# *UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO*

FACULTAD DE INGENIERIA

"AUDITORIA AL AMBIENTE DE REDES DE AREA LOCAL"

T E S I S
Que para obtener el título de
INGENIERO EN COMPUTACION

P r e s e n t a n

ARMANDO GODINEZ DIAZ
EDUARDO GOMORA RAMIREZ
JUAN MOLINA PEREZ
JOSE RAMON MORALES GONZALEZ
LUIS MIGUEL SANCHEZ GONZALEZ

Director:
Ing. Maricela Castañeda Perdomo


México, D.F. 2000

*Agradecemos a la Ing. Maricela Castañeda Perdomo, nuestra directora de tesis, por conducirnos con éxito a la culminación de este proyecto tan importante en nuestras vidas.*

*Agradecemos a la Facultad de Ingeniería y a nuestra alma mater la Universidad Nacional Autónoma de México, por brindarnos la oportunidad de ser profesionales al servicio de nuestra patria.*

# ÍNDICE

# ÍNDICE DE FIGURAS

# INTRODUCCIÓN

El almacenamiento y el análisis de información han sido algunos de los grandes problemas a los que se ha enfrentado el hombre desde que inventó la escritura. No es sino hasta la segunda mitad del siglo XX cuando resuelve parcialmente, ese problema gracias a la invención de la computadora y, años más tarde, mediante la aplicación de métodos ordenados para análisis de datos y toma de decisiones.

En toda organización actual se ve reflejado este avance, derivado de la evolución de los programas de aplicación, equipos e integración centralizada de datos en redes de computadoras conectadas en un ambiente multiusuario, compartiendo recursos y teniendo un sistema de proceso distribuido; por lo que se hizo necesaria la elaboración y aplicación de procedimientos de evaluación a dichas entidades informáticas.

El objetivo principal de estos procedimientos de evaluación, es verificar que los sistemas de información cumplan con el fin para el cual fueron diseñados, así como determinar la confiabilidad que se le puede atribuir a la información que se produce, a través de controles específicos que tiendan a disminuir riesgos e impactos.

Las Redes de Área Local o LAN (Local Area Network en inglés), caen dentro de la necesidad de contar con la centralización y comunicación de datos en las compañías, contando principalmente con los siguientes elementos para su desempeño: **servidor**; para distribuir los recursos y tareas entre los diferentes usuarios de la red, **protocolo de comunicación**; por medio del cual se envía y recibe la información de los usuarios utilizando diversos estándares establecidos, **topología**; es decir, la forma física o lógica de como están conectadas las computadoras a la red y el **sistema operativo**; o sea, el software base de operación de la red.

De este modo, se conjugan la Auditoría en Informática y las Redes de Área Local para establecer procedimientos que permitan contar con sistemas de información eficientes en la totalidad de su operación, incluyendo a aquellas entidades o interfaces que interactúan con los mismos y sobre todo, protegiendo al activo más importante de cualquier organización: **la información**.

Por todo lo anterior, en el presente trabajo se tiene como finalidad mostrar la aplicación de la Auditoría en Informática en un ambiente de Redes de Área Local, integrando procedimientos y controles para revisar y evaluar la información, así como toda la gama de aspectos técnicos y tecnológicos que envuelven a ambos tópicos.

A continuación se presenta una breve descripción de los demás capítulos que integran este trabajo:

El **capítulo 2** muestra los Conceptos Generales de las Redes de Área Local y de la Auditoría.

El **capítulo 3** trata de la Seguridad Informática que se ve involucrada en el Ambiente de Redes de Área Local.

El **capítulo 4** presenta el Marco Teórico en el que se basó la auditoría realizada.

El **capítulo 5** muestra la propuesta de aspectos a considerar para auditar el ambiente de Redes de Área Local.

El **capítulo 6** describe el plan para llevar a cabo la auditoría, así como los elementos que involucran el informe de auditoría y los procedimientos a emplear en el seguimiento a la implantación de recomendaciones.

El **capítulo 7** muestra la aplicación de la Auditoría en una red de área local en una institución financiera, describiendo a detalle la planeación de la revisión, el desarrollo de la auditoría y la elaboración del informe correspondiente.

El **capítulo 8** presenta las conclusiones finales del presente trabajo.

Posteriormente se incluyen los **Apéndices**, en los cuales se integran todos aquellos elementos que formaron parte importante de la revisión, así como un **Glosario** de los términos técnicos y administrativos que fueron empleados en el desarrollo del tema. Finalmente, se presenta la **Bibliografía** que sirvió de apoyo para el desarrollo de cada capítulo.

# CONCEPTOS GENERALES

## 2.1 CONCEPTOS GENERALES DE REDES DE ÁREA LOCAL.

Dentro de un centro de cómputo u oficina donde se tenga instalada una red de área local, se demanda una mayor velocidad en el intercambio de información y una LAN es una alternativa factible. Las redes de área local van creciendo en número de usuarios paulatinamente adecuándose a nuestras necesidades.

Un punto importante que se debe tomar en cuenta es la independencia del hardware con respecto al software, ya que existe una gran variedad de fabricantes de hardware para red, lo que crea diversidad de opciones para solucionar los diferentes tipos de necesidades que se vayan presentando.

### 2.1.1 Definición de Red de Área Local.

**LAN** es el acrónimo de **Local Area Network**, es decir **Red de Área Local**. Este término engloba al conjunto de microcomputadoras que se interconectan por medio de cables y tarjetas de red con el fin de compartir información, servicios (correo electrónico, transferencia de archivos, emulación para acceso a equipos mainframe y minis), dispositivos (impresoras, plotters, módems), etc. Referente a los términos anteriores, una LAN proporciona un medio de transporte y conectividad para toda la información que fluirá a través de los nodos o micros que conforman la estructura de la red. (Fig. 2.1)

**RED DE ÁREA LOCAL**

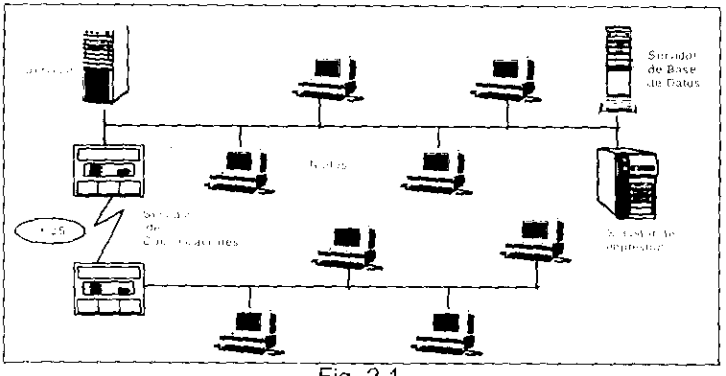


Fig. 2.1

Las redes de área local en la actualidad están constituidas por un dispositivo central llamado FILE SERVER (servidor de archivos) en donde se concentran

todos los recursos que se desean compartir. Esta plataforma necesita de un sistema operativo que controle todos los requerimientos de entrada y salida de datos en las estaciones de trabajo.

Es importante resaltar la diferencia entre una LAN y un sistema de tiempo compartido, como es el caso de las minicomputadoras. Un sistema multiusuario de tiempo compartido se refiere a la plataforma en la cual a un dispositivo central se le conectan terminales denominadas tontas, ya que no poseen ningún poder de procesamiento. El tiempo de la unidad central de proceso (CPU) y la memoria de la computadora central se tienen que repartir entre todos los usuarios. Esto no sucede en un sistema de LAN, cada microcomputadora cuenta con su propia capacidad de proceso y el trabajo se efectúa en cada una de las microcomputadoras que componen la red, mientras que la única tarea del file server es controlar las peticiones de entrada y salida de datos de todos los usuarios en relación con la unidad de almacenamiento compartida.

En un sistema de red el poder de procesamiento se encuentra repartido entre las computadoras personales, mientras que en los sistemas de tiempo compartido existen una o dos computadoras que procesan la información de todos los usuarios.

Es importante mencionar que el término microcomputadora y computadora personal (PC) son sinónimos, entendiéndose por estos conceptos una computadora que funcionalmente es similar a computadoras más grandes, pero sirve solamente a un usuario. Es usada en el hogar y en la oficina. El tamaño de la computadora está basado en su memoria y capacidad de disco, la velocidad en la CPU que la comanda y la calidad visual en la resolución de la pantalla.

### 2.1.2 Características generales de una Red de Área Local.

De manera general, las características óptimas de una LAN son:

- Tener una sola instalación, es decir, que los nodos (servidores, impresoras, microcomputadoras) se encuentren conectados por un mismo cable.
- Tener independencia de los equipos en cuanto al procesamiento de la información, esto es, contar con procesos descentralizados.
- Que pueda administrarse y mantenerse fácilmente.
- Que se puedan compartir dispositivos tanto de almacenamiento como de entrada y salida de datos.

### 2.1.3 Estándares.

Todos los grandes fabricantes de computadoras poseen su propia estructura y arquitectura para comunicar o enlazar sus equipos, lo que ocasiona que algunos no sean compatibles con otros. Ante esta situación, se han diseñado **estándares**

con el propósito de proveer las bases para el desarrollo de diferentes formas que permitan la intercomunicación de equipos con distintas características y logrando que la información se procese en diferentes ambientes de una manera transparente para el usuario.

Dentro del campo de la computación los estándares se establecen principalmente de dos maneras:

- De acuerdo a los fabricantes que dominan el mercado.
- De acuerdo a normas impuestas por organizaciones oficiales

Una de las organizaciones oficiales más importantes en este ámbito es el Comité 802 del IEEE (Institute of Electrical and Electronic Engineers) localizado en los Estados Unidos de Norteamérica. Dicha institución ha definido un modelo para la interconexión de sistemas de cómputo e intercambio de información llamado **OSI (Open System Interconnection)**.

A continuación se mencionan los objetivos del modelo OSI.

- Establecer bases comunes para el desarrollo de estándares.
- Calificar a los productos como "abiertos" debido a que utilizan los estándares.
- Proveer una referencia común para los estándares.
- Definir los puntos de interconexión para el intercambio de información entre los sistemas.
- Proveer la plataforma para que exista un ambiente de múltiples distribuidores y la comunicación entre ellos.

Algunos de los estándares proporcionados por este comité son:

- 802.1 Estándar que coordina la interfase entre los niveles del modelo OSI.
- 802.2 Estándar que define la interfase entre el nivel 2 y 3 (Logical Link Control).
- 802.3 Estándar para la topología del Bus Lineal.
- 802.4 Estándar para la topología de anillo modificado Token Bus.
- 802.5 Estándar para la topología de anillo modificado Token Ring.

Otro modelo para interconexión de sistemas de cómputo es el IBM SNA (System Network Architecure) desarrollado por IBM en 1974 con el objetivo de hacer transparente el servicio de red a los usuarios.

La SNA está compuesta por una variedad de productos de hardware y software que interactúan entre sí.

### 2.1.4 Topologías.

Las LAN's pueden tener sus nodos conectados entre si de diferentes formas o topologías. El término **topología** es la configuración que describe cómo están conectados los componentes de una red y definen tanto el medio físico por el cual se transmite la información, como la manera en que ésta se traslada por dicho medio.

Entre las topologías más utilizadas se encuentran:

**a) Topología de Bus Lineal.**

Consiste de una línea troncal (o bus) a la cual se conectan todos los nodos. La señal viaja en ambas direcciones del cableado y es finalizada en los extremos por medio de una resistencia "terminador". (Fig. 2.2)

Las ventajas de este tipo de red son la facilidad de manejo y la economía, ya que el cable es compartido para la comunicación de todos los usuarios, lo que representa un costo menor. Por otra parte se tiene la desventaja de que el cable, si se trunca o falla en cualquier punto, la red entera deja de funcionar.

**TOPOLOGÍA DE BUS LINEAL**

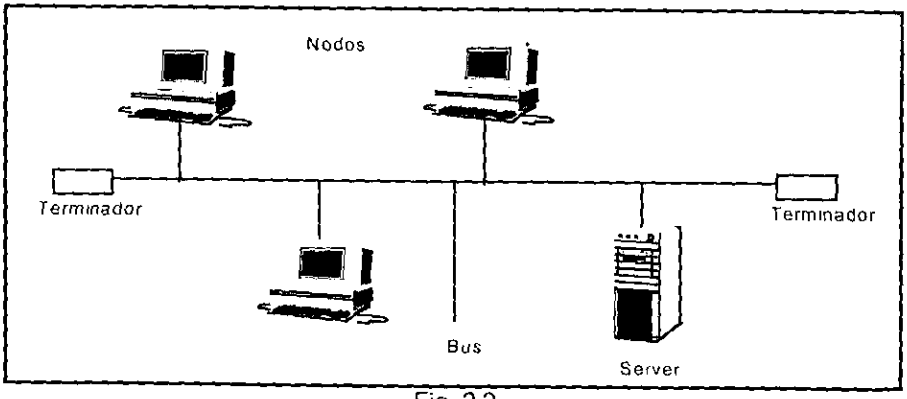


Fig. 2.2

**b) Topología de Anillo, Anillo Modificado y Anillo Doble Redundante (FDDI).**

Bajo esta topología cada microcomputadora se conecta a otras dos a medida que forme un circuito o enlace circular y de la misma manera la información viaja. (Fig.2.3).

Actualmente es muy difícil que exista este tipo de topología, ya que una gran desventaja se presenta si alguno de los nodos o estaciones de trabajo falla, con lo que la comunicación de la red se interrumpe.

**TOPOLOGÍA ANILLO**

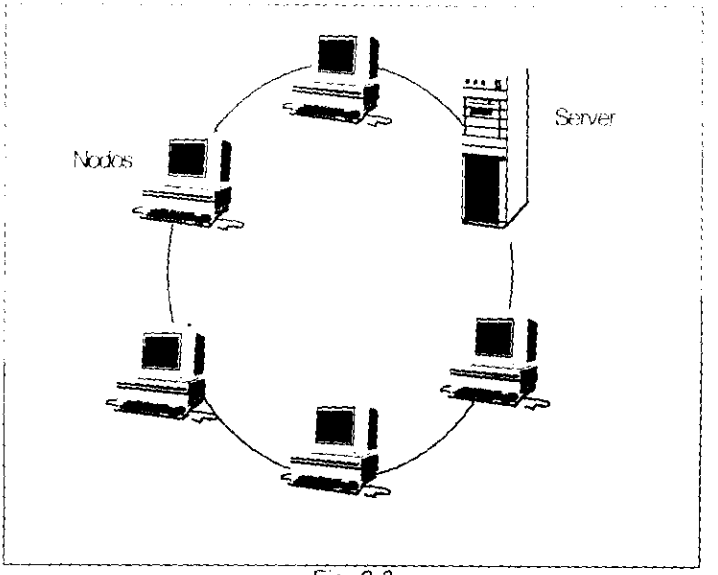


Fig. 2.3

Como solución a lo anterior, surge la topología de **anillo modificado** (Fig. 2.4), que como su nombre lo indica, es una variación de la topología de anillo y que consiste en un dispositivo central generalmente llamado *MAU* (Multistation Access Unit) o centro de alambrado o repetidor, al cual se le conectan cada una de las estaciones. De esta manera, la señal viaja también en forma circular, pero si un nodo falla, el dispositivo central aísla a ese nodo, hace un puente y continúa la comunicación de las otras máquinas sin interrumpir el flujo de la red.

Una desventaja del anillo modificado es que, entre más estaciones de trabajo se agreguen al canal de comunicaciones compartido, el ancho de banda de la red disminuye, lo que provocaría que el tiempo de respuesta sea más lento, puesto que la demanda de intercambio de información, solicitud de servicios (correo electrónico, transferencias de archivos, emulación) y dispositivos sería mayor.

**TOPOLOGÍA ANILLO MODIFICADO**

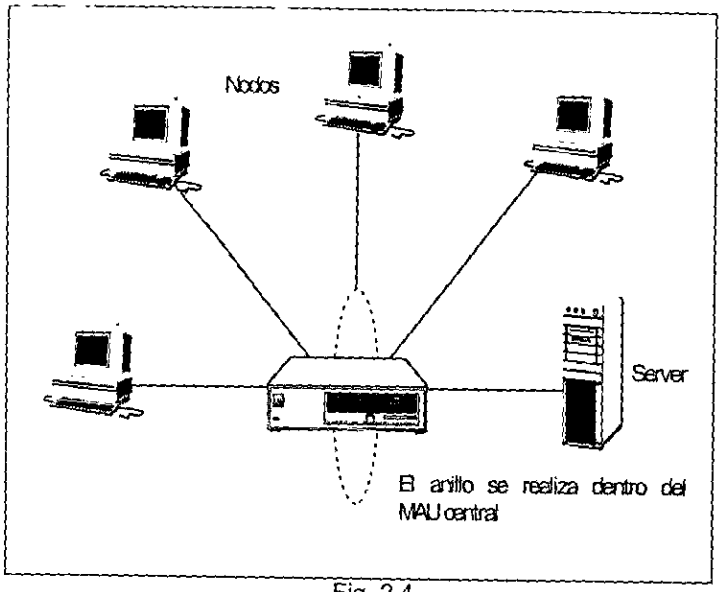


Fig. 2.4

Debido a la necesidad de contar con redes que requieren de alta velocidad surgió, la topología de **Anillo Doble Redundante FDDI** (Fiber Distributed Data Interface), la cual consiste de dos anillos de transmisión en contrasentido. El anillo primario es utilizado como canal principal. Si por alguna razón el anillo primario es interrumpido, el secundario restablece la continuidad del primario en forma automática, actuando como redundancia o anillo de respaldo. (Fig. 2.5)

**TOPOLOGÍA ANILLO DOBLE REDUNDANTE**

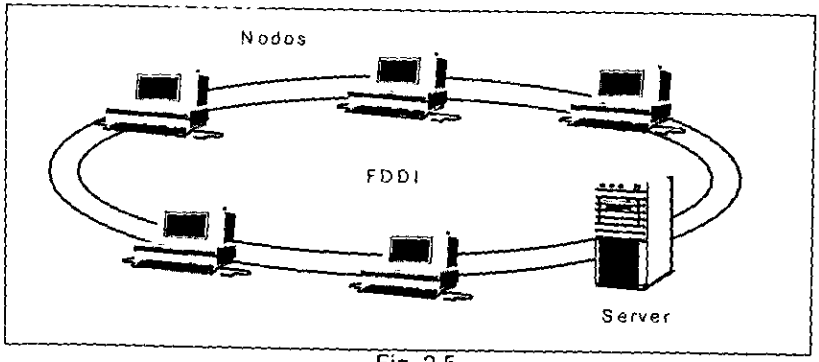


Fig. 2.5

### c) Topología de Estrella.

Consiste de un punto central desde donde se irradian los cables hacia las PC's. Este punto central es lo que se le conoce como servidor, ya que es una computadora dotada con las unidades de almacenamiento e información que van a servir a toda la red, esto es, las que se van a compartir al sevidor como "semáforo" para el flujo de la información. (Fig. 2.6)

**TOPOLOGÍA ESTRELLA**

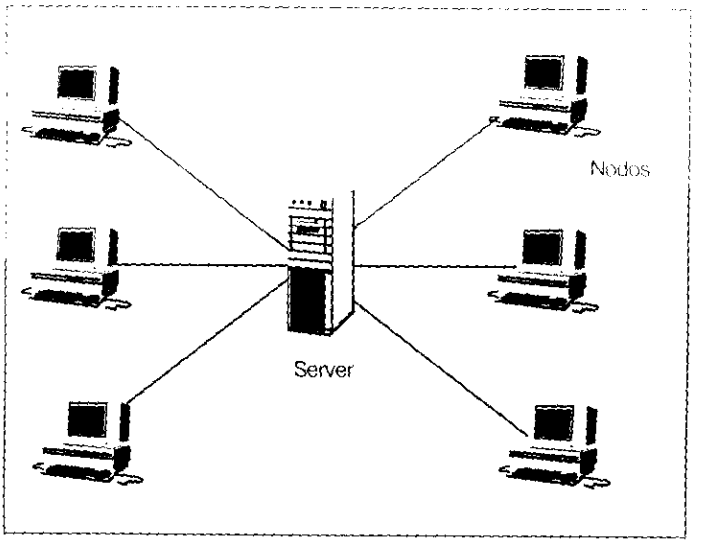


Fig. 2.6

A este nodo central se conectan las microcomputadoras, con su propio canal cada una, lo que resulta más costoso debido a la mayor cantidad de cable utilizado en la conexión. De esta forma, si uno de los cables de la red falla, sólo una de las estaciones de trabajo deja de funcionar sin afectar a las demás. Este tipo de topología se recomienda para una red donde se tenga un número mayor de diez usuarios con accesos frecuentes a disco.

