

"2015. Año del Bicentenario Luctuoso de José María Morelos y Pavón"

Centro Universitario UAEM Zumpango

Ingeniería en Computación

Unidad de Aprendizaje: Auditoría de Redes

Unidad de Competencia V:

Integración de los conceptos y elementos requeridos para el desarrollo de una auditoría a una red.

MTE-MI. Rosa Erendira Reyes Luna

Agosto 2015





INTRODUCCIÓN

El procedimiento para ejecutar la auditoria requiere de una planificación apropiada, además deberá supervisarse adecuadamente.

Para ello es necesario estudiar y evaluar el sistema de control interno para obtener evidencia suficiente y adecuada.





PROPÓSITO

Presentar al alumno los conceptos, fundamentos, metodologías y técnicas básicas, requeridas para la práctica de auditorías en tecnologías de información en materia de redes de voz y datos.





UNIDAD DE COMPETENCIA V

Integración de los conceptos y elementos requeridos para el desarrollo de una auditoría a una red.



Contenido

1. Elementos a auditar
2. Objetivos de Control
 - Gerencia de Comunicaciones
 - Red Física
 - Red Lógica
3. Evaluación
 - Sistema de Red
 - Cobertura de Alcance
 - Diseño de Red
4. Informe





Elementos a auditar

- Auditando la Gerencia de Comunicaciones
- La Red Física
- Auditando la Red Lógica





Objetivos de Control

- Estos se encargan de marcar la existencia de los diferentes indicadores que garantizan el correcto funcionamiento de la red.





UAEM | Universidad Autónoma
del Estado de México

Auditando la Gerencia de Comunicaciones





Objetivos de Control

- Una gerencia de comunicaciones con autoridad para establecer procedimientos y normativa.
- Procedimientos y registros de inventarios y cambios.
- Funciones de vigilancia del uso de la red de comunicaciones, ajustes de rendimiento, registro de incidencias y resolución de problemas.





Objetivos de Control

- Procedimiento para el seguimiento del coste e las comunicaciones y su reparto a las personas o unidades apropiadas.
- Procedimiento para vigilar el uso de la red de comunicaciones, realizar ajustes para mejorar el rendimiento, registrar y resolver cualquier problema.
- Participación activa de la gerencia de comunicaciones en el diseño de las nuevas aplicaciones *on line* para asegurar que se sigue la normativa de comunicaciones.





UAEM | Universidad Autónoma
del Estado de México

Auditando la Red Física



CENTRO UNIVERSITARIO UAEM
ZUMPARGO



www.uaemex.mx



Objetivos de Control

- Áreas controladas para los equipos de comunicaciones, previniendo así accesos inadecuados.
- Protección y tendido adecuado de cables y líneas de comunicaciones, para evitar accesos físicos.
- Controles de utilización de los equipos de pruebas de comunicaciones, usadas para monitorear la red y su tráfico, que impidan su utilización.





Objetivos de Control

- Atención específica a la recuperación de los sistemas de comunicación de datos en el plan de recuperación de desastres en sistemas de información.
- Controles específicos en caso de que se utilicen líneas telefónicas normales con acceso a la red de datos para prevenir accesos no autorizados al sistema o la red.





UAEM | Universidad Autónoma
del Estado de México

Auditando la Red Lógica





Objetivos de Control

- Contraseñas y procedimientos par limitar y detectar cualquier intento de acceso no autorizado a la red de comunicaciones.
- Facilidades de control de errores para detectar:
 - Errores de transmisión
 - Establecer las retransmisiones apropiadas





Objetivos de Control

- Controles para asegurar que las transmisiones van solamente a usuarios autorizados y que los mensajes no tienen porque seguir siempre la misma ruta.
- Registro de la actividad de la red, para ayudar a reconstruir incidentes y detectar accesos no autorizados.





Objetivos de Control

- Técnicas de cifrado de datos donde haya riesgos de acceso impropios a transmisiones sensibles.
- Controles adecuados que cubran la importación o exportación de datos a través de puertas, en cualquier punto de la red, a otros sistemas informáticos.





