37
ZEJ

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

METODOLOGIA PARA LLEVAR A CABO UNA AUDITORIA EN INFORMATICA CON HERRAMIENTAS PARA UNA APLICACION EN REDES

SEMINARIO DE INVESTIGACION INFORMATICA

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

PRESENTAN:

NORMA ANGELICA URDAPILLETA HERRERA

CARMEN ELVIRA DE LA VEGA SEGURA

ASESOR DEL SEMINARIO:

C.P. Y M.B.A JOSE ANTONIO ECHENIQUE GARCIA

MEXICO, D.F. 1995

FALLA DE ORIGEN

Este trabajo lo dedico

A mis papás por haberme mostrado el camino al estudio y a la superación, por apoyarme y ayudarme en los momentos más difíciles, por brindarme su amor y por confiar y creer en mi. A ellos debo lo que soy y por esto gracias.

A mis hermanos Enrique, Jorge y Eryka por tenerme paciencia, apoyarme y quererme.

A todos mis tíos y primos por su cariño y por preocuparse y confiar en mí.

A la familia Castillo por apoyarme en mi desarrollo profesional, por brindarme su amistad y por creer en mí.

A mis amigos por creer en mi, transmitirme el entusiasmo por vivir y seguir adelante.

Agradezco al Ser más importante en mi vida que siempre ha estado conmigo y que ha hecho que exista y me haga presente de esta forma, a Dios.

Norma

Este trabajo se lo dedico

A Dios, quien siempre ha iluminado mi vida con su inmenso amor.

A mis padres, quienes siempre me han encaminado con su amor y confianza, hacia el logro de mis metas.

A mis hermanos, Ale, Edy e Isaac, quienes me han brindado su cariño y comprensión.

A mi hermana Lily, quien siempre me ha proporcionado valiosos consejos y en todo momento estuvo alentándome para elaborar este trabajo.

A mis familiares, quienes han confiado en mí.

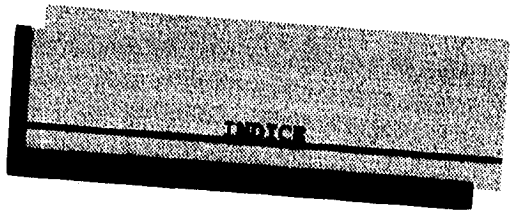
A mis amigos, quienes me han brindado su amistad y apoyo.

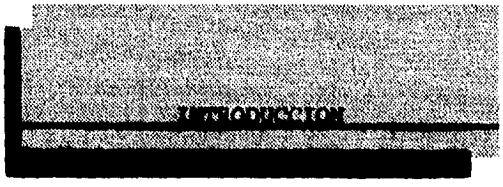
Carmen

Nuestro agradecimiento al M.B.A. José Antonio Echenique G. por el tiempo y dedicación que nos brindó para la realización de este trabajo con su participación como asesor responsable.

Agradecemos también al L.A.E. Mario Novoa y a la Lic. Ma. Teresa Pérez M. que con sus consejos y sugerencias contribuyeron al desarrollo de este trabajo.

Agradecemos a la Universidad por la oportunidad que nos brindó y por que nos hizo ser universitarias y sentir el orgullo que esto representa.





A través de la historia el hombre ha requerido de información para subsistir considerándola como un vínculo entre los individuos de una sociedad.

La información resulta un factor muy importante en todo el mundo en los ámbitos político, económico, social y cultural por su valor en los procesos de organización, coordinación y transmisión de conocimientos.

Hoy en día, la cantidad de información que maneja una organización crece a un ritmo considerable, por lo que para su manejo, se ha desarrollado la Informática. Esta área es fundamental dentro de una organización para procesar y obtener la información de manera oportuna y confiable, contribuyendo a una buena toma de decisiones para alcanzar un nivel de desarrollo, productividad y competitividad entre empresas y las propias naciones. Por este motivo, es considerada no sólo como una ciencia del tratamiento automático sino también racional de la información.

El auge tecnológico en esta área ha abierto nuevos caminos para su desarrollo en la industria, la medicina, la milicia, las comunicaciones, por mencionar algunas.

La sociedad orientada a la informática para obtener un mejor seguimiento en las operaciones de una organización, ha creado el área de auditoría para detectar posibles riesgos y tratar de reducirlos valiéndose de la automatización para minimizar el tiempo requerido para su realización.

A nivel empresarial se requiere eficiencia adecuadamente distribuida, es decir, se requiere de conectividad lo cual se logra precisamente a través de una red que proporcione integración de recursos informáticos y humanos, con el fin de interactuar entre sí compartiendo información y equipos para incrementar la eficiencia de toda la organización.

Las computadoras gracias al avance tecnológico pueden conectarse desde hace más de una década a las redes de comunicaciones para enviar y recibir volúmenes de información a distancia. Las ventajas que estas redes proporcionan a los usuarios han generalizado su uso y, al mismo tiempo, han provocado una revolución en la industria mundial de la informática.

Una auditoría en redes ayuda a determinar si el Departamento de Informática ha establecido políticas y procedimientos claramente definidos en todas las áreas de comunicaciones para el control de selección, adquisición, administración y monitoreo de hardware y software, distribución del contenido de las bases de datos entre los departamentos que usen la red, documentación y capacitación al personal, provisiones de respaldo, revisiones de estructura y actuación, facilidades de seguridad, planes de contingencia, metas, costos y beneficios por el uso del Intercambio Electrónico de Datos, Red Digital de Servicios Integrados y correo electrónico.

Este seminario de investigación tiene como objetivo mostrar una metodología para llevar a cabo una auditoría en Informática con herramientas para una aplicación en redes que proporcione confidencialidad, seguridad, integridad y coherencia de la información para la reducción de riesgos a través de la implantación de controles y asegurar la continuidad en el servicio.

Se abarcan dos capítulos principales y cada uno consta de temas afines.

En cada uno de los capítulos se introduce al lector mediante consideraciones preliminares del contenido e importancia en el tema a tratar y se muestran las citas textuales que le sirven

de sustento y referencia para profundizar y obtener mayor información sobre el mismo.

El primer capítulo trata los **conceptos básicos** que ayudan a la comprensión de los capítulos posteriores. Se definen y explican algunos conceptos relacionados con auditoría en informática, comunicaciones y redes.

En el segundo capítulo, **Metodología para llevar a cabo una auditoría en Informática**, se propone una metodología que sirva como guía para auditar el área de Informática, pudiendo adecuarse a cualquier departamento y dependiendo del tamaño, contexto y complejidad de la organización.

Al finalizar, se presentan las herramientas que desarrollamos para poder ser aplicadas a redes de comunicaciones a fin de probar la metodología propuesta en investigaciones posteriores. Dentro de estas herramientas se contempla una guía para la planeación estratégica basada en la técnica del cuestionario que incluye una tabla de tipo de riesgos detectados, una tabla de controles generales y una tabla de decisión de aplicación de pruebas; una prueba de procedimientos para redes de comunicaciones y una tabla que muestra sus controles específicos.

CAPITULO 1

CONCEPTOS BÁSICOS

Los grandes avances en el desarrollo de la tecnología se han dado a través de los años, han permitido que se pueda transmitir información a grandes distancias por medio del uso de dispositivos y que la gente y las máquinas puedan comunicarse mutuamente.

Las telecomunicaciones son consideradas dentro de la tecnología como un término que soporta comunicaciones. Sin embargo, el sistema total es más que sólo la interconexión de sus componentes. Para lograr una composición de un sistema efectivo de comunicaciones se requiere considerar a la gente, las políticas, los procedimientos, las prioridades, así como la tecnología.

"En el pasado las telecomunicaciones se limitaban a la interconexión de dos sistemas. Con el avance de sistemas de proceso en línea, distribuido y cooperativo, las telecomunicaciones se han convertido en una parte integral de

la aplicación."[1]

Hoy en día, las organizaciones buscan ofrecer un servicio con una alta calidad a sus clientes y ocupar un lugar importante en el mercado. Por ello, se auxilian de áreas como la informática para obtener información oportuna, confiable y veraz que sirva de base para una buena toma de decisiones.

Por lo anterior, resulta de suma importancia para éstas considerar la auditoría en informática como una área para detectar posibles riesgos y establecer controles contribuyendo a su eficiencia y eficacia.

El propósito de este capítulo es mostrar los conceptos básicos sobre auditoría en informática, comunicaciones y redes que permitan la comprensión de los capítulos posteriores.

1.1 Auditoría en Informática.

1.1.1. Concepto de Informática.

INFORMATICA: "Es una palabra de origen francés formada por los vocablos información y automática. La Real Academia Española de la Lengua la define como "el **conjunto de conocimientos**

[1] SYSTEMS AUDITABILITY AND CONTROL, U.S.A., The Institute of Internal Auditors Research Foundation, Telecommunications, abril 1991, Module 8, p. 1.

la aplicación."[1]

Hoy en día, las organizaciones buscan ofrecer un servicio con una alta calidad a sus clientes y ocupar un lugar importante en el mercado. Por ello, se auxilian de áreas como la informática para obtener información oportuna, confiable y veraz que sirva de base para una buena toma de decisiones.

Por lo anterior, resulta de suma importancia para éstas considerar la auditoría en informática como una área para detectar posibles riesgos y establecer controles contribuyendo a su eficiencia y eficacia.

El propósito de este capítulo es mostrar los conceptos básicos sobre auditoría en informática, comunicaciones y redes que permitan la comprensión de los capítulos posteriores.

1.1 Auditoría en Informática.

1.1.1. Concepto de Informática.

INFORMATICA: "Es una palabra de origen francés formada por los vocablos información y automática. La Real Academia Española de la Lengua la define como "el **conjunto de conocimientos**

[1] SYSTEMS AUDITABILITY AND CONTROL, U.S.A., The Institute of Internal Auditors Research Foundation, Telecommunications, abril 1991, Module 6, p. 1.

científicos y técnicos que hacen posible el tratamiento automático de la información por medio de computadoras electrónicas". El término información hace referencia a la yuxtaposición de símbolos con los que se representan convencionalmente hechos, objetos o ideas. La palabra informática suele utilizarse como sinónimo de ciencia e ingeniería de las computadoras."[2]

1.1.2 Concepto y tipos de Auditoría.

AUDITORIA: La auditoría es una disciplina intelectual basada en la lógica, ya que ésta está dedicada al establecimiento de hechos, siendo las conclusiones resultantes falsas o verdaderas.

La auditoría es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados. El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso.

---

[2] PRIETO, Alberto, LLORIS, Antonio y TORRES, Juan Carlos: Introducción a la Informática, 1ª ed., Madrid, McGraw-Hill/Interamericana de España, S.A., 1989, pp. 1 y 2.

Una auditoría debe considerarse como base para futura guía para la administración en la conducción de una empresa y no sólo como un resumen histórico.

Tipos de auditoría.

Dentro de la auditoría tenemos la **auditoría interna** y la **auditoría externa**. Ambas deben coordinar sus esfuerzos para lograr un adecuado manejo de los recursos de una organización, asegurar la adecuada cobertura y minimizar duplicidad de esfuerzos.

AUDITORIA INTERNA: Es una función independiente establecida dentro de una organización para examinar y evaluar sus actividades. 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.

Apoyan y proporcionan información acerca de la adecuada y efectiva funcionalidad del sistema de control interno de la organización y la calidad de la gestión a la Gerencia y al Consejo de Administración quienes son los encargados de aprobar su propósito y establecer sus políticas.

AUDITORIA EXTERNA: Es la llevada a cabo por una persona o firma independiente, de capacidad profesional. El auditor independiente, no es un empleado del cliente. No tiene otra relación con la administración que la de una persona profesional.

La auditoría externa debe juzgar lo presentado por la administración e informar independientemente sobre la situación de la organización así como los resultados de las operaciones. Como uno de los resultados del trabajo de auditoría ejecutado para lograr estos objetivos, se origina la corrección de errores.

1.1.3 Concepto de Auditoría en Informática.

AUDITORIA EN INFORMATICA: "La auditoría en Informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones."[3]

---

[3] ECHENIQUE GARCIA, José Antonio: Auditoría en Informática, 1ª ed., México. D.F., McGraw-Hill, 1991, p. 16.

En esta definición se puede observar claramente la importancia que debe darse a la seguridad e integridad de la información manejada en una organización ya que de ella depende una buena toma de decisiones.

Weber la define de la siguiente manera:

AUDITORIA EN INFORMATICA: "Es el proceso de recolectar y evaluar evidencia para determinar si un sistema de cómputo salvaguarda bienes, mantiene la integridad de los datos, realiza de manera efectiva los objetivos organizacionales y consume eficientemente recursos. Ayuda a la obtención de los objetivos tradicionales de auditoría: objetivos de testimonio (los del auditor externo) que salvaguardan bienes y ven la integridad de los datos, y objetivos de administración (los del auditor interno) que contemplan no solo los objetivos de testimonio sino también los objetivos de efectividad y eficiencia. El proceso de auditoría puede concebirse como una fuerza que ayuda a las organizaciones a conseguir mejor estos objetivos."[4]

En la definición anterior resulta muy importante el **objetivo para salvaguardar bienes** ya que en una organización es trascendental contar con controles internos para proteger la

[4] WEBER, Ron: EDP Auditing: Conceptual Foundations and Practice, 2ª ed., U.S.A., McGraw-Hill, 1988, pp. 8 y 9.

información, el hardware, software y la documentación de los sistemas en el Departamento de Sistemas de Información de algunos daños o de usos no autorizados.

Dentro de una organización resulta de vital importancia contar con datos oportunos y veraces para una buena toma de decisiones tratando de evitar dentro de lo posible la incertidumbre por lo que se requiere contar con un **objetivo para la integridad de los datos**.

Se debe entender que un sistema de procesamiento de datos contempla el **objetivo de efectividad** cuando ha alcanzado sus objetivos. La evaluación de la efectividad implica el conocimiento de las necesidades de los usuarios y qué tanto les facilita la toma de decisiones. La efectividad de un sistema se puede medir después de que se haya usado por un tiempo.

A menudo resulta difícil determinar si un sistema de procesamiento de datos está cumpliendo con el **objetivo de eficiencia**. Un sistema se considera eficiente cuando es efectivo y utiliza la menor cantidad de recursos.

Para el logro de los objetivos mencionados anteriormente se requiere la asesoría y evaluación de los auditores, así como el establecimiento de un sistema de control interno por parte de la Administración de la organización.

Nosotros definimos a la Auditoría en Informática como un examen y validación para ver la continuidad del servicio, confidencialidad, seguridad, integridad y coherencia de la información.

1.2 Comunicaciones.

1.2.1. Concepto de Comunicación y sus componentes.

COMUNICACION DE DATOS: "Es la transferencia de datos de una localidad u operación a otra, para utilizarlos o para seguirlos procesando y este proceso continúa hasta que la información en forma útil llega hasta el usuario final".[5]

Componentes de un sistema de comunicaciones de datos.

Un sistema de comunicaciones de datos generalmente consta de tres componentes básicos que son el **emisor**, el **medio** y el **receptor**. El emisor origina la información; el medio es el camino sobre el cual fluye la información y el receptor es el mecanismo que acepta la información. Una terminal opera tanto como emisor como receptor. El medio sólo son las líneas de comunicación por las que viaja la información.

---

[5] SANDERS, Donald H.: Informática presente y futura, 2ª ed., México, D.F., McGraw-Hill/Interamericana de México, S.A. de C.V., 1990, p. 17.

Cabe mencionar que la capacidad de un canal de comunicación de tecnología digital se determina por el número de bits por segundo que puede transmitir (Bits/s o bps) y tiene una capacidad limitada de transmisión de datos. Una de las limitaciones es el ruido que es un problema inherente a la línea.

1.2.2 Concepto de Telecomunicación y sus componentes.

TELECOMUNICACION: Viene del griego y significa comunicación a distancia. "Se define como dispositivos y procedimientos para comunicar señales. Las telecomunicaciones facilitan que un sistema operativo se comunique con los usuarios remotamente a través de las redes de comunicaciones. Incluye comunicación de datos entre terminales y computadoras, y comunicación de voz usando los teléfonos."[6]

Hoy en día, se utiliza también la comunicación de imagen y video.

Componentes generales de una red de comunicaciones.

- Terminal.

[6] The EDP Auditors Foundation, Inc.: EDPAA CISA Review Manual, U.S.A., The Information Systems Control Association, 1995, p. VI-35.

- Procesador Central (Host).
- Procesador de comunicaciones (Front-End).
- Centrales Privadas de Comunicación (PBX).
- Controladora (Cluster).
- Líneas de comunicación.
- Modem.
- Multiplexor.
- Tarjetas de redes: Arcnet, Ethernet y Token-Ring.
- Puentes (Bridges).
- Ruteadores.
- Concentrador (Hub).
- Transmisor-receptor (Transceiver).
- Ensamblador y desensamblador de paquetes (PAD).
- Convertidor de protocolos.
- Servidores.
- Unidad de servicio de canal (CSU).
- Unidad de servicio de datos (DSU).
- Dispositivo para encriptar.

1.2.3 Medios, técnicas, modos y tipos de transmisión.

Las características físicas de una red se refieren a las condiciones de transmisión de bits a través de un medio físico. Estas características se pueden dividir en dos categorías principales: el **medio físico** usado para las transmisión y la

técnica de transmisión usada para transmitir datos sobre el medio físico.

Dentro de los **medios físicos** usados para la mayoría de las construcciones de redes se tienen los siguientes: cables de par trenzado, cable de cobre, cable coaxial, fibra óptica, microondas, radios digitales y satélite. Cada uno tiene diferentes características de transmisión y diferentes costos.

La **técnica de transmisión** determina cómo es usado el medio físico para las comunicaciones. Existen dos tipos: **banda base** y **banda portadora**. La primera utiliza señales digitales retransmitidas a su forma y fuerza original a través de **repetidores** y la segunda señales analógicas retransmitidas a su fuerza original a través de **amplificadores y moduladores**.

Modos de Transmisión.

Los sistemas que transmiten datos deben tener métodos consistentes de transmisión por los canales de comunicación. En esencia, los datos binarios pueden transmitirse por las líneas de comunicación en modo en **serie** o en **paralelo**. La transferencia interna de los datos dentro de las computadoras modernas se realiza en modo paralelo, es decir todos los bits de un caracter se envían simultáneamente por líneas separadas o en diferentes frecuencias sobre la misma línea. En la

transmisión en serie el dispositivo transmisor envía un bit seguido de un intervalo, luego un segundo bit y así sucesivamente hasta transmitir todo.

La mayoría de las comunicaciones de datos se realizan por la transmisión en serie. Se usan comúnmente dos modos de transmisión: asíncrona y síncrona.

Tipos de transmisión.

Los métodos disponibles de transmisión son **simplex**, **semi-dúplex** (Half Duplex, HDX) y **dúplex completo** (Full Duplex-FDX). En la Fig. 1 se muestran estos métodos.

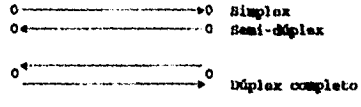


Figura 1 Métodos de transmisión.

1.2.4 Concepto de Encriptamiento de Datos.

ENCRIPTAMIENTO: Es el proceso de transformar un mensaje de su forma comprensible a un mensaje equivalente que no se pueda comprender de inmediato. El proceso inverso se conoce como **desencriptamiento**.

El algoritmo usa una llave de 64 bits de los cuales 8 bits son de paridad y convierte el bloque en código numérico a través de 16 redondeos.

Los criptosistemas más comunes son los siguientes:

- **Criptosistema de llave privada o criptosistema convencional**. Usa llaves secretas comunes para encriptar o desencriptar. Resultan difíciles los controles sobre la distribución de la llave.

- **Criptosistema de llave pública**. Usa diferentes llaves para encriptar o desencriptar un mensaje. La mayoría de las veces es usado para encriptar datos aunque el tiempo para el proceso requerido es relativamente lento en comparación a los criptosistemas de llave privada.

1.2.5 Concepto de La Red Digital de Servicios Integrados (RDSI).

Con la Red Digital de Servicios Integrados (RDSI), se da el primer paso en la evolución del sistema telefónico, al proporcionar un elevado nivel de calidad con los sistemas más adelantados de conmutación y transmisión.

La RDSI suministra un medio de transporte de señales digitales conmutadas y de punto a punto, con todas las modalidades de transmisión de información como voz, datos, textos e imágenes en un solo sistema para construir redes corporativas e institucionales a niveles local y de larga distancia nacional e internacional de la más alta calidad.

Asimismo, incorpora una red multiusuario de satélite para la interconexión de localidades remotas o aisladas que requieren ser integradas a los servicios de la red digital terrestre, así como, una red para transmisión de datos en paquetes para bajos volúmenes de información en tiempos cortos.

Dentro de las características de la red se pueden mencionar las siguientes:

DISPONIBILIDAD

* Infraestructura existente para su contratación inmediata.
* Respaldo de la instalación y supervisión por compañías de prestigio mundial.
* Tiempos mínimos de respuesta en el servicio.

CONFIABILIDAD

* Medio de transmisión de alta calidad inmune al ruido e

interferencias a través de fibra óptica.

* Precisión para completar llamadas con el uso de centrales de conmutación digital.
* Respaldo asegurado mediante la instalación de radios digitales y fibras ópticas de soporte.

CALIDAD

* Alta calidad en la conversación.
* Mínimo promedio de errores en el envío y recepción de datos.
* Absolutamente libre de ruidos e interferencias.

Los principales servicios que ofrece son:

* Acceso digital a un conmutador electrónico o digital.
* Marcación directa entrante.
* Centrex básico.
* Centrex avanzado.
* Videoconferencia.
* Enlace digital de alta velocidad.
* Red privada metropolitana.
* Cruce fronterizo.
* Red global.
* Telefonía de alta calidad.
* Red privada de voz y datos.

* Red de paquetes de datos.
* Red satelital.
* Enlaces virtuales.

Esta red digital, conformada por la red terrestre, la satelital y la de paquetes actualmente brinda sus servicios en Estados Unidos, Japón y Europa donde se está probando para poder así establecer estándares. Hoy en día, Teléfonos de México (TELMEX) ofrece a través de su Red Digital Integrada (RDI) sólo los servicios de enlace digital y cruce fronterizo y tiene en proceso la implantación de los demás servicios para mantenerse a la vanguardia de la tecnología de telecomunicaciones que marca la tendencia a nivel mundial en los 90's.

Es importante mencionar que hasta ahora TELMEX ha sido la única compañía que ha proporcionado servicios de comunicaciones en la ciudad de México. A partir de 1996, compañías asociadas como BANAMEX y MCI (AVANTEL), US SPRINT y BANCOMER, por mencionar algunas, también podrán brindarlos.

1.2.6 Concepto del Correo Electrónico.

CORREO ELECTRONICO: Es un servicio que puede ser público o privado y se utiliza bastante dentro de las comunicaciones de datos combinando software y hardware para enviar textos, datos,

imágenes o mensajes de voz a través de terminales. Un usuario escribe un mensaje desde su terminal y lo envía al archivo de correo para que el destinatario lo reciba. El mensaje se puede recibir a través de la pantalla o enviarlo directamente a la impresora. Posteriormente, se puede contestar y devolver al remitente o redirigir a otros destinatarios.

Esta tecnología proporciona una mayor velocidad de reparto y es más efectivo en costo que el servicio de mensajería convencional.

1.2.7. Concepto del Intercambio Electrónico de Datos (EDI).

EDI es un medio electrónico para transmitir transacciones de negocios entre organizaciones. Las transacciones se transmiten usando formatos altamente estandarizados que permiten a las computadoras procesar los datos sin intervención humana. Se ha usado por 20 años pero hasta hace 5 se le ha dado mayor importancia, ya que las organizaciones buscan diferentes maneras para reducir costos y ser más productivas.

Es una técnica de negocios usada para permitir que las organizaciones operen más eficientemente y como medios técnicos de comunicación de datos de un negocio. El proceso para EDI es una combinación de un software y un sistema de aplicación. El

software provee servicios de utilería que son usados por los sistemas de aplicación. Estos servicios incluyen transmisión, traducción y almacenamiento de transacciones que se originaron o salieron con destino al proceso de aplicación. Como sistema de aplicación, las funciones que lleva a cabo se basan en las necesidades de los negocios y sus actividades.

"Dentro de los beneficios derivados de su uso se incluyen los siguientes:

* Calidad mejorada y disponibilidad de información comercial.
* Aumento en la ventaja estratégica y competitiva.
* Habilidad para conducir negocios con organizaciones que obligan al uso de EDI.
* Aumento de la productividad y calidad.
* Reducción en el costo (entrada de datos redundantes).

Los mecanismos de transporte electrónico disponibles por EDI incluyen lo siguiente:

* Medios de intercambio físico (cintas magnéticas o discos)
* Transmisión punto a punto sobre facilidades de comunicación entre los socios del negocio.
* Servicios de terceras partes como correo de vendedores,

servicios EDI o redes de valor agregado.

Los servicios de terceras partes incluyen lo siguiente:

* Ruteo de datos.
* Uso de la red física.
* Almacenamiento de datos.
* Verificación de datos y formateo.
* Identificación y autorización de usuarios.
* Implementación y consultoría del EDI.
* Conversión de los datos propietarios a estándares de formatos de mensaje EDI."[7]

1.3 Redes.

Diariamente, las redes de comunicaciones ayudan a cubrir las necesidades privadas o comerciales de infinidad de usuarios que las ocupan para operaciones bancarias, gestionan las reservaciones de hoteles y muchas otras operaciones económicas multiplicando de este modo su productividad y eficiencia en el trabajo. Esto se ha acentuado a medida que éstos descubren su potencialidad.

---

[7] SYSTEMS AUDITABILITY AND CONTROL, Module 6, Telecommunications, Price Water House, U.S.A., The Institute of Internal Auditors Research Foundation, abril 1991, pp. 6-69 - 6-91

Las redes de microcomputadoras son consideradas como la primera generación de conectividad, ya que dio paso a una segunda generación en la que este concepto se amplió a todo tipo de sistemas de cómputo, ya fueran micro o macrocomputadoras y redes de características similares o distintas. Esto facilitó la comunicación tanto vertical como horizontal, además de compartir recursos, archivos de datos y herramientas de programación contribuyendo a la eficiencia de la organización.

Las necesidades de comunicación entre organizaciones han dado origen al desarrollo de herramientas entre sistemas de diferente naturaleza, logrando con esto una alta especialización. Aunque, cabe mencionar que uno de los problemas con los que se enfrenta la estandarización es la gran diversificación de productos que no ha permitido que se puedan proporcionar los elementos para la solución integral a los requerimientos de cómputo de una entidad determinada, tornándose esto más difícil si tomamos en cuenta que el parámetro fundamental para la decisión del cliente es la relación de costo-beneficio.

Por lo anterior, se puede apreciar que las redes de comunicaciones son un arreglo complejo de hardware y software que requieren de controles lógicos y físicos para asegurar su confiabilidad e integridad. Por lo tanto, la habilidad para auditar de manera efectiva este ambiente requiere un

entendimiento básico de la terminología así como de la tecnología.

1.3.1. Concepto de red. Ventajas y desventajas.

RED: Es un sistema que provee rutas para la transmisión de información a través de un medio de comunicación que permite que varias terminales puedan accesarse entre sí.

Una red tiene como finalidad transferir e intercambiar datos a distancia entre computadoras y terminales de manera rápida y precisa, así como la operación de aplicaciones desde varias estaciones de trabajo simultáneamente.

Ventajas.

1. Intercambio de datos e información entre usuarios en distintas localidades geográficas.

2. Distintos usuarios de la red pueden compartir los mismos recursos obteniendo así un mejor aprovechamiento de los mismos.

3. Flexibilidad para accesar la red desde localidades distintas a la organización.

4. Monitoreo de las operaciones y actuación de la red, así como de las funciones de los usuarios.

5. Menor tiempo de respuesta y considerable velocidad en los procesos.

6. Favorece la descentralización de operaciones. Los usuarios finales disponen de una gran cantidad de herramientas informáticas que les permiten desarrollar sus propias aplicaciones, apegados a sus necesidades, haciendo su trabajo más productivo.

7. Estandarización de los programas, ya que se utiliza un solo paquete de cada tipo y por lo tanto, el intercambio de datos es completamente natural.

Desventajas.

1. Se requiere de personal especializado para el diseño, estructura, instalación, administración y mantenimiento de la red.

2. Alto costo en el mantenimiento de la red y capacitación a los usuarios para el manejo de la misma.

3. Múltiples configuraciones de redes.

4. Existen aplicaciones en las que, por su magnitud y demanda de recursos no tienen todavía un desempeño adecuado.

5. Posible falta de compatibilidad que puede existir entre productos de distinto fabricante no obteniendo el rendimiento esperado y perdiendo las ventajas que este tipo de esquemas ofrece. Existen características en cada producto, fuera de los estándares, que son definidos por cada fabricante y que pueden afectar la operación de la red o de una aplicación en particular.

1.3.2 Estándares en redes y protocolos.

Una arquitectura de red define protocolos, formatos de mensajes y estándares en los que se deben basar los productos para conectarse con la red. Dentro de las principales organizaciones generadoras de estándares se pueden mencionar a la Organización Internacional de Estándares (ISO) con su **Modelo OSI** el cual certifica la calidad a nivel mundial y se considera como conceptual, IBM con su **Arquitectura de Sistemas en Red (SNA)** considerada como la aplicación física real, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) con su **Proyecto 802**, CCITT con su **serie de recomendaciones** sobre telefonía y telegrafía, ANSI con su estándar **SONET** para transmisiones con fibra óptica.

Estas arquitecturas están desarrolladas adecuadamente por organizaciones de estándares, distribuidores comunes y proveedores de computadoras y redes, y usan niveles de acceso en donde las funciones se encuentran organizadas en grupos y asignadas a niveles funcionales específicos. También definen las interfaces entre niveles en un nodo de red y dentro del mismo nivel en dos nodos diferentes.

Dentro de los primeros protocolos más utilizados en las redes se pueden mencionar el RS-232-C, V.24, V.28, X.25, Control de Enlace de Datos de Alto Nivel (HDLC) y Control de Enlace de Datos Síncronos (SDLC). Actualmente, los protocolos que se encuentran en desarrollo y algunos inclusive ya se están aplicando son el TCP/IP con su subconjunto SNMP, IP, ARP, ICMP, FTP, SMTP y FTAM, así como el frame relay, ATM, FDDI, DQDB, B-ISDN, SIP, SONET, CMIP, MCP, PLCP, TP, TTP, etcétera.

1.3.3 Software usado generalmente para la operación de una red.

La operación de la red tiene como base el siguiente software:
SISTEMA OPERATIVO LOCAL: Reside en cada una de las estaciones de trabajo, se encarga de administrar los recursos de las mismas y de controlar su operación. Dentro de los sistemas operativos se tienen al MS-DOS, Netware de Novell, PC-LAN Program de IBM, UNIX, Windows NT, OS-2/LAN, LANtastic, Banyan

de Vines, por mencionar algunos.

SOFTWARE PARA LA DEFINICION DE RED Y EL ACCESO: Funciona en el nivel de enlace a través del nivel de transporte del modelo OSI. Este software es la interface entre las aplicaciones y la red. Contiene una base de datos de todos los recursos de la red y establece una conexión entre estos recursos y una aplicación. Crea una interface con el sistema de administración de la cinta o de disco, con el sistema de itinerario de trabajos, con archivos de datos y programas de aplicación, librerías autorizadas del sistema operativo, catálogos del sistema, salidas del sistema, conjunto de datos del sistema, reportes del sistema, bases de datos y sistemas de telecomunicaciones en línea. Como ejemplos de este software se pueden mencionar el Netware y software compatible con TCP/IP (PCTCP, NCSA).

SOFTWARE PARA CONMUTACION DE PAQUETES: Funciona en la red y niveles de enlace del modelo OSI. Este software es exclusivo de los proveedores y está ligado con el dispositivo de hardware para conmutar paquetes a través de la implementación de X.25, frame relay, ATM, entre otros.

SOFTWARE DE ADMINISTRACION DE LA RED: Funciona en el nivel de transporte del modelo OSI. Este software provee un conjunto de funciones para controlar y mantener la red. Provee información detallada acerca del estado de todos los componentes de la red.

Permite que las computadoras compartan información y recursos dentro de una red y provee confiabilidad en la red. También permite al operador conocer problemas en la red con una pronta señal de advertencia antes de que afecten la confiabilidad de la red para poder remediar las acciones o prevenirlas a tiempo. El HPopenview, Spectrum, LAN Manager, ManageWise de Novell, CISCOWORKS, Netview/6000, LAN watch, todos basados en SNMP, son algunos ejemplos de este tipo de software.

SOFTWARE DE EMULACION DE LA TERMINAL: Funciona en el nivel de enlace del modelo OSI. Este software trabaja en conjunto con una microcomputadora para hacer que funcione como un tipo particular de terminal de un proveedor. Ejemplos de él son Terminal, PCPLUS, XTalk y los propios de cada fabricante.

1.3.4 Tipos de red: LAN, MAN, WAN y otras.

Las redes se clasifican de acuerdo a su distribución geográfica, velocidad y aplicación primaria en Redes de Area Local (Local Area Networks, LANs), Redes de Area Metropolitana (Metropolitan Area Networks, MANs) y Redes de Cobertura Amplia (Wide Area Networks, WANs). La Fig. 2 muestra esta clasificación.

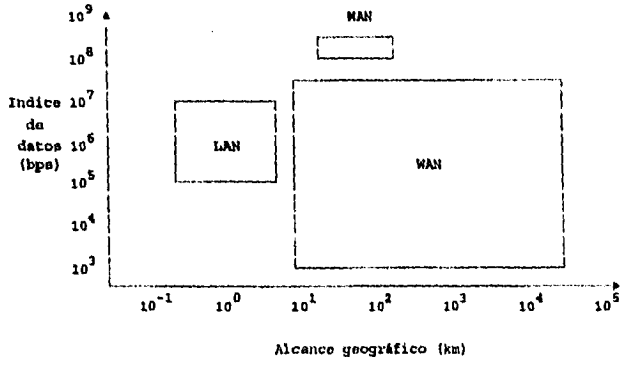


Figura 2 Indice de datos y alcance geográfico para varias clases de redes.

La siguiente definición fue publicada por el IEEE que ha desarrollado un conjunto de estándares para las arquitecturas de las LAN:

LAN: "Un sistema de comunicaciones de datos que permite que se comuniquen directamente un número de dispositivos independientes dentro de una área geográfica de tamaño moderado sobre un canal de comunicaciones físico para índices de datos moderados."[8]

Examinando la definición anterior podemos decir que las LAN permiten enlazar computadoras personales, terminales, mainframes, minicomputadoras y otros periféricos. Transmiten datos a través de un medio físico entre oficinas en el mismo

[8] MARTIN, James Thomas y KAVENAGH, Kathleen: Local Area Networks: Architectures and Implementations, New Jersey, Prentice Hall, 1989, p. 4.

edificio o entre edificios relativamente cercanos localizados a 10 km. a la redonda. Esta cercanía entre los nodos resulta costeable para su interconexión mediante cables de par trenzado, cable coaxial o fibra óptica que permitan velocidades de transmisión de 20 Mbps.

Generalmente las LAN son privadas y su aplicación principal es la transferencia de datos entre PCs.

MAN: "Representa los primeros esfuerzos para unir de manera efectiva la brecha entre los servicios y tecnologías de las LAN y WAN. Se encamina a la interconexión de LANs y hosts en áreas geográficas correspondientes al tamaño de una ciudad grande. Opera a velocidades entre 45 y 150 Mbps y tiene un alcance geográfico de 100 km o más".[9]

Las MAN son redes públicas o privadas ubicadas entre las LAN y WAN y dentro de sus aplicaciones podemos mencionar la interconexión de LANs a través de fibra óptica, voz y datos integrados, facilidad para accesar a bases de datos que almacenen video, documentos e imágenes, facilidad de videoconferencia, facilidad de multilenguajes de audio y video, comunicaciones multimedia, interconexión de PBX y transferencia de imágenes y gráficas de alta resolución.

---

[9] KESSLER, Gary C. y TRAIN, DAvid A.: Metropolitan Area Networks: Concepts, Standards and Services, U.S.A., McGraw-Hill, 1992, p. 9.

WAN: "La Red de Cobertura Amplia transmite información a través de un área geográfica expandida como ciudades y naciones".[10]

Este tipo de red provee la capacidad de conectar varios procesadores de distintas ciudades o naciones a través de fibra óptica, satélite o microondas con estándares de protocolos de transmisión a velocidades que van de 1200 bps hasta 45 Mbps.

Las compañías telefónicas suelen proporcionar los canales para esta red con un determinado costo mensual (distancia x cuota fija) si las líneas son alquiladas y con un costo según la utilización en el caso de líneas normales conmutadas.

1.3.5 Concepto de Arquitectura de una red.

ARQUITECTURA DE UNA RED: Se refiere a cómo trabajan sus componentes en conjunto como un sistema. Define protocolos, formatos de mensaje y topologías para facilitar la compatibilidad entre el hardware y el software. Una arquitectura debe diseñarse de manera tal que permita hacer cambios a la configuración de una manera sencilla y con bajo costo.

---

[10] THE EDP AUDITORS FOUNDATION, INC: EDPAA CISA Review Manual, U.S.A., The Information Systems Control Association. 1995, p. VI-38.

Al realizar la arquitectura de la red se deben conocer las funciones y procedimientos de la organización así como sus necesidades para lograr un buen diseño e implementación basándose en un modelo ya sea el OSI, SNA, Proyecto 802 del IEEE, CCITT u otros.