Al contrario de las topologías anteriores, cada vez que se agrega una computadora a la red, el ancho de banda de la misma se amplía ya que se está sumando un cable más, lo que garantiza un mejor tiempo de respuesta en la demanda de intercambio de información, solicitud de servicios (correo electrónico, transferencias de archivos, emulación) y dispositivos, así como una disminución en los riesgos de fallas existentes en cuanto a tráfico en la red.

### 2.1.5 Modelo de Referencia OSI.

El modelo OSI propone 7 niveles de protocolos para conectar dispositivos.

| | |
|---|---|
| 7 Aplicación | Provee servicios a los usuarios de la red, tales como: Correo electrónico, transferencia de archivos, emulación. |
| 6 Presentación | Realiza transformaciones en la información: Conversión de código, compresión y encriptación. |
| 5 Sesión | Define el procedimiento para iniciar la comunicación entre 2 procesos a nivel presentación. |
| 4 Transporte | Verifica que los paquetes lleguen en el orden requerido (secuenciamiento). |
| 3 Red | Agrupa en paquetes y define el camino de cada paquete (enrutamiento). |
| 2 Enlace | Checa errores de transmisión a nivel de frames (paquetes) y presenta al nivel 3 una línea libre de errores. |
| 1 Físico | Define como se transmitirá la información binaria: Niveles de voltaje, modulación, velocidad de transmisión. |

Fig. 2.7

### 2.1.6 Protocolos de Comunicación.

¿Qué es un protocolo?

Así como entre los seres humanos existen ciertas reglas para la comunicación, entre las computadoras y los elementos de comunicaciones deben existir también procedimientos bien definidos.

"Los protocolos son acuerdos de la manera como las máquinas platican unas con otras". [1]

"Conjunto de reglas acordadas para asegurarse que los equipos de transmisión y recepción de datos se entiendan en la comunicación". [1]

Podemos entonces definir a un protocolo como el conjunto de reglas y procedimientos que deben cumplir dos máquinas a fin de que puedan comunicarse. Evidentemente, debe existir estandarización en los protocolos para permitir la comunicación entre máquinas de diferentes fabricantes.

Funciones de un protocolo

- Establecer el enlace de comunicación entre los dos elementos.

[1] Asesoría en Redes y Telecomunicaciones (ASERCOM), "Curso Datos 01"

- Seleccionar la ruta adecuada.
- Realizar el transporte de la información.
- Verificar que la comunicación se dé libre de errores.
- Administrar los recursos que conforman la red.

Cada una de las topologías que se mencionaron con anterioridad utilizan diferentes protocolos:

**1) CSMA/CD.**

Sus siglas significan Carrier Sense Multiple Access with Collision Detection. Este protocolo es asociado con la topología de Bus Lineal.

En este protocolo los nodos monitorean continuamente a la línea para saber si está ocupada o no y cuando se desocupa, el nodo envía sus paquetes.

En el caso de que dos nodos transmitan su señal simultáneamente se presenta una colisión la cual es detectada por los nodos, que esperarán una cantidad aleatoria de tiempo para reintentar su transmisión.

**2) Token Passing.**

Es utilizado para la topología de Anillo y Anillo Modificado. En él no se gana el acceso cuando se requiere, ya que los nodos desde su lugar deben esperar su turno para recibir la estafeta (token), la cual se intercambia en la forma del anillo.

Cuando un nodo obtiene el "token" cambia el primer bit para identificarlo como un paquete de datos, añade los datos y una dirección y envía la señal hacia la corriente. Cada nodo del anillo checa si el paquete está direccionado a él, si no, el nodo retransmite el paquete. Cuando el nodo direccionado recibe el paquete, verifica que la información sea correcta, copia los datos, marca el paquete como recibido y regresa el paquete original al anillo. El nodo transmisor remueve el paquete original y añade un "token" nuevo.

**3) Poleo.**

Este protocolo generalmente se utiliza con la topología tipo Estrella. Para entender su funcionamiento, se puede imaginar una junta entre varias personas donde se cuenta con un moderador para concederle la palabra a la persona en turno, preguntando a cada una de ellas, de manera secuencial y ordenada, si es que tiene algo que comunicar al grupo, de ser así, la persona designada transmite el mensaje. Si no existe información alguna para transmitir, se cuestiona a la siguiente persona, de tal forma, que el protocolo está evitando la posibilidad de que alguna estación de trabajo (persona) interfiera la comunicación de otra.

**4) ATM.**

Sus siglas significan (Asynchronous Transfer Mode) es un estándar muy reciente que define técnicas de alta velocidad, tanto para redes de área local (LAN) como para redes de área amplia (WAN), por lo que la industria está a la expectativa de sus avances.

ATM es una técnica de red que usa un medio conmutado, es decir, mediante switcheo de paquetes.

ATM tiene la caracteristica de transmitirse de manera asincrona, es decir, la transmisión de datos se efectúa de manera tal que cada caracter es una unidad auto-contenida con sus propios bits de comienzo y final y los intervalos entre caracteres pueden no ser uniformes, no utiliza tramas o frames convencionales, sino que crea celdas de información de tamaño fijo de 53 bytes.

Aprovecha al máximo la velocidad del medio físico, puesto que no crea tramas con información de control de errores; la eficiencia de los medios físicos ha llegado a ser bastante confiable y no es necesario un control de errores tan intensivo.

Una vez comprendidos los conceptos referentes a las diferentes topologías y protocolos existentes, es importante mencionar los tipos de red más utilizados en la actualidad, mismos que se han caracterizado por su rápida implantación, velocidad, flexibilidad y su tolerancia a fallas.

**Arcnet.**

- Creada por Datapoint (1970).
- Velocidad original de 2.5 mbps (megabits por segundo).
- Segmentos de 600 m.
- Nueva versión a 20 mbps.
- Longitud máxima de 6 km.
- Protocolo Poleo.
- Topologia Estrella.

**Ethernet.**

- Creada por Xerox (1977).
- Velocidad de 10 mbps.
- Segmentos de 200/500 m.
- Estándar IEEE 802.3.
- Longitud máxima de 1/2.5 km.
- Protocolo CSMA/CD.
- Topología Bus Lineal.

**Token Ring.**

- Creada por IBM (1980).
- Velocidad de 4/16 mbps.
- Segmentos variables.
- Estándar IEEE 802.4/802.5.
- Longitud máxima de 1 km.
- Protocolo Token Passing.
- Topologías Anillo y Anillo Modificado.

**FDDI.**

- Creada por ANSI (1991).
- Velocidad de 100 mbps.
- Segmentos de 4 km.
- Longitud máxima 40 km.
- Protocolo Token Passing.
- Su futuro es incierto ante la llegada de ATM.
- Topología de Anillo Doble Redundante.

## 2.2 EVOLUCIÓN DE LAS REDES DE ÁREA LOCAL.

En la década de los 50's, el hombre dio un gran salto con la creación de la computadora electrónica. La información ya podía ser enviada en grandes cantidades a un lugar central donde se realizaba el procesamiento de la misma. Surgió entonces el problema que esta información (que se encontraba en enormes cajas repletas de tarjetas), tenía que ser llevada al departamento de proceso de datos.

Con la aparición de las terminales en la década de los 60's, se logró la comunicación directa entre los usuarios y la unidad central de proceso, logrando con esto una comunicación más rápida y eficiente, pero se encontró con un obstáculo, entre más terminales y otros periféricos se agregaban a la computadora central, la velocidad de comunicación disminuía.

Hacia la mitad de la década de los 70's, la delicada tecnología de silicio e integración en miniatura permitió a los fabricantes de computadoras construir mayor capacidad en máquinas más pequeñas. Estas máquinas llamadas microcomputadoras descongestionaron a las viejas máquinas centrales, aunque todavía los equipos minis se seguían utilizando en gran medida.

A principios de la década de los 80's, las microcomputadoras habían evolucionado por completo, así como el concepto de computación personal, sus aplicaciones y

el mercado que lo utilizaba. Como una consecuencia de esta evolución, los encargados de los departamentos de informática fueron perdiendo el control de la información generada a través de las microcomputadoras, debido a que los procesos de las mismas no podían estar centralizados.

A la época referida se le denomina la era del disco flexible (floppy disk). Los vendedores de microcomputadoras decían: "En estos 30 diskettes usted puede guardar toda la información de su archivero".

Sin embargo, de alguna manera se había retrocedido en la forma de procesar la información, ya que ahora había que llevar la información almacenada en los diskettes de una PC a otra y en cierto momento la poca capacidad de los diskettes hacía difícil el manejo de grandes cantidades de información.

Con la llegada de la tecnología *winchester* se lograron dispositivos que permitían almacenar grandes cantidades de información, que iban desde 5 Mb. hasta 100 Mb. Una desventaja de esta tecnología era el alto costo que significaba la adquisición de un disco rígido removible. Además, los usuarios tenían la necesidad de compartir información y programas en forma simultánea.

Estas razones, principalmente aunadas a otras como poder compartir recursos de baja utilización y alto costo, llevó a diversos fabricantes y desarrolladores a la idea de generar las redes locales.

Las primeras LAN estaban basadas en servidores de disco (*disk servers*). Estos equipos permitían a cada usuario el mismo acceso a todas las partes del disco, lo cual causaba obvios problemas de seguridad y de integridad de datos.

La siguiente evolución de las redes fueron los servidores de archivos (*file servers*), en el que todos los usuarios podían tener acceso a la misma información compartiendo archivos y contando con niveles de seguridad, lo que permitía que la integridad de la información no fuera violada.

Desde sus orígenes, las redes locales basadas en el concepto de servidor de archivos han tenido que hacer frente a grandes retos tecnológicos y comerciales.

## 2.3 CONFIGURACIÓN E INSTALACIÓN DE UNA RED DE ÁREA LOCAL.

Este apartado tiene como objetivo presentar los puntos más importantes a considerar para la implantación y/o actualización de una LAN.

### 2.3.1 Configuración de una Red de Área Local.

¿Cómo se configura una red de área local?

Para llevar a cabo este estudio, hay que considerar dos situaciones:

- La primera es elaborar una configuración a partir de cero, es decir, desde el diseño de la red, cuántas estaciones de trabajo van a formar parte de la misma, qué distribución tendrá, las características de hardware y software, etc.
- La segunda es contar con una LAN, previamente configurada y que únicamente se requiere ampliar. En tal caso, se evaluará si la infraestructura de hardware y software con que se cuenta puede soportar el crecimiento de la red garantizando un adecuado funcionamiento, es decir, si los tiempos de respuesta son óptimos o es necesaria alguna actualización.

La tendencia dentro del mercado en los últimos años ha sido una creciente demanda por la adquisición de LAN's como una de las soluciones más populares en cuanto a comunicación se refiere.

Asimismo, ha presentado una evolución significativa desde redes departamentales hasta redes corporativas, dentro de las que se perciben necesidades de diseño por demás complejas, sistemas de cableado más extensos que juegan un papel importante dentro de las decisiones para la adquisición de una red, ya que tienen importancia estratégica a largo plazo, considerando la conexión de múltiples dispositivos que a la par del cableado, deben ser compatibles con diferentes equipos y normas o estándares, así como la diversidad de proveedores en el mercado donde cada uno ofrece una solución a los requerimientos del negocio.

En términos generales los elementos que conforman una red de área local son:

- Servidor.
- Estaciones de trabajo.
- Tarjetas de red.
- Cableado.
- Sistema operativo de red.

**Servidor.**

El servidor es la computadora central que nos permite compartir recursos y es en donde se encuentra alojado el sistema operativo de red.

El servidor es el corazón de la red, ya que provee el acceso controlado a los archivos, permite compartir impresoras y otros recursos dentro de la red,

Actualmente se utilizan microcomputadoras con procesadores Intel 80386 o superiores.

Existen varias reglas que hay que tomar en cuenta para escoger el servidor más adecuado:

- Ser compatible con el tipo de sistema operativo de red que se escoja.
- Proporcionar la suficiente capacidad de procesamiento (memoria, procesador, disco duro) para cubrir los requerimientos actuales y futuros.
- Contar con suficientes ranuras de expansión (tarjetas de expansión, tarjetas de interfase, etc.).

**Estación de trabajo.**

Las estaciones de trabajo son microcomputadoras interconectadas por una tarjeta de interfase. Ellas compartirán recursos del servidor y realizarán un proceso distribuido.

El procesamiento de datos en una red es distribuido, por lo tanto el desempeño de la estación de trabajo se debe definir en función de las aplicaciones que se estarán manejando en ella. Definir y analizar el tipo de aplicaciones que se manejarán en la red es de suma importancia para lograr que la estación de trabajo sea la adecuada.

Existen algunas reglas generales que hay que tomar en cuenta al escoger una estación de trabajo. A continuación, se presentan algunas de ellas:

- Debe existir compatibilidad con la infraestructura instalada.
- Debe cubrir con los requerimientos de memoria, procesador y disco duro que garanticen la correcta operación de las aplicaciones.

**Tarjetas de red.**

Estas tarjetas se conectan a los servidores, estaciones de trabajo e impresoras y son las que controlan el intercambio de datos en una red. Lleva a cabo las funciones electrónicas del método de acceso (protocolo de enlace de datos), tales como Ethernet, Token Ring, etc.

Debido a lo anterior, de la selección de la tarjeta de red que mejor cubra las necesidades, dependerán las características de la red como son la velocidad de transmisión, el tamaño de los paquetes de información, el esquema de acceso y la topología de la red, con lo que se determinará la eficiencia de la misma.

En cuanto a la velocidad de transmisión, se puede hacer notar que es un importante parámetro que ofrece un fácil método de comparación entre diferentes tipos de redes, por ser la medida de velocidad a la que pueden viajar los paquetes de información por el cableado de la red. La mayoría de los estudios en este sentido muestran el predominio de las tarjetas Ethernet, Arcnet y Token Ring.

**Cableado**

Algo muy importante al elegir una red es determinar el tipo de cable apropiado que se va a utilizar y que depende de lo que se quiera transmitir a lo largo de la red: voz, datos, imágenes, etc.

Otros dos factores de consideración son la distancia entre los nodos y el lugar físico por donde se instale el cableado.

Si se lleva a cabo una buena elección, la instalación puede dar servicio de 10 a 15 años antes de ser reemplazada.

El cableado representa un alto porcentaje del costo de la instalación total de la red, dependiendo, como se apuntó anteriormente, de la distancia de las estaciones de trabajo y el tipo de cable, motivo por el cual se recomienda una cuidadosa planeación de acuerdo a las necesidades del cliente.

Los cables comúnmente utilizados son:

- Par Telefónico.

  Se le conoce como par torcido o twisted-pair, se utiliza en las instalaciones telefónicas y en ocasiones los ya existentes en una oficina pueden ser aprovechados para la conexión, ya que es de fácil instalación debido a su flexibilidad y bajo costo.

  Cuenta con 4 hilos o dos pares para la transmisión de voz y datos. La desventaja de este tipo de cable es su estrecho ancho de banda, lo que aumenta la atenuación a grandes distancias, por lo cual, en ocasiones requiere repetidores para alcanzarlas y no soporta altas velocidades de transmisión.

- Cable coaxial.

  Compuesto por un conductor interno separado de uno externo por medio de una gruesa capa de material aislante. El conductor externo actúa como conductor de tierra. La estructura completa está cubierta por un material plástico protector. A través de él se pueden transmitir datos, voz y señales

de video debido a que tiene un ancho de banda mucho mayor (VHF de 80 a 200 MHz).

Este tipo de cable se ofrece en el mercado en una gran variedad de diámetros. Los más anchos permiten transmitir la información a mayores distancias, aunque tienen la desventaja de ser caros y no muy flexibles.

- Fibras ópticas.

Se dice que este tipo de cable constituye el medio de transmisión ideal para las ondas digitales. Utiliza la fibra de vidrio como material, los pulsos electrónicos que genere la computadora son convertidos en señales de luz, que son transmitidos por la fibra de vidrio.

La transmisión es inmune a las transferencias electromagnéticas o de radiofrecuencia del medio ambiente. Soporta velocidades muy altas y grandes distancias.

Las más usadas son las llamadas de índice graduado, con la desventaja de que es un cable muy caro y, debido al material con que está fabricado, tiene muy poca flexibilidad.

**Tabla comparativa de cableado.**

| COSTO | DESEMPEÑO | FACILIDAD DE INSTALACIÓN | INMUNIDAD A LA INTERFERENCIA |
|---|---|---|---|
| 1. Par Trenzado | 1. Fibra Óptica | 1. Par Trenzado | 1. Fibra Óptica |
| 2. Coaxial | 2. Coaxial | 2. Coaxial | 2. Coaxial |
| 3. Fibra Óptica | 3. Par Trenzado | 3. Fibra Óptica | 3. Par Trenzado |

**Tabla de longitud de un segmento de los distintos tipos de cable.**

| TIPO DE CABLE | VELOCIDAD PROMEDIO | LONG. MÁX. SEGMENTO | NÚM. MÁX. CONEXIÓN |
|---|---|---|---|
| Par Trenzado | 4 - 16 Mbps. | 100 mts. | 2 |
| Fibra Óptica | 10 Mbps. | 1 Km. | 2 |
| Coaxial delgado | 10 - 100 Mbps. | 185 mts. | 30 |
| Coaxial grueso | 10 - 100 Mbps. | 500 mts. | 100 |

**Sistema operativo de red.**

Es el software que se encarga de administrar a los usuarios y recursos que se comparten en la red como son: discos duros, impresoras, aplicaciones, etc.

El sistema operativo se escoge según las necesidades de control de la información. Existen algunas características a tomar en cuenta para seleccionar el sistema operativo que de acuerdo a nuestros requerimientos de administración de recursos (usuarios, directorios, archivos, etc.) sean cubiertos por éste, como son:

- El tipo de información que se estará compartiendo.
- Los programas que se utilizarán

El sistema operativo escogido debe ofrecer toda la seguridad que se requiere dentro de la red. La seguridad debe ir desde cual máquina se puede usar, el horario de acceso y los días en que se puede trabajar, hasta claves de acceso, archivos que se podrán compartir y los programas que se ejecutarán.

Dependiendo de las necesidades del negocio, se hace necesaria la instalación de otros productos, como son:

- Concentradores (Hub).