UAEM | Universidad Autónoma
del Estado de México

Evaluación del diseño, instalación y aprovechamiento de la red de cómputo





Aspectos Relacionados con el sistema de Red

- Evaluación del Análisis de una red de Cómputo.
- Evaluación de la existencia de:
 - Metodologías
 - Normas
 - Estándares y políticas para el:
 - análisis
 - diseño de redes de cómputo
- Análisis de la definición de la problemática y solución para instalar redes de cómputo en la organización.





Análisis del cumplimiento de los objetivos de la red de Cómputo

- Evaluando:
 - Forma de compartir recursos informáticos: información y activos → de la organización
 - Cobertura de los servicios informáticos para: la captura, procesamiento y emisión de la información.





- Cobertura de los servicios de comunicación
- Frecuencia con la que los usuarios recurren a los recursos de la red.
- Confiabilidad y seguridad en el uso de la información
- Satisfacción de las necesidades del poder computacional de la organización, sea con redes, cliente/servidor o mainframe.





Análisis de la delimitación de los proyectos de red

- Evaluar la manera en que se cumple con:
 - La delimitación temporal, por el tiempo que se instalará la red
 - La delimitación espacial, por las dimensiones físicas y lógicas del proyecto de red.
 - La delimitación conceptual, por el análisis específico de las necesidades que se deben satisfacer con la red de cómputo.



Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la Red

- Evaluando:
 - La factibilidad:
 - Tecnológica
 - Económica
 - Administrativa
 - Operativa
 - La escalabilidad y aprovechamiento de los recursos informáticos
 - La tolerancia a posibles fallas
 - La transparencia del trabajo para los usuarios





UAEM | Universidad Autónoma
del Estado de México

ESTUDIO CONFORME A LA COBERTURA



www.uaemex.mx

Análisis de las redes de multicomputadoras

- Evaluar el funcionamiento en la cobertura de punto a punto
- Evaluar el funcionamiento de la tecnología que se usa con un solo cable entre las máquinas conectadas.
- Evaluar el funcionamiento de las aplicaciones, usos y explotación de éstas redes.



- Evaluar la cobertura de 10 metros a 1 kilómetro.
- Evaluar el uso adecuado y confiable de la tecnología utilizada para la transmisión de datos, como:
 - Cable Coaxial
 - Cable par trenzado
 - Fibra óptica
 - Sistema de transmisión satelital
- Evaluar la restricción adoptada para establecer el tamaño de la red.
- Evaluar el tiempo promedio de transmisión de la red.
- Verificar que las velocidades utilizadas normalmente en su transmisión estén en el rango de 10 a 100Mbps.

Análisis de la red de área local LAN





Análisis de la Red de Área Metropolitana (MAN)

- Evaluar su cobertura de 10 a 100km.
- Evaluar los criterios adoptados para establecer el tamaño y cobertura de la red.
- Evaluar el funcionamiento de la tecnología utilizada internamente en la transmisión de datos como:
 - Cable coaxial,
 - Cable par trenzado
 - Fibra óptica
 - Transmisión satelital o de microondas
- Evaluar el tiempo promedio de transmisión de la red.
- Evaluar las velocidades utilizadas normalmente en su transmisión.



Análisis de la Red de Área Amplia (WAN)

- Evaluar su cobertura de 100 a 1000km.
- Evaluar el funcionamiento de la composición, consistente en la colección de hosts.
- Evaluar la forma de enviar los paquetes de un enrutador router a otro. Evaluar el funcionamiento de la tecnología utilizada internamente en la transmisión de datos como:
Cable coaxial, Cable par trenzado, Fibra óptica, Transmisión satelital o de microondas
- Evaluar el tiempo promedio de transmisión de la red entre LANs y entre subredes.
- Evaluar las velocidades utilizadas normalmente en su transmisión.





Análisis de las redes públicas incluyendo Internet

- Evaluar la cobertura de 10,000 a 100,000km
- Evaluar la composición de esta red, consistente en la integración de la red Internet a la vinculación con puertas de enlace, computadoras que pueden traducir entre formatos incompatibles.
- Evaluar las velocidades utilizadas normalmente en su transmisión.





Análisis de las redes Inalámbricas

- Evaluar el uso adecuado de este tipo de red según sus características.
- Evaluar el uso adecuado y confiable de la transmisión de datos por medio de radio, microondas, satélites o infrarrojo o cualquier otro medio sin cables.
- Evaluar la posibilidad de combinar las redes inalámbricas con otras computadoras móviles u otras redes.