Para describir la arquitectura de una red es necesario contemplar las tres características siguientes:

Componentes.

Los componentes que conforman una red pueden variar dependiendo de las funciones específicas para las que esté diseñada. Sin embargo, existen componentes comunes a todas ellas como son los siguientes: Medios, técnicas, modos y tipos de transmisión, dispositivos de cómputo y software.

Topologías y protocolos.

TOPOLOGIA: Describe la relación lógica y física de los nodos en una red; es un arreglo esquemático de los enlaces y nodos de la misma. Una arquitectura de red puede incorporar múltiples topologías.

Algunas de las topologías empleadas para LAN son estrella,

anillo y lineal las cuales se muestran en la Fig. 3. Estas pueden combinarse de diversas maneras para formar topologías híbridas. Para las MAN y WAN son punto a punto y multipunto.

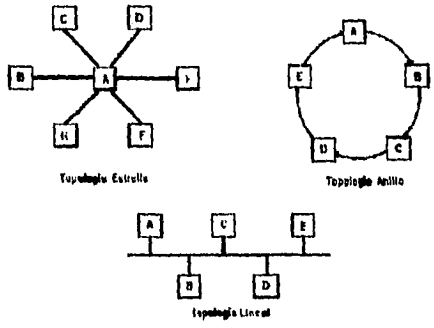


Figura 3 Topologías empleadas en LAN.

Para una mejor comprensión sobre los protocolos en este apartado es necesario saber qué son por lo que a continuación se muestra una definición.

PROTOCOLO: "Es un conjunto de convenciones y reglas para el formato y contenido de datos para ser cambiados entre dos o más dispositivos. En las redes de datos, estas reglas involucran un conjunto de acuerdos (algunas veces basados en estándares internacionales) que pueden cubrir sintaxis (patrones de bits y formatos de campo), semántica (conjunto de peticiones, respuestas y acciones) y tiempo (definición de la secuencia de

eventos). Existen protocolos de IBM, protocolo del sistema de despliegue, los protocolos de BT TYMNET (TYM2), etc."[11]

Para las LAN, MAN y WAN se utilizan los protocolos mencionados en el apartado de estándares en redes y protocolos.

Métodos de control de acceso.

Pueden emplearse diversos métodos de control para compartir el acceso al medio de transmisión, sincronizando convenientemente el envío y la recepción de los mensajes desde cada estación. Para ello, deben considerarse el tipo de topología de red empleada, si el control que se tiene es centralizado, aleatorio o distribuido y los requerimientos de proceso. Cabe señalar que no hay un método mejor que otro; cada uno cuenta con ventajas y desventajas que deben ser consideradas por el implementador de la red.

Dentro de los métodos de control de acceso al medio físico que se pueden emplear en las LAN se tienen los siguientes:

CONTROL ALEATORIO: Cada estación puede transmitir sin ningún permiso. Una estación puede checar el medio antes de transmitir para ver si está libre. Incluye los siguientes controles de

[11] TYMNET INC.: Glossary, U.S.A., marzo 1990, p. 109.

transmisión:

- CSMA/CD.
- Slotted Ring.
- Inserción de registros.

CONTROL DISTRIBUIDO: Sólo una estación a la vez tiene el derecho de transmitir, y ese derecho es pasado de una estación a otra. Sus controles de transmisión son:

- Token passing: Token ring, token bus.
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

CONTROL CENTRALIZADO: Una estación controla toda la red y otorga el permiso a las otras estaciones para poder transmitir. Cuenta con los siguientes controles de transmisión:

- Polling.
- Intercambio de circuitos.
- Acceso Múltiple por División en el Tiempo (TDMA).

De estos métodos, tres son considerados de mayor importancia por que están bajo las bases de los estándares del IEEE para las implementaciones de las LAN: CSMA/CD, token Passing y polling.

Para las MAN y WAN los métodos de control de acceso utilizados son el multiplexado y la conmutación de paquetes.

Otras. Redes Públicas, Privadas y de Valor Agregado.

Redes Públicas.

La introducción de la red pública de transmisión de datos permite tarifas diferenciales mediante las cuales puede utilizarse el medio de transporte únicamente durante el tiempo que sea necesario por pequeño que éste sea. De esta manera suprime el costo por distancia.

RED PUBLICA DE DATOS: Su objetivo es dar servicio a muchos usuarios independientes, es decir, que cualquier usuario utilice la red pública como medio de transporte de sus datos para poder cubrir sus necesidades.

Las redes públicas utilizan la técnica de conmutación de paquetes y la mayoría de ellas, en un principio, habían adoptado los estándares del X.25 para realizar su trabajo. Hoy en día, utilizan el frame relay y TCP/IP por mencionar algunos. Se espera que en un tiempo no muy lejano empleen el ATM que por el momento se encuentra en desarrollo.

Dentro de las principales redes públicas de datos, se tienen

las siguientes:

En Estados Unidos	: TYMNET, ISDN, MCI, AT&T, US Sprint, LDDS y RBOCs.
En Canadá	: DATAPAC y MCI.
En México	: RDI, TELEPAC y TYMNET.
En Gran Bretaña	: IPSS, PSS y Telematic.
En Francia	: TRANSPAC.
En España	: IBERPAC.

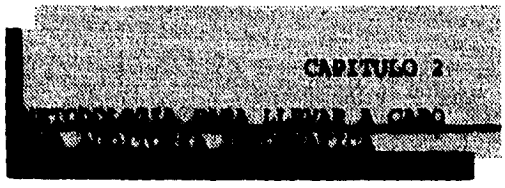
Redes Privadas.

REDES PRIVADAS: También denominadas arrendadas o exclusivas, son dispositivos de transmisión obtenidos de un transportador para uso exclusivo de la organización que las arrenda. Los transportadores son organizaciones autorizadas y controladas que suministran servicios de transmisión a terceros.

En una red privada, el sistema computarizado de una organización está conectado directamente al portador para la transmisión de datos, no siendo necesario utilizar un direccionamiento público para conectarse con las instalaciones del portador. Además de cables de cobre, también suelen utilizarse instalaciones de microondas y satélite.

Redes de Valor Agregado (Value-Added Network, VAN's).

VAN: Son instalaciones públicas que se comparten de igual manera que las redes telefónicas, pero que sólo se utilizan para la transmisión de datos. Se les denomina de "valor agregado" debido a que las organizaciones que operan redes de este tipo obtienen las funciones básicas de transmisión de datos de otras organizaciones, les agregan un valor (por ejemplo: proveer los computadores que interconectan la red) y luego, revenden el servicio a sus clientes. Otro valor agregado es el servicio de detección y corrección
automática de errores de transmisión.



CAPITULO 2

El objetivo de este capítulo es mostrar una metodología que sirva como guía para llevar a cabo una auditoría eficaz y eficiente que se pueda adecuar al tamaño, contexto y complejidad de cualquier organización.

Dicha metodología abarca cinco etapas. En la primera, se lleva a cabo la planeación estratégica en donde se identifica el o las áreas a ser auditadas, se definen los objetivos de la auditoría, se conoce de manera preliminar a la organización y se elabora un plan de trabajo y un presupuesto de acuerdo al alcance que se determine. En la segunda, se hace una evaluación de los componentes que se identificaron con mayor riesgo, mediante la aplicación de pruebas de procedimientos o de saldos a través del uso de computadoras, donde se obtiene información adicional y se documenta la evidencia. En la tercera, se determina si el área a auditar cuenta o no con controles adecuados y si sus operaciones son o no eficientes y eficaces con base en la evidencia obtenida en las dos primeras etapas. En la cuarta, se presenta un informe de auditoría a la Alta Gerencia conteniendo los hallazgos, conclusiones y

recomendaciones sobre la adecuación de los controles y la eficiencia y eficacia de las operaciones así como la designación de las fechas de seguimiento. En esta etapa también se revisa el cumplimiento del plan de trabajo con el cliente y se comentan las diferencias según sea el caso. En la quinta etapa se elabora el informe definitivo incluyendo los comentarios del cliente obtenidos en la etapa anterior para ser anexados en los papeles de trabajo. Finalmente, en la sexta etapa se debe llevar a cabo el seguimiento a las recomendaciones de acuerdo a lo programado en la cuarta etapa.

En resumen, el trabajo de auditoría debe incluir la planeación de la misma, el examen y la evaluación de la información, la comunicación de los resultados y su seguimiento.

2.1 Planeación estratégica.

Los ambientes típicos están caracterizados por una variedad de tecnologías, ambientes que han evolucionado a medida que las compañías han adoptado e integrado una tecnología cambiante a lo largo de los años. Por ello, resulta necesario que el auditor tenga una capacitación constante para hacer frente a cualquier situación que se presente en las distintas organizaciones y pueda contribuir a la mejora de las mismas.

Por otro lado, el auditor debe tener una comprensión cabal y regirse bajo el Código de Etica Profesional promulgado por la Entidad para guiar la conducta profesional y personal de sus miembros. Cabe mencionar que la Entidad es una asociación sin fines de lucro fundada en 1969 con el objeto de promover la educación, comunicación, necesidades de desarrollo profesional e investigación en los campos interrelacionados de la auditoría y sistemas de información.

El Código de Etica Profesional abarca los siguientes aspectos:

Los Auditores en Informática deben:

* **Apoyar** el establecimiento y cumplimiento de normas, procedimientos y controles para los sistemas de información.

* **Cumplir** las Normas de Auditoría en Informática según las adopte la Entidad.

* **Actuar** en interés de sus empleadores, accionistas, clientes y el público en general en forma diligente, leal y honesta y a sabiendas de no contribuir en actividades ilícitas o incorrectas.

* **Mantener** la confidencialidad de la información obtenida en

el curso de sus deberes. La información no será utilizada para propio beneficio 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 capacidad en los campos interrelacionados de la auditoría y los sistemas de información por medio de su participación en actividades de capacitación.

* **Ejercer** sumo cuidado al obtener y documentar material suficiente sobre el cual basar sus conclusiones y recomendaciones.

* **Informar** a las partes involucradas del resultado de las tareas de auditoría llevadas a cabo.

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

* **Mantener** altos estándares de conducta y carácter tanto en las actividades profesionales como en las privadas.

El auditor debe también comprender las Normas Generales para Auditoría en Informática reconocidas por la EDP Auditors Foundation, Inc. (EDPAF), asociación sin fines de lucro fundada en 1976 dedicada a la mejora de la educación, comunicación, desarrollo y estándares profesionales y necesidades de investigación en el campo de la Auditoría en Informática.

Las Normas Generales para Auditoría en Informática son:

1. **Actitud y apariencia**: En todas las cuestiones relacionadas con la auditoría, el auditor en Informática debe ser independiente de quien es auditado en actitud y apariencia.

2. **Relación en la organización**: La función de Auditoría en Informática ha de estar lo suficientemente independiente del área que se audita para permitir una realización objetiva de la auditoría.

3. **Código de ética profesional**: El auditor en Informática debe cumplir el Código de Etica Profesional de la Entidad.

4. **Habilidades y conocimientos**: El auditor en Informática ha de ser competente técnicamente, con las habilidades y conocimientos necesarios para la realización de las tareas de auditoría.

5. **Educación profesional continua:** El auditor en Informática ha de mantener su competencia técnica por medio de la correspondiente educación continua.

6. **Planeación y supervisión:** Las auditorías en Informática han de ser planificadas y supervisadas para brindar seguridad de que se alcanzan los objetivos de auditoría y se cumplen estas normas.

7. **Requerimientos de evidencia:** Durante la realización de la auditoría, el auditor en Informática ha de obtener evidencia que por su naturaleza y suficiencia respalden los hallazgos y conclusiones informadas.

8. **Debido cuidado profesional:** Debe observarse el debido cuidado profesional en todos los aspectos de la tarea del auditor en Informática, incluyendo el cumplimiento de las normas de auditoría aplicables.

9. **Reporte del alcance de auditoría:** Al preparar los informes, el auditor en Informática ha de expresar los objetivos de la auditoría, el periodo que cubre y la naturaleza y extensión de las tareas llevadas a cabo.

10. **Reporte de hallazgos y conclusiones:** Al preparar los informes, el auditor en Informática ha de expresar los

hallazgos y conclusiones respecto de las tareas de auditoría llevadas a cabo, y cualquier reserva o salvedad que el auditor tenga respecto de la auditoría.

2.1.1 Entrevista con la Alta Gerencia, definición de requerimientos y objetivo.

En la planeación estratégica, el socio y el gerente de la Auditoría Informática deben reunirse con la Alta Gerencia para definir su requerimiento.

La Alta Gerencia puede requerir que se lleve a cabo una revisión sobre alguna o algunas áreas en específico simplemente por conocer si se están aplicando de manera adecuada los controles necesarios o por haber identificado algún problema. Los aspectos críticos para las operaciones diarias de una organización que se pueden evaluar en tales áreas pueden ser los siguientes:

* **CONTROLES GENERALES**

  El auditor debe revisar la estructura organizativa, políticas, procedimientos operativos y ambiente de control del área de Informática.

* **SEGURIDAD**

El auditor debe analizar y evaluar los controles de acceso físico, lógico y controles ambientales, que resguarden el centro de cómputo frente a amenazas accidentales, intencionales y naturales que causen daños, destrucciones o usos indebidos.

* **CENTROS DE CÓMPUTO**

El auditor debe revisar las operaciones de las áreas de los centros de cómputo.

* **CONTINUIDAD DE LAS OPERACIONES**

El auditor debe analizar y evaluar las políticas y procedimientos referentes al plan de contingencias para asegurar la capacidad de la organización para responder eficazmente ante desastres y otras situaciones de emergencia.

* **SISTEMAS OPERATIVOS Y UTILITARIOS**

El auditor debe analizar y evaluar las políticas y procedimientos de seguridad y control de desarrollo, adquisición y mantenimiento de software de sistemas

operativos.

* **CICLO DE VIDA DEL DESARROLLO DE SISTEMAS**

  El auditor debe identificar, analizar y evaluar la metodología, normas, tareas y procedimientos usados para el desarrollo y mantenimiento de sistemas.

* **ADQUISICIÓN, CAMBIOS Y MANTENIMIENTO DE HARDWARE Y SOFTWARE**

  El auditor debe revisar la metodología, normas, tareas y procedimientos para la adquisición, cambios y mantenimiento de hardware y software.

* **CONTROL DE APLICACIONES**

  El auditor debe identificar, analizar y evaluar las fortalezas, debilidades, eficiencia y efectividad de control de las operaciones dentro de los sistemas de aplicación existentes.

La organización puede haber identificado la presencia de algunos de los siguientes problemas considerados como los más significativos para una operación eficiente de la misma:

* Actitudes desfavorables de los usuarios finales,
* Costos excesivos,
* Excesos a presupuestos,
* Alta rotación de personal,
* Frecuentes errores en los equipos de cómputo,
* Atraso excesivo de solicitudes de usuario no satisfechas,
* Bajo tiempo de respuesta del equipo de cómputo,
* Numerosos proyectos de desarrollo suspendidos,
* Compras de hardware y software sin respaldo o autorización,
* Cambios frecuentes a versiones superiores de hardware y software,
* Mantenimiento de registros erróneos,
* Contabilidad no aceptable,
* Fraudes y desfalcos,
* Sanciones legales,
* Pérdida o destrucción de activos, y
* Desventajas competitivas.

Posteriormente, debe definirse el objetivo de la auditoría basándose en el requerimiento con el propósito de identificar los controles clave y realizar procedimientos de auditoría para probarlos. Asimismo, puede llegar a descubrirse una variedad de controles fuertes y débiles al evaluar la estructura global y de este modo determinar si minimizan los riesgos de la organización.

Al evaluar los controles, el auditor también debe identificar los tipos de riesgo a que está expuesta la organización, para así poder determinar cuál de las áreas o componentes deben ser auditados y poder planear su auditoría. Para ello, presentamos a continuación una clasificación de riesgos y controles:

RIESGO INHERENTE: Susceptibilidad de la información a errores o irregularidades significativas antes de considerar la efectividad de los sistemas de control. Como factores de riesgo inherente encontramos:

- Naturaleza de la organización que comprende:
  - Naturaleza de los productos,
  - Volatilidad, y
  - Circunstancias económicas.
- Naturaleza de los componentes que comprende:
  - Transacciones del negocio,
  - Subjetividad de la base para contabilizar, y
  - Problemas de realización.
- Naturaleza de los sistemas de información y contabilidad que comprende:

- Grado de automatización,
- Efectividad, y
- Complejidad.

RIESGO DE CONTROL: Es cuando un error significativo no puede ser evitado o detectado en forma oportuna por el sistema de controles internos. Dentro de los factores que pueden provocar este riesgo se encuentran:

- Transacciones nuevas o complejas,
- Volumen excesivo de transacciones,
- Reducción del personal,
- Falta de segregación de funciones,
- Seguimientos o revisiones inadecuadas, y
- Sistemas deficientes.

RIESGO DE DETECCION: Es el riesgo de que los procedimientos de auditoría no puedan descubrir errores o irregularidades significativas. Este riesgo es una función de la efectividad de los procedimientos de auditoría, su alcance, oportunidad y precedencia o interpretación de los hallazgos de auditoría.

RIESGO DE AUDITORIA: Se refiere al riesgo de emitir un informe de auditoría inadecuado porque el proceso no ha detectado errores o irregularidades significativas. Estos comprenden por ejemplo a los errores significativos que pueden estar presentes

en los estados financieros y que no son evitados o detectados por los sistemas de control de la organización ni descubiertos por los procedimientos de auditoría.

RIESGO DEL NEGOCIO: Son aquellos riesgos que pueden afectar la viabilidad a largo plazo de un determinado negocio u organización.

CONTROLES GENERALES: Son controles globales interdependientes válidos para todas las áreas de la organización. Los métodos para llevar a cabo estos controles incluyen políticas y procedimientos establecidos por la gerencia para proveer una razonable garantía de que se han alcanzado los objetivos particulares.

CONTROLES PREVENTIVOS: Son aquellos controles diseñados para evitar que se produzca un error, omisión o acto malicioso.

CONTROLES DE DETECCION: Son aquéllos que detectan que se ha producido un error, omisión o acto malicioso e informan de su aparición.

CONTROLES CORRECTIVOS: Son aquéllos que corrigen errores, omisiones o actos maliciosos una vez detectados.

CONTROLES DE CONTABILIDAD INTERNOS: Forman parte de un sistema

de control interno. Están dirigidos primordialmente a contabilizar las operaciones y conciernen a la salvaguarda de los activos y la confiabilidad de los registros contables.

CONTROLES DE OPERACIONES: Forman parte de un sistema de control interno. Se dedican a garantizar que las operaciones, funciones y actividades diarias satisfacen los objetivos del negocio.

CONTROLES DE ADMINISTRACION: Forman parte de un sistema de control interno. Son aquellos que respaldan los controles operativos relacionados con la eficiencia operativa y el cumplimiento de las políticas de la organización.

CONTROLES COMPENSATORIOS: Son aquellos controles fuertes que respaldan a controles débiles. Esto es, cuando un control respalda la debilidad de otro.

CONTROLES YUXTAPUESTOS: Son aquéllos que pueden mejorar otro control adecuado. En este caso, los dos controles son fuertes.

2.1.2 Conocimiento preliminar de la organización.

En caso de que sea la primera vez que se audita a la organización, el Gerente de la auditoría debe asignar a una persona de su grupo para conocer el giro, tamaño, contexto y

complejidad de la misma en forma general de manera preliminar auxiliándose de todas o algunas de las siguientes técnicas de auditoría para recopilar información:

* Recorrido de las instalaciones de la organización para observar al personal realizando sus actividades,

* Lectura de material sobre antecedentes que incluyan publicaciones sobre la organización, memorias e informes financieros independientes,

* Entrevistas a gerentes claves para comprender los temas comerciales esenciales,

* Aplicación de cuestionarios a personas claves,

* Estudio de los informes sobre normas o reglamentos,

* Revisión de la documentación de sistemas técnicamente complejos y entrevista a especialistas técnicos, y

* Revisión de informes de auditorías previas y planes estratégicos a largo plazo.

Dado que los diversos ambientes de procesamiento varían entre las diferentes instalaciones, un recorrido en general debe dar

una mejor comprensión y percepción al auditor de las tareas, procedimientos y ambiente de control de operaciones en el centro de cómputo en aspectos como las restricciones de acceso físico, controles de riesgos ambientales y fuentes alternativas de energía en las áreas de programación, biblioteca de cintas, estaciones de impresión, oficinas de la gerencia, identificación de todo el equipo de comunicaciones que se muestra en el diagrama de la red y cualquier otro centro de almacenamiento de respaldos fuera de la sede.

La entrevista debe ser una destreza importante para el auditor en Informática, debe organizarla de antemano, seguir un esquema fijo y documentarla con notas. Un buen enfoque es un formulario o cuestionario de entrevista preparado por un auditor en Informática o una lista de control. El auditor debe darse cuenta que el propósito de las entrevistas es recopilar evidencia de auditoría de manera objetiva y tener una naturaleza de descubrimiento y no acusatoria.

Por otro lado, la observación de operaciones es una técnica de auditoría clave para muchos tipos de revisiones, es el mejor método para que el auditor garantice que la persona que está asignada y autorizada a realizar determinada función es la persona que en realidad está cumpliendo la tarea y de este modo tenga oportunidad de ser testigo de cómo se comprenden y aplican las políticas y procedimientos y se asegura la

eficiencia de las operaciones así como la integridad y seguridad de los datos. El auditor no debe ser inoportuno al hacer sus observaciones y debe documentar todo con suficiente grado de detalle como para estar en condiciones de presentarlo posteriormente como evidencia de auditoría.

El auditor debe anexar a los papeles de trabajo toda la evidencia recopilada que respalde los hallazgos de auditoría, lo cual está comprendido en la Norma No. 7 "Requerimientos de evidencia". Dicha evidencia debe incluir las observaciones del auditor, notas tomadas en las entrevistas, material extraído de la correspondencia o documentación interna. El auditor debe decidir qué evidencia es significativa y apropiada para los objetivos de la auditoría, considerando los siguientes factores:

Independencia de quien provee la evidencia. La evidencia que se obtiene de fuentes externas es más confiable que la que proviene de la organización.

Calificación de quien provee la información o evidencia. El auditor debe tener en cuenta las calificaciones de quienes proveen la información. Si un auditor no tiene una buena comprensión de una área técnica bajo examen, la información reunida para probarla puede no ser confiable, especialmente si el auditor no comprende claramente la

prueba.

Objetividad de la evidencia: La evidencia objetiva es mejor que la evidencia que exige juicios de valor o interpretación. El análisis de la eficiencia de una aplicación que hace un auditor, basada en discusiones con determinado personal, puede no constituir una evidencia de auditoría objetiva.

Para conocer a la organización de manera preliminar, se desarrolló una guía para la planeación estratégica basada en la técnica del cuestionario (véase anexo 1, p. A1), la cual permite al auditor llevar a cabo la revisión de:

a) Un manual de organización que permita obtener información como:

* El responsable del Area de Informática, de quién depende y cuánto personal tiene a su cargo.

* La segregación de funciones.

* Si cuenta con el personal con capacidad profesional.

* La rotación de personal.

* Si existe un Comité de Dirección.

* Si el área está organizada en forma centralizada o descentralizada entre varias unidades operativas.

* Si cuenta con una función de auditoría interna que supervise los departamentos.

b) Un manual de procedimientos para :

* Conocer si se están llevando de manera adecuada las funciones y procedimientos de cada una de las áreas que la integran y si son aplicables en todos los centros de procesamiento de manera uniforme en sistemas descentralizados.

* Conocer algunos cambios en las operaciones de los departamentos que se quisieran hacer.

c) Hardware y software con que cuenta la organización para tener una visión general del mismo:

* Tipo, número y lugar de los principales centros de procesamiento (CPUs) y si están interconectados.

* Tipo de procesamiento: Centralizado o descentralizado.

* Modo de ingreso de datos: Se efectúa únicamente en los lugares de procesamiento o en forma remota.

* Arquitectura de la red de comunicación de datos en caso de que la información sea transferida electrónicamente.

* Software de sistemas y comunicaciones utilizado.

* Diagrama que ilustre la relación entre las aplicaciones más significativas y la descripción de cada una.

* Características generales de cada una de las aplicaciones siginificativas.

* Cambios significativos que se han presentado en hardware y software.

De este modo, se puede saber hasta qué punto se encuentra automatizada la organización y la complejidad de sus sistemas.

d) Los aspectos organizacionales significativos para conocer

* Qué cambios se anticipan a nivel organizacional.

* Qué cambios significativos han habido en la estructura organizativa.

* Si se cuenta con un presupuesto anual para el área de Informática y cómo está integrado.

* Si cuenta con un plan maestro de sistemas.

* Los proyectos principales del área de Informática.

* Los problemas o riesgos más relevantes que enfrenta cada uno de los departamentos en su administración.

* Si cuenta con estándares escritos sobre seguridad de datos y desarrollo, pruebas e implantación de sistemas.

* Si se cuenta con un análisis de riesgo formal o informal para el control de accesos de personas no autorizadas.

e) El ambiente de los controles generales a fin de identificar:

* El enfoque que le ha dado la dirección y la gerencia superior.

* Cómo y qué tanto han aplicado las recomendaciones proporcionadas en auditorías internas o externas.

* La manera en que se ejerce el control gerencial.

Al efectuar esta evaluación, el auditor debe apoyarse en la siguiente tabla de controles generales que ha sido preparada para mostrarle cómo verificar la existencia de los medios de control de aplicaciones y del área de Informática y en caso de ausencia de los mismos le explica el riesgo en que se puede incurrir (véase anexo 1, p. A30):

CONTROLES EN SISTEMAS DE APLICACION

FUNCION: 1. Acceso a funciones de procesamiento de las transacciones o registros de datos resultantes.

RIESGO: Personas no autorizadas pueden tener acceso a las funciones de procesamiento de transacciones de los programas de aplicaciones o archivos de datos resultantes, permitiéndoles leer, modificar, agregar o eliminar información.

MEDIOS DE CONTROL:

Segregación de funciones

Para obtener evidencia de control sobre la segregación de funciones el auditor debe:

Al efectuar esta evaluación, el auditor debe apoyarse en la siguiente tabla de controles generales que ha sido preparada para mostrarle cómo verificar la existencia de los medios de control de aplicaciones y del área de Informática y en caso de ausencia de los mismos le explica el riesgo en que se puede incurrir (véase anexo 1, p. A30):

CONTROLES EN SISTEMAS DE APLICACION

FUNCION: 1. **Acceso a funciones de procesamiento de las transacciones o registros de datos resultantes.**

RIESGO: **Personas no autorizadas pueden tener acceso a las funciones de procesamiento de transacciones de los programas de aplicaciones o archivos de datos resultantes, permitiéndoles leer, modificar, agregar o eliminar información.**

MEDIOS DE CONTROL:

Segregación de funciones

Para obtener evidencia de control sobre la segregación de funciones el auditor debe:

- Analizar las responsabilidades de aquellos empleados a quienes se les asignan partes significativas del procesamiento de información. Para ello, el auditor debe determinar si las responsabilidades de iniciación de las transacciones están separadas de las responsabilidades de aprobación, procesamiento y registro de las mismas. Debe asegurarse de que todos los procesamientos por los cuales las transacciones e información directamente relacionada es iniciada o ingresada para su procesamiento hayan sido evaluados, incluyendo los reingresos de transacciones rechazadas.

- Observar a los empleados mientras desempeñan sus tareas para determinar si cumplen con las responsabilidades asignadas.

Controles de acceso

Para verificar los controles de acceso programados el auditor debe llevar a cabo uno o más de los siguientes procedimientos:

- Obtener, revisar y analizar los perfiles o tablas de seguridad del monitor de teleprocesamiento, software de control de acceso o DBMS. El propósito de esta prueba es que el auditor determine si el acceso a las funciones de procesamiento del software de aplicación a los datos

relacionados está apropiadamente restringido para que los usuarios no autorizados y aquellos a quienes se les hayan asignado funciones potencialmente incompatibles no puedan acceder a los mismos. Debe acordar las características de los perfiles con la gerencia de la organización. Es importante analizar la compatibilidad de funciones entre los departamentos como también dentro de un mismo departamento.

- Intentar desplazarse de un menú de aplicación a otro para determinar si existe la posibilidad de realizar funciones incompatibles. Esta prueba permitirá al auditor determinar la efectividad de las restricciones de acceso funcionales y a la vez mejorar su conocimiento de la estructura del menú autorizado para el sistema.

- Determinar si el paquete de software de seguridad en el cual se deposita confianza ha sido implantado adecuadamente desde el punto de vista técnico. El propósito de este paso es determinar si su uso proporciona el nivel de control deseado y verificar que no puede ser eludido con facilidad.

- Determinar la distribución de funciones. Es razonable que el acceso a las funciones más sensitivas sólo será permitido a un reducido grupo de personas y el acceso a

las funciones menos sensitivas podrá ser otorgado a una mayor cantidad de personas. En este sentido, sería útil que el auditor haga un análisis de las funciones de aplicación por cantidad de usuarios.

FUNCION: 2. Datos ingresados para su procesamiento.

RIESGO: Los datos permanentes y de transacciones ingresados para su procesamiento pueden ser imprecisos, incompletos o ser ingresados más de una vez.

MEDIOS DE CONTROL:

Controles de edición y validación

Dentro de la revisión de los controles de edición y validación es necesario que el auditor determine si:

- Las rutinas de procesamiento programadas que contienen los controles de edición y validación funcionan de la manera esperada.

- Los controles que aseguran que las transacciones rechazadas son identificadas y mantenidas en archivos en suspenso funcionan de la manera esperada y no pueden ser

las funciones menos sensitivas podrá ser otorgado a una mayor cantidad de personas. En este sentido, sería útil que el auditor haga un análisis de las funciones de aplicación por cantidad de usuarios.

FUNCION: 2. Datos ingresados para su procesamiento.

RIESGO: Los datos permanentes y de transacciones ingresados para su procesamiento pueden ser imprecisos, incompletos o ser ingresados más de una vez.

MEDIOS DE CONTROL:

Controles de edición y validación

Dentro de la revisión de los controles de edición y validación es necesario que el auditor determine si:

- Las rutinas de procesamiento programadas que contienen los controles de edición y validación funcionan de la manera esperada.

- Los controles que aseguran que las transacciones rechazadas son identificadas y mantenidas en archivos en suspenso funcionan de la manera esperada y no pueden ser

eludidos.

- Empleados autorizados de los departamentos usuarios han tomado las medidas adecuadas con respecto a las excepciones o errores incluidos en los listados generados por el computador.

FUNCION: 3. Datos rechazados y partidas en suspenso

RIESGO: Los datos rechazados y las partidas en suspenso pueden no ser identificadas, analizadas y corregidas.

MEDIOS DE CONTROL:

Controles programados sobre partidas en suspenso

Para probar la existencia de los controles programados sobre partidas en suspenso el auditor debe incluir los siguientes pasos:

- Examinar las conciliaciones efectuadas por la organización de los movimientos de ingreso y egreso de los registros en suspenso.

- Determinar que la organización cumpla con los procedimientos de revisión y seguimiento de las partidas en suspenso.

- Obtener el listado de partidas en suspenso pendientes; seleccionar algunas partidas y determinar que las transacciones hayan sido correctamente registradas y/o eliminadas del archivo en suspenso.

- Diseñar y utilizar transacciones de prueba para confirmar que las transacciones inválidas son rechazadas e incluidas en archivos en suspenso e informes de excepción que serán investigados por el departamento usuario correspondiente.

A fin de evaluar si los procedimientos de seguimiento de los departamentos usuarios relativos a las transacciones rechazadas funcionan apropiadamente, el auditor debe aplicar los siguientes procedimientos:

- Conciliar el movimiento neto del total de partidas rechazadas.

- Seleccionar y examinar una muestra de transacciones incluidas en los informes de excepciones o errores durante el periodo bajo examen y:

- Determinar, a través de observación e indagación, si las excepciones han sido resueltas por personal del departamento usuario correspondiente.

- Determinar que las transacciones hayan sido reingresadas para su procesamiento de acuerdo con los procedimientos establecidos.

- Diseñar y utilizar transacciones de prueba para determinar que las transacciones inválidas son adecuadamente rechazadas e informadas.

FUNCION: 4. Procesamiento y registro de transacciones

RIESGO: Las transacciones reales que han sido ingresadas para su procesamiento o generadas por el sistema pueden perderse o ser procesadas o registradas en forma incompleta o inexacta o en el periodo contable incorrecto.

MEDIOS DE CONTROL:

Para probar la existencia de los controles con respecto a la integridad y exactitud del procesamiento el auditor debe incluir procedimientos para determinar si:

- Las rutinas programadas funcionan de la manera esperada.

- Los controles programados que aseguran que las transacciones rechazadas son identificadas e incluidas en archivo en suspenso funcionan de la manera esperada y no pueden ser vulnerados.

- El personal de los departamentos usuarios ha tomado medidas apropiadas con respecto a las excepciones o errores.

Documentos fuente prenumerados

Si el software de aplicación ha sido programado para asignar números de referencia a las transacciones ingresadas para procesamiento, controlar su secuencia numérica y producir informes de excepción de los documentos faltantes, el auditor debe evaluar este control de la siguiente manera:

- Obteniendo los informes de excepción y verificando que las excepciones informadas hayan sido seguidas de manera adecuada.

- Utilizando técnicas de auditoría asistidas por computador, tales como:

- Técnicas de transacciones de prueba (datos de prueba o procedimientos de prueba integrada).

- Módulos de auditoría incorporados a los programas.

Estas técnicas son tratadas más en detalle en el apartado 2.2.2 Aplicación de las pruebas de procedimientos a las personas clave.

Controles de sesión

Dado que los controles de sesión son efectuados por el software de aplicación, el único método efectivo para probar los mismos es a través de técnicas de transacciones de prueba. Si la aplicación ha sido programada para generar informes de excepción posteriores a la actualización, será necesario que el auditor determine que las excepciones informadas sean analizadas y resueltas en un plazo razonable.

Controles por lotes

Si los controles por lotes sobre el ingreso de datos son considerados clave, el auditor debe probar su efectividad de la siguiente manera:

- Recalculando los totales de control por lotes a partir de

los documentos fuente.

- Siguiendo lotes seleccionados hasta el registro de control de datos.

- Verificando, para periodos seleccionados, que la función de control de datos haya comprobado la secuencia numérica de los lotes a través de todas las etapas del procesamiento.

- Verificando, para periodos seleccionados, que las transacciones rechazadas sean prontamente resueltas.

- Confirmando que los procedimientos de revisión de la autorización de los datos ingresados para procesamiento sean efectivos.

- Probando los procedimientos existentes para la cancelación de los documentos de ingreso.

Controles de balanceo programados

Al igual que los controles de sesión, los controles de balanceo programados son efectuados por el software de aplicación y sólo pueden ser probados en forma efectiva mediante el uso de técnicas de transacciones de prueba.

Control de rótulos internos de archivos

Estos controles son ejecutados automáticamente por el software de administración de operaciones y/o software de administración de archivos de datos, y pueden ser utilizados para asegurar que se utilizan las versiones correctas de los archivos de datos y programas de producción.

Controles de transmisión de datos

Por lo general, no es necesario preocuparse acerca de los dispositivos estándar del software de control de telecomunicaciones, una vez que se ha establecido que se utiliza el paquete apropiado y que el algoritmo de cálculo ha sido correctamente implantado. En ciertas ocasiones, especialmente en instituciones financieras, en las que montos significativos de fondos son transferidos automáticamente en base a transmisiones de datos, los procedimientos y controles de transmisión podrán merecer una consideración especial.

Procedimientos de reenganche y recuperación

Los procedimientos de reenganche y recuperación deben ser probados de la siguiente manera:

- Determinar, a través de una revisión de los registros del

computador (logs) y de indagaciones al personal de los departamentos usuarios y del área de Informática, la frecuencia de fallas del sistema y el nivel de conocimiento y satisfacción que tienen los usuarios sobre los procedimientos de recuperación.

- Comprobar, para una muestra de días en los cuales se suscitaron fallas, que se hayan seguido procedimientos de recuperación adecuados.

- De no haber habido fallas en el sistema, revisar que los procedimientos de recuperación hayan sido claramente definidos y documentados, y que hayan sido probados.

- Controlar que los registros de datos (logs) sean revisados y retenidos verificando que se mantengan copias de los archivos maestros según lo establecido.

Controles de corte programados

El auditor debe revisar y verificar:

- Tablas calendario incluidas en el software de aplicación para comparaciones internas con las fechas de las transacciones.

- Procedimientos para controlar el procesamiento completo y oportuno de los datos ingresados.

- Informes de las excepciones a los criterios de corte.

- Controles de rótulos de encabezamiento de archivos para asegurarse de que al cierre de cada periodo contable se actualizan las versiones correctas de los archivos de datos.

- En sistemas de procesamiento distribuido de datos:

  - Conciliación de los datos procesados localmente en un determinado periodo con los ingresados para procesamiento central.

  - Conciliación de los saldos de los archivos locales y centrales al cierre de cada periodo.

- En los sistemas contables integrados, procedimientos para asegurar que se mantenga un rastro de auditoría para los totales de control y para las transacciones individuales transferidas entre sistemas (es decir, bajo control de programas).

- En sistemas de bases de datos, controles para asegurar un

adecuado corte entre los datos de cada día.

Transacciones generadas

Para probar la existencia de los controles sobre transacciones generadas el auditor debe:

- Verificar que los datos sean generados en el momento correcto.