  Originalmente estos equipos surgieron para hacer más eficiente el cableado en redes de área local, es decir, en vez de tener un bus real con un cable recorriendo todas las estaciones, se tiene un bus estrellado en el que cada estación cuenta con una conexión hacia el concentrador y es dentro de éste que se forma el bus. Esto permite que cualquier estación se desconecte sin perturbar a las demás. (Fig. 2.8)

**CONCENTRADOR**

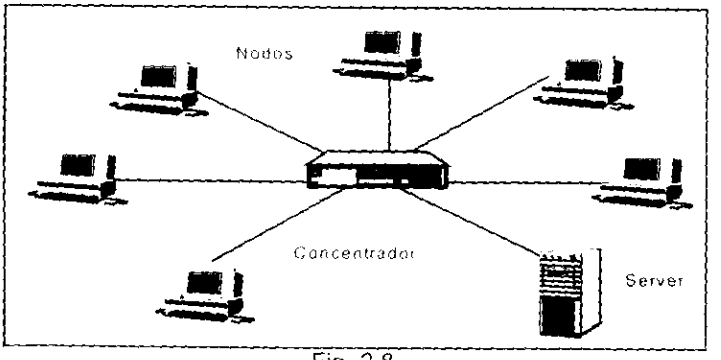


Fig. 2.8

- Repetidores.

  En ocasiones, se desea extender la longitud de una red de área local más allá de lo que permiten las condiciones de atenuación del cableado. A fin de lograr esta tarea, se emplean los repetidores que no son más que regeneradores de la señal eléctrica sin ninguna función en el plano lógico, es decir, tan sólo regeneran la señal desde el punto de vista eléctrico, pero no interpretan la información.

- Puentes.

  Es un dispositivo que conecta redes de igual tipo. Cuando una LAN se encuentra demasiado congestionada, esto es, que el tráfico existente alarga el tiempo de respuesta de los usuarios, se dice que debe segmentarse.

  Esta segmentación consiste en separar la red en dos partes, de manera que el tráfico existente en un lado corresponderá sólo a estaciones presentes en dicho segmento. Al elemento empleado para hacer esta separación se le denomina puente (bridge), el bridge identifica las direcciones contenidas en los mensajes de cada segmento. Así, si una dirección corresponde al otro lado, la dejará pasar, de lo contrario se queda en su segmento.

- Ruteadores.

  En cierta forma se puede equiparar la función de los ruteadores con la de los puentes. Sin embargo, es posible diferenciar el hecho de que el ruteador puede conectar diferentes tipos de LAN´s. Los ruteadores se emplean en redes complejas en las que hay múltiples vías de comunicación entre los usuarios de la red. El ruteador examina la dirección de destino del mensaje y determina la ruta más efectiva.

### 2.3.2 Instalación de una Red de Área Local.

A continuación se mencionan brevemente los aspectos a considerar para la instalación de una red:

- Instalar medidas de seguridad en donde se ubicará la red (detectores de humo y extinguidores, suministros de energía ininterrumpible "UPS", ventilación suficiente, etc.).
- Instalar tomas de energía eléctrica regulada.
- Instalar cableado y dispositivos en caso de requerirse (concentradores, repetidores, puentes, ruteadores).
- Instalar tarjetas de red al servidor, impresoras (en caso de ser necesario) y a todos las microcomputadoras de la red por medio de las cuales se va a

establecer la conexión. Dichas tarjetas se colocan en cualquiera de los slots de expansión contenidos en los equipos; cada una de ellas contiene los conectores para el cable del tipo elegido. Es importante mencionar que algunas tarjetas se configuran automáticamente, de no ser así, se procede a configurarla a través de los diskettes proporcionados al momento de su adquisición.

- Instalar físicamente las microcomputadoras y periféricos, conectándoseles el tipo de cable elegido.
- Instalar el software en el servidor y nodos de la red (sistema operativo de red y software aplicativo). La mayoría de este software ofrece una instalación basada en menúes. Al momento de la instalación se van respondiendo preguntas referentes al tipo de hardware sobre el que se instala la red, los recursos que se quieren compartir, los privilegios de cada uno de los usuarios, esto es, lo que puede desarrollar cada usuario dentro de la red, los directorios del disco a los que se accesan y los dispositivos a los que se les permite hacer uso.
- Administrar el servidor, nodos y periféricos de la red.

En la figura siguiente (Fig. 2.9) se muestran los componentes que se requieren para integrar una red como una semblanza de su estructura.

**COMPONENTES BÁSICOS EN UNA RED ETHERNET CON CABLE UTP**

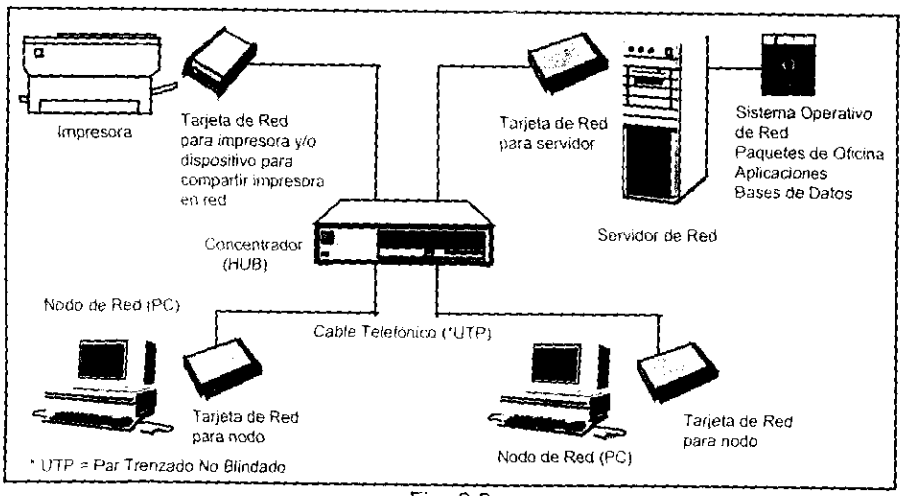


Fig. 2.9

## 2.4 SOFTWARE OPERATIVO PARA UN AMBIENTE DE REDES DE ÁREA LOCAL.

### 2.4.1 Software Operativo.

Actualmente en el mercado mexicano, los sistemas operativos de red más usados son Novell Netware, Microsoft Lan Manager y Windows NT.

El objetivo de este apartado es presentar las consideraciones más importantes que debe presentar un sistema operativo de red para su adquisición, así como los puntos que permiten al auditor definir criterios de auditabilidad y control.

Las consideraciones más importantes que debe contener un sistema operativo de red se pueden clasificar en:

- Características en cuanto al diseño del sistema operativo.
- Características del fabricante y del proveedor del sistema operativo.

**Características en cuanto al diseño del sistema operativo.**

Facilidades como servidor

*Auditoría.*

Estadísticas de actividad.
Intentos de acceso sin éxito.
Intentos de violación de seguridad.
Auditoría de recursos específicos.

*Contabilización.*

Registro de tiempo de acceso de los usuarios.
Registro de lecturas de los usuarios.
Registro de escrituras de los usuarios.
Registro de los requerimientos al servidor.
Registro de uso del espacio por usuario.

*Servicios de alerta.*

Disco lleno.
Errores excesivos.
Alerta contra intrusos.
Problema en la impresora.
Solicitud de impresión completa.

*Parámetros del servidor.*

Máximo número de usuarios por servidor.
Máximo número de archivos abiertos por servidor.

*Utilerías de supervisión.*

Desconexión forzada.
Utilería de chequeo de seguridad.
Lista de los niveles de acceso de los usuarios.
Administración remota de los archivos del servidor.

*Monitoreo del rendimiento.*

Tiempos de respuesta.
Estadísticas de la memoria caché.
Número de paquetes enviados y recibidos.
Número actual de archivos abiertos.
Número actual de conexiones.
Utilización de disco.
Demanda de disco contra el servicio.

Facilidades de compartición de recursos

*Compartición*

Colas de impresión.
Múltiples colas sobre una impresora.
Múltiples impresoras sobre una cola.
Niveles de prioridad en las colas.
Monitoreo de colas.
Retener y liberar el trabajo de impresión.
Pausa a la impresión.
Pausa a la cola.
Las estaciones pueden compartir impresoras.
Lista de las impresoras y colas disponibles.

*Integridad.*

Lectura de archivos.
Escribir o actualizar archivos.
Creación de nuevos archivos.
Borrar archivos.
Modificación de atributos de archivos.
Definición de número máximo de usuarios.
Asignación de permisos por directorio.
Asignación de permisos por archivo.
Asignación de permisos por colas.
Derechos de admisión asignados a un directorio.
Permisos que pueden ser heredados.
Tolerancia a fallas.
Monitoreo del UPS.
Disco espejo.
Servidor duplicado.

*Seguridad.*

Compartición de seguridad.
Creación de grupos de seguridad.
Definición de expiración de cuentas de usuario.
Restricciones de tiempo.
Bloqueo de claves de usuario después de varios intentos de acceso fallidos.
Cambio periódico a las contraseñas para las claves de usuario.
Permitir o prevenir que se fije una clave secreta.
Fijar la longitud mínima de la clave secreta.
Habilitar y deshabilitar claves de usuario.
Auto-desconexión después de un periodo de inactividad.

**Características del fabricante y del proveedor del sistema operativo.**

No únicamente se toma en cuenta el sistema operativo en forma aislada, sino en conjunto con el entorno que es la posición de su fabricante y proveedor en el mercado nacional.

El esquema de soporte y atención al cliente, es un requisito que se exige a los proveedores como cumplimiento a los sistemas operativos que distribuye. En pocas palabras se debe tener:

- Disponibilidad de actualizaciones.
- Disponibilidad de apoyo en casos de contingencia.
- Distribuidores en el territorio nacional.
- Disponibilidad de soporte en sitio.
- Disponibilidad de soporte vía telefónica.
- Disponibilidad de información de tendencias tecnológicas.

## 2.5 CONCEPTOS GENERALES DE AUDITORÍA.

### 2.5.1 Auditoría.

A menudo la palabra auditoría se emplea incorrectamente, considerándola únicamente como una evaluación que pretende detectar errores y fallas; incluso se ha llegado a implantar la frase "tiene auditoría" como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por consiguiente se está efectuando la auditoría. Sin embargo, el concepto de auditoría es más amplio: no sólo detecta errores, sino que es un examen crítico que se realiza con objeto de evaluar el control interno de una sección o de un organismo.

La auditoría, desde un aspecto general se define como:

**La evaluación y revisión de cualquier actividad susceptible de ser controlada.**

Otras definiciones son las que a continuación se mencionan:

"La auditoría es un examen independiente, crítico y sistemático de:

a) la dirección interna

b) estados, expedientes y operaciones contables preparados anticipadamente por la organización,

c) los documentos restantes y expedientes jurídicos y financieros de una empresa comercial o industrial, con el fin de cerciorarse de la exactitud, integridad y autenticidad de estos estados, expedientes y documentos".[2]

"La auditoría se ocupa de la verificación del sistema de información y de su funcionamiento, con el fin de determinar la confiabilidad que se le puede atribuir a la información que produce".[3]

"La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben seguirse y estimar los resultados obtenidos".[4]

Al analizar estas definiciones, se desprenden las funciones más importantes correspondientes a la auditoría como son: evaluar, verificar y analizar la información proporcionando observaciones y recomendaciones significativas para el negocio.

**Tipos de auditoría.**

**a) Con base en el personal que la efectúa:**

- **Interna.**

Desempeñada por auditores que forman parte de la empresa.

---

[2] Holmes, Arthur W. "Principios básicos de auditoría".
[3] Centro Latinoamericano de Desarrollo (IBM), "Auditoría, seguridad y control en Informática".
[4] Instituto Mexicano de Contadores Públicos, "Boletín C Normas y Procedimientos de Auditoría".

- **Externa.**

Desempeñada por auditores que no forman parte de la empresa.

**b) De acuerdo al objetivo que persigue:**

- **Financiera.**

Este tipo de auditoría verifica que las operaciones se hayan registrado de acuerdo a los principios de contabilidad y que los estados financieros reflejen el total de las mismas.

Ejemplos:

- Verifican los saldos bancarios.
- Ffectúan arqueos de caja.
- Comparan el inventario físico vs. inventario contable.

- **Operativa.**

Este tipo de auditoría verifica que los controles operativos garanticen la protección de los fondos de la empresa.

Ejemplos:

- Verifican el apego a políticas y estándares establecidos.
- Evalúan las normas de seguridad física y lógica.
- Analizan la subutilización y aprovechamiento del equipo.

**Diferencias entre la auditoría financiera y la auditoría operativa.**

| | ***Financiera*** | ***Operativa*** |
|---|---|---|
| • Personal que la efectúa. | Contador. | La gerencia. |
| • Áreas de aplicación. | Sectores financieros y contables. | Todos los sectores de la empresa. |
| • Marco de referencia. | Principios generalmente aceptados, estados contables. | Controles administrativos. |

### 2.5.2 Control Interno.

Por la complejidad de las organizaciones en las grandes empresas y por su desarrollo económico, hoy en día es necesario contar con un control interno adecuado que impida una administración muerta por desconocimiento de medios eficientes de trabajo, una contabilidad rudimentaria de registros, la carencia de presupuestos y estadísticas que ocasionan fracasos constantes a las empresas, así como errores y fraudes periódicos.

Para poder comprender lo que es el control interno, el boletín E-02 del Instituto Mexicano de Contadores Públicos señala:

> "El estudio y evaluación del control interno se efectúa con el objeto de cumplir con la norma de ejecución del trabajo que requiere que: el auditor efectúe un estudio y evaluación adecuados del control interno existente; le sirvan de base para detectar el grado de confianza que va a depositar en él; y asimismo, le permitan determinar la naturaleza, extensión y oportunidad que va dar a los procedimientos de auditoría".[5]

Por consiguiente, el control interno comprende el plan de organización, incluyendo todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar la integridad de sus activos, verificando la razonabilidad y confiabilidad de su información financiera, promoviendo la eficiencia operacional y provocando la adherencia a las políticas establecidas por la administración.

Es importante señalar los objetivos básicos y generales del control interno para poder entender su alcance.

**Objetivos básicos del control interno.**

Con base en lo expuesto anteriormente, se desprenden los cuatro objetivos básicos del control interno:

1) Protección de los activos de la empresa.
2) Obtención de información veraz, confiable y oportuna.
3) Promoción de la eficiencia en la operación del negocio.
4) Cumplimiento de las políticas establecidas por los administradores de la empresa en la ejecución de las operaciones.

Los dos primeros corresponden al aspecto de control interno contable y los dos últimos se refieren a controles internos administrativos.

[5] Instituto Mexicano de Contadores Públicos. "Boletín E-02 Normas y Procedimientos de Auditoría".

**Objetivos generales del control interno.**

Los objetivos generales de control aplicables a todos los sistemas se desarrollan a partir de los objetivos básicos del control interno enumerados anteriormente, siendo más específicos para facilitar su operación.

Es por eso que los objetivos generales de control interno de sistemas pueden resumirse como se muestra a continuación:

a) De autorización.

- Todas las operaciones deben realizarse de acuerdo con autorizaciones generales o específicas de la administración.
- Las autorizaciones deben estar de acuerdo con criterios establecidos por el nivel apropiado de administración.
- Las transacciones deben ser válidas para conocerse y someterse oportunamente a su aceptación. Todas aquellas que reúnan los requisitos establecidos por la administración deben reconocerse como tales y procesarse a tiempo.

b) De procesamiento y clasificación de transacciones.

- Todas las operaciones deben registrarse para permitir la preparación de estados financieros, de conformidad con los principios de contabilidad generalmente aceptados o con cualquier otro criterio aplicable a los estados y para mantener en archivos apropiados los datos relativos a los activos sujetos a custodia.
- Las transacciones deben clasificarse en forma tal que permitan la preparación de estados financieros, de conformidad con los principios de contabilidad generalmente aceptados y el criterio de la administración.
- Las transacciones deben quedar registradas en el mismo período contable, cuidando específicamente que se registren aquellas que afectan a más de un ciclo.

c) De salvaguarda física.

- El acceso a los activos sólo deben permitirse de acuerdo con autorizaciones de la administración.

d) De verificación y evaluación.

- Los datos registrados relativos a los activos sujetos a custodia deben compararse con los activos existentes a intervalos razonables y tomar las medidas apropiadas respecto a las posibles diferencias que existan.

Estos objetivos generales del control interno de sistemas son aplicables a todos los ciclos. No se trata de que se usen directamente para evaluar las técnicas de control interno de una organización, pero representan una base para desarrollar objetivos específicos de control interno por ciclos de transacciones que sean aplicables a una empresa individual.

El área de informática puede contribuir de dos maneras en el control interno. La primera es servir de herramienta para llevar a cabo un adecuado control interno y la segunda es tener un control interno del área y del departamento de informática.

En la primera situación se lleva a cabo el control interno por medio de la evaluación de una organización, utilizando la computadora como herramienta que auxiliará el logro de los objetivos del control interno, lo cual se puede efectuar por medio de paquetes de auditoria.

En la segunda situación se lleva a cabo el control interno del área informática. Es decir, como se señala en los objetivos del control interno, se deben proteger adecuadamente los activos de la organización por medio del control para que se obtenga la información en forma veraz, oportuna y confiable, se mejore la eficiencia de la operación de la organización mediante la informática y en la ejecución de las operaciones de informática se cumplan las políticas establecidas por la administración de todo aquello que deba ser considerado como control interno de informática.

### 2.5.3 Informática.

El concepto de informática es más amplio que el simple uso de equipos de cómputo, o de procesos electrónicos.

El sentido etimológico de la palabra **Informática**, tiene su origen en la lengua francesa INFORMATIQUE, misma que es resultado de unir las palabras INFORMATION y AUTOMATIQUE.

Constituye un recurso para dominar todos los elementos que intervienen en el proceso de la información.

En 1966, la academia francesa reconoció este nuevo concepto y lo definió del modo siguiente:

> "Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas, de la información contemplada como vehículo del saber humano y de la comunicación en los ámbitos técnico, económico y social" [6].

[6] Revista informática, artículo "Informática, una nueva ciencia".

Existen también definiciones formales de especialistas que en esta materia han enunciado:

> "Ciencia que estudia los sistemas inteligentes de información" [7].
>
> "Conjunto de técnicas de la colección, clasificación, puesta en memoria, transmisión y utilización de la información tratada automáticamente con la ayuda de programas a través de computadoras" [8].

En algunas ocasiones se emplean como sinónimos los conceptos de proceso electrónico, computadora e informática. El concepto de informática es más amplio, ya que se considera el total del sistema de información y su manejo, el cual puede usar los equipos electrónicos como una de sus herramientas.

Es evidente la unión entre la informática y la auditoría, ya que al compaginarse, permiten un mayor aprovechamiento de los recursos y por consiguiente una mayor productividad al negocio.

### 2.5.4 Concepto de Auditoría en Informática.

Después de analizar los conceptos de auditoría, informática y los diferentes tipos de auditoría, surgen las siguientes preguntas: ¿ Qué es auditoría en informática ? y ¿ Cuál es su campo de acción ?

> "Auditoría en informática es la revisión y evaluación de los controles, sistemas y procedimientos de informática de los equipos de cómputo, su utilización, eficiencia y seguridad, así como 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" [9].