UAEM | Universidad Autónoma
del Estado de México

Evaluación del diseño e instalación de la red según su configuración





- El concepto de Servidor único.
- El concepto cliente/Servidor
- Punto a Punto (Uno a Uno)
- Multipunto (uno a muchos; muchos a muchos)
- Red lógica, basada en el concepto de conexión entre terminales sin cables.
- Red virtual basada en el concepto de tecnología y comunicación vía Internet.

Red basada en:





- Estudio de las necesidades de cobertura con la topología física de la red.
- Estudio de las necesidades de cobertura con la topología lógica de la red.

Análisis del diseño e implementación de la topología de cobertura de la red





- Capas Físicas
- Capas de enlace
- Capas de Transporte
- Capa de Sesión
- Capa de presentación
- Capa de Aplicación

**Análisis del diseño del modelo
OSI evaluando el
funcionamiento de las
siguientes capas:**





Análisis de los estándares adoptados

- Ethernet (norma IEEE 802.3)
- Token Ring (norma IEEE 802-5)
- ARCnet (Attached Resource Computer Network, Red de Computadoras de Recursos Conectados)
- IPX (Internetwork Packet Exchange, Intercambio de Paquetes entre Redes)





Análisis del funcionamiento de los protocolos

- IP (Protocolo de Internet)
- ICPM (Protocolo de Mensajes de Control de la Transmisión)
- TCP (Protocolo de Control de la Transmisión)
- UDP (Protocolo de Datagramas de Usuario)
- FTP (Protocolo de Transferencia de Archivos)
- SMTP (Protocolo Simple de Administración de la Red)
- SNMP (Protocolo Simple de Administración de Red)
- DNS (Sistema de Nombres de Dominio)
- Telnet (Red de Telecomunicaciones)





UAEM | Universidad Autónoma
del Estado de México

Informe



www.uaemex.mx



Sencillez

- Es expresar con naturalidad las ideas, los conceptos, hechos y observaciones sin utilizar adornos excesivos, rebuscamientos, ni tecnicismos inútiles para mostrar mayor cultura.
- Así que es utilizar franca espontaneidad, así como frases y palabras.
- El auditor puede asimilarlo como si tuviera que platicar lo que ha encontrado o estuviera dirigiendo una conferencia.





Consejos para el Auditor

- Evitar, al redactar el informe final, el uso de frases y palabras rebuscadas y sofisticadas cuyo significado se desconozca.
- Utilizar un lenguaje moderno, con términos actuales y propios para el entendimiento del tema.
- Eliminar las palabras extranjeras que tienen un equivalente en castellano, siempre y cuando no se entorpezca, ni se limite lo que se quiere plasmar en el texto.
- Evitar traducir al español los términos informáticos en inglés cuyo uso se haya popularizado en los ambientes de sistemas, ya que todos los usuarios lo entienden.





Ilación

Nexo lógico entre el consiguiente y las premisas, es decir, conexión razonada entre varias ideas y un discurso.

Consiguiente: que depende y se deduce de otra cosa. En una proposición de dos términos, el segundo (consecuente).

Premisa: que precede. Cada una de las proposiciones del silogismo de las que se saca una conclusión. Por extensión, base de la argumentación.

Inferir: conjeturar, es decir conducir a un resultado.





Tono y Fuerza

- La forma de redactar, la intensidad que se le da al escrito y la profundidad con la que se expresan los términos plasmados en un informe de auditoría.
- Esta se define por la fuerza que el auditor da a lo que está reportando, a fin que se entienda lo que quiere expresar; justo en el tono que les quiere dar a los términos utilizados y con la fortaleza que quiere destacar.
- En los informes de pueden utilizar diversos tonos desde los muy tenues y cálidos, otros demasiado fuertes y acalorados, algunos más tibios y temerosos.



