tráfico en la red.
- Distribución y uso de los protocolos de comunicaciones

Finalmente, se realiza el informe de 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.

- Auditoría de la disponibilidad de redes

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

- Planificación de servicios: objetivos de alta disponibilidad, gestión de niveles y acuerdos de servicios 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 cambio; verificación de actualización en 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, autenticación de métodos y políticas de intranet y extranet.

Para concluir, se planifica una presentación con el personal directivo y con personal 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 de la red, obstáculos y factores críticos.

- Auditoría de la Seguridad de la Red

Una auditoría de red adecuada, es incompleta sin una evaluación de la seguridad de la red. La seguridad de la red debe ser evaluada contra los problemas de seguridad actuales para garantizar que las medidas de seguridad están actualizadas y en su lugar. Esto incluye, comprobar que tenga un firewall seguro, servidores y dispositivos de detección y prevención de intrusión actualizados con el último software estable. También es importante que los ID de usuario y contraseña obsoletas sean descubiertos y borrados. La fase de seguridad es uno de los pasos más importantes en el proceso de auditoría ya que un lapso en la seguridad podría hacer irrelevantes todas las demás medidas pertinentes. (Hernández, 2000).

3.1.5 Legislación, mejores prácticas y técnicas de Auditoría Informática

Las mejores prácticas, son directrices que permiten a las empresas modelar sus procesos para que se ajusten a sus propias necesidades. Además proporcionan métodos utilizados para estandarizar procesos y administrar de una mejor manera los entornos de TI.

ITIL

La Biblioteca de Infraestructura de Tecnologías de Información, ITIL (del inglés *Information Technology Infrastructure Library*), es una guía de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda la infraestructura, desarrollo y operaciones de TI.

ITIL, fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en

aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del costo, y el resto se invierte en el desarrollo del producto. De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI centralizados o descentralizados, con servicios TI internos o suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de coste aceptable. (OSIATIS S.A., s.f.)

Librerías ITIL

ITIL cuenta las versiones 1 y 3, 8 volúmenes para la primera y 5 para la versión 3. Tomando en cuenta ITIL v3 se describen los 5 libros que forman el ciclo de vida de ITIL:

Libro	Objetivo	Temas principales
Estrategia de Servicio	Diseña el plan de acción para la organización de las TIC	<ul style="list-style-type: none"> • Gestión del servicio • Diseño organizacional • Procesos y actividades clave • Gestión de la demanda • Herramientas para la estrategia • Otros
Diseño de Servicios	Diseño de Servicios TI	<ul style="list-style-type: none"> • Diseño de Arquitecturas (requisitos, limitantes) • Diseño de Políticas • Documentación • Gestión de niveles de servicio • Gestión de capacidad • Otros
Transición del Servicio	Cambios que se han de producir en los servicios	<ul style="list-style-type: none"> • Planificación y soporte • Gestión del cambio • Validación y prueba del servicio • Evaluación • Gestión de configuraciones • Otros
Operación del Servicio	Mejores prácticas para un servicio acorde a los requerimientos y necesidades del cliente	<ul style="list-style-type: none"> • Comunicación • Documentación • Eventos, incidentes y problemas • Atención de requerimientos • Monitoreo y control • Otros
Mejora Continua del Servicio	Mejora continua como fuente de desarrollo y mejora de los niveles de servicio de TI	<ul style="list-style-type: none"> • Medición del servicio • Modelos, estándares y calidad • Herramientas de soporte • Implementación • Innovación, corrección y mejoramiento.

COBIT

COBIT, es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio, y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT, brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas.

COBIT brinda las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI. El uso de las TI, es una inversión importante que debe ser gestionado. COBIT, ayuda a los ejecutivos a comprender y gestionar las inversiones de TI durante su ciclo de vida, y proporciona un método para evaluar si los servicios de TI y las nuevas iniciativas satisfacen los requisitos empresariales, y sea probable que entreguen los beneficios esperados.

Debido a que COBIT, es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, su implementación es una señal de buena gestión en una organización. Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección. Como ocurre con muchos procesos de negocio genéricos, existen estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI. COBIT, se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas.

Marco de trabajo: Explica cómo es que COBIT organiza la gestión del gobierno de TI, los objetivos de control y las mejores prácticas de los procesos y dominios de TI, y los relaciona con las necesidades del negocio. Los representa a través del denominado “Cubo de COBIT”. (ISACA, 2014)

Así como ITIL, COBIT contiene las versiones: 1, 2, 3, 4.0, 4.1 y 5, las cuales han ido evolucionando y complementado para formar un Marco de referencia empresarial.

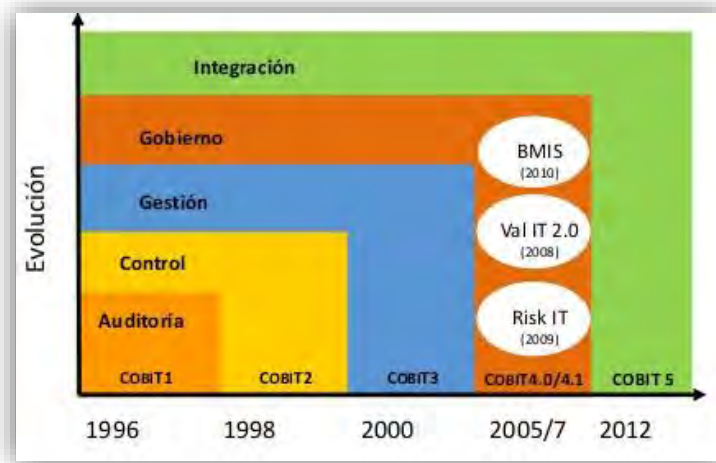


Figura 8 Evolución de COBIT. Fuente OGC

¿Por qué utilizar COBIT e ITIL como mejores prácticas?

ITIL, porque la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

- Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
- Asignarse y entregarse de forma eficaz y eficiente.
- Revisarse y mejorarse de forma continua.

COBIT

- Las auditorías serán más eficientes y exitosas.
- Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección

- Las directrices de gestión ofrecen herramientas para ayudar a asignar responsabilidades y medir el desempeño.
- El modelo de madurez proporciona perfiles de los procesos de TI que describen los posibles estados actuales y futuros.

CAPÍTULO IV

Metodología Propuesta

4.1 Metodología para la Auditoría de Red

Una auditoría, se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática: entre ellos se encuentran COBIT e ITIL.

La siguiente metodología, surge de la necesidad de revisar el estado de la infraestructura de red Institucional en los aspectos de:

- Arquitectura→ Topología Lógica y Física.
- Rendimiento→Velocidad-Ancho de Banda, Flujo de tráfico- Protocolos activos.
- Disponibilidad→Servicios.
- Seguridad→ Firewall, políticas de seguridad-filtrado.

A fin de formar una serie de pasos, que fomenten la existencia de futuras investigaciones en el ámbito de la evaluación de las redes de datos se creó y desarrollo una metodología de Auditoría aplicada a la red de datos de la Universidad de Quintana Roo, y como subsecuente aplicable a cualquier institución que cuente con dicha infraestructura.

Algunos puntos importantes que se tomaron en cuenta para formar esta metodología, fueron procesos específicos de los modelos internacionales COBIT e ITIL, que como “mejores prácticas” proporcionan un marco de referencia para el manejo y mejora de las TIC. COBIT, define qué debemos controlar e ITIL define cómo debemos hacerlo. Como parte de la estructura, la metodología propuesta se divide en tres partes, las cuales a su vez se organizan de acuerdo a las técnicas y procedimientos a utilizar para la evaluación de la red Universitaria.

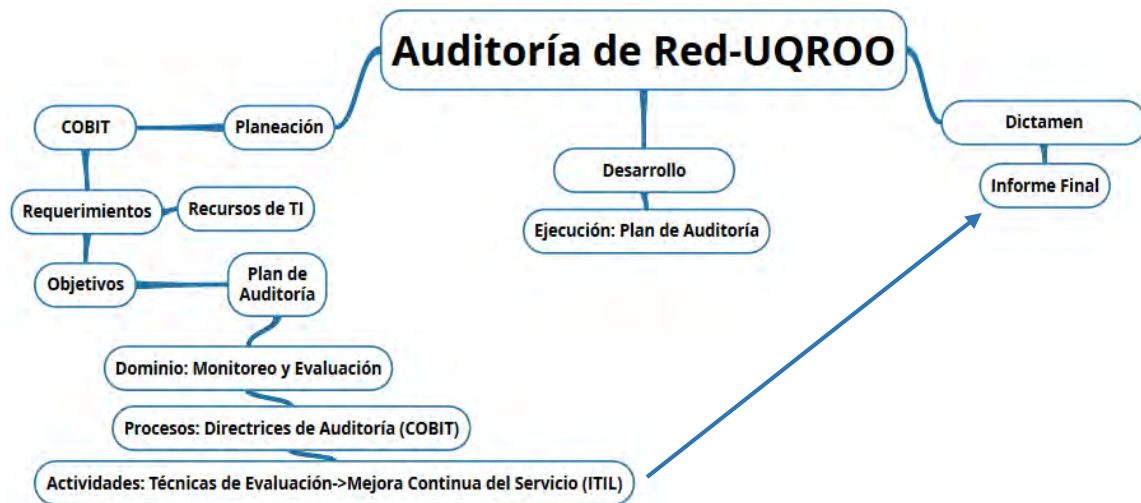


Figura 9 Auditoría de Red. Metodología Propuesta con base en COBIT e ITIL

Planeación

Requerimientos de Negocio (UQROO, campus Chetumal)

Origen

En este punto, se declara el porqué de la Auditoría, es el fundamento del inicio de la evaluación de la red. Aquí se realiza una plática con el administrador de red para averiguar cuáles son los requerimientos de la Universidad.

Objetivo

A partir de la entrevista, se establece el objetivo principal y específico, con los cuales se da la pauta para establecer los procedimientos a seguir y los recursos a utilizar.

Puntos a evaluar

Se declaran las partes a evaluar de la red de acuerdo a los objetivos planteados. Estos puntos se describen de manera general, ya que en el formato del Plan de la Auditoría se describen las actividades específicas a ejecutar.

Recursos

De acuerdo al tipo de Auditoría Informática, se requiere de la obtención de ciertos recursos (físicos, humanos, técnicos o financieros) con los cuales se pueda llevar a cabo tal Auditoría. Estos se describen de acuerdo al objeto de su utilización.

Para una Auditoría de Red los recursos a utilizar son principalmente en:

Software: Aplicaciones de monitoreo de redes especializadas en administración de dispositivos, tráfico y políticas de seguridad y rendimiento.

Hardware: Dispositivo específico para el monitoreo de la red, el cual tenga permisos de acceso y disposición a todo recurso e evaluar en la red.

Plan de Auditoría

COBIT contempla 4 dominios en su metodología, de acuerdo a los requerimientos de la Auditoría de red, el dominio a utilizar será el de Monitoreo y Evaluación, para lo cual se requieren de herramientas proporcionadas también por COBIT, llamadas Directrices de Auditoría (para el dominio a utilizar). En el siguiente Plan de Auditoría toma en cuenta el dominio de COBIT para las actividades a realizar.

Elaboración del Plan de Auditoría

El plan de Auditoría, es una tabla en la cual se citan las actividades a realizar durante la Auditoría, así como el encargado de realizar tal actividad y el período de realización.

Previo a la realización de este esquema es fundamental declarar cuáles serán las actividades a realizar, así como la descripción de cada una. Una vez hecho, esto se establece una cita con el administrador de la red para programar el período de realización de la auditoría. Con un período establecido se organizan las tareas y se ordenan de acuerdo al tiempo que tomará ejecutar cada una.

A continuación se describe cada actividad del plan de Auditoría de la Red Universitaria.

1. Elaboración del plan de Auditoría:

En este punto se analizan los requerimientos y objetivos y con base en ellos, se propone el programa de actividades, los lineamientos y políticas de evaluación, así como los recursos y técnicas que se utilizarán para llevar a cabo la Auditoría de red.

2. Aprobación del plan de Auditoría

Aquí el coordinador del área, podrá dar su punto de vista con respecto a las actividades propuestas por el auditor, a fin de dar disposición de los recursos de la red y permisos de visualización.

3. Obtención de los recursos e instrumentos de evaluación

A través de la aprobación del plan de Auditoría, el coordinador configurará algún equipo mediante el cual se podrá acceder e instalar las herramientas de evaluación.

Monitoreo de Procesos (Dispositivos, Infraestructura)

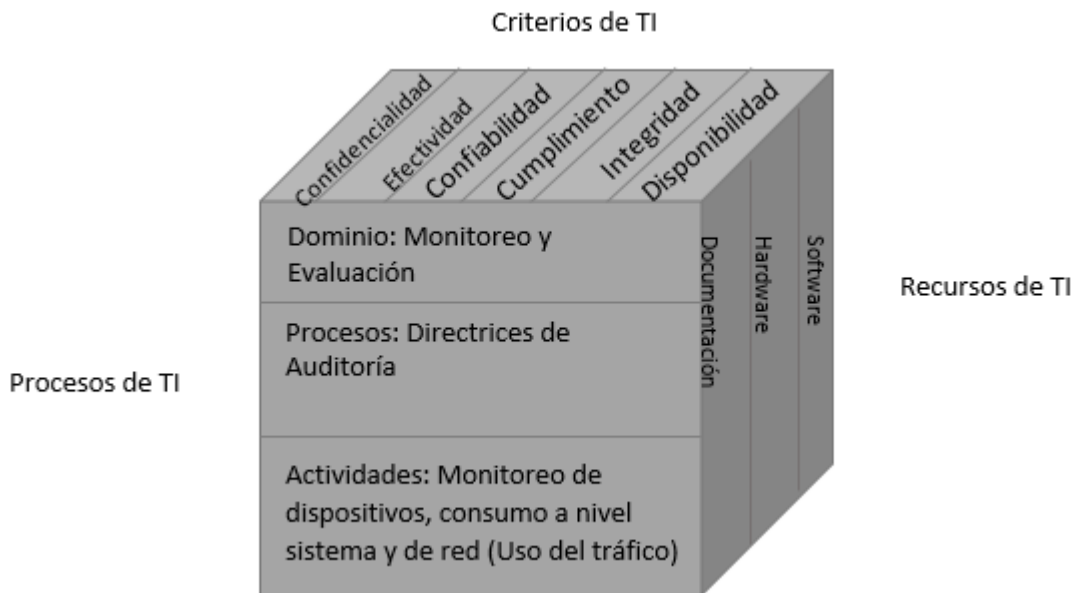


Figura 10 Cubo de COBIT para la Auditoría de Red

Criterios de Información:

- Efectividad
- Eficiencia
- Confidencialidad
- Integridad
- Disponibilidad
- Cumplimiento
- Confiabilidad

Recursos de TI

- Información
- Aplicaciones
- Tecnología
- Personas
- Instalaciones

4. Revisión de la topología lógica y física de la red: Primera actividad en la fase de ejecución en la cual se realiza el diseño lógico y físico de la red.
5. Revisión de los dispositivos de comunicación: Segunda actividad en la fase de ejecución donde se monitorea el estado de cada uno de los equipos principales, formulando un inventario y analizando el rendimiento y configuración de estos.
6. Revisión del tráfico de red: Tercera actividad en la fase de ejecución, en la cual se monitorea el tráfico de red, con respecto a los segmentos. Este monitoreo brindará información sobre el uso de la red así como de los protocolos y servicios más utilizados. El consumo de ancho de banda³⁸ y las políticas que se toman en cuanto a la administración de este.
7. Revisión de los servidores de red: Cuarta actividad en la fase de ejecución, en la cual se monitorea el consumo y aprovechamiento de los servidores y servicios más críticos en la red.
8. Elaboración del informe: Punto principal al concluir las evaluaciones, ya que se presenta un documento formal, en el cual se dictaminan los resultados de la auditoría y se brindan las conclusiones y recomendaciones con respecto a esta.

Esta fase del Plan de Auditoría es el más importante, ya que de este Informe, se generan las posibles sugerencias de implementación para mejorar la red de datos. Para este punto se hace uso de la Metodología ITIL.

³⁸ Ancho de banda. Es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s. Fuente: (Pfaffenberger, 1999)

ITIL desempeña un papel fundamental al ser la metodología más reconocida mundialmente para la mejora de la calidad en la prestación y el aumento de la productividad y eficiencia en la gestión de los servicios de TI.

Para este punto, la fase de ITIL a utilizar, será la de Mejora Continua del Servicio, colocando los siguientes puntos dentro del informe final a partir de los resultados obtenidos:

- Conocer en profundidad la calidad y rendimiento de los servicios TI ofrecidos.
- Detectar oportunidades de mejora.
- Proponer acciones correctivas. (OSIATIS S.A., s.f.)

9. Presentación del informe: Una vez aprobado el informe, se cita a los coordinadores y directores para presentar el resultado de la Auditoría.

Normas para la Auditoría de Red

Al tratar directamente con la fuente de comunicación del campus Chetumal, es importante tomar en cuenta ciertos puntos que rijan el comportamiento de la Auditoría.

Para el auditor	Para la ejecución de la Auditoría
Independencia e Integridad profesional	Planeación y supervisión
Obtención y evaluación de evidencia	Obtención de evidencia suficiente y competente
Rango de conocimiento en el área	Estudio y evaluación
Confidencialidad y responsabilidad de la Información	

Tabla 1 Normas a utilizar en la Auditoría de red

Instrumentos y técnicas de recopilación y evaluación de la Información

En este punto de la planeación de la Auditoría, se diseñan los documentos, guías y los medios para llevar a cabo la auditoría de red, con el fin de obtener la información deseada.

Técnicas de Evaluación

- Revisión Documental: Con esta técnica, se verifica la existencia de documentación acerca de la red y sus componentes, bitácoras, diagramas de red, tablas de direccionamiento, etc.
- Inspección: La técnica de inspección se realiza con el fin de verificar y juzgar el cumplimiento de las funciones de los sistemas computacionales, en el caso de la Auditoría de la red, de los dispositivos de comunicación:
 - Distribución geográfica de dispositivos
 - Uso, funcionalidad y configuración de la red.
 - Aplicaciones
 - Conexiones, etc.
- Confirmación: Esta técnica, permite comprobar la veracidad de los datos obtenidos durante la revisión de la documentación de la red, comprobada y reafirmada mediante el monitoreo de la red y posteriormente presentada en el Informe de la Auditoría.
- Modelo de Madurez: COBIT
- Guía de Evaluación: La guía de evaluación, se permitió tener el control y seguimiento de las actividades durante la Auditoría, así como conocer el procedimiento y las herramientas a utilizar.

Ref.	Actividad	Procedimiento	Herramienta	Observaciones

Tabla 2 Formato Guía de Evaluación

Instrumentos de recopilación de información

- **Entrevista:** La entrevista, es el primer instrumento en la Auditoría de red por medio del cual, se recopila la información inicial del área a estudiar, tiene el propósito de completar y verificar la información analizada por medio de la revisión documental.
- **Observación:** La observación, va de la mano con la técnica de monitoreo, y a que se vigila las actividades de los usuarios en la red a través de un programa sniffer.
- **Inventario:** Los inventarios, permiten tener una lista ordenada de hardware o software existente, así como sus características físicas y lógicas. Aquí un ejemplo del formato a utilizar

Formato de Inventario de Switches:

No. Inventario	Nombre	Marca	Modelo	Dirección IP	Dirección MAC	No. Puertos	No. Tarjetas

Tabla 3 Formato de Inventario

- **Muestreo:** Ya que sería imposible tener e dato exacto de todas y cada una de las actividades, transacciones de red, etc., se hace uso del muestreo, esto a través del análisis de datos dentro de un período. Es así como la Auditoría, se programa para un mes y se seleccionan los días y horarios de monitoreo y recopilación de datos.

CAPÍTULO V Desarrollo

5.1 Introducción

Una Auditoría, requiere de la realización de una serie de pasos y procedimientos, los cuales deben ser diseñados previamente de manera secuencial, cronológica y ordenada, de acuerdo a las etapas y actividades que se requieran aplicar. Además, estos procedimientos se deben adaptar de acuerdo al tipo de auditoría que se vaya a realizar, y con estricto apego a las necesidades, técnicas y métodos de evaluación del área en que se desarrollará.

Al realizar una Auditoría de red, es fundamental que estos procedimientos se basen en una metodología y una previa planeación la cual permita manejar la información de manera eficiente a través de un control de procesos y estándares. Para la planeación de esta Auditoría de la red Universitaria, se combinaron procesos específicos de los Estándares COBIT e ITIL, ya que en el transcurso de la Evaluación toman parte primordial para la correcta gestión de los servicios y recursos de la red.

Tanto COBIT como ITIL influyen directamente en el servicio a los usuarios mediante las TIC, COBIT en las mejores prácticas de la administración de recursos tecnológicos e ITIL en las mejores prácticas de prestación de servicios tecnológicos. Es por ello, que en una Auditoría de Red unir estos 2 métodos significa el aprovechamiento de las utilidades específicas de cada uno para formar una estructura de Control para la Auditoría en una Red, ITIL para lograr una mejora en los servicios y COBIT para verificar la conformidad en cuanto a disponibilidad, rendimiento, eficiencia y riesgos asociados a dichos servicios con los objetivos y estrategias de la Institución, usando para ello métricas claves y cuadros de mando que reporten dicha información.

Las Directrices de Auditoría en COBIT, ofrecen una herramienta complementaria para la fácil aplicación de los Objetivos de Control COBIT dentro de las actividades de auditoría y evaluación.