La misión de auditoría en informática es vigilar que la institución cuente con un sistema de control interno que permita la protección de activos informáticos, a través de la evaluación de los sistemas de información y la tecnología en que se soportan para la obtención de información oportuna y veraz, apegándose a políticas, normas y estándares establecidos.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistema o procedimiento específico, sino que además

---

[7] Mora, José Luis y Molina, Enzo, "Introducción a la informática".
[8] Petí Robert, Le Robert, "Diccionario de la lengua francesa".
[9] Echenique, José Antonio, "Auditoría en Informática".

habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización especifica (departamento de cómputo, departamento de administración de redes, gerencia de procesos electrónicos, etc.), que hará posible el uso de los equipos de cómputo.

Su campo de acción es:

a) La evaluación administrativa del departamento de procesos electrónicos.

b) La evaluación de los sistemas y procedimientos y de la eficiencia que se tiene en el uso de la información.

c) La evaluación del procesamiento de datos y de los equipos de cómputo (redes, computadoras, periféricos, etc.).

**Objetivos de la Auditoria en Informática.**

Los objetivos de la auditoría en informática pueden variar de acuerdo al tipo de situación, pero generalizando, los retos más importantes son:

Gestión, adquisición y/o renta de bienes informáticos

Verificar que el departamento de adquisiciones lleve un control permanente a los contratos con los proveedores de equipo, maquiladores de software, empresas que brinden mantenimiento preventivo y correctivo, así como con las empresas con que se tengan convenios en caso de contingencia.

Administración y operación

Evaluar las funciones en las áreas de diseño, administración, operación y mantenimiento.

Documentación

Verificar el contenido de la documentación, que debe estar determinada y delineada por las normas y/o estándares establecidos por la empresa.

Inventario de equipo y software

Realizar chequeos de la ubicación física de cada uno de los dispositivos del equipo, su estado y mantenimiento. Lo mismo se hace con el software disponible, ya sea contratado o desarrollado internamente.

Normas y estándares del área de sistemas

Verificar que el área de sistemas desarrolle las normas y estándares que determinen las actividades de análisis, diseño, programación, operación, etc., debiéndose difundir e implantar a toda la institución.

Cambios y problemas

Evaluar los controles existentes para el registro, atención y solución de fallas, así como la actualización y mantenimiento a la plataforma de redes de área local.

Niveles de servicio

Verificar que el área encargada de la administración cumpla con los niveles de servicio pactados, así como evaluar el control que se efectúa para su calificación.

Cronogramas de trabajo

Evaluar periódicamente el cumplimiento de los planes de trabajo en cuanto a resultados obtenidos contra resultados planeados.

Licencias de software

Verificar que el área administrativa y el proveedor de servicios mantengan un control adecuado en cuanto a la existencia de paqueteria [illegible]izada y actualización del software de acuerdo a convenios y contratos establecidos.

Mantenimiento del software

Verificar estrictamente que las modificaciones a cualquier programa se realicen con la autorización debida y apegándose a las normas y estándares establecidos.

Seguridad física

Verificar que el área disponga de instalaciones adecuadas para el equipo de cómputo, en cuanto a pisos falsos, estabilizadores, protección contra incendio, seguridad en el acceso del personal y demás aspectos relacionados con seguridad.

Seguridad lógica

Evaluar los controles existentes para la protección de bibliotecas y archivos vitales, asignación de perfiles y atributos a administradores y usuarios.

Plan de contingencia

Verificar que el área responsable desarrolle y mantenga un plan en caso de desastre por suspensión temporal o indefinida de los servicios proporcionados.

Equipos alternos

Asegurar la realización de un convenio con otra instalación similar para lograr un respaldo en caso de suspensión temporal o total de los procesos, a efecto de dar continuidad a las operaciones.

Bóveda fuera de sitio (B.F.S.)

Constatar la existencia de un lugar externo a las oficinas y de las instalaciones que albergan a los equipos de cómputo, donde se mantengan copias de respaldo que permitan aplicar un plan de reprocesos de la operación.

### 2.5.5 Necesidad de la Auditoría en Informática en un ambiente de Redes de Área Local.

Conforme han evolucionado, las computadoras se han vuelto más rápidas, la administración del centro de cómputo se ha complicado, por lo que se requiere de personal mejor capacitado y de un mayor control de datos e información.

La auditoría en informática en un ambiente de redes de área local, surge como necesidad de la empresa para establecer un control sobre todas las actividades, personal, riesgos y eficiencia del área de redes, requiriendo para la realización de dichas actividades la formación de auditores en esta área, personas que posean conocimientos para determinar y calificar las condiciones de la misma.

Las instituciones hoy en día requieren que la administración y operación de su infraestructura de cómputo satisfaga las necesidades del negocio, cuente con los controles y esquemas de seguridad suficientes que garanticen la protección de activos, continuidad en el servicio y una adecuada utilización de recursos.

Básicamente las necesidades para auditar el ambiente de redes de área local son:

- Cumplimiento en la gestión, adquisición y/o renta de bienes informáticos.
- Administración y operación adecuadas.
- Apego a estándares, políticas y procedimientos.
- Atención a cambios y problemas.
- Cumplimiento en los niveles de servicio pactados.
- Uso correcto y aprovechamiento de licencias de software.
- Seguridad física y lógica.
- Plan de contingencia acorde a las necesidades del negocio.

# SEGURIDAD INFORMÁTICA EN EL AMBIENTE DE REDES DE ÁREA LOCAL

El desarrollo de las redes de computadoras (LAN) ha propiciado un mayor manejo de los recursos de cómputo que se comparten entre todos los usuarios, también ha aumentado el intercambio de datos e información.

En este ambiente de intercambio de recursos, la protección de la información y de los recursos físicos de cómputo se vuelven para algunas organizaciones algo imperativo, llegando algunas a valorar su información como el recurso más importante de la organización (por encima de sus recursos físicos, de capital, etc.).

Estas tareas de protección o seguridad impactan en forma diferente a cada uno de los recursos, así tenemos la seguridad física, referida básicamente al hardware y equipos relacionados y la seguridad lógica, donde se involucra al software y programas producto.

También es necesario desarrollar las políticas de uso y procedimientos de seguridad según los recursos de que se trate, pero si en algún momento llegara a fallar la seguridad por cualquier acontecimiento, es necesario desarrollar un **Plan de Contingencia** que pueda ayudar a que el daño sea menor.

## 3.1 SEGURIDAD FÍSICA.

### 3.1.1 Concepto General.

Mantener la seguridad física es un primer paso para proteger las instalaciones de cómputo y comunicaciones. Podemos definirla básicamente como "un conjunto de lineamientos y procedimientos cuyo objetivo es evitar o disminuir la exposición a riesgos ya sean internos o externos en las instalaciones físicas de cómputo".

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, debido a contingencias como incendio, inundación, condiciones ambientales, ataque por intrusos, disturbios, sabotaje, etc., y continuar en un medio de emergencia hasta que sea restaurado el servicio completo.

#### 3.1.1.1 Ubicación.

En el pasado se acostumbraba instalar los equipos de cómputo en un lugar visible, con grandes ventanales constituyendo el orgullo de la organización, por lo que se consideraba necesario que estuviese a la vista del público y con una gran cantidad de invitados a visitarlos. Esto ha cambiado de modo radical, principalmente por el

riesgo de terrorismo o sabotaje. Pensemos que una persona que desea perjudicar a la organización querrá dañar su cerebro o centro de información, por lo que en la actualidad se considera extremadamente peligroso tener el centro de cómputo en las áreas de alto tráfico de personas.

Para planear la instalación de un centro de cómputo deben intervenir desde el principio los especialistas de las áreas de informática, inmuebles o construcciones, organización y de seguridad, de tal manera que se encuentre un equilibrio entre la magnitud del equipo y sus operaciones, el valor o confidencialidad de la información que procesará, así como las pérdidas en caso de suspensión de operaciones, la disponibilidad de espacios o terrenos, recursos económicos disponibles y la capacidad técnica y de recursos humanos del área de seguridad.

Las rutas de acceso al centro de cómputo tienen que ser limitadas, no debe tener muros exteriores ni ventanas. El centro de cómputo no debe situarse en sótanos ni planta baja, tampoco en el último piso del edificio (sobre todo en un edificio alto). Tampoco deben instalarse en zonas con fallas geológicas. En general, son preferibles las zonas suburbanas para instalar centros de cómputo y éstos deben encontrarse por lo menos a 60 metros de distancia del acceso público más cercano. No deben estar junto a áreas públicas tales como centros comerciales (por riesgo de bombas), estacionamientos (por riesgo de autobombas) o restaurantes (por riesgo de explosiones en las cocinas).

En lo posible, se deben tomar precauciones en cuanto a la orientación del centro de cómputo (por ejemplo, evitar los lugares expuestos a periodos prolongados de luz solar). Se deben evitar en lo posible los grandes ventanales, los cuales además de que permiten la entrada de la luz solar y calentamientos innecesarios en los equipos, pueden ser un riesgo para la seguridad del centro de cómputo.

### 3.1.1.2 Tolerancia a fallas.

Las computadoras poseen especificaciones muy estrictas de energía y condiciones ambientales, como temperatura y humedad. La carencia de éstas conducen a una significativa pérdida de tiempo de trabajo. Esta categoría incluye los siguientes riesgos importantes:

Falla de la Corriente Eléctrica

Las consecuencias de una interrupción en el suministro de electricidad son proporcionales al grado de dependencia en la computadora.

Falla en el Sistema de Aire Acondicionado

Este sistema controla la temperatura y la humedad, pudiendo proporcionar filtración de aire. Una falla en este sistema causa un paro inmediato del procesamiento, ya que la temperatura aumenta rápidamente dado que las computadoras y en especial dispositivos como unidades de disco y cinta (que contienen motores), generan grandes cantidades de calor.

Humedad

La humedad afecta no sólo a los equipos sino también a las cintas, discos y papel, por esta razón se deben instalar sistemas de detección de fugas de líquidos. No deben pasar tuberías por encima ni debajo ni a los lados directamente del centro de cómputo, almacenes de cintas, discos, papel, etc. Se debe tener cuidado con fugas de agua de equipos enfriados por este líquido y fugas de los aparatos de aire acondicionado.

Temperatura

Las instalaciones de cómputo son muy sensibles a la temperatura, incluso temperaturas de 50 a 60 grados centígrados pueden tener efectos muy dañinos en equipo y medios de almacenamiento de información. Por lo tanto deben existir sistemas de aire acondicionado con salidas bien distribuidas. La construcción del centro de cómputo tiene que estar bien diseñada, de modo que no haya fugas de aire frío ni entradas de aire caliente, polvo o luz solar.

En todas las instalaciones existen grandes problemas con el aire acondicionado, ya que éste implica un doble riesgo: las fluctuaciones o la descompostura del sistema de A.C., pueden ocasionar que los equipos tengan que ser apagados, además de ser una fuente de incendios frecuente. También son susceptibles a la intrusión física, especialmente a través de los ductos.

Para afrontar estos riesgos, se requiere instalar equipos de A.C. de respaldo, instalar rejillas de protección en todo el sistema de ductos, así como detectores de incendios en los mismos.

### 3.1.1.3 *Alimentación eléctrica.*

Todo centro de procesamiento de datos deberá considerar la instalación de equipos que garanticen un suministro eléctrico en todo momento y con las especificaciones adecuadas como los Uninterruptable Power Source (UPS). La selección de estos equipos debe decidirse basándose en los requerimientos de energía, reserva de electricidad y confiabilidad (determinar en promedio cuantas veces al día se usarán las pilas del UPS).

Sin embargo, las pilas que tienen la mayoría de los UPS no duran más de 20 minutos, por lo que para proveer electricidad por un tiempo mayor es necesario instalar un generador de respaldo (normalmente funcionan con diesel). El suministro de energía debe considerar el consumo del equipo de aire acondicionado, la computadora y sus periféricos, así como equipos de redes y telecomunicaciones.

### 3.1.1.4 Control de acceso.

Este tipo de sistemas garantizan que sólo el personal autorizado podrá ingresar al Centro de Procesamiento de Datos, con lo cual se disminuirá considerablemente el riesgo de robo, destrucción o manipulación no autorizada de equipos e información. Los controles durante los descansos y cambios de turno son de especial importancia. El medio que permite identificar al personal, puede ser a través de teclados y claves numéricas, otros realizan la identificación mediante lectores de tarjetas codificadas o tarjetas con cintas magnéticas, otros más lo hacen con una combinación de los sistemas mencionados.

Existen otros sistemas de identificación que se basan en quién es la persona y no en que tiene la persona, como los de reconocimiento de firmas, de huellas digitales, sistemas de reconocimiento de las líneas de la mano, de voz, reconocimiento de la retina, etc., llamados sistemas biométricos. A los sistemas descritos anteriormente se les llama "sistemas de identificación y autentificación", ya que intentan no sólo conocer la identidad del usuario, sino de saber si esa identidad es auténtica. Cuando se utilicen estos sistemas automáticos para las puertas, debe existir una puerta adicional que se usa como salida de emergencia. Las aperturas que se usen para recepción y entrega de datos deberían estar en una área separada del centro de cómputo con una división a prueba de fuego.

Tomando en cuenta que el centro de cómputo está (en la mayoría de los casos) dentro del edificio de oficinas de la empresa, las medidas de control de acceso al centro de cómputo comienzan con las medidas de control de acceso al edificio.

Barreras de protección

Básicamente hay cuatro niveles jerárquicos:

a) Protección perimetral: los controles ubicados en el área externa del predio y que lo limitan con las colindancias inmediatas, por ejemplo: bardas, rejas, puertas de acceso, casetas de vigilancia, etc.

b) Protección de inmueble: se consideran los controles ubicados en la periferia del edificio mismo, por ejemplo: muros de material fuerte, puertas, etc.

c) Protección del área: se logra con la sectorización, que consiste en el agrupamiento de las áreas por funciones, de tal manera que no existan cruces de personal ni de información entre las mismas. Con esto se obtiene una distribución racional de los recursos de seguridad con que se cuente. Deben vigilarse las entradas normales al área y otras como ductos de aire acondicionado con sistemas de alarma, sistemas electromecánicos de detección de intrusos, etc.

d) Protección de objeto: esta última barrera nos permite diseñar la protección de áreas específicas que por su importancia o valor requieran de un tratamiento especial, por ejemplo: man-traps, sistemas sofisticados de detección de intrusos como sistemas fotométricos, sistemas de detección de movimientos por sonido, ultrasonido o microondas, sistemas de detección de ruido y vibración (acústicos y sísmicos), detectores de metales en las entradas, etc.

Guardias y Monitoreo Electrónico

Se emplea personal policiaco que permanece constantemente a la entrada del centro de cómputo, vigilando o al menos haciendo rondas periódicas o monitoreando a través de un circuito cerrado de televisión.

Procedimientos Administrativos

Se utilizan gafetes de identificación, listas de acceso, áreas restringidas, etc.

Control de Acceso a Terceras Personas

Aquí se incluye al personal de limpieza, a los técnicos de los diversos sistemas localizados en el centro de cómputo (por ejemplo: aire acondicionado, impresoras, etc.) y a los visitantes. Todos ellos deben ser identificados plenamente, controlados y vigilados en sus actividades durante el acceso.

Sistemas Biométricos

Cinco tecnologías biométricas son las que se están comercializando principalmente: patrón de huellas digitales, geometría de la mano, "scaneo" retinal, verificación de voz y dinámica de firmas, que a continuación revisaremos brevemente. La necesidad de un buen sistema de identificación es por lo que muchos consumidores compran sistemas biométricos, pero éstos no pueden ser cien por ciento exactos todo el tiempo. Existen dos tipos de errores: el dispositivo biométrico rechaza a una persona cuya identidad es válida y la frecuencia con que el dispositivo acepta a un impostor.

Patrón de Huellas Digitales

Es una técnica de identificación personal con la que estamos muy familiarizados, por lo que el mercado rápidamente la aceptó. Hay dos tecnologías: comparación de patrones y comparación de minutas, siendo esta última la de mayor credibilidad porque es la que usa la Oficina Federal de Investigaciones de los Estados Unidos (FBI).

Geometría de la mano

Estos sistemas miden, graban y comparan la longitud de dedos, translucidez de la piel, grosor de la mano o forma de la palma.

"Scaneo" retinal

Los patrones de venas en el ojo humano son únicos. Un scanner retinal analiza esas venas para determinar la identidad de una persona. Esta tecnología, se usa principalmente en instalaciones de alta seguridad. Muchos consumidores estaban preocupados acerca de contraer gérmenes, pero ahora los scanners de retina no requieren contacto.

Verificación de voz

Los primeros sistemas tenían tasas de error muy altos, por ejemplo, un resfriado podía alterar la voz y dejar a un usuario autorizado sin la posibilidad de ser aceptado. Afortunadamente, esto se ha corregido casi en su totalidad.

Dinámica de Firma

Desafortunadamente, los falsificadores son muy hábiles para duplicar firmas. Por esta razón, las firmas estáticas no son útiles como identificación personal. Las técnicas más nuevas se basan en un censo electrónico y en la medición de los movimientos de la pluma mientras se está firmando. La falsificación de este tipo de firma es casi imposible. Estos sistemas ahora se basan en un tapete sensible, donde se firma. Debido al tiempo extra y el esfuerzo para firmar, este método no es un buen candidato para el control de acceso físico a áreas con alto volumen de tráfico, especialmente donde las mismas personas están entrando y saliendo constantemente. Su aplicación para control de acceso es más adecuada para terminales o entradas a instalaciones de alta seguridad.

### 3.1.1.5 Riesgo de inundación.

Se considera inundación al flujo o a la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por

falta o insuficiencia de drenaje tanto natural como artificial. Esta es la causa del mayor número de desastres en instalaciones de cómputo. Entre las causas más comunes de inundaciones están: fugas de tuberías de agua, aire acondicionado (fugas de agua o condensación), sistemas de enfriamiento por agua (así se enfrían algunos equipos computacionales), rociadores, etc.

Resulta importante tanto la ubicación como el diseño del edificio y del centro de cómputo, el sistema de drenaje debe ser adecuado y suficiente (no deben pasar tuberías por encima ni debajo ni a los lados directamente del centro de cómputo). También es necesario contar con cubiertas plásticas anti-inflamables para el equipo de cómputo y detectores de agua, e idealmente con bombas para evacuar rápidamente el agua. Resulta necesario contar con medidas para detectar la intrusión de agua antes de que sea necesario apagar la computadora. Existen sistemas para detectar la presencia de agua bajo el piso antes de que se vuelva peligrosa para el equipo. Además de señalar fugas con una alarma, estos sistemas deben proveer los medios para quitar automáticamente la energía a los equipos.

### 3.1.1.6 Protección contra incendios.

Los incendios son definidos como la ignición no controlada de materiales inflamables y explosivos, dado el uso inadecuado de combustibles, fallas en instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. Los daños que produce un incendio son generados por el fuego, el calor, los productos de combustión, el agente extinguidor y tienen como consecuencia destrucción de construcciones y estructuras. Los incendios son comúnmente considerados como el principal y el más temido riesgo en instalaciones de cómputo; sin embargo, estadísticamente el agua es la causa del mayor número de desastres en instalaciones de cómputo.

Las medidas de prevención de incendios empiezan desde el diseño y construcción del edificio y del centro de cómputo, así como la selección de su ubicación. Es importante utilizar muebles de oficina no combustibles (deben ser metálicos), gabinetes de almacenamiento resistentes al fuego, cajas de seguridad contra incendios, pegar placas con la descripción (clara y breve) de los procedimientos de emergencia. Son de gran importancia los sistemas de detección de humo y de calor (el detector de humo que se elija debe ser capaz de detectar los distintos tipos de gases que desprendan los cuerpos en combustión), los cuales deben ser instalados de acuerdo a las corrientes de aire, ya que los conductores de A.C. pueden difundir el calor o el humo y no permitir que se active el detector.

