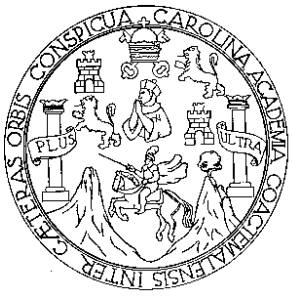
Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES

EVELYN YESENIA LOBOS BARRERA
ASESORADA POR INGA. SANDRA MARÍA LEMUS

Guatemala, abril de 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

EVELYN YESENIA LOBOS BARRERA

ASESORADA POR INGA. SANDRA MARÍA LEMUS

AL CONFERÍRSELE EL TÍTULO DE
INGENIERA EN CIENCIAS Y SISTEMAS

GUATEMALA, ABRIL DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Carlos Humberto Pérez Rodríguez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Ligia María Pimentel Castañeda
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADOR	Ing. Virginia Victoria Tala Ayerdi
SECRETARIO	Ing. Carlos Humberto Pérez Rodríguez

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES

Tema que me fuera asignado por la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería con fecha 10 de enero de 2004.

Evelyn Yesenia Lobos Barrera

Guatemala, marzo de 2005.

Ing. Carlos Alfredo Azurdia Morales
Coordinador Comisión de Trabajos de Graduación
Escuela de Ciencias y Sistemas
Facultad de Ingeniería USAC

Estimado Ingeniero:

Por medio de la presente hago de su conocimiento, que he procedido a revisar el trabajo final de graduación titulado: **AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES**, elaborado por la estudiante Evelyn Yesenia Lobos Barrera, y de acuerdo a mi criterio, se encuentra concluido y cumple con los objetivos propuestos para su desarrollo.

Agradeciendo de antemano la atención que le preste a la presente, me suscribo a usted,

Atentamente.

Inga. Sandra María Lemus
Asesora

Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Carrera de Ciencias y Sistemas

Guatemala marzo de 2005

Ingeniero
Luis Alberto Vettorazzi España
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Vettorazzi:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación de la estudiante **EVELYN YESENIA LOBOS BARRERA,** titulado: "**AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
Y Revisión de Trabajos de Graduación

Universidad de San Carlos de Guatemala
Facultad de Ingeniería

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor, del trabajo de graduación titulado "**AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES"**, presentado por la estudiante **Evelyn Yesenia Lobos Barrera,** aprueba el presente trabajo y solicita la autorización del mismo.

ID Y ENSEÑAD A TODOS

Ing. Luis Alberto Vettorazzi España
DIRECTOR
INGENIERIA EN CIENCIAS Y SISTEMAS

Guatemala, abril 2005

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado "**AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES**" presentado por la estudiante universitaria Evelyn Yesenia Lobos Barrera, procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Sydney Alexander Samuels Milson
DECANO

Guatemala, abril de 2005

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

COBIT (Control Objetives for Information an Related Technology) Objetivos de control para la información y tecnologías relacionadas. Desarrollado para representar un estándar internacional sobre conceptos de control en tecnología de información.

Commit Realiza la transacción actual. Todos los cambios realizados por la transacción son visibles a las otras transacciones, y se garantiza que se conservan sí se produce una caída de la máquina.

Datagramas El servicio de datagramas ofrece una conexión no estable entre una máquina y otra. Los paquetes de datos son enviados o difundidos (broadcasting) de una máquina a otra, sin considerar el orden como éstos llegan al destino o si han llegado todos.

DNS El DNS (Domain Name Service) es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y viceversa. Aunque Internet sólo funciona con base a direcciones IP, el DNS permite que los humanos usemos nombres de dominio que son bastante más simples de recordar.

Encripción Es un proceso a través del cual utilizamos software para proteger información sensible mientras se encuentra en tránsito.

Firewall Dispositivo de seguridad utilizado para filtrar la información que se transmite entre dos redes, a conveniencia y seguridad de las mismas.

FTP (File Transfer Protocol) - protocolo de transferencia de archivos está diseñado, como indica su nombre, para transferir todo tipo de archivos entre computadoras. Existen dos tipos de transferencias:

Descarga (download). Consiste en traer un archivo a nuestro ordenador desde un servidor remoto. También se dice "bajar un archivo".

Carga (upload). Consiste en llevar un archivo de nuestro ordenador a un servidor.

Hackers Término denostado por los medios de comunicación que se refiere al informático especializado o con inquietudes de salvar determinados retos complejos. Popularmente se le considera dedicado a la infiltración en sistemas informáticos con fines destructivos.

Hardware Elementos físicos que integran una computadora

Hosts Se denomina así a la computadora que se encarga de suministrar lo necesario a una red, dependiendo de cual sea la finalidad de ésta.

ICMP (Internet Control Message Protocol) es el responsable de proporcionar información de control sobre la capa IP. Se encarga, por ejemplo, de informar a la máquina origen de los posibles errores IP que puedan surgir a lo largo del tránsito de un datagrama.

ISACA (Information System audit. And Control Association)

Asociación de auditores de sistemas de información y control, su misión es capacitar, proporcionar estándares y desarrollo profesional a sus miembros y comunidad profesional en general. Es el ente certificador de CISA.

Netbios Es una interfaz entre aplicaciones que fue desarrollada por IBM para acceder a los recursos de redes locales.

OSI (Open Systems Interconnection) Sistema creado por ISO en el que se especifica estándares de funcionamiento de cada una de las partes o capas en las que puede constar una arquitectura de red. Las divide en siete niveles denominados: físico, de enlace, de red, de transporte, de sesión, de presentación y de aplicación. Son numerados del 1 al 7 y las referencias se suelen hacer sobre el número, por ejemplo el nivel 3 OSI se entiende como el de red.

Router Dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de brodcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast.

Ruteo Es básicamente informar y decidir cual es la ruta más eficiente para enviar información.

Scripts Es un programa que puede acompañar a un documento o que puede estar incluido en él. El programa se ejecuta en la máquina del cliente cuando se carga el documento o en algún otro instante.

SMTP (Simple Mail Transfer Protocol). Este protocolo es un estándar de Internet para el intercambio de correo electrónico.

Software Programas o aplicaciones instaladas en una computadora que tienen una funcionalidad especifica y ayuda al usuario a interactuar con el computador.

Sunpc Es un software que proporciona la emulación de un ambiente Microsoft, para poder ejecutar aplicaciones de DOS, Windows 3.11® y Windows 95® en estaciones de trabajo con sistema operativo Solaris.

Switch Dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos.

TCP/IP TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto TCP/IP. Es el protocolo común utilizado por todas las computadoras conectadas a Internet, de manera que éstos puedan comunicarse entre sí.

TI Siglas utilizadas en el cuerpo del trabajo, para resumir e identificar las palabras tecnología de la información

Tunning Mejorar el rendimiento de un sistema

Web Servidor de información www. Se utiliza también para definir el universo WWW en su conjunto.

RESUMEN

En muchas organizaciones la información y la tecnología con la que se cuenta son los activos más importantes y valiosos. En este contexto, las empresas enfrentan nuevos riesgos que deben ser mitigados a partir del establecimiento de normas respecto a la administración de la información, a la tecnología que la soporta, a los ambientes requeridos para la fundación de un área de sistemas, y a la estructura organizacional del área, entre otras.

Además, las organizaciones deben establecer una estructura de control diseñada de manera tal que contribuya; por una parte, al logro de los objetivos trazados por la organización y, por otra, a la detección de aspectos no previstos que pudieran impedir el logro de dichos objetivos. En ese sentido, los sistemas computarizados tienen el papel de contribuir a alcanzar dichos objetivos.

Las comunicaciones son una de las bases de los negocios modernos, sin las cuales ninguna empresa podría sobrevivir. Por eso la auditoría de telecomunicaciones cobra cada vez más relevancia, tanto a nivel nacional como internacional; debido a las constantes vulnerabilidades que se encuentran en las redes.

La auditoría de telecomunicaciones es un análisis orientado a proporcionar información y recomendaciones que les permite a las empresas determinar las acciones necesarias para crecer y alcanzar un nivel de rendimiento y disponibilidad de la red, acorde a las necesidades actuales y futuras de su negocio; sin comprometer la seguridad empresarial o institucional.

Cuando se realiza la auditoría de telecomunicaciones se evalúa el estado de la red, desde la perspectiva de su arquitectura, rendimiento y disponibilidad. El gerente de la empresa recibe un informe personalizado, que reporta el estado actual de cada componente, su nivel de impacto en el rendimiento de la red y las recomendaciones respectivas. Junto al diseño de la solución que le permitirá alcanzar el nivel de rendimiento y disponibilidad requeridos en la red.

OBJETIVOS

General

Desarrollar un estudio completo de la metodología utilizada actualmente en el ámbito guatemalteco para la realización de auditorías de telecomunicaciones.

Específicos

1. Definir la auditoría de telecomunicaciones y sus tendencias actuales en el mercado guatemalteco.

2. Identificar los riesgos más comunes en el área de telecomunicaciones.

3. Definir la minimización de riesgos mediante la utilización de la auditoría de telecomunicaciones.

4. Describir los estándares existentes para la auditoría de telecomunicaciones

INTRODUCCIÓN

Cada día es mayor el número de situaciones irregulares que se presentan, como consecuencia del uso y aplicación de la Tecnología de Información (TI.), en las diferentes organizaciones, entidades, empresas y compañías en general.

El conocimiento de esta tecnología se ha ampliado a todas las esferas; la gente aprende cada día más, es más estudiosa y conocedora; pero no todos están orientados puramente al conocimiento como aumento de calidad en todos los campos; a algunos les interesa aprender más que todo, para ver cómo efectúan o generan irregularidades en provecho propio; como producto de lo que conocen, adquieren destreza para utilizarlas con fines alevosos y malintencionados; situación que ligada a la pérdida de valores morales, éticos y religiosos en todos los niveles y estratos de la sociedad, ha originado todo tipo de acciones fraudulentas, y que se haga imposible para la administración, establecer controles que disminuyan los riesgos presentados.

Aunado a lo anterior, las aperturas comerciales, la globalización, las alianzas estratégicas, y las integraciones de todo tipo, de alguna manera han venido a complicar la situación en cuanto al sistema de control interno se refiere; también han recargado las funciones que deben realizar los auditores de sistemas.

1. AUDITORÍA DE SISTEMAS

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

La auditoria en tecnología de información es un conjunto de metodologías y herramientas que tienen por objeto principal el buscar que los recursos tecnológicos, humanos y económicos estén orientados a alinear los procesos de las organizaciones hacia los objetivos buscados.

La auditoría en informática deberá incluir no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar todos los procesos desde sus entradas, procedimientos, organización de centros de información, controles, archivos, seguridad y obtención de información.

La auditoría en informática es importante para el desempeño de los sistemas de información, ya que proporcionan los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

1.1 Conceptos de auditoría de sistemas

La palabra auditoría viene del latín *auditorius* y de esta proviene auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

- Es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relacionados con la planificación, control eficacia, seguridad y adecuación del servicio informático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vistas a mejorar en:

    - Rentabilidad
    - Seguridad
    - Eficacia

Algunos autores proporcionan otros conceptos pero todos coinciden en enfatizar en la revisión, evaluación y elaboración de un informe para el ejecutivo encaminado a un objetivo específico en el ambiente computacional y los sistemas.

Auditoría de sistemas es:

- La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación, para evaluar su efectividad y presentar recomendaciones a la Gerencia.

- La actividad dirigida a verificar y juzgar información.

- El examen y evaluación de los procesos del área de procesamiento automático de datos (PAD) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.

- El proceso de recolección y evaluación de evidencia para determinar si un sistema automatizado cumple con los controles internos necesarios.