- Confirmar que los usuarios hayan revisado las salidas impresas, tanto por partidas individuales como globalmente, y que las partidas inusuales hayan sido investigadas.

- Seleccionar, de las salidas impresas, una muestra de transacciones generadas y:

  - Conciliar los datos permanentes con los registros del usuario tales como nóminas de personal y listas de precios.

  - Conciliar las imputaciones contables con las copias impresas del mayor general.

  - Revisar las salidas impresas y obtener explicaciones

satisfactorias de los usuarios acerca de las partidas más significativas o inusuales.

- Controlar las conciliaciones efectuadas por los usuarios de los informes de actualización de archivos.

- En ausencia de salidas impresas adecuadas, utilizar datos de prueba para controlar el correcto funcionamiento de los programas más importantes.

Cálculos programados

Los controles sobre cálculos programados deben ser probados mediante:

- Selección, a partir de las salidas impresas, de una muestra de transacciones y recreación de los cálculos para comprobar su exactitud.

- Utilización de datos prueba para controlar el correcto funcionamiento de los programas de cálculo.

Controles sobre la extracción y presentación de información contenida en archivos magnéticos

Para verificar estos controles el auditor debe evaluar los

procedimientos programados a través de:

- Rastro de auditoría para identificar la inclusión de transacciones y saldos individuales en totales y resúmenes emitidos por el computador.

- Recuento de los registros de archivos leídos en el análisis y extracción de datos.

- Revisión de controles de razonabilidad aplicados a los totales y resúmenes del computador.

- Conciliación de los totales y resúmenes del computador con los registros de control de archivos.

- Revisión de controles de registros faltantes y duplicados.

- Revisión de controles de programa a programa cuando se utiliza más de un programa en secuencia para el análisis, extracción y presentación de datos.

y los procedimientos del usuario a través de:

- Conciliación de totales generados por el computador con la información de salida relacionada.

- Revisión de controles de razonabilidad de la información de salida (global y muestras).

- Conciliación de los informes de recuento de registros con registros manuales y la información de salida relacionada.

- Revisión de la especificación de los criterios para informes de excepción.

- Revisión del adecuado seguimiento de los informes de excepción.

- Revisión de la distribución restringida de información confidencial.

CONTROLES DEL AREA DE INFORMATICA

FUNCION: 5. Estructura organizativa y procedimientos de operación del área de Informática

RIESGO: La estructura de organización y los procedimientos operativos del área de Informática no garantizan un ambiente de procesamiento de datos que conduzca a la preparación de información confiable.

Segregación de funciones

La verificación de la segregación de funciones incluye los siguientes procedimientos:

- Análisis de la efectividad con que se han segregado las funciones incompatibles.

- Indagación a los empleados a fin de que el auditor confirme su comprensión de las responsabilidades laborales y las correspondientes limitaciones.

- Observación, cuando fuese apropiado, del desempeño de los empleados, de la supervisión que se ejerce sobre los mismos y de la efectividad aparente de la misma.

Controles operativos diarios del área de Informática

El auditor debe probar la existencia de los controles operativos diarios a través de:

- Examinar los informes del sistema de registro de trabajos (job accounting) o los registros impresos de la consola y

verificar:

- La secuencia para comprobar que haya explicación del uso del computador.
- Que exista evidencia de su aprobación por la gerencia.
- Que se hayan tomado acciones apropiadas.

- Establecer si la gerencia ha recibido y aprobado un resumen del uso del computador.

Además debe examinar:

- Los **manuales de operación** para determinar que incluyan procedimientos escritos claramente definidos para todas las actividades operativas, incluyendo procedimientos de corrida para los operadores, procedimientos de reenganche y recuperación, por mencionar algunos.

- La **supervisión de usuarios privilegiados** que a través del software de control de acceso utilicen utilitarios sensitivos y editores en línea y generen los informes correspondientes, para poder:

  - Establecer si el software de control de acceso ha sido implantado de manera adecuada para asegurar que

los informes de actividad sean generados adecuadamente.

- Observar y probar la forma en que los supervisores utilizan dichos informes para supervisar las actividades de los empleados.

- Determinar que los dispositivos del software de control de acceso no puedan ser eludidos mediante software sensitivo.

Los procedimientos que el auditor puede aplicar respecto de los usuarios privilegiados incluyen:

- Determinar qué empleados deben ser considerados usuarios privilegiados.

- Establecer si la gerencia revisa los informes generados, ya sea por el software de control de acceso o por el software de administración de bibliotecas a fin de determinar si el acceso a los programas de aplicación y a los archivos de datos está autorizado.

- **El control sobre software sensitivo** para:

- Obtener un listado de todo el software sensitivo.

- Obtener comprensión de los controles que aseguran que todo el software instalado está autorizado y registrado.

- Seleccionar una muestra de módulos de software de sistemas y verificar la autorización de la gerencia del área de Informática para su incorporación, partiendo de los directorios de las bibliotecas.

- Determinar si los controles de acceso al software sensitivo son adecuados y si funcionan de la manera esperada.

- Confirmar que la gerencia supervisa el uso del software sensitivo y que queda constancia de dicha supervisión.

- En los casos en que los utilitarios son mantenidos separados, probar las autorizaciones para su reinstalación y uso, y confirmar que los programas sean borrados inmediatamente al concluirse la tarea autorizada.

- Los **controles sobre el desarrollo de sistemas** para:

- Revisar las especificaciones escritas referentes a las nuevas aplicaciones.

- Determinar si las especificaciones para nuevas aplicaciones y las modificaciones de las aplicaciones existentes fueron preparadas de acuerdo con las normas de instalación.

- Determinar si el usuario está satisfecho de que en las especificaciones se hayan incorporado sus requerimientos.

- Determinar a través de conversaciones con los usuarios y el personal del área de sistemas, el alcance de las modificaciones realizadas en las aplicaciones contables significativas y si la participación del usuario fue la necesaria en el desarrollo de sistemas.

FUNCION: 6. Procedimientos para cambios a programas

RIESGO: Los programadores pueden realizar cambios incorrectos no autorizados en el software de aplicación, lo cual reducirá la confiabilidad de la información financiera procesada en el sistema.

Controles sobre cambios a programas

El auditor debe obtener evidencia sobre la confiabilidad de los procedimientos de cambios a los programas seleccionando cambios representativos y determinando si los procedimientos de revisión y aprobación han sido respetados. Los cambios efectuados a los programas pueden ser determinados en base a los dispositivos automáticos de numeración ascendente del software de administración de bibliotecas o a los informes automáticos generados cada vez que el programa es modificado.

El auditor debe confirmar que los programadores:

- Sólo pueden acceder a los programas de aplicación en las bibliotecas de prueba.

- No pueden transferir los programas modificados a producción si no se han cumplido los procedimientos en vigencia para cambios a los programas.

El auditor debe alcanzar estos objetivos de la siguiente forma:

- Determinando si se han establecido bibliotecas separadas

de producción y de prueba, en forma tal que sea técnicamente posible restringir el acceso de los programadores a los programas de producción.

- Revisando los perfiles de autorización del software de control de acceso para determinar que las bibliotecas de producción sean recursos restringidos a los que los programadores no puedan acceder.

- Determinando que los comandos de administración del software de control de acceso no permitan a los programadores eludir los dispositivos de restricción de acceso.

Enfoques alternativos

Si no existen fuertes controles sobre los cambios a los programas, el auditor debe considerar enfoques alternativos para determinar si:

- El software de administración de bibliotecas ha sido programado de manera adecuada para generar un informe por cada nueva versión de un programa.

- Los dispositivos automáticos de control de versiones del software no pueden ser eludidos.

- Los cambios a los programas fuente son identificados e informados por los dispositivos de comparación de código fuente.

- Los programas en código fuente son una representación exacta de los programas en código objeto.

FUNCION: 7. Acceso general a los datos o programas de aplicación

RIESGO: Personas no autorizadas pueden tener acceso directo a los archivos de datos o programas de aplicación utilizados para procesar transacciones, permitiéndoles realizar cambios no autorizados a los datos o programas.

MEDIO DE CONTROL:

Software de control de acceso

Dependiendo de las características del sistema de la organización, el auditor debe aplicar uno o más de los siguientes procedimientos para probar la existencia de los controles sobre el acceso no autorizado implantados a través de un software de control de acceso:

- Observar los controles de acceso al sistema para que confirme su comprensión del proceso.

- Obtener copias de los perfiles de seguridad y tablas de contraseñas e identificaciones del usuario con el acceso a recursos protegidos (por ejemplo: archivos de datos, programas, utilitarios, editores en línea), y revisarlas para determinar su integridad y consistencia con la comprensión del auditor respecto de las restricciones al acceso.

- Intentar llevar a cabo violaciones a la seguridad para establecer que el software de seguridad restringe el acceso de manera efectiva y que los intentos de violación son incluidos en los informes de seguridad.

- Seleccionar una muestra de informes de seguridad y verificar que el encargado de la seguridad de datos u otro empleado responsable haya investigado las violaciones informadas, y haya supervisado y efectuado el seguimiento de las actividades de los usuarios privilegiados.

- Analizar las interacciones del paquete de software de seguridad con los demás paquetes de software de sistemas utilizados por el cliente (por ejemplo: sistemas operativos, monitores de teleprocesamiento, DBMS). El

objetivo de este procesamiento es:

- Determinar si todos los dispositivos de los paquetes de software interrelacionados necesarios para hacer que el software de seguridad sea operativo han sido activados.

- Determinar si existen dispositivos de otro software de sistemas en uso que inhiban la efectividad del software de control de acceso.

Registro de operaciones (o de consola)

El auditor debe:

- Obtener información del registro de operaciones y determinar la naturaleza de la información contenida en el mismo, como por ejemplo la descripción de los programas que han sido corridos y usuarios que han accedido al sistema.

- Determinar si se ha informado alguna actividad inusual.

- Establecer si la gerencia ha investigado las actividades inusuales.

Controles basados en informes especiales para la gerencia

El auditor debe saber cómo son utilizados los paquetes de software de sistemas por la gerencia para controlar y supervisar el acceso y las operaciones. Para determinar si los informes generados por esos paquetes son efectivamente utilizados con fines de control, debe revisar algunos y verificar que se efectúe un seguimiento adecuado de las actividades inusuales.

Restricción del acceso físico

Para probar la existencia de los controles que restringen el acceso físico a los recursos del sistema, el auditor debe:

- Observar los controles físicos sobre el acceso al centro de cómputo, biblioteca de cintas, documentos y diccionario de datos de los programas.

- Obtener listados del personal que tiene acceso a cada una de las áreas de los lugares en donde están instalados los computadores y determinar si estos listados han sido autorizados.

- Determinar que la documentación de sistemas y programas sólo esté a disposición de los empleados autorizados.

- Probar los registros y autorizaciones de entregas y devoluciones de cintas y archivos de discos hacia y desde la biblioteca.

- Obtener listados de las terminales y considerar su seguridad física.

- Analizar los procedimientos de seguridad en turnos nocturnos y de fin de semana con los operadores y personal de seguridad.

La guía de planeación estratégica además tiene un cuestionario complementario que el auditor debe aplicar por cada centro de procesamiento (véase anexo 1, p. A25). El cuestionario comprende:

- Una columna de atributos que el auditor debe evaluar haciendo referencia a tres riesgos asociados de la tabla de controles generales: 5. Estructura organizativa y procedimientos de operación del área de Informática, 6. Procedimientos para cambios a programas y 7. Acceso general a los datos o programas de aplicación,

- Una columna de evaluación inicial en donde debe explicar los resultados obtenidos, y

- Una columna para hacer referencia a la tabla de factores de riesgo inherente y de control en caso que haya determinado la ausencia de controles.

Una vez realizados todos los pasos hasta aquí descritos, el auditor debe realizar el resumen de información de la planeación estratégica englobando:

* Las tareas a desarrollar, la estimación del tiempo para su realización y fecha para su inicio (véase anexo 1, p. A2).

* Enfoque de auditoría esperado para los componentes individuales considerados como significativos y el tipo de prueba que se les debe aplicar a partir de su evaluación con la tabla de decisión (véase anexo 1, p. A3).

  Esta tabla contempla dos tipos de pruebas: procedimientos y saldos que se explicarán en el punto 2.2.2 y 2.2.3, respectivamente y ayuda al auditor a decidir si debe aplicar la primera en caso de que el riesgo inherente sea alto y el riesgo de control bajo o la segunda si ambos son altos.

* Aspectos más importantes relativos a: Ambiente de los sistemas de información, ambiente de control,

factores de riesgo inherente y de control, otros temas que sean considerados como relevantes por el auditor y oportunidad de servicio al cliente.

Para la identificación de factores de riesgo inherente y de control, el auditor debe resumir en una tabla la función donde se detectó ausencia de control, las áreas afectadas, lo que provoca o provocaría, es decir, los riesgos derivados, el tipo de riesgo, el tratamiento que se le debe dar en la auditoría y la referencia del cuestionario complementario (véase anexo 1, p. A7).

* Estructura organizativa.

El auditor debe ordenar la guía de la planeación estratégica de manera que este resumen quede en la parte superior, en medio el detalle y hasta abajo la evidencia.

Si la organización ha sido auditada con anterioridad, el auditor debe indagar si han ocurrido cambios significativos en los controles clave a través de la actualización de la guía de planeación estratégica determinando si no afectan la confianza que se había depositado en los mismos.

El encargado de la auditoría debe hacer una evaluación después

de finalizar la planeación estratégica para poder decidir:

* Si confía en los controles internos.

* Qué controles son críticos para la auditoría.

* Cómo deben ser probados los controles para su cumplimiento.

* Qué extensión de las pruebas de procedimiento y saldos se necesita.

* Si el sistema ha salvaguardado satisfactoriamente sus activos determinando si pueden ser dañados o utilizados para propósitos no autorizados, si ha mantenido la integridad de los datos y logrado los objetivos organizacionales de manera efectiva y consume recursos eficientemente.

2.1.3 Alcance de auditoría a través de la elaboración de un plan de trabajo.

El encargado debe presentar al Gerente los resultados obtenidos en la guía de planeación estratégica para que conozca el grado de confianza depositado en los controles generales existentes,

verifique si entre los componentes que se han de probar y evaluar se encuentran los requeridos por la Alta Gerencia o se detectaron nuevos y defina así el alcance de la auditoría a través de la elaboración de un plan de trabajo en donde considere la disponibilidad del personal de la organización que se está auditando, los recursos humanos, económicos y materiales que se van a requerir para llevarla a cabo y las actividades ya realizadas en la planeación estratégica.

Dentro de los recursos humanos debe contemplar cuántas personas integrarán el equipo de auditoría y el grado de especialización requerido.

En cuanto a lo económico, debe elaborar un presupuesto para la auditoría dependiendo de la especialización de sus miembros, del tiempo necesario y de las pruebas que se utilizarán para su realización.

Como recursos materiales debe determinar el hardware, software y artículos de oficina necesarios que faciliten la ejecución de la auditoría.

Para la elaboración del plan de trabajo, el gerente debe utilizar una herramienta como la gráfica de Gantt para mostrar las actividades, el tiempo y los responsables de la auditoría. Esta gráfica debe servirle al grupo de auditoría para comparar

el progreso real con lo estimado en ella a medida que avance la auditoría y para firmar las actividades a medida que sean ejecutadas a fin de proveer un rastro de responsabilidad y realización.

Finalmente, el gerente debe presentar el plan de trabajo y el presupuesto a la Alta Gerencia para su revisión y discusión haciendo mención, si es el caso, de los componentes críticos que se hayan detectado con ausencia de control diferentes al o los definidos por ésta al inicio de la auditoría. Adicionalmente debe destacar que las pruebas de saldos son más costosas que las de procedimientos por la especialización del personal, el equipo necesario y el nivel de detalle requerido para efectuarlas.

La Alta Gerencia debe decidir si se auditan dichos componentes y se aplican las pruebas sugeridas o en su caso hacer los ajustes necesarios de acuerdo a lo pactado por ambas partes.

2.2 Evaluación de los componentes para la determinación de la confiabilidad de sus controles.

A partir de esta etapa las actividades deben estar en función a lo especificado en el plan de trabajo.

Resulta de suma importancia que el encargado de la auditoría y su equipo tengan claros los procedimientos a aplicar para así poder alcanzar el objetivo de la misma.

En esta etapa, el encargado debe dividir al equipo de auditoría en grupos de trabajo y asignarles tareas específicas sobre cada componente en los que se encontraron controles deficientes al aplicar la guía de planeación estratégica. De este modo, cada grupo de trabajo debe aplicar pruebas específicas sobre su componente, evaluar los resultados obtenidos en las mismas y emitir sus conclusiones sobre la confiabilidad de los controles.

2.2.1 Presentación del grupo de auditoría al área o áreas que se van a evaluar.

Antes de iniciar la aplicación de las pruebas, es necesario que la Alta Gerencia informe a los responsables de las áreas a ser auditadas de la presencia del grupo de auditoría, el objetivo y el tiempo que se estima para la revisión con el objeto de que éstos lo expliquen a su personal y le brinden todo el apoyo requerido.

El grupo de auditoría debe anticiparse y contactar con la gente responsable del área a ser auditada para requerirle la

información necesaria y la preparación de un ambiente de prueba, según sea el caso, con objeto de agilizar su trabajo y no afectar las actividades normales de la organización.

Cuando el equipo de auditoría se presenta en la fecha acordada para iniciar la revisión, cada grupo de trabajo debe dirigirse con el responsable del área que va a auditar para ser presentado con el personal.

2.2.2 Aplicación de las pruebas de procedimientos a las personas clave.

El grupo de auditoría debe contar con pruebas de procedimientos, es decir, con cuestionarios desarrollados por personas especializadas para cada uno de los componentes específicos del área de Informática (véase anexo 2 p. B3). Estas pruebas deben determinar si los controles se aplican tal como se describe en la documentación de la organización o según lo describe su personal y también si los controles se aplican de manera que cumplen con las políticas y procedimientos de la gerencia.

Una vez identificadas las personas clave, el grupo de auditoría debe aplicar la o las pruebas de procedimientos, con el fin de hacer una evaluación más detallada sobre el componente en el

cual se identificó la ausencia de controles generales y los riesgos a que se expone la organización por prescindir de ellos.

Al estar aplicando la prueba de procedimientos, el grupo de auditoría debe cerciorarse de que la información que está obteniendo a través de la entrevista es veraz. Para ello, debe solicitar se le proporcione la documentación que respalde lo comentado, validar los controles mediante la interacción con el sistema en un ambiente de prueba y/o en un ambiente real u observar directamente los procedimientos.

Para validar los controles mediante la interacción con el sistema en un ambiente de prueba y/o en un ambiente real el auditor debe utilizar las técnicas de transacciones de pruebas las cuales prueban el software para obtener satisfacción de que los controles de procesamiento y funciones de procesamiento computarizadas operan correctamente mediante el ingreso de datos de prueba. Los resultados obtenidos del procesamiento son luego comparados con resultados predeterminados.

El auditor debe revisar:

* El ingreso de transacciones significativas: cantidades, precios y montos de las facturas de proveedores.
* La aprobación de transacciones

* Cálculos: sumas y multiplicaciones
* La actualización de archivos: agregar, modificar o eliminar información almacenada en archivos electrónicos.
* Clasificación de información en un orden predeterminado.
* La modificación del formato de datos para permitir su transferencia entre sistemas.
* La impresión de informes o lectura de información por pantalla: transacciones rechazadas, tales como facturas de proveedores cuyas cantidades no coinciden con las de los informes de recepción.

Las principales técnicas que puede utilizar son:

* **Datos de prueba.**

El auditor debe procesar las transacciones de prueba de aplicación de la organización en un modo "no productivo", o sea, en forma separada del procesamiento normal las cuales deben ser registradas en archivos simulados o archivos para copia de datos (o sea, no en archivos vivos). Puede seleccionarse de las transacciones reales, de las que se utilizaron para probar el software de aplicación durante la etapa de desarrollo y aceptación o pueden ser transacciones diseñadas específicamente en base a los requerimientos de la prueba. Una vez finalizado el procesamiento, el auditor debe comparar los resultados reales de la prueba con los resultados

predeterminados para asegurarse de que el programa de producción opera de la manera prevista.

Para su uso, el auditor no requiere de conocimientos técnicos profundos del procesamiento u operación del computador pero sí que se comprenda el diseño del sistema, incluidos los controles de procesamiento y funciones de procesamiento computarizadas.

El uso de esta técnica puede ser la manera más efectiva de que el auditor pruebe la continua efectividad de los controles y funciones cuando ha decidido confiar en ellas.

* **Procedimiento de prueba integrada.**

El auditor procesa las transacciones de prueba a través del sistema en un modo productivo, o sea, utilizando los mismos procedimientos de ingreso y procesamiento de datos que se emplean para las transacciones reales; pero debe tener la precaución de excluir la empresa simulada de la información final de la organización. El procesamiento de la información es integrado cuando los datos ingresados o generados automáticamente, actualizan archivos de datos utilizados en más de una aplicación.

Esta técnica es más efectiva cuando el auditor ha perdido el rastro de auditoría o cuando la complejidad del sistema

dificulta el seguimiento del flujo de transacciones. Su mejor uso es en sistemas que utilizan procedimientos de ingreso de datos en forma interactiva y procesamiento con actualización inmediata para grandes volúmenes de datos. Esta técnica es especialmente útil para que el auditor pruebe controles y funciones de procesamiento computarizadas integradas y complejas.

En caso de emplearla el auditor debe asegurarse de que las transacciones de prueba no ingresan a los registros contables reales o en caso de ingresar son eliminadas. Esto debe tratarlo desde la planeación de auditoría.

* **Pruebas en línea.**

El auditor debe efectuar el ingreso de datos en modo interactivo y actualizar los registros contables son actualizados de manera inmediata. Las pruebas de edición y validación de datos deben evitar la aceptación de transacciones erróneas o no autorizadas. La mayoría de los sistemas que tienen ingreso de datos interactivo están diseñados para rechazar inmediatamente las transacciones inválidas sin dejar evidencia de este rechazo. Por este motivo, puede no existir un rastro visible que le permita al auditor confirmar que sólo hayan sido aceptadas las transacciones válidas. También el riesgo de que las transacciones rechazadas no sean

identificadas, analizadas y corregidas en forma oportuna puede ser mayor. La prueba en línea puede ser el único medio efectivo de que el auditor pruebe los controles de edición y validación.

Cuando el auditor aplica la prueba en línea para probar los controles de edición y validación debe intentar ingresar una transacción que no debería ser aceptada por el sistema para su procesamiento. Luego de efectuar intentos con distintas combinaciones de transacciones válidas y no válidas, puede determinar que las transacciones no válidas son rechazadas por el software y que las válidas son aceptadas.

El auditor debe planear estas pruebas con el personal de la organización responsable antes de llevarlas a cabo. Existe la posibilidad de que el sistema acepte una transacción errónea. Si esto sucede, el auditor debe asegurarse junto con el personal de la organización responsable de que la transacción sea reversada.

Estas pruebas también pueden utilizarse para probar los controles que evitan el acceso no autorizado a través de terminales.

El grupo de trabajo de auditoría a cargo de aplicar las pruebas necesita obtener evidencia de que los controles y las funciones de procesamiento computarizadas probadas con técnicas de

transacciones de prueba han operado en forma efectiva durante el periodo bajo examen y no únicamente en el momento en que las técnicas son aplicadas.

A continuación se muestran los pasos que debe considerar el auditor al estar aplicando la prueba de procedimientos para evaluar el o los aspectos críticos requeridos:

SEGURIDAD

Identificación del ambiente de información

Debe obtener una clara comprensión del ambiente técnico, gerencial y físico del centro de procesamiento de información a través de entrevistas, recorridos físicos, examen de documentos y evaluación de riesgos para identificar, revisar y evaluar los componentes del hardware, los requisitos de buenas políticas de seguridad, controles físicos, lógicos y ambientales y exposiciones a riesgos.

*** Revisión de diagramas de red**

Necesita:

- Evaluar los enlaces para determinar si están vigentes los controles de acceso lógico y físico.

- Inventariar las diversas conexiones de terminales para asegurarse de que el diagrama es exacto.

*** Documentación de la seguridad de acceso**

Debe comprobar la correcta implantación y la correcta seguridad de acceso físico y lógico de cada componente.

Debe ver la secuencia lógica de:

- **Terminales**

  - Debe verificar que esté resguardada físicamente y que utilice un log-on y un password para establecer la sesión.

  - Debe tomar una muestra de las tarjetas y llaves de terminales e intentar lograr acceso más allá del autorizado.

  - Necesita saber si el Administrador de Seguridad hizo un seguimiento de cualquier violación infructuosa que se haya intentado.

  - Puede trabajar con el Gerente de la red para obtener un listado de las direcciones y ubicaciones de las

terminales y realizar un inventario de ellas, investigando las registradas incorrectamente, faltantes o adicionales. También debe seleccionar una muestra de ellas para asegurarse que están identificadas en el diagrama de red.

- **Software de telecomunicaciones**

Debe asegurarse que han sido definidas todas las aplicaciones, que sean adecuados y aprobados por la gerencia los diversos controles optativos de telecomunicaciones y las funciones de procesamiento utilizadas.

- **Software de procesamiento de transacciones**

Debe asegurarse de la correcta identificación del usuario y la autorización del mismo para poder tener acceso a la aplicación. Debe estar determinado por tablas internas, cuyo acceso debe estar limitado únicamente al Administrador de Seguridad.

- **Software de aplicación**

  - Debe verificar que solamente el coordinador de implantación puede tener acceso a la biblioteca de

software en producción.

- Debe asegurarse de que la lógica del programa cumple con las intenciones de la gerencia.

- **Sistema de administración de bases de datos**

Debe asegurarse de que todos los elementos de datos están identificados en el diccionario de datos y que el acceso a este último está limitado al Administrador de base de datos y todos los elementos de datos están sujetos al control de acceso lógico.

* **Software de control de acceso**

Debe asegurarse de que:

- Todos los componentes estén definidos en el software de control de acceso.

- Las reglas definen quién puede tener acceso sobre qué y restringen las tablas de seguridad a todos salvo al Administrador de Seguridad.

*** Entrevistas al personal de sistemas y redes**

Debe solicitarse al Administrador de Seguridad que identifique las responsabilidades y funciones de su cargo. Si las respuestas que da a esta pregunta respaldan prácticas de control razonables, o no están conforme a la descripción de las tareas escritas, el auditor debe compensarlo expandiendo el alcance de las pruebas de los controles de acceso.

*** Examen de los informes generados por el software de control de acceso**

- Debe hacer una revisión de una muestra de los informes de seguridad para determinar si se está monitoreando el cumplimiento de:
  - Las políticas de seguridad en cuanto a la identificación del usuario,
  - Restricciones de acceso,
  - Registros históricos (log),
  - Accesos e intentos de acceso, y
  - Si se suministra suficiente información para respaldar una investigación.

- Para probar la eficacia y oportunidad de la respuesta del Administrador de seguridad y el dueño de los datos ante

los intentos de violación informados, el auditor debe buscar evidencia de la investigación y seguimiento. Si no se encuentra tal evidencia, debe realizar más entrevistas para determinar por qué existe tal situación.

- Para probar la generación de informes de violaciones de acceso, el auditor debe intentar efectuar transacciones o acceder a datos para los cuales el acceso no está autorizado. Los intentos infructuosos informados deben identificar la hora, la terminal, el log-on y el archivo al cual se intentó acceder. Esta prueba debe coordinarse con el dueño de los datos y el Administrador de Seguridad a fin de evitar violaciones a normas de seguridad.

Examen de las políticas y procedimientos escritos

El auditor debe revisar las políticas y procedimientos para determinar si fijan un nivel de seguridad adecuado y brindan los medios para asignar la responsabilidad para mantener un ambiente de procesamiento computarizado seguro.

*** Políticas de acceso físico**

El auditor debe observar si la organización cuenta con:

1. **Controles físicos** tales como:

- Cerraduras con llave, con combinación, electrónicas o biométricas de puertas.
- Registro histórico manual o electrónico de la entrada.
- Identificaciones con fotografía.
- Cámaras de video.
- Guardia de seguridad.
- Acceso controlado de visitantes.
- Puertas dobles de seguridad.
- No visibilidad o identificación de la ubicación de los centros sensibles.
- Cerrojos en las terminales.
- Punto único de entrada monitoreado por una recepcionista.
- Sistema de alarma.

2. **Controles ambientales** como:

- Detectores de agua.
- Extintores portátiles.
- Alarmas de incendio.
- Detectores de humo.
- Sistemas de supresión de incendios.
- Ubicación estratégica de la sala del computador para reducir riesgos de inundaciones.
- Inspección periódica del departamento de bomberos.

- Paredes, pisos y techos falsos e incombustibles alrededor del centro de cómputo.
- Protectores de picos de tensión.
- Provisión ininterrumpible de energía.
- Llave de desconexión de energía.
- Conexiones a dos líneas de provisión de electricidad.
- Cableado ubicado en páneles y cañerías para electricidad.
- Prohibición de comer, beber y fumar dentro del centro de cómputo.
- Equipo de oficina resistente al fuego.

Debe también revisar que el plan de recuperación y evacuación de emergencia esté totalmente documentado y probado.

*** Políticas de acceso lógico**

El auditor debe evaluar si se tienen contempladas:

1. **La exposición a riesgos** por:

   - Posibles causantes de las violaciones de acceso lógico tales como:

     - Piratas informáticos.
     - Empleados.

- Ex-empleados.
- Terceros interesados o capacitados.
- Legos por accidente que pueden eludir la seguridad.

2. **Las exposiciones de carácter técnico:**

- Manipulación de datos.
- Virus.
- Ataques asincrónicos.
- Fugas de datos.
- Intercepción de líneas.
- Interrupción del servicio.

3. **Las exposiciones a riesgos del negocio:**

- Pérdidas financieras.
- Repercusiones legales.
- Pérdida de credibilidad o margen de competitividad.
- Chantaje o espionaje industrial.
- Divulgación de información confidencial, sensible o embarazosa.
- Sabotaje.

También debe verificar el **nivel adecuado de controles de acceso**

lógico como:

- **IDs y passwords para limitar el acceso**

  - El auditor debe intentar adivinar el password de una muestra de IDs de log-on de empleados. Esto debe hacerlo de manera discreta para evitar perturbar a los empleados.

  - Debe hacer un recorrido en las áreas de trabajo de los usuarios finales y programadores en busca de passwords adheridos a los costados de las terminales y el interior de los cajones.

  - Debe entrevistar a una muestra de usuarios para determinar si se les obliga a cambiar sus passwords luego de un periodo determinado.

  - Debe probar el borrado de passwords inactivos obteniendo un listado de IDs de log-on activos. Por medio de un muestreo, debe relacionar esa lista con los empleados actuales y buscar IDs de log-on asignados a empleados o consultores que ya no trabajan en la empresa.

  - Para probar la sintaxis de los passwords, debe

intentar crearlos con un formato inválido, por ejemplo, muy pequeños o demasiado grandes, repeticiones de passwords anteriores, con una mezcla no correcta de caracteres alfabéticos y numéricos.

- Debe probar la desactivación automática tras un número de intentos infructuosos de acceso. El ID de log-on debe desactivarse luego de que se haya ingresado una cantidad preestablecida de passwords inválidos.

- También debe preocuparse por cómo el Administrador de Seguridad reactiva el ID de log-on. Si por una simple llamada telefónica sin verificación de la identificación conlleva la reactivación, entonces la función no está controlada correctamente.

- Para probar el enmascaramiento de los passwords en las terminales, debe hacer un log-on en una terminal y observar si exhibe el password cuando se le ingresa.

- **Encriptamiento**

  - Para probarlo, el auditor debe trabajar con el Administrador de Seguridad para intentar ver la tabla

de passwords. Si es posible hacerlo, su contenido debe ser ilegible.

- **Desconexión automática de terminales**

  - El auditor debe hacer un log-on en una cantidad de terminales y no ingresar más transacciones. Luego simplemente esperar que las terminales se desconecten tras el intervalo establecido. Antes de comenzar esta prueba, debe verificar con el Administrador de Seguridad que la función de desconexión automática vale para todas las terminales.

- **Procedimientos de devolución de llamada**

  - Para probar la autorización de la llamada, el auditor debe llamar al computador desde un número de líneas telefónicas autorizadas y no autorizadas. Si los controles son adecuados, la conexión exitosa sólo puede realizarse únicamente desde los números autorizados.

  - También debe probar los controles lógicos que se invocan luego de lograr la conexión autorizada con el computador utilizando conexiones de comunicación directa para intentar lograr accesar a archivos no

autorizados. Esta prueba debe coordinarse con el Administrador de Seguridad a fin de evitar violaciones a las normas de seguridad.

- **Autorización de cambios a la red**

  - El auditor puede probar su control de cambios:

    - Realizando un muestreo de solicitudes de cambios recientes, buscando la autorización apropiada y relacionando la solicitud con el dispositivo de red real, y

    - Relacionando cambios recientes a la red con solicitudes de cambio autorizadas.

Un control adicional que el auditor debe determinar es quién tiene acceso al software para cambio de la red. Este acceso debe estar restringido a la Gerencia del Departamento de Comunicaciones.

- **Controles de recursos de producción**

  - El auditor debe trabajar junto con el Analista de Software de Sistemas y el Gerente de Operaciones para determinar los recursos de producción sensitivos.

- Al trabajar con el Administrador de Seguridad, el auditor debe determinar quién puede tener acceso a los recursos y qué puede hacerse con ese acceso.

*** Percepción de la seguridad y entrenamiento formales**

El auditor debe realizar entrevistas a los empleados para determinar su percepción global sobre las razones de las diversas medidas de seguridad y las repercusiones de violarlas.

*** Usuario y dueño de los datos**

- El auditor debe utilizar la información sobre asignación de responsabilidades para determinar que se ha asignado la propiedad de los datos en forma correcta.

- Asimismo, debe entrevistar a los dueños de datos, responsables de datos y Administrador de Seguridad para determinar si perciben su responsabilidad por la propiedad de ellos.

- Verificar que los dueños de datos tienen la responsabilidad de autorizar el acceso, asegurarse de que se actualizan las reglas de acceso para los datos cuando se presentan cambios en el personal y que en

forma periódica hacen un inventario de ellas y garantizan un correcto mantenimiento de la seguridad. Los responsables de datos deben almacenar y salvaguardar los datos.

*** Autorizaciones documentadas**

- El auditor debe hacer un examen de una muestra de documentos de autorización de acceso para verificar que está identificado y que se suministra un correcto nivel de autoridad por escrito.

- Debe además obtener un informe de las reglas de acceso al computador y realizar una muestra para:

  - Determinar si el acceso se hace porque realmente se necesita.

  - Intentar relacionar la muestra de esas reglas con los documentos de autorización.

Si no se encuentran autorizaciones escritas, ello indica una ruptura de controles y ello puede implicar una necesidad de mayores exámenes para determinar las exposiciones a riesgos y sus consecuencias.

*** Descripción de tareas del Administrador de Seguridad**

- El auditor debe revisar la descripción para asegurarse de que el área o la responsabilidad del Administrador de Seguridad protege los bienes de la empresa pero le restringe la autoridad para hacer decisiones unilaterales respecto de los controles y políticas de acceso de seguridad.

- El auditor debe verificar que estén correctamente definidas las funciones en el controlador de comunicaciones a fin de que se establezca adecuadamente el procesamiento de transmisión de mensajes, la recuperación de errores y la seguridad de transmisión.

- También debe verificar que el software que se utiliza para realizar cambios sobre esas funciones sólo esté disponible para el Administrador de la Red.

CENTROS DE COMPUTO

Revisión de documentación

*** Plan estratégico de la empresa y del procesamiento de información**

Los procedimientos de auditoría deben incluir una revisión del plan estratégico para determinar si se han establecido y seguido las diversas categorías de gastos del departamento tales como hardware, mantenimiento del computador, adquisición y mantenimiento de software, por mencionar algunos.

*** Organigrama**

- El auditor debe incluir la obtención del organigrama para lograr una mejor comprensión de cuál es la responsabilidad de cada una de las áreas y para determinar si cada centro de responsabilidad tiene el personal adecuado para satisfacer los requerimientos de servicio y de recursos de los usuarios finales.

- Además debe revisar las responsabilidades individuales a fin de asegurarse de una adecuada segregación de funciones.

*** Políticas y procedimientos de operaciones**

El auditor debe revisar las políticas y procedimientos de operaciones para asegurarse de que han sido establecidos correctamente por la gerencia del centro de cómputo y que los usuarios finales y el personal de operaciones del computador los cumplen de acuerdo con la intención y autorización de la

gerencia.

*** Observación del personal realizando sus tareas**

El auditor debe observar al personal del centro de cómputo cuando realiza sus tareas para determinar si los controles están implantados para asegurar:

- La eficiencia de las operaciones.
- El cumplimiento de las normas y políticas establecidas.
- Una supervisión adecuada y revisión de la gerencia del área de Informática.
- La seguridad de los datos.

Observación y prueba de diversas funciones de operaciones

*** Operación del computador**

El auditor debe revisar los manuales del operador para determinar si las instrucciones son adecuadas respecto de:

- La operación del computador y su equipo periférico.
- Los procedimientos de encendido y apagado.
- Las acciones que han de cumplirse en caso de falla de hardware y software.

- Los registros que deben conservarse.
- Las tareas de trabajos rutinarios y actividades restringidas.

En suma, el auditor debe realizar pruebas para determinar si los procedimientos coinciden con la intención y autorización de la gerencia.