COBIT, proporciona las Directrices de Auditoría en cada uno de los procesos de gestión de TI, en el caso de una Auditoría de Red, el dominio a utilizar es el de

Monitoreo y Evaluación, ya que es el proceso necesario para la verificación de dispositivos, conexiones, rendimiento y aprovechamiento de la red.

ITIL entre tanto proporciona tanto en el desarrollo como en el dictamen las medidas para analizar los datos, creación de informes y la sugerencia de mejoras mediante acciones correctivas propuestas.

5.2 Desarrollo de la Auditoría de Red

Caso práctico: Auditoría de la red informática de la Universidad de Quintana, campus Chetumal.

5.2.1 Planeación de Auditoría

a) Origen de la Auditoría

A petición de la Dirección de Informática, se llegó a la conclusión de que era necesaria la revisión de la de red de datos de la Universidad, en el campus Chetumal, ya que debido al incremento de servicios y usuarios era necesaria la implementación de nuevas tecnologías y configuraciones al sistema de red, pero se debía tener un antecedente del esquema actual de la red.

b) Objetivo de la Auditoría de Red

“Valorar los procesos, servicios, rendimiento y niveles de seguridad en los servidores y los principales dispositivos de comunicación de la Universidad de Quintana Roo, campus Chetumal.”

c) Puntos a revisar en la Auditoría de Red

De acuerdo al objetivo se procede a la formulación de los puntos a evaluar:

- Revisión del estado de dispositivos de Red
- Revisión de Servicios y Protocolos de Red
- Revisión del Uso de la Red

Recursos a utilizar

De acuerdo a los puntos a evaluar y la forma de obtener los datos, se requerirá del uso de los siguientes recursos:

1. Un servidor virtual: Este servidor virtual, tendrá configurado un direccionamiento IP dentro de un segmento con acceso a toda la red del campus.
2. Software de Monitoreo de Red: WhatsUp Gold, Axence netTools, OpManager, CheckPoint y NetCrunch.

d) Plan de Auditoría de Red

Dispuestos los objetivos, los puntos a evaluar y los recursos necesarios para adquirir los resultados, se desarrolla el siguiente Plan de Auditoría de red:

Plan Auditoría de Red

Institución: Universidad de Quintana Roo **Período:** 15/05/2014 – 15/06/2014

Auditor: Br. Karlibeth Eliodoro Hernández **Área auditada:** Infraestructura de red

No.	Actividad Nombre	Responsable	Semanas			
			1	2	3	4
1	Elaboración del plan de Auditoría	Auditor	X			
2	Aprobación del plan de Auditoría	Coordinador de área	X			
3	Obtención de los recursos e instrumentos de evaluación	Auditor Coordinador de área	X			
4	Inicio de la Auditoría	Auditor		X		
5	Evaluación de la topología física y lógica de la Red	Auditor		X		

No.	Actividad Nombre	Responsable	Semanas			
			1	2	3	4
6	Evaluación de los dispositivos de comunicación	Auditor		X	X	
7	Evaluación del tráfico de red	Auditor		X	X	
8	Evaluación de los servidores de red	Auditor		X	X	
9	Elaboración del Informe	Auditor				X
10	Presentación del Informe	Auditor				X

Tabla 4 Plan de Auditoría

Guía de Auditoría

Una vez hecho el Plan de Auditoría y aprobado, se realiza la guía de Auditoría, la cual tiene como fin llevar un cronograma de las actividades a ejecutar dentro del plan. Estas actividades tienen un orden y cada una se rige bajo un procedimiento específico.

Ref.	Actividad	Técnica de Evaluación	Instrumento	Procedimiento	Observaciones
A1	Elaboración del plan de Auditoría	a)Revisión documental b)Análisis	Entrevista	Solicitar una cita con el coordinador del área.	
A2	Aprobación del plan de Auditoría	a)Confirmación	Plan de Auditoría	Una vez aceptado el plan, iniciar con las actividades establecidas en él	
A3	Obtención de los recursos e instrumentos de evaluación	a)Análisis y Evaluación b)Inspección	-	Búsqueda, descarga e instalación de herramientas de monitoreo, en el dispositivo correspondiente.	
A4	Inicio de la Auditoría	a)Monitoreo	Software de Monitoreo	Empezar con el monitoreo.	
A5	Evaluación de la topología física y lógica de la Red	a)Monitoreo b)Análisis y Evaluación c)Inspección	Software de Monitoreo Software de diseño Observación	Mapeo de dispositivos, de acuerdo a la documentación de direccionamiento de la Universidad. Verificación y diseño de la topología física y lógica de la red actual.	
A6	Evaluación de los dispositivos de comunicación	a)Monitoreo b)Análisis y Evaluación	Software de Monitoreo	Verificación de la configuración lógica de los dispositivos de comunicación.	

Ref.	Actividad	Técnica de Evaluación	Instrumento	Procedimiento	Observaciones
		c)Inspección	Muestreo Observación Inventario	Verificación de la capacidad.	
A7	Evaluación del tráfico de red	a)Monitoreo b)Análisis y Evaluación c)Inspección	Software de Monitoreo Muestreo Observación Inventario	Monitorear el tráfico de la red y evaluar el ancho de banda asignado y el consumo. Análisis del consumo de tráfico por protocolo.	
A8	Evaluación de los servidores de red	a)Monitoreo b)Análisis y Evaluación c)Inspección	Software de Monitoreo Muestreo Observación Inventario	Evaluar el consumo de recursos y capacidad de los servidores.	
A9	Elaboración del Informe	a)Análisis y Evaluación c)Confirmación	Dictamen	En base en el monitoreo, realizar un informe que contenga las situaciones encontradas.	

Ref.	Actividad	Técnica de Evaluación	Instrumento	Procedimiento	Observaciones
				De acuerdo al análisis, recomendar alguna solución o mejora.	
A10	Presentación del Informe	a)Exposición	-Presentación Digital	Presentar el informe al administrador de la red	

Tabla 5 Guía de Evaluación

5.2.2 Ejecución de la Auditoría

De acuerdo al plan de la Auditoría y la guía de evaluación se procede al desarrollo de las actividades, a partir de la actividad A3:

A3: Obtención de los recursos e instrumentos de evaluación

Para el monitoreo de la red Universitaria, se utilizó una máquina virtual con las siguientes características:

- SO: Windows 7 Enterprise 64 bits
- Memoria RAM 6 GB
- Disco duro de 80 GB
- Procesadores Intel: 2

También se descargaron las aplicaciones siguientes:

- Axence netTools 5: potente sistema de monitoreo para redes, que permite conocer cierta información a través de sus 8 herramientas:
 - ✓ NetWatch, para monitorear la disponibilidad de hosts.
 - ✓ WinTools, para ver qué tiene instalado algún equipo en la red
 - ✓ NetStat, revisa la entrada y salida en tu red
 - ✓ Local info, una tabla con información detallada de tu equipo
 - ✓ Network scanner, un escáner de red para ver los nodos de tu red
 - ✓ Service & port scanner, para conocer los servicios y puertos en un host o red.
 - ✓ TCP/IP workshop, prueba diferentes servicios
 - ✓ SNMP Browser y otras herramientas para enviar Pings, etc.
- Axence nVision 7: Al igual que netTools, proporciona herramientas para el inventario de dispositivos en la red, además de conocer el consumo de tráfico en servidores.

Aplicaciones proporcionadas por el Administrador de la Red:

- Check Point: Esta consola de gestión centralizada se utiliza para definir las políticas de seguridad; ver representaciones gráficas de la topología de seguridad de una organización; monitorear e informar sobre los datos de red y de seguridad.
- WhatsUp Gold: realiza monitoreo de aplicaciones y de redes, este software es profundo y fácil de utilizar, permitiendo a los gerentes de TI la conversión de datos de la red a información de negocios. Al monitorear proactivamente todos los servicios y dispositivos críticos, el WhatsUp Gold reduce el tiempo caído de red, que suele ser costoso e impactante al negocio. Con su interfaz Web, permite el control total de la infraestructura y de las aplicaciones de la red, para que el trabajo estratégico, táctico y que trae resultados no sea interrumpido. El WhatsUp Gold provee fácil configuración, escalabilidad robusta, simplicidad de utilización y rápido retorno de inversión. Este software aísla los problemas de la red y proporciona visibilidad y comprensión sobre rendimiento y disponibilidad de la red. Las características principales de este software son:
 - Identificar y mapear todos los dispositivos de red.
 - Enviar notificaciones cuando surgen problemas.
 - Reúne información periódica sobre la red y genera reportes.
 - Proporciona monitoreo de red a cualquier hora y desde cualquier lugar

A5: Revisión de la topología física y lógica de la Red

Diagrama físico de la red

Conexión entre dispositivos: Cable UTP Cat 5e y UTP Cat 6.

Conexión entre edificios: Cable de fibra óptica multimodo.

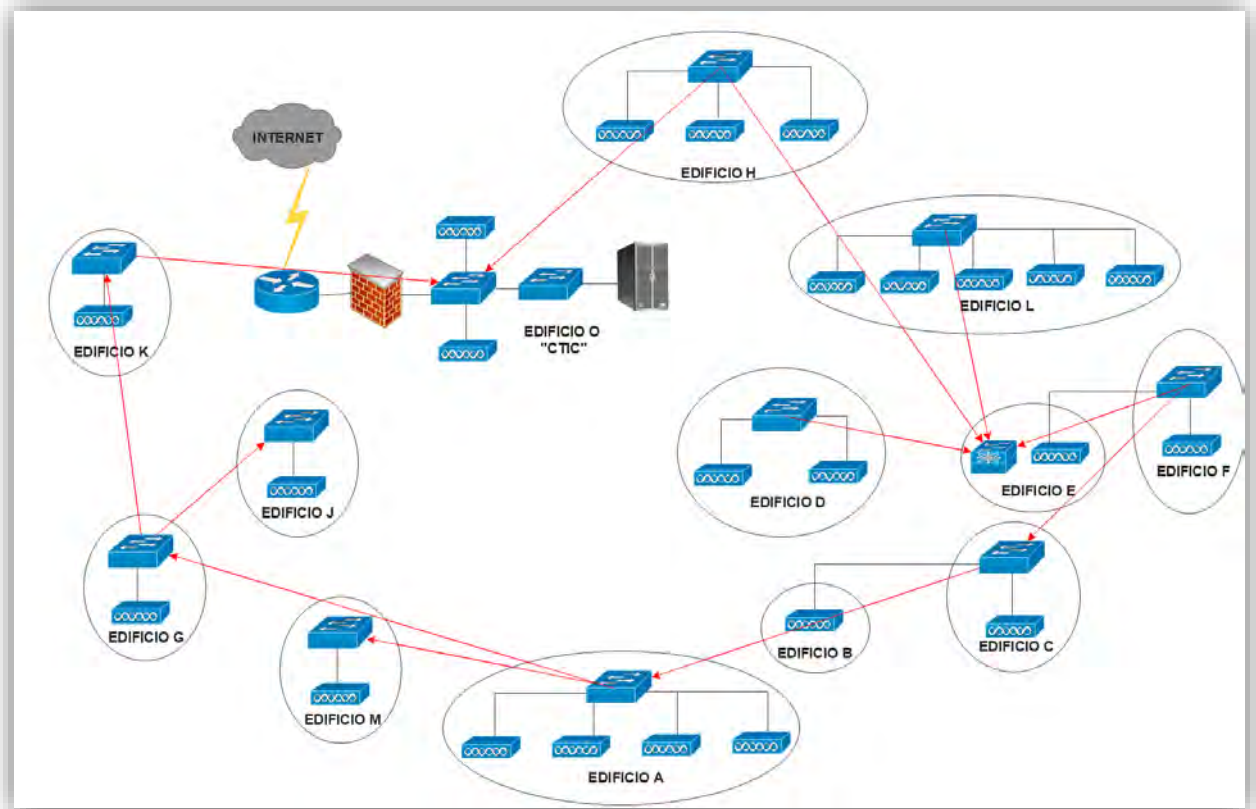


Figura 11 Diagrama Físico de Red UQROO Chetumal

Descripción por edificio

Edificio A

El edificio A, consta de 1 switch marca Enterasys modelo E7 con 4 tarjetas, una tarjeta de enlaces con 6 puertos Gigabit de fibra óptica, y tres tarjetas con 48 puertos Fast Ethernet. Así también 1 access point marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio B y C

Los edificios B y C, se compone de 1 switch marca Cisco modelo 3750 G con 52 puertos Gigabit Ethernet. Así también 2 access point, uno marca UBNT modelo

NanoStation2 en el edificio B y otro marca Linksys modelo WAP54G en el edificio C, éste último no soporta el protocolo SNMP. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio D

El edificio D está compuesto por 1 switch marca Enterasys modelo Matrix E7 con 4 tarjetas, una tarjeta de enlaces con 2 puertos Gigabit de fibra óptica y 24 puertos Fast Ethernet, dos tarjetas con 48 puertos Fast Ethernet, y una tarjeta más con 48 puertos Ethernet. Así también 1 access point marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificios E y F

Los edificios E y F se conforma de 1 switch marca Enterasys modelo Matrix E7 con 2 tarjetas, una tarjeta de enlaces con 6 puertos Gigabit de fibra óptica y otra tarjeta con 48 puertos Fast Ethernet. Así también 2 access point, uno en el edificio E marca TRENDnet modelo TEW-637AP y otro en el edificio F marca Proxim modelo AP-2000, ambos access point no soportan el protocolo SNMP. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio G

El edificio G, consta de 1 switch marca Enterasys modelo SmartSwitch 6000 con 2 puertos Gigabit de fibra óptica y 24 puertos Fast Ethernet. Además 1 access point marca Proxim modelo AP-4000N, éste access point no soporta el protocolo SNMP. La conexión entre dispositivos, es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio H

El edificio H, se compone de 1 switch marca Enterasys modelo E7 con 4 tarjetas, una tarjeta de enlaces con 2 puertos Gigabit de fibra óptica y 24 puertos Fast Ethernet, dos tarjetas con 48 puertos Fast Ethernet, y otra tarjeta más de enlaces con 6 puertos Gigabit de fibra óptica. Además tres access point, uno marca Linksys modelo WAP54G y otros dos marca Proxim modelo AP-4000M, éstos access point no soportan el protocolo SNMP. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio K

El edificio K, está conformado por 1 switch marca Enterasys modelo Matrix E7 con 3 tarjetas, una tarjeta de enlaces con 6 puertos Gigabit de fibra óptica, y dos tarjetas con 48 puertos Fast Ethernet. Además de 2 access point marca Enterasys modelo RBT3K-AG, ambos access point tampoco soportan el protocolo SNMP. La conexión entre dispositivos es mediante cableado UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio J

El edificio J, se conforma por 1 switch marca Cisco modelo 2960 G con 48 puertos Gigabit Ethernet. Así también 1 access point marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio L

El edificio L, está compuesto por 1 switch marca Enterasys modelo Matrix S8 con 2 tarjetas, una tarjeta con 60 puertos Gigabit Ethernet y otra tarjeta más con 48 puertos Gigabit Ethernet. Además, 5 access point marca Enterasys modelo RBT-4102C. La conexión entre dispositivos es mediante cable UTP Cat 6 y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio M

El edificio M se compone de 1 switch Cisco 2960 S con 52 puertos Gigabit Ethernet. Así también de 1 access point marca UBNT modelo NanoStation2. La conexión entre dispositivos es mediante cable UTP Cat 5e y la conexión entre edificios es por cable de fibra óptica multimodo.

Edificio O

El edificio O, está conformado por 1 switch marca Enterasys modelo N7 que incorpora 2 tarjetas, una con 48 puertos Gigabit Ethernet y otra con 12 puertos de fibra óptica, así también 1 switch marca Cisco modelo 2950 con 24 puertos Fast Ethernet. 1 router marca Cisco modelo 2911 con 3 puertos Gigabit Ethernet. 2 Access point, uno marca Linksys modelo WAP4400N y otro marca UBNT modelo NanoStation2. La conexión entre dispositivos, es mediante cable UTP Cat 6 y la conexión entre edificios es por cable de fibra óptica multimodo.

Diagrama lógico de la Red Universitaria.

La configuración lógica de la red en el campus Chetumal, se define con la conexión Ethernet y Fibra Óptica entre los dispositivos, así como el direccionamiento comprende el ámbito de los segmentos de servidores, switches, APs y el router conectado al ISP. A continuación, el diagrama lógico de la red de la Universidad de Quintana Roo, campus Chetumal.

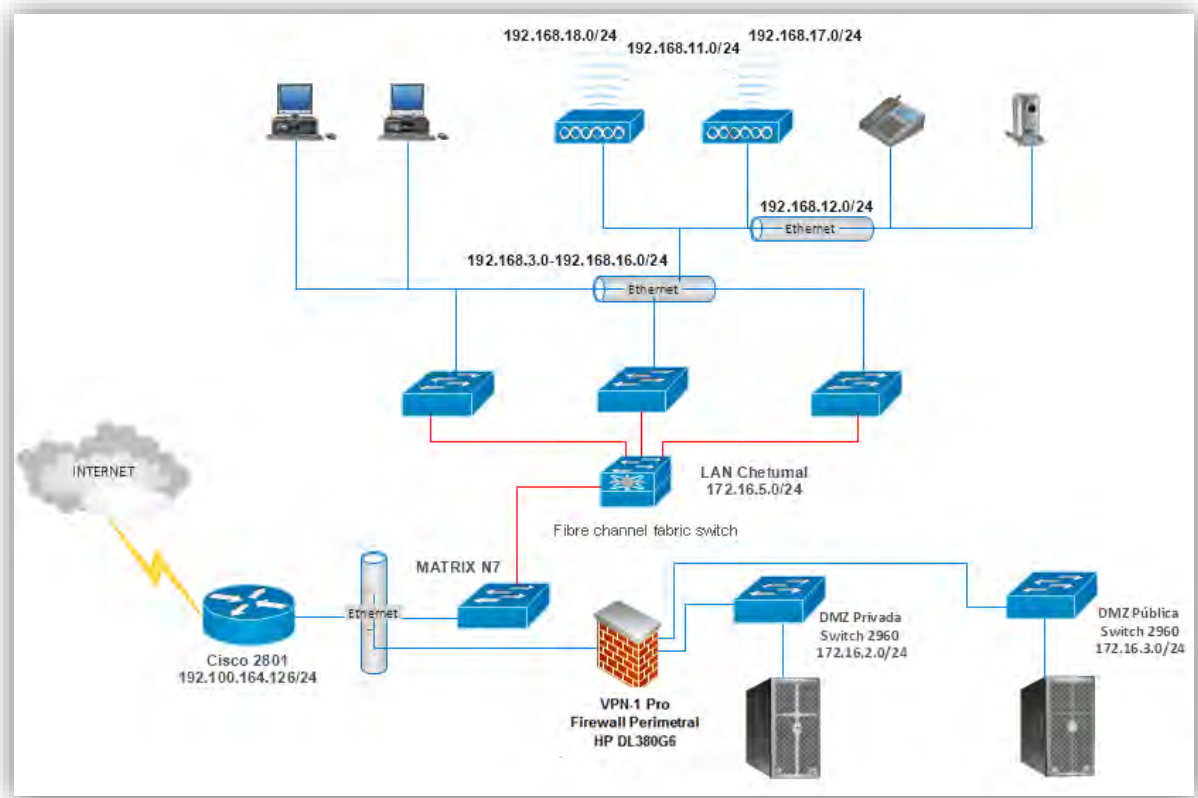


Figura 12 Diagrama Lógico de Red UQROO Chetumal

Inventario Total de los dispositivos de comunicación en la red

Edificio	Nombre	Marca	Modelo	Año de Adquisición	Dirección IP	Dirección MAC
A	T3-Rectoria	Enterasys	6H302-48 Rev 04.08.50	2002	172.16.5.11/24	00:E0:63:D5:67:A3
A	T4-Rectoria	Enterasys	6H302-48 Rev 04.08.50	2002	172.16.5.12/24	00:E0:63:BD:00:74
A	T2-Rectoria	Enterasys	6H302-48 Rev 04.08.50	2002	172.16.5.10/24	0:E0:63:D8:2E:64
D	T1-Enlaces-D	Enterasys	6H352-25 Rev 04.08.24	2001	172.16.5.19/24	00:E0:63:6C:B5:AD
D	T4-EdificioD	Enterasys	6E233-49 Rev 04.08.24	2001	172.16.5.22/24	00:E0:63:1A:75:16
D	T2-EdificioD	Enterasys	6H302-48 Rev 04.08.24	2001	172.16.5.20/24	0:E0:63:95:EE:28
D	T3-EdificioD	Enterasys	6H302-48 Rev 04.08.50	2002	172.16.5.21/24	0:E0:63:AA:A4:FD
D	sysName	Enterasys	6E122-26 Rev 04.11.08	2001	172.16.5.23/24	0:0:1D:A1:65:B3
F	T1-Enlaces01	Enterasys	6G306-06 Rev 04.08.50	2002	172.16.5.9/24	00:E0:63:AC:C8:F8
H	T1-Enlaces01-Biblioteca	Enterasys	6H352-25 Rev 04.08.24	2001	172.16.5.25/24	00:E0:63:B8:5A:D3
H	T1-Enlaces01-Ing	Enterasys	6G306-06 Rev 04.08.50	2002	172.16.5.14/16	00:E0:63:DA:2C:85
H	T2-Biblio	Enterasys	6H302-48 Rev 04.08.24	2001	172.16.5.26/24	00:E0:63:A9:17:B1
H	T4-Enlaces02-Ing	Enterasys	T4-Enlaces02-Ing	2003	172.16.5.17/16	00:E0:63:98:1D:79
H	T2-Ingenierias	Enterasys	6H302-48 Rev 04.08.22	2001	172.16.5.15/24	0:E0:63:AA:A4:91
H	T3-Ingenierias	Enterasys	6E122-26 Rev 04.11.08	2001	172.16.5.16/24	0:0:1D:5B:D4:D4
H	T3-Biblio	Enterasys	6H302-48 Rev 04.08.50	2002	172.16.5.27/24	0:E0:63:AA:A3:EF
H	sysName	Enterasys	6E122-26 Rev 04.11.08	2001	172.16.5.28/24	0:0:1D:6D:29:F0
K	T2-EdificioK	Enterasys	6H302-48 Rev 04.08.50	2002	172.16.5.35/24	00:E0:63:D5:54:05
K	T5-Enlaces02	Enterasys	6G306-06 Rev 05.05.05	2003	172.16.5.13/24	00:E0:63:96:3A:0E
K	T3-EdificioK	Enterasys	6H302-48 Rev 04.08.50	2002	172.16.5.36/24	0:E0:63:D8:64:D0
K	T1-EnlaceK				172.16.5.34/24	
L	Matrix_S8	Enterasys	Rev 07.02.01.0007	2009	172.16.5.45/24	00:1F:45:5C:A9:3E
M	Switch-EdificioM	CISCO	Catalyst 2960S Stack Module WS-C2960S V12.2 SO	2012	172.16.5.44/24	0C:D9:96:2E:C9:40
O	Computo	CISCO	Catalyst WS-C3750G-48TS V12.2 SO	2007	172.16.5.43/24	18:EF:63:C2:2C:CO
O	Sistemas	CISCO	catalyst295024 V12.1 SO	2004	172.16.5.41/24	00:12:7F:4B:0A:00