1.2.- Objetivos generales de una auditoría de sistemas

El objetivo de la auditoría de sistemas informáticos es el de evaluar la eficiencia y eficacia con que se está operando para que se tomen decisiones que permitan corregir los errores, en caso de que existan o mejorar la forma de actuación.

Otro objetivo de la auditoría es la verificación de la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, deben revisarse sucesivamente y en este orden:

1. **Las normas generales de la instalación informática**. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta normativa general informática no está en contradicción con alguna norma general no informática de la empresa.

2. **Los procedimientos generales informáticos**. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de control de calidad. El alta de una nueva aplicación no debería producirse si no existieran los procedimientos de respaldo y recuperación correspondientes.

3. **Los procedimientos específicos Informáticos**. Igualmente, se revisara su existencia en las áreas fundamentales. Así, el área de control de calidad no debería certificar una aplicación sin haber exigido a desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los procedimientos específicos no se opongan a los procedimientos generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la normativa y los procedimientos generales de la propia empresa, a los que el área de informática debe estar sometida.

Entre los objetivos generales de la auditoría de sistemas informáticos se encuentran:

- Identificar procedimientos de control que minimicen los riesgos asociados a los sistemas informáticos.
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información.
- Buscar la seguridad del personal, los datos, el *hardware*, el *software* y las instalaciones.
- Conocer la situación actual del área informática para lograr los objetivos.
- Proporcionar el apoyo de la función informática a las metas y objetivos de la organización.
- Proporcionar seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Incrementar la satisfacción de los usuarios de los sistemas informáticos.
- Proporcionar capacitación y educación sobre controles en los Sistemas de Información.

- Apoyar la búsqueda una mejor relación costo-beneficio de los sistemas automáticos.

Los objetivos específicos de las normas técnicas de auditoría de sistemas son:

- Establecer una estructura básica, uniforme y eficiente de control interno administrativo y financiero en las entidades, proyectos y programas.

- Promover la evaluación oportuna, eficiente y económica de los sistemas administrativo y financiero de las entidades, proyectos y programas.

1.3.- Justificación para efectuar una auditoría de sistemas

Derivado de la importancia de la tecnología informática como factor crítico de éxito para las organizaciones. La toma de conciencia en las empresas de los riesgos inherentes a la actividad informática y de la necesidad de protección de altas inversiones que se dedican al diseño e implementación de sistemas de información.

Entre las razones prioritarias para efectuar una auditoría de sistemas se puede mencionar:

- Aumento considerable e injustificado del presupuesto del PAD (Departamento de Procesamiento de Datos)
- Desconocimiento en el nivel directivo de la situación informática de la empresa.
- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Descubrimiento de fraudes efectuados por medio de sistemas de información.
- Falta de una planificación informática.
- Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del recurso humano.
- Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados.
- Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción.

1.4. Tipos de auditoría aplicados en el mercado

1.4.1 Auditoría interna

Existen algunos tipos de auditoría entre los que la auditoría de sistemas integra un mundo paralelo pero diferente y peculiar resaltando su enfoque a la función informática. Entre los principales tipos de auditoría tenemos los siguientes discutidos a continuación.

"La Auditoría Interna es una función independiente de evaluación establecida dentro de una organización, para examinar y evaluar sus actividades como un servicio a la organización. El objetivo de la auditoría interna consiste en apoyar a los miembros de la organización en el desempeño de sus responsabilidades. Para ello la auditoría interna les proporciona, análisis, evaluaciones, recomendaciones, asesoría e información concerniente con las actividades revisadas."[1]

Es un control que funciona midiendo y evaluando la confiabilidad y eficiencia del sistema integral de control interno de la entidad con miras de lograr su mejoramiento.

1.4.2 Auditoría de gestión o auditoría operacional 1.4.3 Auditoría financiera y de cumplimiento

1.4.4 Auditoría integral

Es el examen integral de la gestión de un ente o empresa (o de una parte de ellos) en todos sus aspectos y en todos sus niveles, tomando en consideración los elementos humanos, materiales y económicos con el propósito de evaluar los defectos existentes, así como evaluar la eficiencia y eficacia de los resultados, tomando en cuenta para ello:

- Las metas y objetivos fijados.
- Los recursos humanos, financieros y materiales empleados.
- La organización y coordinación de dichos recursos y los controles establecidos para:
    - Determinar los defectos y proponer mejoras
    - Determinar las causas de los desvíos y proponer correcciones
    - Determinar el origen de los problemas y proponer soluciones.

Todo ello se traduce en un informe donde se suministran las recomendaciones, el profesional prestará la colaboración necesaria para alcanzar ese fin.

La auditoría financiera y de cumplimiento, cuyo objetivo es el de expresar una opinión sobre la razón de los estados financieros de conformidad con principios de contabilidad generalmente aceptados, evaluar el cumplimiento de las disposiciones legales, reglamentarias, contractuales, normativas y/o políticas aplicables y la evaluación de la eficacia de los sistemas de administración.

1.4.4 Auditoría Informática

Es la investigación, consulta, revisión, verificación, comprobación y evidencia. Aplicada a la empresa es el examen del estado financiero de una empresa realizada por personal cualificado e independiente, de acuerdo con normas de contabilidad, para esperar una opinión con que tales estados contables muestran lo acontecido en el negocio.

El departamento de informática posee una actividad proyectada al exterior, al usuario, aunque el **exterior** siga siendo la misma empresa. He aquí, la **auditoría informática de usuario.** Se hace esta distinción para contraponerla a la informática interna, en donde se hace la informática cotidiana y real. En consecuencia, existe una auditoría informática de actividades internas.

El control del funcionamiento del departamento de informática con el exterior, con el usuario se realiza por medio de la dirección. Su figura es importante, en tanto es capaz de interpretar las necesidades de la compañía. Una informática eficiente y eficaz requiere el apoyo continuado de su dirección

frente al **exterior**. Revisar estas interrelaciones constituye el objeto de la **auditoría informática de dirección**. Estas tres auditorías, mas la auditoría de seguridad, son las cuatro áreas generales de la auditoría informática más importantes.

Dentro de las áreas generales, se establecen las siguientes divisiones de auditoría informática: de producción, de sistemas, de comunicaciones y de desarrollo de proyectos. Estas son las áreas específicas de la auditoría informática más importantes.

Tabla I. Áreas específicas contra áreas generales de la auditoría informática

Áreas específicas	Áreas generales			
	Interna	Dirección	Usuario	Seguridad
Producción				
Desarrollo				
Sistemas				
Comunicaciones				
Seguridad				

Cada área específica puede ser auditada desde los siguientes criterios generales:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

1.4.4.2 Auditoría informática de producción

La producción se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La producción informática se puede considerar como una fabrica con ciertas peculiaridades que la distinguen de las reales. Para realizar el control de calidad se dispone de una materia prima, los datos, que sean necesarios transformar, y que se sometan previamente a controles de integridad y calidad. La transformación se realiza por medio del proceso informático, el cual está gobernado por programas. Después de obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar la producción consiste en auditar las secciones que la componen y sus interrelaciones. La producción informática se divide en tres grandes áreas: planificación, producción y soporte técnico, en la que cada cual tiene varios grupos.

La función de desarrollo es una evolución del llamado análisis y programación de sistemas y aplicaciones. A su vez, engloba muchas áreas,

tantas como sectores informáticos tiene la empresa. Muy escuetamente, una aplicación recorre las siguientes fases:

- Prerrequisitos del usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Codificación
- Pruebas
- Entrega al usuario final

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costos, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la máquina sean exactamente los previstos y no otros.

Una auditoría de aplicaciones pasa indiscutiblemente por la observación y el análisis de cuatro consideraciones:

- **Revisión de las metodologías utilizadas**: se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras versiones de la aplicación y el fácil mantenimiento de las mismas.

- **Control Interno de las aplicaciones**: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de desarrollo:

    - Estudio de vialidad de la aplicación
    - Definición lógica de la aplicación.
    - Desarrollo técnico de la aplicación.
    - Diseño de programas.
    - Métodos de pruebas
    - Documentación
    - Equipo de programación

- **Satisfacción de usuarios***:* una aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aprobación del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la aplicación

- **Control de procesos y ejecuciones de programas críticos***:* el auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de desarrollo de aplicaciones. Se ha de comprobar la correspondencia entre los programas fuente y los programa módulo no coincidieran podrá provocar, desde errores de bulto que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las librerías de programas; aquellos programas fuente que haya sido dado por

bueno por desarrollo, son entregados a control de calidad para que realice las validaciones correspondientes.

1.4.4.3 Auditoría informática de sistemas

Como este sistema para auditar y dar el alta a una nueva aplicación es bastante arduo y complejo, algunas empresas lo usarán, otras no. Otra metodología consiste en que el futuro usuario de esta aplicación use la misma como si la estuviera usando en producción para que detecte o se denoten por sí solos los errores de la misma. Estos defectos que se encuentran se van corrigiendo a medida que se realicen las pruebas.

Todas estas pruebas, auditoría lo tiene que controlar, tiene que evaluar que las mismas sean correctas y que exista un plan de prueba donde se encuentre involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan.

Se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones, líneas y redes de

las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de sistemas.

- **Sistemas operativos**: engloba los subsistemas de teleproceso, entrada/salida, etc. Debe verificarse en primer lugar que los sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los sistemas operativos permite descubrir las posibles incompatibilidades entre otros productos de *software* básico adquiridos por la instalación y determinadas versiones. Deben revisarse los parámetros variables de las librerías más importantes de los sistemas, por si difieren de los valores habituales aconsejados por el constructor.

- ***Software* básico**: es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al *software* desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no condicione al sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costos, por si hubiese opciones más económicas.
- ***Software* de teleproceso (tiempo real)**: no se incluye en *software* básico por su especialidad e importancia. Las consideraciones anteriores son válidas para éste también.

- ***Tunning****:* es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto. Las acciones de *tunning* deben diferenciarse de los controles habituales que realiza el personal técnico de sistemas. El *tunning* posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

    - Cuando existe sospecha de deterioro del comportamiento parcial o general del sistema
    - De modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor deberá conocer el número de *tunning* realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

- **Optimización de los sistemas y subsistemas**: el personal técnico de sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de *tunnings* preprogramados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la operatividad de los sistemas.

Una auditoría de redes es:

1.4.4.4 Auditoría Informática de comunicaciones y redes

1 Una valoración analítica de las políticas de seguridad en funcionamiento:

- **Internas** que verifican el estado de seguridad interior de la empresa, contemplando los controles a sus usuarios internos, la aplicación de sistemas antivirus, las restricciones de acceso, los sistemas de autenticación y la correcta configuración de los distintos servidores y equipos de comunicaciones en funcionamiento como *switches, routers*, servidores de correo y servidores *web*
- **Externas** que verifican la aplicación de las políticas de seguridad concernientes a reglas de cortafuegos, filtros de contenidos, accesos remotos, protecciones contra denegación de servicios y accesos no autorizados.

2 Una evaluación del correcto funcionamiento de un aplicativo desde el punto de vista de la privacidad y el control de acceso.

- Para obtener como resultado un conocimiento real de las políticas de seguridad en el momento de su aplicación y ejecución, en la mayoría de los casos luego de una auditoria y según las recomendaciones de los auditores, además de revisarse las políticas de seguridad, se efectúan modificaciones en los distintos sistemas y dispositivos.

- Para trabajar con conocimiento del funcionamiento y estructura de la empresa, los auditores realizan entrevistas al personal y verificaciones de las configuraciones de los sistemas operativos, tareas que pueden desarrollarse de manera presencial o remota.

Para el informático y para el auditor informático, el entramado conceptual que constituyen las redes, concentradores, multiplexores, redes locales, etc. no son sino el soporte físico-lógico del tiempo real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en comunicaciones y en redes locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de redes locales, diseñadas y cableadas con recursos propios).