*** Capacidad de acceso del bibliotecario**

El auditor debe verificar:

- Que se restrinja el acceso del encargado de la biblioteca al hardware del computador.
- Que su acceso esté sólo limitado al sistema de administración de cintas.
- Que el acceso a las instalaciones de la biblioteca esté limitado sólo al personal autorizado.
- Que la eliminación de datos esté restringida a la planeación de producción.
- Que se lleve adecuadamente un registro del ingreso y salida de datos.

*** Contenido y ubicación de los archivos fuera de línea**

Verificar que los medios de almacenamiento de archivos fuera de línea conteniendo programas y datos del sistema en producción tienen claramente marcado su contenido.

*** Instalaciones de la biblioteca**

- El auditor debe verificar que las instalaciones de la biblioteca estén alejadas del centro de cómputo.

- También debe revisar las políticas y procedimientos de:

  - Administración de la biblioteca.

  - Chequeo del ingreso y egreso de cintas incluyendo las autorizaciones firmadas.

  - Identificación, etiquetado, entrega y recuperación de archivos de respaldo de otras sedes.

  - Sistema de inventario para las cintas en esa y otras sedes incluyendo ubicaciones específicas de almacenamiento para cada cinta.

  - Eliminación y borrado de archivos de cintas,

incluyendo autorizaciones firmadas.

*** Procedimiento de manejo de archivos**

- El auditor debe revisar los procedimientos establecidos para controlar la recepción de archivos y medios magnéticos de almacenamiento secundario de y a otras sedes para determinar si son adecuados y coinciden con la intención y autorización de la gerencia.

- También debe realizar pruebas para determinar si esos procedimientos han sido seguidos.

*** Control de ingreso de datos**

El auditor debe revisar los controles y procedimientos para determinar si:

- El personal del centro de cómputo cumple las políticas establecidas.

- Se tiene una adecuada segregación de tareas.

- Se producen, llevan y revisan los informes de control.

- Los informes de control son exactos y completos.

- Los formularios de autorización son completos y contienen las firmas correspondientes.

Revisión de informes de las actividades de operaciones y de seguimiento de la gerencia del área de Informática

*** Informe de administración de problemas**

- El auditor debe asegurarse de que se han desarrollado procedimientos adecuados para guiar al personal de operaciones del centro de cómputo en cuanto a documentación, análisis y resolución de problemas en forma oportuna de acuerdo con la intención y autorización de la gerencia.

- El auditor debe realizar procedimientos para asegurarse de que se mantiene de manera adecuada el mecanismo de administración de problemas y que los errores pendientes de resolución se tratan adecuadamente y son resueltos. Estos procedimientos deben incluir:

  - Entrevista al personal de operaciones del centro de cómputo.

  - Una revisión de los procedimientos para restringir, evaluar y resolver cualquier problema operativo o de

procesamiento utilizados en el centro de cómputo para determinar si son adecuados para el análisis de servicios.

- Una revisión de los registros de actuación para determinar si existen problemas durante el procesamiento.

- Una revisión de las razones de las demoras en el procesamiento de programas de aplicación para determinar si son válidas.

- Una revisión de los procedimientos utilizados en el centro de cómputo para recopilar estadísticas respecto del rendimiento del procesamiento en línea para determinar si el análisis es exacto y completo.

- Determinar si el centro de cómputo ha establecido procedimientos para manejar problemas de procesamiento de datos.

- Determinar si todos los problemas identificados a o por operaciones del centro de cómputo se registran para su verificación y solución.

- Determinar si se han identificado problemas

significativos y recurrentes y se han tomado acciones para evitar su repetición.

- Determinar si los problemas de procesamiento se resolvieron en forma oportuna y la solución fue completa y razonable.

- Revisión de los informes de administración del área de Informática generados por el sistema de administración de problemas para asegurarse de obtener evidencia de una adecuada revisión gerencial.

- Revisión de entradas al registro histórico de errores pendientes de solución que describen problemas a ser resueltos para obtener una adecuada documentación y asegurarse de que son tratados en forma oportuna.

- Revisión de la documentación de operaciones para asegurarse que se han desarrollado procedimientos para la asignación de los problemas no resueltos a una instancia superior de la gerencia del área de Informática.

*** Informe de utilización y disponibilidad de hardware**

El auditor debe llevar a cabo una:

- Revisión del plan de monitoreo del rendimiento del hardware y comparación con el registro histórico de problemas, registros de procesamiento, informes del sistema de contabilización de jobs, planes e informes de mantenimiento preventivo para determinar la validez del proceso.

- Revisión del registro histórico de problemas para determinar si los problemas de funcionamiento del hardware, repeticiones de corridas, el uso de utilerías de software, terminaciones anormales de sistemas y las acciones del operador han sido revisadas por la gerencia del área de Informatica para asegurar su validez.

- Revisión del plan de mantenimiento preventivo para:

  - Determinar si se realiza con la frecuencia recomendada por los respectivos proveedores de hardware.

  - Verificar que no se realiza durante periodos pico de trabajo, evitando así la disminución de la disponibilidad del hardware.

  - Determinar que no se realiza cuando se están procesando aplicaciones de naturaleza crítica o

sensitiva.

- Revisión de los informes de disponibilidad y utilización del hardware para determinar que la asignación de trabajos es adecuada para satisfacer los planes de carga de trabajo y los requerimientos de los usuarios.

- Revisión del plan de carga de trabajo y los informes de disponibilidad y utilización del hardware para determinar que la asignación de trabajos tiene la flexibilidad necesaria para dar tiempo al mantenimiento preventivo de hardware necesario.

- Determinación de si los recursos del centro de cómputo están prontamente disponibles para procesar aquellos programas de aplicación que exigen un alto nivel de disponibilidad de recursos.

*** Asignación de trabajos**

El auditor debe:

- Obtener una lista de aplicaciones que se planifiquen en forma regular y la información relacionada tal como fechas límites para la entrada, tiempo de preparación de los datos, tiempo estimado de procesamiento y fechas límites

para la respectiva salida a fin de determinar si se han incluido en los acuerdos del servicio.

- Revisar el registro histórico de consola a fin de determinar si los trabajos planificados fueron completados de acuerdo con el plan. Si el procesamiento se realiza de manera diferente del planeado, analizar las razones para comprobar que sean válidas.

- Revisar el plan para determinar si se han determinado las prioridades de procesamiento para cada aplicación.

- Determinar si la asignación de trabajos de urgencias y repeticiones de corridas son congruentes con la prioridad que tienen asignada.

- Determinar si se han identificado las aplicaciones de alta prioridad para en caso de falta de planes de producción sean procesadas primero.

- Determinar si los procedimientos de asignación de trabajos utilizados facilitan el uso óptimo de los recursos del computador a la vez que satisfacen los requerimientos del servicio.

- Determinar si el personal asignado a cada turno es

adecuado para poder soportar la carga de trabajo.

CONTINUIDAD DE LAS OPERACIONES

*** Evaluación del almacenamiento en un centro alternativo**

- El auditor debe evaluar la instalación de almacenamiento en un centro alternativo para asegurarse de la presencia, sincronización, actualización y transferencia de los medios magnéticos críticos así como de su documentación. Ello incluirá:

  - o Archivos de datos,
  - o Software y documentación de aplicaciones,
  - o Software y documentación de sistemas,
  - o Documentación de operaciones,
  - o Insumos necesarios,
  - o Formularios especiales, y
  - o Una copia del plan de contingencias.

- El auditor debe realizar un examen detallado de inventario.

  Ese inventario debe incluir poner a prueba:

  - o Los nombres correctos del conjunto de datos,

- Los números de serie de volumen,
- Los periodos contabilizados,
- La ubicación de los depósitos de las cintas, y
- Una revisión de la documentación.

y además debe verificar que se corresponda con documentación de producción actual.

*** Revisión de la cobertura de seguros**

El auditor debe revisar la adecuación de la cobertura de seguros para daños a medios magnéticos, interrupción del negocio, reemplazo del equipo y procesamiento de contingencia. A fin de determinar la adecuación, debe obtener una copia de la o las pólizas de seguro de la empresa y evaluar la adecuación de la cobertura.

*** Conocimiento de los procedimientos de recuperación por parte del personal**

El auditor debe entrevistar al personal clave que se necesita para la recuperación con éxito de las operaciones de la organización. Todo el personal clave debe tener una comprensión de las responsabilidades asignadas, así como documentación detallada y actualizada que describa sus tareas.

*** Seguridad física en la instalación en un centro alternativo**

El auditor debe evaluar la seguridad física en el centro alternativo para asegurarse de que tienen controles correctos de acceso y ambientales.

*** Examen del contrato de procesamiento alternativo**

- El auditor debe obtener una copia del contrato con el proveedor de la instalación de procesamiento alternativo y revisarlo asegurándose de lo siguiente:

  - Que sea un proveedor confiable y ponga por escrito todo lo que promete.

  - Que el contrato esté redactado claramente y sea comprensible para un juez.

  - Que la cobertura de seguro se vincula y cubre todo o la mayoría de los gastos del desastre.

  - Que pueden realizarse pruebas en el hot-site a intervalos regulares.

- Debe asegurarse además de que un abogado especializado revise los contratos exigibles de depósito del código

fuente en manos de un tercero.

- Debe determinar hasta qué punto se puede exigir el cumplimiento por otro en caso de incumplimiento contractual.

- Debe prestar atención a los requerimientos de comunicaciones para el centro de respaldo.

*** Revisión del plan de contingencias**

- El auditor debe verificar que son evidentes los elementos de un plan bien desarrollado. Debe realizarse un verificación específica de la información contenida dentro del plan.

- Debe obtener una copia del plan de recuperación en caso de desastres, compararla contra las copias distribuidas a fin de verificar que están actualizadas y evaluar la eficacia de los procedimientos documentados para iniciar el esfuerzo de recuperación en caso de desastre.

- Debe verificar si el plan incluye la identificación y soporte de todas las aplicaciones críticas incluyendo sistemas basados en PCs o desarrollados por usuarios finales.

- Para revisar la integridad de la lista de personal de recuperación en caso de desastre debe tomar una muestra de personas y verificar que los números telefónicos y su domicilio son correctos. Además debe verificar los contactos de emergencia con el hot-site y con proveedores.

- Debe evaluar el procedimiento de actualización y distribución del manual, así como verificar los responsables de mantenerlo documentado.

- Debe determinar si todos los equipos de recuperación tienen procedimientos escritos a seguir en caso de un desastre, si los procedimientos de recuperación del usuario están documentados y si se contempla la reubicación en una nueva instalación de procesamiento de información en el caso de que no pueda restaurarse el centro original.

- Debe verificar si el plan contempla la carga de datos procesados manualmente al sistema automatizado.

*** Evaluar los resultados de pruebas previas**

El auditor debe revisar los resultados de pruebas del plan de contingencias previos para determinar si las acciones que

requerían corrección han sido incorporadas al plan, determinar si han sido apropiadas y evaluarlas para verificar que se han completado sus objetivos en forma total y exacta.

SISTEMA OPERATIVO Y UTILITARIOS

*** Entrevistar al servicio técnico y otro personal**

El auditor debe:

- Revisar y aprobar el proceso de selección.
- Probar los procedimientos para la implementación de software.
- Revisar y aprobar los procedimientos de los resultados de las pruebas, los procedimientos de implementación y los requerimientos de documentación.

*** Revisar el estudio de factibilidad y el proceso de selección para determinar lo siguiente:**

- Que sean consistentes los objetivos y propósitos del sistema con las peticiones propuestas,
- Se aplica el mismo criterio de selección a todas las

propuestas, y

- Los resultados de la pruebas son consistentes y válidas.

*** Revisar la documentación de los sistemas específicamente en aspectos como:**

- Establecimientos de control en la instalación,
- Tablas de parámetros,
- Definiciones de salida, y
- Reportes de actividad de logs.

*** Revisar y probar la implementación del software de sistemas para determinar la adecuación de controles en:**

- Procedimientos de cambios,
- Procedimientos de autorización,
- Funciones de seguridad de acceso,
- Requerimientos de documentación,
- Documentación de las pruebas de los sistemas,
- Pistas de auditoría, y
- Controles de acceso sobre el software en producción.

*** Revisar la documentación de autorización para determinar si:**

- Se ha documentado cómo agregar, borrar o cambiar las autorizaciones de acceso, y

- Se han documentado los reportes de intentos de violaciones y el seguimiento que ha de darse.

*** Revisar el plan de adquisición de hardware para:**

- Determinar si se compara el plan de adquisición de hardware de manera regular con el plan de la Alta Gerencia,

- Determinar si el medio ambiente es adecuado para el hardware instalado y para el nuevo según el plan aprobado de adquisición,

- Comparar el plan de adquisición de hardware de la Alta Gerencia con los planes del centro de cómputo para identificar cualquier deficiencia en el primero,

- Determinar si el plan de adquisición de hardware de la gerencia ha considerado la obsolescencia tecnológica del equipo instalado y la adquisición del equipo nuevo, y

- Verificar que sea adecuada la documentación de las especificaciones de hardware y software, requerimientos de

instalación y el tiempo probable asociado con la adquisición planeada.

* **Revisar los procedimientos de administración de la capacidad del hardware y de la evaluación de actuación del mismo para determinar:**

- Si esto asegura la revisión continua de la capacidad y actuación del hardware, y

- Si los criterios usados por la Alta Gerencia en el plan para el monitoreo de la actuación del hardware se basan en datos históricos obtenidos de registros de problemas, horarios de proceso, reportes de sistema de contabilización de jobs, reportes y horarios de mantenimiento preventivo.

* **Revisar los controles de administración de cambios para lo siguiente:**

- Determinar si el responsable de fijar el tiempo fue avisado de manera oportuna respecto de los cambios al software de sistemas, al software de aplicación y a la configuración del hardware.

- Verificar que la Alta Gerencia ha desarrollado y forzado

los horarios de cambios que permitan la asignación del tiempo para la instalación y pruebas adecuadas del nuevo hardware y software.

- Verificar que la documentación del operador usada en el centro de cómputo se revisa apropiadamente antes de la implementación de cambios en hardware y software.

- Seleccionar una muestra de cambios de hardware y software que han afectado el tiempo programado del proceso y determinar si los planes para cambios se están aplicando de manera oportuna.

- Cerciorarse que todos los cambios de hardware y software han sido comunicados a los programadores de sistemas y de aplicación y al personal de centro de cómputo para asegurarse que los cambios y pruebas son coordinados apropiadamente.

- Evaluar la efectividad de los cambios para asegurarse que no interfieren con el proceso de programas de aplicación normal.

*** Revisar los controles del sistema de administración de las bibliotecas de los medios magnéticos para lo siguiente:**

- Determinar si los encargados de las bibliotecas de medios magnéticos verifican periódicamente la exactitud de la información creada y mantenida por el sistema automatizado de administración de bibliotecas de medios magnéticos,

- Verificar que el inventario de la biblioteca especifica el número del medio magnético, el tiempo de retención, la custodia actual y la ubicación física,

- Seleccionar una muestra de los medios magnéticos inventariados (cinta/disco/cartucho) y verificar que tengan una identificación de etiquetas internas,

- Verificar que las etiquetas internas contienen:

  - El nombre del archivo,
  - La fecha de creación,
  - El número del programa creado,
  - El tiempo de retención para el medio magnético, y
  - El número de registros o bloques contenidos en él,

- Verificar que los procedimientos para restringir el uso del software de control de las etiquetas internas son razonables y eficaces,

- Verificar que se estén cumpliendo los procedimientos de

mantenimiento para el ciclo de limpieza, y

- Verificar que se han establecido y se están cumpliendo los estándares para la actuación y retiro de los medios magnéticos individuales.

* **Revisar los procedimientos de selección del software de sistemas para determinar que:**

- Tratan los planes de largo plazo y de negocios de sistemas,
- Incluyen requerimientos de procesamiento y control,
- Incluyen un resumen de las capacidades del software y opciones de control, y
- Satisfacen los requerimientos del centro de cómputo.

* **Revisar el análisis de costo-beneficio de los procedimientos del software de sistemas para determinar que han sido considerados los siguientes aspectos:**

- Los costos financieros directos asociados con el producto,
- El costo del mantenimiento del producto,
- Los requerimientos y capacidad de hardware,

- Requerimientos de entrenamiento y soporte técnico,
- El impacto del producto sobre la confiabilidad del proceso,
- El impacto sobre la seguridad de los datos, y
- La estabilidad financiera de las operaciones del proveedor.

*** Revisar la instalación de los controles de los cambios del software de sistemas para determinar que:**

- Se estableció un plan por escrito para los cambios de prueba del software de sistemas,
- Se están completando y planeando las pruebas,
- Se resolvieron los problemas encontrados durante la prueba y se volvieron a probar los cambios,
- Los procedimientos de prueba son adecuados para brindar una seguridad razonable de que los problemas en los cambios al software de sistemas serán identificados antes que sean implantados en el ambiente de producción, y
- El programa de tiempo para los cambios del software de sistemas considera el más mínimo impacto para el proceso del centro de cómputo.

* **Revisar las actividades de mantenimiento del software de sistemas para determinar que:**

- Están documentados todos los cambios hechos al software de sistemas, y

- Todas las versiones actuales del software están soportadas por el proveedor.

* **Revisar los controles de cambios al software de sistemas para determinar que:**

- El acceso a las bibliotecas que contienen el software de sistemas está limitado solamente a personas autorizadas,

- Los cambios al software son documentados y probados de manera adecuada antes de la implementación, y

- El software debe estar autorizado de manera apropiada antes de trasladarlo del ambiente de prueba al ambiente de producción.

* **Revisar la seguridad del software de sistemas para lo siguiente:**

- Se han establecido los procedimientos para restringir las

posibilidades de eludir el acceso de seguridad lógica provisto por el software de sistemas,

- Se han establecido procedimientos que limiten el acceso a las facilidades de interrupción del sistema,

- Son adecuadas las medidas de seguridad lógica y física existentes para restringir el acceso a las consolas maestras, y

- Fueron cambiados los passwords suministrados por el proveedor del software de sistemas cuando se instaló.

* **Revisar los controles de acceso y la administración de los passwords para determinar lo siguiente:**

- Existen procedimientos para agregar personas a la lista de los autorizados a tener acceso a los recursos de cómputo, cambiar sus facilidades de acceso y borrarlos de la lista,

- Existen procedimientos para asegurar que los passwords individuales no son revelados inadvertidamente,

- Los passwords son de una longitud adecuada, no pueden adivinarse fácilmente, y no contienen caracteres repetidos,

- Los passwords se cambian periódicamente,

- Las organizaciones usuarias periódicamente validan las facilidades de acceso que se proveen actualmente a los miembros de sus departamentos,

- Los procedimientos proveen la suspensión de los códigos de identificación del usuario o la desactivación de la terminal, microcomputadora, o actividad del dispositivo de entrada de datos después de una cantidad determinada de violaciones de procedimientos de seguridad, y

- La identificación física del centro de cómputo es discreta y limitada.

*** Revisar los controles de los sistemas de información soportados por las bases de datos para determinar lo siguiente:**

- Controles sobre el acceso a datos compartidos,

- Controles sobre la organización de los datos,

- Controles sobre datos compartidos,

- Se utilizan procedimientos de control de cambios adecuados

para asegurar la integridad del software de administración de las bases de datos,

- Se mantiene la integridad del diccionario de datos del software de administración de las bases de datos,

- El software de administración de las bases de datos reduce al mínimo la redundancia de datos, cuando existen datos redundantes se mantienen referencias cruzadas adecuadas dentro del diccionario de datos del sistema u otra documentación, y

- Se provee el acceso a personas autorizadas a datos específicos con una base de datos particular,

* **Revisar los controles de las operaciones de la red para determinar lo siguiente:**

- Se desarrollaron planes de implementación, conversión y pruebas de aceptación apropiados para la red,

- Se establecieron planes de implementación y pruebas para los enlaces de comunicaciones y el hardware de la red,

- Existen provisiones de operación para la red de procesamiento de datos distribuido para determinar la

consistencia con las leyes y regulaciones gubernamentales de transmisión de datos,

- Se han establecido mecanismos para asegurar el manejo de los datos entre las aplicaciones a medida que la red crece en tamaño y complejidad,

- Se aplican los procedimientos para asegurarse de que se maneja correctamente la compatibilidad de datos de la red y que puede ejercerse en forma oportuna,

- Se han identificado todos los datos sensibles y se han determinado los requerimientos para su seguridad,

- Se establecieron procedimientos para asegurar los controles eficaces sobre el hardware y software usado por los departamentos servidos por la red,

- Se han instalado los mecanismos adecuados de reinicio y recuperación para cada localidad de usuario servida por la red,

- La red se ha diseñado de manera que asegure que una falla en el servicio en algún departamento va a tener un efecto mínimo sobre la continuidad del servicio de otros sitios servidos por la red,

- Todos los cambios que se hacen en los nodos de usuario o por la gerencia al software de sistema operativo usado para la red están controlados y pueden ser detectados rápidamente por el administrador de la misma o por el responsable,

- Las personas tienen acceso sólo a aplicaciones, procesadores de transacciones y conjuntos de datos autorizados,

- Todos los usuarios de la red tienen prohibido ingresar comandos desde una terminal y ejecutarlos en otra,

- Los comandos del sistema que afectan más de un nodo de la red están restringidos a una terminal y sólo una persona autorizada con la responsabilidad del control total de ella puede ejecutarlos,

- El encriptamiento se utiliza en la red para datos sensibles, y

- Se ha aplicado la protección de seguridad apropiada:

  - **Altamente distribuida**
    La seguridad está bajo el control de la gerencia usuaria.

- **Distribuida**

  La seguridad está bajo la dirección de la gerencia usuaria, pero se rige por las directivas establecidas por la gerencia de Informática.

- **Mixta**

  La seguridad está bajo la dirección de la gerencia usuaria, pero toda la responsabilidad recae en la gerencia de Informática.

- **Centralizada**

  La seguridad está bajo la dirección de la gerencia de Informática, pero ésta tiene una relación muy estrecha con la gerencia usuaria.

- **Altamente centralizada**

  La seguridad está bajo el control absoluto de la gerencia de Informática.

* **Revisar los controles de las LAN para determinar lo siguiente:**

- Los estándares están de acuerdo a la arquitectura de la red, y

- Los procedimientos están de acuerdo al diseño, selección

y costo-beneficio de la arquitectura de la red de área local.

CICLO DE VIDA DEL DESARROLLO DE SISTEMAS (CVDS)

Es recomendable que el auditor participe como consultor en las fases de CVDS.

*** Revisar el proceso de CVDS**

- El auditor debe obtener la documentación disponible necesaria de las diferentes fases así como asistir a las juntas del equipo de proyectos ofreciendo asesoramiento a lo largo del proceso de desarrollo de sistemas.

- El auditor también debe analizar los riesgos asociados y exposiciones inherentes en cada fase asegurando que los mecanismos de control adecuados están vigentes para minimizarlos de manera eficaz en cuanto a costos.

*** Estudio de factibilidad**

- El auditor debe revisar la documentación producida en esta fase para comprobar su razonabilidad.

- Deben verificarse todas las justificaciones de costos y

beneficios junto con el programa de cuándo se anticipa que se obtendrán los beneficios.

- Identificar si actualmente existe la necesidad de la organización para justificar el sistema y hasta qué punto lo necesitan.

- Determinar si se puede lograr una solución con los sistemas que ya se tienen. Si no, revisar la evaluación de las soluciones alternativas para corroborar su razonabilidad.

- Determinar la razonabilidad de la solución escogida.

*** Definición de los requerimientos**

El auditor debe obtener la documentación de la definición de los requerimientos detallados y verificar su exactitud a través de entrevistas con los departamentos de usuario quienes lo solicitaron y son los afectados.

- Identificar los miembros clave del equipo del proyecto y verificar que todos los grupos de usuario afectados tienen una representación apropiada.

- Verificar que la gerencia aprobó el inicio del proyecto

así como su costo.

- Revisar los diagramas de flujo de datos y el diseño conceptual para asegurar que contemplan las necesidades del usuario.

- Revisar el diseño conceptual para asegurarse de la existencia de controles apropiados.

- Revisar las propuestas dadas al proveedor para asegurarse que cubren el alcance verdadero del proyecto y los requerimientos de los usuarios.

- Determinar que se han solicitado las propuestas a los proveedores apropiados.

- Determinar si esta aplicación es apropiada para el uso de una rutina de auditoría. Si es así, solicitar que la rutina sea incorporada en el diseño conceptual del sistema.

*** Fase de diseño detallado y programación**

- Revisar los diagramas de flujo del sistema para el diseño general. Verificar que se dieron las aprobaciones apropiadas para cualquier cambio y que fue discutido con

así como su costo.

- Revisar los diagramas de flujo de datos y el diseño conceptual para asegurar que contemplan las necesidades del usuario.

- Revisar el diseño conceptual para asegurarse de la existencia de controles apropiados.

- Revisar las propuestas dadas al proveedor para asegurarse que cubren el alcance verdadero del proyecto y los requerimientos de los usuarios.

- Determinar que se han solicitado las propuestas a los proveedores apropiados.

- Determinar si esta aplicación es apropiada para el uso de una rutina de auditoría. Si es así, solicitar que la rutina sea incorporada en el diseño conceptual del sistema.

*** Fase de diseño detallado y programación**

- Revisar los diagramas de flujo del sistema para el diseño general. Verificar que se dieron las aprobaciones apropiadas para cualquier cambio y que fue discutido con

y aprobado por el grupo de usuarios afectado.

- Revisar los controles de entrada y salida diseñados en el sistema para comprobar que sean apropiados.

- Entrevistar a los usuarios clave del sistema para determinar su comprensión de cómo operará y determinar su nivel de entrada en el diseño de formatos de pantalla y reportes de salida.

- Determinar la adecuación de auditorías incorporadas al sistema para rastrear la información de los recursos claves.

- Verificar la corrección de los cálculos y los procesos claves.

- Verificar que el sistema pueda identificar y procesar correctamente datos erróneos.

- Revisar los resultados de seguridad de calidad de los programas desarrollados durante esta fase.

- Verificar que se hicieron todas las correcciones recomendadas a los errores de programación y que fueron incorporados todos los módulos de auditoría en los

programas apropiados.

*** Fase de pruebas**

El auditor debe involucrarse en la revisión de esta fase para:

- Revisar el plan de pruebas para verificar su integridad con la evidencia indicada de la participación del usuario, tal como escenarios de situaciones de prueba desarrollados por el usuario y/o aprobación escrita de aceptación de los resultados. Considerar la repetición de pruebas críticas.

- Deben realizarse conciliaciones de los totales de control y datos convertidos.

- Revisar los reportes de errores para comprobar su precisión al reconocer los datos erróneos y para resolverlos.

- Verificar el proceso cíclico para corrección (Por ejemplo, a fin de mes, a fin de año).

- Entrevistar a usuarios finales del sistema para ver su comprensión sobre los nuevos métodos, procedimientos e instrucciones operativas.

- Revisar todo el sistema y la documentación del usuario final para determinar que está completo y verificar su exactitud durante la fase de pruebas.

- Revisar todos los resultados de prueba paralelos para ver su exactitud.

- Verificar que la seguridad del sistema está funcionando como se diseñó mediante intentos de acceso.

*** Implantación**

El auditor debe verificar que esta etapa se haya iniciado sólo si se tuvo una fase de pruebas exitosa, qué precauciones se tomaron al transferir el nuevo sistema a un ambiente de producción y qué aprobaciones existieron antes de su implantación.

- Revisar los procedimientos programados que se utilizan para correr el sistema.

- Revisar la documentación del sistema a fin de asegurarse de que está completo y que todas las actualizaciones posteriores a la fase de pruebas han sido incorporadas.

- Verificar toda la conversión de datos para asegurarse de

que es correcta y está completa antes de implantar en producción el sistema.

*** Post-implementación**

Después de que se ha estabilizado el nuevo sistema en el ambiente de producción, debe llevarse a cabo una revisión de post-implementación. Para mantener la objetividad, esta revisión debe ser llevada a cabo por un auditor que sea independiente de las otras fases del ciclo de vida del desarrollo de sistemas. Antes de esta revisión, es importante que se otorgue el tiempo suficiente para estabilizar el sistema en producción. De este modo, podrá surgir cualquier problema significativo.

- Determinar si se lograron los requerimientos de objetivo del sistema. Durante esta revisión, se debe prestar atención a la utilización y entera satisfacción del sistema por parte de los usuarios finales. Esto será un indicador de si los requerimientos de objetivo se lograron.

- Determinar si se han medido, analizado y reportado adecuadamente a la gerencia los costos y beneficios identificados en el estudio de factibilidad.

- Revisar todas las solicitudes de cambios a programas llevadas a cabo para determinar el tipo de cambios requeridos en el sistema. El tipo de cambios solicitados puede indicar problemas en el diseño, programación o interpretación de los requerimientos del usuario.

- Revisar todos los controles para asegurar que están operando de acuerdo al diseño. Si se incluyó un módulo de auditoría en el sistema, debe usarlo para probar las operaciones claves.

- Revisar los registros históricos de errores del operador para determinar si existe cualquier problema de recursos u operaciones que son inherentes al sistema. Los registros le pueden indicar una planeación o pruebas inapropiadas al sistema antes de la implementación.

- Revisar los saldos y reportes de control de entradas y salidas para verificar que el sistema está procesando los datos con exactitud.

*** Cambios a programas**

El auditor debe verificar si se cuenta con una metodología estándar para llevar a cabo y registrar los cambios necesarios en los sistemas después que éstos han sido desarrollados,

probados e implantados en el ambiente de producción. Debe asegurarse que dicha metodología contemple:

- Procedimientos de autorización para cambios. Verificar que se tengan procedimientos que aseguren que los cambios de emergencia a programas no ponen en riesgo sus controles.

- Un registro de todas las solicitudes para cambios y aprobaciones y está disponible para su revisión. Debe verificarse que esta documentación tenga la razón del cambio, el análisis de costo-beneficio, la solución propuesta, el tiempo estimado para su término, descripción de los cambios realizados y cualquier procedimiento de prueba con sus resultados. Revisar que esta documentación sea actualizada cuando se requiere.

- Aviso al encargado de auditoría después de cualquier cambio para que se puedan hacer los cambios necesarios al módulo y de este modo no se afecte la obtención de evidencia.

- Verificar la integridad del código objeto y fuente del programa en el ambiente de producción.

- Controles de acceso a los programas que aseguren la ejecución apropiada del software de producción.

- Revisión de la documentación como narrativas de programas, diagramas de flujo, diccionario de datos, diagramas de entidad-relación, libros de corrida del sistema, así como la documentación de procedimientos del usuario final para asegurarse de que está actualizada.

ADQUISICION, CAMBIOS Y MANTENIMIENTO DE HARDWARE Y SOFTWARE

Revisión de la adquisición de hardware y software

- La gerencia de Informática ha establecido políticas por escrito referentes a la adquisición de software y hardware que han sido comunicadas a los usuarios, y ha establecido procedimientos y formularios para facilitar su proceso de aprobación,

- Verificar que el estudio de factibilidad contenga el por qué se decidió comprar o arrendar el hardware o software, el motivo por el cual se decidió que este último no fuera desarrollado por personal de la misma organización y que se haya contado con cotizaciones de tres diferentes proveedores a quienes se les informó sobre las especificaciones y marcas requeridas. Esta documentación debe analizarse para determinar que la decisión fue apropiada.

- Checar que la organización haya examinado varios productos del proveedor para determinar cuál de ellos ofrecía la mejor solución en cuanto a costo-beneficio e investigado los siguientes aspectos sobre él antes de firmar el contrato:

  - **Viabilidad del proveedor**

    Verificar la reputación del proveedor sobre su suministro (número de años ofreciendo el producto y número de clientes usándolo), su estabilidad financiera y el nivel de satisfacción de otros clientes.

  - **Soporte del proveedor**

    Verificar que el proveedor tenga disponible una línea completa de productos de respaldo y cumpla con su servicio.

  - **Disponibilidad de documentación confiable y completa**

    Verificar que el proveedor sea capaz de proveer la documentación del sistema o equipo para su revisión antes de la adquisición. El nivel de detalle y precisión encontrado en la documentación puede ser un

indicador del detalle y precisión utilizado dentro del diseño y programación del mismo sistema y equipo.

- Además el auditor debe:

Revisar que el contrato del software contemple las cláusulas para:

- Adquirir el código fuente.
- Entrenamiento.
- Actualizaciones y arreglos a programas.
- Descripción específica de la entrega.
- Promesa de fecha de entrega.
- Permiso para que la organización que está adquiriendo pueda hacer cambios.
- Acuerdos de mantenimiento.
- Permiso de copiar el software para ser usado en caso de recuperación de desastres.
- Documentación.

Revisar que el contrato de hardware contemple las cláusulas para:

- Descripción específica de la entrega.
- Promesa de fecha de entrega.
- Acuerdos de mantenimiento.

- Entrenamiento.
- Documentación.

- El auditor debe además verificar a través de entrevistas a personas clave si se tuvo un ambiente de prueba donde se identificaron, analizaron y evaluaron los estándares, tareas, procedimientos y controles del software y/o hardware antes de su adquisición.

- Verificar que se cuente con las licencias de propiedad del software.

- Verificar las partes involucradas en la adquisición.

- Verificar cómo se evalúa la seguridad del hardware y software de comunicaciones.

- Si durante la auditoría la organización está adquiriendo software y/o hardware, el auditor debe observar cómo se lleva a cabo lo anterior.

SISTEMAS DE APLICACION

Revisión de la documentación de los sistemas de aplicación para obtener una comprensión de los componentes funcionales de ellos

El auditor debe revisar los manuales de usuario y técnicos si la aplicación fue suministrada por un proveedor. También debe revisar la siguiente documentación para obtener una comprensión del desarrollo de la aplicación:

- Documentos de la metodología de desarrollo del sistema. Estos documentos deben incluir análisis de costo-beneficio y requerimientos del usuario.

- Especificaciones funcionales del diseño. Se deben revisar los puntos de control claves en las especificaciones de diseño.

- Cambios a programas. La documentación de cualquier cambio al programa debe estar disponible para su revisión. Cualquier cambio debe proveer evidencia de autorización y debe estar referenciado al código fuente.

- Manuales de usuario. Una revisión de ellos provee una comprensión de cómo el usuario está utilizando la aplicación y puede mostrar las debilidades de control.

- Documentación técnica de referencia. Incluye cualquier manual técnico proporcionado por el proveedor para una aplicación comprada, además de la documentación generada internamente. Deben revisarse las reglas y la lógica de

acceso.

Analizar el flujo de las transacciones a través del sistema

El auditor debe revisar los puntos donde se ingresan, se procesan y se da salida a las transacciones para identificar debilidades en los controles.

Preparación de un modelo de evaluación de riesgos para analizar los controles de aplicación

A través de un modelo de evaluación de riesgo el auditor debe verificar los siguientes factores:

- La calidad de los controles internos.
- Condiciones económicas.
- Cambios recientes al sistema de contabilidad.
- Tiempo transcurrido desde la última auditoría.
- Complejidad de las operaciones.
- Cambios en las operaciones y en el medio ambiente.
- Cambios recientes en puestos claves.
- Tiempo de existencia.
- Medio ambiente competitivo.
- Activos bajo riesgo.
- Resultados de auditorías previas.
- Rotación de personal.

- Volumen de transacciones.
- Volumen monetario.
- Sensibilidad de las transacciones.
- Impacto de las fallas de una aplicación.

El auditor debe darle a cada factor un peso para determinar su importancia relativa con los demás. El riesgo total de la aplicación va a ser la combinación de todos los factores.

Observación y prueba de los procedimientos de actuación de los usuarios

*** Segregación de tareas**

El auditor debe observar y revisar las descripciones de las actividades así como los niveles de autorización y procedimientos para verificar la existencia de una adecuada segregación de tareas.

*** Autorización de entrada**

- El auditor debe probar la autorización de ingreso revisando los documentos de ingreso y checando la autorización apropiada o revisando las reglas de acceso al computador.

- Debe revisarse el reporte de actividades de errores para probar la evidencia de revisión gerencial. Si existen muchos errores, esto puede indicar la necesidad de modificar las rutinas de validación y edición para mejorar la eficiencia.

*** Balanceo**

El auditor debe verificar que se concilian bajo bases regulares los totales de control de corrida a corrida y otros totales de la aplicación. Debe probarse el balanceo con una repetición o revisando las conciliaciones anteriores de error.

*** Control de error y corrección**

- El auditor debe revisar los reportes de errores para verificar si se tuvo una revisión, búsqueda y tratamiento de corrección apropiada.

- Además debe revisar los errores y rechazos de ingreso antes del tratamiento.

*** Distribución de reportes**

- El auditor debe verificar que se produzcan reportes de salida críticos, se tengan en una área segura y sean

distribuidos de manera autorizada. El proceso de distribución lo puede probar observando y revisando los registros de las salidas de distribución.

- Debe verificar que esté restringido el acceso a los reportes de salida en línea. Este acceso en línea puede probarlo a través de la revisión de las reglas de acceso o monitoreando la salida del usuario.

Revisión y pruebas de las autorizaciones y facilidades de acceso

*** Tablas de control de acceso**

El auditor debe probar los niveles de acceso por persona revisando las reglas de acceso para asegurarse de que ha sido otorgado tal como lo decidió la gerencia.

*** Reportes de actividades**

El auditor debe revisar los reportes de actividad que proveen detalles de usuarios, de actividad, volumen y horas para asegurarse de que las actividades se desarrollan sólo durante las horas normales de operación.

*** Reportes de violaciones**

- El auditor debe revisar los reportes de violaciones para verificar cualquier intento de acceso no autorizado o sin éxito.