Tienen que instalarse detectores en los gabinetes, ductos de A.C. bajo el piso falso, en el techo, etc., y estar conectados a sistemas de alarma (o directamente al departamento de bomberos) y además deben señalar la ubicación exacta de la

fuente. Estos sistemas de detección pueden proveer otras funciones, como abrir salidas de emergencia, cerrar puertas, controlar elevadores, apagar los equipos y ventiladores, etc. Los mecanismos de liberación del agente extinguidor "agua", dióxido de carbono o gas halón deben trabajar automáticamente con opción a inhibirse manualmente.

Adicionalmente, deben instalarse extinguidores manuales en lugares apropiados de acceso inmediato (los operadores deben estar capacitados en el uso de estos equipos y de todos los procedimientos de emergencia). Estos extinguidores y el equipo de gas se deben revisar con regularidad para asegurar su buen funcionamiento. El equipo respiratorio debe estar a la mano, porque las cintas magnéticas quemadas despiden humo nocivo. Es necesario señalar que un riesgo asociado al incendio es la posterior inundación por el agua utilizada por los bomberos para extinguir el incendio, si los sistemas de drenaje no son adecuados. Asimismo, se debe establecer un plan de evacuación del personal.

Una importante, pero frecuentemente desapercibida causa de incendios, es la contaminación ambiental. La entrada de partículas contaminantes al equipo electrónico, puede causar algún corto circuito e incluso iniciar incendios en los equipos. Pero: ¿cómo se introducen los contaminantes al ambiente supuestamente limpio del centro de cómputo? Mientras que ciertos contaminantes son introducidos por los operadores (incluyendo fibra de ropa, partículas de cabello y piel, ceniza, etc.), la mayoría de las partículas son traídas por el aire y transportadas dentro de los equipos sensibles a través de las entradas de aire debajo del piso falso. Algunos de los contaminantes más comunes son: el polvo de cemento, yeso y tierra, contaminación "urbana" y partículas metálicas (conductoras de electricidad). Muchos contaminantes pueden absorber humedad además de conducir electricidad.

## 3.2 SEGURIDAD LÓGICA.

### 3.2.1 Concepto general.

El software y los datos son valiosos activos de las empresas y los daños considerables tales como pérdidas financieras, pueden presentarse si éstos se pierden, son robados o modificados sin control. Implementando y forzando controles de seguridad en la información, se evita cualquier revelación accidental o intencional de información a personas no autorizadas a modificarla o destruirla.

Los recursos de la red que deben ser considerados al estimar la seguridad lógica, son:

- Software. Programas fuente, programas objeto, utilerías, programas de diagnósticos, sistemas operativos, programas de comunicaciones, etc.
- Datos. Durante la ejecución, almacenados en línea, archivos fuera de línea, apoyos, bitácoras de auditoría, bases de datos, en tránsito sobre medios de comunicación.
- Gente. Usuarios, personal para operar sistemas.
- Documentación. Programas, sistemas y procedimientos administrativos.

Una vez identificados los recursos que necesitan protección, se deberán identificar las amenazas a tales recursos.

### 3.2.1.1 Virus.

Es un programa parásito escrito intencionalmente para alterar la forma de operar de la computadora sin su permiso o conocimiento.

En una red local, basta que una de las computadoras (terminal con disco), esté contaminada para que toda la red corra peligro. Es fundamental que el servidor de la red esté constantemente protegido y que como mínimo, cada terminal con disco sea probada antes de conectarse lógicamente a la red. La situación ideal es que todas las terminales posean sistemas de protección.

Además de los sistemas de protección, es necesario que los datos sean respaldados (copiados o duplicados) constantemente. De esta forma, en caso de que ocurra una fatalidad, los perjuicios serán mínimos.

Existen algunos virus específicos para redes. Uno de ellos es el denominado CZ2986. Fue desarrollado en Checoslovaquia en 1991. Permanece residente en la memoria, interceptando llamadas a NetWare. Recoge 15 nombres y claves de usuario, guardándolas en un archivo infectado.

Otro virus similar, denominado GP1 (Get Password 1 ó Verificar Clave 1), fue descubierto en Europa en 1991. Es una variante del virus Jerusalén que intenta amenazar la clave de los usuarios. Este virus no funciona en versiones de NetWare posteriores a 1987.

En general, los esquemas de seguridad de las redes, pueden impedir la propagación de los virus, minimizando su acción.

Sin embargo, surgen algunos problemas, los archivos de datos no pueden ser protegidos contra modificaciones. Naturalmente, si un usuario puede alterar el contenido de un archivo, un virus también puede hacerlo. Los programas pueden ser protegidos con atributos del tipo " ejecutable only " (no provisto en el DOS). De

esa forma, esos archivos no pueden ser modificados, sólo se ejecutan. Los archivos de datos no pueden contar con ese atributo.

Algunas sugerencias para evitar virus en redes locales se muestran a continuación:

- Realice backup de archivos y programas con frecuencia.
- Evite ingresar a la red como gerente o supervisor. La facilidad de acceso, permite una propagación más rápida de virus eventuales.
- Mantengase informado acerca de los principales tipos de virus, nuevos lanzamientos, nuevos productos, etc. De esta manera usted podrá saber si su red es vulnerable a alguna plaga y cómo proceder para evitar cualquier tipo de problema.
- Procure proteger a los archivos .EXE y .COM con el atributo " read only ".
- Mantenga informados a los empleados y demás personas que trabajan con la red.
- Utilice un buen software antivirus que tenga condiciones para trabajar en red. Procure probar la integridad de un cliente cuando ingresa. Pruebe los disquetes que son de terceras personas. Procure utilizar programas residentes que automaticen la verificación de los disquetes.

Algunas sugerencias en caso de contaminación, se muestran a continuación:

- Apague la máquina (cuanto más tiempo esté encendida más tiempo estará actuando el virus).
- Inicie el sistema desde un disquete limpio y protegido contra escritura.
- Utilice algún software del tipo cazador y revise la computadora infectada. No conecte el equipo a la red.
- Recupere o elimine los programas o sectores infectados.
- Conéctese a la red como un usuario común (con acceso de lectura e indagación de archivos y programas). No ingrese como gerente o supervisor o cualquier otra categoría que implique el acceso a grabar datos en la red, modificar archivos, etc. Revise todos los archivos y programas.
- Revise otras computadoras conectadas a la red. Siempre conéctese con los mínimos derechos posibles (acceso a lectura e indagación de archivos y programas).
- Analice cómo pudo haber ocurrido la contaminación y asegúrese de evitar que eso se repita.

### 3.2.1.2 Claves de acceso.

Password

**Definición de acceso no autorizado**. Solo se permite el acceso a los recursos de red a usuarios autorizados. A esto se le llama *acceso autorizado*. Una amenaza común es el acceso no autorizado, el cual puede ser de diferentes formas, como utilizar la cuenta de otro usuario para obtener acceso a la red y sus recursos. En general, el uso de cualquier recurso de red sin el permiso previo se considera *como acceso no autorizado*.

**Riesgo de divulgar información.** La divulgación de información, ya sea voluntaria e involuntaria, es otro tipo de amenaza. Se deberá determinar el valor o sensibilidad de la información guardada en las computadoras, por ejemplo, en los hospitales, compañías de seguros e instituciones financieras se mantiene en confidencialidad la información. Su divulgación podría ser dañina para sus clientes y para la reputación de su compañía.

**Servicio denegado.** Las redes enlazan recursos valiosos como computadoras y bases de datos y proporcionan servicios de los cuales depende una organización.

La mayoría de los usuarios de esas redes confía en estos servicios para realizar de manera eficiente su trabajo y si estos servicios no están disponibles, hay una pérdida o disminución en la productividad.

Ejemplos de como afecta a la red un servicio denegado son:

- Una red puede volverse inservible mediante los actos de un paquete extraviado.
- Una red puede volverse inservible a causa del flujo de tráfico.
- Una red podrá ser fraccionada al inhabilitar un componente crítico de la red, como un ruteador que une los segmentos de red.
- Un virus podrá restar velocidad o inhabilitar un sistema de cómputo al consumir los recursos del sistema.
- Los dispositivos para proteger la red podrían revertirse.

Uso de la red y responsabilidades

Se deben contemplar los siguientes aspectos:

¿ A quién se le permite utilizar los recursos ?

¿ Cuál es el uso correcto de los recursos ?

¿ Quién está autorizado para garantizar el acceso y aprobar el uso ?

¿ Quién debe tener privilegios de administración del sistema ?

¿ Cuáles son los derechos y responsabilidades del usuario ?

¿ Cuáles son los derechos y responsabilidades del administrador del sistema frente a los del usuario ?

¿ Cómo identificar a quién se le permite utilizar los recursos de la red ?

Puede hacerse una lista de los usuarios que requieren ingresar a los recursos de la red. No es necesario tomar en cuenta a cada usuario de la red. La mayoría de los usuarios se dividen en grupos como usuarios de cuenta, abogados corporativos, ingenieros, etc. También se tendrá que incluir una clase de usuarios llamados usuarios externos. Estos pueden ser aquellos que no son empleados.

Identificar el uso correcto de un recurso

Después de determinar a cuáles usuarios se les permite ingresar a los recursos de la red, deberá proveer guías para el uso aceptable de los recursos, las guías dependerán de la clase de usuario, como son usuarios externos, programadores, desarrolladores de software, etc. La política debe establecer que tipos de uso de red son aceptables e inaceptables y que tipo de uso será restringido.

Además, la política de seguridad de la red deberá identificar a quién esté autorizado a otorgar el acceso a sus servicios. Al poder identificar a las personas encargadas de otorgar el acceso a la red, se podrá averiguar que tipo de acceso o control ha sido otorgado.

El reto es balancear el acceso restringido con privilegios especiales para hacer a la red más segura, esto es, darle acceso a la gente que necesita estos privilegios para llevar a cabo su trabajo otorgando solamente el privilegio necesario para desempeñar las tareas necesarias.

También se debe contar con políticas en la selección de una contraseña inicial. Esta contraseña deberá ser lo más segura posible a fin de que el sistema no sea fácilmente vulnerable.

Cabe señalar que es un error permitir que los usuarios continúen utilizando la contraseña inicial por tiempo indefinido. Se deberá forzar a los usuarios a cambiar las contraseñas frecuentemente. Algunos sistemas cuentan con una política de caducidad de contraseña.

¿ Qué hacer con la información delicada ?

Se deberá determinar que tipo de datos delicados tienen que ser guardados en un sistema específico, los datos extremadamente delicados deberán restringirse a algunos anfitriones y administradores del sistema.

Antes de otorgar el acceso a los usuarios a un servicio, es necesario considerar los servicios e información existentes a los cuales puede ingresar un usuario. Si el usuario no tiene necesidad de manejar los datos delicados, entonces no deberá tener acceso a dichos datos.

Confidencialidad

La confidencialidad puede definirse como el acto de mantener las cosas ocultas o secretas. Esta es una consideración importante para varios tipos de datos delicados.

Las siguientes son algunas situaciones en las que la información es vulnerable de ser divulgada:

- Cuando la información se guarda en el sistema de cómputo.
- Cuando la información está en tránsito hacia otro sistema en la red.
- Cuando la información se guarda en cintas de respaldo.

El acceso a la información que se guarda en una computadora se controla con permisos de archivo, listas de control de acceso y otros mecanismos similares. La información que está en tránsito puede protegerse mediante encriptación o compuertas de barreras de protección. Es posible utilizar la encriptación para proteger las tres situaciones.

¿ Cómo detectar y vigilar la actividad no autorizada ?

Cualquier intento de intrusión deberá ser detectado lo más rápido posible. Es factible implantar varios procedimientos simples para detectar los usos no autorizados de un sistema de cómputo. Algunos procedimientos descansan en las herramientas suministradas por el proveedor del sistema operativo.

Procedimientos para manejo de cuentas

Al crear cuentas de usuario se deberá tener cuidado en examinar el archivo de contraseñas privilegiadas. Las cuentas sin contraseña son peligrosas, incluso si carecen de un intérprete de comando, como las cuentas que existen sólo para observar quién está registrado en el sistema. Si estas cuentas no se preparan bien, la seguridad del sistema puede verse comprometida. Por ejemplo, si la

cuenta del usuario anónimo utilizada por FTP (protocolo de transferencia de archivos) no se establece de manera correcta, podría permitir que cualquier usuario entre al sistema y retire archivos. Si se cometieran errores al establecer esta cuenta y el acceso de escritura al sistema de archivos se otorgara en forma inadvertida, un intruso podría cambiar el archivo de contraseñas o destruir el sistema.

Cuando un usuario privilegiado abandona la organización, también se debe estar alerta para cambiar las contraseñas de las cuentas privilegiadas. Además, es necesario eliminar las cuentas para todos aquellos usuarios que hayan abandonado la compañía.

### 3.2.1.3 Encriptación.

¿ Cómo utilizar la encriptación para proteger la red ?

La encriptación puede utilizarse para proteger los datos en tránsito, así como los datos guardados.

La *encriptación* puede definirse como el proceso de tomar información que existe de manera legible y convertirla en una forma que otros no puedan entender.

Si el receptor de los datos encriptados desea leer los datos originales, éste deberá convertirlos al original mediante un proceso llamado *desencriptación*. Para realizar la desencriptación, el receptor debe poseer una pieza especial de datos llamada clave.

La ventaja de usar la encriptación es, que aunque otros métodos para proteger sus datos (listas de control de acceso, permiso de archivo, contraseñas, etc.) fueran vencidos por un intruso, los datos todavía carecerán de significado para él.

Métodos de encriptación

*Estándar de encriptación de datos (DES)*

DES es un mecanismo de encriptación de datos de uso generalizado. Este transforma la información de texto llano en datos encriptados llamados *texto cifrado* mediante el uso de un algoritmo especial y valor *semilla* llamado clave.

*Crypt.*

En los sistemas UNIX es posible utilizar el comando crypt para encriptar los datos. Este método no es muy seguro, ya que aun y cuando las rutinas que se necesitan

para encriptar la información están disponibles, los programas que desencriptan los datos no están disponibles fuera de Estados Unidos.

*Correo de privacidad mejorada (PEM)*

El correo electrónico con frecuencia es enviado a través de Internet por medio de SMTP (protocolo de transferencia de correo simple). Este protocolo es muy simple y transmite datos a la vista. Más aún, se puede usar para transmitir sólo datos de texto ASCII. Si desea enviar un mensaje encriptado tendrá que utilizar medios indirectos. Primero deberá encriptar el mensaje. Esto convierte al mensaje en un archivo binario. Puesto que SMTP no puede emplearse para transmitir datos binarios, deberá codificar los datos binarios como texto.

Una forma popular de realizar esto en Internet, es hacer uso de una utilería llamada uuencode. El receptor del correo electrónico debe recurrir a la utilería uuencode para convertir el mensaje de texto a su forma binaria encriptada original. Si el receptor conoce la clave, podrá desencriptar el mensaje.

Otro enfoque es PEM (correo de privacidad mejorada), el cual proporciona los medios para encriptar de manera automática los mensajes de correo electrónico antes de enviarlos. No hay procedimientos separados que se tengan que invocar para encriptar el mensaje de correo. Por lo tanto, aunque fuera interceptado en un anfitrión de distribución, el interceptor no podrá leer el correo encriptado.

### 3.2.1 Autenticación.

Autenticación del origen

Cuando se recibe un correo electrónico, el encabezado indica quién envió el mensaje, pero es posible que alguien falsifique el encabezado para que aparezca un mensaje enviado desde otra dirección. A esto se le llama *suplantación* de dirección de correo electrónico. Para evitar esto, se utiliza una técnica llamada autenticación del origen.

La autenticación del origen brinda los medios para evaluar si el autor del mensaje es quien dice ser. La autenticación del origen es implantada por lo general por un criptosistema de clave pública.

Un *criptosistema* utiliza dos claves. Éstas son independientes en el sentido de que una no puede derivarse de la otra mediante cualquier procedimiento matemático o algorítmico. Una de las claves es una clave pública, lo que significa que puede ser hallada con facilidad por cualquier persona y que no se ha intentado esconderla. La otra clave se llama clave privada, esto es, que la conoce sólo el grupo que la posee.

En un criptosistema de clave pública, el originador utiliza una clave privada para encriptar el mensaje. El receptor emplea la clave pública que obtiene de quien originó el mensaje para desencriptar dicho mensaje. La clave pública se usa para autenticar que sólo el originador podría haber usado su clave privada.

Integridad de la información

Cuando un archivo o documento es enviado en la red, se debe tener alguna forma de verificar que el archivo o documento no ha sido alterado. Esto se llama integridad de la información y se refiere al proceso que verifica que la información enviada esté completa y sin cambios desde la última vez que se verificó.

Si la información es enviada en forma electrónica por la red, una manera de asegurarse que no ha sido modificada es utilizar sumas de verificación.

¿ Cómo usar las sumas de verificación ?

La suma de verificación (checksums) son un mecanismo muy simple y efectivo para verificar la integridad de un archivo.

Un procedimiento simple de suma de verificación puede utilizarse para calcular el valor de un archivo y después verificarlo con su valor previo.

Si las sumas de verificación se igualan, el archivo no ha sufrido cambios. De no ser así, el archivo habrá sido alterado.

Las sumas de verificación aritméticas son fáciles de implantar. Están formadas al añadir elementos de archivo de 16 ó 32 bits para llegar al número de las sumas de verificación. Éstas no son muy seguras, debido a que se puede modificar y añadir datos al archivo para que la suma de verificación aritmética calcule el valor correcto.

La CRC (suma de verificación de redundancia cíclica), también conocida como *suma de verificación polinomial*, es más segura que la aritmética. Su implantación es parecida a la aritmética.

Sumas de verificación criptográfica

En las sumas de verificación criptográficas, llamadas también criptosellado, los datos se dividen en grupos más pequeños y se calcula una suma de verificación CRC para cada grupo de datos. Entonces las CRC de todos los grupos de datos se mezclan.

Este método dificulta la alteración de los datos, ya que el interceptor no conoce el tamaño de los grupos de datos que usaron. El tamaño de datos es variable y puede calcularse mediante el uso de técnicas seudoaleatorias.

Otro método llamado código de detección de manipulación (MDC) o función desmenuzadora de una vía puede utilizarse para detectar modificaciones a un archivo. Esta función se llama así porque dos entradas no pueden producir el mismo valor, los datos en el archivo se emplean como la entrada a la función desmenuzadora de una vía para producir un valor desmenuzado, si los datos en el archivo se modifican, tendrán un valor desmenuzado diferente.

¿ Cómo usar los sistemas de autenticación ?

La autenticación puede definirse como el proceso de proporcionar una identidad declarada a la satisfacción de alguna autoridad que otorgue permisos.

Los sistemas de autenticación son una combinación de hardware y software y mecanismos de procesamiento que permiten al usuario tener acceso a los recursos de la computadora.

Los mecanismos de autenticación van desde tarjetas inteligentes hasta dispositivos biométricos como lectores de huellas digitales, lectores de frecuencia de voz y verificación de retina.

Una tarjeta inteligente es un dispositivo portátil manual (HHP), que tiene un microprocesador, puertos de entrada/salida y algunos kilobytes de memoria no volátil. El usuario debe poseer un dispositivo de éstos para poder registrarse.

En esta autenticación la computadora anfitrión le indica al usuario que muestre un valor obtenido de una tarjeta inteligente cuando la computadora le pide una contraseña. A veces, la máquina anfitrión le da al usuario alguna información que el usuario deberá introducir a la tarjeta inteligente. Ésta tarjeta despliega entonces una respuesta que deberá introducirse a la computadora. Si la respuesta es acertada, se establecerá la sesión.