El auditor de comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la red de comunicaciones, actualizada, ya que la no actualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre la cuantas líneas existen, cómo son y dónde están instaladas, supondría que se bordea la inoperatividad informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes (pantallas, servidores de redes locales, computadoras con tarjetas de comunicaciones,

impresoras entre otros). Todas estas actividades deben estar muy coordinadas y de ser posible, dependientes de una sola organización.

1.4.4.5 Auditoría de la seguridad informática

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado **virus** de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización (**piratas**) y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias **piratas** o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos para modificar la información con propósitos fraudulentos.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes

1.5 Etapas o pasos de la auditoría

Se requieren varios pasos para realizar una auditoría. El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos. El proceso de auditoría exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia. Asimismo, la gerencia de auditoría debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoría además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

Planificación, entendiendo por tal la elección del tipo de auditorias a realizar, la plasmación documental de los procedimientos de realización de las mismas, en el caso de la realización de una auditoría del producto, es necesaria

la programación de mediciones y ensayos a partir de los planos y normas de ensayo, la elección del personal auditor que puede ser único, o distinto en función del tipo de auditoría a realizar, y la fijación de su periodicidad (mensual, anual). En ocasiones, es conveniente asignar una única persona para planificar y dirigir la realización de todas las auditorias, es decir, nombrar un líder que reúna unas características idóneas en cuanto a formación y carácter, para la realización de esta tarea.

Realización de auditorías según procedimiento y plan definidos. Es conveniente que el personal que va a ser auditado conozca con antelación tal hecho, y lo mejor desde el punto de vista práctico es que la realización de auditorias sea sistemática, y el propio director o responsable del área a auditar transmita a sus subordinados afectados las fechas concretas en las que estas auditorias sistemáticas van a realizarse para que presten su mayor colaboración.

Posiblemente si se sigue este sistema, al recibir los responsables esta comunicación, tratarán de inculcar en sus subordinados la necesidad de que todo esté "en perfecto estado de revista" como se decía antiguamente, lo que inicialmente podría alterar los resultados, pero si las auditorias son periódicas, esto dejará de producirse, y sin embargo el que el responsable comunique a sus subordinados las fechas de realización, así como la recomendación de que presten su máxima colaboración, confiere a las auditorias un papel destacado e importante dentro del sistema. Los documentos que recojan los resultados de las auditorias, es decir, respuestas, comprobaciones, resultados de medidas y ensayos, entre otros, han de estar consensuados entre auditor y auditado, de tal forma que recojan la conformidad de ambos, evitándose discusiones inútiles.

Se trata de auditar la efectividad del sistema, tanto a través del propio sistema y su grado de cumplimiento, como a través de la calidad del producto obtenido, por lo que es necesario, para poder establecer las acciones correctoras, determinar el grado de cumplimiento del sistema, y su relación con la calidad del producto final. Si el fin del establecimiento de un sistema de calidad es obtener un producto de calidad es totalmente necesario comprobar su efectividad, sino se consigue este objetivo es necesario cambiar el sistema, y discutir o perseguir a las personas que lo aplican.

Evaluación de los resultados de la auditoría. Toda auditoría ha de realizarse para obtener una nota final que sirva, aunque solo sea comparativamente, para medir la evolución, tanto de la implementación del sistema, como de la calidad del producto. Lo que se pretende es la obtención de una valoración totalmente objetiva por lo que el sistema de valoración ha de ser consensuado, y además, experimentado durante cierto tiempo, para poder fijar las señales de alerta, índices de ponderación, entre otros.

Redacción de informe y propuesta de medidas correctoras: una vez valorada la auditoría y antes de la redacción del informe final y propuesta de las medidas correctoras, es conveniente la reunión con el director o responsable máximo afectado por la auditoría para que sea el primer informado y pueda incluso colaborar en la propuesta de medidas correctoras así como en la decisión sobre la urgencia de las mismas, pues es conveniente que tanto el informe de la auditoría como la propuesta de medidas correctoras, lo asuma como algo propio, entre otras cosas porque a veces,

podrá ejercer más presión sobre la gerencia que el propio auditor, sobretodo si alguna de las medidas propuestas corresponden o requieren inversiones.

2. ESTÁNDARES Y MODELOS DE CALIDAD EN AUDITORÍA DE TELECOMUNICACIONES

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) es reconocida internacionalmente como la entidad rectora y señala que las normas definen los requerimientos mandatarios para la auditoría de sistemas e informes relacionados.

El marco de estándares para la práctica profesional de la auditoría de sistemas de información está compuesto por las normas, las directivas y los procedimientos. Las normas son de cumplimiento obligatorio por parte de los auditores de sistemas. Las directivas son pautas de como se espera que el auditor cumpla con las exigencias planteadas por las normas. ISACA brinda ejemplos de procedimientos que podría seguir un auditor de sistemas de información. Los documentos contienen procedimientos que proporcionan información sobre la manera de cumplir con las normas al realizar tareas de auditoría de sistemas de información, pero no establecen la naturaleza especial de la auditoría de sistemas de información.

El desarrollo y distribución de estándares es la piedra angular de la contribución profesional que realiza ISACA a la comunidad de auditores

Los objetivos de las normas ISACA son

"L*os de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el código de ética profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto "*[2]

El alcance y autoridad de los estándares de auditoría de sistemas de ISACA provee múltiples niveles de estándares:

Estándares: definen los requerimientos obligatorios para la auditoría de sistemas y la generación de informes.

Guías: proveen una guía para la aplicación de los estándares de auditoría de sistemas. El auditor de sistemas debería tenerlos en consideración al implementar los estándares, usar su criterio profesional para aplicarlos y estar preparado para justificar cualquier diferencia.

Procedimientos: provee ejemplos de procedimientos que el auditor de sistemas puede utilizar en una revisión. Los procedimientos ofrecen información

de cómo cumplir con los estándares al realizar una auditoría de sistemas pero no especifican requerimientos.

Según el código de ética profesional de los auditores de sistemas de información están comprometidos a sostener las siguientes prácticas:

- Apoyar el establecimiento y cumplimiento de normas, procedimientos, controles y procesos de auditoría de sistemas de información.

- Cumplir las normas de auditoría de sistemas de información.

- Actuar en interés de sus empleadores, accionistas, clientes y del público en general en forma diligente, leal y honesta y no a sabiendas de ser parte de actividades impropias o ilícitas.

- Mantener la confidencialidad de la información obtenida en el curso de las actividades asignadas.

- La información no será utilizada para beneficio propio o divulgada a terceros no legitimados.

- Cumplir con sus deberes en forma independiente y objetiva, y evitar toda actividad que comprometa, o parezca comprometer su independencia.

- Mantener su competencia en los campos interrelacionados de la auditoría y los sistemas de información por medio de su participación en actividades de desarrollo profesional.

- Tener sumo cuidado al obtener y documentar suficiente material provisto por el cliente cuya consistencia servirá para basar sus conclusiones y recomendaciones.

- Informar a las partes involucradas acerca de los resultados de las tareas de auditoría llevadas a cabo.

- Apoyar la educación de la gerencia, los clientes, sus colegas y al público en general para mejorar la comprensión en materia de auditoría y de sistemas de información.

- Mantener altos los estándares de conducta y carácter tanto en las actividades profesionales y privadas como en las evidencias obtenidas en el desarrollo de la auditoría.

2.1 Estándar de la ISACA modelo por dominios COBIT

La Asociación de Auditoría y Control de Sistemas de Información (ISACA), a través de su fundación publicó en diciembre de 1995 el Cobit (*Control objectives for information and related Technology*) como consecuencia de cuatro años de intensa investigación y del trabajo de un gran equipo de expertos internacionales.

El marco de Cobit es la definición de estándares y conducta profesional para la gestión y control de los sistemas de información en todos sus aspectos, y unificando diferentes estándares, métodos de evaluación y controles anteriores.

Esta metodología aporta un factor diferencial enormemente importante como es la orientación hacia el negocio. Esta diseñada no solo para ser utilizada por usuarios y auditores sino también para gestionar los procesos de negocios.

La misión de COBIT es: "Investigar, desarrollar, publicar y promover un conjunto de objetivos de controlen tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores." [3]

COBIT está diseñado como un estándar aplicable y aceptable en general para la buena práctica de la auditoría de las tecnologías de la Información en todo el mundo. COBIT utiliza los Objetivos de Control de ISACA, mejorados con estándares específicos de tipo técnico, profesional, normativo e industrial existentes y emergentes.

Los objetivos de control se han desarrollado para su aplicación en una amplia visión de sistemas de información en la empresa. Estos objetivos de control tienen en cuenta lo siguiente:

- Adecuación a los estándares y normativas legislativas y de hecho existentes que se aplican en el marco global, así como en los objetivos de control individuales.

- Revisión crítica de las diferentes actividades y tareas bajo los dominios de control y posibilitando la especificación de indicadores de prestaciones importantes (normas, reglas entre otros).

- Establecimiento de unas directrices y fundamentos para proporcionar investigación consistente sobre los temas de auditoría y control de Tecnología e Información.

El sistema consiste en objetivos de control de tecnología e información de alto nivel y una estructura global para su clasificación y funcionamiento. La teoría para la clasificación elegida, con las experiencias de re-ingeniería, es que hay, en esencia tres niveles de esfuerzos cuando se considera la gestión de los recursos en tecnología e información:

- **Actividades**: las actividades, junto con las tareas están en el nivel inferior. Las actividades tienen el concepto de ciclo de vida mientras que las tareas se consideran discretas en el tiempo.

- **Procesos**: se definen en un nivel superior como series de actividades unidas con puntos de controles naturales.

- **Dominios**: correspondientes al nivel superior, son agrupaciones de procesos. COBIT distingue cuatro dominios en línea con el ciclo de gestión o el ciclo de vida aplicables a los procesos de Tecnología e Información (ver figura 1)

Dominios de COBIT

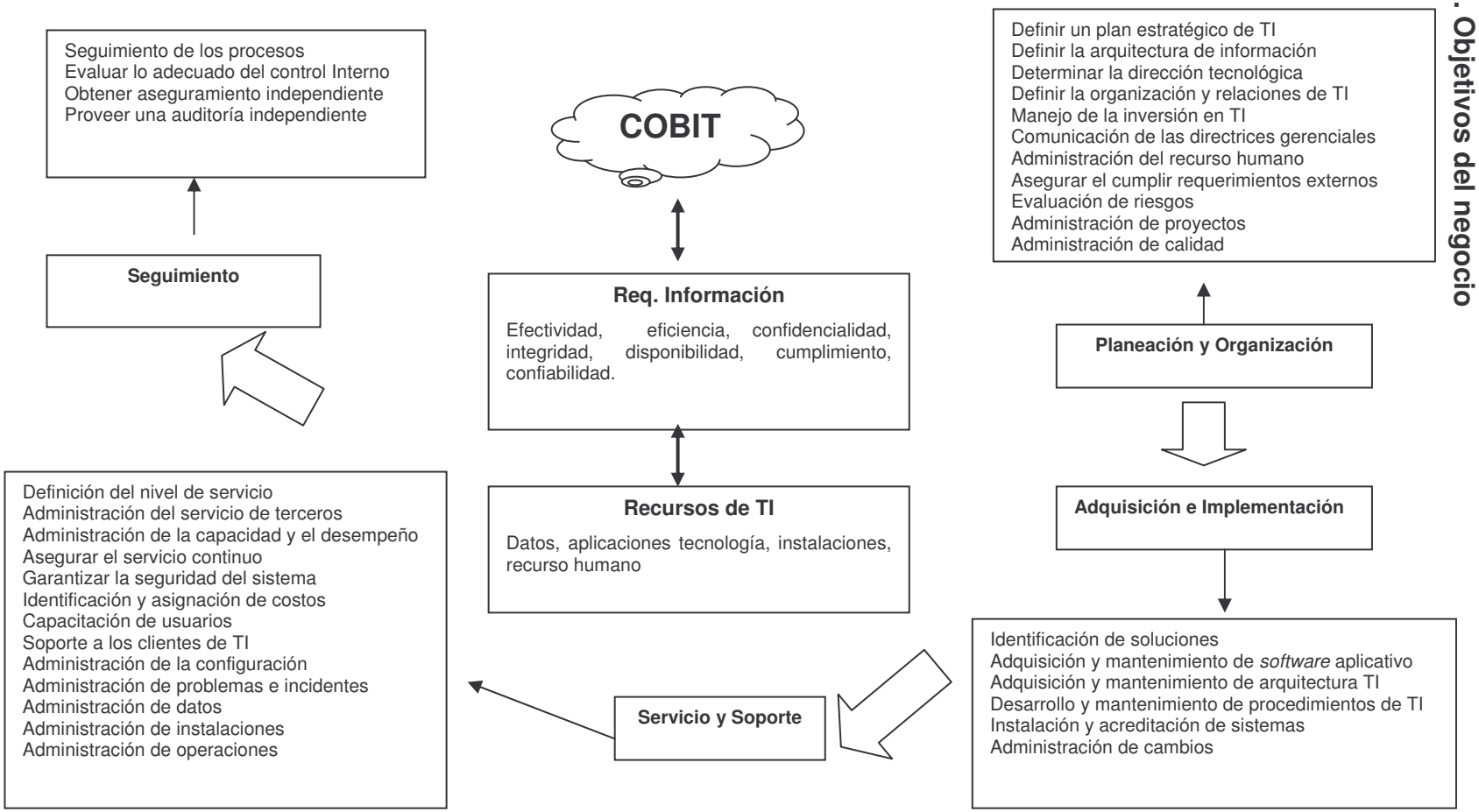
- **Planificación y organización.** Conduce la estrategia y las tácticas y corresponde a la identificación de la forma en que la información tecnológica puede contribuir mejor a alcanzar los objetivos de gestión.