- Debe revisar que incluyan la ubicación de la terminal, fecha y hora cuando se intentó el acceso.

- Estos reportes le deben proporcionar evidencia de revisión gerencial. Si el auditor encuentra que hay violaciones de acceso no autorizadas repetidas, esto le puede indicar que los intentos evaden los controles de acceso.

- En esta prueba, el auditor debe incluir una revisión de los procedimientos de seguimiento.

*** Datos de prueba**

- El auditor debe crear datos de entrada para pruebas. Debe procesar los datos con los programas de aplicación que fueron seleccionados para la prueba, después comparar la salida con los resultados anticipados.

- Puede usar la prueba de datos para comprobar las rutinas de validación de entrada, la detección de errores de

lógica y controles de procesamiento, los cálculos estándares, la modificación a programas y procedimientos manuales en uso.

Cabe mencionar que están contemplados únicamente los aspectos que consideramos relevantes, por lo que el auditor puede encontrar otros no mencionados y tener que valerse de su criterio profesional para su evaluación.

Adicionalmente, por cada pregunta que esté evaluando el auditor en la prueba de procedimientos, debe referirse a una tabla de controles específicos que sea diseñada especialmente para ella para identificar los riesgos en que se pueda incurrir en caso de ausencia de controles (véase anexo 3, p. C1). Asimismo, debe contestar las preguntas en un formato donde se anote el número de pregunta, se describa la respuesta, se identifique si existe o no deficiencia y se haga referencia a la evidencia obtenida. En caso de que la pregunta no sea aplicable a la organización, el auditor debe indicarlo en dicho formato (véase anexo 2, p. B22).

Al finalizar la prueba de procedimientos, el auditor debe hacer un sumario por cada una de las secciones evaluadas a fin de concluir si resultan apropiados los controles para poder depositar confianza en la integridad del proceso y debe anexarlo al inicio de la prueba (véase anexo 2, p. B1).

Es importante que se anexe la documentación a los papeles de trabajo y se hagan comentarios por escrito sobre la evidencia obtenida con el ambiente de prueba y/o ambiente real o con la observación directa. La evidencia debe contemplar la presencia o ausencia de controles.

El auditor tiene que usar su criterio profesional en la selección de evidencia apropiada. El debe considerar cualquier elemento que permita hacer posteriormente una evaluación objetiva y expresar un informe de naturaleza profesional.

2.2.3. Aplicación de las pruebas sustantivas o de saldos.

Debe aplicarse una prueba de saldos cuando en la planeación estratégica se comentó a la Alta Gerencia y ésta lo aprobó por considerarlo pertinente.

Las pruebas de saldos son aquellas que debe aplicar el auditor para validar la razonabilidad de cifras y probar los cálculos programados a fin de garantizar la integridad y consistencia de la información emitida a través de sistemas de aplicación en la que se apoya la Alta Gerencia de una organización para la toma de decisiones.

Dentro de los tipos de pruebas de saldos que puede aplicar el

auditor se tienen las siguientes:

- Pruebas para identificar procesos erróneos.
- Pruebas para determinar la calidad de los datos.
- Pruebas para identificar datos inconsistentes.
- Pruebas para comparar los datos con los inventarios.
- Confirmación de los datos con fuentes externas.

Estas pruebas las debe realizar el auditor auxiliándose de técnicas de auditoría asistidas por el computador. Por ello, debe tener una cabal comprensión de ellas y saber dónde aplicarlas. Esta comprensión debe incluir tanto la utilización de software de auditoría generalizado como técnicas más avanzadas tales como generadores de datos de prueba y técnicas para instalaciones de prueba integrada. Además de seleccionar la técnica correcta basada principalmente en la evidencia que se desea obtener, el auditor debe comprender la importancia de documentar los resultados de tales pruebas con fines de evidencia de auditoría.

Las técnicas de auditoría asistidas por el computador que debe utilizar son:

*** Programas de recuperación y análisis**

Están escritos de acuerdo a especificaciones de auditoría para

permitirle organizar, combinar, calcular, analizar excepciones o extraer datos computarizados y para rehacer cálculos y otras funciones de procesamiento computarizadas para la obtención de evidencia sustantiva. Ejemplos de ellos son Easytrieve y FOCUS.

Si el auditor decide desarrollar estos programas puede requerir la asistencia del cliente en la obtención o preparación de la información técnica, incluyendo descripciones de archivos y especificaciones de los equipos instalados. Por lo general, es más eficiente utilizar para estas tareas personal de la organización que realizarlas el propio auditor debido a que:

- Está familiarizado con las operaciones del área de Informática, archivos de datos y equipos de cómputo de la organización, lo cual contribuye a reducir el tiempo de desarrollo y procesamiento de las aplicaciones de auditoría.

- Los programas pueden ser desarrollados más rápidamente si la organización cuenta con personal que sea usuario frecuente del software de auditoría.

- El personal de departamento usuario puede ser útil al auditor en la sección de transacciones que eligió para ser probadas.

Pero no debe descartar que el personal de la organización puede tener mayores oportunidades de manipular los datos, ya que conocen las pruebas de auditoría que se llevan a cabo.

Cuando el volumen de los datos del sistema a ser evaluado es muy extenso, el auditor debe usar el muestreo estadístico para realizar pruebas en forma eficiente y eficaz y de este modo poder inferir a todo el universo y reducir el tiempo de revisión.

Cuando el auditor encuentre excepciones, es decir, cualquier registro que salga de un rango o parámetro predeterminado, debe generar informes de ellas. Como ejemplos, se pueden mencionar los siguientes:

- Los registros de tiempo de empleados que totalizan una cantidad de horas superior al parámetro establecido.

- Las cuentas por cobrar vencidas que superen un periodo preestablecido.

- Los pagos a proveedores que superen un monto preestablecido.

* **Recuperación, análisis de datos y otras técnicas utilizando microcomputadoras.**

El auditor debe identificar los datos que serán transferidos de un mainframe a microcomputadores (downloading) para luego revisarlos, estratificarlos, probar los cálculos, seleccionarlos y analizar estadísticas. Estas técnicas le permiten la transferencia de las pruebas de auditoría de un sistema de información central a un ambiente de trabajo individual.

Si el auditor decide utilizar el downloading debe:

- Identificar los datos que serán transferidos desde el computador central al microcomputador.

- Determinar el método que utilizará para transferir datos desde el computador central al microcomputador. Puede ser que decida establecer una conexión directa entre los computadores con cable coaxial o copiar en una cinta magnética los datos del cliente y luego, desde una unidad de cintas transferirlos al microcomputador.

- Si fuera necesario, convertir los datos del cliente a un formato que pueda ser utilizado por el software utilizado en la microcomputadora.

El auditor debe restablecer procedimientos para obtener totales de control que concilien con los registros del cliente para

asegurarse de que no se han efectuado ajustes posteriores a la transferencia de los datos. Estos totales de control pueden ser controles de sesión, recuento de registros y otros totales de control generados durante el procesamiento utilizados para detectar transacciones no autorizadas, faltantes, duplicadas o erróneas.

El auditor puede utilizar esta técnica para:

- Comparar los estados financieros del cliente en diferentes fechas, o de los estados financieros y datos relacionados con estadísticas relativas a la industria.

- Transferir al microcomputador los precios y cantidades de existencias de las líneas de productos más significativas para compararlas con periodos anteriores y el uso proyectado.

- Análisis de los efectos impositivos de consideraciones relativas a nuevas situaciones.

El auditor debe considerar que al usar esta técnica elimina la necesidad de digitación para ingresar al microcomputador los datos de los archivos computarizados del cliente y el riesgo de errores y le demuestra al cliente su conocimiento y utilización de las tecnologías más recientes.

Por otro lado, como el personal de la organización puede manifestar preocupación con respecto a la seguridad de los datos con motivo de la posibilidad de acceder a ellos en forma directa, el auditor debe hacer énfasis de que los archivos transferidos serán utilizados únicamente con el propósito de la auditoría y no serán revelados.

En caso de que el auditor haya decidido trabajar en el computador central de la organización, debe transferirle los programas de recuperación y análisis diseñados en el microcomputador para su ejecución (uploading). Esto le brinda asistencia técnica y apoyo operativo por parte del personal de la organización así como observación del procesamiento para obtener una mejor comprensión de los controles del área de Informática. Los procedimientos de seguridad y control relacionados con el uploading deben ser acordados de antemano con el responsable.

El auditor debe considerar los siguientes controles sobre las técnicas de auditoría computarizadas para proporcionar una adecuada seguridad de que:

- El programa de recuperación y análisis o los datos de prueba alcanzarán el objetivo preestablecido.

    - Se ha planificado y documentado el programa de

recuperación y análisis o la técnica de transacciones de prueba.

- Se han efectuado pruebas para asegurar que la lógica de los programas de recuperación y análisis es correcta.

- No se han producido manipulaciones o usos no autorizados de los programas o datos de prueba desde la última vez que se utilizaron.

- Se han considerado los controles de biblioteca para prevenir accesos no autorizados en caso de que sean mantenidos en ella.

  - Antes de correr nuevamente un programa se ha comparado con la última corrida para asegurarse de que no se le han efectuado modificaciones.

  - Se ha mantenido en los archivos una copia de los programas y transacciones de prueba.

- Los programas se han aplicado a los archivos de datos correspondientes y los datos de prueba han sido procesados por el programa correspondiente.

- Se ha preparado la documentación necesaria que describe cómo se debe correr la aplicación de auditoría, cuándo y qué archivos y programas se deben utilizar.

  - Se ha obtenido un listado del programa y del estado de ejecución de tareas con sus correspondientes resultados para asegurarse de que se emplearon las versiones correctas de los programas y de que los programas de recuperación y análisis leyeron los archivos correctos.

  - Se han conciliado los totales producidos por una aplicación de transacciones de prueba con totales de auditoría predeterminados.

  - Se ha revisado el registro de operaciones para verificar si hubo inferencias en la corrida de la aplicación de auditoría y para determinar si se utilizaron los archivos y programas correctos.

  - Se ha considerado la conveniencia de presenciar el procesamiento.

Además de las técnicas ya mencionadas, el auditor puede utilizar el software de auditoría generalizado para realizar las siguientes funciones:

- Acceso a los archivos.
- Reorganización de los archivos.
- Selección, estadísticas, aritmética, estratificación y análisis de frecuencia.
- Creación y actualización de archivos.
- Verificación de la calidad de los datos y del proceso del sistema así como la correspondencia de los datos con el mundo real.
- Generación de reportes.

Como ejemplo de este software se pueden mencionar el ACL, Audassist, Audit Reporter, Computer File Analyzer, Interactive Data Extraction and Analysis (IDEA).

Si los auditores deciden desarrollar su propio software para propósitos de auditoría, se incrementa su independencia. Tienen un mejor entendimiento de sus programas de aplicación y no dependen de otra gente para la disponibilidad de software para propósitos de recolección de evidencia. Como consecuencia, el personal de administración y de procesamiento de datos electrónico los van a respetar más si perciben que cuentan con la suficiente competencia técnica para escribir sus propios programas.

Es importante mencionar que cuando el auditor solicite a la organización bases de datos para efectuar sus pruebas debe

hacerlo por escrito. Debe entregar el original al Gerente de Sistemas quien debe a su vez firmar la copia que contenga la fecha de la requisición y la fecha en que promete su entrega. En caso de que el auditor obtenga diferencias en los resultados de las pruebas, debe comentarlo con el Gerente del área de Informática para encontrar el origen de las mismas y darle seguimiento. En caso contrario, debe hacer de su conocimiento la terminación satisfactoria de la prueba.

Finalmente, el auditor debe documentar los pasos para la realización de las pruebas a fin de:

- Registrar las decisiones importantes, los procedimientos que se llevaron a cabo, rutinas probadas, los controles existentes y los resultados obtenidos.

- Registrar, si es el caso, los detalles relativos a la preparación del programa, incluyendo el software y los controles usados durante el desarrollo así como las especificaciones de la corrida que contemplen entrada, pasos del procesamiento y salida de datos.

- Documentar el trabajo realizado con los datos de salida.

- Documentar la resolución de los errores, excepciones o partidas inusuales detectadas.

- Documentar los problemas administrativos y técnicos detectados y cómo fueron solucionados.

- Emitir una conclusión (en relación con los requerimientos de auditoría).

- Comparar los costos reales con los presupuestados.

- Facilitar el uso de la aplicación en años posteriores, proporcionando información de planeación que incluya detalles de problemas detectados y cambios recomendados.

Debe anexar esta documentación a los papeles de trabajo como evidencia.

2.2.4 Evaluación de los resultados de las pruebas de procedimientos y de saldos para determinar los riesgos e integración de los obtenidos en la planeación estratégica.

El encargado y el equipo de auditoría deben reunirse para integrar la documentación obtenida en la aplicación de la guía para la planeación estratégica y la o las pruebas de procedimientos y/o saldos.

El encargado debe revisar que se hayan cubierto todos los pasos del plan de trabajo y que las pruebas estén debidamente documentadas.

Por cada deficiencia detectada en las etapas anteriores deben utilizar un formato llamado "cédula de deficiencias y recomendaciones" en el cual anoten el número de la hoja en donde se identificaron, hagan una descripción de la misma y emitan la sugerencia para corregirla, definan si aumentan o no el alcance de la auditoría, describan los comentarios del cliente y determinen cuáles deben incluirse en la carta de recomendaciones de acuerdo al riesgo que representen para la organización (véase anexo 3, p. C29).

El encargado debe verificar que no exista duplicidad en las deficiencias.

Todas las cédulas elaboradas deben anexarse al inicio del legajo.

2.3 Revisión por el gerente de la auditoría a la documentación obtenida. (papeles de trabajo)

El encargado debe presentar al Gerente los papeles de trabajo para su revisión. Este último debe revisar el cumplimiento del

plan de trabajo y verificar que se hayan cubierto correctamente todos los puntos de la guía para la planeación estratégica, de la o las pruebas de procedimientos y/o saldos y determinar su grado de correspondencia con la evidencia obtenida. Con esta revisión, el Gerente puede detectar deficiencias que no estén identificadas como tales y pedirle elaboren las cédulas de deficiencias y recomendaciones pertinentes.

Además debe revisar las cédulas de deficiencias y recomendaciones para dar su aprobación sobre las que proponen incluir en la carta de recomendaciones o decidir cuáles deben excluir.

Esta etapa exige al Gerente un buen juicio basándose en su experiencia ya que debe decidir cuáles hallazgos presentar a la Alta Gerencia y evaluar lo que podría ser significativo para diferentes niveles gerenciales. Si bien se aplica durante todo el proceso de auditoría la Norma general No. 8 "Debido cuidado profesional", es especialmente importante para él al evaluar las fortalezas y debilidades encontradas en la documentación obtenida.

El Gerente debe concluir esta revisión cuando considere que se ha cumplido con el objetivo de la auditoría.

2.4 Elaboración de la carta de recomendaciones para ser discutida y presentada a la Alta Gerencia.

El Gerente después de revisar los resultados de la auditoría y determinar las deficiencias que deben incluirse, debe formular una carta de recomendaciones basándose en las cédulas de deficiencias y recomendaciones para informar sobre los hallazgos.

El Gerente debe saber que su responsabilidad final es la Alta Gerencia quien por lo general no conoce directamente lo que acontece en realidad y que es a ella a la que debe comunicar sin restricciones todos los hallazgos importantes de manera objetiva sin permitir que ningún nivel gerencial por debajo de ésta coarte su independencia. Respecto a ello, debe comprender las Normas generales Nos. 1 y 2 sobre independencia.

El Gerente debe comprender los componentes básicos de la carta y cómo comunicar adecuadamente los hallazgos de auditoría a la Alta Gerencia. Por ello, debe entender las Normas generales No. 9, "Reporte del alcance de auditoría", y No. 10, "Reporte de hallazgos y conclusiones".

El Gerente debe incluir dentro de la carta de recomendaciones la siguiente estructura y contenido:

* Nombre de la compañía que se auditó,

* Periodo cubierto,

* Introducción al informe que incluya los objetivos de auditoría y una expresión general sobre la naturaleza y extensión de los procedimientos de auditoría realizados,

* Nombre del componente auditado,

* Riesgos encontrados,

* Areas que se están viendo afectadas,

* Controles que se sugieren para mejorar los procedimientos,

* Comentarios de la Alta Gerencia sobre los hallazgos,

* Seguimiento que se ha dado a las recomendaciones emitidas en la auditoría anterior si así es el caso.

* Conclusión global del Gerente de auditoría expresando una opinión sobre la adecuación de los controles o procedimientos revisados, respaldada por el resto del contenido de la carta y por la evidencia global recopilada para de este modo poder brindar un nivel mayor de

respaldo.

La carta de recomendaciones debe ser de fácil lectura, gramaticalmente correcta y breve de manera que presente los hallazgos a la Alta Gerencia en forma comprensible. La mayoría de los ejecutivos no están versados en la jerga de la computación, por lo que la carta debe carecer de terminología técnica.

Una vez presentada la carta, la Alta Gerencia puede auxiliarse de las áreas auditadas para discutirla con el Gerente de auditoría. Este último debe utilizar alguna técnica de exposición como las transparencias para retroproyector o diapositivas generadas por paquetes de software graficador para comunicar mejor los objetivos, el alcance y los resultados de la auditoría. Además, debe proporcionar a los gerentes de las áreas auditadas anexos de naturaleza más técnica donde se detalle cómo corregir las situaciones informadas. Es importante que lleve consigo el legajo en caso de que le exijan que demuestre las deficiencias encontradas con evidencia.

El Gerente de auditoría debe explicar por cada componente los riesgos encontrados, hacer énfasis sobre las áreas que se están viendo afectadas y sobre los controles que se recomiendan para hacer más eficientes y eficaces los procedimientos. Por cada uno de ellos, la Alta Gerencia debe emitir sus comentarios y

éstos deben ser asentados en la carta. El Gerente de auditoría debe reconocer que tal vez la Alta Gerencia no esté en condiciones de implantar todas las recomendaciones de auditoría en forma inmediata ya que pueden tenerse restricciones tales como limitaciones de personal, presupuestos, u otros proyectos. Por ello, dentro de los comentarios debe proporcionarse una fecha de implantación del control sugerido que sirva para ver el seguimiento o progreso de la implantación de las recomendaciones. Luego, en caso de que la organización haya sido auditada anteriormente, el Gerente de Auditoría debe presentar el seguimiento que han dado las áreas a las acciones correctivas prometidas. Posteriormente, el Gerente de auditoría debe explicar sus conclusiones globales sobre la adecuación de los controles o procedimientos examinados y fijar una fecha para la entrega de la carta definitiva.

Finalmente, el Gerente de auditoría también debe revisar con la Alta Gerencia el cumplimiento del plan de trabajo y en caso de que existan modificaciones en el mismo deben discutirse para determinar los excesos en el presupuesto.

2.5 Elaboración de la carta de recomendaciones definitiva.

Una vez expuestos los hallazgos encontrados a la Alta Gerencia, el Gerente debe elaborar la carta de recomendaciones definitiva

con las correcciones acordadas si así es el caso y con los comentarios del cliente para enviársela en la fecha acordada.

El encargado debe anexar una copia de la carta definitiva al inicio del legajo el cual debe ser archivado para poder ser utilizado en auditorías posteriores.

2.6 Seguimiento de las recomendaciones.

Una vez terminada la auditoría, debe comprobarse si las áreas auditadas han implantado los controles recomendados prometidos. Para ello, los auditores deben tener un programa de seguimiento elaborado con la fechas proporcionadas por la Alta Gerencia cuando se discutió la carta de recomendaciones. Dichos resultados del seguimiento deben ser comunicados a los niveles gerenciales correspondientes.

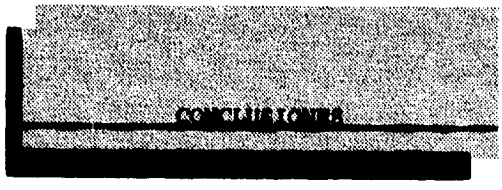
El nivel de la revisión de seguimiento del auditor debe depender de diversos factores. En algunos casos, el auditor debe tal vez sólo preguntar sobre la situación actual de los controles de la organización. En otros, debe realizar ciertos pasos de auditoría como observar, entrevistar y/o probar los procedimientos para cerciorarse si la gerencia ha implantado las acciones correctivas acordadas.

Dentro de los procedimientos que el auditor debe utilizar son:

- Procedimientos para evaluar y probar la eficiencia y eficacia de las operaciones,

- Procedimientos para probar controles, y

- Revisar y evaluar la razonabilidad de los documentos, políticas y procedimientos.



Hoy en día, las organizaciones buscan alcanzar un nivel de desarrollo, productividad y competitividad. Para lograrlo, deben dar vital importancia a la información que manejan ya que les sirve de base para una buena toma de decisiones. Esta debe ser confiable, segura, íntegra y coherente a través de un procesamiento eficaz y eficiente que garantice una continuidad en el servicio.

En ocasiones, no alcanzan el nivel deseado debido a que en alguna o algunas áreas no se cuenta con controles adecuados en el procesamiento de información lo que ocasiona se presenten problemas considerados como significativos para sus operaciones eficientes.

Por otro lado, pueden estar alcanzando el nivel deseado pero también requerir que se lleve a cabo una revisión sobre algún componente en específico como controles generales, seguridad, centros de cómputo, continuidad de las operaciones, sistemas operativos y utilitarios, ciclo de vida del desarrollo de sistemas, adquisición, cambios y mantenimiento de hardware y

software, y control de aplicaciones, simplemente por conocer si se están aplicando de manera adecuada los controles necesarios.

Por lo anterior, resulta de suma importancia para éstas considerar la auditoría en Informática como un área para detectar posibles riesgos y establecer controles adecuados contribuyendo a su eficiencia y eficacia.

En primera instancia, el auditor en Informática debe comprender de manera cabal el Código de Etica Profesional para regir bajo él su conducta profesional y personal, y las Normas Generales para auditoría en Informática.

Una vez comprendido lo anterior, debe seguir una metodología para llevar a cabo una auditoría en Informática que se pueda aplicar a cualquier departamento del área de Informática y adecuarse al tamaño, contexto y complejidad de cualquier organización.

Para realizar la auditoría en Informática, el auditor debe contar con la capacitación y especialización requerida debido a que las organizaciones cuentan con tecnología diferente a la que debe hacerle frente buscando ser eficaz y eficiente en su manejo. También debe tener bien claros los procedimientos que se deben aplicar en dicha metodología para lograr el objetivo de la auditoría.

La metodología debe contemplar una planeación estratégica, aplicación de pruebas de procedimientos y/o saldos, un examen y evaluación de la información obtenida, la comunicación de los resultados y un seguimiento.

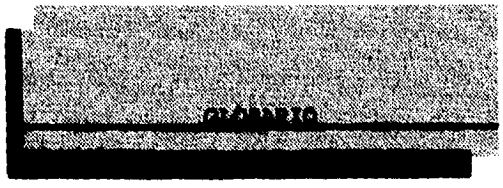
En la planeación estratégica, el auditor debe, a partir de un requerimiento, definir el objetivo de la auditoría. Posteriormente, conocer de manera preliminar el ambiente de sistemas. Debe aplicar pruebas de procedimientos y/o saldos en los componentes y en caso de identificar debilidades determinar los riesgos a que está expuesta la organización a través de la evaluación y sugerir. Debe valerse de la automatización para minimizar el tiempo requerido para la realización de la auditoría apoyándose en técnicas y herramientas asistidas por el computador.

Toda la información obtenida debe considerarse como evidencia de auditoría, tener una naturaleza de descubrimiento y no acusatoria y haberse conseguido de manera objetiva después de aplicar alguna o todas las técnicas de recopilación de información.

En la actualidad, en nuestro país, no se ha dado la importancia relativa al área de auditoría en Informática ya que sólo se le ha considerado para llevar a cabo revisiones como apoyo al área contable sin poder dictaminar como ocurre en esta última. Por

ello, la metodología presentada en este trabajo pretende ser una guía para los auditores en Informática que estamos seguras estará en auge en un tiempo no muy lejano dándole la sociedad en Informática todo el valor correspondiente.

Este trabajo puede servir para investigaciones posteriores sobre el tema y para probar su aplicación en el departamento de comunicaciones haciendo uso de las herramientas presentadas.



Acceso digital un computador

Mediante este servicio, los conmutadores del usuario puedan ser conectados a la RDSI a través de troncales de 64 Kb/s y enlaces de 2.048 Mb/s incorporando así a sus comunicaciones todo el potencial y calidad que la tecnología digital ofrece en la actualidad en la transmisión de información tanto de voz como de datos.

Amplificadores

Dispositivos que retransmiten las señales analógicas a su forma y fuerza original. La forma de onda que representa la señal mantiene sus características de un extremo a otro del canal.

Amplitud

Medida de una señal basada en la cantidad de variación desde su valor cero. Altura de la onda que se mide de su punto medio a la punta; esto es importante cuando se considera el volumen. Una amplitud de onda está asociada con el nivel de voltaje que se lleva en el cable. En una fibra óptica la amplitud de onda se refiere a la intensidad de un haz de luz.

Ancho de banda

Diferencia entre la frecuencia más alta y la más baja que viajan sobre el canal. Tiene una relación directa con la capacidad de un canal de comunicación que se determina por el número de bps que se puedan transmitir.

ANSI

American National Standard Institute. Instituto Americano de Normalización que desarrolló el código ASCII y coordina y sanciona las actividades de las organizaciones americanas generadoras de estándares.

ARP

Address Resolution Protocol. Protocolo de dirección. Forma parte del conjunto de protocolos TCP/IP.

ASCII

American Standard Code for Information Interchange. Intercambio de información a través de un código estándar americano apoyado y desarrollado por ANSI. Código estándar básico para el que se diseña casi todo el equipo de comunicaciones. Clave de 8 bits con 128 configuraciones válidas de caracteres.

ATM

Asynchronous Transfer Mode. Protocolo de transmisión que proveerá servicios B-ISDN y/o SMDS (video, datos y voz a diferentes rangos de velocidades).

B-ISDN

Broadband ISDN. Protocolo que extiende la capacidad de la ISDN para poder soportar transmisiones a velocidades más rápidas.

Banda portadora

Utiliza tecnología analógica sobre múltiples canales. Las señales fluyen a través de un medio de transmisión en forma de ondas electromagnéticas. Utilizan un modem para inyectar en el medio de transmisión señales portadoras, que son después moduladas por una señal digital. Debido a su naturaleza analógica, las redes de banda ancha suelen estar multiplexadas por división en frecuencia. Su denominación se debe a que trabajan en una banda de frecuencia de radio de alta

frecuencia (entre 10 y 400 MHz).

Banda base Técnica de transmisión que se lleva a cabo sobre un solo canal. Las redes de banda base utilizan tecnología digital. El término "banda base" suele referirse a las señales no moduladas. Con esta forma de transmisión, un dispositivo de emisión envía pulsos de datos directamente sobre el canal de comunicación y el dispositivo receptor los detecta.

BellCore Bell Communications Research. Compañía que se formó para investigar y desarrollar las 7 RBOCs en los Estados Unidos después de la ruptura de AT&T. Define los servicios de MAN que pueden ofrecer las compañías telefónicas. Define los estándares de implementación y requerimientos de servicio para las RBOCs. Participa, al igual que AT&T en el proceso de estándares nacionales e internacionales.

Bps Bits por segundo. Ver ancho de banda.

Byte Grupo de bits consecutivos que se tratan como una unidad o carácter. Por lo general, un byte está formado por 8 bits y representa un carácter. Sin embargo, en las comunicaciones de datos algunos códigos comunes utilizan 5, 6, 7, 8, 10 u 11 bits para representar un carácter. Esas diferencias en el número de bits por carácter se deben a que cada código representa un número distinto de caracteres y tiene distintas consideraciones para la detección de errores.

Cable de cobre Conductor metálico más común. Usado para transmitir señales localmente. Resulta familiar para muchos porque se usa para conectar el teléfono de la central telefónica a teléfonos de hogares y comercios.

Cable coaxial Consiste en un cilindro hueco de cobre (malla) u otro conductor cilíndrico que rodea a un conductor de alambre simple. El espacio entre la malla de cobre y el conductor interno se rellena con un aislante, que separa el conductor externo del conductor interno. Estos aislantes están espaciados a pocos centímetros. Puede transmitir a frecuencias mucho más altas que un par de alambres. Está sujeto a menos interferencias, líneas cruzadas o pérdida de señal por lo que constituye un mejor medio de transmisión que los cables de pares trenzados. Puede colocarse al lado de objetos metálicos sin ningún problema, puede soportar índices de datos hasta 100 Mbps. Puede colocarse bajo las calles, correr bajo el agua o a través de un edificio en las paredes, techos y pisos.

Cables de par trenzado Cable que consiste de dos tiras aisladas de cobre entrelazadas. Un número de cables entrelazados se agrupan juntos y se encierran dentro una cubierta protectora para formar un cable. Un cable lleva la electricidad al teléfono o al modem y el otro lleva la electricidad del teléfono o del modem. Esto reduce la oportunidad de interferencia entre pares. Existe el cable blindado de pares trenzados que usa una cubierta protectora de más alta calidad ya que está sujeto a menos interferencias eléctricas y puede soportar transmisiones a grandes distancias. La mayoría de los sistemas de comunicación de datos emplean para sus transmisiones este tipo de cable.

CCITT Comité Consultor Internacional de Telefonía y Telegrafía que opera bajo la dirección de ITU. Estableció el X.25, V.24 y V.28 entre otros. Hace recomendaciones sobre telefonía y telegrafía las cuales tienen influencia internacional y están identificadas por una letra seguida por un número en donde la primera indica el tema general de la serie de recomendación. Produce estándares describiendo el acceso a las redes públicas.

Centrales privadas de Conocida como PBX. Conmutador telefónico privado. Instalación dentro de la organización del suscriptor donde terminan todas las líneas telefónicas de

conmutación la organización. Por lo general, se tienen varias líneas que van del conmutador hasta una oficina terminal. La línea entre la oficina terminal y cada suscriptor individual o un suscriptor de organización se conoce como circuito local, o sea una línea telefónica entre la instalación comercial y la oficina terminal de la compañía telefónica local que da servicio a esa instalación. Se conocen también como PABX.

Centrex avanzado Completando la versión básica de este servicio, se integran facilidades más avanzadas de la tecnología digital, dotando al usuario desde el inicio de la posibilidad de manejar en su empresa voz, datos y video, en las mismas condiciones financieras, económicas y operativas del caso básico.

Centrex básico Con esta facilidad, en las instalaciones del usuario se ubica un módulo de la central de conmutación de la RDSI, dotando así al cliente de los servicios y funciones básicas equivalentes de un conmutador privado, con la responsabilidad del mantenimiento por parte de la central telefónica y sin necesidad de inversiones en equipo, aunado a que de forma inmediata, se puedan incorporar funciones y servicios más avanzados, evitando la obsolescencia en sus comunicaciones.

Cluster Ver Controladora.

CMIP Common Management Information Protocol. Protocolo desarrollado por ISO para la administración de la información.

Codificar Consiste en representar un conjunto de símbolos mediante otro. Por ejemplo, el representar el carácter A mediante un grupo de 7 bits (digamos 1000001) es una codificación.

Código Grupo de caracteres que tiene un significado particular. También es un término general usado para referirse a programas de computación o porciones de programas. Sistema de símbolos que representa datos o instrucciones de una computadora. Algunos de los códigos comunes son el ASCII, EBCDIC y Manchester.

Concentrador Repetidor multipuerto. En FDDI, es un nodo que tiene puertos adicionales además de los que requiere para su propia conexión a la red. Estos puertos adicionales se usan generalmente para la conexión de estaciones adicionales individuales a la red.

Conmutación de mensajes Esta tecnología sigue empleándose bastante en algunas aplicaciones, como el correo electrónico. El conmutador suele ser un ordenador especializado, que se encarga de aceptar tráfico de los ordenadores y terminales a él conectados mediante líneas alquiladas o conmutadas. El ordenador examina la dirección que aparece en la cabecera del mensaje y conmuta (encamina) el paquete hacia el equipo terminal de datos que ha de recibirlo. Es una tecnología que a diferencia de la conmutación de circuitos telefónica, permite grabar la información para atenderla después, gracias a la capacidad de almacenamiento (por lo general en forma de disco) que posee el conmutador.

Conmutación de paquetes Los datos de usuario (mensajes, por ejemplo) se descomponen en trozos más pequeños. Estos fragmentos, o paquetes, están insertados dentro de informaciones del protocolo, y recorren la red como entidades independientes. Distribuye el riesgo a más de un conmutador, reduce la vulnerabilidad ante fallos en la red y permite una mejor utilización del canal.

Conmutación telefónica También conocida como conmutación de circuitos. Ver intercambio de circuitos.

Conmutación — Se logra desconectando y conectando líneas en diferentes configuraciones para establecer un camino continuo entre el emisor y el receptor. Existe conmutación telefónica, de mensajes y de paquetes.

Controlador de comunicaciones — Ver Procesador de comunicaciones.

Controladora. — También conocido como cluster. Dispositivo que controla todas las comunicaciones entre un número de terminales u otros dispositivos y una computadora central. En una red, se conecta por medio de un programa de software residente en la terminal de la red a la interface de la computadora central para establecer comunicación.

Convertidor de protocolos — Dispositivo que interconecta redes diferentes o heterogéneas y provee funciones de conversión de protocolos y ruteo. Interconecta LANs a otros tipos de redes, particularmente WANS.

CPU — Central Processor Unit. Ver Procesador central.

Cruce fronterizo — Capacidad de interconectar a las empresas o instituciones de las ciudades fronterizas, principalmente la industria maquiladora con las ciudades o poblaciones equivalentes en Estados Unidos de América a través de enlaces de la RDSI de hasta 2.048 Mbs, para la transmisión de todo tipo de señales, optimizando las comunicaciones y operaciones de los clientes.

CSMA/CA — Carrier-Sense Multiple Access with Collision Avoidance. Método de control de acceso distribuido donde una estación transmite un mensaje a otra y esta última le envía una respuesta manteniendo un diálogo eficiente o donde una estación que ha transmitido debe esperar hasta que todas las otras estaciones hayan tenido la oportunidad de transmitir antes de que ésta transmita de nuevo. Esto asegura que las estaciones de más bajo nivel tengan una oportunidad de transmitir.

CSMA/CD — Carrier-Sense Multiple Access with Collision Detection. Método de control de acceso aleatorio que se emplea en la topología lineal o en la de árbol. Para iniciar el envío de la información es necesario que cada estación espere a que el canal de la red se encuentre sin transmisión. En caso de que otra estación esté enviando un mensaje al mismo tiempo, frenará la transmisión e intentará enviarlo hasta que el canal esté desocupado. Si se cae el maestro otra estación lleva a cabo sus funciones. Este método de acceso es usado comúnmente cuando el tráfico no es muy pesado y son pocas las estaciones, ya que en caso contrario se alenta el proceso. Lo utiliza Ethernet.

CSU — Channel Service Unit. Ver Unidad de servicio de canal.

DEC — Digital Equipment Corporation. Organización que fabrica equipo de cómputo. Desarrolló el protocolo DECnet.

DECnet — Digital Equipment Corporation Network. Protocolo desarrollado por la empresa DEC para comunicar equipos diferentes de ella misma, incluso computadoras personales.

Detección de errores — Chequeo para asegurar la correcta transmisión y recepción de un mensaje.

Dispositivo — Modifica las señales para hacerlas indescifrables durante la transmisión en

para encriptar la red. Se debe utilizar un dispositivo adecuado para desencriptar en la localidad receptora para almacenar la señal original.

DLCI Data Link Connection Identifier. Identificador del circuito virtual permanente.

DoD Departamento de Defensa de Estados Unidos.

DQDB Distributed Queue Dual Bus. Protocolo estándar del IEEE 802.6 para las MAN que provee servicios integrados de voz, datos y video sobre una ciudad grande. Fue adoptado en 1990.

DSU Data Service Unit. Ver Unidad de servicio de datos.

E1 En el TDM digital usado fuera de Norte América y Asia, se utiliza este tipo de enlace de 2.048 Mbps multiplexando 30 canales de voz o datos en 64 Kbps cada uno (E0); lleva 8 bits por cada uno de los 30 canales de voz o datos más 8 bits para señalización y otros 8 bits para sincronización. Por lo tanto, comprende 256 bits; 8000 E1s por segundo.

EBCDIC Extended Binary Coded Decimal Interchange Code. Código de Intercambio Decimal Codificado Binario Extendido que se usa en los sistemas 360/370 de IBM y en la mayoría de los equipos grandes. Tiene 256 combinaciones válidas de caracteres. Dentro de sus funciones se tienen el control de los dispositivos, la representación de los datos y el control de los protocolos.

EDI Electronic Data Interchange. Medio electrónico para transmitir transacciones de negocios entre organizaciones.

EIA Electronica Industries Association. Asociación de industrias electrónicas que ha establecido estándares de comunicaciones. Ver RS-232-C.

Enlace digital de alta velocidad Establecimiento de un canal de 2.048 Mbps punto a punto para la transmisión de señales de información como voz, datos e imágenes. Permite la optimización y racionalización de las comunicaciones al facilitar la administración de su capacidad ya que puede modularse de acuerdo a las necesidades de cada usuario, pudiendo manejar desde 30 comunicaciones de voz de 64 Kb/s hasta 240 con voz comprimida, así como 30 de datos también de 64 Kb/s hasta 180 de 9.6 Kb/s o las combinaciones de ambas modalidades.