Figura 13 Inventario de Switches

Edificio	Nombre	Marca	Modelo	Dirección IP	Dirección MAC
A	AP-Rectoria	Avaya	AP-4000M v4.0.12	192.168.12.213/24	00:20:A6:6B:5C:2D
A	WAP440N	Linksys	-	192.168.12.195/24	00:21:29:70:B9:25
A	AP Planeacion	Enterasys	RoamAbout R2 Wireless Access Platform RBTR2	192.168.12.191/24	-
A	RECTORIA_AP1_723643	ALCATEL		192.168.12.241/24	
B	Edif_B_AP1_BT0755394	ALCATEL		192.168.12.243/24	
D	AP-EdificioD	Avaya	AP-4000 v3.1.0	192.168.12.215/24	00:20:A6:6B:4A:93
D	AP-EdificioD	Avaya	AP-4000 v3.1.0	192.168.12.206/24	00:20:A6:6B:9A:DD
G	EDIF_G_AP1_723646	ALCATEL		192.168.12.240/24	
H	BIBLIO_AP1_783648	ALCATEL		192.168.12.237/24	
H	BIBLIO_AP2_783641	ALCATEL		192.168.12.238/24	
H	BIBLIO_AP3_783650	ALCATEL		192.168.12.239/24	
K	AP Edificio k PB	Enterasys	RoamAbout AP-3000 V2.6.7	192.168.12.198/24	00:01:F4:7A:FF:9D
L	CIG	Enterasys	RoamAbout4102RoamAbout 4102	192.168.12.230/24	00:1F:45:5A:58:6E
L	Ordenamiento	Enterasys	RoamAbout4102RoamAbout 4102	192.168.12.231/24	00:1F:45:21:04:3B
L	Posgrado-L	Enterasys	RoamAbout4102RoamAbout 4102	192.168.12.128/24	00:1F:45:5A:58:6D
L	Redes1-AP	Enterasys	RoamAbout4102RoamAbout 4102	192.168.12.226/24	00:1F:45:5A:57:EB
L	Redes2-AP	Enterasys	RoamAbout4102RoamAbout 4102	192.168.12.227/24	00:1F:45:5A:58:7C
M	EDIF_M_AP1_723642	ALCATEL		192.168.12.242/24	
O	CTIC_AP1_723649	ALCATEL		192.168.12.235/24	
O	CTIC_AP2_723647	ALCATEL		192.168.12.236/24	
	MEDICINA_AP1	ALCATEL		192.168.6.37/24	
	MEDICINA_AP2	ALCATEL		192.168.6.38/24	

Figura 14 Inventario de Access Point

Cabe destacar, que algunos dispositivos no se visualizaron en WhatsUp Gold, debido a que no soportan SNMP por el tiempo de antigüedad de más de 10 años.

A6: Revisión de los dispositivos de comunicación

Rendimiento de dispositivos:

A través de la aplicación WhatsUp Gold se fueron monitorizando los dispositivos por segmento, una vez detectados se agregaron a un grupo de acuerdo al tipo de dispositivo.

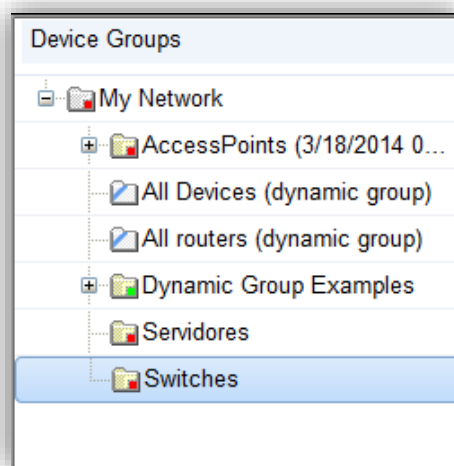


Figura 15 Creación de grupos de dispositivos. WhatsUp Gold

Display Name	Host Name	Address	Device Type	Status
Switch-EdificioM	172.16.5.44	172.16.5.44	Cisco Switch	
T1-Enlaces01-Ing	172.16.5.14	172.16.5.14	Enterasys Networks Switch	
T2-Biblio	172.16.5.26	172.16.5.26	Enterasys Networks Switch	
T1-Enlaces01	172.16.5.9	172.16.5.9	Enterasys Networks Switch	
T4-Enlaces02-Ing	172.16.5.17	172.16.5.17	Enterasys Networks Switch	
T5-Enlaces02	172.16.5.13	172.16.5.13	Enterasys Networks Switch	
T2-Ingenierias	172.16.5.15	172.16.5.15	Enterasys Networks Switch	
T2-Rectoria	172.16.5.10	172.16.5.10	Enterasys Networks Switch	Fast Ethernet(Down at least 20 min); Fast Ethern...
Computo	172.16.5.43	172.16.5.43	Cisco Switch	GigabitEthernet1/0/44(Down at least 20 min); Gig...
T3-EdificioK	172.16.5.36	172.16.5.36	Enterasys Networks Switch	Fast Ethernet(Down at least 20 min); Fast Ethern...
sysName	172.16.5.28	172.16.5.28	Enterasys Networks Inc. Switch	FTM Backplane Port 3(Down at least 20 min); FT...
T3-Biblio	172.16.5.27	172.16.5.27	Enterasys Networks Switch	Fast Ethernet(Down at least 20 min); FTM Backp...
sysName	172.16.5.23	172.16.5.23	Enterasys Networks Inc. Switch	Ethernet Frontpanel(Down at least 20 min); Ether...
T3-EdificioD	172.16.5.21	172.16.5.21	Enterasys Networks Switch	Fast Ethernet(Down at least 20 min); Fast Ethern...
T3-Ingenierias	172.16.5.16	172.16.5.16	Enterasys Networks Inc. Switch	Ethernet Frontpanel(Down at least 20 min); Ether...

Figura 16 Adición de dispositivos WhatsUp Gold

Una vez agregados todos los dispositivos, se configuraron los recursos a monitorear. Con esto se obtuvieron las gráficas de desempeño y uso en cada uno:

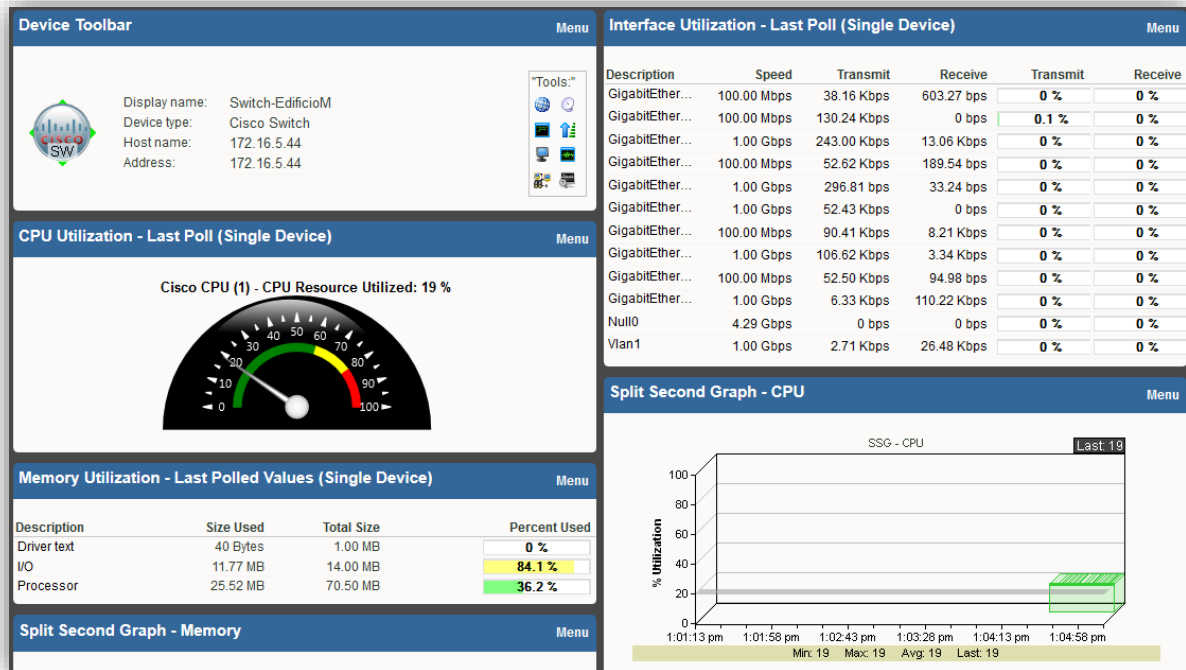


Figura 17 Monitoreo de rendimiento de dispositivos

Realizando el monitoreo con cada uno, se pudo constatar el uso, obteniendo la gráfica de los dispositivos: Switches, Servidores y APs más utilizados en las distintas características de recurso.

Top 10 en uso de Memoria



Figura 18 Top 10. Consumo de memoria en dispositivos de red

Top 10 en uso de CPU

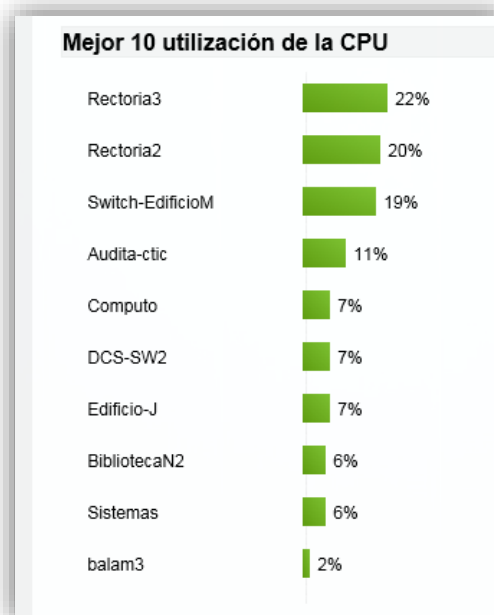


Figura 19 Top 10. Consumo de CPU en dispositivos de red.

Top 10 en uso de Disco

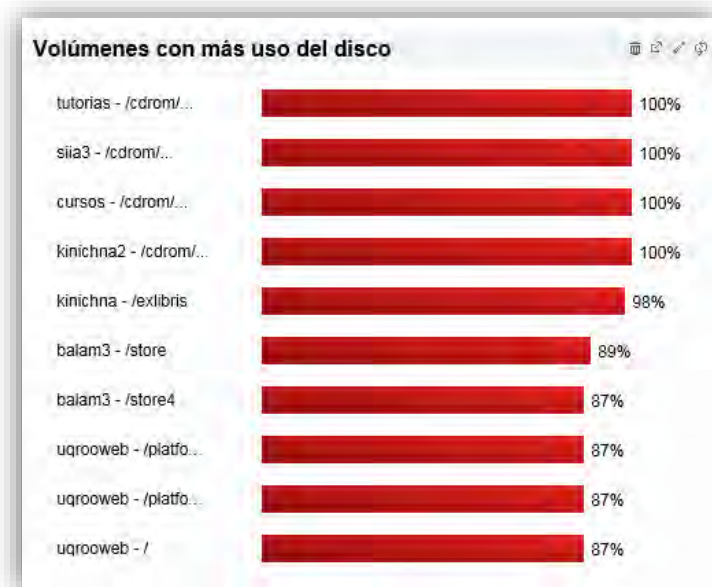


Figura 20 Top 10. Capacidad de disco en dispositivos de red

Nota: En cuanto al uso, se puede notar que los servidores son los dispositivos que más consumen sus recursos, puesto que son los que brindan los servicios de la Universidad.

A7: Evaluación del tráfico de red

Para el análisis del tráfico de la Red, se hizo uso de la aplicación Check Point, puesto que la Unidad ya cuenta con esta y sirve actualmente para vigilar el consumo de ancho de banda por protocolos. Además, cuenta con un apartado mediante el cual se configuran las políticas para asegurar la QoS.

Mediante la herramienta CheckPoint, se pudieron analizar las siguientes gráficas de consumo por protocolo:

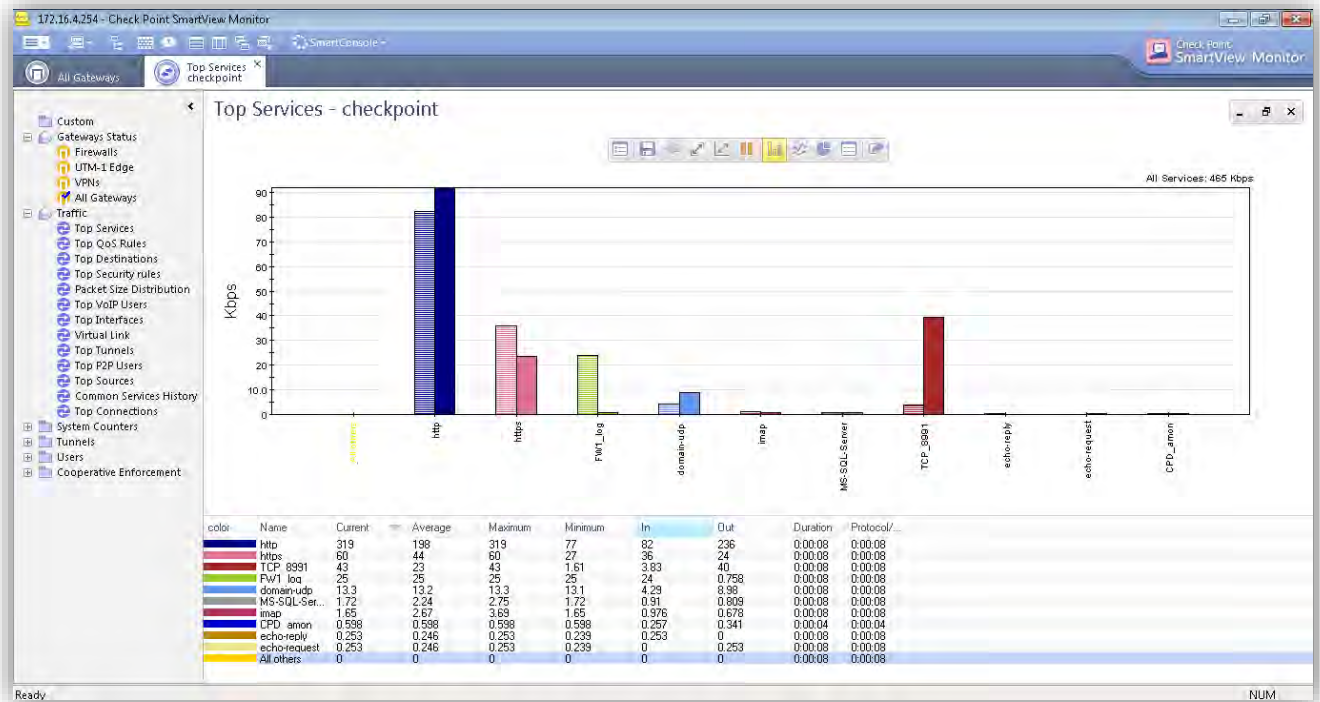


Figura 21 Top 10, Protocolos en el campus Chetumal

Siendo los de principal consumo, los protocolos HTTP y HTTPS. A su vez estos protocolos pudieron ser monitoreados de manera particular para analizar que usuario o usuarios estaban consumiendo y corriendo tales aplicaciones.

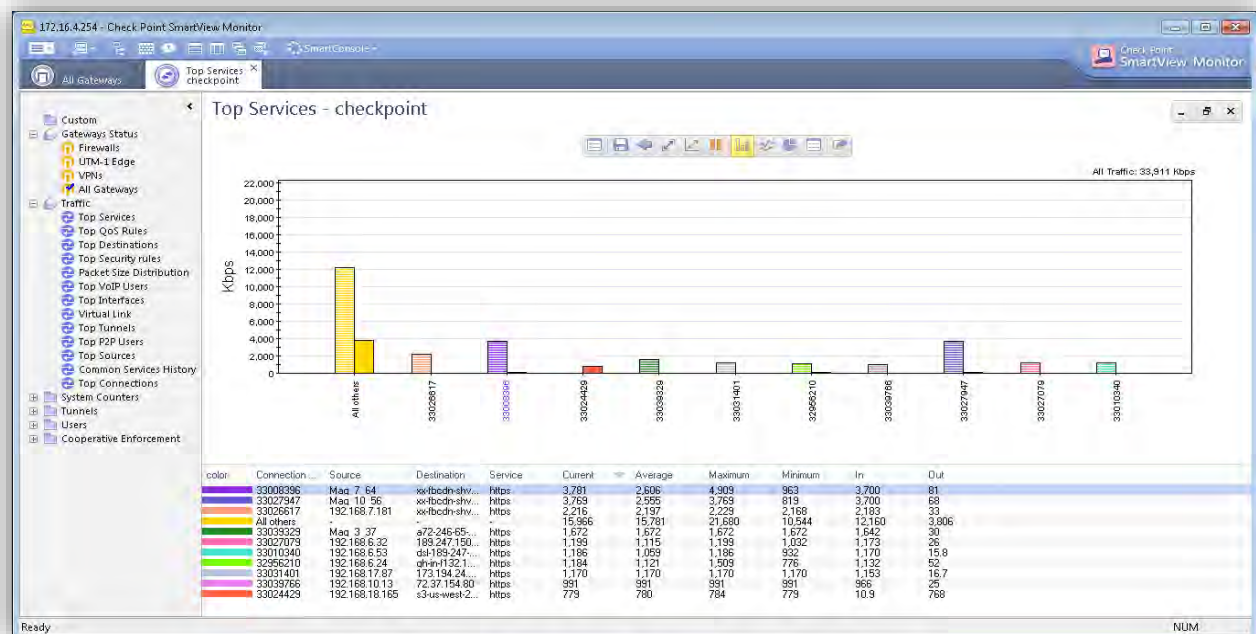


Figura 22 Top 10 Usuarios-Usos del Protocolo HTTPS.

Una vez finalizado el análisis del consumo de ancho de banda a través de protocolos, mediante la misma aplicación de Checkpoint, se pueden generar políticas o reglas de conexión para distribuir el consumo de ancho de banda o para limitar a ciertos usuarios su consumo en la red. Estas reglas, también pueden visualizarse a través de la aplicación.

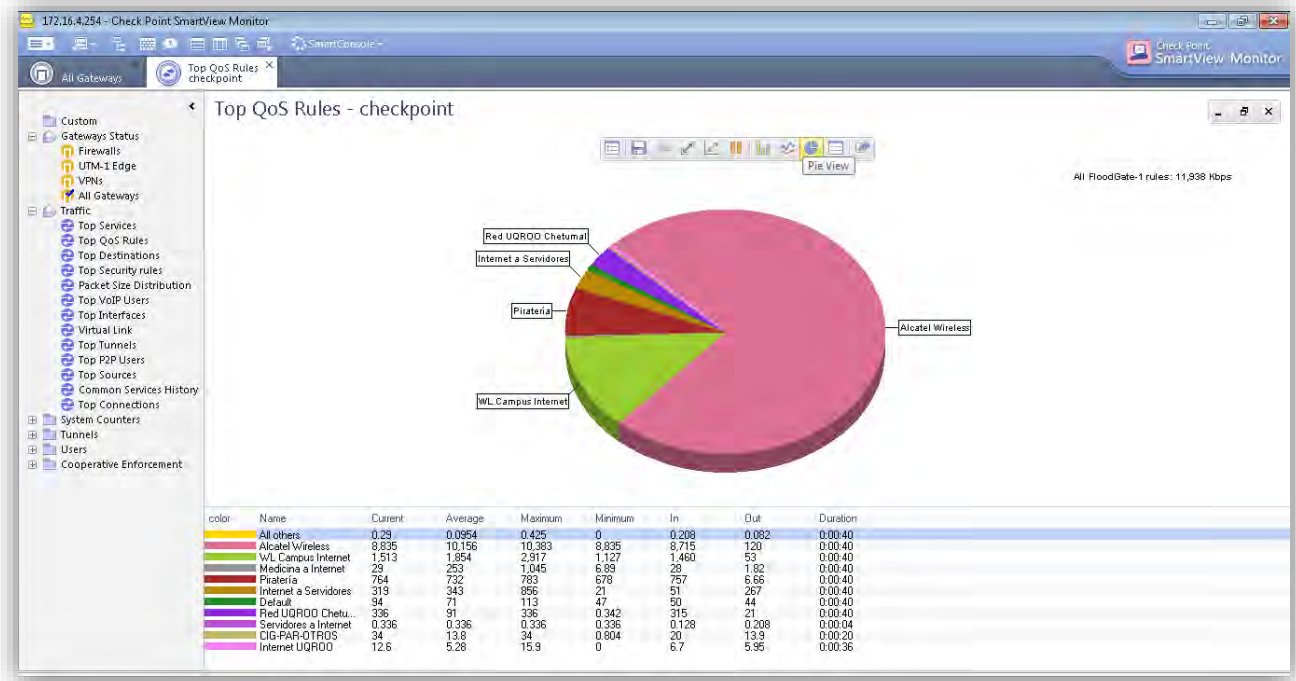


Figura 23 Reglas QoS en campus Chetumal

Algunas políticas ya han sido generadas por el administrador, pero es de vital importancia estar visualizando cotidianamente para tener un mejor control de los usuarios que consumen y generan más tráfico.