Oportunidad

- Consiste en presentar a tiempo las desviaciones que fueron observadas, a fin de corregirlas de inmediato y tomar las medidas necesarias para que no vuelva a ocurrir.
- La esencia durante la auditoría de sistemas es reportar lo que se observa durante una evaluación, a fin de que los directivos sepan cómo está el funcionamiento en el área de operaciones y cómo se están utilizando los recursos.
- Por otro lado oportunidad también quiere decir entregar y comentar a tiempo los resultados de la evaluación practicada: tanto la elaboración del borrador y los comentarios con los auditados, la elaboración de los reportes de situaciones encontradas y situaciones relevantes, como su presentación a los directivos del área de sistemas y la entrega del informe final a los directivos de la empresa.



Precisión

- Redactar el informe utilizando sólo conceptos completos, sin agregar datos innecesarios, pero sin omitir ninguna información que se considere importante.
- Se dice que una situación es precisa cuando expresa con exactitud el asunto que se está reportando.





UAEM | Universidad Autónoma
del Estado de México

Oportunidad para una buena redacción

PREGUNTAS QUE DEBERÍA HACERSE UN AUDITOR PARA DESARROLLAR EL INFORME





¿Qué?

1. ¿Qué se quiere o se debe informar?
2. ¿Qué se desea hacer notar de la evaluación?
3. ¿Qué se debe o se puede evitar de las observaciones?
4. ¿Qué es lo importante y qué es lo irrelevante de la evaluación realizada?
5. ¿Qué tipo de redacción se utilizará en el reporte?
6. ¿Qué formatos se utilizarán para reportar situaciones encontradas, las situaciones relevantes y el dictamen de auditoría?
7. ¿Qué criterio se debe seguir para jerarquizar las situaciones que se van a reportar?
8. ¿Qué tan importante es esta observación para reportarla?





¿Quién?

1. ¿Quién leerá este informe?
2. ¿A quién le interesa el contenido del informe?
3. ¿Quién aceptará lo escrito y quién lo rechazará?
4. ¿Quién o quiénes recibirán el informe?
5. ¿Quién será el afectado con lo que se reporte?
6. ¿Con quién comparar el informe?
7. ¿Con quién consultar su contenido?





¿Cuándo?

1. ¿Cuándo se piensa a redactar la situación?
2. ¿Cuándo se termina de redactar la situación?
3. ¿Cuándo se incluye determinada parte y cuándo no?
4. ¿Cuándo se elimina o se agrega información?
5. ¿Cuándo es borrador del dictamen?
6. ¿Cuándo brincar el párrafo?
7. ¿Cuándo se entregará el informe?
8. ¿Cuándo ampliar y cuándo reducir la información?
9. ¿Cuándo utilizar información técnica de los sistemas y cuándo evitarla?
10. ¿Cuándo incluir anexos y cuadros adicionales?





¿Dónde?

1. ¿Dónde se empieza el informe?
2. ¿Dónde se termina el informe?
3. ¿Dónde va este comentario?
4. ¿Dónde se pone una cita textual?
5. ¿Dónde se anexan gráficas o cuadros estadísticos?
6. ¿Dónde dar énfasis y dónde ser útil?
7. ¿Dónde destacar lo importante?
8. ¿Dónde va cada parte?



¿Cómo?

1. ¿Cómo redactar cada parte del informe?
2. ¿Cómo redactar todo el informe?
3. ¿Cómo jerarquizar las situaciones que se reportan?
4. ¿Cómo señalar adecuadamente el contenido del informe y del dictamen?
5. ¿Cómo determinar las partes del informe, sus capítulos, temas y anexos?
6. ¿Cómo especificar las situaciones, las causas y soluciones?
7. ¿Cómo evitar preferencias, distorsiones y desvíos de la información que se reporta?
8. ¿Cómo concentrar las situaciones en el dictamen?
9. ¿Cómo distinguir las situaciones importantes de las irrelevantes?
10. ¿Cómo supervisar la elaboración correcta del informe?





¿Por qué?

1. ¿Por qué redactar el informe?
2. ¿Por qué anotar cada situación, causa y solución?
3. ¿Por qué esta parte del dictamen va antes y aquella después?
4. ¿Por qué se tiene que reportar esta observación o por qué no se debe hacer?
5. ¿Por qué dividir el informe en capítulos, temas y anexos?
6. ¿Por qué resumir las situaciones encontradas en situaciones relevantes?
7. ¿Por qué se redacta de determinada manera cada situación?
8. ¿Por qué se tiene que redactar el dictamen?



¿Para qué?