Enlaces virtuales Permite ofrecer a los usuarios de la RDSI enlaces semipermanentes conmutados de 64 Kb/s punto a punto bajo demanda previa y por tiempo determinado, mediante simples comandos en el centro de control de la red.

Ensamblador y desensamblador de paquetes También conocido como PAD. Tipo específico de convertidor de protocolo diseñado para usarse en redes de conmutación de paquetes. Le da el formato específico requerido por la red de paquetes y los arregla de nuevo para uso local en la localidad receptora.

ETCD Equipo terminal de Circuitos de Datos (Data Circuit Terminating Equipment, DCE). Ver Modem.

ETD Equipo Terminal de Datos (Data Terminal Equipment, DTE). Ver Terminales.

Fase Punto al cual ha avanzado la onda en su ciclo. Una onda de fase generalmente

se describe en términos de grados, comenzando el ciclo en 0°, un cuarto de ciclo a los 90°, la mitad de ciclo 180°, tres cuartos de ciclo a los 270° y el ciclo completo a los 360°.

FDDI Fiber Distributed Data Interface. Protocolo estándar de ANSI con una velocidad rápida de 100 Mbps para interconectar MANs y equipo periférico usando como medio la fibra óptica. Se utiliza para el tráfico de paquetes de datos. Se basa en el token ring de IEEE 802.5.

FDM Frequency Division Multiplexing. Ver Multiplexado por división en frecuencia.

FDX Full Duplex. Ver transmisión dúplex completo.

Fibra óptica Son filamentos delgados de vidrio. Consiste en un cilindro delgado de vidrio rodeado de un nivel concéntrico de vidrio llamado revestimiento metálico. Emplean la luz como fuente de la señal. La luz es generada mediante diodos emisores de luz o láseres y se transmiten a través de un circuito cable transmisor de la luz hecho con un material parecido al vidrio. El emisor enciende y apaga la luz para representar los datos de usuario mediante el código binario. Comparada con los cables, tiene una mayor capacidad, es inmune a las interferencias eléctricas, son muy pequeñas y ligeras, es más segura. Las señales que lleva la fibra pueden transmitirse con una regeneración necesaria cada 100 kms. Hoy en día las redes la utilizan para proveer una regeneración de señales cada 35 km.

Frame relay Concepto más nuevo de conmutación de paquetes diseñado para maximizar el volumen transmitido por unidad de tiempo y minimizar los costos simplificando el procesamiento en la red. Sus velocidades de transmisión están en un rango que va de 64 kbps a 1.544 Mbps. Su campo dirección contiene un DLCI de 10-bits. Utiliza sólo las dos primeras capas del modelo OSI. La recomendación I.122 de la CCITT, de 1988, introdujo este protocolo; posteriormente, también la ANSI generó recomendaciones al respecto en su T1.606.

Frecuencia Número de ciclos u oscilaciones completas que la onda hace por segundo - esto es importante cuando se considera el grado de inclinación. El índice de frecuencia de una oscilación por segundo se define como hertz.

Front-End Ver Procesador de comunicaciones.

FTAM File Transfer Access Management. Protocolo de ISO para la administración del acceso de transferencia de archivos. Forma parte del conjunto de protocolos TCP/IP.

FTP File Transfer Protocol. Forma parte del conjunto de protocolos TCP/IP y se utiliza en la transferencia de archivos.

HDLC Norma publicada por ISO. Ámbito que engloba a muchos otros protocolos. Proporciona una gran variedad de funciones y cubre un amplio campo de aplicaciones. Protocolo que permite realizar transmisiones dúplex y semidúplex, configuraciones punto a punto o multipunto, y canales conmutados o no conmutados.

HDX Half Duplex. Ver transmisión semi-dúplex.

Host Cualquier dispositivo que esté conectado a la red, como una computadora, PC o terminal.

ICMP Internet Control Message Protocol. Protocolo para el control de mensajes de Internet. Forma parte del conjunto de protocolos TCP/IP.

IEEE Institute of Electronics and Electrical Engineers. Organización en los Estados Unidos conformada por Ingenieros Eléctricos y electrónicos que ha desarrollado estándares sobre arquitecturas para redes LAN y MAN. Creó el proyecto 802.

Inserción de registros Muchas redes en anillo utilizan este método para controlar el tráfico. Cada estación cuenta con un registro igual al tamaño máximo de datos usados en la red. También se cuenta con un buffer del mismo tamaño del registro. Los datos se almacenan en el registro: cada bit va ocupando una localidad de derecha a izquierda y el apuntador se va recorriendo hasta llegar a la primera localidad vacía; se envía cada bit al buffer de la siguiente estación, ésta identifica la dirección de destino y determina si necesita procesar los datos. En caso negativo, la estación comienza a transferir los bits a su registro para enviarlos a la siguiente estación del anillo. En caso afirmativo, la estación acepta los datos para procesarlos. Los datos pueden ser borrados del registro y removidos del anillo, o retransmitidos.

Intercambio de circuitos Método de control de acceso centralizado utilizado por las PBX para sistemas de telefonía convencional. Una estación que desea transmitir debe solicitar el establecimiento de una conexión, o circuito, con otra estación. La estación controladora central determina si puede hacerse la conexión. En caso afirmativo, se conectan físicamente las estaciones emisoras y receptoras. Pueden entonces transmitir mensajes en ambas direcciones, y el circuito que están usando permanece dedicado para su uso. Cuando las dos estaciones terminan su diálogo, son desconectadas y el circuito es liberado. Si la controladora central falla toda la red estrella falla.

IP Internet Protocol. Protocolo de administración de redes. Forma parte del conjunto de protocolos TCP/IP.

IPX/SPX Internet Packet Exchange/Sequenced Packet Exchange. Protocolo desarrollado por Novell, quien tiene el privilegio de ser la empresa con mayor número de sistemas operativos de red instalados en el mundo, por lo que está ampliamente extendido.

ISDN Integrated Services Digital Networks. Ver RDSI.

ISO International Standards Organization. Organización de estándares internacional formada en 1947 que publicó la norma HDLC. Ver OSI.

ITU International Telecommunication Union. Agencia de las Naciones Unidas que tiene bajo su dirección al CCITT. Ver CCITT.

LAN Local Area Network. Redes de área local. Ver IEEE.

Líneas de comunicación Son una conexión física. Son cables de comunicación, guías de onda o cables que conectan computadoras e otros sistemas y usuarios. Pueden ser utilizadas en redes privadas para uso individual, redes privadas compartidas, redes públicas limitadas, redes públicas nacionales y redes públicas internacionales. También se conocen como enlaces o canales.

LSI Large Scale Integration. Circuitería de integración a gran escala. Ver señal digital.

MAC Media Access Control. Esquema que define las condiciones bajo las cuales las estaciones de trabajo accesan al medio de transmisión: CSMA/CD, token passing, etcétera. Responsable de la comunicación libre de errores, especifica aspectos como tramado, dirección, detección de errores en los bits y reglas que gobiernan el acceso al medio.

Manchester Código usado generalmente para representar valores binarios. Requiere un ancho de banda el doble de grande que el de la transmisión. Permite al receptor extraer el sincronismo de las propias transiciones de la línea. Se emplea en las LAN.

Marcación directa entrante Servicio que permite que las extensiones del conmutador del usuario conectado a la RDSI puedan ser accesadas desde el exterior como un número directo sin necesidad de la intervención de la operadora.

Mbps Mega bits por segundo.

MCP Mac Convergence Protocol. Protocolo que tiene aplicación en el DQDB.

Medio físico Cualquier sustancia material que puede ser, o es usada para la propagación de señales, usualmente en la forma de radio modulada, luz u ondas acústicas de un punto a otro tales como fibras ópticas, cable, agua, aire o espacio libre.

Mensaje Cualquier información que contiene unidades de datos con un formato ordenado, enviada por medio de procesos de comunicaciones a una red conocida o una interface. Se compone de tres partes: Un encabezado, que contiene un indicador apropiado del principio del mensaje junto con parte de o toda la siguiente información: fuente, destino, fecha, hora, ruta; un cuerpo que contiene la información por comunicar; una parte terminal que contiene un indicador apropiado del fin del mensaje.

Microondas La transmisión se logra a través de torres de microondas generalmente espaciadas de 40 hasta 48 km. entre sí, evitando obstáculos como edificios o montañas para que la la transmisión no se vea afectada a través del aire. El sistema es un método de transmisión alineado con precisión (al receptor debe ver al transmisor). Cada torre toma la señal transmitida de la torre anterior, la amplifica y retransmite a la siguiente torre de microondas.

Modem La palabra modem es una abreviatura de modulador / demodulador. Es un dispositivo periférico que permite establecer comunicación entre dos dispositivos digitales. Este proceso consiste en codificar las señales digitales provenientes de una computadora emisora y convertirlas a señales analógicas para ser enviadas a través de un canal de transmisión. Cuando el modem recibe las señales analógicas, éstas son decodificadas en señales digitales para que los datos sean procesados por la computadora receptora. Las siglas utilizadas para hacer referencia a este equipo son ETCD. Su misión es conectar los equipos ETD a la línea o canal de comunicaciones.

Modulación Proceso en donde se alteran o modifican algunas características para transmitir información.

Multiplexado por división en frecuencia Conocido como FDM. Se llevan a cabo simultáneamente diferentes transmisiones sobre diferentes canales. Método que permite que un canal de comunicaciones sea compartido por varios usuarios asignando a cada uno una porción del espectro de frecuencia. Lo usan las comunicaciones analógicas.

Multiplexado Conocido como TDM. Se divide el acceso de un mismo canal para la transmisión

por división en el tiempo

de datos cuando múltiples dispositivos lo comparten. Provee a cada usuario de todo el espectro de frecuencia por periodos breves. Lo usan las comunicaciones digitales.

Multiplexor

Dispositivo que permite que varias terminales o puertos compartan una misma línea de comunicación, por lo general un canal telefónico. Transmite y recibe mensajes y controla las líneas de comunicación permitiendo el acceso a múltiples usuarios al sistema. También liga varias líneas de baja velocidad a una línea de alta velocidad para aumentar las capacidades de transmisión, permite reducir de forma sustancial el número de canales de comunicación necesarios. Existe multiplexado por división en el tiempo y por división en frecuencia.

NASA

National Aeronautic Space Administration.

Net BIOS

Network Basic Input Output System. Desarrollado por IBM. Protocolo genérico de red ya que es compatible con muchos sistemas operativos.

NFS

National Science Foundation.

Nodo

Dispositivo de intercambio.

OCU

Unidad de canal situada en la central de la red.

OSI

Open Systems Interconnect. Modelo de referencia de interconexión de sistemas abiertos desarrollado por la ISO para la construcción modular de software para comunicaciones de datos y sirve como una guía funcional para comunicación universal de computadoras. Se compone de siete niveles: aplicación, presentación, sesión, transporte, red, enlace y físico.

PABX

Private Automatic Branch Exchange. Centrales automáticas privadas de comunicación. Ver Centrales Privadas de Comunicación.

PAD

Packet Assembler/Disassembler. Ver Ensamblador y desensamblador de paquetes.

PBX

Private Branch Exchange. Ver Centrales Privadas de Comunicación.

PLCP

Physical Layer Convergence Protocol. Protocolo que tiene aplicación en el DQDB.

Polling

Conocido como bajada múltiple. Método de control de acceso centralizado comúnmente usado en la topología de estrella, ya que se requiere de una estación maestra para controlar la transmisión. Esta estación maestra pregunta a cada una de las estaciones si tiene algún mensaje que enviar. En caso afirmativo, el mensaje es leído y transmitido a la estación correspondiente, en caso contrario, se le pregunta a la siguiente estación. De esta manera, se logra que una estación no interfiera en la comunicación de otra. Su implementación resulta simple y con bajo costo. Sin embargo, la estación maestra debe ser compleja y si ésta falla, falla toda la red. También el hecho de enviar dos veces el mensaje, primero a la estación maestra y luego a la estación receptora, puede incrementar las demoras en la transmisión.

Procesador central

También conocido como CPU. Dispositivo compuesto de circuitos electrónicos, controles para el hardware, una unidad lógica aritmética y memoria principal. Implementa todas las funciones de telecomunicaciones desde el nivel de red hasta el nivel de aplicación.

Procesador de comunicaciones

También llamado controlador de comunicaciones o Front-End. Conecta todas las líneas de comunicación de una red a una computadora central para liberarla de ciertas tareas en el proceso de las comunicaciones tales como controles de línea sobre la red, tareas sobre mensajes y funciones de conversión necesarias para la transmisión de datos entre el host de la computadora y una red que empaque datos.

Protocolo

Conjunto de convenciones y reglas para el formato y contenido de datos para ser cambiados entre dos o más dispositivos. En las redes de datos, estas reglas involucran un conjunto de acuerdos (algunas veces basados en estándares internacionales) que pueden cubrir sintaxis, semántica y tiempo. Dentro de los protocolos se tienen: Frame relay, TCP/IP, FDDI, DQDB, HDLC, CMIP, MCP, TTP, SDLC, DECnet y Net Bios entre otros.

Proyecto 802

Conjunto de estándares sobre arquitecturas para redes de área local desarrollado por el IEEE. Se refiere sólo a los niveles más bajos, el nivel físico y el nivel de enlace. Este último está dividido en enlace lógico y control de acceso a los medios.

Puentes

Dispositivo para interconectar LANs similares u homogéneas punto a punto. Su función consiste en la lectura-traslado de dirección. Identifican la fuente y dirección del destino del paquete de datos. Cuando la dirección corresponde a una estación de la red remota, envía el paquete y cuando corresponde a una estación de la red local, lo filtra.

Radio digital

Terminología utilizada en RDI para establecer una comunicación por microondas de señales digitales específicamente de canales E1.

RBOCs

Regional Bell Operating Companies. Compañías telefónicas que proveen servicios locales de telecomunicaciones. Están activas en el proceso de estándares.

RDSI

Red Digital de Servicios Integrados conformada por la red terrestre, la satelital y la de paquetes. Sus siglas en inglés son ISDN. Proporciona un acceso y servicios digitales integrados de voz, video, imagen y transporte de datos. Requiere una MAN o WAN.

Red privada de voz y datos

Permite integrar las funciones que una empresa lleva a cabo en diferentes localidades mediante los servicios de la RDSI, los cuales ofrecen una conectividad total para domicilios y ciudades.

Red privada metropolitana

Capacidad de interconectar a través de la RDSI todas las ubicaciones de un cliente en una misma ciudad con las facilidades y servicios de una red privada, con enlaces de muy alta calidad y velocidad que permiten la administración adecuada de los recursos de la empresa y con la tecnología digital, la utilización de diversas modalidades de transmisión como voz, datos e imagen como si fuera un solo edificio, optimizando la operación diaria.

Red satelital

Suministra servicios digitales de RDSI a aquellas empresas que se encuentran localizadas en ciudades donde no se cuenta con infraestructura terrestre digital.

Red de paquetes de datos

La RDSI permite la transferencia electrónica de datos, el acceso a bases de datos (videotexto) y el uso de correo electrónico entre empresas e instituciones eficientando su operación.

Red global

Permite la formación de redes de alta capacidad de tecnología digital con

funciones y facilidades asociadas a una red privada y con alcances internacionales, enlazando localidades de diversos países para el establecimiento de comunicaciones efectivas y competitivas.

Repetidores Dispositivos que permiten la regeneración periódica de la señal digital. Se colocan a lo largo del canal a intervalos definidos. Su separación depende de la calidad y tamaño del conductor, de la cantidad de ruido presente en el conductor, de su ancho de banda y de la velocidad de transmisión en baudios. En los primeros sistemas digitales se empleaban separaciones de 1,800 metros. En la actualidad, los canales de fibra óptica permiten transmitir de forma fiable con repetidores separados entre 35 y 55 kilómetros.

RS-232-C Estándar de la EIA que suele emplearse para conectar los ETD y los ETCD. La C comprendida en la denominación se refiere a la cuarta versión que fue aprobada en 1981.

Ruteadores Dispositivo similar a un puente pero está diseñado para redes que usen diferentes direcciones de nivel MAC. Actúa como un switch entre varias LANs. Pueden escoger el camino más conveniente para la comunicación entre dos nodos considerando factores como tiempo, costo, distancia, etcétera.

Satélite Proporciona una forma especial de transmisión de relevo de microondas. Es una torre de microondas colocada a muchos kilómetros de altitud sobre la superficie de la tierra, generalmente sobre el Ecuador. De esta manera puede retransmitir señales a distancias mayores que las posibles sobre la superficie terrestre debido a que la curvatura, montañas y otros obstáculos de la tierra bloquean la transmisión de microondas sobre líneas visuales entre las torres terrestres. Al igual que las microondas sus señales pueden verse afectadas por el clima.

SDLC Protocolo de IBM del ámbito HDLC. Utiliza varias opciones del HDLC. Usa el modo de respuesta normal no equilibrado. Emplea bastantes comandos que no aparecen en ninguna norma ni sistema HDLC. Sus comandos y respuestas permiten establecer una topología en bucle. Por lo tanto, puede manejar configuraciones punto a punto, multipunto o en anillo.

Señal digital Señal eléctrica de pulsos discretos. En comunicaciones de datos los pulsos se codifican para representar información (1's y 0's). Es continua, se repite a sí misma, tiene carácter periódico y presenta cambios muy abruptos en su voltaje. Los sistemas digitales se basan en LSI, de gran robustez y fiabilidad.

Señal portadora Señal osciladora para transmitir información si se altera la amplitud o se interrumpa el voltaje de forma en que los pulsos correspondan a algún código conocido. Es el voltaje oscilatorio continuo.

Señal analógica Onda de forma continua compuesta de ondas sinusoides. Cada onda sinusoide tiene las siguientes características: amplitud, frecuencia y fase.

Servidor dedicado Al ejecutarse un programa únicamente desempeña una función especial.

Servidor no dedicado Desempeña una función especial y se utiliza como estación de trabajo.

Servidor También conocido como server. Es un dispositivo que proporciona una función especial a todos los usuarios de la red. Existen servidoras de: archivos, de impresión, de bases de datos y de comunicaciones. De acuerdo a la función que desempeñan se clasifican en dedicados, no dedicados y de redes.

Servidor de comunicaciones Equipo dedicado a atender las comunicaciones entre estaciones de trabajo remotas y los demás dispositivos de la red.

Servidor de impresión Controla las colas de impresión y da acceso a la o las impresoras conectadas a él.

Servidor de archivos Provee área de almacenamiento y acceso a programas y archivos de datos compartidos.

Servidores de redes Desempeñan eficientemente varias funciones de servidores a la vez.

SIP SMDS Interface Protocol. Protocolo de interface del SMDS que consta de tres niveles. Define el acceso del cliente a la red, la estructura del paquete, la dirección, control de error y transporte de datos.

Slots Transmisiones de longitud fija.

Slotted Ring Método de control de acceso aleatorio que permite que las estaciones de una red en anillo continuamente envíen varios slots, de una estación a la siguiente. Cada slot tiene una marca al principio que indica si está vacío o contiene datos. Si una estación tiene un mensaje para transmitir, espera un slot vacío, cambia la marca, inserta la dirección de destino, agrega el mensaje en el slot y lo transmite a la siguiente estación del anillo. Cuando una estación reciba el slot que contenga los datos debe chacar la dirección de destino para ver si debe procesar el mensaje. En caso afirmativo, la estación acepta los datos y retransmite el slot a la siguiente estación del anillo. Cuando el mensaje regresa al emisor original, éste debe quitar el mensaje del anillo y transmitir un slot vacío. Con este método, una estación no puede transmitir en cualquier momento; debe esperar hasta que reciba un slot vacío.

SMDS Switched Multi-megabit Data Service. Es un servicio usado en las MANs. Estándares para la interface de usuario, estructuras de servicio, componentes de red, administración de red. Define servicios de paquetes de alta velocidad a través de un enlace dedicado.

SMTP Simple Mail Tranefer Protocol. Protocolo para la transferencia de correo electrónico.

SNA Systems Network Architecture. Arquitectura para sistemas de red propiedad de IBM que describe la estructura lógica, formatos, protocolos y secuencias operacionales para transmitir unidades de información y controla la configuración de redes. Comprende 7 niveles: servicio de transacción, servicio de presentación, control de flujo de datos, control de transmisión, control de ruta, control de enlace y control físico.

SNMP Simple Network Management Protocol. Protocolo de administración de redes. Forma parte del conjunto de protocolos TCP/IP.

SONET Synchronous Optical Network. Estándar de ANSI descrito en ANS T1.105 y T1.106. Define un estándar internacional para formatos de paquetes a alta velocidad en sistemas de transmisión con fibra óptica. Describe una red de transporte. Desea encontrar aplicaciones en SMDS, B-ISDN y FDDI.

Tarjeta Ethernet Combina el método de acceso Carrier-Sense Multiple Access/Collision Detection (CSMA-CD) y la topología de bus; trabaja a una velocidad de transmisión de 10 Mbits/seg. Se Pueden utilizar para su conexión los cables de par trenzado,

cable coaxial de doble blindaje y la fibra óptica. El tipo de tarjeta Ethernet depende del procesador que utilice la microcomputadora donde se va a instalar. Tiene un costo relativamente bajo y puede conectar equipos grandes.

Tarjeta Arcnet Utiliza una topología de árbol, método de acceso Token-Passing y transmite a una velocidad de 2.5 Mbits/seg. Utiliza cable coaxial y requiere que en cada rama del árbol se conecten repetidoras para mantener la señal en una intensidad adecuada. Fue creada por Data Point Corporation. A la fecha es la tarjeta más utilizada en el mundo. Tiene una gran flexibilidad en el cableado, lo que le permite en el caso de redes grandes, formar redes pequeñas, de 20 nodos, que se unen mediante puentes. Sin embargo, es baja su velocidad de transmisión y no se encuentra avalada por ninguna institución de estándares.

Tarjeta Token-ring Combina la topología de anillo con el método Token-Passing y transmite a velocidades desde 4 hasta 16 Mbits/seg. Fue creado por IBM. Es más conveniente que la Ethernet por su mayor alcance, sin embargo su instalación y mantenimiento son más complicados. Su rendimiento no se degrada al aumentar el número de nodos de la red. Sin embargo, su costo es considerablemente alto, así como el de las adiciones de equipo y de programas de comunicación requeridos para su operación.

Tarjeta de red Adaptador de red a la que se conectan los cables que unen las estaciones de trabajo con los servidores. Controla las comunicaciones de la estación de trabajo con los demás puntos de la red.

TCP/IP Transmission Control Protocol/Internet Protocol. Conocido también como Internet Protocol Suite. Protocolo desarrollado por el DoD y mejorado por el NFS y la NASA. Conjunto de protocolos que se utilizan en la Internet y se ha generalizado para la interconexión de redes heterogéneas: SNMP, IP, ARP, ICMP, FTAM, FTP.

TDM Time Division Multiplexing. Ver Multiplexado por división en el tiempo.

TDMA Time-Division Multiple Access. Método de control de acceso centralizado en redes de estructura lineal. Cada estación en el bus tiene un tiempo específico para transmitir. Si una estación no tiene nada que transmitir durante ese tiempo, ese tiempo de transmisión se asigna como no usado. El ciclo empieza por una estación maestra que envía un mensaje de tiempo con su prioridad. Cada estación se sincroniza con la estación maestra y transmite cuando le llegue su turno. Si se cae la estación maestra se cae toda la red, por lo que se requiere tener una estación maestra adicional.

Telefonía de alta calidad Permite suministrar los servicios de RDSI, en los polos de desarrollo turístico e industrial donde no se cuenta aun con infraestructura digital y se requiere proporcionar en corto plazo.

Terminales Dispositivos de entrada y salida, equipos en una red capaz de recibir o enviar la información transmitida por las líneas de comunicación. Incluyen terminales teletipo, terminales de video, estaciones de trabajo remotas, terminales de transacción y terminales inteligentes. Las siglas DTD suelen emplearse en forma genérica para aludir a la máquina que emplea el usuario final.

Token Ring Utiliza el token passing en una topología de anillo.

Token Passing Método de control de acceso distribuido que funciona por medio de una señal especial que circula por la red conocida como "token". Una estación puede enviar la información cuando recibe el token marcándolo como ocupado. El token pasará por todas las estaciones hasta encontrar su destino y posteriormente,

regresará a la estación emisora para ser marcado como libre. Cuando una estación no tiene información que enviar, simplemente dejará pasar el token a la siguiente estación. Este método de acceso no se degrada si se aumentan el número de estaciones en la red. Se ha dividido en dos métodos de acceso: **Token Ring** y **Token Bus**.

Token Bus Utiliza el token passing en una topología lineal.

Token Mensaje particular o patrón de bits que significa permiso para transmitir.

Topología lógica Describe cómo opera la red lógicamente.

Topología Multipunto Un nodo puede recibir o enviar mensajes de o a varios nodos.

Topología física Describe la posición física de las estaciones y cómo son conectadas a otras estaciones.

Topología punto a punto Los mensajes que son enviados de un host a otro son transferidos en forma serial a cada uno de los nodos sobre la ruta entre los dos hosts.

Topología de Estrella También conocida como star. Cada estación está conectada directamente a un equipo central, generalmente el servidor de la red. Cuando un nodo desea comunicarse con otro nodo, el equipo central establece un circuito o una ruta dedicada entre los dos nodos. Tiene algunas desventajas como en el uso excesivo de cable y la dependencia que existe en caso de falla, del equipo que queda al centro de la red.

Topología Lineal También conocida como bus. Tanto los servidores como las estaciones de trabajo se conectan a un cable (o bus) que atraviesa la red. Es la más extendida de las topologías en las LAN por su flexibilidad y confiabilidad, ya que las fallas en un punto no tienen efecto en la operación global.

Topología de Anillo También conocida como ring. El cable pasa a través de cada estación y los servidores, hasta formar un anillo y en caso de falla de alguno de los nodos la operación de la red se suspende. Una estación al recibir un mensaje determina si lo acepta y procesa. Sin embargo, después de recibir el mensaje, cada estación actúa como un repetidor, retransmitiéndolo a su fuerza original.

TP Transport Protocol. Protocolo desarrollado por el CCITT.

Transceiver Adaptador o conector por el cual se conecta uno a la red para poder accesar a una red específica.

Transmisión síncrona Se utiliza para la transmisión de un bloque de caracteres y tanto el dispositivo emisor como el receptor, operan simultáneamente y se sincronizan. La sincronización se establece y mantiene cuando la línea está ociosa (no se están transmitiendo señales) o justo antes de la transmisión de una señal de datos.

Transmisión simplex La información se transmite sólo en una dirección y los papeles del transmisor y receptor están fijos. Un ejemplo de transmisión simplex lo constituye una campana de la puerta de una residencia. Esta transmisión no se utiliza en las redes de datos convencionales.

Transmisión semi-dúplex

También se le conoce como bidireccional alternada o HDX. Una estación transmite información a otra y al conducir la operación, se invierte la comunicación. En otras palabras, permite la transmisión en ambas direcciones pero sólo en una a la vez (alternada). Una conversación cortés en que ninguno de los datos participantes interrumpe al otro es un ejemplo de esta transmisión. Los sistemas de comunicaciones de datos que utilizan la red de comunicación telefónica de direccionamiento público por lo general transmiten en semi-dúplex.

Transmisión asíncrona

Transmisión en donde cada byte (carácter) de datos incluye señales de arranque y parada (o lo que es lo mismo, señales de sincronización) al principio y al final. La misión de estas señales consiste, en primer lugar, en avisar al receptor de que está llegando un dato, y en segundo lugar, darle tiempo suficiente para realizar algunas funciones de sincronismo antes de que llegue el siguiente byte. Los bits de arranque y de parada en realidad no son otra cosa que señales específicas y únicas que el dispositivo receptor es capaz de reconocer. Esta transmisión comúnmente se aplica para índices de datos bajo 19.2 kbps y por la mayoría de las terminales ASCII.

Transmisión dúplex completo

También llamada bidireccional simultánea o FDX. Ambas estaciones pueden transmitir y recibir simultáneamente. La información puede fluir por las líneas en ambas direcciones a la vez. Una discusión en que ambos participantes hablan a la vez es un ejemplo de esta transmisión.

Transmisión

Envío de una señal o un mensaje a través de un medio (radio, telégrafo, teléfono, fax u otro medio). Serie de caracteres, mensajes o bloques que incluyen control de información y datos del usuario; señalización de datos sobre canales de comunicación.

TTP

Timed-Token Protocol. Protocolo que tiene aplicación en el FDDI.

Unidad de servicio de canal

Sus siglas en inglés son CSU. Se ocupa de aspectos como el acondicionamiento de la línea (ecualización), con el fin de mantener constantes las características del canal en todo el ancho de banda, la regeneración de la señal mediante la cual se construye la corriente de pulsos binarios y verificación del bucle de retorno que incluye la transmisión de señales de prueba entre el CSU y la OCU. Permite la transmisión de señales digitales a través de un circuito digital. Protege la transmisión de la red previniendo al usuario final de conectar directamente a la línea de transmisión equipo que contenga fallas.

Unidad de servicio de datos

Sus siglas en inglés son DSU. Convierte las señales de datos procedentes de la terminal en señales digitales bipolares. Se encarga de la temporalización, la regeneración de la señal y la ecualización del canal.

V.24

Interface estándar editada por el organismo de normalización CCITT. Muchos productos se consideran compatibles con esta norma la cual incluye las definiciones de los canales (líneas) que unen los ETD y los ETCD. Las funciones que realiza son muy similares a las del RS-232-C. Están definidos más canales que en RS-232-C. Se considera que RS-232-C es un subconjunto de ella.

V.28

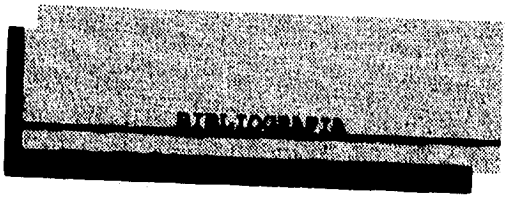
Interface que comprende funciones similares a las del RS-232-C. Editada por el CCITT. Las recomendaciones eléctricas para las interfaces no equilibradas entre ETD y ETCD están especificadas en esta norma. Los valores positivos mayores que +3 voltios comprenden la condición de activado (0) y los valores negativos menores que -3 voltios la condición de desactivado (1).

Videoconferencia

Capacidad de transmitir señales de video, interactivo y en diversas localidades a través de enlaces de la RDSI, estableciendo una comunicación efectiva y

dinámica que permite optimizar tiempo y costos de las empresas con aplicaciones como reuniones y juntas de trabajo, cursos de capacitación, comunicados al personal, distribución de información y su discusión inmediata, todo esto sin necesidad de traslados innecesarios, incrementando la productividad de la institución.

X.25 Protocolo a nivel de red establecido por el CCITT. Define las capacidades de servicio y las características que la red proporciona al usuario. La Red Pública de Transmisión de datos Telepac de la Secretaría de Comunicaciones y Transportes y algunas redes privadas han adoptado este protocolo de comunicaciones. Dentro de las funciones que realiza en la Interface Usuario/Red se encuentran en el **Nivel 1** la sincronización, en el **Nivel 2** la detección de errores y en el **Nivel 3** el establecimiento y liberación de canal.



BLACK, Uyless: Computer Networks Protocols, Standards and Interfaces, New Jersey, Prentice Hall, 1987.

CONNECTIVITY, REFERENCE GUIDE, Bridges, Routers and Gateways, U.S.A., Compaq Computer Corporation, 1990.

COOK, John William y WINKLE, Gary M.: Auditoría: Filosofía y técnica, 3ª ed., México D.F., Interamericana, 1988.

ECHENIQUE GARCIA, José Antonio: Auditoría en Informática, 1ª ed., México D.F., McGraw-Hill/Interamericana de México, S.A. de C.V., 1991.

ESTRATEGIAS TECNOLÓGICAS EN REDES LOCALES, Resumen de conferencias, México, NOVELLCO, 1990.

FITZGERALD, Jerry y EASON, Tom S.: Fundamentos de comunicación de datos, 1ª ed., México D.F., Limusa, 1989.

HEWLETT-PACKARD: Multivendor Network Management, U.S.A., 1989.

INTERSYS: Excelencia en conectividad integrada, México, NOVELL Latino América, 1993.

INTRODUCTION TO TELECOMMUNICATIONS, 2-day course, U.S.A., Price Waterhouse, October 22 and 23, 1991.

KEEN, Peter G. W. y CUMMINS, J. Michael: Business Choices and Telecommunications Decisions, Belmont California, Wadsworth Publishing Co., 1994.

KESSLER, Gary C. y TRAIN, David A.: Metropolitan Area Networks: Concepts, Standards, and Services, U.S.A., McGraw-Hill, 1992.

LINDBERG, Roy A. y COHN, Theodore: Auditoría de Operaciones, México, D.F., Técnica S.A., 1981.

MADRON, Thomas William: Local Area Networks: The Second Generation, New York, John Wiley & Sons, Inc, 1988.

MARTIN, James Thomas: Data Communication Technology, New Jersey, Prentice Hall, 1988.

MARTIN, James Thomas y KAVENAGH, Kathleen: Local Area Networks: Architectures and Implementations, New Jersey, Prentice Hall, 1989.

MILLER, Mark A.: Lan Troubleshooting Handbook, U.S.A., M & T Books, 1989.

MOELLER, Robert: Computer Audit, Control and Security, New York, John Wiley & Sons, Inc., 1990.

MURPHY, Michael A. y PARKER, X. L.: Handbook of EDP Auditing, Boston, Ma., Parker, Warren, Gorham & Lamont, Inc., 1989.

NOVELL NETWARE PRACTICE AID, Draft, U.S.A., Price Waterhouse, June 28, 1990.

PRIETO, Espinosa Alberto, LLORIS, Antonio y TORRES, Juan Carlos: Introducción a la Informática, 1ª ed., Madrid, McGraw-Hill/Interamericana de España, S.A., 1989.

REDES 90, Documento de Seminario, México D.F, UNAM-COMPER, 1990.

SANDERS, Donald H.: Informática: presente y futuro, 2ª ed., México D.F., McGraw-Hill/Interamericana de México, S.A. de C.V., 1990.

SERIE DE GUIAS DE AUDITORIA, Guía complementaria, Sistemas de información computarizados, México D.F., Price Waterhouse, 1991.

SYSTEMS AUDITABILITY AND CONTROL, Module 8, Telecommunications, Price Waterhouse, U.S.A., The Institute of Internal Auditors Research Foundation, April 1991.

THE EDP AUDITORS FOUNDATION, INC: EDPAA CISA Review Manual, U.S.A., The Information Systems Control Association, 1995.

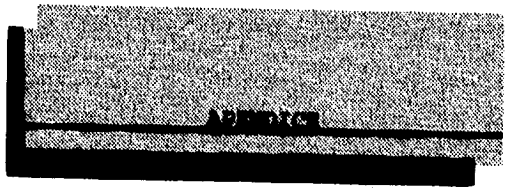
THE EDP AUDITOR JOURNAL: CONNECTIVITY, U.S.A., The Information Systems Control Foundation, Volume II, 1992.

THE EDP AUDITORS FOUNDATION, INC.: EDPAA 1992 Supplement CISA Review Manual, U.S.A., The Information Systems Control Association, 1992.

THE EDP AUDITOR JOURNAL: NOVELL, U.S.A., The Information Systems Control Foundation, Volume IV, 1992.

TYMNET INC.: Glossary, U.S.A., marzo 1990.

WEBER, Ron: EDP Auditing: Conceptual Foundations and Practice, 2ª ed., U.S.A., McGraw-Hill, 1988.



ANEXO 1

GUIA PARA LA PLANEACION ESTRATEGICA

COMPAÑIA: _____

UNIDAD OPERATIVA: _____

PREPARACION Y REVISION

	INICIALES Y FECHA
	Auditoria en Informática
Encargado	
Gerente	
Socio	

REUNION DE PLANEACION CON AUDITORIA EN INFORMATICA

Fecha:	
Participantes:	

ACTUALIZACION AÑO: _____

	INICIALES Y FECHA
	Auditoria en Informática
Encargado	
Gerente	
Socio	

ACTUALIZACION AÑO: _____

	INICIALES Y FECHA
	Auditoria en Informática
Encargado	
Gerente	
Socio	

ACTUALIZACION AÑO: _____

	INICIALES Y FECHA
	Auditoria en Informática
Encargado	
Gerente	
Socio	

RESUMEN DE INFORMACION PARA LA PLANEACION ESTRATEGICA	G1 Hoja 1

A2

CRONOGRAMA DE REVISIONES A CARGO DE AUDITORIA EN INFORMATICA

Tarea a desarrollar	Estimación de tiempo (horas de campo)	Fecha de revisión		
		19....	19....	19....