Sistema Kerberos

Kerberos es un sistema de autenticación. En otras palabras, es un sistema que valida la identidad de un principal. Un *principal* puede ser un usuario o un servicio.

En cualquier caso, el principal se define por cualquiera de los componentes siguientes:

- Nombre primario.
- Instancia.
- Reino.

*Nombre primario* en el caso de una persona es el identificador de registro, para un servicio, es el nombre del servicio. En cualquier caso, el *reino* se emplea para distinguir entre diferentes dominios de autenticación. Por medio del reino, es posible tener un servidor Kerberos distinto para cada unidad pequeña dentro de una organización en lugar de uno grande.

Los principales *Kerberos* obtienen boletos para servicios de un servidor especial conocido como *servidor despachador de boletos*.

Cada boleto consiste en información diversa que identifica al principal que está encriptado en la clave privada para ese servicio. Puesto que sólo Kerberos y el servicio conocen esta clave, se considera auténtica. El boleto otorgado por el servidor despachador de boletos contiene una nueva clave de sesión privada que también conoce el cliente. Esta clave se usa con frecuencia para encriptar las transacciones que ocurren durante la sesión.

## 3.3 PLAN DE CONTINGENCIA.

Una contingencia en la seguridad de una computadora (o de una red de ellas) es el acontecimiento donde el potencial de las operaciones de un sistema cae, de este modo se interrumpen las funciones vitales de un negocio y donde la seguridad tanto física como lógica han sido afectadas. Un acontecimiento puede ser la caída de voltaje, falla de hardware, fuego, etc. Si el acontecimiento es muy destructivo, entonces es llamado desastre.

Para impedir una contingencia o desastre potencial y minimizar el daño que causa, las organizaciones deben tomar una serie de acciones para controlar los acontecimientos, generalmente llamadas Plan de Contingencia, donde se relacionan las actividades que manejan los incidentes, el cual primeramente se dirige a amenazas técnicas maliciosas como son los hackers y virus.

### 3.3.1 Concepto general.

La planeación de contingencias implica más que la planeación de un desastre que destruye el centro de datos. Es también la guía de como respaldar en una organización las funciones criticas de operación en el caso de falla, ya sean grandes o pequeñas. Esta perspectiva en un plan de contingencia está basada en la distribución de computadoras a través de una organización.

El proceso para el desarrollo de un plan de contingencia implica los siguientes pasos:

- Identificación de la misión de las funciones críticas.
- Identificación de los recursos que soportan las funciones críticas.
- Anticipar las contingencias o desastres potenciales.
- Selección de las estrategias de los planes de contingencia.
- Implementar las estrategias de contingencia.
- Probar y revisar constantemente las estrategias.

### 3.3.1.1 Respaldo del equipo.

Identificación de la misión de funciones críticas

Proteger la continuidad de la misión o negocio de una organización es muy difícil si no se tiene identificado y así saber que recursos apoyan la realización de estas funciones críticas. Los administradores necesitan entender la organización desde un punto de vista que usualmente se extiende mas allá del área de su control.

La definición de la misión o funciones del negocio es a menudo llamado **business plan**. El desarrollo de un business plan puede ser usado para soportar el plan de contingencia, es necesario no únicamente para identificar las misiones críticas o de negocio, sino también para conjuntar las prioridades de ellas. En el caso de un desastre, ciertas funciones no podrían ejecutadas. Si la prioridades apropiadas han sido conjuntadas (y aprobadas por el administrador en jefe), darán la diferencia en la organización para poder sobrevivir a un desastre.

Identificación de los recursos que soportan las funciones críticas

Después de identificar la misión de las funciones críticas y del negocio, es necesario identificar los recursos que son utilizados para el desarrollo de dichas funciones y el tiempo en el cual cada recurso es utilizado (¿el recurso es usado constantemente o únicamente a fin de mes ?) y el efecto en la misión o negocio de la indisponibilidad del mismo. En la identificación de los recursos, un problema tradicional ha sido que los diferentes directores ven diferentes recursos. Esto por no darse cuenta como es la interacción de recursos para soportar la misión o negocio de la organización. Muchos de estos recursos no son recursos de cómputo. La planeación de contingencias debe dirigir todos los recursos necesarios para ejecutar la función, indiferente si están relacionados a la computadoras.

El análisis de recursos necesarios debe ser conducido por aquellos que entienden como es ejecutada la función y la dependencia de varios recursos en otras relaciones críticas. Esto puede llevar a una organización a asignar prioridades de recursos donde no todos los elementos son cruciales para funciones críticas.

Los elementos que se deben tomar en cuenta para el análisis de los recursos son:

*Recursos Humanos.*

Las personas son probablemente en la organización, el más obvio de los recursos. Algunas funciones requieren del esfuerzo de individuos específicos, algunas requieren de expertos y algunas únicamente requieren de individuos capacitados para ejecutar una tarea específica. En el interior del campo de la tecnología de la información, los recursos humanos incluyen tanto a los técnicos o programadores de sistemas, como a los usuarios (como capturistas o analistas de información).

*Capacidad de Procesamiento.*

Tradicionalmente la planeación de la contingencia tiene un enfoque sobre el potencial de procesamiento. Aun y cuando en los centros de cómputo se respalden las operaciones vitales, se deben considerar otros lugares alternativos de procesamiento, como LAN's, minicomputadoras, workstations y computadoras personales en todas las formas centralizadas y distribuidas de procesamiento.

*Aplicaciones automatizadas y datos.*

Los sistemas computacionales ejecutan aplicaciones que procesan datos. Sin ambas, el procesamiento computarizado no podría ser posible. Si el procesamiento es ejecutado en un hardware alterno, las aplicaciones deben ser compatibles con ese hardware, los sistemas operativos, otro software (incluyendo versión y configuración) y otros factores técnicos, por lo que es necesario verificar periódicamente la compatibilidad.

*Servicios basados en computadoras.*

Una organización usa diferentes tipos de servicios basados en computadoras para ejecutar sus funciones. Las dos más importantes son los servicios de comunicación y los servicios de información. Las comunicaciones pueden estar categorizadas como comunicaciones de datos y voz, mientras que en muchas organizaciones estas son manejadas por el mismo servicio. Los servicios de información incluyen cualquier fuente de información fuera de la organización. Muchas de estas fuentes son automatizadas, incluyendo servicios on-line, bases de datos privadas, servicios de noticias y bulletin boards.

*Infraestructura física.*

Para que el personal trabaje eficientemente, se requiere de un medio ambiente de trabajo seguro, así como de equipo y útiles apropiados. Esto puede incluir espacio de oficina, aire acondicionado, electricidad, teléfonos, fax, computadoras personales, terminales, servicios de mensajería, archiveros, etc.

*Documentos.*

Muchas funciones confían en registros vitales y varios documentos, papeles y formas. Estos registros pueden ser importantes por una necesidad legal (como la existencia de una copia firmada de un préstamo) o porque son los únicos registros de información. Los registros pueden mantenerse en papel, microficha, microfilm, medios magnéticos o discos ópticos.

Anticipando Contingencias o Desastres Potenciales

Aunque es factible pensar que todos los componentes de puede tener problemas, es importante identificar un probable rango de e desarrollo de escenarios puede ayudar a una organización a desarrollar un plan para dirigir su atención a ciertos problemas.

Los escenarios pueden incluir pequeñas o grandes contingencias. Mientras que algunas clases generales de escenarios de contingencias son obvios, es necesario imaginar y tener creatividad, así como investigar para apuntar otras posibles pero menos obvias contingencias. La contingencia y los escenarios deben dirigirse hacia cada uno de los recursos descritos anteriormente. A continuación se presentan algunos ejemplos de preguntas que los escenarios de contingencia pueden dirigir:

- Recursos Humanos: ¿ Puede la gente llegar a trabajar ? ¿ Las actividades y conocimientos críticos son poseídos por una sola persona ? ¿ Puede la gente fácilmente tener un lugar alternativo de trabajo ?
- Capacidad de Procesamiento: ¿ Qué tipo de daño pueden tener las computadoras ? ¿ Qué pasa si alguna de las computadoras es inoperable ?
- Aplicaciones automatizadas y los datos: ¿ La integridad de los datos ha sido afectada ? ¿ Se puede sabotear la aplicación ? ¿ Puede una aplicación correr en una diferente plataforma ?
- Servicios basados en computadoras: ¿ Pueden las computadoras comunicarse ? ¿ A dónde ? ¿ Puede la gente comunicarse ? ¿ Pueden los servicios caerse ? ¿ Por cuánto tiempo ?
- Infraestructura: ¿ La gente tiene un lugar para trabajar ? ¿ Tienen equipo para realizar su trabajo ?
- Documentos y papeles: ¿ Pueden encontrarse fácilmente los registros necesarios ? ¿ Pueden ser leídos ?

### 3.3.1.2 Procedimientos de respaldo y recuperación de archivos.

**Selección de las estrategias del Plan de Contingencia.**

El siguiente paso es planear como recuperar los recursos necesarios. En las alternativas de evaluación, es necesario considerar aquellos controles usados para prevenir y minimizar las contingencias. No se pueden implementar todas los controles debido al costo - efecto, ni prevenir todas las contingencias, por lo que es necesario coordinar la prevención y los esfuerzos de recuperación.

Una estrategia de planeación de contingencias normalmente consiste de 3 partes:

- Respuesta a la emergencia.
- Recuperación.
- Reanudación.

Respuesta a emergencias son las acciones iniciales que se toman para proteger vidas y limitar los daños.

Recuperación se refiere a los pasos que son tomados para continuar el soporte de las funciones criticas.

La reanudación es el regreso a las operaciones normales. La relación entre recuperación y reanudación es importante, ya que deben de considerarse las dos interrogantes siguientes: ¿ cuánto tiempo toma regresar a las operaciones normales ? y ¿ cuánto tiempo puede la organización esperar para operar normalmente ?

La selección de una estrategia necesita estar basada en consideraciones practicas, incluyendo factibilidad y costo. El aseguramiento del riesgo puede ser usado como auxiliar en la estimación del costo de las opciones para decidir una estrategia optima. Un ejemplo claro es considerar si comprar y mantener un generador implica mayores riesgos y costos que migrar el procesamiento de información a un lugar alternativo, considerando la probabilidad de perder energía eléctrica varias veces. O bien, ¿ las consecuencias de perder recursos de cómputo son lo suficientemente altas para garantizar el costo de varias estrategias de recuperación ? El aseguramiento del riesgo se debe enfocar en áreas donde se tiene identificada la mejor estrategia.

En el desarrollo de la estrategia de los planes de contingencia, hay muchos factores a considerar en el sentido de cada uno de los recursos que soportan funciones criticas.

Recursos Humanos

Una organización debe tener empleados con las habilidades, capacitación y documentación necesarios. Durante una contingencia mayor, las personas pueden estar bajo un gran stress y tener pánico. Si la contingencia es un desastre regional, su primera preocupación pueden probablemente ser su familia y propiedades. Por lo que la gente puede estar indispuesta o incapaz para realizar su trabajo. El usar personal adicional puede introducir vulnerabilidad en la seguridad.

El plan de contingencia, especialmente para respuestas de emergencia, normalmente toma el mayor énfasis en la protección de la vida humana.

Capacidad de procesamiento

Las estrategias para la capacidad de procesamiento están normalmente agrupadas en 5 categorías: hot site, cold site, redundancia, convenios recíprocos e híbridos. Estos términos originados con estrategias de recuperación para centros de cómputo pueden ser aplicados a otras plataformas.

**Hot site.** Construcción de un sitio alterno que este listo para operar con equipo, con las capacidades de procesamiento y otros servicios.

**Cold site.** Es un sitio para albergar procesadores que pueden ser fácilmente adaptados para su uso.

**Redundant site.** Un lugar equipado y configurado exactamente como el lugar primario. En el plan de algunas organizaciones, se tiene reducida la capacidad de procesamiento y se usa redundancia parcial. La acción de ahorrar personal de computadoras o LAN servers también provee alguna redundancia.

**Convenios recíprocos.** Un convenio lleva a dos organizaciones a ayudarse mutuamente. Mientras que este acceso a menudo suena deseable, los expertos en planes de contingencia notan que es una alternativa que tiene grandes oportunidades de fallar, debido a problemas que tienen los convenios y los planes de actualización de sistemas y a cambios de personal.

**Híbridos.** Cualquier combinación de los antes descritos.

La recuperación puede incluir varias etapas marcadas por el incremento en la disponibilidad y por la capacidad de procesamiento. El plan de reanudación puede incluir contratos, disponibilidad de lugares o reemplazo de equipo.

Aplicaciones automatizadas y datos

Normalmente una estrategia de contingencia para aplicaciones y datos incluye respaldos de información y almacenamientos fuera de sitio, considerando la periodicidad del respaldo, políticas y procedimientos a seguir para el almacenamiento fuera de sitio, así como el transporte de la información.

Servicios basados en computadoras

En las líneas portadoras de voz y datos, la información a menudo pueden ser reenrutada (transparentemente al usuario) a nuevas localidades. Los hot sites usualmente son capaces de recibir voz y datos. Si un proveedor del servicio falla, es posible usar otro. Los servicios locales de voz pueden ser llevados en sistemas celulares. En las comunicaciones locales de datos, especialmente de grandes volúmenes, normalmente es más difícil este procedimiento. En adición, el restablecimiento de las operaciones normales puede requerir otro reenrutamiento de los servicios de comunicación.

Infraestructura física

Los hot sites y cold sites pueden ofrecer espacio de oficina para soportar la capacidad de procesamiento. Otro tipos de convenios contractuales involucran la administración del espacio físico de las oficinas, servicios de seguridad y asignación de mobiliario en caso de una contingencia. Si el plan de contingencia utiliza la opción de cambiarse a un lugar alterno, se deben de tener los procedimientos necesarios para asegurar que su desarrollo sea en una forma segura y poder asegurar el regreso a las aplicaciones prioritarias de la organización. La protección de infraestructura física es normalmente parte importante de un plan de emergencia, como es el uso de extinguidores o equipo de protección contra daño por agua.

Documentos y papeles

La estrategia primaria para el plan de contingencia, está referida en respaldar periódicamente el medio magnético, óptico, microficha, papel u otro medio y almacenar estos respaldos en otro lugar. Los documentos en papel son generalmente más difíciles de respaldar que los electrónicos.

**Implementación de Estrategias de Contingencia.**

Una vez que los planes de contingencia han sido seleccionados, es necesario hacer las preparaciones apropiadas, llevar a cabo estrategias de documentación y capacitar a los empleados.

Se requiere de mucha preparación para implementar las estrategias de protección de funciones o aplicaciones críticas y de recursos de soporte. Por ejemplo, una preparación común es establecer procedimientos de respaldo de archivos y aplicaciones. Otro es establecer contratos y/o convenios, si la estrategia de contingencia los necesita. Otra preparación puede ser la compra de equipo, especialmente para soportar capacidad redundante.

La preparación debe también incluir formalmente la designación de las personas responsables de varias tareas en el caso de contingencia. Estas personas son identificadas como el equipo responsable de contingencias. Este equipo está compuesto por las personas que fueron parte del equipo de planeación de contingencias.

¿ Cuántos planes ?

Algunas organizaciones tienen solamente un plan general y otras tienen un plan para cada sistema distinto de computadora, aplicación u otros recursos. Otras cuentan con un plan para cada negocio o misión, con planes separados, para salvaguarda y respaldo de recursos críticos.

La respuesta a la cuestión, por consiguiente, depende de las circunstancias únicas de cada organizacion, por lo que es de suma importancia definir conjuntamente con gerentes de recursos humanos y gerentes de funciones la misión del negocio y los objetivos a cumplir.

Hay varios factores importantes que implementar en una organización. Dos de los más importantes se refieren a cuantos planes deben ser desarrollados y quien prepara cada plan. Ambas cuestiones giran alrededor de la organización, que abarca todo la estrategia para el plan de contingencia. La respuesta debe ser documentada dentro de las políticas y procedimientos de la organización

¿ Quién prepara el plan ?

El coordinador del Plan de Contingencia centraliza los planes en conjunto con personal de rango importante en la empresa, así como con los encargados de tomar decisiones fundamentales en el seguimiento y continuidad del negocio.

Documentación

El Plan de Contingencia debe estar por escrito y mantenerse actualizado de acuerdo con la evolución de los sistemas y equipos dentro de la organización, así como almacenarlo en un lugar seguro. Debe estar escrito en un lenguaje simple, con tareas secuenciales a ser ejecutadas en el acontecimiento de una contingencia, de tal manera que pueda ser ejecutado de manera sencilla y

estructurada. Es deseable guardar las copias actualizadas del plan de contingencia en varios lugares, incluyendo cualquier localidad fuera de sitio, como es un lugar de procesamiento alternativo o facilidades de almacenamiento de datos de respaldo.

Capacitación

Todo el personal debe capacitarse en tópicos relacionados con contingencias. El nuevo personal debe ser capacitado al integrase a la organización.

La capacitación es un factor importante para un efectivo tiempo de respuesta empleado durante emergencias, ya que se debe actuar de inmediato ante cualquier imprevisto. Es necesario hacer pruebas y simulacros periódicos para estar en posibilidades de reaccionar correctamente, especialmente cuando vidas humanas están involucradas.

### 3.3.1.3 Programa de archivos vitales.

En el desarrollo de un plan de contingencia también es necesario evaluar los archivos y fuentes de información que son importantes para la organización, así como sus funciones críticas, la forma en que están respaldados y asegurados y como diseñar un programa óptimo que salvaguarde esta información.

Una vez identificada la información vital, se deben evaluar, autorizar y poner en marcha métodos y procedimientos de respaldo (ya sea en equipos secundarios, cintas o disquetes) en forma independiente al respaldo de toda la información.

### 3.3.1.4 Prueba del plan de contingencia.

**Pruebas y revisión.**

Un plan de contingencia debe ser probado y actualizado periódicamente, ya que esto puede indudablemente señalar fallas en el mismo y en su implementación. La responsabilidad para tener el plan de contingencia actualizado, debe ser asignada concretamente al personal encargado del centro de cómputo, de tal manera que se calendarice junto con los demás procesos prioritarios de la organización.

La extensión y frecuencia de las pruebas puede variar entre cada organización y el volumen de transacciones que éstas manejen. Hay varios tipos de pruebas, incluyendo revisión, análisis y simulación de desastres. Una revisión al documento del plan de contingencia, puede ser una simple prueba para evaluar la funcionalidad y vigencia del mismo.

Por ejemplo, revisar si la lista de personas involucradas en el plan de contingencia son aún parte de la organización y que cuenten con las funciones y

responsabilidades que les fueron asignadas al ser incluidos en el plan, puede proporcionar información relevante para que se tomen decisiones que permitan actualizar el plan. La revisión puede determinar además, si los archivos pueden ser restaurados de las cintas de respaldo o si los empleados conocen los procedimientos de emergencia.

Las organizaciones pueden también simular desastres. Estas pruebas proveen información de gran valor acerca de los defectos en el plan de contingencia y proveen prácticas para una emergencia real. Lejos de resultar cara, esta prueba proporciona además información crítica que puede ser usada para la continuidad de funciones importantes dentro de la organización.