- **Distribución y soporte.** Corresponde con la distribución normal de los servicios requeridos, que van desde las tradicionales operaciones sobre seguridad y continuidad hasta la formación.

- **Adquisición e implementación.** Para llevar a cabo la estrategia es necesario identificar, desarrollar y adquirir soluciones de TI apropiadas, así como implementarlas e integrarlas en los procesos de gestión.

- **Monitorización.** Todos los procesos de TI deben evaluarse regularmente en el tiempo para comprobar su calidad

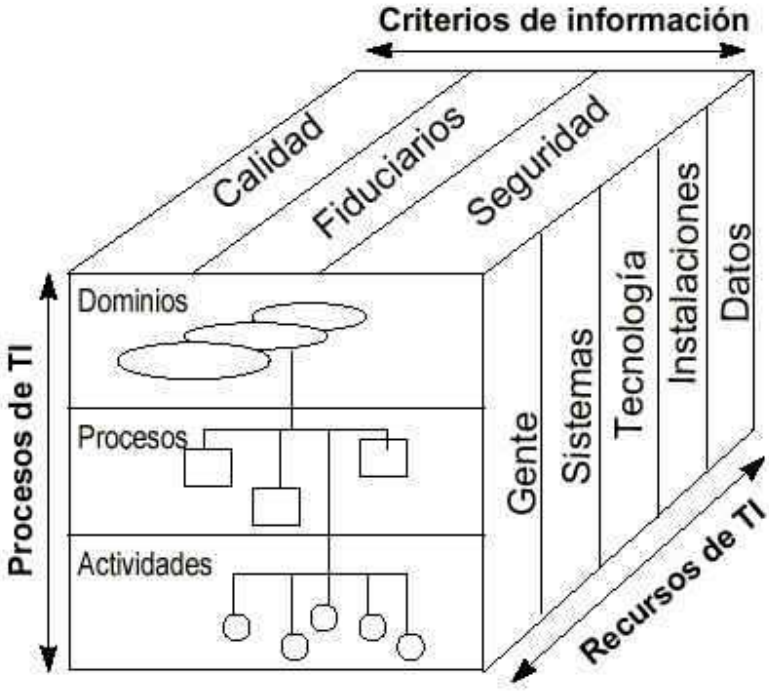
Figura 1. Objetivos del negocio



Fuente: CObIT–Objetivos de Control para la Información Pública y Tecnologías Relacionadas

El marco conceptual se enfoca desde tres puntos de vista distintos: criterios de gestión para la información, recursos de TI y procesos de TI. Estos tres puntos de vista se ensamblan en un formato cúbico y permiten que se obtengan referencias cruzadas en dicho marco y se pueda acceder a él eficientemente (ver figura 2).

Figura 2. Cubo de CobiT Relación entre los componentes



Fuente: COBIT–Objetivos de Control para la Información Pública y Tecnologías Relacionadas

Los objetivos de control de tecnología e información están organizados inicialmente por proceso/actividad, pero las ayudas para la navegación que se aportan, facilitan la entrada desde cualquier punto estratégico. También facilitan la adopción de enfoques combinados o globales, tal como la instalación/implementación de un proceso, responsabilidades de gestión global para un proceso, y el uso de los recursos de TI por un proceso.

La información que los procesos de gestión necesitan está proporcionada por el uso de los recursos de tecnología e información. Para asegurar que los requisitos de gestión para la información se aplican, se tiene que definir medidas de control adecuadas, se tiene que implementarlas y monitorizarlas sobre estos recursos. Está claro que no todas las medidas de control satisfarán los requisitos de gestión en el mismo grado, así que se hace una distinción en COBIT contemplando el cumplimiento:

Normas de auditoría de sistemas de información

- **Responsabilidad y autoridad**. La responsabilidad y autoridad de las funciones de la auditoría de sistemas de información deben ser correctamente documentadas en los estatutos de la auditoria.

- **Independencia profesional**. En todos los casos relacionados con la auditoria, el auditor de sistemas debe ser independiente del auditado tanto en actitud como en apariencia.

- **Relación organizacional**. La función de auditoria de sistemas debe ser suficientemente independiente del área que esta siendo auditada para permitir la culminación objetiva de la auditoria.

- **Ética profesional y normas**. El auditor de sistemas deberá cumplir con el código de ética profesional de la asociación.

- **El debido cuidado profesional**. Además de la observancia de las normas profesionales de auditoría aplicables deben llevarse a cabo en todos los aspectos del trabajo de auditoria de sistemas.

- **Competencia.** El auditor de sistemas debe ser técnicamente competente, teniendo las habilidades y conocimientos necesarios para llevar a cabo el trabajo del auditor.

- **Educación profesional continua**. El auditor de sistemas deberá mantener su competencia técnica por medio de una apropiada educación profesional continua.

- **Desempeño del trabajo de auditoría.** El personal de auditoría de sistemas deberá ser apropiadamente supervisado para garantizar que los objetivos de la auditoría sean logrados y que las normas de auditoria profesional aplicables se cumplan.

2.2 Estándares para la auditoría de la seguridad de redes

La política de auditoría y seguridad informática debe formar parte de los lineamientos generales a desarrollarse en base a las directivas emanadas de la gerencia general y formará parte del compromiso de ésta en su aplicación. En ella se deberá establecer con claridad y precisión las metas a alcanzar y las responsabilidades asignadas. Se puede sintetizar cuatro ejes por los cuales debería establecerse esta política:

- Programa general de auditoría y seguridad general de la organización.
- Programa de auditorías informáticas a implementar.
- Programa sobre temas específicos como contingencias, seguridad física, entre otros.
- Programas específicos sobre sistemas de información determinada.

Estos ejes de desarrollo deberán propender a la utilización de la información con una óptima relación costo-beneficio permitiendo compartir la información y ayudar a aprovechar mejor los recursos destinados a la tecnología informática (TI) en todo su potencial. Algunos de los elementos a tener en cuenta al momento de implementar una política de auditoría y seguridad informática serán, por ejemplo:

- Establecimiento de una función que lleve a cabo la administración del programa de auditoría y seguridad informática que sea reconocida por toda la organización.

- Estándares, normativas, entre otros que respalden las medidas tomadas.

Por último, se deberá analizar con detalle las pautas a considerar para la evaluación del nivel de cobertura existente ante situaciones de desastres, la identificación en forma anticipada de los factores de riesgo y la planificación de las acciones a seguir.

A nadie escapa la formidable expansión que ha tenido en estos últimos años la "red de redes" o lo que comúnmente se le llama "autopista de la información" permitiendo el acceso de la información de todo tipo a todo el mundo a un costo considerablemente bajo. Además, esta nueva tecnología realmente ha convertido el modo de comunicarse, relacionarse comercial, académica y profesionalmente, de una manera como nunca antes existió. Este formidable cambio, en tan poco tiempo, ha hecho que, tecnológicamente, aún no se hayan desarrollado los elementos de seguridad suficientes para garantizar una absoluta privacidad e integridad de los datos que viajan por la red.

No obstante, los expertos en seguridad informática han desarrollado sistemas que, bajo ciertas condiciones, y, con determinados elementos, nos permiten la utilización de la red con un grado de seguridad aceptable.

En estas primeras etapas del desarrollo de seguridad en *Internet*, se ha comenzado ha trabajar con cuatro componentes fundamentales, que son:

- **Autenticación e identificación: t**écnica que nos permiten individualizar al autor de determinada acción.
- **Autorización:** técnica que permite determinar a qué información tienen acceso determinadas personas.
- **Integridad de datos**: técnica que garantiza que los datos que viajan por la red lleguen intactos a su destino.
- **Privacidad de datos**: técnica que determina quién puede leer la Información una vez que salió del sistema de almacenamiento.

El grado de avance en estas tecnologías utilizando sistemas de *firewalls* físicos y lógicos como así también, *encripción* de datos nos permite, con un diseño apropiado utilizar esta tecnología como la interfase natural de comunicación en todos nuestros sistemas de información, permitiendo que de cualquier parte del mundo se pueda acceder a ellos con la seguridad adecuada.

2.3 Estándares para la administración de acceso a la información

Se puede decir que los controles de acceso a la información constituyen uno de los parámetros más importantes a la hora de administrar seguridad. Con

ellos se determina quién puede acceder a qué datos, indicando a cada persona un tipo de acceso (perfil) específico.

Para este cometido se utilizan diferentes técnicas que se diferencian significativamente en términos de precisión, sofisticación y costos. Se utilizan por ejemplo, palabras claves, algoritmos de *encripción,* listas de controles de acceso, limitaciones por ubicación de la información, horarios, etc.

Una vez determinados los controles de accesos a la información, se hace imprescindible efectuar una eficiente administración de la seguridad, lo que implica la implementación, seguimiento, pruebas y modificaciones sobre los **perfiles** de los usuarios de los sistemas.

Este es uno de los puntos fundamentales a tener en cuenta para garantizar la seguridad y al mismo tiempo una correcta accesibilidad a la información. En efecto, en todo proyecto informático que pretenda brindar información a diferentes niveles, garantizando correcta toma de decisiones y accesibilidad a un amplio espectro de usuarios, se deberá prestar mucha atención a este punto.

Para ello, es importante que se plantee en la organización, la necesidad de establecer estándares para la administración de seguridad de accesos. Con ello se garantizará un eficiente, seguro y al mismo tiempo correcto uso de la información

3. METODOLOGÍA DE UNA AUDITORÍA DE TELECOMUNICACIONES

La auditoría en telecomunicaciones debe respaldarse en un proceso formal que asegure su previo entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la empresa. Al igual que otras funciones en el negocio, la auditoría en informática efectúa sus tareas y actividades mediante una metodología.

No es recomendable fomentar la dependencia en el desempeño de esta importante función sólo con base en la experiencia, habilidades, criterios y conocimientos sin una referencia metodológica. Contar con un método garantiza que las cualidades de cada auditor sean orientadas a trabajar en equipo para la obtención de resultados de alta calidad y de acuerdo a estándares predeterminados.