Continúa en ref.: ________

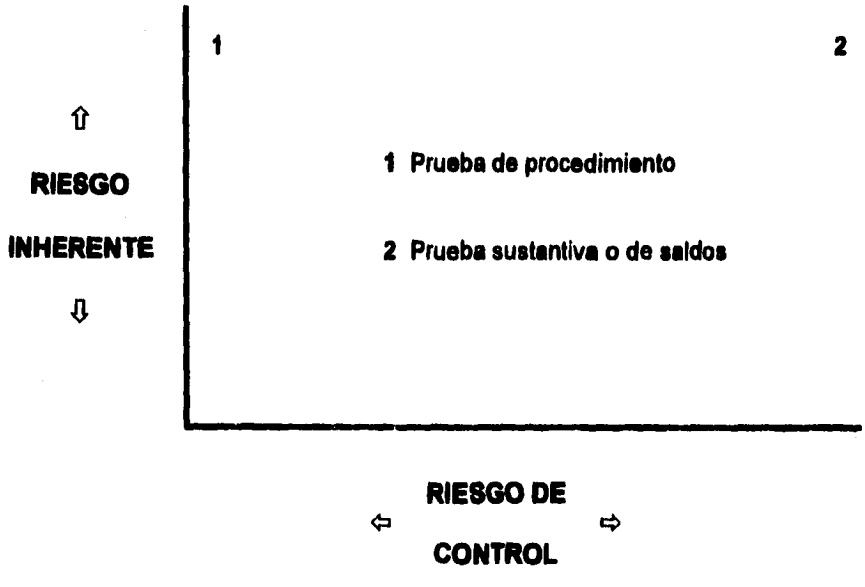
Gerente de Auditoría: ____________________ Fecha: ____________

Gerente de Auditoría en Informática ____________________ Fecha: ____________

Nota: Esta sección debe ser completada en oportunidad de la reunión de planeación con Auditoría en Informática..

A3

TABLA DE DECISION DE APLICACION DE PRUEBAS



RESUMEN DE INFORMACION PARA LA PLANEACION ESTRATEGICA	G1 Hoja 2

CONSIDERACIONES DE PLANEACION

Enfoque de auditoría esperado para los componentes individuales

Identificar los componentes importantes afectados por el uso de sistemas de información computarizados e indicar en qué medida el enfoque de auditoría esperado implica confianza en controles y/o funciones de procesamiento computarizados, o predominantemente procedimientos sustantivos (en este caso, indicar el uso esperado de técnicas de auditoría computarizadas).

COMPONENTE	ENFOQUE DE AUDITORIA ESPERADO

Continúa en ref.: _____

Participación de especialistas en Auditoría en Informática

Indicar la participación requerida de especialistas en Auditoría en Informática en las fases de planeación detallada y/o ejecución del examen. Completar el cronograma adjunto de revisiones.

Continúa en ref.: _____

Nota: Esta sección debe ser completada en oportunidad de la reunión de planeación con Auditoría en Informática.

RESUMEN DE INFORMACION PARA LA PLANEACION ESTRATEGICA	G1 Hoja 3

Resumir aquellos aspectos más importantes relativos a los sistemas de información de la compañía. Cuando sea apropiado, incluir referencias a las cédulas detalladas que respaldan las conclusiones.

Ambiente del sistema de información

¿Se han identificado cambios significativos (planeados o implantados) a los sistemas de información que puedan afectar el examen del año actual? (Considerar específicamente el impacto de los cambios efectuados sobre aplicaciones, planeadas o existentes, de técnicas de auditoría computarizadas).

Continúa en ref.: _____

Ambiente de control

Con base a la información obtenida, ¿ha implantado la Gerencia procedimientos adecuados para planear, supervisar y controlar las actividades del área de informática?.

Continúa en ref.: _____

Factores de riesgo inherente y de control

¿Se han identificado factores de riesgo inherente y de control relacionados con sistemas de información que deberían ser considerados al seleccionar el enfoque de auditoría para los componentes individuales?.

Sí ☐ No ☐

(Si la respuesta es Sí, detalle dichos factores en las hojas G1/5 y G1/6)

Nota: Este formulario debe completarse una vez recabada la información requerida por los formularios G2 o G5 y otra que se considere relevante.

RESUMEN DE INFORMACION PARA LA PLANEACION ESTRATEGICA	G1 Hoja 4

Otros temas

Enumerar a continuación otros temas identificados que deberían ser considerados por el Socio y Gerente:

Continúa en ref.: _____

¿En qué medida (y cómo) depende la compañía de sus sistemas de información?.

Continúa en ref.: _____

¿Se han identificado expectativas específicas del cliente relativas a sistemas de información que deberían ser consideradas por el Socio y el Gerente?.

Continúa en ref.: _____

Nota: Este formulario debe completarse una vez recabada la información requerida por los formularios G2 o G5 y otra que se considere relevante.

RESUMEN DE INFORMACION PARA LA PLANEACION ESTRATEGICA

G1
Hoja 5

Factores de riesgo inherente y de control (deben ser trasladados a las plantillas de decisiones preliminares para los componentes)

Ausencia de control	Areas afectadas	Lo que provoca o provocaría	Nivel de riesgo	
			I(1)	C(2)

(1): Riesgo inherente; (2): Riesgo de control; para ambos indique si el mismo es "A" = Alto, "M" = Medio, o "B" = Bajo.

(3): Referencia a los Papeles de Trabajo (P/T), si fuese necesario.

- Véase Tabla de controles generales del área de informática.

RESUMEN DE INFORMACION PARA LA PLANEACION ESTRATEGICA

G1
Hoja 6

Factores de riesgo inherente y de control (deben ser trasladados a las plantillas de decisiones preliminares para los componentes)

Ausencia de control	Areas afectadas	Lo que provoca o provocaría	Nivel de riesgo	
			I(1)	C(2)

(1): Riesgo inherente; (2): Riesgo de control; para ambos indique si el mismo es "A" = Alto, "M" = Medio, o "B" = Bajo.

(3): Referencia a los Papeles de Trabajo (P/T), si fuese necesario.

- Véase Tabla de controles generales del área de informática.

RESUMEN DEL PERSONAL DEL AREA DE INFORMATICA	G1 Hoja 7

Estructura organizativa

Confeccione o adjunte un organigrama general y uno por cada centro de procesamiento (planta) en el cual se procese información con significación de auditoría. Consigne el nombre de las personas responsables por las posiciones clave y la cantidad de personal a su cargo.

Continúa en ref.: _____

RESUMEN DEL PERSONAL DEL AREA DE INFORMATICA	G1 Hoja 8

Estructura organizativa

¿Ha habido cambios significativos en la estructura organizativa del área de informática?. Si ☐ No ☐

Comentarios: _____

_____

_____

_____

Continúa en ref.: _____

¿Es apropiada la dotación del área de informática, en el contexto de su tamaño y complejidad (Considerar tanto el número de personas como su capacidad profesional)?. Si ☐ No ☐

Comentarios: _____

_____

_____

Continúa en ref.: _____

¿Qué cambios anticipa en el futuro para la dirección, el personal, etc.?.

_____

_____

¿Se observa un alto nivel de rotación de personal en alguna de las áreas que integran el área de informática?. Si ☐ No ☐

Comentarios: _____

_____

_____

Continúa en ref.: _____

¿Existen indicios de una inadecuada separación de funciones en el área de informática?. Si ☐ No ☐

Comentarios: _____

_____

_____

Continúa en ref.: _____

ESTRUCTURA ORGANIZATIVA DE LAS OPERACIONES DEL AREA DE INFORMATICA

G2
Hoja 1

Gerencia y organización

¿Quién es el responsable de la administración del área de informática?.

¿De quién depende?.

¿Existe un Comité de Dirección (Steering Committe) a nivel gerencial? Si ☐ No ☐

De existir, indicar quiénes son sus miembros y responsable, de quién depende dicho comité, con qué frecuencia se reúne, cuáles son sus términos de referencia y cualquier otra información que se considere relevante.

Continúa en ref.: _____

En caso contrario, explicar cómo se efectúa el control gerencial de las actividades de procesamiento de datos.

Continúa en ref.: _____

¿Existe un plan maestro de sistemas u otro documento equivalente?. Si ☐ No ☐

De existir, describalo.

Continúa en ref.: _____

¿Se contempla un presupuesto anual para el área y cómo está integrado?.

Describa los proyectos principales del área que se llevarán a cabo este año.

ESTRUCTURA ORGANIZATIVA DE LAS OPERACIONES DEL AREA DE INFORMATICA	G2 Hoja 2

Gerencia y organización

¿Existen estándares (políticas y procedimientos) escritos relativos a la seguridad de datos, su administración y tiempo de existencia?. Sí ☐ No ☐

¿Quién es el responsable de la seguridad?.

Comentarios: _____

_____

_____

Continúa en ref.: _____

¿Se lleva a cabo algún análisis de riesgo formal o informal para el control de acceso de personas no autorizadas?. Sí ☐ No ☐

Comentarios: _____

_____

¿Existen estándares (normas y procedimientos) escritas para el desarrollo, prueba e implantación de sistemas?. Sí ☐ No ☐

Comentarios: _____

_____

_____

Continúa en ref.: _____

¿Existe una función de auditoría interna en informática (independiente del área de informática) que supervise los departamentos existentes?. Sí ☐ No ☐

De existir, ¿Qué departamentos se han auditado? y describa el alcance y resultados.

Comentarios: _____

_____

_____

Continúa en ref.: _____

ESTRUCTURA ORGANIZATIVA DE LAS OPERACIONES DEL AREA DE INFORMATICA	G2 Hoja 3

¿Cuál es el problema o riesgo más relevante que considera enfrenta cada uno de sus departamentos en su administración?.

Si Usted tuviera que cambiar una o dos situaciones que enfrenta la operación de su departamento, ¿cuáles cambiaría?.

¿Han detectado indicios de un inadecuado control gerencial de las actividades de procesamiento de datos?. Si ☐ No ☐

Comentarios:

Continúa en ref.: _____

Adquisición de hardware, software y servicios

¿Existen políticas y procedimientos estándares escritos para la adquisición de hardware y software?. Explique incluyendo las partes involucradas y los procesos de aprobación. Si ☐ No ☐

Comentarios:

Continúa en ref.: _____

¿Bajo qué circunstancias se requeriría una justificación formal para una adquisición?.

ESTRUCTURA ORGANIZATIVA DE LAS OPERACIONES DEL AREA DE INFORMATICA	G2 Hoja 4

¿Qué proceso existe para establecer especificaciones del producto y marcas?.

Continúa en ref.: _____

¿Cómo se les informa a los vendedores de las especificaciones y marcas requeridas?.

Si se requiere un análisis financiero (arrendamiento contra adquisición, periodo de pago), ¿quién lo lleva a cabo?.

¿Qué papel juegan los usuarios en la adquisición de los productos?.

¿Qué papel juega el auditor?.

¿Qué papel juegan los consultores?.

¿Existe alguna diferencia en los procedimientos para las adquisiciones de hardware, software y servicios?.

ESTRUCTURA ORGANIZATIVA DE LAS OPERACIONES DEL AREA DE INFORMATICA | **G2 Hoja 6**

¿Qué procedimientos lleva a cabo para realizar pruebas a los productos antes de la adquisición?. ¿Se prueban en PC's y se verifica que no contengan virus antes de ser instalados en el servidor de archivos?. ¿Son probados siempre con otros componentes del sistema?.

Continúa en ref.: _____

¿Cómo evalúa la seguridad del hardware y software de comunicaciones para el proceso de adquisición?.

¿Cómo se evalúa el proceso de adquisición?.

Otros aspectos de interés

Continúa en ref.: _____

Principales centros de procesamiento en el área de informática con significación de auditoria potencial (incluyendo servicios externos)

Continúa en ref.: _____

Nota: Para cada uno de estos centros, complete los formularios G3/1 y G1/7,8.

CONFIGURACION DEL AREA DE INFORMATICA	G3 Hoja 1

Centro de procesamiento del área de informática:

_____

Hardware
CPU (Proveedor y modelo). Interconexión con otras CPU's (indicar cuáles).

_____

Continúa en ref.: _____

Unidad de cinta: _____

Continúa en ref.: _____

Software de sistemas

Sistema(s) operativo(s) y versión(es): _____

Monitor(es) de teleprocesamiento y versión(es): _____

Editor(es) on line: _____

Lenguaje(s) de cuarta generación: _____

DBMS: _____

Software de administración de archivos: _____

Software de administración de bibliotecas: _____

Software de administración de cintas: _____

Software de seguridad: _____

Queries: _____

Otros: _____

_____

Continúa en ref.: _____

Nota: Procure indicar la arquitectura lógica (por máquina virtual/partición de memoria) del software instalado, a través de un diagrama general, siempre que sea aplicable.

Nota: Debe prepararse un formulario G3/1 para cada centro de procesamiento del área de informática en el cual se procese información significativa para los estados financieros.

CONFIGURACION DEL AREA DE INFORMATICA	G3 Hoja 2

Comunicaciones

Si los datos son transferidos electrónicamente entre distintas instalaciones de procesamiento y/o entre terminales remotas de entrada de datos e instalaciones de procesamiento, incluir un diagrama de la arquitectura de la red de comunicación de datos. Los medios de comunicación de datos (por ej.: líneas privadas (alquiladas), públicas (acceso por discado), de valor agregado (VAN), o locales (LAN)), modos, tipos y técnicas de transmisión, protocolos y métodos de acceso deben ser indicados en el diagrama, teniendo en cuenta que cada uno de ellos presenta distintos grados de riesgo de acceso no autorizado.

Continúa en ref.: _____

CONFIGURACION DEL AREA DE INFORMATICA	G3 Hoja 3

Ambiente de microcomputación

Hardware **Cantidad**

IBM o compatible (indicar modelo y capacidad).

_____ _____

_____ _____

_____ _____

_____ _____

Otros (especificar cuáles).

_____ _____

_____ _____

_____ _____

_____ _____

Continúa en ref.: _____

Software

No.Licencia

Sistema(s) operativo(s) y versión(es): _____ _____

Hoja(s) electrónica(s): _____ _____

Procesador(es) de palabras: _____ _____

DBMS: _____ _____

Utilerías: _____ _____

Software de seguridad _____ _____

_____ _____

_____ _____

_____ _____

_____ _____

Continúa en ref.: _____

Cambios significativos que se han presentado en el hardware y software.

_____

Continúa en ref.: _____

CONFIGURACION DEL AREA DE INFORMATICA	G3 Hoja 4

Ambiente de microcomputación

Conexiones microcomputadora-computadora central

Describir los mecanismos de conexión, el software utilizado, las habilidades de la conexión (downloading, uploading) y la principal información afectada.

Continúa en ref.: _____

Redes de microcomputadoras

Describir la configuración (hardware y software) de las redes de microcomputadoras utilizada para procesar aplicaciones con significación de auditoría.

Continúa en ref.: _____

CONFIGURACION DEL AREA DE INFORMATICA	G3 Hoja 5

Ambiente de microcomputación

Aplicaciones procesadas en microcomputadora

Detallar las aplicaciones (por ej., planillas electrónicas) con significación de auditoría procesadas en microcomputadora. Considerar la inclusión de visiones globales (Forma. G/4) de aquellas aplicaciones de especial relevancia.

Sector usuario	Nombre y propósito de la aplicación	Software utilizado

Continúa en ref.: _____

Otros aspectos de interés

Continúa en ref.: _____

APLICACIONES SIGNIFICATIVAS

G4
Hoja 1

Detallar a continuación las principales aplicaciones que respaldan a los componentes significativos. Adjuntar una visión global de cada una de las mismas.

Componente / Actividades del negocio	Aplicaciones que los respaldan	Ref. Sec. G4

Continúa en ref.: _____

APLICACIONES SIGNIFICATIVAS	G4 Hoja 2

Visión global del sistema de información

Adjuntar o transcribir un diagrama que ilustre la relación entre las aplicaciones que respaldan a los componentes significativos. Incluir referencias a las respectivas visiones globales.

Continúa en ref.: _____

APLICACIONES SIGNIFICATIVAS	G4 Hoja ___

APLICACION: _____

1. Propósito de la aplicación: _____

_____

_____

2. Aplicación desarrollada / adquirida: _____

3. Si se trata de software adquirido, nombre del proveedor y disponibilidad el código fuente:

_____

_____

4. Cambios desde la última planeación: _____

_____

_____

5. Trabajos recientes / planeados de auditoría interna: _____

_____

_____

6. Otras unidades operativas que usan la aplicación: _____

_____

_____

7. Acceso de terceros a funciones de la aplicación: _____

_____

_____

8. Volumen aproximado de transacciones: _____

_____

_____

9. Método de ingreso de datos: _____

_____

_____

APLICACIONES SIGNIFICATIVAS	G4 Hoja ___

APLICACION: _____

10. Método de actualización de archivos: _____

11.Organización de los archivos de la aplicación (de ser base de datos, identificar el DBMS):

12. Lenguaje de programación utilizado: _____

13. Tipo de procesamiento: _____

14. Interfases con otras aplicaciones: _____

15. Software de control de acceso: _____

16. Atributos de los programas: _____

17. Atributos de los archivos: _____

18. Otros temas de relevancia: _____

Continúa en ref.: _____

CUESTIONARIO COMPLEMENTARIO

G5
Hoja 1

Centro de Procesamiento del área de Informática: _____

	Atributo evaluado	Riesgo asociado			Evaluación inicial	Referencia formularios G1
		5	6	7		
1	Realiza el cliente trabajos de desarrollo de sistemas o de mantenimiento/cambios a los sistemas ya existentes.	*	*			
2	Se requieren soluciones rápidas en materia de sistemas de información como consecuencia de necesidades del negocio o presiones competitivas.	*	*			
3	Se recurre a personal de proveedores de software o a personal contratado para el desarrollo de sistemas/funciones de soporte técnico.			*		
4	Están los sistemas en desarrollo sujetos a revisiones de control y seguridad previas a su implantación.	*				

CUESTIONARIO COMPLEMENTARIO

G5 Hoja 2

Centro de Procesamiento del área de Informática: _____

	Atributo evaluado	Riesgo CIS asociado			Evaluación inicial	Referencia formularios G1
		5	6	7		
5	Existe una función de soporte técnico con la habilidad para mantener o modificar el software de sistemas o de comunicaciones.	*	*	*		
6	Se mantienen bibliotecas separadas de producción y desarrollo.		*	*		
7	Se han incorporado enmiendas al sistema operativo por parte del personal del cliente.		*			
8	Existe una función de control de redes u otra similar con responsabilidad sobre: a) Configuración e implantación de redes. b) Cambios al software de comunicaciones o tablas de control.	*	*			

CUESTIONARIO COMPLEMENTARIO

G5 Hoja 3

Centro de Procesamiento del área de Informática: _____

	Atributo evaluado	Riesgo CIS asociado			Evaluación inicial	Referencia formularios G1
		5	6	7		
9	Dependan las aplicaciones con significación de auditoría de la integridad o continuidad de otras aplicaciones.	*				
10	Se han realizado/planeado cambios de importancia al hardware o al sistema operativo.	*				
11	Ha tenido conocimiento de dificultades operativas relacionadas con la capacidad del equipo, tiempos de respuesta, tiempos de indisponibilidad, recuperación y reenganche, etc.	*				
12	Se utilizan facilidades de comunicación por medio de líneas telefónicas comunes (dial-up).			*		

CUESTIONARIO COMPLEMENTARIO

G5
Hoja 4

Centro de Procesamiento del área de Informática: _____

	Atributo evaluado	Riesgo asociado			Evaluación inicial	Referencia formularios G1
		5	6	7		
13	Existe algún disco (DASD) compartido.			-		
14	Se utilizan utilerías poderosas en los ambientes de producción o desarrollo.			-		
15	Es posible el acceso lógico por parte de terceros a alguna de las facilidades de procesamiento del cliente.			-		
16	Se utilizan técnicas de autenticación y/o encriptado para proteger datos sensitivos o transacciones bancarias.			-		

CUESTIONARIO COMPLEMENTARIO

G5
Hoja 5

Centro de Procesamiento del área de Informática: _____

	Atributo evaluado	Riesgo asociado			Evaluación inicial	Referencia formularios G1
		5	6	7		
17	Existe una función independiente de administración de seguridad.	*		*		
18	De tratarse de un banco, opera con redes compartidas con otras organizaciones (por ej., Redes de cajeros automáticos).			*		
19	Se ha desarrollado y probado un plan escrito de recuperación en caso de desastre.	*				

TABLA DE CONTROLES GENERALES DEL AREA DE INFORMATICA

FUNCION	RIESGO	MEDIO DE CONTROL
1. **Acceso a funciones de procesamiento de las transacciones o registros de datos resultantes.**	Personas no autorizadas pueden tener acceso a las funciones de procesamiento de transacciones de los programas de aplicaciones o archivos de datos resultantes, permitiéndoles leer, modificar, agregar o eliminar información.	• Segregación de funciones. • Control de acceso.
2. **Datos ingresados para su procesamiento.**	Los datos permanentes y de transacciones ingresados para su procesamiento pueden ser imprecisos, incompletos o ser ingresados más de una vez.	• Controles de edición y validación.
3. **Datos rechazados y partidas en suspenso.**	Los datos rechazados y las partidas en suspenso pueden no ser identificadas, analizadas y corregidas.	• Controles programados sobre partidas en suspenso. • Controles sobre partidas en suspenso. • Control sobre transacciones rechazadas.
4. **Procesamiento y registro de transacciones.**	Las transacciones reales que han sido ingresadas para su procesamiento o generadas por el sistema pueden perderse o ser procesadas o registradas en forma incompleta o inexacta o en el periodo contable incorrecto.	• Documentos fuente prenumerados. • Controles de sesión. • Controles por lotes. • Controles de balanceo programados. • Controles de rótulos internos de archivos. • Controles de transmisión de datos. • Procesos de reenganche y recuperación. • Controles de corte programados. • Controles sobre datos generados y cálculos programados. • Controles sobre extracción y presentación de información contenida en archivos magnéticos.

TABLA DE CONTROLES GENERALES DEL AREA DE INFORMATICA

FUNCION	RIESGO	MEDIO DE CONTROL
5. Estructura organizativa y procedimientos de operación del área de informática.	La estructura organizativa y los procedimientos operativos del área de informática no garantizan un ambiente de procesamiento de datos que conduzca a la preparación de información financiera confiable.	• Segregación de tareas en el área de informática. • Controles operativos del área de informática.
6. Procedimientos para cambios a programas.	Los programadores pueden realizar cambios incorrectos no autorizados en el software de aplicación, lo cual reducirá la confiabilidad de la información financiera procesada en el sistema.	• Controles sobre cambios a programas. • Enfoques alternativos.
7. Acceso general a los datos o programas de aplicación.	Personas no autorizadas pueden tener acceso directo a los archivos de datos o programas de aplicación utilizados para procesar transacciones, permitiéndoles realizar cambios no autorizados a los datos o programas.	• Software de control de acceso. • Registro de operaciones. • Controles basados en informes especiales para la gerencia. • Restricción del acceso físico.
8. Adquisición de hardware, software y servicios.	Incompatibilidad en los equipos. No satisfacen las necesidades del usuario. Instalación de software con virus.	• Políticas y procedimientos para la adquisición de hardware, software y servicios.

ANEXO 2

SUMARIO DE LA PRUEBA

Por favor complete esta hoja para sumarizar las áreas principales de interés durante la revisión de la red. Provea explicaciones completas y haga referencia a los papeles de trabajo en donde se requiera. Cada respuesta corresponde a una sección de la prueba de procedimientos.

1. ¿Resultan apropiados los controles de la administración de la red para poder depositar confianza en la integridad del proceso?.

2. ¿Resultan apropiados los controles de la operación de la red para poder depositar confianza en la integridad del proceso?.

3. ¿Resultan apropiados los controles del software de la red para poder depositar confianza en la integridad del proceso?.

4. ¿Resultan apropiados los controles de la distribución de las bases de datos en la red para poder depositar confianza en la integridad del proceso?.

Elaborado por: _____	Revisado por: _____
FECHA :__ / __ / __	

5. ¿Resultan apropiados los controles de la seguridad de los datos en la red para poder depositar confianza en la integridad del proceso?.

6. ¿Resultan apropiados los controles del correo electrónico usado en la red para poder depositar confianza en la integridad del proceso?.

7. ¿Resultan apropiados los controles de los servicios de consultores, asesores externos o proveedores en la red para poder depositar confianza en la integridad del proceso?.

8. ¿Resultan apropiados los controles de la contabilidad y cargos para los servicios de comunicaciones en la red para poder depositar confianza en la integridad del proceso?.

Elaborado por: _____	Revisado por: _____
Fecha :__ / __ / __	

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

1.0 ADMINISTRACION DE LA RED.

ARQUITECTURA.

1.1 ¿Se ha desarrollado para la arquitectura algún plan formal en los sistemas de comunicaciones?. ¿Se encuentran involucrados los auditores en este proceso?.

1.2 ¿Qué procesos existen para asegurarse que la arquitectura de los sistemas de comunicaciones (voz y datos) sustentan planes corporativos?.

DISEÑO.

1.3 ¿Cómo son identificadas y asignadas las tareas y responsabilidades dentro del departamento con respecto a las funciones de diseño, instalación y operación?.

1.4 ¿Se utiliza una metodología formal para el diseño de los sistemas de comunicaciones?. Describa.

¿Existe una metodología informal?. Describa.

1.5 ¿Existen algunas partes externas involucradas en el diseño o en el proceso de revisión del diseño (área de informática, personal de auditoría, vendedores o consultores)?. Explique.

1.6 ¿Qué papel juegan los usuarios en el proceso de diseño de la red?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

LEYES Y REGLAMENTOS SOBRE LA SEGURIDAD EN COMUNICACIONES.

1.7 ¿Cuál ha sido la intervención de los departamentos legales o de auditoría en la planeación de seguridad y administración de comunicaciones? ¿Se encuentra enterado de la existencia de algunas tareas legales o reglamentarias en relación a ellas?. Mencione algunas.

OPTIMIZACION DE LA RED INCLUYENDO EFECTIVIDAD Y EFICIENCIA.

1.8 ¿Con qué frecuencia se llevan a cabo los estudios de la optimización de la red y se comparan con el análisis de costo-beneficio?.

ADMINISTRACION DE CAMBIOS.

1.9 Existe algún proceso formal o informal para los cambios en comunicaciones (instalar una nueva terminal, cambiar la asignación de un puerto, modificar el código de un programa). Describa.

1.10 ¿Se lleva a cabo preliminarmente un análisis en un ambiente de prueba para asegurar el impacto de los cambios propuestos en el ambiente de producción?. Describa.

1.11 ¿Se llevan a cabo pruebas de "stress" para ver la actuación y confiabilidad de la red modificada?. ¿Se utilizan paquetes de software de vendedores para simular patrones de tráfico diferentes?. Describa.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

1.12 ¿Bajo qué circunstancias son permitidas las desviaciones de los procedimientos?.

1.13 ¿Qué asociación existe entre el proceso de cambios y el control de inventarios de comunicaciones?. ¿Se tiene automatizado y centralizado el proceso de control de inventarios?.

1.14 ¿Qué control se tiene sobre los cambios al sistema operativo?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

2.0 OPERACION DE LA RED.

REVISION DE LA RED ANTES DE SU IMPLEMENTACION.

2.1 ¿Se llevan a cabo revisiones de las facilidades de comunicaciones para asegurar la liberación de los servicios requeridos y la satisfacción del usuario?. Describa.

RESPALDO DE SOFTWARE Y HARDWARE.

2.2 ¿Con qué frecuencia realiza el respaldo del hardware y software usado en la red y cuántas copias se hacen?.

2.3 ¿En qué lugar se encuentran almacenadas?.

PLAN DE MANTENIMIENTO.

2.4 ¿Cada red principal cuenta con un plan de mantenimiento o un horario para asegurar una actuación óptima?. Describa los procedimientos para el mantenimiento de los sistemas de comunicaciones. ¿Cómo se inician las peticiones de mantenimiento?.

DETECCION AL DESCONECTARSE LOS DISPOSITIVOS.

2.5 ¿Cómo se detecta la desconexión de algún dispositivo de la red?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

DOCUMENTACION Y CAPACITACION AL USUARIO DE LA RED.

2.6 ¿Existe documentación actualizada de la configuración del software y hardware de la red?. ¿Cómo se provee y actualiza la documentación para el grupo de operaciones?.

2.7 Qué tipo de entrenamiento o capacitación se da al personal involucrado en la red?.

ACCESO A LAS OPERACIONES DE LA RED Y A LAS FACILIDADES DE PROCESO.

2.8 ¿Cómo se evita el acceso no autorizado a los programas y librerías del software de comunicaciones?.

2.9 ¿Cómo se previene, permite o detecta el acceso a la red?.

2.10 ¿Cómo se previene, permite o detecta que diferentes usuarios accesen al mismo tiempo a una misma aplicación?.

2.11 ¿Se cuenta con controles de acceso en los sistemas de aplicación usados en ella?.

2.12 ¿Cómo se reportan las violaciones?. ¿Quién revisa los reportes de violación?. ¿Qué acciones se llevan a cabo para investigar y seguir las violaciones?.

2.13 ¿Cuál es la estructura de los directorios usados en la red?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

SEGURIDAD AL MARCAR.

2.14 ¿Existen algunos controles especiales usados en el ambiente para marcar?.

2.15 ¿Qué dispositivos de seguridad en (dial-in), si existen, son usados?

2.16 ¿Qué controles se tienen sobre los números telefónicos a marcar?.

2.17 ¿Cómo monitorea la administración las violaciones de acceso para marcar?. ¿Qué tipos de reportes se generan?. ¿Qué acciones se llevan a cabo para investigar y darle seguimiento a las violaciones?.

CONMUTACION DE PAQUETES.

2.18 Describa los controles de acceso sobre las facilidades del intercambio de paquetes de datos.

2.19 ¿Con qué aspectos de seguridad de las redes públicas de datos (TYMNET o Telenet) cuenta para mantener la integridad y seguridad de los mismos?.

REVISION DE LA POST-IMPLEMENTACION DE LA RED (ESTRUC. Y ACTUACION).

2.20 ¿Se lleva a cabo una revisión de la post-implementación de la estructura y actuación de la red para asegurar que los controles se estén aplicando de manera adecuada y el monitoreo se está llevando correctamente?. ¿Utiliza algún software para monitoreo?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

2.21 ¿Existen definiciones de requerimientos de actuación y funciones documentadas para los servicios de voz y datos en las comunicaciones?. ¿Cuáles son los criterios de medición?.

2.22 ¿Se asignan prioridades a los procesos?.

2.23 ¿Cuenta el cliente con un UPS para prevenir la pérdida de datos y permitir una degradación paulatina?.

2.24 ¿Cuenta con procedimientos de recuperación en caso de desastre en la red?. Describa.

2.25 ¿Qué políticas se incluyen en el plan de contingencias?.

2.26 ¿Cada cuánto es probado y actualizado y quiénes intervienen?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

3.0 SOFTWARE DE LA RED.

3.1 ¿Su software de la comunicaciones cuenta con las siguientes facilidades?.

3.1.1 Identificación para enviar y recibir.

3.1.2 Chequeo sobre la dirección del mensaje.

3.1.3 Código de detección o corrección de errores para un índice de transmisión bajo en errores.

3.1.4 Reconocimiento positivo.

3.1.5 Conciliación periódica de mensajes.

3.2 ¿Se emite algún reporte de errores en la transmisión?.

3.3 ¿Se cuenta con procedimientos establecidos para la transmisión de datos?. Describa.

3.4 ¿Dichos procedimientos se basan en las políticas relevantes de la administración de la organización?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

4.0 DISTRIBUCION DE LAS BASES DE DATOS.

4.1 ¿Se ha clasificado la información (como sensitiva, crítica)?. En caso afirmativo, ¿cómo impactó esto para diseñar el acceso a la red?.

4.2 ¿Cómo se distribuye el contenido de las bases de datos entre los departamentos usuarios?.

4.3 ¿Se cuenta con un diccionario de datos?. ¿Cada cuánto se actualiza?.

4.4 ¿Se tiene algún procedimiento para efectuar cambios en los datos?. Describa.

4.5 ¿Cómo se evita, previene y detecta la duplicidad de datos?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

5.0 SEGURIDAD DE LOS DATOS EN LA RED.

5.1 ¿Los protocolos de la red cuentan con funciones automáticas para checar los errores asegurando la exactitud en la transmisión de los mensajes entre sus nodos?. ¿Emplea algunos de los siguientes controles en sus sistemas de comunicaciones para promover la integridad y calidad de los datos?.

5.1.1 Señales de tiempo y fecha.

5.1.2 Chequeo en la secuencia de los números.

5.1.3 Bitácora de transacciones.

5.1.4 Encriptamiento y desencriptamiento.

5.1.5 Código para la redundancia de llave.

5.2 ¿Con qué otros controles cuenta?. ¿Cómo se aplican?.

5.3 Describe las políticas, estándares y procedimientos documentados de seguridad física y lógica de la red.

5.4 ¿Qué precauciones se han tomado en los sitios con el host y las terminales remotas para proteger físicamente las comunicaciones del acceso no autorizado?

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

5.5 ¿Qué facilidades de conexión, reporte y vigilancia se tienen en el software de la red para proveer una auditoría adecuada de las actividades de la misma y alertar sobre accesos no autorizados?.

5.6 Describa algunos problemas de seguridad que hayan ocurrido en los últimos dos años y qué pasos se llevaron a cabo para corregirlos?.

5.7 ¿Existe alguna vulnerabilidad específica en la comunicación que no pueda preveer?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

6.0 CORREO ELECTRONICO.

6.1 ¿Cuenta con correo electrónico en su sistema de comunicaciones?.

6.2 ¿Qué control se tiene para mantener la privacidad en los datos manejados en él?.

6.3 ¿Qué control se tiene para detectar errores y omisiones en los datos?.

6.4 ¿Qué controles se tienen para asegurar la continuidad en sus operaciones?.

6.5 ¿Se cuenta con algún procedimiento para dar de alta y baja a los usuarios?. Describa.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

7.0 SERVICIO DE CONSULTORES, ASESORES EXTERNOS O PROVEEDORES.

7.1 ¿De cuál de los siguientes grupos depende para asesoría sobre la selección de productos, planeación estratégica y facilidades de operación y mantenimiento?.

7.1.1 Carriers.

7.1.2 Proveedores de servicios tales como VANs.

7.1.3 Vendedores de hardware para mainframe.

7.1.4 Otros vendedores de hardware.

7.1.5 Consultores.

7.1.6 Seminarios, conferencias.

7.2 ¿Existen otros servicios que ellos le provean?.

7.3 ¿Qué métodos utiliza para verificar la propuesta o información que obtenga de estas fuentes?.

7.4 ¿Existe algún contrato por la prestación de sus servicios?.

7.5 ¿Quién hizo el cableado de la red?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

7.6 Las áreas externas tienen acceso a:

- La red.
- Recursos del sistema.
- Software del sistema.
- Documentación.

7.7 ¿Qué controles existen sobre su acceso?.

7.8 ¿Qué controles existen para asegurar que las operaciones y mantenimiento recibidos por una parte externa son llevadas a cabo efectivamente?. ¿Qué criterios se utilizan para medir y en qué áreas?.

7.9 ¿Le proporcionan manuales de usuario bien documentados?.

7.10 ¿Se cuenta con un plan de recuperación por parte del usuario en caso de desastre en el proceso de datos cuando el consultor o asesor externo esté prestando su servicio?.

ADMINISTRACION DE LA RED DIGITAL DE SERVICIOS INTEGRADOS (RDSI) Y DE LOS RECURSOS DE COMUNICACIONES DE LOS USUARIOS.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

7.11 Si cuenta con la RDSI, ¿Cuál de los siguientes servicios utiliza en su organización y hasta qué punto?.

7.11.1 Acceso digital a un conmutador electrónico o digital.

7.11.2 Marcación directa.

7.11.3 Videoconferencia.

7.11.4 Enlace digital de alta velocidad.

7.11.5 Red privada metropolitana.

7.11.6 Cruce fronterizo.

7.11.7 Red global con comunicaciones internacionales.

7.11.8 Telefonía analógica de alta calidad.

7.11.9 Red privada de voz y datos.

7.11.10 Red de paquetes de datos.

7.11.11 Red satelital.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

7.12 ¿Se tiene por escrito las metas y beneficios a obtener con los servicios de la RDSI?.

7.13 ¿Cómo se evalúa su disponibilidad, confiabilidad y calidad?.

7.14 ¿Con qué procedimientos cuenta para el control de la administración de la RDSI y de los recursos de comunicaciones de los usuarios?.

7.15 ¿Se cuenta con medios de transmisión de respaldo?.

7.16 ¿Se emiten reportes de tráfico y consumo?.

ADMINISTRACION DE INTERCAMBIO DE DATOS ELECTRONICOS (EDI).

7.17 Si cuenta con el servicio de EDI, ¿Se tienen por escrito las metas y beneficios a obtener con él?.

7.18 ¿Qué departamentos estuvieron involucrados para el establecimiento del EDI?.

7.19 ¿Se cuenta con un contrato por la prestación del servicio de EDI?. Describa los términos y condiciones.

7.20 ¿Se cuenta con un registro de las transacciones?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

7.21 ¿Se tienen copias de los archivos de transacciones? ¿Por cuánto tiempo se conservan?.

7.22 ¿Se utiliza el encriptamiento y desencriptamiento de datos?. ¿Quién es el responsble de la administración de la llave?.

7.23 ¿Cuál es el índice de error aceptable en el proceso de transmisión?.

7.24 ¿Cómo se evalúa la disponibilidad del EDI en cuanto al tiempo de respuesta que ofrece?.

7.25 ¿Se cuenta con procedimientos para modificar o borrar registros de archivos?. Describa.

7.26 ¿Se cuenta con un control de autenticidad por niveles de mensajes?. Describa.

7.27 ¿Se lleva un control sobre la transmisión de mensajes?. Describa.

7.28 ¿Se lleva a cabo un mantenimiento acorde con el plan de recuperación en caso de desastre?.

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

7.29 ¿Se lleva a cabo una revisión de las actividades de los empleados del proveedor del servicio?.

7.30 ¿Qué controles se tienen sobre el acceso de los usuarios para el uso del EDI?.

7.31 ¿Qué controles se tienen sobre los cambios y llamadas a programas del EDI?.