### 3.3.1.5 Evaluación del plan de contingencia.

Un análisis puede ser ejecutado en todo el plan o porciones de él, como los procedimientos de respuesta en emergencias. Los resultados son benéficos si el análisis es ejecutado por alguien que no ayudo a desarrollar el plan de contingencia, pero que tiene amplio conocimiento en las funciones críticas y los recursos soportados. El analista puede mentalmente seguir las estrategias del plan de contingencia y la lógica usada en el desarrollo del mismo.

El analista puede también entrevistar a los gerentes funcionales, gerentes de recursos y su staff para descubrir si falta algo o si se paso por alto algún detalle en el plan.

# CONTROLES DE SISTEMAS DE INFORMACIÓN PARA LA OBTENCIÓN DE PROPUESTA

## 4.1. NECESIDAD DE CONTAR CON CONTROLES EN LOS SISTEMAS DE INFORMACIÓN.

**Definición de control.**

El control ha jugado un papel vital en el avance de la ingeniería y de la ciencia. Tradicionalmente, controlar es verificar que todo ocurra de acuerdo con las reglas establecidas y las órdenes impartidas.

Dentro del concepto de sistemas, el control es definido como un medio para obtener una mayor flexibilidad operativa así como para evitar, en lo posible, riesgos e impactos en la información. En todo sistema, donde el flujo de información está sujeto a variaciones, los errores se vuelven inevitables y la inestabilidad aumenta a medida que se incrementan las variables externas e internas que influyen en dicho sistema.

La información histórica es el medio para saber qué es lo que se va a corregir. Si la acción correctiva se realiza con demora, tal vez se logrará afianzar más el error en vez de corregirlo. El sistema debe ser proyectado de tal forma que pueda corregirse a sí mismo cuando sea necesario, es decir, que cuente con medios para redistribuir recursos a medida que se modifiquen las condiciones.

Por lo tanto, los controles son necesarios dentro de los sistemas de información, ya que realzan las excepciones y las variaciones especificas de las aplicaciones y permiten tomar decisiones para actuar tanto preventiva como correctivamente.

**Proceso y reglas.**

1. Es necesario distinguir, ante todo, los pasos o etapas de todo control:

    - Establecimiento de los medios de control.
    - Operaciones de recolección y concentración de datos.
    - Interpretación y valoración de los resultados.
    - Utilización de los mismos resultados.

2. Entre la innumerable variedad de medios de control posibles a aplicar en los sistemas de información, se deben seleccionar los que puedan considerarse como puntos estratégicos de control. Las siguientes preguntas pueden ayudar a encontrar estos puntos:

- ¿ Qué mostrará mejor lo que se ha perdido o no se ha obtenido ?
- ¿ Qué puede indicar lo que podría mejorarse ?
- ¿ Cómo medir de manera más rápida cualquier desviación anormal ?
- ¿ Qué medio informará mejor sobre "quién" es responsable de las fallas ?

3. Los controles deben reflejar en todo lo posible, la estructura del sistema de información:

   - La organización del sistema de información es la expresión de la planeación del mismo y es a la vez un medio de control.
   - Dentro de la organización del sistema de información, deben estar contemplados los controles tanto administrativos como operativos.
   - Los mismos controles pierden eficacia. Muchas veces el dato escueto no sirve, pues necesita de la interpretación o adiciones que deben hacerles tanto los usuarios como los desarrolladores del sistema. Aquí es donde tiene participación el Proceso Aseguramiento de la Calidad de los Sistemas como otro medio de control.

4. Al establecer los controles, hay que tener en cuenta su naturaleza y la de la función controlada de los sistemas de información, a fin de aplicar el más útil.

5. Los controles deben ser flexibles. Cuando un control es inflexible, un problema que exija rebasar lo calculado en la planeación del sistema de información provoca que no pueda realizarse adecuadamente la función, o bien, se tienda a catalogar el control como inservible.

6. Los controles deben reportar rápidamente las desviaciones. El control de tipo "histórico" mira hacia el pasado. De ahí que, muchas veces cuando se reporta una desviación o anomalía, ésta es ya imposible de arreglarse. Por lo tanto, los controles deben estar lo más actualizados que se pueda.

7. Los controles deben ser claros para todos cuantos han de usarlos.

8. Los controles deben conducir a quien los use a la acción preventiva. No sólo deben mostrar "que algo está mal", sino "dónde, por qué, quién es el responsable", etc.

9. En la utilización de los datos que proporcione la utilización del control, se deben seguir los siguientes pasos:

   - Análisis e interpretación de los hechos.
   - Adopción de medidas aconsejables
   - Monitoreo constante.
   - Registro de los resultados obtenidos.

10 Los controles pueden servir para:

- Proveer seguridad en el manejo y procesamiento de la información.
- Prevención y corrección de los defectos.
- Mejora continua en resultados obtenidos.
- Mejora en planes.

**Objetivos básicos de control.**

Todo control aplicado a sistemas de información cuenta con los siguientes objetivos básicos:

- Totalidad.
- Exactitud.
- Autorización.
- Mantenimiento
- Oportunidad.
- Utilidad.

A continuación se describe cada uno de ellos:

| Objetivo Básico | Consideraciones |
|---|---|
| **Totalidad** | Incluye la completa integración de datos, herramientas, procedimientos, etc., que necesita el sistema de información para funcionar. |
| **Exactitud** | Considera que los datos importantes de cada operación o actividad son correctos durante el procesamiento de la información. |
| **Autorización** | Contempla que sólo se procesen operaciones, actividades o cambios a componentes autorizados y calendarizados previamente por un comité de preproducción. La autorización debe ser anterior al registro de los procesos o actividades. |
| **Mantenimiento** | Considera que toda aplicación debe permanecer completa y exacta en el tiempo. El mantenimiento se da inevitablemente, debido a la constante evolución de los objetivos de negocio para los cuales fueron diseñados los sistemas de información.<br><br>Por tanto, deben implementarse medidas estrictas de aseguramiento de calidad de la información dentro del mantenimiento, tal como el control de cambios a componentes y reprocesos. |

| | |
|---|---|
| **Oportunidad** | Considera que los sistemas de información deben proporcionar datos oportunos que cubran los requerimientos de negocio, así como información de tipo ejecutivo para la toma de decisiones. |
| **Utilidad** | Contempla que se distribuya correctamente la información, generada por los sistemas hacia los usuarios finales de la misma. |

**Disciplinas sobre los controles básicos.**

Las disciplinas sobre los controles básicos son aquellos aspectos de un sistema de información que garantizan que tales controles operan adecuadamente, tal como fueron diseñados, además de detectar errores oportunamente.

| Disciplina | Consideraciones |
|---|---|
| **Segregación de funciones** | Permite que el trabajo de un programa actúe como la verificación del trabajo de otro.<br><br>Reduce la posibilidad de errores o fraudes. |
| **Adecuada custodia de activos** | Se refiere a la seguridad física de software, hardware, archivos, documentación, dispositivos de almacenamiento y respaldo, reportes, especificaciones técnicas, formas preimpresas, etc. |
| **Supervisión** | Probablemente es la disciplina más importante sobre los controles básicos, ya que aumenta la confiabilidad de la información. |

**Procedimientos de control en el manejo de datos e información.**

Partiendo del esquema básico de procesamiento de información (entrada-proceso-salida), es posible llevar a cabo un análisis a los controles que se emplean en los dos tipos de procesamiento de los sistemas: por lotes (Batch) y Línea (On-Line).

El procesamiento batch en un sistema de información comienza cuando el procesamiento on-line ha finalizado, es decir, cuando las aplicaciones son "cerradas" para la captura y procesamiento de transacciones. El procesamiento batch toma los datos que generó la línea para alimentarse y generar resultados. Es muy común que en el batch se lleve a cabo alguna captura de datos, a fin de complementar la información de la línea.

El procesamiento On-line involucra sistemas de teleprocesamiento, en los cuales los datos son alimentados al sistema de información directamente desde el punto

de origen y los datos son transmitidos a los lugares donde son utilizados. En el procesamiento batch, se ven involucrados los siguientes controles:

| Entrada de Datos | |
|---|---|
| **Etapa 1. Origen de la Transacción** | |
| **Controles Administrativos** | **Controles Operativos** |
| • División de funciones.<br>• Formularios preimpresos y foliados.<br>• Establecimiento de niveles de autorización.<br>• Identificación de transacciones críticas para las aplicaciones. | • Conteo de documentos y transacciones.<br>• Totales de control.<br>• Gestión de errores con intervención de diferentes niveles de autorización.<br>• Control del archivo de captura.<br>• Control de envío y recepción de documentos. |
| **Etapa 2. Grabación de Transacciones** | |
| **Controles Administrativos** | **Controles Operativos** |
| • Uso de programas predefinidos de grabación.<br>• Identificación correcta de lotes a los que pertenecen las transacciones.<br>• Totalizar campos críticos de documentos. | • Captura-verificación de transacciones.<br>• Cuenta de transacciones.<br>• Totales de control.<br>• Control de dígito autoverificador. |
| **Etapa 3. Asignación de Lotes** | |
| **Controles Administrativos** | **Controles Operativos** |
| • Creación de archivos de movimientos con identificación de documentos y lote. | • Conteo de transacciones.<br>• Totales de control.<br>• Número de lote. |
| **Etapa 4. Validación y Control** | |
| **Controles Administrativos** | **Controles Operativos** |
| • Fijación de estándares para el control de campos, registros y archivos.<br>• Establecimiento del uso de códigos autoverificadores para los campos de escasa variación.<br>• Uso de totales de control para todos los campos de contenido imprevisible.<br>• Archivos de movimientos con claves de acceso. | • Pruebas para verificar la integridad y confiabilidad de la información durante el procesamiento.<br>• Establecimiento de procedimientos automatizados para la detección oportuna de errores. |

| Etapa 5. Tratamiento de errores | |
|---|---|
| **Controles Administrativos** | **Controles Operativos** |
| • Verificación de errores detectados. | • Detección del error.<br>• Corrección del error.<br>• Reingreso de datos corregidos. |

| Proceso | |
|---|---|
| **Etapa 1. Procesamiento en Producción** | |
| **Controles Administrativos** | **Controles Operativos** |
| • Bibliotecas de procedimientos totalmente estandarizadas.<br>• Operación de aplicaciones con manuales de operación.<br>• Procedimientos establecidos para contingencias o situaciones no *estándar.*<br>• Políticas de manejo de archivos de respaldo, incluidas en los procedimientos estandarizados.<br>• Controles automáticos para evitar el uso indebido de archivos.<br>• Rotación del personal y supervisión de operaciones. | • Totales de control después de la terminación de cada programa.<br>• Control contable de salidas y archivos.<br>• Listado de archivos procesados.<br>• Conservación del "log" por periodos preestablecidos.<br>• Control de formularios críticos.<br>• Análisis de la rutina de contabilidad de operaciones de la computadora. |

| Salida | |
|---|---|
| **Etapa 1. Salida de datos** | |
| **Controles Administrativos** | **Controles Operativos** |
| • Calificación precisa de la documentación que se produce.<br>• Procedimientos específicos para el envío y entrega de información.<br>• Comparación de la información producida en cantidad, calidad, *forma* y *tiempo.*<br>• Identificación del personal que va a hacer el retiro del material. | • Balance y conciliación de la información producida con los datos y archivos de entrada.<br>• Tratamiento de la información de acuerdo a su calificación de seguridad.<br>• Recepción, control y almacenamiento *de recibos de recepción de datos.*<br>• Preparación de reportes de salidas y entregas. |

| Etapa 2. Almacenamiento y recuperación de archivos | |
|---|---|
| **Controles Administrativos** | **Controles Operativos** |
| • Cuidadosa selección y capacitación de los encargados de la biblioteca.<br>• Establecimiento para retiro y entrega de materiales y para la administración general de la biblioteca.<br>• Normas para rotulación externa de archivos<br>• Normas que obliguen al uso efectivo de rótulos internos (label) tanto del sistema como de los usuarios.<br>• Inventarios físicos periódicos. | • Clara denominación de los archivos, estableciendo número de versión y fecha de creación y expiración.<br>• Entrega y recepción de material debidamente documentado.<br>• Procedimientos de depuración automática de medios magnéticos de almacenamiento que contengan archivos vencidos o caducos. |

En el procesamiento On-line, se ven involucrados los siguientes controles:

| Entrada de Datos | |
|---|---|
| **Etapa 1. Origen de la Transacción** | |
| **Controles Administrativos** | **Controles Operativos** |
| • Establecimiento de vigencia y niveles de autorización para captura de transacciones.<br>• Identificación de transacciones críticas para las aplicaciones. | • Validar el nivel de autoridad del user-id de la persona que esta ingresando datos al sistema.<br>• Proteger los datos contra intercepciones en la transmisión de información mediante la encriptación. |

| Proceso | |
|---|---|
| **Etapa 1. Procesamiento en Producción** | |
| **Controles Administrativos** | **Controles Operativos** |
| • Procedimientos para recepción de datos totalmente estandarizados.<br>• Identificación y documentación de archivos que afectan transacciones.<br>• Identificación y documentación de interfaces con otras aplicaciones. | • Desencriptación de información.<br>• Procesamiento de transacciones en aplicaciones e interfaces.<br>• Conteo de transacciones que afectan a los archivos maestros.<br>• Establecimiento de niveles de servicio para procesamiento de información. |

| Salida | |
|---|---|
| Etapa 1. Reenvío de Información | |
| **Controles Administrativos** | **Controles Operativos** |
| • Procedimientos para encriptación de datos al ser reenviados al origen.<br>• Identificación y documentación de los archivos que afectaron las transacciones. | • Encriptación de información.<br>• Generación del "log" de transacciones para su posterior revisión.<br>• Establecimiento de niveles de servicio para entrega de información procesada. |

## 4.2 COBIT (Control Objectives for Information and Related Technology).

### 4.2.1 Descripción general.

La estructura COBIT responde a la necesidad de un Sistema de Control Interno para Tecnología Informática, diseñado para ser empleado por usuarios, auditores e incluso como un check list para propietarios de los procesos del negocio. COBIT parte de la siguiente premisa: "Los recursos de la tecnología informática necesitan ser administrados por un conjunto de procesos agrupados de forma natural para proporcionar la información que la empresa necesita para alcanzar sus objetivos".

COBIT está diseñado para ser comprensible a la administración y para operar en un nivel más elevado que los estándares de administración de sistemas de información.

El principal objetivo de COBIT es habilitar el desarrollo de políticas y estándares para controlar tecnologías de información a nivel mundial. El control es alcanzado mediante la búsqueda de la información que se necesita para soportar los procesos de negocio y el análisis de información que resulta de la combinación de aplicaciones.

Las siglas COBIT significan lo siguiente:

| | |
|---|---|
| C | (Competition and Change)<br>La competencia y cambio son dos de los aspectos medulares para que las expectativas de administración a tecnologías de información se cristalicen en el cumplimiento de sus funciones, permitiendo:<br>• Incrementar la calidad de los productos.<br>• Decrementar el tiempo de entrega.<br>• Cumplir con los niveles de servicio definidos. |

| | |
|---|---|
| O | (Organizations)<br><br>Las organizaciones deberán satisfacer, tanto para su información como para todos sus activos, requerimientos de calidad y seguridad. La administración deberá balancear el uso y disponibilidad de recursos técnicos y humanos, tecnología, sistemas y datos mediante la implantación y puesta en marcha de un adecuado esquema de control interno. |
| B | (Business)<br><br>La orientación del negocio es el principal tema de COBIT. Su estructura debe estar acorde a las necesidades de un sistema de control interno en tecnologías de información. La estructura de COBIT provee herramientas que facilitan la descarga de responsabilidades de procesos de negocio. |
| I | (It)<br><br>Su estructura se basa en 32 objetivos de control agrupados en 4 dominios (Planeación y Organización, Adquisición e Implementación, Entrega y Soporte y Monitoreo), los cuáles cubren todos los aspectos de información y tecnología. |
| T | (The management)<br><br>La administración de la empresa necesita garantizar su existencia en el mercado mediante la implantación y apego a estándares de seguridad y control en tecnologías de información |

**Principios de COBIT.**

Cada aplicación y proceso está apoyado en recursos de tecnologías de información tales como datos, sistemas aplicativos, tecnología, facilidades y recursos humanos.

| | |
|---|---|
| • Datos | Toda la documentación externa e interna: archivos, manuales, políticas, estándares, gráficos, etc. |
| • Sistemas Aplicativos | Procedimientos programados. |
| • Tecnología | Hardware, sistemas operativos, bases de datos, redes, multimedia, Internet, etc. |
| • Facilidades | Ubicación física y soporte a los sistemas de información. |
| • Recursos Humanos | Habilidades y conocimientos del personal, productividad, organización, monitoreo a los sistemas de información. |

Para satisfacer los objetivos del negocio, la información necesita cumplir con ciertos criterios, a los que COBIT llama requerimientos de información del negocio:

| | |
|---|---|
| • Requerimientos Financieros | Efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes regulatorias. |
| • Requerimientos de Seguridad | Confidencialidad, integridad, disponibilidad. |
| • Requerimientos de Calidad | Calidad, costo y distribución. |

Entendiéndose lo siguiente para cada uno de ellos:

- Efectividad — Se relaciona con la información relevante y pertinente para procesos de negocio, así como la oportunidad, confiabilidad y consistencia de la información.
- Eficiencia — Proporcionar información a través del uso óptimo de recursos (económica y productivamente).
- Confidencialidad — Se refiere a la protección sobre divulgaciones no autorizadas de información sensitiva o vital.
- Confiabilidad — Se relaciona a la precisión y totalidad de la información, así como su validez de acuerdo con los valores y expectativas.
- Disponibilidad — Se refiere a la disponibilidad de información requerida por los procesos de negocio presentes y futuros, la salvaguarda de los recursos necesarios y capacidad.
- Cumplimiento — Contempla el apego a leyes, regulaciones y contratos a los cuales los procesos de negocio se encuentran sujetos.
- Calidad — Se refiere a la calidad de información proporcionada a los administradores para operar la entidad y cumplir con sus responsabilidades de reportar las finanzas del negocio.