Con la herramienta Axence netTools, es posible verificar el consumo de ancho de banda por dispositivo, es decir, se puede visualizar el consumo de ancho de banda por Switch, y así conocer de manera más distribuida que dispositivos y segmentos de red consumen más.



Figura 24 Consumo de Ancho de banda

A8: Evaluación de los servidores de red

En el caso de los servidores, las herramientas NetCrunch y netTools fueron fundamentales. La primera para conocer las características del sistema, el estatus de flujo de tráfico en los servidores y sus interfaces, la segunda aplicación para medir el ancho de banda por servidor.

Analizando el rendimiento de los servidores

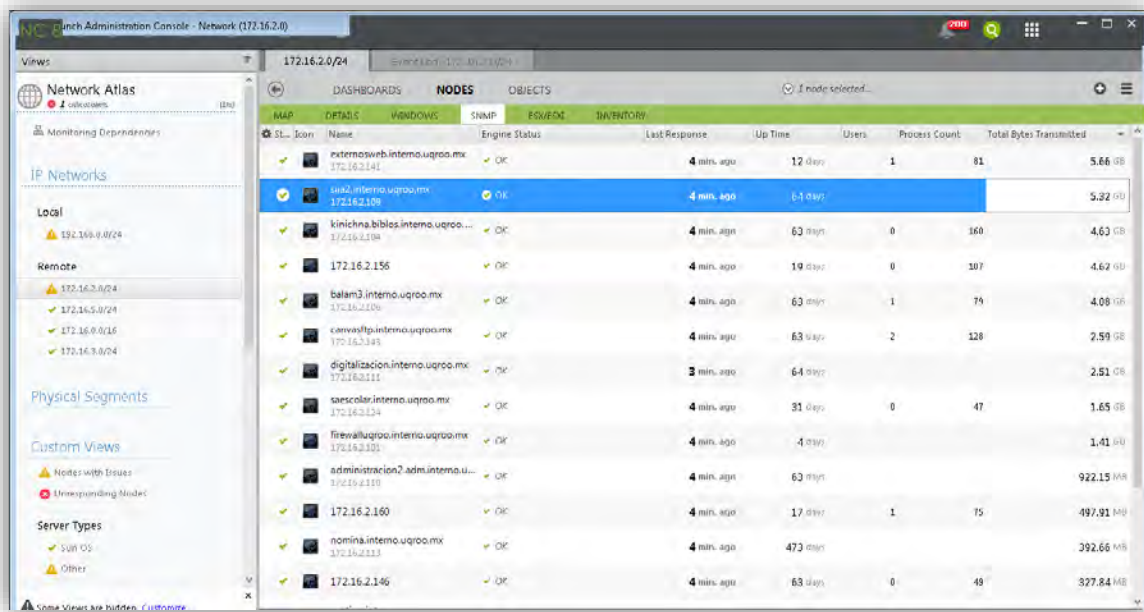


Figura 25 Monitoreo de Servidores en NetCrunch

Se analizan el uso de los servicios y consumo en las interfaces de cada servidor

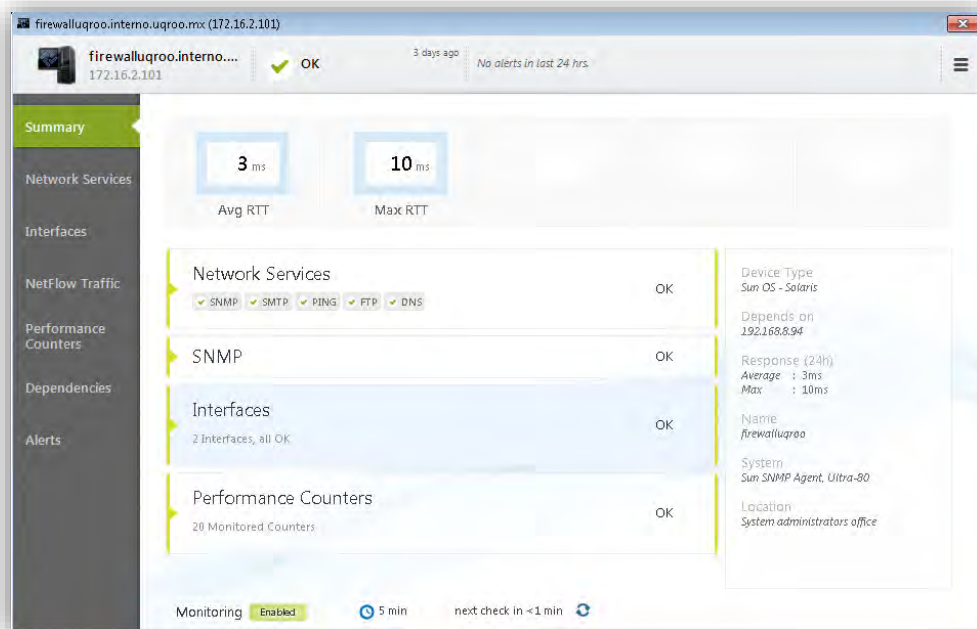


Figura 26 Ventana de detalles de monitoreo de Servidores

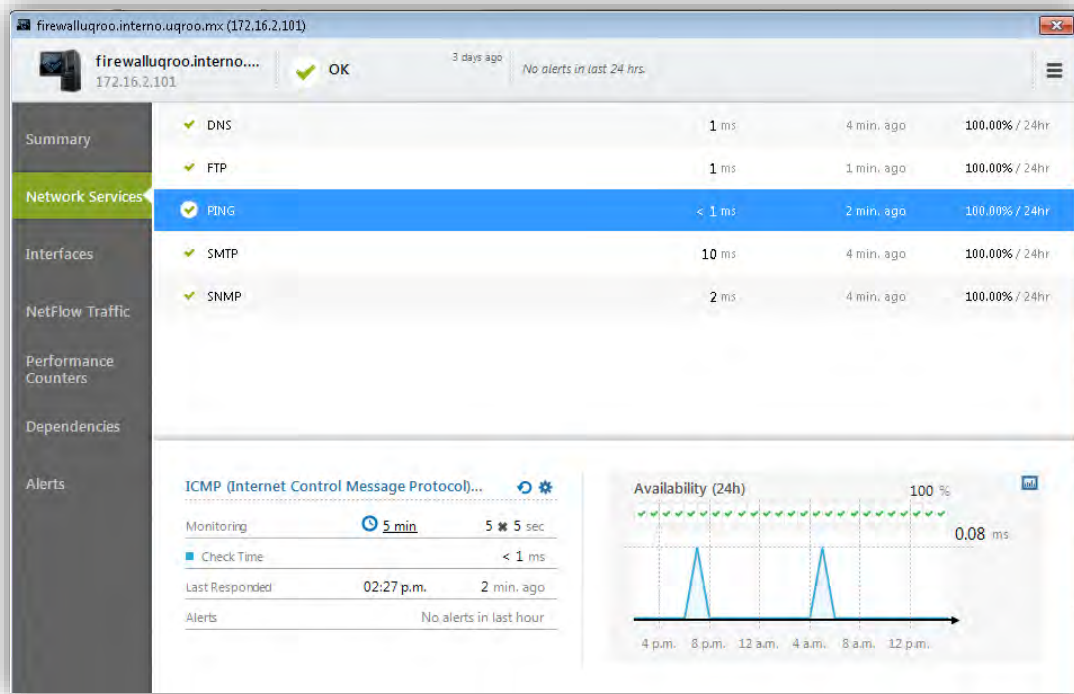


Figura 27 Servicios de red en Servidores

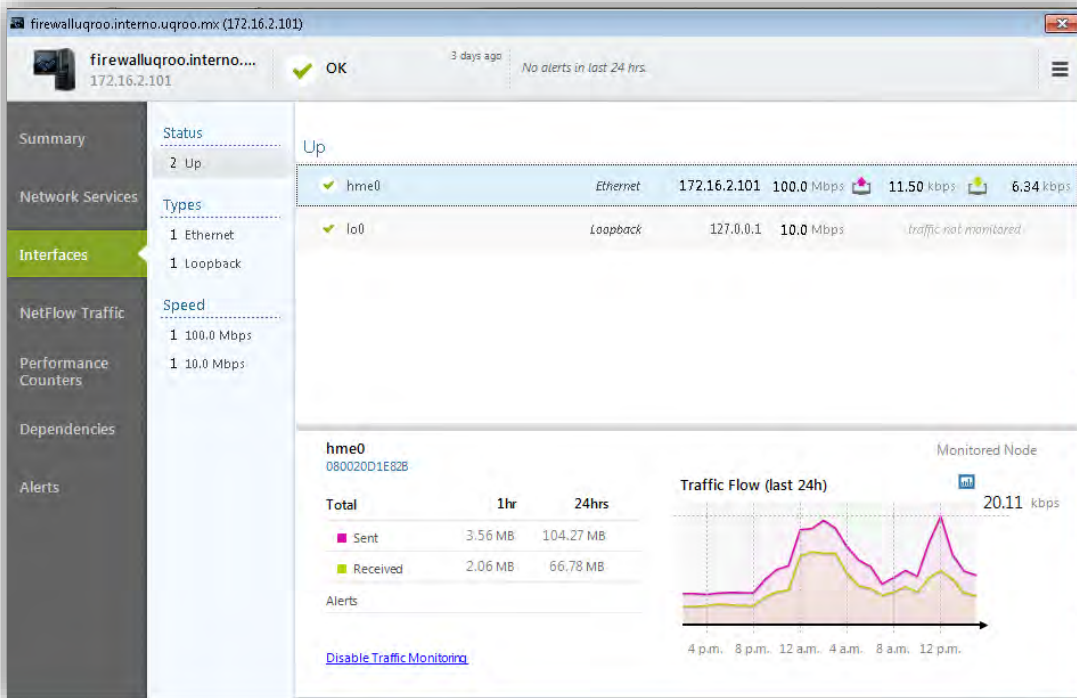


Figura 28 Flujo de tráfico en interfaces de Servidor

Mediante netTools se verifica el consumo de ancho de banda así como la recepción o pérdida de paquetes.

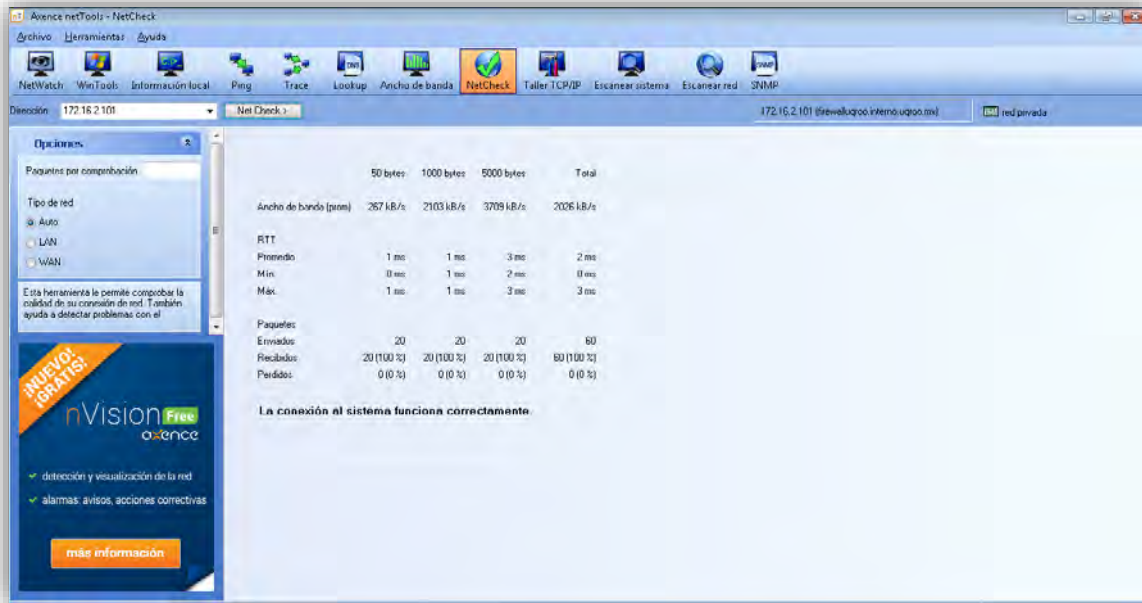


Figura 29 Consumo de ancho de banda en Servidores

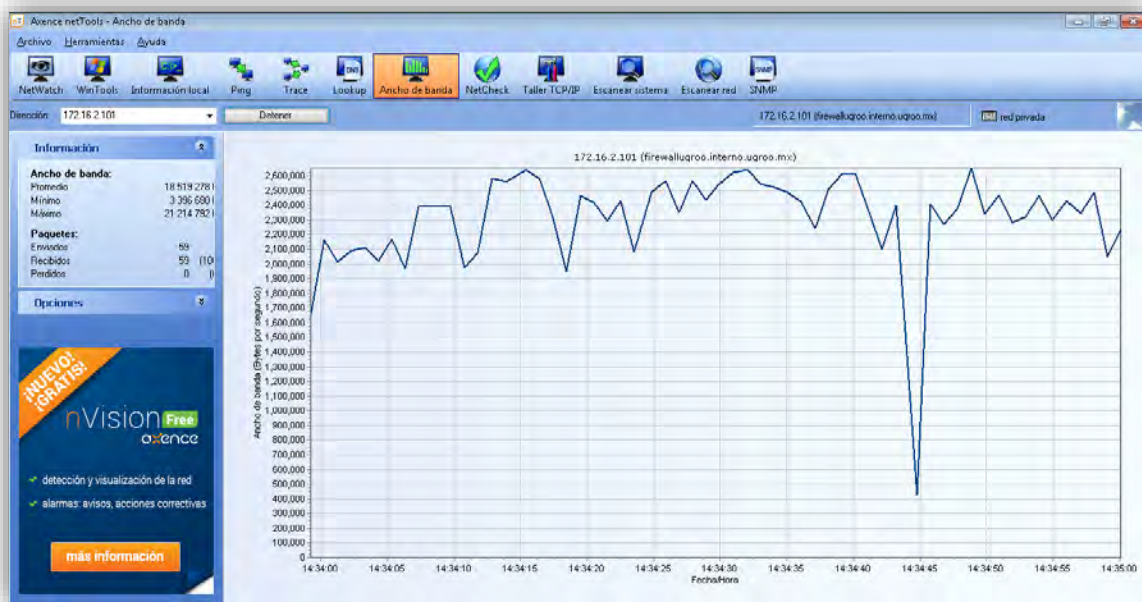


Figura 30 Gráfica de Consumo de ancho de banda en servidores

Mediante Op Manager se conocen los servicios altamente disponibles











Servicios por disponibilidad				
	Nombre del Dispositivo	Nombre de servicio	Disponibilidad (%)	
1	firewalluqroo	DNS		100 %
2	externosweb	MySQL		100 %
3	uqrooweb	MySQL		100 %
4	updown	MySQL		100 %
5	cursos	MySQL		100 %
6	moodle	MySQL		100 %
7	canvasftp	MySQL		100 %
8	sau	MySQL		100 %
9	kinichna	Oracle		100 %
10	siia3	Oracle		100 %

Figura 31 Servicios más solicitados

Servicios por tiempo de respuesta								
	Nombre del dispositivo	Nombre del servicio	Minu	Máx.	Prorr			
1	balam3	SMTP	1	722	3.73			
2	balam3	Web	1	3	1.00			
3	bidi	Web	1	2	1.00			
4	canvasftp	MySQL	1	3	1.50			
5	canvasftp	Web	1	4	1.00			
6	cursos	MySQL	1	3	1.32			
7	cursos	Web	1	4	1.00			
8	externosweb	MySQL	1	2	1.00			
9	externosweb	Web	1	3	1.41			
10	firewalluqroo	DNS	1	2	1.00			
11	firewalluqroo	SMTP	1	3	1.14			
12	gestion	Web	1	4	1.05			
13	kinichna	Oracle	1	3	1.00			
14	moodle	MySQL	1	2	1.45			
15	moodle	Web	1	2	1.00			
16	sau	MySQL	1	12	1.05			
17	sau	Web	1	2	1.14			
18	siia3	Oracle	1	2	1.41			
19	tutorias	Web	1	3	1.32			
20	updown	MySQL	1	3	1.09			
21	updown	Web	1	2	1.00			
22	uqrooweb	MySQL	1	14	1.18			
23	uqrooweb	Web	1	7	1.05			

Figura 32 Servicios por tiempo de respuesta

Es así como se conocen cada una de las características de los dispositivos y su uso y consumo en la red de datos de la Universidad. Una vez analizados los monitoreos y gráficas mostradas en cada aplicación, se procede a la resolución del Informe final a través de la fase de Dictamen de la Auditoría de Red.

5.2.3 Dictamen de la Auditoría

La elaboración del dictamen consiste en la elaboración del Informe final el que se presenta la descripción de las situaciones encontradas, las desviaciones y el punto de vista que se da con respecto a la evaluación.

Este informe se basó en el monitoreo y análisis de la red de datos, y conforme a la etapa de Mejora Continua del Servicio de ITIL donde indica que efectivamente, los tiempos modernos nos exigen continuos cambios y éstos deben tener un solo objetivo en el campo de la gestión de servicios TI: ofrecer mejores servicios adaptados a las siempre cambiantes necesidades de los usuarios-clientes y todo ello mediante procesos internos optimizados que permitan mayores retornos a la inversión y mayor satisfacción.

Pero este objetivo de mejora sólo se puede alcanzar mediante la continua monitorización y medición de todas las actividades y procesos involucrados en la prestación de los servicios TI:

- Conformidad: los procesos se adecúan a los nuevos modelos y protocolos.
- Calidad: se cumplen los objetivos preestablecidos en plazo y forma.
- Rendimiento: los procesos son eficientes y rentables para la organización TI.

De acuerdo entonces a esta fase es posible y con respecto a la auditoría realizada, se pudo; Recomendar mejoras para todos los procesos y actividades involucrados en la gestión y prestación de los servicios TI, los cuáles permitirán:

- Mejorar la calidad de los servicios prestados.
- Incorporar nuevos servicios que se adapten mejor a los requisitos de los clientes y el mercado.
- Mejorar y hacer más eficientes los procesos internos de la organización TI.

A continuación el informe se presenta en el Anexo D

Resultados obtenidos y recomendaciones

Resultados obtenidos

De acuerdo a la evaluación realizada, mediante la Auditoría de la red de la Universidad en el campus Chetumal, se obtuvieron los siguientes resultados.

Dispositivos de Comunicación y Servidores

- Diagrama físico de la red universitaria

Se diseñó el diagrama físico de la red actual, puesto que anteriormente se habían hecho cambios en el cableado y desplazamiento de algunos dispositivos; switches y APs.

Con este diagrama se obtiene una visualización completa de donde se encuentran físicamente los dispositivos y los enlaces de comunicación tanto Ethernet como fibra óptica.

- Diagrama lógico de la red universitaria

Se diseñó el diagrama lógico de la red actual, con este nuevo diagrama, y comparando con la metodología de diseño Top-Down de Cisco expuesta en el capítulo 3, se puede deducir que existe un diseño jerárquico y en capas, el cual proporciona a la red beneficios como: rendimiento, escalabilidad, facilidad de administración, facilidad de mantenimiento, redundancia y seguridad.

- Inventario de los dispositivos de comunicación y servidores existentes.

Utilizando la herramienta de administración y monitoreo WhatsUp Gold, se obtuvieron las características de los dispositivos principales en la red. Estos dispositivos fueron clasificados de acuerdo a su función, con lo cual se pudo obtener de manera cómoda la información de cada uno. Desde esta primera instancia, se supo que algunos dispositivos no contaban o no soportaban las credenciales SNMP actuales.

Además, se observó la inexistencia de VLANs en los Switches, todas las interfaces se encontraban en la VLAN por defecto: 1.

Rendimiento de los Dispositivos de Comunicación y Servidores

- Rendimiento a nivel sistema de Switches, APs y Router: Mediante el monitoreo de los dispositivos principales que permiten la comunicación a todos los usuarios en el campus Chetumal se obtuvo la captura de los principales dispositivos con más consumo de recursos en: memoria RAM, Uso de disco y CPU, según el caso.