7.32 ¿Qué controles se tienen sobre las transacciones de entrada y salida del sistema y el mantenimiento al archivo maestro?

PRUEBA DE PROCEDIMIENTOS PARA DETERMINAR LA EXISTENCIA DE CONTROLES ESPECIFICOS

8.0 CONTABILIDAD Y CARGOS PARA LOS SERVICIOS DE COMUNICACIONES.

8.1 ¿Los beneficios del Departamento de Telecomunicaciones son mayores a sus costos?.

SERVICIOS DE VOZ Y DATOS.

8.2 Por favor describa el sistema para la contabilidad y/o cargos de servicios de comunicaciones (voz y datos).

8.3 ¿Existe algún cargo adicional para llamadas automáticas o envíos de llamadas?.

8.4 ¿Qué pruebas de conformidad se llevan a cabo para cotejar el sistema de contabilidad con la facturación?.

8.5 ¿Venden Ustedes los servicios de comunicaciones a partes externas (otras divisiones de su organización y otra compañía) o planea hacerlo (servicios de arrendamiento). Por favor describa las circunstancias (servicios vendidos, a quién, precio, etc.)

8.6 ¿La venta de sus servicios somete a su organización a algún reglamento?. Por favor explique.

8.7 Utiliza el mismo sistema de contabilidad para la facturación a usuarios externos?.

Fecha: __ /__ /__

NOMBRE DE LA COMPAÑIA: _____

		DEFICIENCIA			
No. PREGUNTA	RESPUESTA	SI	NO	N/A	REF. EVIDENCIA

Elaborado por: _____ Revisado por: _____

ANEXO 3

FUNCION:	1. ADMINISTRACION DE LA RED	
REF.	**RIESGO**	**MEDIO DE CONTROL**
1.1	Se tienen bien definidos los componentes, topología, protocolos, métodos de acceso y controles adecuados para la organización.	Plan formal para la arquitectura de la red.
1.2	No se toman en cuenta las necesidades de proceso de datos de los usuarios de la red en diferentes localidades.	La arquitectura de la red sustentada en planes corporativos.
1.3	No se tienen identificados a los responsables de mantener los controles en la red.	Asignación de tareas y responsabilidades en la red.
	No se cuenta con los manuales de organización que se refieran a las actividades que pueden ser procesadas en la red.	
	No se han distribuido los manuales de procedimientos de operación de la red a los Departamentos Usuarios.	
1.4 1.5 1.6	No se puede hacer frente a las fallas por un mal diseño en la red, lo que ocasiona no haya continuidad en las operaciones.	Metodología para diseñar el sistema de comunicaciones.
1.7	No se es consistente con las leyes y regulaciones que gobiernan la transmisión de datos dentro del país, con las leyes internacionales y con la transmisión de datos transfrontera.	Conocimiento de leyes y reglamentos sobre la seguridad en comunicaciones.

REF.	RIESGO	MEDIO DE CONTROL
1.8	No se ha preparado adecuadamente el análisis de costo-beneficio por lo que no se han obtenido los resultados estimados.	Elaboración de un buen análisis de costo-beneficio.
	No son probados y evaluados periódicamente los recursos de la red.	Estudios de la optimización de la red.
	Se implementa un software o hardware que no es el adecuado para la red.	
1.9	Se puede instalar una nueva terminal o cambiar la asignación de un puerto y no funcionar correctamente la red por haber asignado una configuración errónea.	Procedimientos para administrar los cambios en comunicaciones.
1.10	El cambio da un impacto negativo en el ambiente de producción provocando que no funcione correctamente la red.	
1.11	Al modificar el hardware o software de la red, se puede degradar la velocidad y no soportar incrementos en las cargas de tráfico.	Pruebas de stress.
1.13	No se tiene conocimiento del equipo de comunicaciones con el que se cuenta por lo que no se puede asegurar todo.	Control de inventarios.

REF.	RIESGO	MEDIO DE CONTROL
1.8	No se ha preparado adecuadamente el análisis de costo-beneficio por lo que no se han obtenido los resultados estimados.	Elaboración de un buen análisis de costo-beneficio.
	No son probados y evaluados periódicamente los recursos de la red.	Estudios de la optimización de la red.
	Se implementa un software o hardware que no es el adecuado para la red.	
1.9	Se puede instalar una nueva terminal o cambiar la asignación de un puerto y no funcionar correctamente la red por haber asignado una configuración errónea.	Procedimientos para administrar los cambios en comunicaciones.
1.10	El cambio da un impacto negativo en el ambiente de producción provocando que no funcione correctamente la red.	
1.11	Al modificar el hardware o software de la red, se puede degradar la velocidad y no soportar incrementos en las cargas de tráfico.	Pruebas de stress.
1.13	No se tiene conocimiento del equipo de comunicaciones con el que se cuenta por lo que no se puede asegurar todo.	Control de inventarios.

REF.	RIESGO	MEDIO DE CONTROL
1.8	No se ha preparado adecuadamente el análisis de costo-beneficio por lo que no se han obtenido los resultados estimados.	Elaboración de un buen análisis de costo-beneficio.
	No son probados y evaluados periódicamente los recursos de la red.	Estudios de la optimización de la red.
	Se implementa un software o hardware que no es el adecuado para la red.	
1.9	Se puede instalar una nueva terminal o cambiar la asignación de un puerto y no funcionar correctamente la red por haber asignado una configuración errónea.	Procedimientos para administrar los cambios en comunicaciones.
1.10	El cambio da un impacto negativo en el ambiente de producción provocando que no funcione correctamente la red.	
1.11	Al modificar el hardware o software de la red, se puede degradar la velocidad y no soportar incrementos en las cargas de tráfico.	Pruebas de stress.
1.13	No se tiene conocimiento del equipo de comunicaciones con el que se cuenta por lo que no se puede asegurar todo.	Control de inventarios.

REF.	RIESGO	MEDIO DE CONTROL
1.8	No se ha preparado adecuadamente el análisis de costo-beneficio por lo que no se han obtenido los resultados estimados.	Elaboración de un buen análisis de costo-beneficio.
	No son probados y evaluados periódicamente los recursos de la red.	Estudios de la optimización de la red.
	Se implementa un software o hardware que no es el adecuado para la red.	
1.9	Se puede instalar una nueva terminal o cambiar la asignación de un puerto y no funcionar correctamente la red por haber asignado una configuración errónea.	Procedimientos para administrar los cambios en comunicaciones.
1.10	El cambio da un impacto negativo en el ambiente de producción provocando que no funcione correctamente la red.	
1.11	Al modificar el hardware o software de la red, se puede degradar la velocidad y no soportar incrementos en las cargas de tráfico.	Pruebas de stress.
1.13	No se tiene conocimiento del equipo de comunicaciones con el que se cuenta por lo que no se puede asegurar todo.	Control de inventarios.

REF.	RIESGO	MEDIO DE CONTROL
1.8	No se ha preparado adecuadamente el análisis de costo-beneficio por lo que no se han obtenido los resultados estimados.	Elaboración de un buen análisis de costo-beneficio.
	No son probados y evaluados periódicamente los recursos de la red.	Estudios de la optimización de la red.
	Se implementa un software o hardware que no es el adecuado para la red.	
1.9	Se puede instalar una nueva terminal o cambiar la asignación de un puerto y no funcionar correctamente la red por haber asignado una configuración errónea.	Procedimientos para administrar los cambios en comunicaciones.
1.10	El cambio da un impacto negativo en el ambiente de producción provocando que no funcione correctamente la red.	
1.11	Al modificar el hardware o software de la red, se puede degradar la velocidad y no soportar incrementos en las cargas de tráfico.	Pruebas de stress.
1.13	No se tiene conocimiento del equipo de comunicaciones con el que se cuenta por lo que no se puede asegurar todo.	Control de inventarios.

REF.	RIESGO	MEDIO DE CONTROL
1.8	No se ha preparado adecuadamente el análisis de costo-beneficio por lo que no se han obtenido los resultados estimados.	Elaboración de un buen análisis de costo-beneficio.
	No son probados y evaluados periódicamente los recursos de la red.	Estudios de la optimización de la red.
	Se implementa un software o hardware que no es el adecuado para la red.	
1.9	Se puede instalar una nueva terminal o cambiar la asignación de un puerto y no funcionar correctamente la red por haber asignado una configuración errónea.	Procedimientos para administrar los cambios en comunicaciones.
1.10	El cambio da un impacto negativo en el ambiente de producción provocando que no funcione correctamente la red.	
1.11	Al modificar el hardware o software de la red, se puede degradar la velocidad y no soportar incrementos en las cargas de tráfico.	Pruebas de stress.
1.13	No se tiene conocimiento del equipo de comunicaciones con el que se cuenta por lo que no se puede asegurar todo.	Control de inventarios.

REF.	RIESGO	MEDIO DE CONTROL
	No existe una relación de la identificación de los dispositivos lógicos y físicos usados en la red por lo que resulta difícil determinar la actualización de los manuales.	
1.14	El Departamento de Comunicaciones no tiene un control sobre los cambios al software de sistema operativo usado en la red por lo que pueden existir cambios no autorizados por miembros del departamento responsable de la administración de las operaciones de la misma.	Control sobre los cambios al sistema operativo.

FUNCION:	2. OPERACION DE LA RED.	
REF.	**RIESGO**	**MEDIO DE CONTROL**
2.1	No se apegan las facilidades de comunicaciones a los servicios requeridos y a las necesidades del usuario.	Procedimientos para una revisión de la red antes de su implementación.
	No se incluyen a todos los usuarios e interfaces en el plan de implementación.	
	No se identifican los riesgos asociados con la red.	Plan de implementación.
2.2 2.3	No se hacen respaldos diarios ni se cuenta con copias de ellos en sitios seguros que garanticen su uso oportuno cuando exista alguna interrupción en las operaciones de la red.	Control de respaldo del hardware y software usado en la red.
2.4	No se ha establecido la disponibilidad de la red lo que ocasiona problemas en el tiempo de respuesta, almacenamiento, respaldo, mantenimiento y requerimientos de proceso y operación para todas las aplicaciones.	Control sobre la administración de las operaciones de la red.
	No se cuenta con registros de mantenimiento por lo que no se conocen las fallas que ha presentado el equipo y si ha sido infectado de virus.	

REF.	RIESGO	MEDIO DE CONTROL
	No se da un mantenimiento adecuado al software de comunicaciones por lo que no se puede asegurar que los usuarios no hayan utilizado juegos o software no autorizado e infectado de virus la red.	Plan de mantenimiento.
	No se elaboran reportes de actuación general y de problemas de la red por lo que no se conoce su disponibilidad, adherencia a los horarios, tiempos de respuesta, eficiencia en los sitios de proceso y problemas de actuación.	
2.5	No se tienen establecidos procedimientos operacionales para el intercambio de hardware de telecomunicaciones para operaciones de respaldo de la red por lo que puede presentarse y no ser detectado por el software de comunicaciones.	Detección al desconectarse los dispositivos.
2.6	No existe o no se actualiza la documentación de las operaciones y los planes de capacitación por lo que las peticiones no son atendidas a tiempo bajo las bases establecidas.	Procedimientos para proveer una documentación adecuada y una suficiente capacitación al usuario de la red.
2.7	No existe una distribución de la documentación de operaciones o una capacitación adecuada a los departamentos que usan la red por lo que no pueden identificar y corregir problemas en la misma.	

REF.	RIESGO	MEDIO DE CONTROL
2.8 2.9 2.11	No se cuenta con procedimientos de seguridad establecidos por lo que personas no autorizadas tienen acceso a los sitios de proceso central o a las facilidades de la red, a las pruebas de hardware de la misma, a los programas y librerías del software de comunicaciones, a los sistemas de aplicación y a las líneas locales o privadas.	Procedimientos para restringir el acceso a las operaciones de la red y a las facilidades de proceso.
2.9	No se usan passwords en línea lo cual provoca que no se identifiquen a los usuarios de las terminales o de las microcomputadoras conectadas a la red. Se utilizan passwords o IDs compartidos. No existe un procedimiento de no impresión cuando se introduce un password por lo que cualquier usuario puede conocer la clave de otros imprimiéndolos y de este modo accesar a la red. Los passwords no son lo suficientemente grandes, se usan palabras de diccionario y no se modifican periódicamente por lo que la gente que quisiera hacer un daño puede ser capaz de adivinarlos.	Control sobre passwords

REF.	RIESGO	MEDIO DE CONTROL
	Personas no autorizadas pueden tener acceso a los comandos de control de la red y activar y desactivar nodos.	
	No se revisan y corrigen periódicamente las políticas y estándares de control aplicados a la red.	Actualización y adecuación de las políticas y estándares establecidos para el control general de la red.
2.13	La información es almacenada en las estaciones de trabajo sin ningún control de acceso por lo que no se puede confiar en la integridad de los datos.	Estructura de los directorios usados en la red con un control de acceso. Información sensitiva almacenada en el servidor de la red.

REF.	RIESGO	MEDIO DE CONTROL
	No se han establecido los pérfiles de los usuarios de la red en su sistema operativo para restringir los recursos a que tienen acceso por lo que pueden hacer uso de las aplicaciones, procesos de transacción y archivos de datos no autorizados, teclear comandos desde una estación de trabajo y ejecutarlos en otra estación diferente, usar comandos del sistema que afectan más de una red y que sólo una persona autorizada con toda la responsabilidad y una seguridad apropiada pudiera ejecutarlos.	
	No se tiene definido un número predeterminado de accesos por lo que cualquier persona no autorizada puede lograr accesar a la red.	Número predeterminado de accesos.
	No existe un procedimiento automático de desconexión de las terminales o microcomputadoras de la red que impida intentos de acceso no autorizados.	Desconexión automática de terminales cuando no se estén utilizando.
2.10	Diferentes usuarios accesan a la misma aplicación originando conflictos en el proceso de transacciones y quedando éstas incompletas.	Control sobre el acceso de varios usuarios a la misma aplicación.
2.12 2.17 5.5	No se cuenta con reportes regulares conteniendo todas las violaciones de acceso por un Departamento de Usuario lo cual indica que no se lleva un mantenimiento y monitoreo de la seguridad de la red.	Revisión y seguimiento de reportes de violaciones y actividades de la red.

REF.	RIESGO	MEDIO DE CONTROL
2.14	No se puede identificar la localidad de alguien que intente lograr accesar a la red a través de las facilidades de marcar en comunicaciones.	Procedimiento de llamadas en forma manual o automática.
2.15	No se checa que la llamada provenga de los lugares permitidos y de la persona autorizada.	Dispositivos de autenticidad personal, servicio de dial-back, bases de datos.
2.16	Los números telefónicos usados para lograr el acceso a la red no son cambiados periódicamente y se tienen en una lista lo cual permite que personas no autorizadas o que ya no laboren en la organización puedan hacer mal uso de información confidencial.	Cambios periódicos a los números telefónicos usados para accesar a la red, dispositivos para protección de puertos e identificadores de terminales.
2.18	Cualquier persona no autorizada puede accesar a las facilidades del intercambio de paquetes y conocer o dañar la información.	Control sobre el acceso al intercambio de paquetes.
2.20	No se monitorea la red después de su implementación por lo que no se puede determinar si se está apegando a los requerimientos del usuario y está siguiendo los objetivos especificados para su actuación. No se cuenta con software para monitoreo de la actuación que periódicamente mida la red, la eficiencia de los procesos y permita la corrección de errores.	Revisión de la post-implementación de la estructura y actuación de la red.

REF.	RIESGO	MEDIO DE CONTROL
2.21	No existen mecanismos dentro de la red que monitoreen los tiempos de respuesta y el número y duración de las funciones para servicios de voz y datos.	Definición de requerimientos de actuación y funciones documentados para servicios de voz y datos.
2.22	No existe una estructura que asegure que el proceso con mayor prioridad se esté llevando a cabo y transmitiendo primero.	Asignación de prioridades a los procesos.
2.23	No existen controles de hardware y software que eviten se degrade significativamente la actuación de la red y se pierdan datos.	UPS
2.24 2.25	No existen procedimientos relacionados con la restauración del proceso de datos distribuido de la organización después de una interrupción en sus operaciones o de un desastre lo cual no permite conocer las condiciones bajo las cuales se deberá actuar y la o las personas que serán responsables de llevarlas a cabo con el conocimiento de la ubicación y acceso al hardware así como de los recursos de los suministros necesarios de recuperación, minimizar la participación del usuario para su reestablecimiento. Tampoco conocer la clasificación y estándares de información, así como medidas de seguridad física y la entrada de datos.	Procedimientos probados y actualizados de recuperación en caso de desastre en la red que aseguran una restauración oportuna de la misma.
2.24 2.25 2.26	En caso de que existan procedimientos para restauración de la operación de la red y no sean probados periódicamente pueden no operar adecuadamente en caso de desastre.	

FUNCION:	3. SOFTWARE DE LA RED.	
REF.	**RIESGO**	**MEDIO DE CONTROL**
3.1	No se han asignado prioridades de transmisión para el envío de mensajes por la red lo cual ocasiona un tráfico y un tiempo de respuesta menor.	Identificación para enviar y recibir.
	No se verifican los mensajes de salida por lo que no se puede tener la seguridad de que tengan la dirección de destino válida.	Chequeo sobre la dirección del mensaje.
3.1 3.2	Los sitios servidos por la red pueden tener conflictos al tratar de establecer una comunicación, identificar al emisor y receptor de cada mensaje transmitido y al conciliar los mensajes recibidos y enviados pudiéndose recibir mensajes incompletos.	Procedimientos estándares de transmisión de comunicaciones. Reporte de errores en la transmisión. Conciliación periódica de mensajes. Código de detección o corrección de errores.
3.1	No se tiene respuesta sobre la recepción satisfactoria del mensaje.	Reconocimiento positivo.
3.4	Se cuenta con procedimientos de transmisión inconsistentes con las políticas relevantes de la administración las cuales no satisfacen las necesidades de los usuarios.	

FUNCION: 4. DISTRIBUCION DE LAS BASES DE DATOS.		
REF.	**RIESGO**	**MEDIO DE CONTROL**
4.1	No se tienen identificados datos sensibles y la información crítica contenida en la red.	Clasificación de la información.
4.2	No se conoce la distribución del contenido de la base de datos entre departamentos que usan la red. Asignación errónea de datos errónea entre departamentos.	Controles y medidas de seguridad establecidos para la distribución adecuada del contenido de las bases de datos entre los departamentos que usan la red.
	No se cuenta con una función centralizada para controlar de mejor manera el uso de los datos por los diferentes Departamentos de Usuarios servidos por la red.	Control de acceso a los datos de la red.
4.3	No se tienen bien definidos los tipos de datos que se manejan en la red (compatibilidad entre aplicaciones). No se cuenta con una actualización de la documentación de los datos para la red por lo que se puede tener un mal manejo de ellos.	Controles sobre los estándares de los datos de la red (diccionario de datos).
4.3 4.5	Inconsistencia, duplicidad y mala definición de los datos.	
4.4	No existen procedimientos para cambios en los datos.	

FUNCION: 5. SEGURIDAD DE LOS DATOS EN LA RED.		
REF.	**RIESGO**	**MEDIO DE CONTROL**
5.1	No se cuenta con un registro de las transacciones efectuadas en un periodo en la red que muestre a la persona, la transacción y la hora en que se efectuó.	Bitácora de transacciones.
	No existen políticas conscernientes a la protección de datos sensibles dentro de la organización por lo que cualquier persona no autorizada puede accesar a la información y dañarla.	Procedimientos de seguridad de los datos sensibles dentro de la red a través del encriptamiento y desencriptamiento.
	Las políticas existentes para proteger la información crítica para la organización no garantizan una protección adecuada de los datos.	
	Los manuales de procedimientos relevantes sobre la protección de los datos no están restringidos adecuadamente lo cual permite que personas no autorizadas conozcan el algoritmo usado para encriptamiento y desencriptamiento y tengan acceso a la información confidencial.	
5.3 5.4	No se tiene definido el tipo de protección de seguridad por lo que no se conoce si su control es altamente distribuido, distribuido, mezclado, centralizado o altamente centralizado.	Procedimientos para el mantenimiento y revisión de la seguridad física y lógica de la red.

REF.	RIESGO	MEDIO DE CONTROL
	Se está aplicando en una red altamente centralizada una protección de seguridad de tipo altamente distribuida lo cual indica que el tipo de protección de seguridad de la red resulta inapropiada con la configuración actual.	
5.3	No se cuenta con manuales adecuados o actualizados de procedimientos para seguridad de la red en los Departamentos Usuarios por lo que no se protegen las facilidades físicas de la red, la integridad de su software de aplicación y los datos de entrada y salida almacenados.	
5.4	Se lleva a cabo una revisión de la seguridad de todos los sitios servidos por la red de manera inconsistente por lo que cualquier problema encontrado a través de estas revisiones no es comunicado de manera oportuna a la administración y ésta no les puede dar una pronta respuesta.	Protección física de los sitios con el host y terminales remotas de comunicaciones ante accesos no autorizados.
5.4 5.5	No existen procedimientos de revisión de la seguridad de la red de los departamentos de usuarios que incluyan un eamen sobre el hardware de proceso y comunicaciones, sistemas operativos, procesos de transacciones y datos, una revisión de toda la documentación relevante sobre seguridad para determinar que está actualizada y una prueba a los usuarios sobre el conocimiento de las políticas y procedimientos de seguridad.	

REF.	RIESGO	MEDIO DE CONTROL
5.5	No se generan reportes sobre los resultados de estas revisiones por lo que los departamentos afectados no pueden establecer mejoras.	Reportes sobre los resultados de las revisiones de la seguridad de la red.

FUNCION:	6. CORREO ELECTRONICO.	
REF.	**RIESGO**	**MEDIO DE CONTROL**
6.2	No se cuenta con políticas de seguridad de información, controles de acceso sobre los datos y buzones que aseguren la entrada de individuos autorizados y un encriptamiento por lo que cualquier persona no autorizada puede hacer un mal uso de la información.	Controles para mantener la privacidad en los datos manejados en el correo electrónico (password, encriptamiento, buzones).
6.3	Los usuarios reciben mensajes incompletos o erróneos.	Procedimientos para detectar errores y omisiones en los datos utilizados en el correo electrónico.
6.4	No se cuenta con planes de contingencia y medios de comunicación alternativos como son el fax o teléfonos que garanticen la continuidad de las operaciones en caso de que falle la red y no se pueda utilizar el correo electrónico.	Controles para mantener una continuidad en las operaciones del correo electrónico ante fallas presentadas en la red (Plan de contingencias).
6.5	No se cuenta con un control centralizado para llevar a cabo una depuración periódica de los usuarios que deban tener acceso al correo por lo que personal que ya no labore en la empresa puede hacer uso de él.	Procedimientos para dar de alta y baja a los usuarios.

FUNCION:	7. SERVICIOS DE CONSULTORES, ASESORES EXTERNOS O PROVEEDORES.	
REF.	**RIESGO**	**MEDIO DE CONTROL**
7.2 7.4	Se tiene un contrato mal estructurado por lo que no se tienen bien definidos los costos del diseño del sistema, programación, tiempo de computadora, reportes regulares, reportes especiales, las responsabilidades del usuario, la responsabilidad del consultor o asesor externo para revisar la seguridad de los procesos de salida, arreglar problemas identificados e inicializar de nuevo el proceso, proteger contra daños o pérdidas los datos mientras está bajo su control.	Contar con un contrato detallando los derechos y responsabilidades del consultor o asesor externo por la prestación de sus servicios.
7.5	El cableado de la red no fue llevado a cabo correctamente ya que no fue instalado con una canaleta exponiéndose a daños y repercutiendo en el funcionamiento de la red. Además de que no se tienen identificadas las rosetas y dificulta la pronta restauración de la red en caso de falla.	Control sobre la instalación del cableado de la red.
7.6 7.7	Los consultores o asesores externos pueden accesar a áreas no autorizadas o a información confidencial.	Control de acceso de los consultores o asesores externos (passwords).
7.8	Si el contrato no permite que auditores externos e internos lleven a cabo, si es necesario, una auditoría sobre las actividades del consultor o asesor externo, no pueden proponer mejoras a los procedimientos de control.	Auditoría a las actividades de los consultores o asesores externos.

REF.	RIESGO	MEDIO DE CONTROL
	No se revisan los reportes de auditoría por lo que no se conoce el alcance y debilidades de los controles de las operaciones relevantes del consultor o asesor externo. No se llevan a cabo auditorías periódicas por terceras partes por lo que no se puede asegurar el buen funcionamiento de EDI. Se llevan a cabo auditorías periódicas pero no se tiene un control sobre la frecuencia, alcance, actualización, tiempo y adecuación de estas revisiones.	
7.9	El consultor o asesor externo no provee manuales de usuario bien documentados por lo que los usuarios no llevan a cabo sus funciones de manera apropiada ya que no tienen un entendimiento general adecuado de las entradas, procesos y salidas de los sistemas de aplicación.	Manuales de usuario elaborados por el consultor o asesor externo.
7.10	No se revisa y actualiza periódicamente el plan de recuperación en caso de desastre en el proceso de datos del usuario por lo que resulta imposible determinar si las aplicaciones críticas procesadas por el consultor o asesor externo pueden almacenarse antes de que las actividades del usuario se vean impactadas negativamente.	Plan de recuperación por parte del usuario en caso de desastre en el proceso de datos cuando el consultor o asesor externo esté prestando su servicio.

RED DIGITAL DE SERVICIOS INTEGRADOS (RDSI).		
REF.	**RIESGO**	**MEDIO DE CONTROL**
7.11 .1	No se incorpora a las comunicaciones todo el potencial y calidad que la tecnología digital ofrece en la actualidad en la transmisión de voz y datos.	Acceso digital a un conmutador electrónico o digital.
7.11 .2	No se utiliza la marcación directa que remplaze la intervención de la operadora.	Marcación directa.
7.11 .3	No se establece una comunicación efectiva y dinámica que permita optimizar tiempo y costos de la empresa sin necesidad de traslados innecesarios e incrementar la productividad y obteniendo aplicaciones como reuniones y juntas de trabajo, cursos de capacitación, comunicados al personal, distribución de información y su discusión inmediata.	Optimizar tiempo y costos a través de la videoconferencia.
7.11 .4	No se cuenta con una administración adecuada que optimice y racionalice las comunicaciones.	Administración de las comunicaciones a través del enlace digital de alta velocidad.
7.11 .5	No se encuentran interconectadas todas las ubicaciones del cliente en una misma ciudad ni se cuenta con enlaces de alta calidad y velocidad que permitan la administración adecuada de sus recursos ni con la tecnología digital para la utilización de diversas modalidades de transmisión como voz, datos e imagen como si fuera un solo edificio de manera que optimice la operación diaria.	Conexión de todos los sitios del cliente a través de una red privada metropolitana.

REF.	RIESGO	MEDIO DE CONTROL
7.11 .6	Existen comunicaciones deficientes entre la empresa e instituciones en ciudades fronterizas debido a que no utilizan un servicio adecuado de comunicaciones.	Conexión de la organización con empresas en ciudades fronterizas a través del cruce fronterizo.
7.11 .7	No se cuenta con redes de alta capacidad de tecnología digital con funciones y facilidades asociadas a una red privada y con alcances internacionales que sirvan de enlace en localidades de diversos países y establezca comunicaciones efectivas y competitivas.	Administración de la red global.
7.11 .8	No se puede contar con todos los servicios de la RDSI. No se puede establecer una buena comunicación debido al ruido e interferencia en la línea.	Telefonía analógica de alta calidad.
7.11 .9	No se integran las funciones de voz y datos que la empresa lleva a cabo en diferentes localidades.	Establecimiento de una red privada de voz y datos.
7.11 .10	No se cuenta con una transferencia electrónica de datos, el acceso a bases de datos (videotexto) y el uso de correo electrónico que haga más eficiente su operación.	Establecimiento de una red de paquetes de datos.
7.11 .11	No se pueden hacer enlaces con empresas que se encuentran localizadas en otras ciudades donde no se cuenta con infraestructura terrestre digital.	Establecimiento de una red satelital.

REF.	RIESGO	MEDIO DE CONTROL
7.12	No se cuenta con los acuerdos sobre las metas y beneficios que proporcionan los sevicios de la RDSI a la organización por lo que se desconoce si incorpora a sus comunicaciones todo el potencial y calidad que la tecnología digital ofrece en la actualidad en la transmisión de información tanto de voz como de datos.	Emisión por escrito de las metas, costos y beneficios a obtener con los servicios de la RDSI.
7.13	No se conocen los procedimientos con que cuenta la RDSI por lo que no se puede medir su disponibilidad en: infraestructura, respaldo de la instalación y supervisión y tiempos de respuesta en el servicio.	Control general de la disponibilidad de la RDSI: Tiempos mínimos de respuesta. Supervisión por compañías de prestigio mundial.
	No se evalúa la confiabilidad de la RDSI por lo que no se sabe si sus medios de transmisión son de alta calidad e inmunes al ruido e interferencias, cuál es la precisión con que se cuenta para completar llamadas al usar centrales de comunicación digital, y si la instalación de radios digitales y fibras ópticas de soporte están asegurando un respaldo confiable.	Control sobre la confiabilidad de la RDSI: Medios de transmisión inmunes al ruido e interferencias. Respaldo mediante la instalación de fibras ópticas y radios digitales de soporte.
	No se evalúa la calidad de la RDSI por lo que puede no estar contando con una alta calidad en la conversación, tener un alto índice de errores en el envío y recepción de datos y no ser inmune a ruidos e interferencias.	Control sobre la calidad de la RDSI: Alta calidad en la conversación, mínimo promedio de errores en el envío y recepción de datos, inmunidad a ruidos e interferencias.

REF.	RIESGO	MEDIO DE CONTROL
7.14	No se cuenta con procedimientos claros sobre la RDSI que muestren la manera en que facilita y optimiza su mantenimiento y continuidad.	Políticas y procedimientos establecidos para el control de la administración de la RDSI y de los recursos de comunicaciones de los usuarios. Diagnósticos y monitoreos sistemáticos del servicio y su calidad.
7.15	No se hacen revisiones al reenrutamiento inmediato de medios de transmisión de respaldo por lo que no se pueden asegurar tiempos mínimos de respuesta al usuario.	Reenrutamiento inmediato a medios de transmisión de respaldo.
7.16	No se tienen reportes de tráfico y consumo por lo que no se puede hacer un análisis de la asignación y optimización de recursos.	Reportes de tráfico y consumo.

INTERCAMBIO DE DATOS ELECTRONICO (EDI)		
REF.	**RIESGO**	**MEDIO DE CONTROL**
7.17	No se llevó a cabo un análisis de costo-beneficio sobre EDI por lo que puede ser que no cubra las necesidades o que sus metas y beneficios no sean razonables y alcanzables.	Emisión por escrito por parte de la administración de los aspectos sobre las metas y beneficios a obtener con el Intercambio de datos Electrónico (Electronic Data Interchange, EDI).
7.18	No se tomó en cuenta a la administración del Departamento Legal de la organización, los Departamentos de Seguridad y Riesgo y los Departamentos de Usuario afectados para el establecimiento de EDI por lo que su operación, seguridad, control y costo pueden ocasionar conflictos impidiendo el logro de sus metas.	Participación de los departamentos involucrados para su establecimiento.
7.19	No se hace una revisión de los contratos con los proveedores de EDI por lo que no se conoce la razonabilidad y adecuación de sus términos y condiciones tales como mensajes y formatos de transacción y establecimiento de verificación y autenticidad por la Asociación de Industrias u organización de establecimientos de estándares entre socios comerciales; la resposabilidad para reportes y pagos de los valores agregados y otros impuestos generados por las transacciones originadas por el acuerdo; el seguro contra accidentes y cobertura por bonos de fidelidad, responsabilidades	Establecimiento de los términos y condiciones a través de contratos con los socios de EDI o con proveedores de sus servicios.

REF.	RIESGO	MEDIO DE CONTROL
	del proveedor de servicios, sus agentes y subcontratistas, y responsabilidades de la organización; la propiedad y confidencialidad de los datos y los medios usados para impedir su revelación por los empleados del proveedor de servicios, agentes o subcontratistas, y evitar se interfieran los datos mientras se está en transmisión; los medios para identificar al usuario del sistema, para evaluar y resolver las anomalías en los registros y el flujo de registros de transacción de datos como ayuda para la corrección de discrepancias en el proceso, para evitar resultados falsos y detectar actividades fraudulentas; cómo el proveedor de servicio debe revelar a terceras partes los nombres, números teléfonicos, nombramientos de trabajo y otra información sobre los empleados de la organización encargados del proceso de EDI de manera efectiva y limitadamente y cómo proveerá capacidades operacionales alternativas para permitir una pronta restauración del proceso de EDI después de que ocurra un desastre.	
7.20	No se cuenta con un registro de las transacciones por lo cual no se puede llevar a cabo una revisión de auditoría o que la organización lleve un control sobre el costo por transacción entre periodos o por los cargos del acceso a la red y transmisión de transacciones.	Registro de transacciones.

REF.	RIESGO	MEDIO DE CONTROL
	No se tiene un reporte o registro automático de las transacciones de procesos no satisfactorios por lo que no se facilita una solución oportuna de los defectos y retransmisión de los registros.	
7.21	No se conservan las copias de archivos de transacciones por un número específico de años por lo que los usarios del sistema no pueden consultar la historia de una transacción en particular.	Respaldo de los archivos de transacciones (periodo de vida).
7.22	El encriptamiento y desencriptamiento de datos y los procesos de administración de la llave no operan de manera efectiva.	Administración del encriptamiento y desencriptamiento.
7.23	Se tiene un índice de error muy alto en el proceso de transmisión por lo que la información no es confiable y afecta a la toma de decisiones.	Control sobre el índice de errores permitido en el proceso de transmisión.
7.24	No se conoce el tiempo de respuesta que ofrece EDI por lo que no se puede hacer frente a cualquier interrupción o degradación del servicio.	Controles sobre la disponibilidad de EDI (tiempo de respuesta).
7.25	Se borran o modifican otras transacciones o datos diferentes a los deseados.	Procedimientos para modificar y borrar registros de archivos maestros, de transacción y de datos.

REF.	RIESGO	MEDIO DE CONTROL
7.26	Se permiten accesos no autorizados al sistema y/o no se respetan los niveles de confidencialidad de mensajes.	Código de autenticidad de mensajes y/o totales encriptados.
7.27	No existe una transmisión de mensajes numerados del sistema en forma consistente que evite errores en el conocimiento y retransmisión de ellos.	Control sobre la transmisión de mensajes.
	No se puede identificar la posible presencia de virus en la computadora y no se pueden detectar problemas de código o datos afectados.	Revisión rutinaria del contenido de la transmisión.
7.28	La red presenta fallas que podrían prevenirse si se tuviera un mantenimiento adecuado.	Mantenimiento acorde al plan de recuperación en caso de desastre.
7.29	El representante de la organización no lleva a cabo una vigilancia adecuada de las actividades de cualquier empleado del proveedor de servicios por lo que no se sabe si todos los problemas son resueltos de manera razonable.	Revisión de las actividades de los empleados del proveedor.
7.30	La administración no ha establecido controles: que limiten la habilidad de los usuarios para iniciar actividades específicas sensibles por lo que cualquiera puede segregar y transmitir transacciones de alto valor y riesgo; sobre el empleo de passwords y mecanismos de identificación sobre la autenticidad de la	Identificación y verificación del usuario.

REF.	RIESGO	MEDIO DE CONTROL
	localidad del usuario y del socio comercial; para asegurar que un predeterminado número de fallas consecutivas en el password desconetará la localidad del usuario del sistema y requerirá la aprobación del supervisior antes de que se restablezca la conexión. No existe una validación sobre los emisores y receptores de mensajes por lo que personas no autorizadas podrían hacer uso de ellos.	
7.31	No se tiene un registro sobre los cambios y llamadas a los programas de EDI por lo que no se puede identificar cualquier cambio no autorizado, o determinar el tiempo, fecha, persona y propósito del acceso.	Control para cambios y llamadas a los programas de EDI.
7.32	No se puede asegurar que las transacciones estén autorizadas, completas, exactas, seguras y sujetas a procedimientos de corrección en caso de error.	Controles para las transacciones de entrada y salida del sistema y mantenimiento al archivo maestro

FUNCION: 8. CONTABILIDAD Y CARGOS PARA LOS SERVICIOS DE COMUNICACIONES.		
REF.	**RIESGO**	**MEDIO DE CONTROL**
8.1	Los costos son mayores a los beneficios.	Análisis de costo-beneficio.
8.2	No se puede llevar a cabo una comparación de costos entre los sevicios de voz y datos.	Control de la contabilidad de servicios de comunicaciones.
8.4	No se tienen capturadas todas las facturas en el sistema de contabilidad. No se contemplan todos los cargos por los servicios de comunicaciones, por lo que sus estados financieros no reflejan los costos reales en que incurre el departamento.	Procedimientos para cotejar la facturación contra lo registrado en contabilidad.
8.5 8.6 8.7	No se estima correctamente el costo por los servicios ofrecidos.	Control sobre la contabilidad de servicios ofrecidos a terceros.

Fecha: __ /__ / _ C29

NOMBRE DE LA COMPAÑIA: _____

COMPONENTE : _____

CEDULA DE DEFICIENCIAS Y RECOMENDACIONES

			RESOLUCION	
REF. HOJA RESP.	DEFICIENCIA O SUGERENCIA	AUMENTA ALCANCE SI/NO	COMENTARIOS DEL CLIENTE O DEL GERENTE DE AUDITORIA	CARTA

Elaborado por: _____ Revisado por: _____

Discutido con: _____