La metodología de auditorías de telecomunicaciones depende de lo que se pretenda revisar o analizar, pero como estándar se analizarán las cuatro fases básicas de un proceso de revisión:

- **Estudio preliminar**. Incluye definir el grupo de trabajo, el programa de auditoría, efectuar visitas a la unidad informática para conocer detalles de la misma, elaborar un cuestionario para la obtención de información para

evaluar preliminarmente el control interno, solicitud de plan de actividades, manuales de políticas, reglamentos, entrevistas con los principales funcionarios.

- **Revisión y evaluación de controles y seguridades**. Consiste en la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas criticas, revisión de procesos históricos (respaldos), revisión de documentación y archivos, entre otras actividades.

- **Examen detallado de áreas críticas.** Con las fases anteriores el auditor descubre las áreas criticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcance recursos que usara, definirá la metodología de trabajo, la duración de la auditoría, presentará el plan de trabajo y analizara detalladamente cada problema encontrado con todo lo anteriormente analizado en este folleto.

- **Comunicación de resultados**. Se elaborara el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el cual presentará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la auditoría. El informe debe contener lo siguiente:

- Motivos de la auditoría
- Objetivos
- Alcance
- Estructura orgánico-funcional del área informática
- Configuración del *hardware* y *software* instalado
- Control interno
- Resultados de la auditoría

3.1. Introducción a las metodologías

La metodología es un conjunto de métodos que se siguen en una investigación científica, lo cual significa que cada proceso científico debe estar sujeto a una disciplina definida con anterioridad a la cual se le da el nombre de metodología.

La metodología se hace necesaria en materias como la informática, ya que sus aspectos son muy complejos y la cual se utiliza en cada doctrina que compone dicha materia, siendo de gran ayuda en la auditoría de los sistemas de información.

El nacimiento de metodología en el mundo de la auditoría y el control informático se puede observar en los primeros años de los ochenta, naciendo a la par con la informática; la cual utiliza la metodología en disciplinas como la seguridad de los sistemas de información, la cual la definimos como la doctrina que trata de los riesgos informáticos, en donde la auditoría se involucra en este

proceso de protección y preservación de la información y de sus medios de proceso.

En informática existen riesgos los cuales pueden causar grandes problemas en entidades, por lo cual hay que proteger y preservar dichas entidades con un entramado de contramedidas, la calidad y la eficacia de la mismas es el objetivo a evaluar para identificar sus puntos débiles y mejorarlos; esta es una función de los auditores informáticos. Una contramedida nace de la composición de varios factores como:

- **La normativa**: es donde se define de forma clara y precisa todo lo que debe de existir y ser cumplido. Se inspira en estándares, políticas, marco jurídico, y normas de la empresa.
- **La organización**: la integran personas con funciones específicas y con actuaciones concretas, procedimientos definidos y aprobados por la dirección de la empresa.
- **Las metodologías**: son muy necesarias para desarrollar cualquier proyecto que queramos hacer de forma ordenada y eficaz.
- **Los objetivos de control**: son los objetivos a cumplir en el control de procesos
- **Los procedimientos de control**: son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control, por lo cual deben estar aprobados por la dirección
- **La tecnología de seguridad**: esta en todos los elementos, ya sea *hardware* o *software*, que ayuden a controlar el riesgo informático.

- **Las herramientas de control**: son los elementos *software* que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

Todos estos factores están relacionados entre sí, así como la calidad de cada uno de ellos con la de los demás y al evaluar el nivel de seguridad en una entidad, lo que se está evaluando son estos factores y se plantea un plan de seguridad nuevo que mejore todos los mismos a medida que se va realizando los distintos proyectos del plan, dicho plan de seguridad no es más que una estrategia planificada de acciones y proyectos que lleven a mejorar un sistema de información.

En la seguridad de sistemas se utilizan todas las metodologías necesarias para realizar un plan de seguridad además de la auditoría informática. Existen dos metodologías de evaluación de sistemas son las de **Análisis de Riesgos** y las de **auditoria informática**, con dos enfoques distintos. La auditoría informática solo identifica el nivel de exposición por la falla de controles, mientras el análisis de riesgos facilita la evaluación de los riesgos y recomienda acciones en base al costo-beneficio de las mismas.

3.2. Herramientas de control y auditoría informática

Las herramientas de control son elementos que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control. Son los métodos prácticos de investigación y prueba que el auditor utiliza para comprobar la racionabilidad de la información que le permita emitir su opinión profesional.

Las herramientas de control son de dos tipos lógicos y físicos, desde el punto lógico son programas que brindan seguridad. Las herramientas han sido instrumento para integrar la auditoría interna y el riesgo de la administración.

Para el buen desempeño de la auditoría en informática es importante definir las técnicas y herramientas necesarias y fundamentales para revisar eficientemente cada área seleccionada.

Un claro ejemplo es el *software* que incluyen un conjunto de técnicas como análisis, documentación, muestreo, entre otros, resultan elementos indispensables para asegurar la calidad y confiabilidad de la auditoría.

La experiencia profesional que se haya obtenido en cada una de las áreas (desarrollo, telecomunicaciones, mantenimiento, base de datos, seguridad, entre otros) hace más viable la auditoría como la definición de soluciones

Las herramientas de control interno, deberán estar integradas en los procedimientos y acciones normales de la entidad. Las herramientas permiten alcanzar los objetivos de control interno y se resumen en cuatro grupos:

3.2.1 Cuestionarios

- De validación que comprenden los mecanismos de autorización, comparación y verificación de validez.
- De perfección que incluyen la numeración consecuencial, los totales de control, los archivos dependientes y las listas de recordatorio.
- De reejecución que se refieren a la doble verificación y al control previo.
- De disciplina que están dadas por la segregación de funciones, el acceso restringido, la supervisión y la auditoría interna.

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando el cumplimiento de cuestionarios preimpresos que se envían a las personas concretas que el

auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

3.2.2. Entrevistas

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado

La entrevista es una de las actividades personales más importante del auditor; en ellas, se adquiere más información, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
- Mediante 3.2.3 Listas de cotejo entrevistas en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
- Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con esmero a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de

análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas redundantes que no conducen a nada. Por el contrario, el auditor conversará y hará preguntas normales, que en realidad servirán para la complementación sistemática de sus listas de cotejo.

Hay opiniones que descalifican el uso de las listas de chequeo, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto, no es usar listas de chequeo, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de listas de chequeo. Salvo excepciones, las listas de chequeo deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el modo del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de auditoría Informática guardan sus listas de chequeo, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. Debe recordarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la lista de cotejo de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las listas de cotejo utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas, el auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o lista de cotejo responden fundamentalmente a dos tipos de filosofía de calificación o evaluación:

- **Lista de cotejo por rango**. Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)
- **Lista de cotejo binaria**. Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Las listas de cotejo por rango son adecuadas si el equipo auditor no es muy mayor y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la lista de cotejo binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las listas de cotejo del tipo binario siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen listas de cotejo estándar para todas y cada una de las instalaciones informáticas por auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

3.2.4.7 Trazas o huellas

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos *software* muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del sistema, los auditores informáticos emplean productos que comprueban los valores asignados por técnica de sistemas a cada uno de los parámetros variables de las librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones desnivelan el número con el cual se inicia los trabajos de determinados entornos o toman criterios especialmente restrictivos en la asignación de unidades de servicio según los tipos de carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

Las bitácoras son un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan las bitácoras para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la aplicación (grabar, modificar, borrar) dentro de esa transacción, queda grabado en la bitácora. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por alguna razón, lo que se hace es volver para atrás. Las bitácoras permiten analizar cronológicamente que es lo que sucedió con la información que está en el sistema o que existe dentro de la base de datos.

3.2.6 *Software* de interrogación

Hasta hace ya algunos años se han utilizado productos *software* llamados genéricamente paquetes de auditoría, capaces de generar programas para auditores escasamente calificados desde el punto de vista informático.

Posteriormente, los productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos de *software* especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de archivos y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del *software* nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía cliente-servidor, han llevado a las firmas de *software* a desarrollar interfaces de transporte de datos entre computadoras personales y *mainframe,* de modo que el auditor informático copia en su propia computadora la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la compañía. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de procesadores de texto, paquetes de gráficos, hojas de cálculo, entre otros.

3.3. Metodologías de evaluación de sistemas

En el mundo de la seguridad de sistemas se utilizan todas las metodologías necesarias para realizar un plan de seguridad además de las de auditoría informática.

Las dos metodologías de evaluación de sistemas por excelencia son las de análisis de riesgos y las de auditoría informática, con dos enfoques distintos. La auditoria informática solo identifica el nivel de exposición por la falta de controles, mientras el análisis de riesgo facilita la evaluación de los riesgos y recomienda acciones en base al costo-beneficio de las mismas.

Algunas definiciones para profundizar en estas metodologías son las siguientes:

- **Amenaza:** una persona o cosa vista como posible fuente de peligro o catástrofe.
- **Vulnerabilidad:** la situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera hacerse y así afectar al entorno informático.

- **Riesgo:** la probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad
- **Exposición o impacto**: la evaluación del efecto del riesgo.

Las amenazas reales se presentan de forma compleja y son difíciles de predecir.

3.4. Metodología de análisis de riesgos

Las metodologías de análisis de riesgo se utilizan desde los años sesenta, en la industria del seguro basándose en grandes volúmenes de datos estadísticos agrupados en tablas actuarías. Se emplearon en la informática en los ochenta, y adolecen del problema de que los registros estadísticos de incidentes son escasos y por tanto el rigor científico de los cálculos probabilísticas es pobre. Aunque existen bases de incidentes en varios países, estos datos no son muy fiables por varios motivos: la tendencia a la ocultación de los afectados, la localización geográfica, las distintas mentalidades, la informática cambiante, el hecho de que los riesgos se presenta en un periodo solamente.

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: Las cuantitativas y las cualitativas, de las que existen gran cantidad de ambas clases y sólo se mencionaran algunas.

Con base en la realización de cuestionarios se identifican vulnerabilidades y riesgos y se evalúa el impacto para más tarde identificar las contramedidas y el costo.

3.4.1 Análisis y gestión de riesgos

De forma genérica, las metodologías existentes se diferencian en:

- Si son cuantitativas o cualitativas, o sea si utilizan un modelo matemático o algún sistema cercano a la elección subjetiva.

- Se diferencian en el propio sistema de simulación

El esquema básico de una metodología de análisis de riesgo es en esencia el siguiente:

La generalización del uso de las tecnologías de la información y de las comunicaciones es potencialmente beneficiosa para los ciudadanos, las empresas y la propia administración pública, pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en su utilización.

No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a estos

riesgos, al estado de la tecnología y a los costos (tanto de la ausencia de seguridad como de las salvaguardas).

La metodología de análisis y gestión de riesgos de los sistemas de información, es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos

3.5. Metodología de auditoría y control informático

Las únicas metodologías en la auditoría informática son de dos familias distintas; las auditorías de controles generales como producto estándar de las auditorías profesionales, que son una verificación de las mismas a nivel internacional, y las metodologías de los auditores internos.

El objetivo de las auditorías de controles generales es ofrecer una opinión sobre fiabilidad de los datos del ordenador para la auditoría financiera. El resultado exterior es un resumido informe como parte del informe de auditoria donde se destacan las vulnerabilidades encontradas. Están basados en

pequeños cuestionarios estándares que dan como resultado informes muy general.

Tienen aparatos para definir pruebas y anotar sus resultados. Ésta es una característica clara de la diferencia con las metodologías de evaluación de la consulta como las de análisis de riesgo que no tienen estos aparatos, aunque también tratan de identificar vulnerabilidades o falta de controles. Este tipo de auditorías deben de demostrar con pruebas todas sus afirmaciones, y por ello siempre debe contener el apartado de las pruebas. Llegando al extremo de que hay auditorías que se basan sólo en pruebas como la auditoria de integridad.