Switches

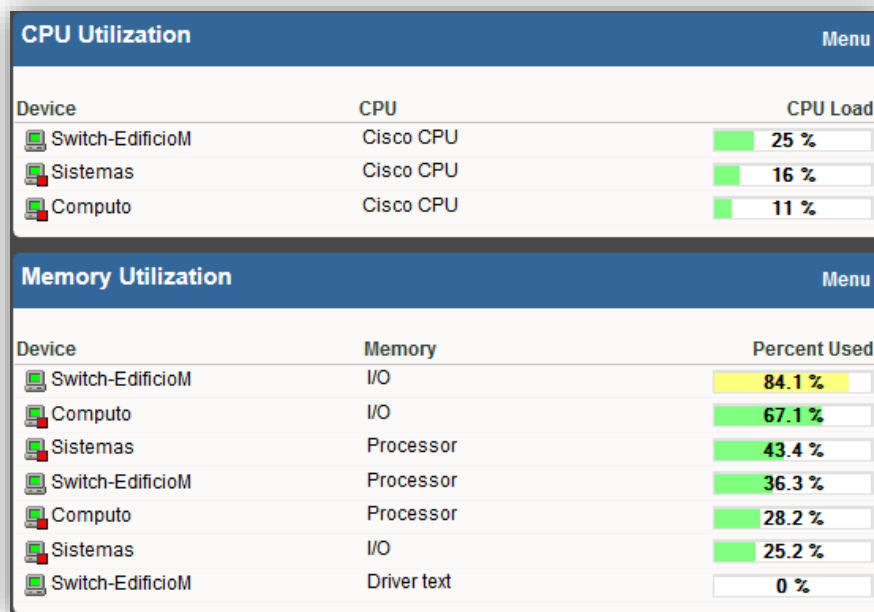


Figura 33 Rendimiento de Sistema -Switches

- Rendimiento a nivel sistema de Servidores: Se monitorearon los servidores para saber cuáles contaban con un mayor uso o consumo de sus recursos, ya que dependiendo de la capacidad física y el servicio que brinda cada servidor, es necesario saber si su desempeño va de acuerdo a los procesos que se generan en ellos.



Figura 34 Uso de disco-Servidores



Figura 35 Utilización de CPU-Servidores



Figura 36 Uso de Memoria-Servidores

Con la información recopilada se pudo sustentar la revisión de los dispositivos con mayor consumo de recursos y así realizar cambios y adiciones.

Las siguientes tablas muestran los dispositivos añadidos a la red del campus Chetumal de acuerdo a las necesidades expuestas mediante la Auditoría de red.

Switches

Ubicación	Marca	Modelo	# Dispositivos	Costo Unitario
Edificio A Rectoría	Cisco	2960S	3	\$32 500 MX
Edificio F Talleres	Alcatel	OS6450-48	1	\$61 100 MX
DCS	Cisco	2960S	3	\$32 500 MX
	Alcatel	OS6450-24	1	\$21 739 MX
Edificio L	Alcatel	OS6450-24	2	\$21 739 MX
	Cisco	2960S	1	\$32 500 MX
Campus Cozumel	Cisco	4500	1	\$58 900 MX
Campus Playa del Carmen	Cisco	2960S	1	\$32 500 MX

Tabla 6 Adición de Switches a la red UQROO

APs

Campus	Marca	Función	Modelo	# APs	Costo Unitario
Chetumal	Alcatel	AP	105	10	\$5 096 MX
	Alcatel	Controladora de APs	105	1	\$5 096 MX
Playa DC	Alcatel	AP	105	2	\$5 096 MX
	Alcatel	Controladora de APs	105	1	\$5 096 MX
Cozumel	Alcatel	AP	105	2	\$5 096 MX
	Alcatel	Controladora de APs	105	1	\$5 096 MX

Tabla 7 Adición de APs a la red UQROO

Servidores

Ubicación	Marca	modelo	# Dispositivos	Costo Unitario
Edificio O - CTIC	Cisco	UCS C240	2	\$35 110 MX

Tabla 8 Adición de Servidores a la red UQROO

Rendimiento en el tráfico de red

- Se realizó el monitoreo del tráfico de red para obtener el consumo total, el consumo por protocolo, el consumo por red, en este caso de los switches, ya que son los que proporcionan el acceso a todos los usuarios en la red.

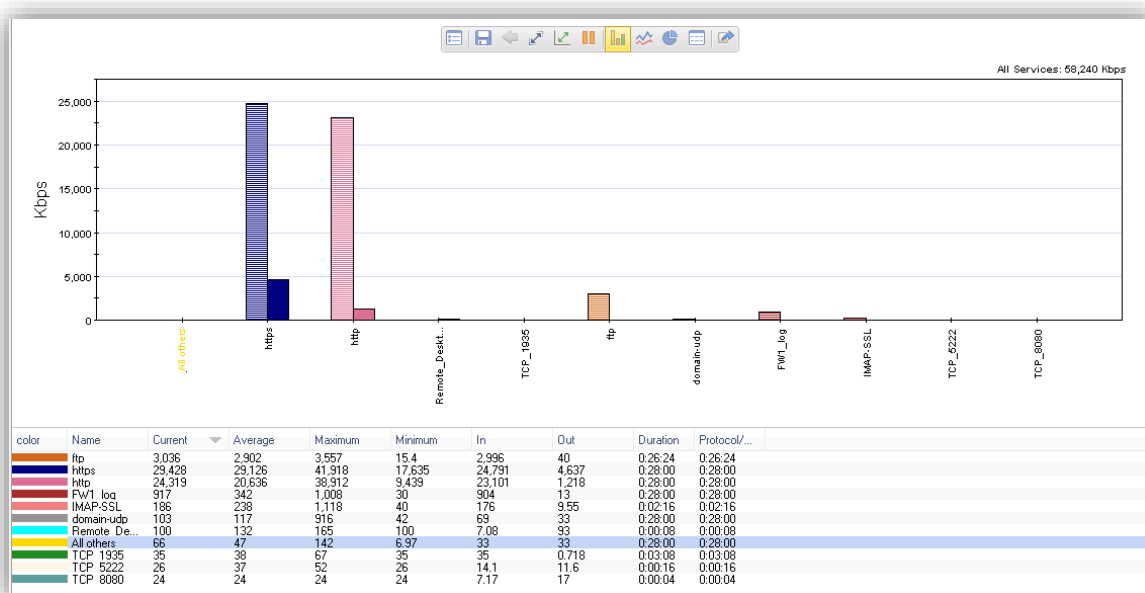


Figura 37 Protocolos de red más consumidos



Figura 38 Medición de ancho de banda

Viendo el aumento en las conexiones se destacó la importancia de aumentar el ancho de banda en cada campus de la Universidad y los enlaces MPLS. Con un aumento en el ancho de banda había la posibilidad de generar más transacciones en la red, y aumentaría la velocidad.

- Junto con el aumento en el ancho de banda, se analizó la necesidad de controlar las conexiones a través de políticas QoS para asegurar el rendimiento en el uso del tráfico. Algunas políticas ya han sido configuradas, pero existe la necesidad de conformar aún más.

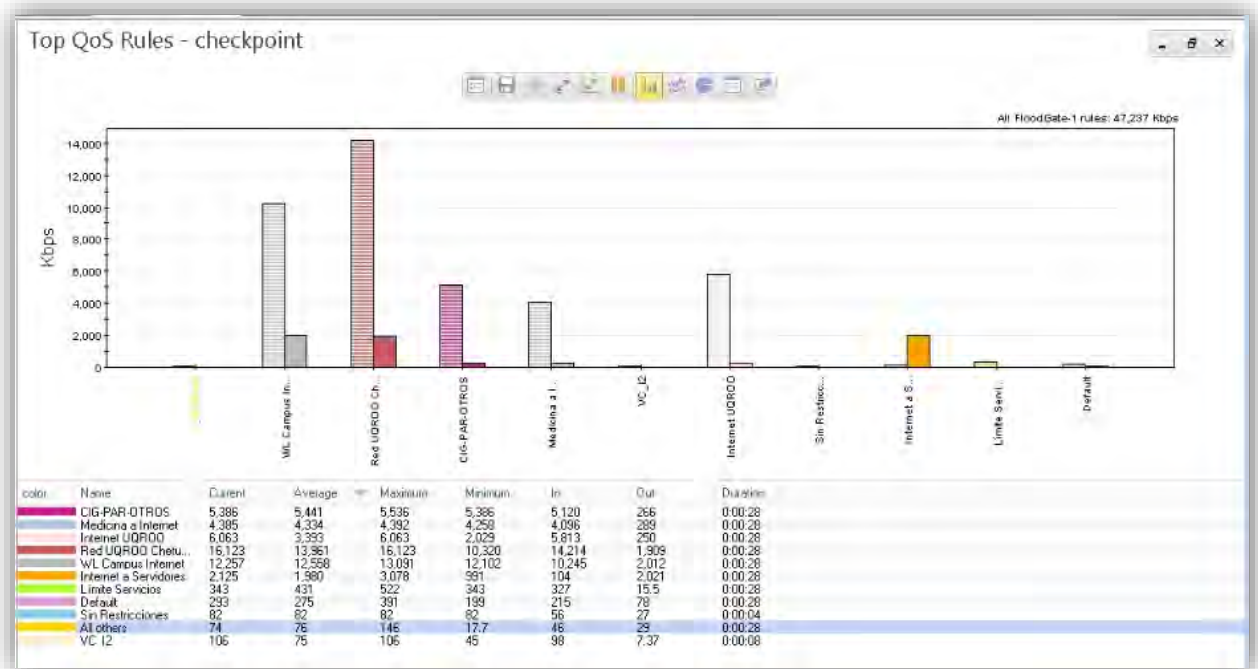


Figura 39 Top 10. Reglas QoS en la UQROO

- En cuanto al uso de protocolos de red, se generaron las gráficas de consumo, ya que de esta forma se toman parámetros para crear las políticas de QoS. Hasta el momento la siguiente gráfica muestra el consumo en Kbps de las políticas creadas por el administrador actualmente:

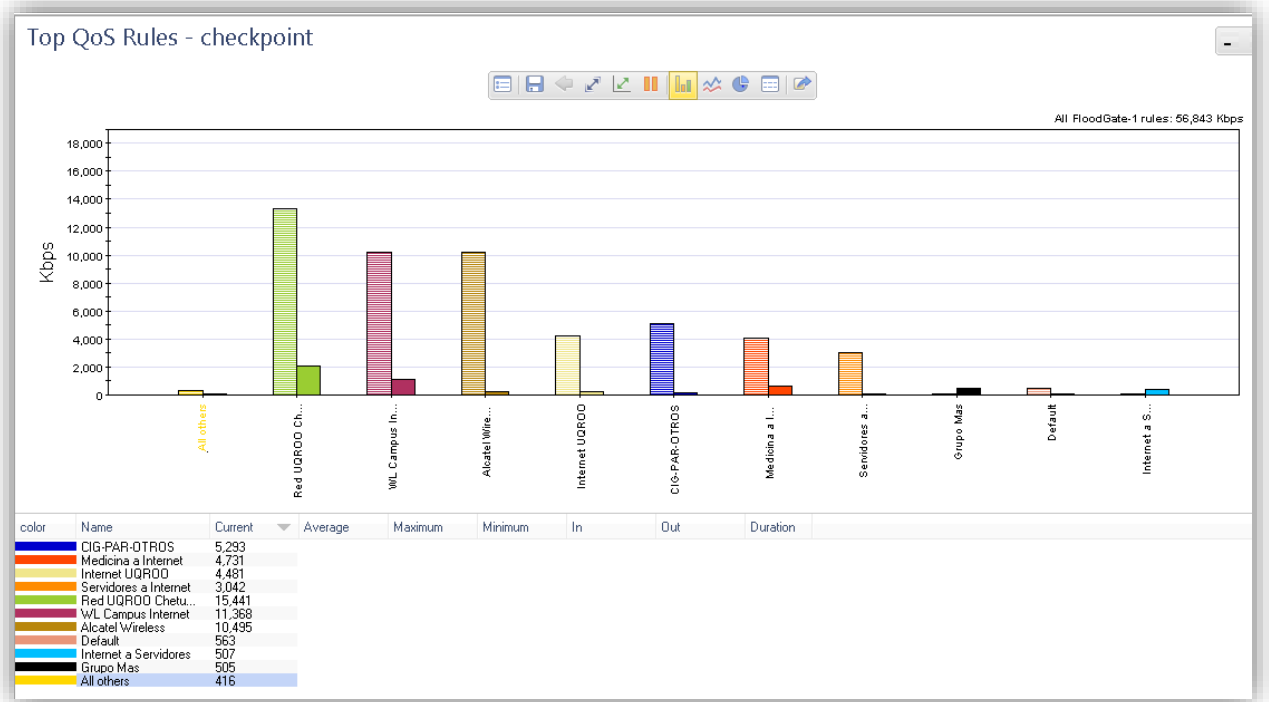


Figura 40 Top 10. Reglas QoS en la UQROO_2

Recomendaciones

De acuerdo a los resultados obtenidos de la Auditoría de red, de la Universidad en el campus Chetumal, se proponen los siguientes como recomendaciones para las situaciones encontradas.

- Como se ha promovido en capítulos anteriores, la aplicación de una Auditoría no sólo implica la detección de errores o fallas, es mucho más que eso, se realiza con la finalidad de mejorar la eficiencia y eficacia de una organización. Con la aplicación de Auditorías constantes a la infraestructura de la red Universitaria en cualquiera de sus campus, mejorará las condiciones y el

mantenimiento de los principales dispositivos de comunicación, además de perfeccionar los controles calidad, el nivel de los servicios y el procesamiento de la información que viaja a través de esta.

2. La red universitaria en el campus Chetumal ha crecido en número de usuarios y servicios, por ello es necesario el aumento de la capacidad de transferencia en la comunicación. Un aumento de ancho de banda daría una mejor disponibilidad y estabilidad en los servicios y en el flujo del tráfico.
3. Aunado al aumento de ancho de banda, se requerirá de un mejor control del tráfico y de la implementación de políticas para aumentar la QoS, para ello es importante, monitorear constantemente cuáles son los protocolos, servicios y aplicaciones que más consumen tráfico, así como los usuarios, segmentos y dispositivos que hacen uso desmedido de éste.
4. No existe una administración totalmente centralizada. A pesar de contar con el software adecuado no todos los dispositivos son monitoreados, debido a la discontinuidad en el uso del protocolo SNMP actual en dispositivos “antiguos”. Se necesita de la actualización de equipos, ya sea en software si es el caso, o con el reemplazo a equipos más actuales. Con esto se pretende que al haber alguna problemática, se sepa inmediatamente de donde proviene a través de la herramienta.
5. Existe un solo dominio de broadcast, por lo que falta definirlos a través de la configuración de VLANs.
6. No existe la configuración de VTPs hasta el momento, por lo que se requiere de la implementación de éstas redes para hacer más segura la comunicación entre los campus de la Universidad, ya que es la forma en la que se podría manejar remotamente el soporte y mantenimiento a otros dispositivos de red. Siendo el campus Chetumal, el punto central y de conexión de todas las redes de datos de la Universidad de Quintana Roo.
7. Aunque existen actualmente más dispositivos de acceso inalámbrico, estos todavía no alcanzan los lugares donde existe demanda de conectividad.

Conclusiones

Conclusiones

La información en la actualidad es el activo máspreciado de toda Institución, en el caso de la UQROO en su campus Chetumal, este activo es esencial para brindar la comunicación a los usuarios. Mediante una sólida infraestructura de red, es posible ir mejorando algunos aspectos, sobre todo en el ámbito de la prestación de servicios y el rendimiento de las actividades realizadas a través de plataformas, aplicaciones, entre otros.

Todos los servicios se generan y distribuyen a través de dispositivos de comunicación, y estos a su vez tienen la responsabilidad de dar soporte a los mismos.

Por eso es fundamental que toda infraestructura de red sea evaluada constantemente para conocer el estado de los mismos, observando la configuración, administración y a su vez recomendando el reemplazo o modificación de aquellos aspectos que disminuyen el nivel de los servicios y la comunicación. Con una Institución como la Universidad de Quintana Roo, es imposible generar estas evaluaciones ya que no existen personas totalmente dedicadas al monitoreo diario de la red. A través de la Auditoría y de la implementación de herramientas de monitoreo se pudo constatar de cómo se encontraba la red en aspectos técnicos, de soporte, administración y control. Como una institución de nivel superior es importante tener una base fuerte de TICs, ya que de esto depende la imagen de la Universidad, la confianza en los usuarios sobre la seguridad y control de los servicios de TI, la optimización de procesos en el área de redes y soporte, la disminución de errores, fallas, la atención ante cualquier problema con los dispositivos de red, todo con la finalidad de disminuir la pérdida de tiempo y dinero al momento de solucionar problemas relacionados con la infraestructura de red.

Al utilizar el descubrimiento de la dispositivos a través de SNMP, como método de monitoreo de la red, se constató cuán importante es la obtención de dispositivos que cubran con los requerimientos a futuro de la universidad, ya que algunos dispositivos por los años de adquisición son obsoletos a la hora de administrarlos,

y como característica importante de todo diseño de red, es la posibilidad de tener una administración centralizada.

Al utilizar diversas herramientas de monitoreo de red gratuitas y por tiempo de evaluación, se comparó que el resultado concordará con las aplicaciones de Check Point y WhatsUp Gold, puesto que éstas son aplicaciones adquiridas por la Universidad y ya habían sido previamente instaladas y configuradas. Con esto se pudo corroborar que los datos obtenidos de la Auditoría eran reales. En este punto de selección de herramientas fue fundamental conocer a ciencia cierta cuáles eran los datos que importaba conocer y con esto adquirir de manera gratuita el software que se adaptará a las necesidades de la guía de la Auditoría.

Finalmente y como punto fundamental de este trabajo, conlleva que al realizar una Auditoría de red es importante diseñar una metodología que se rija por directrices, estándares y guías para las buenas prácticas asociadas a la Auditoría, ya que de esto depende el desarrollo y el dictamen de los resultados obtenidos con base en el trabajo realizado. En el caso personal fue la sustentación de 2 estándares, COBIT e ITIL, en los cuáles se basó la implementación de la Auditoría a la red Universitaria. Fue también muy importante conocer a profundidad de qué trataba cada estándar, conocer su marco de referencia y con base en ello, seleccionar los procedimientos que se adecuarán a una Auditoría de red.

Una vez expuesto la metodología fue mucho más fácil poder llevar a cabo cada actividad propuesta en el plan y así concluir con un informe ejecutivo, en el cual se infunden las situaciones encontradas así como el punto de vista personal sobre los resultados de la Auditoría de red.

Resumiendo cada punto y como conclusión al desarrollo de la Auditoría de Red se exponen los siguientes puntos:

1. La red de la Universidad de Quintana Roo no es homogénea en cuanto a marcas y modelos de dispositivos.
2. Existen algunos principales dispositivos de comunicación que proporcionan acceso a la red de datos universitaria y no soportan el protocolo SNMP.
3. La administración de los dispositivos de red de la Universidad de Quintana Roo en el campus Chetumal no es centralizada.
4. El diseño lógico y físico de la red no presenta inconsistencias y cuenta con un diseño jerárquico, además de inexistencia de direcciones desperdiciadas,
5. La configuración de políticas para asegurar la QoS es tediosa, y que plantea un monitoreo constante y especializado.
6. No se cuenta con herramientas de monitoreo especializadas en aplicaciones, o con las que se cuenta, no cuentan con los módulos para aplicar ciertas políticas configuraciones de seguridad y administración en la red.
7. De acuerdo a la metodología propuesta: COBIT e ITIL no proporcionan una estructura formal y específica de cómo desarrollar un plan de auditoría y su ejecución posterior, sino que ofrecen una serie de guías de cómo realizar el análisis y evaluación de las TICs, en el área correspondiente y de acuerdo a los puntos a evaluar según los requerimientos de la organización a auditar.
8. De igual manera, no siempre la documentación, las guías y los procesos de estos dos estándares coinciden exactamente con la Auditoría a realizar, de aquí el trabajo de investigación y la documentación adicional analizada para poder llevar a cabo una Auditoría de este tipo y combinando características de éstos 2 modelos.
9. La red de la Universidad de Quintana Roo no cuenta con un plan de Auditoría constante para evaluar y diagnosticar la infraestructura de las TICs. Y con la cual se tenga información actual del estado de la red, sus componentes y los procesos que se generan con el tiempo.

Trabajos a futuro

Con los resultados de un Informe de Auditoría de Red se pueden realizar los siguientes trabajos:

- Reingeniería de red de datos: Toda base de Reingeniería de red de datos conlleva la realización de una Auditoría de la red previa, ya que esta requiere del estudio del estado actual para luego aplicar metodologías de cambios, implementaciones, modificaciones, entre otros para implementar un nuevo concepto de la red de datos a cambiar.
- Generación de reportes y solución de problemas: En casos particulares, pueden generarse monitoreos y reportes sobre un aspecto en especial de la red, y que requiera del soporte constante. Con esto poder generar manuales para solución de problemas o prevención de éstos.
- Implementación de mejoras en la red de datos: Para cualquier organización es o deber ser vital aplicar cambios que mejoren el desempeño de los procesos, servicios, gestión y sobre todo de la seguridad de la información que fluye a través de cada dispositivo de red sobre una infraestructura de red de datos. Para poder saber qué cambios o implementaciones a realizar en cuanto a configuraciones, conexiones o dispositivos, es necesario conocer el estado actual de la red y si el funcionamiento de los recursos es óptimo o no, para fundamentales tales implementaciones.