1. ¿Para qué redactar el informe de auditoría?
2. ¿Para qué se evaluó y revisó el área, sistema o actividad informática?
3. ¿Para qué se tiene que reportar esta observación?
4. ¿Para qué se divide el informe en situaciones, causas y soluciones?
5. ¿Para qué pulir la redacción y presentación de la informe?
6. ¿Para qué concentrar las situaciones encontradas en situaciones relevantes, y éstas en el informe final y en el dictamen de la auditoría?
7. ¿Para qué elaborar el dictamen del auditor?





¿Obvias o no?

- Las interrogantes anteriores pueden ser apreciadas como irrelevantes o demasiado obvias y, por consiguiente sería a priori considerarlas, sin embargo la experiencia entre los mejores ha demostrado que al omitir muchas de estas preguntas en la redacción del informe, se generan deficiencias en la presentación del mismo.



Exactitud

- Justo, conforme a la regla o la verdad. «Puntualidad y fidelidad en la ejecución de una cosa».
- En la redacción del informe, esto significa dar el sentido exacto a las palabras, a fin de hacer el texto entendible y enfocarlo justo a lo que se quiere dar a conocer al lector del informe, es decir, lo que el auditor quiere reportar en su evaluación.
- Concretamente, significa plasmar ideas, aportaciones, conclusiones y comentarios conforme se necesitan, y con la minuciosidad y escrupulosidad que se requiere de los vocablos adecuados, a fin de que el lector del informe entienda exactamente lo que quiere expresar de la auditoría practicada.



Imparcialidad

- Uno de los requisitos más estrictos para el auditor es que sea íntegro y profesional en la elaboración de su reporte de auditoría, anotando las observaciones tal y cómo las encontró dentro de su evaluación, es decir, que reporte de manera ecuánime las situaciones que informa, que no tome partido, ni para perjudicar enfatizando la gravedad de las desviaciones, ni para solapar ni minimizar los errores encontrados durante su evaluación.

Qué solo reporte lo justo





Objetividad

- Es el entendimiento de las cosas, ideas y valores por si mismos y no por lo que piensa, razona e interpreta.
- En el caso del informe de auditoría es la descripción apegada a la realidad de lo que se ve; en este caso de lo que se comprueba por medio de la evaluación, con el propósito de redactar las observaciones tal y como se presentan, describiendo los resultados de la auditoría lo más naturalmente posible.





Congruencia

- Es reportar lo correspondiente a lo que verdaderamente esta ocurriendo, de tal forma que solo muestre las cosas que el auditor conoce, siempre y cuando éstas corresponden al objeto y tema de la auditoría.



Bibliografía

1. ECHENIQUE, García José Antonio. Auditoría en Informática. Edit. Mc Graw Hill. 2001. 2a. edición.
2. MUÑOZ, Razo Carlos. Auditoría en Sistemas Computacionales. Edit. Pearson Educación. México, 2000.
3. Systems Auditability and Control. Edit. The Institute of Internal Auditors. USA, 1994
4. José Acha Iturmendi. Paraninfo, Auditoria Informática en la empresa 1994.
5. Control Objectives. Illinois, USA, 1992) EDP Association, EDP Auditing, McGraw Hill, 1988. VALLABHANENI S. RAQ. AUDITING COMPUTER SECURITY.





UAEM | Universidad Autónoma
del Estado de México

GRACIAS

Auditoría de Redes

Unidad de Competencia V

MTE-MI. Rosa Erendira Reyes Luna

rereyesl@uaemex.mx



www.uaemex.mx



UAEM | Universidad Autónoma
del Estado de México

GUÍA EMPLEO DE MATERIAL

Auditoria de Redes
Unidad de Competencia V



GUÍA EMPLEO DE MATERIAL

Las primeras diapositivas muestran el propósito, justificación y objetivos de la unidad de aprendizaje. Se presentan para que el alumno identifique dichos elementos.

A partir de la diapositiva 6 se enlistan los objetivos de control para evaluar cada entidad perteneciente al sistema de red informática.

En la diapositiva 18 se integran los criterios de evaluación del sistema de red, así como el alcance de y diseño de la red.

La diapositiva 37 muestra las características que debe cubrir el documento que informa el estado de la red auditada.