Estas metodologías están muy desprestigiadas, pero no porque sean malas en sí mismas, sino porque dependen mucho de la experiencia de los profesionales que las usan y existen una práctica de utilizarlas profesionales sin ninguna experiencia.

Es necesario decir que la metodología de auditor interno debe ser diseñada y desarrollada por el propio auditor, y esta será la significación de su grado de experiencia y habilidad.

Entre las dos metodologías de evaluación de sistemas (análisis de riesgo y auditoría) existen similitudes y grandes diferencias. Ambas tienen papeles de trabajo obtenidos del trabajo de campo tras el plan de entrevistas, pero los

cuestionarios son totalmente distintos. El auditor interno debe crear sus metodologías necesarias para auditar los distintos aspectos o áreas que defina en el plan auditor.

3.5.1 Plan del auditor informático

El plan de auditoría es el esquema metodológico más importante del auditor informático. Este documento define los métodos, procedimientos y calendarios de las auditorías informáticas, deberá ser elaborado de acuerdo con los objetivos, políticas y prioridades de la empresa.

El objetivo del plan de auditoría es organizar la actividad de la función de auditoría en relación de los riesgos y de las exigencias legales, así como de los recursos y costos necesarios.

Las partes de un plan auditor informático deben ser al menos las siguientes:

- Debe existir una clara segregación de funciones con la informática y control interno informático y debe ser auditado también. Deben describirse las funciones de forma precisa, y la organización interna del departamento con todos sus recursos.
- Procedimientos para las distintas tares de las auditorias. Entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoria, redacción de informe final, etc.

- Tipos de auditoría que realiza. Metodologías y cuestionarios de las mismas.
- Sistema de evaluación y los distintos aspectos que evalúa. Independientemente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar como nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas, etc., así como realizar una evaluación global de resumen para toda la Auditoría.
- Plan de trabajo anual. Deben estimarse tiempos de manera racional y componer un calendario que una vez terminado nos dé un resultado de horas trabajo previstas y por tanto de los recursos que se necesitan

3.6. El informe de la auditoría

En una primera aproximación, puede decirse que el informe de auditoria de sistemas de información es un documento que presenta el trabajo efectuado por el auditor y su opinión profesional sobre la totalidad.

El objetivo de la auditoría variara según se observe ante una situación u otra, pero el resultado final reflejará un conjunto de los elementos personales, temporales, identificativos de alcance y de opinión, que incluye conclusiones recomendaciones, salvedades (reservas y calificaciones) y fallos significativos detectados. La finalidad y los usos de dicho informe, sean cuales fueren, justifican la auditoría y su realización por el susodicho auditor, en función de dos

de sus atributos capitales: la competencia técnica profesional y la independencia.

Si se parte del hecho de que quien realiza auditorias de sistemas de información es un auditor de sistemas de información, sobreviene inmediatamente un problema: la legislación. Por tanto, bien cabe apuntar que los auditores de sistemas de información no existen (oficialmente) ante la escasa doctrina que se presenta sobre los mismos.

El objetivo de la auditoría de sistemas de información es el informe, documento inequívocamente vinculado a su autor o autores, convenientemente autenticado, con garantías de integridad y de acceso permitido a quienes estén autorizados, en el que el auditor da su opinión profesional independiente al destinatario. Este informe tiene valor para el auditado, y también en ciertos supuestos y escenarios, para terceros y para organismos de control.

El informe de auditoría es el producto final del trabajo del auditor de sistemas, este informe es utilizado para indicar las observaciones y recomendaciones a la gerencia, aquí también se expone la opinión sobre lo adecuado o lo inadecuado de los controles o procedimientos revisados durante la auditoría, no existe un formato específico para exponer un informe de auditoría de telecomunicaciones; pero, generalmente, presenta la siguiente estructura o contenido:

- Introducción al informe, donde se expresara los objetivos de la auditoría, el período o alcance cubierto por la misma, y una expresión general sobre la naturaleza o extensión de los procedimientos de auditoría realizados.
- Observaciones detalladas y recomendaciones de auditoría.
- Respuestas de la gerencia a las observaciones con respecto a las acciones correctivas.
- Conclusión global del auditor expresando una opinión sobre los controles y procedimientos revisados.

4. AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES

En un medio cambiante y en especial en las nuevas tecnologías informáticas y de comunicación, no ha pasado mucho tiempo sin que las condiciones varíen, esto puede llevar a nuevos riesgos y debe actuarse pro-activamente para lograr los sistemas auto controlados que tanto se pregonan.

La labor de auditoría entendida como la evaluación y análisis de esa realidad, en forma critica, objetiva e independiente, con el objeto de evaluar el grado de protección que presenta una instalación ante las amenazas a que está expuesta; es parte importante del diseño e implantación de políticas de seguridad. No basta con diseñar buenas políticas es necesario llevarlas a la práctica en forma correcta y garantizar que se adecuan a nuevas condiciones.

Día a día, las compañías depositan su confianza en redes internas y externas como forma de enviar y recibir información crítica entre clientes, proveedores y personas, y manipular así sus bases de datos. Sin embargo, hay muchos puntos de la red donde pueden interceptarse, copiarse y desviarse los datos o mensajes. A pesar de que las compañías aplican mecanismos de alta seguridad para mantener a los que las atacan lejos de sus redes, es probable que algunos consigan entrar. Los procesos de cifrado y autentificación garantizan que, aunque haya una violación de seguridad, externa o interna, la información de la empresa esté segura.

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales; entre otros.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

La seguridad informática se la puede dividir como general y como especifica (seguridad de explotación, seguridad de las aplicaciones, etc.). Así, se podrán efectuar auditorias de la seguridad global de una instalación informática –seguridad general- y auditorías de la seguridad de un área informática determinada – seguridad específica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la seguridad informática a nivel físico. Los accesos y conexiones indebidos a través de las redes de comunicaciones, han acelerado el desarrollo de productos de seguridad lógica y la utilización de sofisticados medios.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales).
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una auditoría informática de seguridad global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran matrices de riesgo, en donde se consideran los factores de las amenazas a las que está sometida una instalación y los impactos que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada (amenaza-impacto), en

donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

Tabla II. Matriz de amenaza contra impacto

Impacto	Amenaza				1: Improbable 2: Probable 3: Certeza 4:Despreciable
	Error	Incendio	Sabotaje	……..	
Destrucción de *hardware*	-	1	1		
Borrado de Información	3	1	1		

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

4.1.1 Auditoría de la calidad

Una auditoría de calidad es una revisión independiente realizada para verificar que el sistema de calidad implementado alcance los objetivos establecidos.

El término independiente es importante y su significado es que el auditor, no es la persona responsable de la efectividad del sistema que se audita. Una auditoría independiente proporciona un panorama no sesgado del desempeño.

La auditoría de calidad es un examen y evaluación sistemática, independiente, para determinar si las actividades de calidad y los resultados cumplen con lo planeado, si se implementa de manera efectiva y son adecuados para lograr los objetivos.

El propósito de las auditorías de calidad es proporcionar el aseguramiento de que:

1. Los planes de calidad son tales, que si se siguen, se logrará la calidad que se persigue.
2. El producto o servicio que se entrega es útil al usuario.
3. Se cumplen los estándares de calidad y requisitos establecidos en Normas para la Acreditación o Certificación.
4. Existe conformidad con las especificaciones.
5. Los procedimientos son adecuados y se siguen.
6. El sistema de datos proporcione información precisa y adecuada sobre la calidad a todos los interesados.
7. Se identifiquen las deficiencias y se tomen acciones correctivas.
8. Se identifiquen las oportunidades de mejoramiento y se comunican al personal pertinente.

Todos los temas mencionados anteriormente dan cuenta de que una auditoría tiene implícita la idea de ayuda para mejorar continuamente, esto no se entiende así siempre sino que se percibe como una amenaza, como algo que sacará a relucir todas las fallas. Si se logra cambiar este concepto resulta tremendamente beneficioso para todas las partes.

4.1.1 Características del control de calidad

Para lograr que los auditados se enfrenten a este proceso con una actitud constructiva, se necesita contar con las siguientes condiciones:

- Auditados honestos y sin temores a decir la verdad.
- Auditores con los conocimientos necesarios y una actitud personal constructiva y no crítica.
- Que la gerencia o dirección de la entidad auditada posea el criterio y la claridad suficiente, para entender que las deficiencias no parten de las personas, sino del sistema en que se desempeñan.
- Se brindan estas condiciones para la ejecución de un proceso de auditoría, sin duda que será muy beneficioso y se logrará entender el real espíritu que ellas tienen, ya que fueron creadas para propiciar la mejora y el crecimiento continuo de las organizaciones

El control de la calidad se posesiona como una estrategia para asegurar el mejoramiento continuo de la calidad. Es un programa para asegurar la continua satisfacción de los clientes externos e internos mediante el desarrollo permanente de la calidad del producto y sus servicios.

Es un concepto que involucra la orientación de la organización a la calidad manifestada en sus productos, servicios, desarrollo de su personal y contribución al bienestar general.

El mejoramiento continuo es una herramienta que en la actualidad es fundamental para todas las empresas porque les permite renovar los procesos administrativos que ellos realizan, lo cual hace que las empresas estén en constante actualización; además, permite que las organizaciones sean más eficientes y competitivas, fortalezas que le ayudarán a permanecer en el mercado.

Para la aplicación del mejoramiento es necesario que en la organización exista una buena comunicación entre todos los órganos que la conforman, y también los empleados deben estar bien compenetrados con la organización, porque ellos pueden ofrecer mucha información valiosa para llevar a cabo de forma óptima el proceso de mejoramiento continuo.

"Un conjunto de atributos del producto software a través de los cuales la calidad es descrita y evaluada".[4]

Las características de calidad del software pueden ser precisadas a través de múltiples niveles de sub-características. Dicha norma define seis características:

Funcionalidad: conjunto de atributos que se refieren a la existencia de un conjunto de funciones y sus propiedades específicas. Las funciones son tales que cumplen unos requerimientos o satisfacen unas necesidades implícitas.

Fiabilidad: conjunto de atributos que se refieren a la capacidad del software de mantener su nivel de rendimiento bajo un las condiciones especificadas durante un periodo definido.

Usabilidad: conjunto de atributos que se refieren al esfuerzo necesario para usarlo, y sobre la valoración individual de tal uso, por un conjunto de usuarios de usuarios definidos o implícitos

Eficiencia: conjunto de atributos que se refieren a las relaciones entre el nivel de rendimiento del *software* y la cantidad de recursos utilizados bajo unas condiciones definidas.

---

[4] Norma ISO 9126

Mantenibilidad: conjunto de atributos que se refieren al esfuerzo necesario para hacer modificaciones específicas.

4.1.2 Objetivos de la auditoría de la calidad

Portabilidad: conjunto de atributos que se refieren a la habilidad del software para ser transferido desde un entorno a otro.

La definición de una estrategia asegura que la organización está haciendo las cosas que debe hacer para lograr sus objetivos. La definición de su sistema determina si está haciendo estas cosas correctamente. La calidad de los procesos se mide por el grado de adecuación de estos a lograr la satisfacción de sus clientes (internos o externos).