Anexos

Anexo A:

Instalación de Axence netTools

Descripción: Kit de herramientas gratuitas para escanear, monitorear y administrar redes. Axence NetTools incluye 10 herramientas tales como escáner de red, listado de conexiones entrantes y salientes del equipo, escáner de puertos, etc. Entre muchas otras funciones, este programa ofrece las siguientes:

- Monitoreo de la disponibilidad y tiempo de respuesta de múltiples sistemas.
- Notificaciones (vía email, mensaje de texto SMS, sonido) en caso de problemas con la disponibilidad del sistema.
- Gráficos actuales e históricos de los tiempos de respuesta y del porcentaje de paquetes perdidos.
- Exportación de datos a XML, HTML, TXT.
- Monitoreo del tiempo de respuesta y el porcentaje de paquetes perdidos para HTTP, POP3, SMTP, FTP y 50 servicios más.
- Monitoreo de cualquier puerto TCP.
- Identificación de sistemas en base a DNS; verificación automática de direcciones cada 10 minutos.
- Exportación/ importación de sistemas.
- Soporte a protocolos TLS/SSL en emails de alerta.
- Escáner de red, puertos y servicios.
- Vista de procesos y servicios activos
- Diagnóstico de servicios TCP/IP y navegador SNMP
- Traceroute

Asimismo incluye las siguientes herramientas:

- NetStat: listado de conexiones entrantes y salientes, así como de puertos abiertos.
- Información local: tablas con información sobre la configuración local: estadísticas de TCP/UDP.

- Lookup: registros DNS y WHOIS
- Ancho de banda: evaluación del ancho de banda de la red
- NetCheck: comprobación de la calidad de los equipos y del cableado de la red

Requerimientos de sistema

Sistema Operativo: Win98/NT/2000/XP/2003/Vista/2008/7/8

RAM: 3 Gb mínimo

Disco duro: 30 Gb mínimo

Procesador: 2 núcleo

Instalación de Axence NetTools

1. Descargue la aplicación desde la página Oficial: <http://cdn.axence.net/netToolsSetup.exe>
2. Ejecute la aplicación, y a continuación, seleccione el idioma de su preferencia

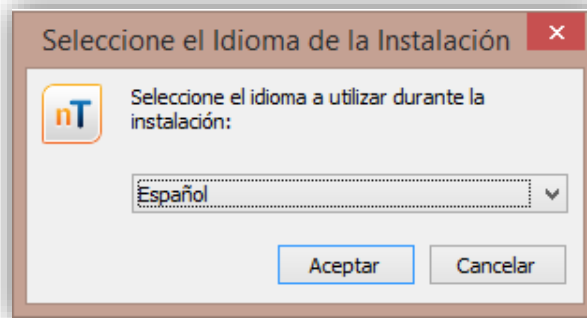


Figura 41 Instalación de netTools_Selección de Idioma

3. Se abrirá el asistente de instalación. Seleccione "Siguiente".

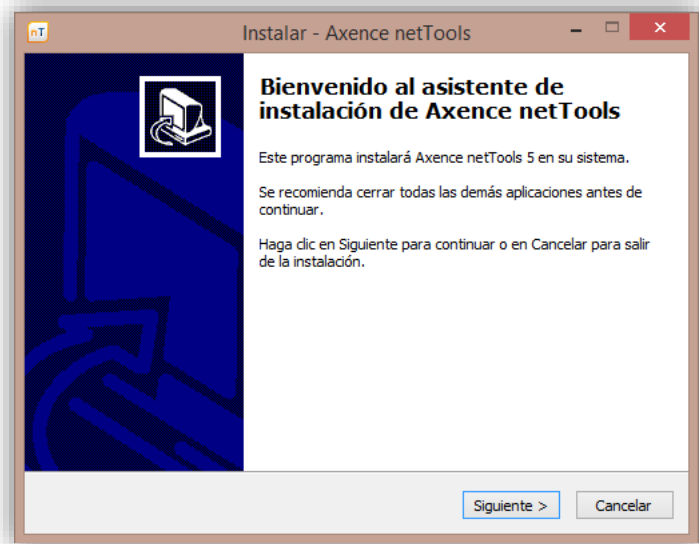


Figura 42 Instalación de netTools. Asistente

4. Acepte las condiciones de Licencia, y después la opción “Siguiente”.

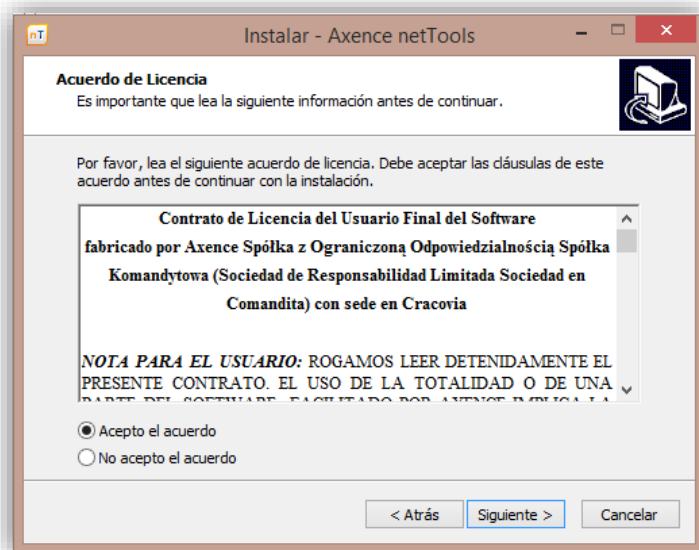


Figura 43 Instalación de netTools. Licencia

5. Seleccione la ruta en la que se guardarán los archivos de la aplicación, seleccione “Siguiente”.

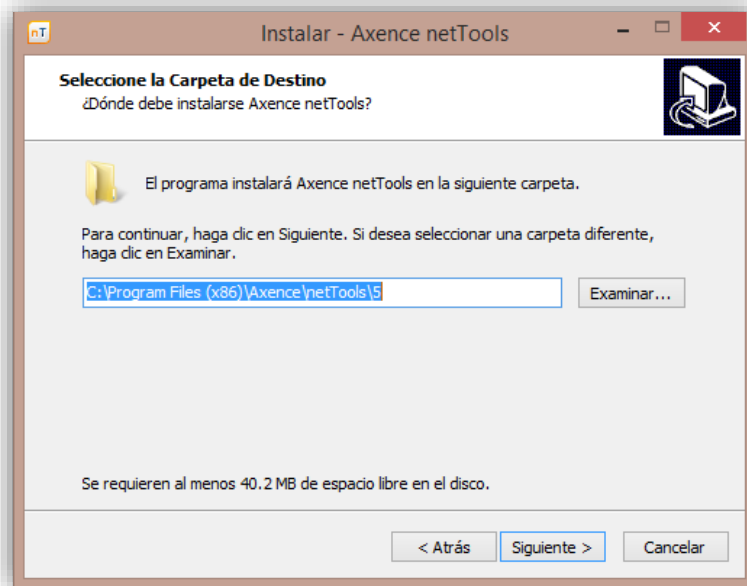


Figura 44 Instalación de netTools. Carpeta de destino

6. Seleccione el lugar donde se crearán los accesos directos de la aplicación, seleccione “Siguiente”

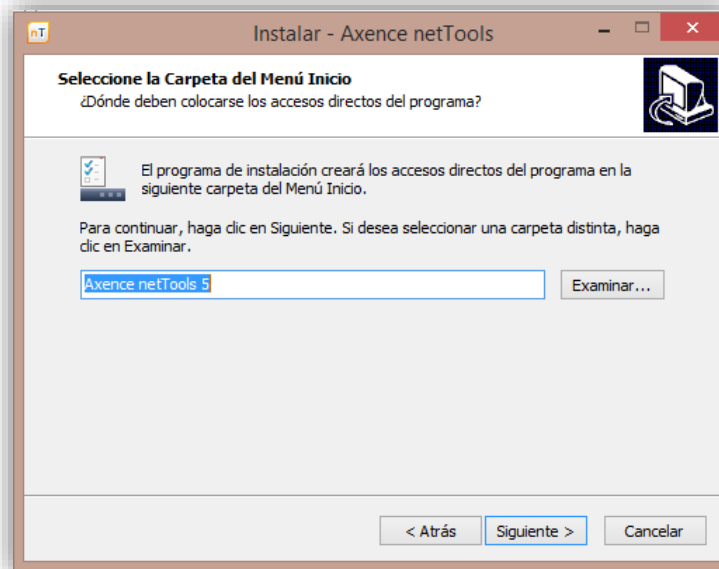


Figura 45 Instalación de netTools. Acceso directo

7. Puede seleccionar la opción de crear un icono de la aplicación en el escritorio, seleccione “Siguiente”

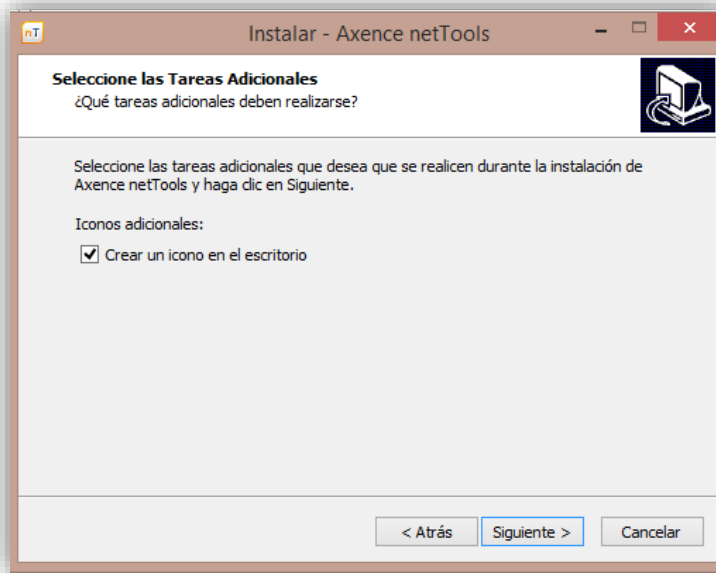


Figura 46 Instalación de netTools. Icono en Escritorio

8. Finalmente se selecciona la opción de “Instalar”.

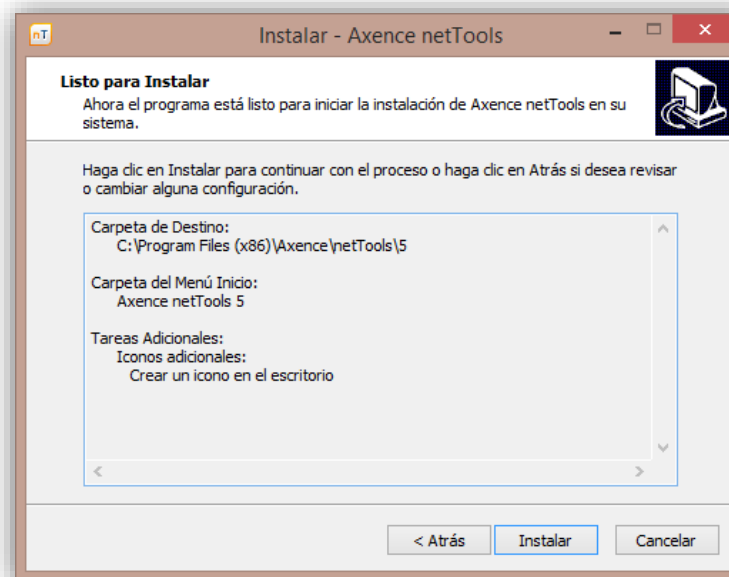


Figura 47 Instalación de netTools. Finalización

En algunos casos, se solicita agregar la aplicación al firewall para que permita el uso de funciones de monitoreo saliente y entrante

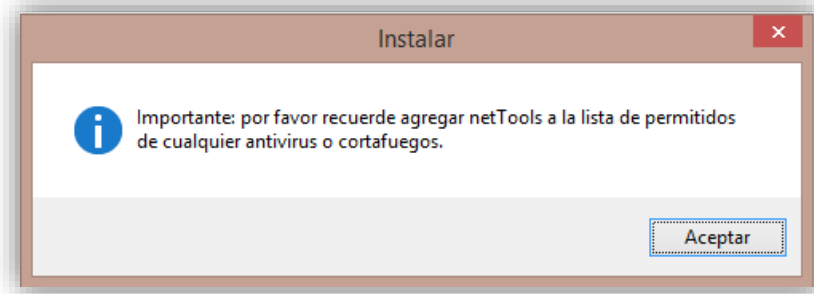


Figura 48 Instalación de netTools. Aviso

Detalles del entorno

NetTools contiene las siguientes herramientas dentro de su entorno gráfico:

- NetWatch, para monitorear la disponibilidad de hosts.
- WinTools, para ver qué tiene instalado algún equipo en la red.
- NetStat, revisa los servicios de entrada/salida de la red en la que se encuentra el equipo.
- Local info, una tabla con información detallada del equipo local.
- Network scanner, un escáner de red para ver los nodos de red.
- Service & port scanner, para ver los servicios y puertos activos.
- TCP/IP workshop, prueba diferentes servicios de red.
- SNMP Browser y otras herramientas para lanzar Trazas, Pings, etc.

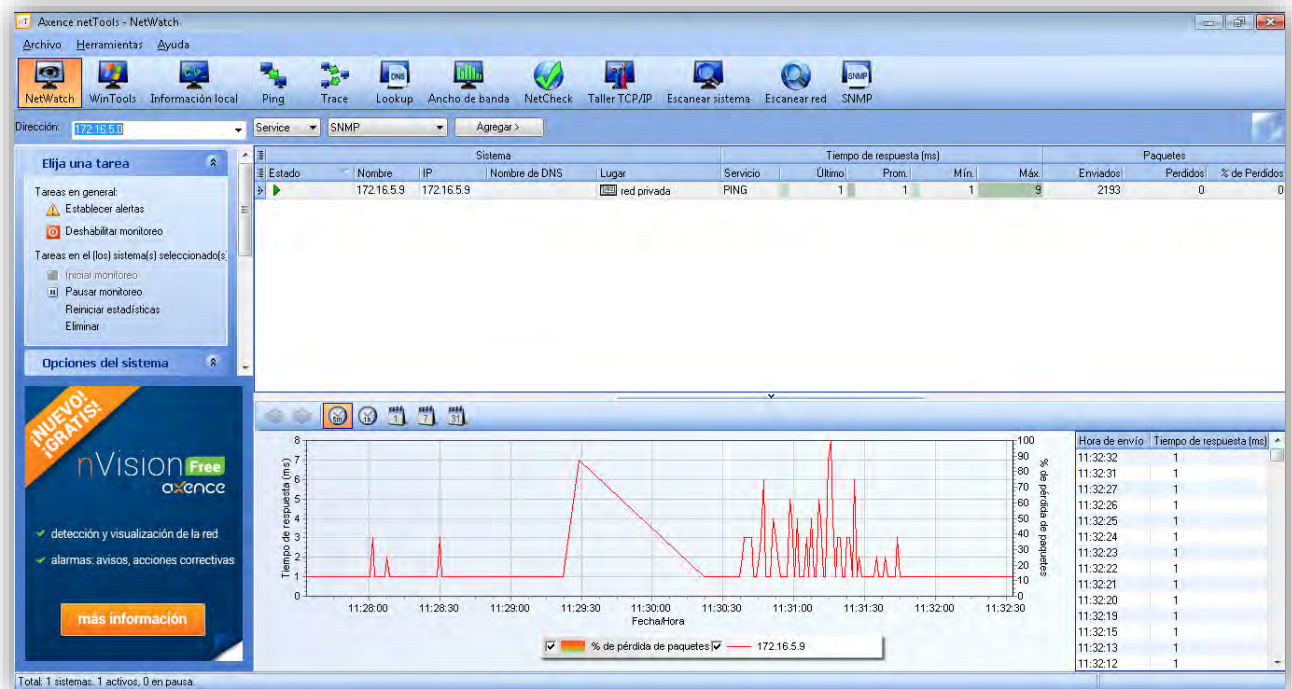


Figura 49 Entorno gráfico de netTools

El entorno de NetTools es muy amigable, simplemente basta con conocer los segmentos de red y el direccionamiento de los dispositivos principales a monitorear. Aplicando estas direcciones IP en cada uno de los campos de monitoreo especializado se obtuvieron las gráficas de los dispositivos expuestas en el Desarrollo de la Auditoría.

Anexo B: Instalación y configuración de OpManager

Descripción: OpManager es una plataforma de monitorización de infraestructuras, redes, servidores y aplicaciones, que ofrece una funcionalidad avanzada para monitorizar los recursos críticos de TI tales como routers, enlaces WAN, switches, firewalls, VoIP, servidores físicos, servidores virtuales, controladores de dominio y otros dispositivos de infraestructura de TI.

Requerimientos del sistema:

# dispositivos/interfaces	Procesador	RAM	Capacidad libre en disco duro	Sistemas Operativos Soportados
Hasta 50 dispositivos o 30 interfaces	1.7 Ghz	1 GB	40 GB	Windows: 2012, 2008, 2003 Server, Vista, 2000 Professional+SP4, XP Professional.
Hasta 300 dispositivos o 2000 interfaces	3.4 Ghz	2 GB		
Hasta 1000 dispositivos o 5000 interfaces	2 * 3.4 Ghz	4 GB	80 GB	Linux: RedHat 7.x and above, Debian 3.0, Suse, Fedora & Mandrake
Más de 1000 dispositivos o 5000 interfaces	4 * 3.4 Ghz	8 GB		

Instalación

Se descargó la versión de prueba del programa OpManager, ya que sólo se requería de unas semanas de monitoreo. Esta versión constaba de 30 días de evaluación.

1. Se descargó la versión Essential 64 bits, para más de 500 dispositivos, del siguiente link <http://www.manageengine.com/network-monitoring/download.html>