Es el proceso de alcanzar los objetivos de calidad durante las operaciones. Para el efecto, se deberán desarrollar los siguientes pasos:

a. Elegir qué controlar
b. Determinar las unidades de medición
c. Establecer el sistema de medición
d. Establecer los estándares de rendimiento
e. Medir el rendimiento actual
f. Interpretar la diferencia entre lo real y el estándar
g. Tomar acción sobre la diferencia

El término calidad se ha convertido en una de las palabras clave de nuestra sociedad, alcanzando tal grado de relevancia que iguala e incluso supera en ocasiones al factor precio, en cuanto a la importancia otorgada por el posible comprador de un producto o servicio. La gestión de la calidad es el conjunto de actividades llevadas a cabo por la empresa para obtener beneficios mediante la utilización de la calidad como herramienta estratégica

Una auditoría de calidad tiene como objetivo el mostrar la situación real para aportar confianza y destacar las áreas que pueden afectar adversamente esa confianza.

- Establecer el estado de un proyecto.
- Verificar la capacidad de realizar o continuar un trabajo específico.
- Verificar qué elementos aplicables del programa o plan de aseguramiento de la calidad han sido desarrollados y documentados.
- Verificar la adherencia de esos elementos con el programa o plan de aseguramiento de la calidad.

El propósito y la actividad de la auditoría es recoger, examinar y analizar la información necesaria para tomar las decisiones de aprobación. La auditoría debe tener capacidad para investigar la pericia técnica, el desarrollo del *software* o la calidad del departamento de desarrollo, el esfuerzo disponible, el soporte del mantenimiento o la efectividad de la gestión. En la auditoría debe acordarse el dirigirse a criterios específicos tales como la realización del código *software*.

Cuando se identifiquen los puntos débiles, los auditores deberán tomar una actitud positiva y utilizar sus conocimientos y experiencias para hacer recomendaciones constructivas. En realidad, una función del auditor es pactar la idoneidad de cualquier acción correctiva propuesta. Este papel, si es usado adecuadamente es uno de los vínculos más valorados entre las partes.

4.2 Auditoría de la seguridad

La existencia de amenazas que afectan la disponibilidad, integridad y confidencialidad de los datos es real. Es crítico para las organizaciones identificar esas amenazas y adoptar recomendaciones que permitan prevenir, detectar y protegerse de ellas. La diversidad y la heterogeneidad de los sistemas de información que requieren las organizaciones actuales, sumado a la globalización a la que se enfrentan al conectar esos sistemas al mundo de Internet, genera un sinfín de incertidumbres en lo referente a la seguridad de la información.

Las soluciones integrales de seguridad que abarcan desde el diagnóstico de la situación actual, hasta la implementación y puesta en marcha de las mismas en todos los niveles de la organización, incluyendo el análisis y la definición de los elementos de seguridad que deben ser implantados a nivel técnico.

El punto de partida para un sistema de seguridad informática es la realización del diagnóstico de la situación actual, para proyectar las soluciones necesarias a cada caso.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes ha las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan ha llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y

debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

4.2.2 El término política de seguridad informática

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, con relación a los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las políticas de seguridad informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro asunto importante es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

4.2.4 Parámetros para establecer políticas de seguridad

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos, bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos de su área.

- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes son los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los gerentes de informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: **"***más dinero para juguetes del Departamento de Sistemas***"**.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes

de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

4.3. Auditoría y control de la seguridad física

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos (*hackers,* virus, ataques de sistema operativo, entre otros); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación.

La seguridad física es una de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad

4.3.1 Las principales amenazas que se prevén en seguridad física

física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de respaldo de la sala de cómputo, que intentar acceder vía lógica a la misma.

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

1. Desastres naturales, incendios accidentales, tormentas e inundaciones
2. Amenazas ocasionadas por el ser humano
3. Disturbios, sabotajes internos y externos deliberados.

Evaluar y controlar permanentemente la seguridad física de las instalaciones de cómputo y del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- Disminuir sinistros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

4.4. Auditoría y control de la seguridad lógica

Después de ver como nuestro sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la seguridad física sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física que la asegure. Estas técnicas las brinda la seguridad lógica.

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la seguridad lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Asegurar que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
5. Asegurar que la información recibida sea la misma que ha sido transmitida.
6. Asegurar que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Asegurar que se disponga de pasos alternativos de emergencia para la transmisión de información.

Es recomendable que este tipo de seguimientos sean realizados a la par con procedimientos de escaneo de vulnerabilidades internas y externas para conocer los puntos débiles de la organización en cuanto a *software* y ofrecer soluciones integradas de seguridad

4.4.1. Controles de acceso

Las nuevas tecnologías de la información han potenciado la comunicación y el acceso a la información. Por ello, la sociedad de la Información, en la que estamos inmersos, debe de garantizar la seguridad de los sistemas.

Los sistemas de información deben estar preparados para prevenir, detectar y reaccionar ante las posibles amenazas.

Se entiende por amenaza a una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo)

Para hacer frente a las amenazas contra la seguridad, se definen una serie de servicios que hacen uso de uno o varios mecanismos de seguridad. Unos de ellos están enfocados a garantizar la inviolabilidad de los datos (confidencialidad, integridad y disponibilidad), mientras que otros se orientan a protegerlos del entorno (autenticación, no repudio y control de acceso).

- **Confidencialidad:** garantiza que la información sea accesible únicamente por las entidades autorizadas, protegiendo la identidad de las partes implicadas. Se utilizan métodos de cifrado.
- **Autenticación**: garantiza la identidad de las partes implicadas en la comunicación. Las tecnologías más aplicadas son "firma digital", biometría, tarjetas de banda magnética, contraseñas, etc.
- **Integridad:** garantiza que la información sólo pueda ser modificada por las entidades autorizadas. Requiere el uso de tecnologías como el *hash criptográfico* con firma digital, y los *time-stamps* (marcas de tiempo).

Entre los principales controles de acceso que se pueden mencionar están:

- **Uso autorizado**

1. Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la empresa y se usarán exclusivamente para actividades relacionadas con la misma.
2. Ninguna cuenta de usuario podrá ser usada para propósitos ilegales, criminales o no éticos.

3. Las cuentas en los sistemas son estrictamente personales e intransferibles.
4. Para reforzar la seguridad de la información de la cuenta, el usuario bajo su criterio deberá hacer respaldos de su información dependiendo de la importancia y frecuencia del cambio de la misma.

- **Tiempo de uso de las cuentas**

1. Se prohíbe dejar sesiones abiertas sin control alguno.
2. Por razones de seguridad todo usuario que salga temporalmente de la institución tiene la obligación de notificar al administrador las máquinas de las cuales se conectará a la red.
3. Cuando el usuario deje de tener alguna relación oficial con la empresa o la cuenta deje de ser utilizada por un tiempo definido por los administradores, esta debe ser removida.
4. Cuando el usuario deje de laborar o de tener una relación con la empresa, este debe notificarlo al administrador de sistemas para proceder y tomar las medidas pertinentes con su información y cuenta de acceso.

- **Gestión de claves**

Contraseñas reutilizadas, sencillas o fácilmente adivinables a nivel de estación de trabajo pueden poner en peligro la seguridad de sus servidores. Cuentas de usuarios o de prueba con excesivos privilegios

Es 4.4.2. Controles sobre el uso de servicios importante para las empresas regular y controlar el uso que sus empleados hacen de Internet y el correo electrónico. Sin embargo, la mayoría carece con políticas escritas sobre los procedimientos de uso y mecanismos de control respecto a estas nuevas tecnologías.

Entre los principales controles de los servicios que deben de tener se pueden mencionar:

1. Control sobre el uso de los servicios de comunicación para que no se utilicen para intimidar, insultar, o molestar a otros.
2. Control sobre la utilización del correo electrónico para que no se utilice para envío masivo, materiales molestos, obscenos, ilegales o innecesarios.
3. Control sobre la utilización de herramientas de hardware o software para realizar monitoreo no autorizado en los medios de comunicación.
4. Control sobre el acceso remoto a computadoras y equipo de red que no se le hayan designado explícitamente.

4.5. Auditoría y control de las redes y comunicaciones

La organización en la parte de las redes de comunicaciones de computadores es un punto de viraje bastante importante; es por ello, que uno de los modelos de red más conocidos es el modelo OSI. a grandes rasgos. El modelo OSI, dado por capas, está dividido en:

Capa física: se encarga de garantizar la integridad de la información transmitida por la red; por ejemplo, si se envía un 0, que llegue un 0.

Capa de enlace: garantiza que la línea o canal de transmisión, esté libre de errores.

Capa de red: determina como se encaminan los paquetes, de la fuente al destino. Igualmente, debe velar por el tráfico de la red, evitando al máximo las congestiones. Para ello, debe llevar un registro contable de los paquetes que transitan.

Capa de transporte: divide los datos en unidades más pequeñas y garantiza que tal información transmitida, llegue correctamente a su destino. De igual forma, crea una conexión de red distinta para cada conexión de transporte requerida, regulando así el flujo de información. Analiza también, el tipo de servicio que proporcionará la capa de sesión y finalmente a los usuarios de red.

Capa de sesión: maneja el sentido de transmisión de los datos y la sincronización de operaciones; es decir, si uno transmite, el otro se prepare

para recibir y viceversa o situaciones *Commit*, donde tras algún problema, se sigue tras ultimo punto de verificación.

Capa de presentación: se encarga de analizar si el mensaje es semántica y sintácticamente correcto.

Capa de aplicación: implementación de protocolos y transferencia de archivos. Lo anterior, nos permite describir tres tipos de fallos en la seguridad de la red:

1. **Alteración de bits**: se corrige por código de redundancia cíclico.
2. **Ausencia de tramas**: las tramas se desaparecen por el ambiente o una sobrecarga del sistema; para ello, se debe tener un número de secuencia de tramas.
3. Alteración de la secuencia en la cual el receptor reconstruye mensaje.

Otro de los tipos de modelos de referencia más conocidos, es el *TCP/IP*, hoy día, con algunas variaciones, como el de encapsular varios protocolos, el *TCP/IP* da replicación de los canales para posibles caídas del sistema. Bajo ésta política, entonces se ha definido como clases de redes:

- *Intranet* = Red interna de la empresa.

- *Extranet* = Red externa pero directamente relacionada a la empresa.
- *Internet* = La red de redes.

El problema de tales implementaciones, es que por los puertos de estandarización pública de *TCP/IP*, se puede entrar cualquier tercero para afectar la red de la compañía o su flujo de información

Tal asunto es recurrente sobretodo en el acceso de la red interna de la compañía a la Internet, para lo cual, y como medida de protección, se usan *Firewall* (cortafuegos) que analizan todo tipo de información que entra por Internet a la compañía, activando una alarma, en caso de haber algún intruso o peligro por esa vía a la red. La compañía puede definir dos tipos extremos de políticas de seguridad:

- **Políticas paranoicas**: toda acción o proceso está prohibido en la red.
- **Políticas promiscuas**: no existe la más mínima protección o control a las acciones de los usuarios en la red.

No importa lo que haga la empresa, siempre va a haber un punto de fallo, para adelantarse a intrusos, entonces se han ideado algunas herramientas para probar la eficacia de las políticas de seguridad en red de la empresa. Estas empiezan probando la fiabilidad de las contraseñas de usuario usando algunas

técnicas de indagación como es el leer el tráfico de la red buscando en tal información sobre nombres de usuarios y contraseñas respectivas, probar la buena fe de los 4.5.1 Vulnerabilidad en redes usuarios mandándoles mensajes de la administración solicitando su contraseña a una especificada por la herramienta o probando contraseñas comunes o por defecto en muchos sistemas.