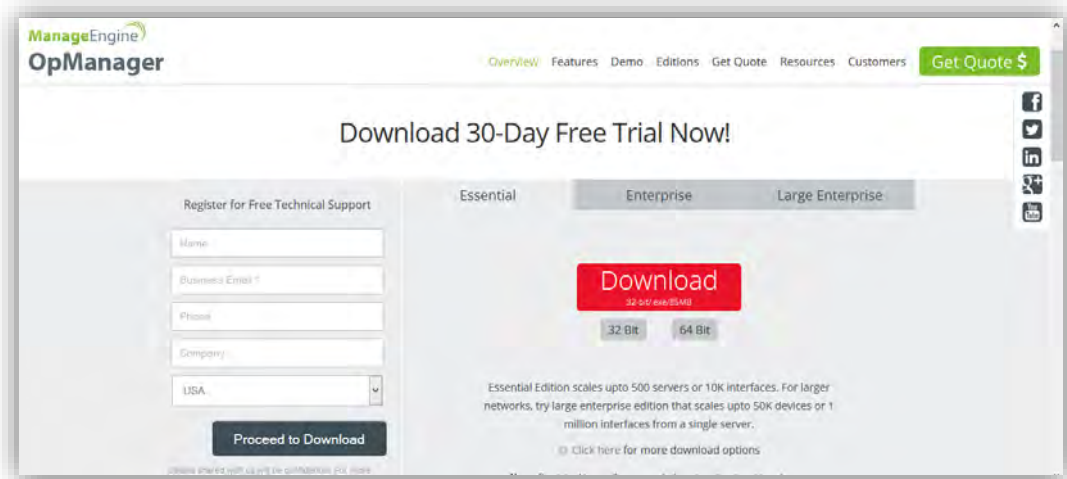


Figura 50 Descarga de OpManager

2. Ejecución del programa OpManager

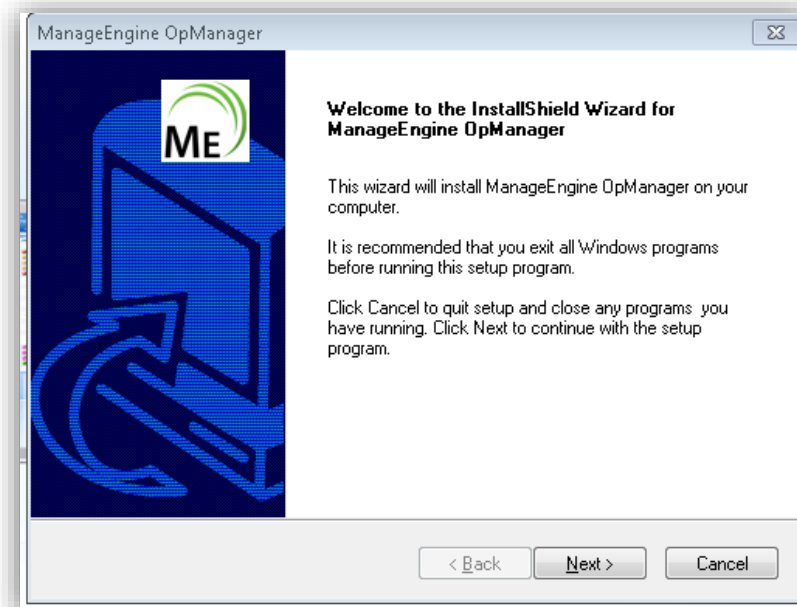


Figura 51 Instalación de OpManager. Bienvenida

3. Aceptación de términos y condiciones

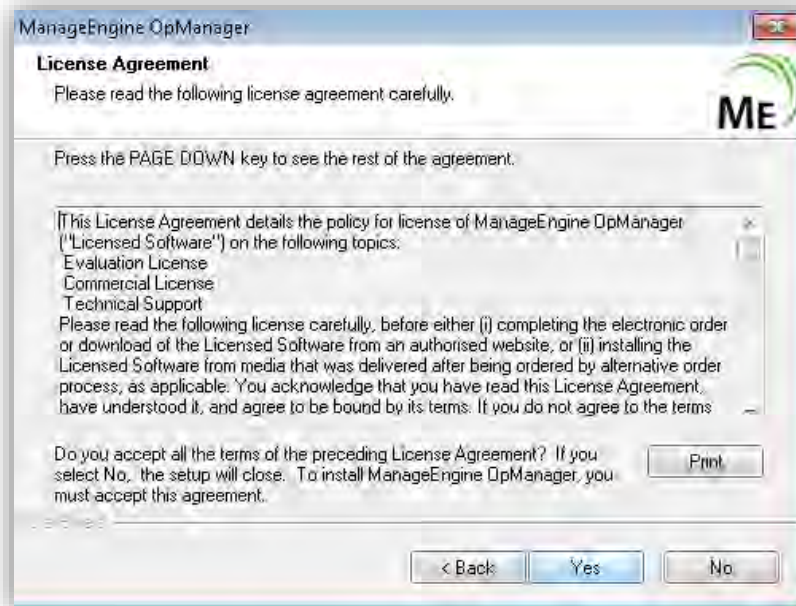


Figura 52 Instalación de OpManager. Licencia

4. Selección del tipo de evaluación del programa.

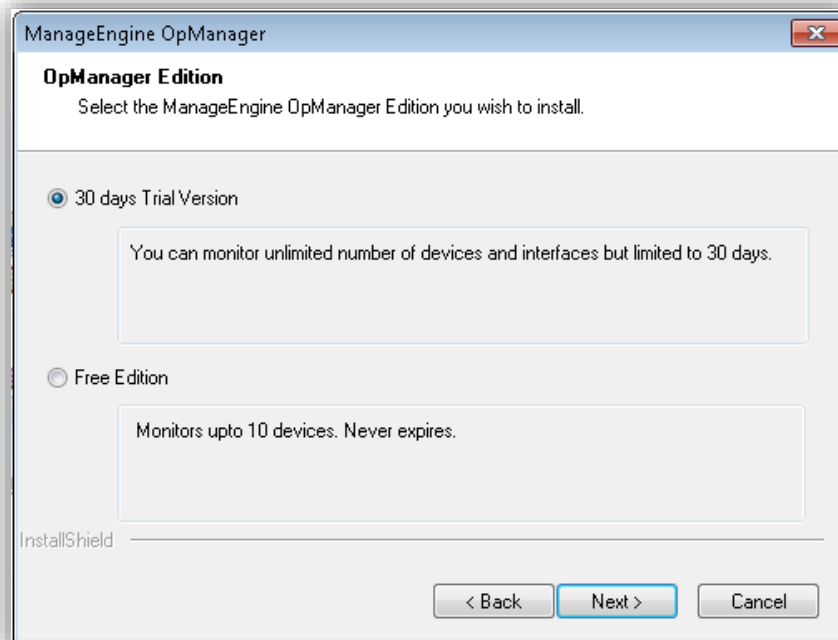


Figura 53 Instalación de OpManager. Tipo Instalación

5. Selección del idioma



Figura 54 Instalación de OpManager. Lenguaje

6. Selección de la carpeta de destino del programa.

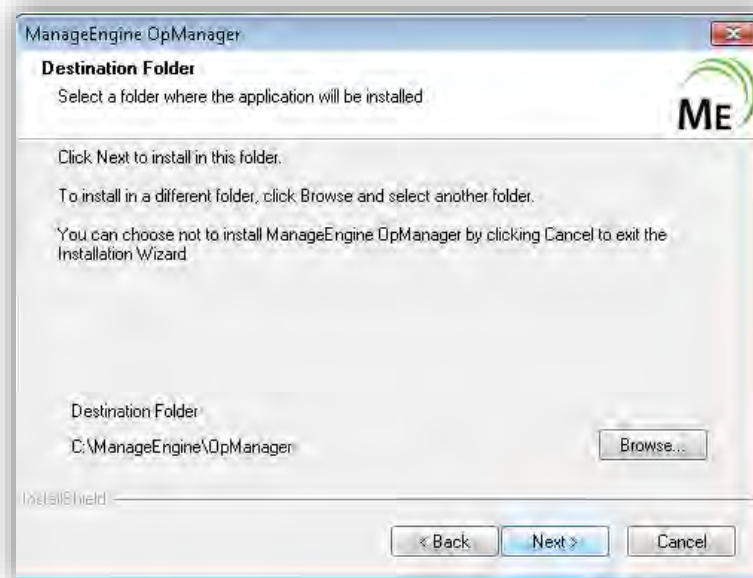


Figura 55 Instalación de OpManager. Selección de Carpeta

7. Instalación de OpManager como servicio en Windows

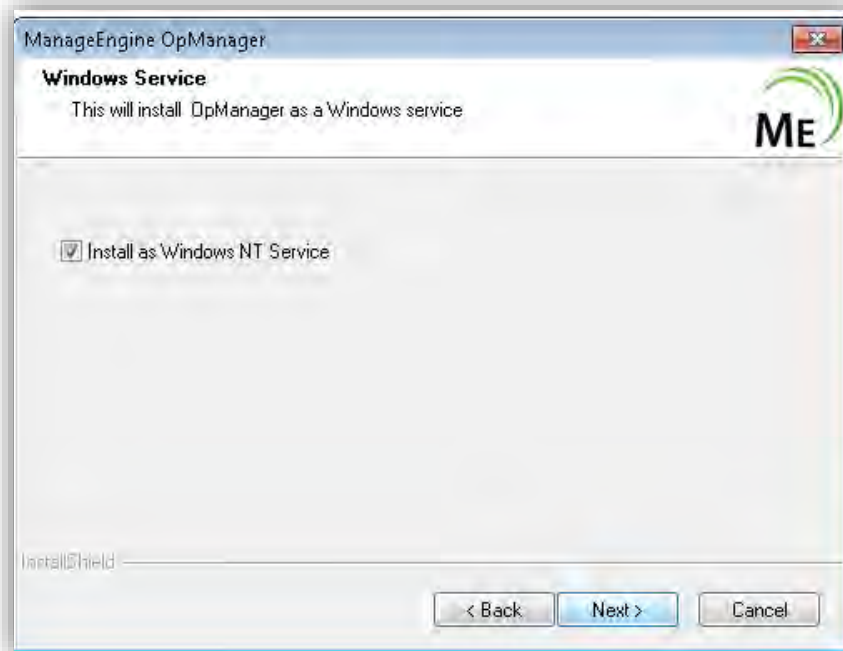


Figura 56 Instalación de OpManager. Windows NT Service

8. Selección del nombre de la carpeta para el programa OpManager

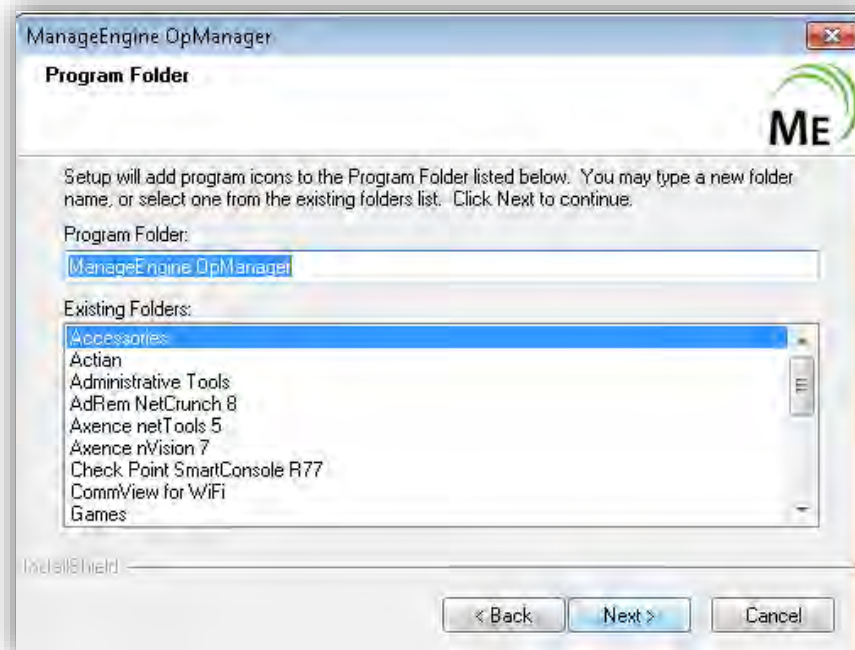


Figura 57 Instalación de OpManager. Accesorios

9. Selección del puerto para el servidor web de OpManager.

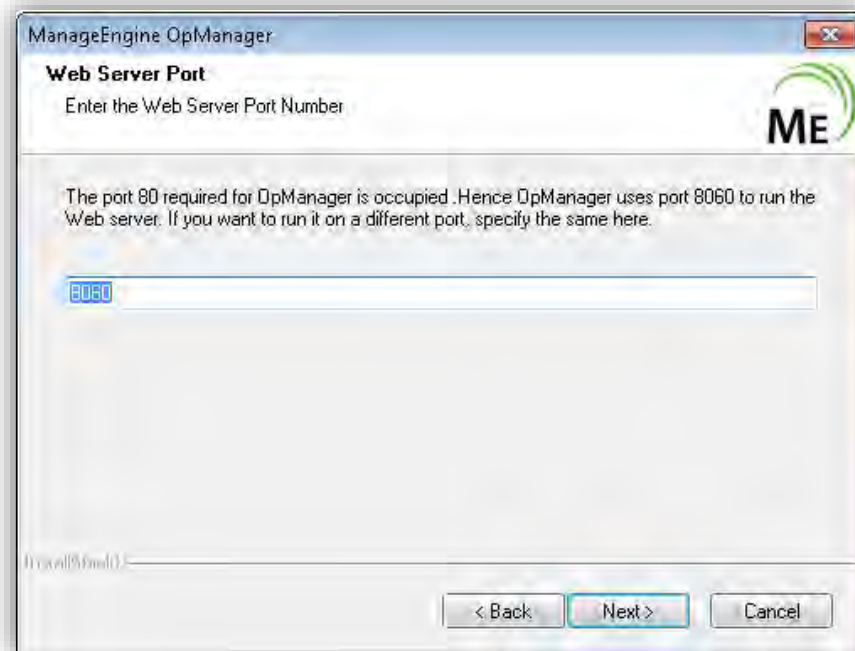


Figura 58 Instalación de OpManager. Puerto

10. Opción de registro para apoyo técnico del programa

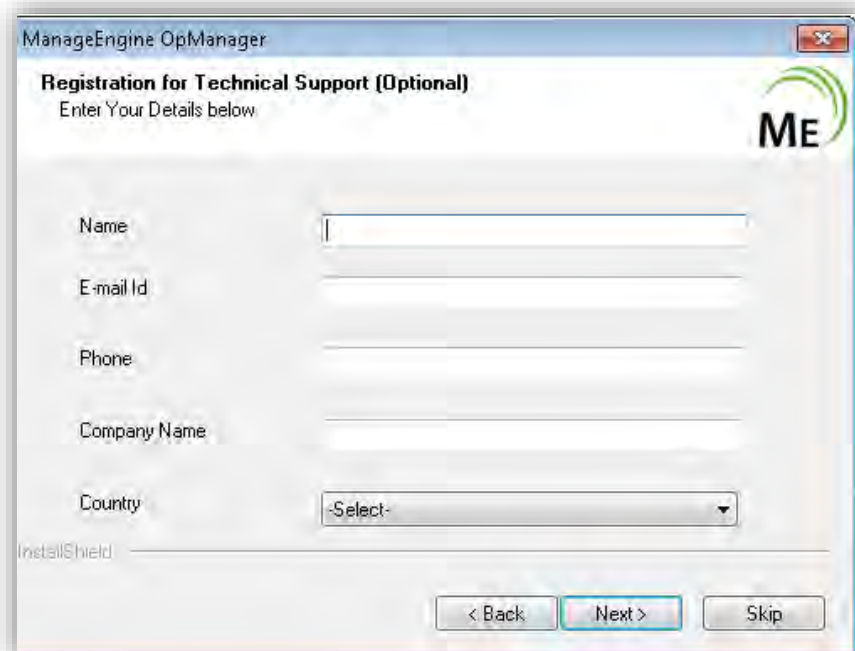


Figura 59 Instalación de OpManager. Registro Opcional

11. Finalización de la instalación de OpManager.

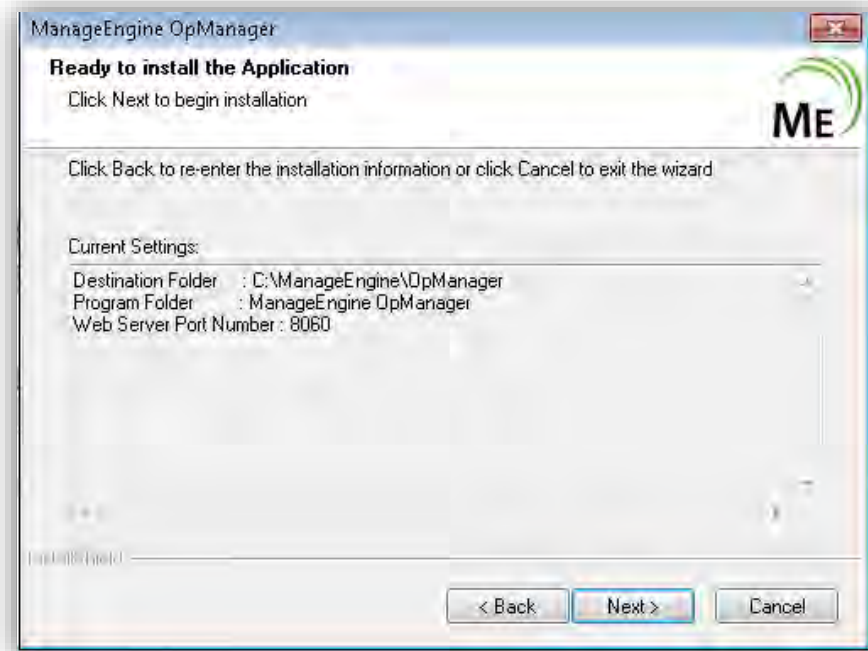


Figura 60 Instalación de OpManager. Finalización

12. Selección del modo de servidor a instalar.

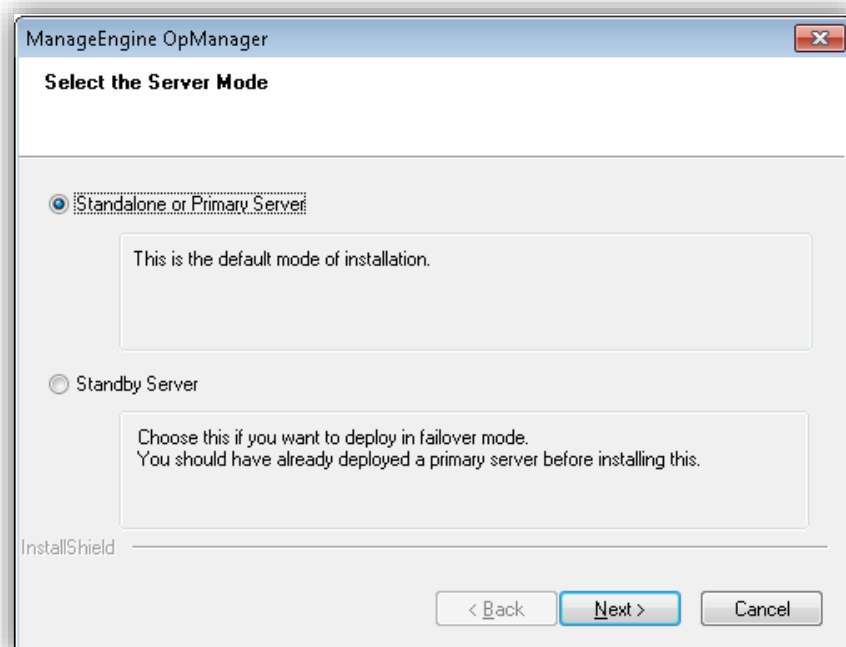


Figura 61 Instalación de OpManager. Tipo de Servidor

13. Selección del tipo de base de datos a instalar para OpManager

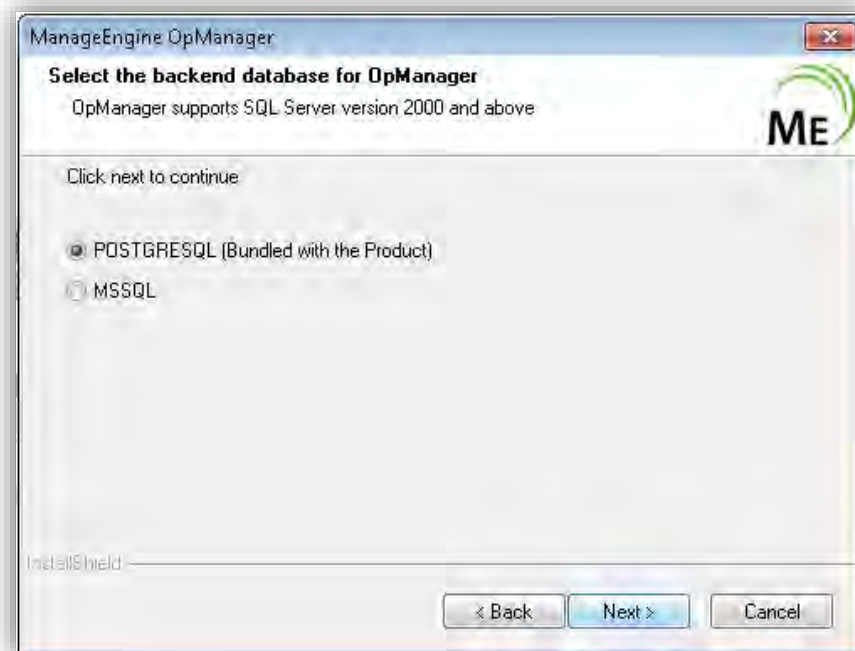


Figura 62 Instalación de OpManager. Base de datos

14. Inicio de la aplicación OpManager

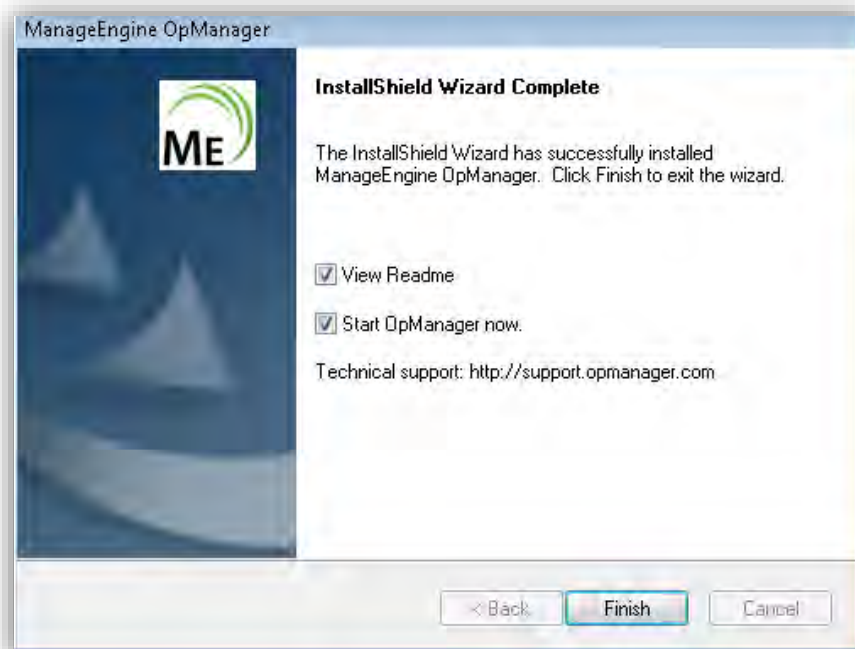


Figura 63 Instalación de OpManager. Inicio de aplicación

Configuración de OpManager

Una vez instalado el programa de OpManager, se procedió a descubrir los segmentos de red principales para el monitoreo de la red y sus dispositivos. En la siguiente imagen se muestra la forma de descubrimiento de redes, al añadir el segmento de red de los switches y servidores.



Figura 64 OpManager. Adición de red



Figura 65 OpManager. Adición de red Servidores

Anexo C:

Instalación y configuración de WhatsUp Gold

Descripción:

Diseñado sobre una arquitectura amplia y escalable, con WhatsUp Gold puede descubrir, crear mapas y gestionar toda su infraestructura en cuestión de minutos desde una sola consola. WhatsUp Gold ahora ofrece un completo conjunto de herramientas de monitoreo de registros y eventos, recopilación, almacenamiento y generación de informes de manera modular, flexible y escalable que pueden ayudarle a iniciar y hacer crecer las estrategias de gestión de eventos que escoja.

WhatsUp Gold permite ampliar las capacidades de red con los módulos de complementos que facilitan el monitoreo y reportes estadísticos de la red.

Algunas características de descubrimiento de WhatsUp Gold son:

- Redes IP y subredes.
- Subredes no contiguas.
- Cambiar la conectividad portuaria.
- Hardware virtualizado VMware.
- Conectividad de Capa 2/port-to-port.
- Conectividad VLAN.
- Dispositivos sin direcciones IP.
- VMware OS.
- Direccionamiento de Capa 3.
- Spanning tree port info / Puente.
- Hardware físico VMware.
- Hardwares desaparecidos.
- Inventario de software instalado.
- Actualizaciones de software.
- Inventario del sistema operativo.
- Inventario de BIOS.
- Información sobre la garantía.

- Inventario de servicios de Windows.
- Servidores.
- Estaciones de Trabajo.

Requisitos de Sistema

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003

Requisitos de Hardware

	Recomendado	Requerido
Procesador	WhatsUp Gold: Doble núcleo Flow Monitor: Cuatro núcleos	WhatsUp Gold: Núcleo Unico Flow Monitor: Doble núcleos
Velocidad de procesador	2 GHz o mas	2 GHz
Memoria RAM	WhatsUp Gold: 4 GB Flow Monitor: +4 GB	WhatsUp Gold: 2 GB Flow Monitor: +2 GB
Espacio en disco duro para aplicaciones, aplicación de base de datos SQL Server Express Edition y compatibilidad de Framework	3 GB	2 GB
Espacio en disco duro para la base de datos y los registros de la base de datos	WhatsUp Gold: 8 GB o más Flow Monitor: +16 GB o más	WhatsUp Gold: 4 GB Flow Monitor: +8 GB
Tarjeta de interfaz de red	1 Gbps	100 Mbps

Instalación del WhatsUp Gold

Después de descargar el software del WhatsUp Gold, el proceso de instalación es sencillo y rápido. Ejecutamos el archivo de software.exe e inicia el asistente de instalación.

Nos da la bienvenida a la instalación del programa con la versión del software y le damos clic en siguiente.

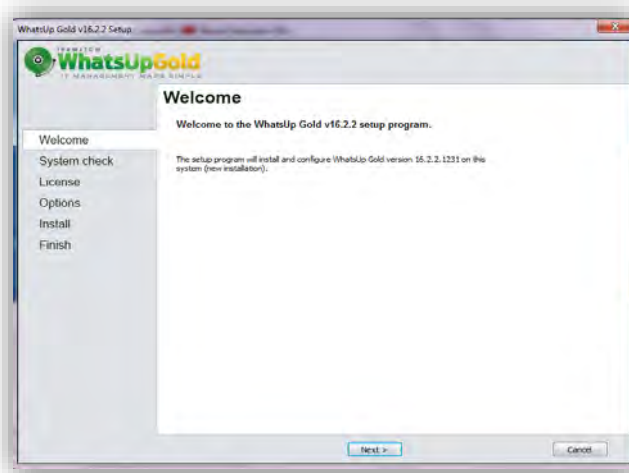


Figura 66 Inicio de la instalación.

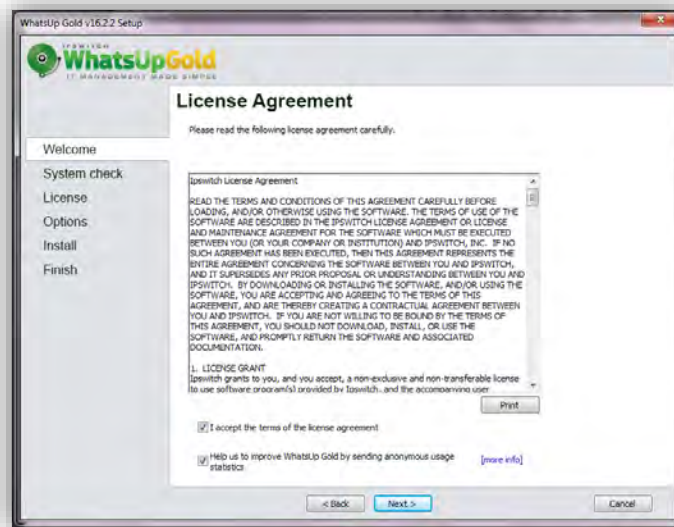


Figura 67 Términos y Condiciones.

Nos pide aceptar los términos de licencia para continuar. Clic en I accept the terms of the licence agreement y clic en siguiente.

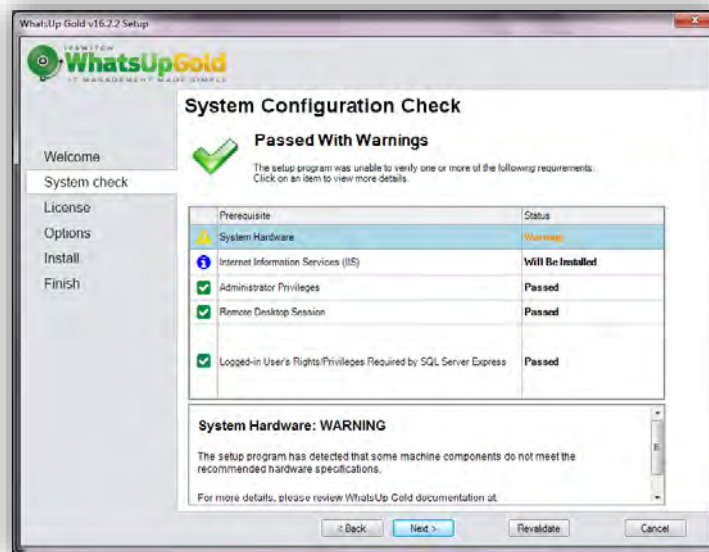


Figura 68 Requerimientos de sistema.

Nos muestra un chequeo de nuestro sistema y nos dice que requerimientos tenemos y cuáles no. Damos clic en siguiente.

En esta ventana nos pregunta que si queremos instalar una copia local del SQL del servidor para guardar los datos que obtenga en WhatsUp Gold. Hacemos clic en sí que instale.

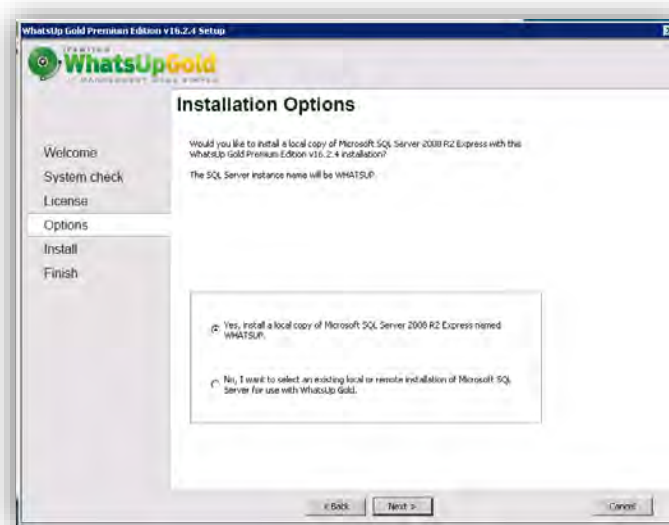


Figura 69 Instalación de SQL.

En la siguiente ventana muestra las opciones de la ruta de instalación de la aplicación de la base de datos de SQL y la ruta donde se guardarán los datos obtenidos.

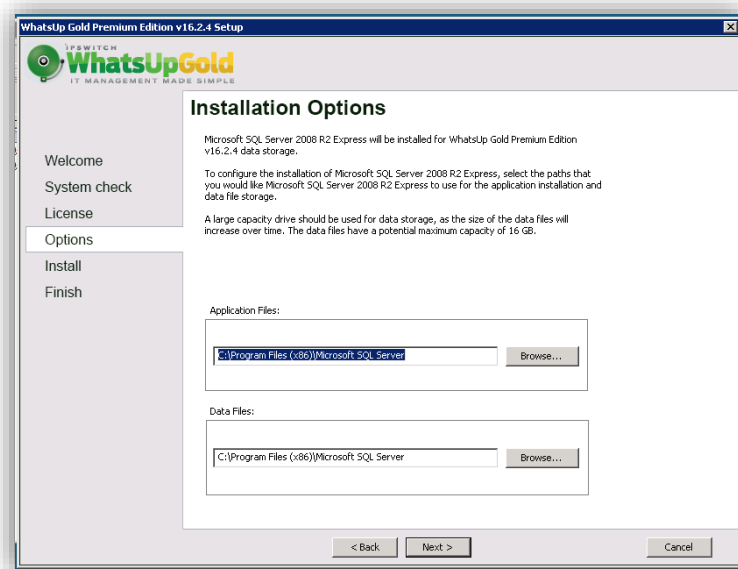


Figura 70 Ruta de Instalación.

En la siguiente ventana pide una contraseña para acceder a la base de datos con una cuenta de administrador de Super Usuario (SA).

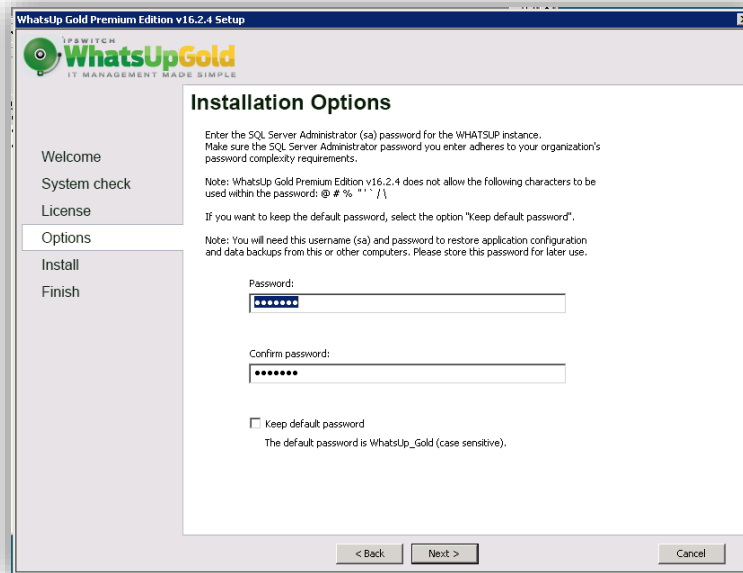


Figura 71 Ingreso de Contraseña de Súper Usuario.

En este caso la contraseña que se asigno es: M0nI7or30.

En la siguiente ventana nos permite ponerle nombre a la base de datos. En este caso se queda con el nombre por default que es WhatsUp.



Figura 72 Ingreso de Nombre de la Base de Datos.

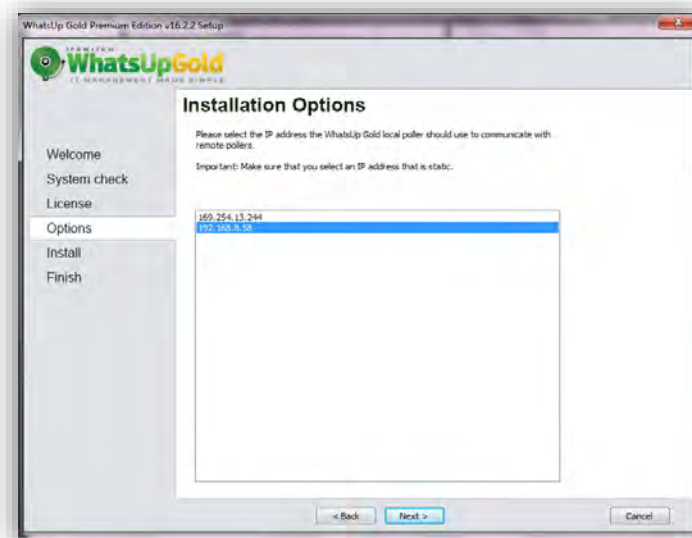


Figura 73 Dirección IP del servidor.

Nos pide seleccionar una dirección IP para el whatsUp local para los remotos sondeos. Seleccionamos la que esté asignada a nuestro servidor.

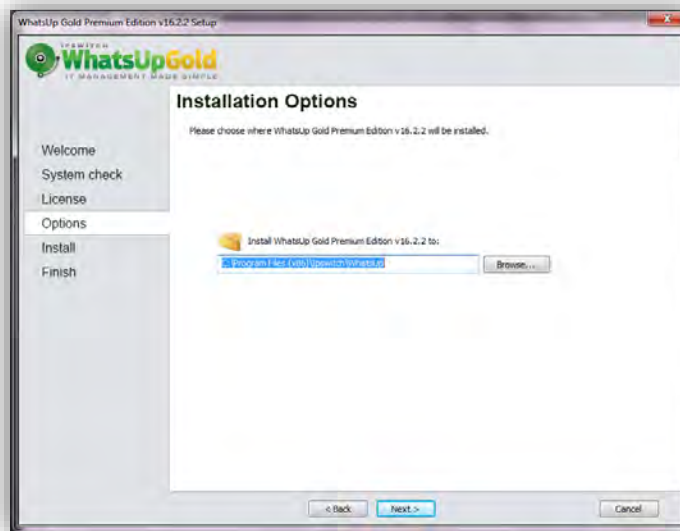


Figura 74 Selección de carpeta contenedora.

Muestra la ruta de la carpeta donde se instalara el Software de WhatsUp Gold. Clic en siguiente.

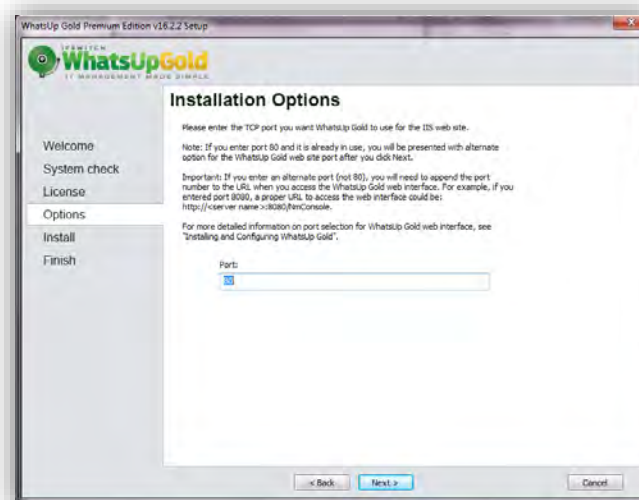


Figura 75 Asignación de Puerto de Interfaz Web.

Asignamos un puesto de salida para la interfaz Web. Dejamos el puerto 80 por default y clic en siguiente.

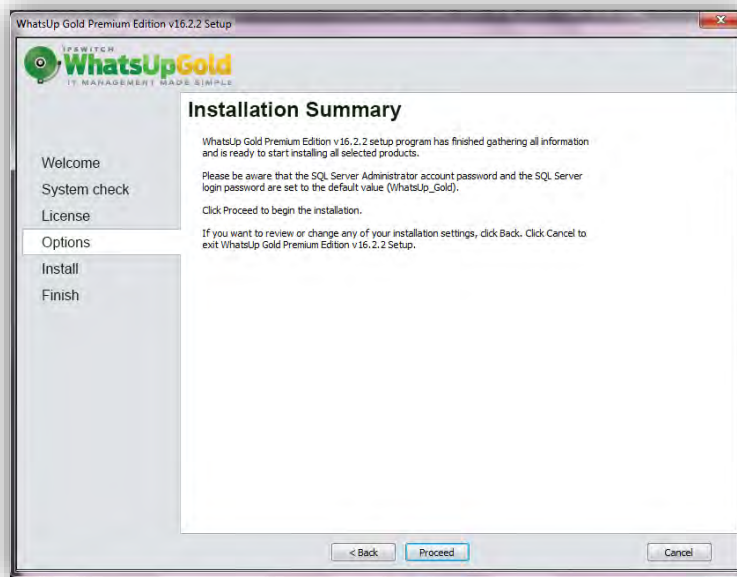


Figura 76 Resumen de Instalación.

Muestra un resumen de la instalación y clic en proceder.

Anexo D: Informe Final

Introducción

Prólogo

El presente documento contiene los resultados generados a partir de la aplicación de una Auditoría de Redes a la Universidad de Quintana Roo, sede Chetumal. Basados en la Metodología tradicional de una Auditoría derivada de los Sistemas Computacionales y de los procesos de COBIT e ITIL, el siguiente Informe muestra las situaciones encontradas al analizar la red informática y las posibles sugerencias que derivan de esta evaluación.

Objetivo

Tener una línea base con la cual conocer el estado actual de la red en cuanto a dispositivos, tráfico, ancho de banda, servicios y protocolos para posteriormente realizar cambios, reconfiguraciones o simplemente mediciones que dan soporte a la misma.

Justificación

La red de datos universitaria se encuentra en constante evolución y crecimiento, tanto en el número de usuarios como en los servicios que soporta. Como parte de la mejora continua, la infraestructura informática fue evaluada de acuerdo a metodologías y estándares internacionales buscando la calidad en los servicios que proporciona, en este caso de los proporcionados en el campus Chetumal.

Metodología

Al realizar la Auditoría de red fue fundamental basarse en una metodología que rija el comportamiento y los procedimientos a seguir para llevarla a cabo. En el ámbito de las mejores prácticas se utilizaron 2 herramientas; COBIT e ITIL, estándares internacionales dedicados a la mejora de los procesos y servicios al usuario en el ámbito de las Tecnologías de Información.

Presentación

Auditoría de Red

Universidad de Quintana Roo, campus Chetumal

Chetumal, Quintana Roo a 6 de Noviembre de 2014

Lic. Luis Fernando Mis Ramírez

Coordinador del área de Redes

De acuerdo con las instrucciones y necesitadas externadas, me permito remitir a usted el dictamen de la Auditoría practicada a la red informática de la Universidad de Quintana Roo en su campus Chetumal, mismo que se llevó a cabo del 00/00/00 al 00/00/00.

De los resultados obtenidos durante la evaluación me permito informarle las siguientes observaciones

- Estado y administración de los dispositivos de comunicación
- Esquema del tráfico de red
 - Uso del ancho de banda
 - Uso de protocolos
 - Flujo de tráfico
 - Consumo de Servidores
 - Políticas y QoS - Firewalls
- Servidores y servicios críticos

De acuerdo con las pruebas realizadas al funcionamiento y operación y de acuerdo con los criterios de evaluación para las redes computacionales, me permito dictaminar:

La infraestructura de red necesita de la Universidad cuenta con diseño de red modular pero también es fundamental que junto con este diseño modular exista una administración centralizada de los dispositivos que proporciona conectividad a los usuarios finales, para tal caso algunos dispositivos, Switches y APs, no cuenta con el soporte SNMP lo cual es fundamental ya que todo programa de monitoreo en la actualidad dispone de las credenciales SNMP más recientes para obtener la información de los dispositivos en la red. Algunos dispositivos cuentan con más de 10 años de adquisición y esto a largo plazo ocasionará menor rendimiento. Además de la administración centralizada, mediante la auditoría se supo que no existe configuración de VLANs y esto genera que no pueda haber escalabilidad ya que todos los puertos están al máximo

En cuanto al uso del tráfico en la red, las gráficas proporcionadas muestran un aumento en la carga en cada uno de los campus de la Universidad, los cuales son administrados desde Chetumal, por lo cual es necesario agregar políticas y reglas de seguridad en los Firewalls para que equilibren el consumo de ancho de banda y aseguren la QoS. En cuanto al uso de los protocolos se puede ver que los protocolos con más consumo son HTTP y HTTPS.

Con respecto a los servidores es importante mencionar que debido a la migración y virtualización de algunos servidores, existen algunos puertos abiertos y que son de riesgo, por lo cual se sugiere

la necesidad de administración. En cuanto al desempeño, los servicios de DNS, Correo y Web son lo más solicitados y los que requieren de mayor rendimiento en sus sistemas.

Formato de Situaciones Encontradas - Relevantes

Empresa:
Universidad de Quintana Roo

Área auditada:
Red Informática – Campus Chetumal

Referencia	Situaciones	Causas	Solución	Fecha de Solución	Responsable
1	Administración no centralizada de dispositivos de comunicación- Falta de rendimiento	Soporte SNMP Equipos de 10 años de adquisición	Actualización de equipos y configuración	A partir de la fecha de término de la Auditoría	Administrador de red
2	Falta de conexiones dedicadas seguras	Falta de VPNs	Configuración de VPNs	A partir de la fecha de término de la Auditoría	Administrador de red
3	No existe control en el dominio de la difusión	Falta de VLANs	Configuración de VLANs, en la capa de Acceso de la Red	A partir de la fecha de término de la Auditoría	Administrador de red
4	Incremento del ancho de banda	Incremento de usuarios y dispositivos	Aumento y distribución correcta del ancho de banda	A partir de la fecha de término de la Auditoría	Administrador de red

Bibliografía

Bibliografía

- Andreu, J. (2011). *Redes locales de datos (Redes locales)*. Editex.
- Derrien, Y. (1994). *Técnicas de la Auditoría Informática*. MARCOMBO S.A.
- Gerencia COBIT, I. G. (2000). *COBIT, Directrices Gerenciales (3 ed.)*. ISACA.
- Hernández, E. H. (2000). *Auditoría en Informática*. Continental.
- ISACA. (2014). *COBIT, AN ISACA FRAMEWORK*. Obtenido de <http://www.isaca.org/cobit/pages/default.aspx>
- McCabe, J. D. (2003). *Network Analysis, Architecture & Design*. Morgan Kaufmann Publishers.
- Oppenheimer, P. (2004). *Top-Down Network Design (2 ed.)*. Cisco Press.
- OSIATIS S.A. (s.f.). *Fundamentos de la Gestión TI - ITIL*. Obtenido de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php
- Peña, d. I. (2008). *Auditoría. Un enfoque práctico*. Paraninfo.
- Pfaffenberger, B. (1999). *Diccionario de términos de computación*. México: PRENTICE HALL.
- Piattini, M. (s.f.). *Auditoría informática, un enfoque práctico. (2 ed.)*. Alfaomega.
- Razo, C. M. (2002). *Auditoría en Sistemas Computacionales (1 ed.)*. Naucalpan de Juárez, Edo. de México., México: PEARSON EDUCACIÓN.
- Teare, D. (2005). *Campus Network Design Fundamentals*. Cisco Press.
- Vallina, M. M. (s.f.). *Infraestructuras de redes de datos y sistemas de telefonía*. Paraninfo.