- **Dispositivos de conectividad**: esto se refiere a utilización de dispositivos de tecnología pasada, de varios años, esto se da cuando no existe una renovación constante, inversión de capital. Hoy día, existe tecnología que otorgan muchos beneficios y esquemas de seguridad a un alto costo.
- **Cableado Estructurado**: el cableado físico no cumple con los estándares. Esto se da muchas veces por reducción de costos en la implementación del cableado.
- **Rendimiento:** la capacidad de rendimiento que la red pueda tener, esta va de la mano por la calidad de dispositivos de conectividad de red que se posea.
- **Mantenimiento Preventivo y correctivo:** muchas veces no se cuenta con un contrato de mantenimiento, tanto preventivo como correctivo. Esta parte puede afectar mucho el tiempo de respuesta ante una falla y conlleva a dar una imagen de debilidad en la red

Controles Inadecuados a *Router, switch hosts*

Un ACL del *router* que se haya configurado erróneamente puede permitir la filtración de información a través de determinados protocolos de transmisión (*ICMP, IP, NetBIOS*) y permitir los accesos no autorizados a determinados servicios en sus servidores de la red interna.

Los cortafuegos o las ACL de *routers* mal configurados pueden permitir el acceso a sistemas internos originando que los servidores quede comprometido.

Los puntos de accesos remotos no seguros y no vigilados es uno de los nodos más sencillos para acceder a su red corporativa, al igual que los *hosts* que ejecutan servicios innecesarios tales como: *sunpc*, FTP, DNS y SMTP dejan caminos abiertos.

Servidores mal configurados de *Internet*, *Scripts* CGI en servidores *web* y *FTP* anónimos

4.5.2. Redes abiertas (TCP/IP)

Una red es una configuración de computadora que intercambia información. Pueden proceder de una variedad de fabricantes y es probable que tenga diferencias tanto en *hardware* como en *software*, para posibilitar la comunicación entre estas es necesario un conjunto de reglas formales para su interacción. A estas reglas se les denominan protocolos. Un protocolo es un

conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos.

4.5.2.1 Definición TCP / IP

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas. El más utilizado es el Internet *Protocol Suite*, comúnmente conocido como *TCP / IP*.

Es un protocolo que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP proviene de dos protocolos importantes de la familia, el *Transmission Control Protocol* (TCP) y el *Internet Protocol* (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, mini computadoras y computadoras centrales sobre redes de área local y área extensa. *TCP / IP* fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el *ARPANE*T una red de área extensa del departamento de defensa.

El modelo de estratificación por capas de *TCP/IP* de *Internet*

El segundo modelo mayor de estratificación por capas no se origina de un comité de estándares, sino que proviene de las investigaciones que se realizan respecto al conjunto de protocolos de TCP/IP. Con un poco de esfuerzo, el modelo OSI puede ampliarse y describir el esquema de estratificación por capas del *TCP/IP*, pero los presupuestos subyacentes son lo suficientemente distintos para distinguirlos como dos diferentes.

En términos generales, el *software TCP/IP* está organizado en cuatro capas conceptuales que se construyen sobre una quinta capa de *hardware*. El siguiente esquema muestra las capas conceptuales así como la forma en como los datos pasan entre ellas.

Tabla III. Capas del Modelo *TCP/IP*

INTERFAZ DE RED **APLICACIÓN**
FÍSICA
TRANSPORTE
INTERNET

Capa de aplicación. Es el nivel mas alto, los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red de redes *TCP/IP*. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continúo de octetos. El programa de aplicación pasa los datos en la forma requerida hacia el nivel de transporte para su entrega.

Capa de transporte. La principal tarea de la capa de transporte es proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte regula el flujo de información. También puede proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el *software* de protocolo de transporte tiene el lado de recepción enviando acuses de recibo de retorno y la parte de envío retransmitiendo los paquetes perdidos.

El *software* de transporte divide el flujo de datos que se está enviando en pequeños fragmentos (por lo general conocidos como paquetes) y pasa cada paquete, con una dirección de destino, hacia la siguiente capa de transmisión. Aun cuando en el esquema anterior se utiliza un solo bloque para representar la

capa de aplicación, una computadora de propósito general puede tener varios programas de aplicación accesando la red de redes al mismo tiempo.

La capa de transporte debe aceptar datos desde varios programas de usuario y enviarlos a la capa del siguiente nivel. Para hacer esto, se añade información adicional a cada paquete, incluyendo códigos que identifican qué programa de aplicación envía y qué programa debe recibir, así como una suma de verificación para comprobar que el paquete ha llegado intacto y utiliza el código de destino para identificar el programa de aplicación en el que se debe entregar.

Capa Internet. La capa Internet maneja la comunicación de una máquina a otra. Ésta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. La capa Internet también maneja la entrada de *datagramas*, verifica su validez y utiliza un algoritmo de ruteo para decidir si el *datagrama* debe procesarse de manera local o debe ser transmitido. Para el caso de los *datagramas* direccionados hacia la máquina local, el software de la capa de red de redes borra el encabezado del *datagrama* y selecciona, de entre varios protocolos de transporte, un protocolo con el que manejará el paquete. Por último, la capa Internet envía los mensajes *ICMP* de error y control necesarios y maneja todos los mensajes *ICMP* entrantes.

Capa de interfaz de red. El *software TCP/IP* de nivel inferior consta de una capa de interfaz de red responsable de aceptar los *datagramas IP* y transmitirlos hacia una red específica. Una interfaz de red puede consistir en un

dispositivo controlador (por ejemplo, cuando la red es una red de área local a la que las máquinas están conectadas directamente) o un complejo subsistema que utiliza un protocolo de enlace de datos propios.

4.6. Auditoría de la continuidad de operaciones

Es uno de los puntos que nunca se deberían pasar por alto en una auditoria de seguridad, por las consecuencias que puede tener el no haberlo revisado o haberlo hecho sin la suficiente profundidad; no basta con ver un manual cuyo título sea Plan de Contingencias o denominación similar, sino que es imprescindible conocer si funcionaría con la garantías necesarias y cubriría los requerimientos en un tiempo inferior al fijado y con una duración suficiente.

En un plan de contingencia se presume que hay un lapso de tiempo, tiempo sobre el cual se declara la emergencia, y entran a operar una serie de procedimientos que permiten que el servicio se restablezca en el menor tiempo posible. Una vez resuelta la emergencia, se disparan otra serie de procedimientos que vuelven la operación a su normalidad, procesos que pueden ser bastante engorrosos de ejecutar, en especial cuando de sincronizar la información se trata.

El enfoque del plan de contingencia se basa en la minimización del impacto financiero que pueda tener un desastre en la compañía, mientras que el plan de continuidad está orientado a asegurar la continuidad financiera,

satisfacción del cliente y productividad a pesar de una catástrofe. Mientras que el plan de contingencia se concentra en la recuperación de eventos únicos que producen una interrupción prolongada del servicio, el plan de continuidad se ejecuta permanentemente a través de la administración de riesgos tanto en la información como en la operación. Los riesgos que se enfrentaban en la planeación anterior eran desastres con baja frecuencia pero muy alto impacto.

Hoy los riesgos son casi todos de muy alto impacto por las implicaciones que tienen en la empresa ampliada (socios de negocios) y de muy alta ocurrencia. Ya todas las empresas están expuestas a ataques con virus, problemas de seguridad en la información, calidad del *software*, almacenamiento de datos inapropiado, arquitecturas tecnológicas complejas y hasta políticas poco efectivas de administración de recursos que pueden abrirle las puertas a una catástrofe con el mismo impacto en el negocio (y hasta mayor) que el impacto causado por una amenaza física como un incendio o un terremoto.

Un plan de continuidad tiene como objetivo tratar de alcanzar una disponibilidad de cinco nueves (99.999%) para la infraestructura crítica, lo que implica que el sistema siempre estará disponible. Hoy existe la tecnología para poder obtener estos resultados; sin embargo, el costo de esta tecnología todavía no está al alcance de todas las empresas. El plan de contingencia tiene como beneficio para la empresa garantizar la recuperación de servicios que están desmejorados por la falla, en un período de entre 12 y 72 horas.

Un plan de contingencia se refleja en un documento que especifican las tareas que hay que hacer antes, durante y después de la contingencia, además de los responsables de cada acción. Un plan de continuidad se basa en las tecnologías emergentes (como unidades de discos para redes, SAN, y cintas para copias de respaldo de altísima velocidad), y la excelencia operativa del centro de cómputo.

Un plan de continuidad no es excluyente de un plan de contingencia, sino más bien que el segundo está dentro del primero. Un plan de continuidad para el negocio debe incluir: un plan de recuperación de desastres, el cual especifica la estrategia de un negocio para implementar procedimientos después de una falla; un plan de reanudación que especifica los medios para mantener los servicios críticos en la ubicación de la crisis; un plan de recuperación que especifica los medios para recuperar las funciones del negocio en una ubicación alterna; y un plan de contingencia que especifica los medios para manejar eventos externos que puedan tener serio impacto en la organización.

En la auditoría es necesario revisar si existe tal plan; si es completo y actualizado; si cubre los diferentes procesos, áreas y plataformas, o bien si existen planes diferentes según entorno, evaluar en todo caso su idoneidad, así como los resultados de las pruebas que se hayan realizado.

Si las revisiones no nos aportan garantías suficientes debemos sugerir pruebas complementarias o hacerlo constar en el informe, incluso indicarlo en el apartado de limitaciones

CONCLUSIONES

1. Dependiendo de cómo la tecnología de la información es aplicada en la organización, esta podrá tener un alto impacto en el logro de su visión, misión u objetivos estratégicos.

2. La seguridad en las redes es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio inseguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad

3. Las empresas o instituciones deberán de contar con un adecuado control interno sobre todas sus áreas y en especial sobre el área de telecomunicaciones para garantizar una mejor utilización de sus recursos.

4. A través de la auditoría de telecomunicaciones se lleva a cabo un exhaustivo análisis del estado de seguridad de telecomunicaciones y de sus sistemas frente a usuarios de Internet y usuarios de su propia organización.

RECOMENDACIONES

1. Deben realizarse evaluaciones periódicas sobre el nivel de cumplimiento de los procesos relacionados con la administración de sistemas y debe de evaluarse si estos cubren las necesidades de la empresa de manera adecuada y dentro de los períodos preestablecidos.

2. Al momento de tener el informe de la auditoría de telecomunicaciones se deberá de implementar las recomendaciones planteadas para subsanar las debilidades de control interno encontradas, por el auditor, y el área de informática deberá preocuparse en el futuro en detectar e incorporar las nuevas soluciones que vayan apareciendo respecto a vulnerabilidades correspondientes al área de telecomunicaciones.

3. Las políticas y normas de seguridad de telecomunicaciones deben estar formalmente definidas, documentadas y aprobadas. Adicionalmente, deberán contener objetivos de control de alto nivel que definan los requerimientos de administración de seguridad en redes.

REFERENCIAS

Traducción realizada por el Instituto Mexicano de Auditores Internos autorizada su reproducción por el IIA con sede en Florida EEUU

[2] *Information Systems Audit & Control Association (ISACA*)

[3] ISACAF-EXS, 2000.

BIBLIOGRAFÍA

1. Acha Iturmendi, J. José. **Auditoría Informática en la empresa** 1994

2. ISACF. **Objetivos de Control para la Información y Tecnología Relacionada**. COBIT-ISACF, 1998

3. ISACA. **Normas Generales del Estándar de la ISACA**. ISACA, 2002.

4. Ministerio de Administraciones Públicas. **MAGERIT*:* guía de procedimientos**. MAP y BOE, 2001.

5. **Monografías**.http://www.monografias.com/trabajos/maudisist/maudisist.shtml, Junio 2004.

6. **Monografías**. http://www.monografias.com/trabajos7/inaud/inaud.shtml, Mayo 2004

7. Pattini M. y Navarro E. del Peso. **Auditoría informática**. **Un enfoque práctico** *(2ª Edición)*. RA-MA, 2001.

8. **Rincondelvago**. http://html.rincondelvago.com/auditoría-de-los-sistemas-de-informacion.html, Abril 2004.

9. **scorpionsistemas**. http://www.scorpionsistemas.com/htm/Networking/inicio/networking_1.htm, Mayo 2004.

10. Weber R. **Information systems control and audit**. New Jersey: Prentice Hall, 1999.