### 4.2.2 Objetivos de control.

Como se mencionó anteriormente, la estructura de COBIT se basa en 32 objetivos de control agrupados en 4 grandes dominios de la siguiente manera:

ESTRUCTURA DE COBIT

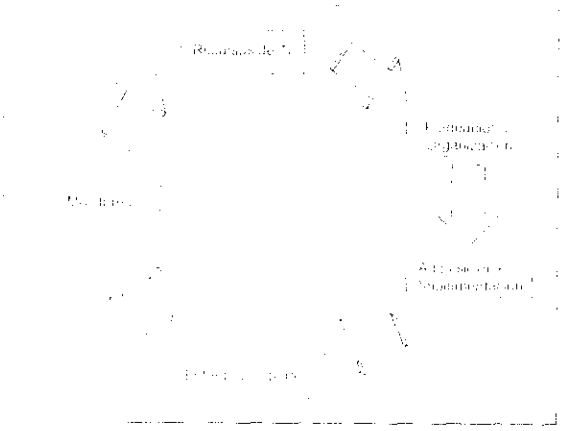

Fig. 4.1

**A) Organización.**

Contempla la estrategia y táctica que permite identificar la mejor forma en que las tecnologías de información pueden contribuir al logro de los objetivos del negocio. Permite contar con una visión estratégica para planear, comunicar y administrar en diferentes perspectivas. Finalmente, una organización apropiada, así como una infraestructura tecnológica, deben ser implementadas de acuerdo con los pasos siguientes:

| | |
|---|---|
| 1. Definición de un plan estratégico. | Las tecnologías de información deben ser parte de un plan a corto y largo plazo, considerando estructura, cambios y servicios de información. |
| 2. Definir la arquitectura de información. | Establecer un modelo de arquitectura de información, diccionario de datos corporativo, esquemas de clasificación de datos y niveles de seguridad. |
| 3. Determinar la dirección tecnológica. | Considerar una planeación de la infraestructura tecnológica, monitorear tendencias futuras y regulaciones, verificar contingencia y adquisición de hardware y software. |

| | |
|---|---|
| 4. Definir la estructura de la organización. | Considerar la creación de un comité de dirección, revisar objetivos organizacionales, definir roles y responsabilidades, identificar y definir propietarios de los datos, considerar segregación de funciones, elaborar descripciones de puestos. |
| 5 Administración de la inversión. | Verificar el presupuesto anual para servicios de información, monitorear costos y su justificación. |
| 6. Comunicar objetivos a la organización | Implementar un medio de control de información, desarrollando, actualizando y difundiendo políticas organizacionales, procedimientos y estándares. |
| 7. Administrar recursos humanos. | Reclutamiento, evaluación y promoción de personal, capacitación, cambios en la organización, terminación de relación laboral. |
| 8. Cumplimiento con entidades reguladoras. | Revisar requerimientos externos, prácticas y procedimientos para cumplimiento de dichos requerimientos, comercio electrónico, flujo de datos y acatamiento a contratos de seguros. |
| 9. Evaluación de riesgos. | Efectuar periódicamente análisis de riesgos de negocio, identificando posibles impactos y elaborar plan para corrección. |
| 10. Administración de proyectos. | Establecer marcos de referencia para administración de proyectos, participación del usuario cuando éstos inicien, definir responsabilidades del equipo de trabajo, criterios de aceptación, plan para aseguramiento de calidad, estrategia de pruebas, capacitación y evaluación de post- instalación. |

| | |
|---|---|
| 11. Administración de la calidad. | Elaborar un plan general de calidad, que contemple el aseguramiento de la calidad y apego a estándares, procedimientos, metodología de desarrollo de sistemas, adquisición y mantenimiento de infraestructura tecnológica, documentación y pruebas a programas y sistemas. |

**B) Adquisición e Implementación.**

Para realizar la estrategia de tecnologías de información, las soluciones deben ser identificadas, desarrolladas o adquiridas e implementadas en los procesos de negocio, considerando los cambios y mantenimientos de sistemas existentes.

| | |
|---|---|
| 1. Identificar soluciones. | Elaborar estudio de factibilidad que permita identificar necesidades y requerimientos de información, beneficios a la organización y apego a lineamientos legales, contables y fiscales. |
| 2. Adquisición y mantenimiento de aplicaciones. | Proveer funciones automatizadas que soporten adecuadamente los procesos del negocio a través de la elaboración de un diseño funcional, diseño de pruebas funcionales, revisión de licencias y contratos, documentación y controles de seguridad. |
| 3. Adquisición y mantenimiento de tecnología. | Proveer la plataforma apropiada que soporte las aplicaciones del negocio, mediante implementación de controles para adquisición de nuevo hardware y software, mantenimiento preventivo, cambios a componentes y sistemas de seguridad. |
| 4. Desarrollar y mantener procedimientos de tecnología de información. | Asegurar el correcto uso de aplicaciones y su solución tecnológia, mediante definición de requerimientos operacionales futuros, niveles de servicio, elaboración de manuales y material de capacitación, así como procedimientos de usuario y operación. |

| | |
|---|---|
| 5. Instalar sistemas. | Verificar y confirmar que la solución es la más óptima, a través de la aplicación de pruebas de desempeño, funcionalidad, volumen, seguridad, operación y revisión de su administración en la fase de post-instalación. |
| 6. Administrar cambios. | Minimizar el riesgo de pérdida de información, cambios sin autorización y problemas mediante la identificación de cambios, categorización, prioridad, criterios de aceptación, documentación y mantenimiento. |

**C) Entrega y Soporte.**

Contempla la liberación de los servicios requeridos, cuyo rango son las operaciones tradicionales, las referentes a seguridad y continuidad, aspectos en los que se requiere una capacitación, así como la implementación de procesos de soporte.

| | |
|---|---|
| 1. Acordar niveles de servicio. | Definidos con las áreas, deben contemplar responsabilidades, tiempos de respuesta, dependencias, proceso de monitoreo y medición y matrices de escalamiento. |
| 2. Administrar outsourcing. | Asegurar que las responsabilidades y actividades de personal externo, se encuentren claramente definidas y satisfagan los requerimientos del usuario. |
| 3. Administrar capacidad y desempeño. | Asegurar que la capacidad sea adecuada, se encuentre disponible y se aproveche de manera óptima mediante la implantación de un plan que verifique y controle la disponibilidad de los servicios de información. |
| 4. Asegurar continuidad de operaciones. | Definir la estrategia para implantación de plan de contingencia en base a un análisis de impactos al negocio, considerando los procedimientos de mantenimiento, funcionalidad y pruebas periódicas. |

| | |
|---|---|
| 5 Seguridad en los sistemas. | Establecer mecanismos de autenticación, control de acceso y encriptación de información sensitiva, administración de claves de usuario y perfiles, así como monitoreos a intentos de violación. |
| 6. Identificar y atribuir costos. | Asegurar una adecuada conscientización de que los costos sean atribuibles a servicios de tecnología de información. |
| 7. Capacitar usuarios | Asegurar que los usuarios estén haciendo uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades que sus facultades y permisos pueden efectuar en las aplicaciones, identificando necesidades de capacitación y educación en principios de seguridad de la información. |
| 8. Orientar a las áreas usuarias. | Proporcionar asistencia y soporte a los usuarios en tecnologías de información, estableciendo mecanismos para su correcto registro, oportuna atención y solución. |
| 9. Administrar la configuración. | Establecer procedimientos que aseguren que los componentes cuenten con mecanismos para prevenir alteraciones no autorizadas, la existencia de registros que reflejen el estatus actual de los componentes incluyendo la historia de sus cambios. |
| 10. Administrar problemas e incidencias. | Asegurar que todos los reportes problema e incidencias sean resueltas, efectuando análisis para identificar el origen del problema y determinando estrategias para su corrección dentro del margen establecido para minimizar los impactos al servicio. |

| | |
|---|---|
| 11. Administrar datos. | Asegurar la existencia y funcionalidad de los procedimientos automatizados que impidan el procesamiento erróneo de datos, así como la suficiencia, consistencia y calidad de la información generada para control del sistema y sus interfaces. |
| 12. Administrar instalaciones. | Definir políticas y procedimientos para control de acceso e implantación de dispositivos físicos que impidan el acceso a personal no autorizado y protección de componentes críticos. |
| 13. Administrar operaciones. | Generar políticas y procedimientos de operación, establecer horarios de trabajo y procesamiento, procesos de continuidad, logs de operación y procedimientos de respaldo y recuperación. |

**D) Monitoreo.**

Todos los procesos de tecnologías de información necesitan ser monitoreados regularmente para verificar su calidad y cumplimiento con respecto a los requerimientos de control y necesidades actuales del negocio.

| | |
|---|---|
| 1. Monitorear al proceso. | Verificar que los objetivos se estén cumpliendo de acuerdo con los requerimientos del usuario. |
| 2. Certificar al proceso. | Incrementar los niveles de confidencialidad de la información mediante establecimiento de políticas, procedimientos, estándares de protección y normatividad institucional. |

## 4.3 SAC (Systems Auditability and Control).

### 4.3.1 Descripción general.

El proyecto **SAC** fue creado por el **Institute of Internal Auditors Research Foundation (IIA RF)** con la finalidad general de brindar una herramienta que soporte la profesión de la auditoría interna. Bajo este esquema, se involucró a un grupo especializado de organizaciones expertas en Auditoria en Informática para

generar un producto que pudiera beneficiar a todos los niveles (desde directivos hasta operativos) de las empresas y organizaciones que recurren a los servicios de la Auditoría Interna.

Como resultado de lo anterior, el proyecto SAC provee una serie de procedimientos, técnicas y guías con las que es posible generar informes de auditoría con observaciones y recomendaciones derivadas de la evaluación a la tecnología de información de las organizaciones, tales como redes de computadoras, sistemas desarrollados para automatización de funciones, sistemas para generar información ejecutiva para toma de decisiones, bases de datos, comunicaciones, centros de cómputo, etc.

Cabe mencionar que el proyecto SAC plantea consideraciones estratégicas que facilitan la aplicación apropiada de la auditoría interna en las organizaciones, poniendo especial énfasis en:

- creación de métodos para medir los beneficios que derivan del uso de la información, es decir, aplicar Procesos de Aseguramiento de la Calidad (Quality Assurance Process),
- identificación y priorización de problemas y necesidades de información,
- experiencia de otras auditorías llevadas a cabo,
- análisis de las condiciones financieras de la organización, para considerar el tipo de equipos con que se procesa la información.

Asimismo, su alcance también involucra la evaluación de los factores que influyen los posibles riesgos relacionados con la administración de los recursos y los productos generados por los sistemas de información centralizada. De acuerdo a lo anterior, los factores de riesgo a considerar son:

- organización de la funciones y responsabilidades,
- administración de recursos de los equipos de cómputo, incluyendo mantenimiento y funciones de soporte por parte de personal especializado (proveedores),
- ambiente operativo,
- seguridad física de instalaciones en donde se encuentran los equipos de cómputo,
- seguridad lógica, para resguardo de la información generada,
- sistemas de software, diseñados para cumplir con los requerimientos de información de las organizaciones, operando y controlando las capacidades de procesamiento de los equipos de cómputo.

Por otro lado, el SAC proporciona técnicas para administrar los sistemas de información en las organizaciones. Este proceso involucra los conceptos **de Planeación de Sistemas, Administración de la Información y Desarrollo y**

**Mantenimiento de Sistemas**, tomando en cuenta los posibles riesgos que se presenten, así como controles y consideraciones para atacarlos.

La **Planeación de Sistemas** considera la obtención, estructuración y análisis de la información que requieren los sistemas o equipos de cómputo para satisfacer las necesidades de los usuarios. El resultado de la planeación es la obtención de un modelo de sistema bien definido que incluye los recursos y estrategias en las que se basará el desarrollo de software a crear o el equipo de cómputo a adquirir.

El objetivo de la **Administración de la Información** es transformar los datos en "bruto" en información que sea un recurso valioso. Un sistema de información transforma las entradas (datos) en salidas (información). Tal información forma las bases para la toma de decisiones y la calidad está directamente relacionada con la precisión de la información proporcionada a los ejecutivos de la organización.

En el **Desarrollo y Mantenimiento de Sistemas**, existe un concepto que es de suma importancia para alcanzar los objetivos de un desarrollo, el **Ciclo de Vida del Sistema**, mismo que se puede definir como el conjunto de actividades y productos que conformarán un sistema, el cual debe contener los productos que garanticen el éxito del mismo.

Asimismo, el ciclo de vida del sistema debe incluir para su realización, metodologías de desarrollo, herramientas para administración de proyectos, así como procedimientos de soporte, técnicas y herramientas relacionadas con el sistema a desarrollar o el equipo de cómputo a implantar.

La mayoría de los ciclos de vida de sistemas se dividen en los siguientes pasos:

Definición del proyecto

Hacer un diseño conceptual del proyecto, evaluando y definiendo el tipo de solución que se implantará, reutilizando sistemas, comprando paquetes y equipos, o bien, desarrollando un nuevo sis

Análisis

Asegurar la alineación del proyecto con el Plan Estratégico de Tecnología, Elaborar análisis preliminares y diseños conceptuales y conformando el equipo de trabajo que ejecutará el plan.

Diseño

Establecer en forma general las características y facilidades del sistema o equipo de cómputo.

Estimar costos necesarios del proyecto, desde su inicio hasta su terminación, así como el costo estimado de mantenimiento, es decir, elaborar un análisis costo - beneficio - riesgos.

Establecer planes de tiempos y costos globales del proyecto.
Identificar a detalle los requerimientos de usuarios.
Contar con justificación de negocio del proyecto.

Construcción

Elaborar el diseño del sistema de acuerdo con la información recopilada.
Desarrollar un diseño funcional del sistema para el usuario, identificando entradas y salidas del mismo, así como el manejo de los datos.
Definir políticas y procedimientos del sistema.
Generar diagrama estructural del sistema, desarrollando, si se requiere, un prototipo.
Generar el diseño técnico del sistema y de las entidades de datos.
Identificar las condiciones y datos de prueba con los usuarios.
Establecer, diseñar y ejecutar los planes de pruebas unitarias, modulares, integrales y de regresión.
Generar documentación para el usuario, así como capacitarlo.

Instalación

Instalación de Hardware y Software.
Soporte y seguimiento a la instalación.
Monitoreo en producción.
Revisión Post-Instalación.

### 4.3.2 Objetivos de Control.

**El rol del auditor.**

El rol principal del auditor es desarrollar una apreciación independiente de los sistemas de control interno de las organizaciones. Cumpliendo con lo anterior, debe conjuntar, analizar y evaluar grandes cantidades de información por demás compleja.

El auditor debe tener acceso a las tecnologías que soporten las necesidades de información para la realización de la auditoria de una manera efectiva y económica. La figura 4.2 ilustra el flujo de información en una auditoría interna.

Punto de control: Desarrollo del Plan de Auditoria

El desarrollo del plan de auditoría es un elemento que requiere dedicación y utilización de recursos. La tecnología de información puede emplearse para recoger y analizar información usada para soportar el desarrollo de este plan.

Dependiendo del tamaño y necesidades de la auditoría que se lleve a cabo, las tareas necesarias para desarrollar un plan de auditoría (descritas a continuación),

pueden estar asistidas por diferentes herramientas para generar reportes, exposiciones, hojas de cálculo o bases de datos.

*Definición del universo de auditoría.*

La definición del universo de auditoría involucra la identificación de localidades auditables, así como el establecimiento de factores de riesgo, planeación de actividades para conducir la auditoría, identificación de pistas de auditoría y priorización de hallazgos.

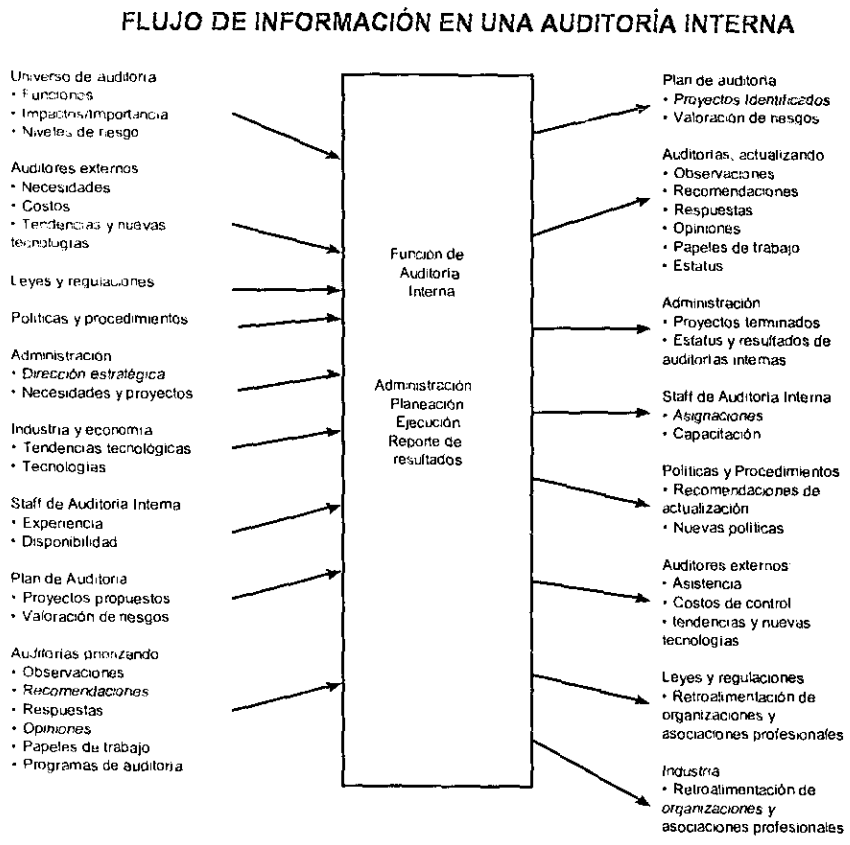


Fig. 4.2

*Establecimiento de frecuencia de auditorías.*

La organización que está siendo auditada y los auditores, deben establecer el alcance de la auditoría, basándose en la actividad de los procesos de negocio, es decir, tratando de no impactar el ritmo normal de los sistemas.

*Creación del Plan de Auditoría.*

La creación del plan de auditoría involucra la identificación, cuantificación y comparación de información similar de diferentes áreas, operaciones o funciones. Los factores de riesgo normalmente se ven relacionados con la estabilidad de operaciones, complejidad en la información de los sistemas y en la multiplicidad de entes involucrados en los procesos de negocio.

*Medición de la efectividad del Plan de Auditoría.*

Las mismas herramientas automatizadas pueden ser usadas para registrar y medir los resultados que se vayan obteniendo contra lo planeado. Por ejemplo, datos como la fecha de inicio del plan, la duración del mismo, el esfuerzo de trabajo de cada recurso, el número de auditores empleados, etc., pueden ser administrados por **Microsoft Project**, de tal manera que el desarrollo de la auditoría pueda ser medido con eficiencia desde el principio hasta el final.

*Software para la Planeación.*

La paquetería de software especificamente diseñada para soportar el desarrollo del plan de auditoría, ofrece varias funciones, incluyendo las siguientes:

- Definición y evaluación de riesgos.
- Evaluación de la importancia de las áreas a auditar.
- Identificación y análisis del perfil del personal que se va a reclutar, capacitar y asignar a la auditoría.
- Desarrollo de planes de auditoría a corto, mediano y largo plazo, basados en evaluación de riesgos, cumplimiento de metas, etc.

*Ventajas del uso de Tecnología de Información en la planeación.*

Las ventajas del uso de Tecnología de Información para soportar el desarrollo del plan de auditoría, incluyen lo siguiente:

- Definición y evaluación de riesgos, así como lograr que dichas evaluaciones sean precisas y consistentes.
- La cantidad de información puede ser eficientemente analizada conforme vaya creciendo.

- El impacto de los diferentes escenarios de planeación, tales como el decremento en la frecuencia de auditorías o la necesidad de ampliar el alcance de las mismas, es fácilmente determinado.

Punto de control: Desarrollo del Calendario Detallado de Auditoría

Una vez que el plan de auditoría está terminado, debe realizarse un calendario detallado para la realización de las auditorías (se recomienda usar **Microsoft Project**). En el calendario de auditoría deben plasmarse, entre otros puntos, las actividades a realizar, así como la dependencia que existe entre las mismas, fechas de inicio y terminación de cada actividad, recursos empleados, esfuerzos generados, costos, etc.

Esto permitirá contar con un control estricto en el cumplimiento del plan, así como marcar la pauta para modificar, si es el caso, el alcance de la auditoría.

Punto de control: Desarrollo y Administración de Recursos Humanos

El reclutamiento, desarrollo y administración de recursos calificados son responsabilidades administrativas de la auditoría que pueden estar soportadas por la tecnología de información en dos formas:

*Seguimiento al desarrollo y desempeño del staff de auditores.*

Con la finalidad de cumplir con el plan y el calendario, los auditores deben tener la capacidad de identificar áreas de oportunidad y necesidades de capacitación de acuerdo a las entidades que se estén auditando. Asimismo, es posible proveer esta información en un web site de los despachos de auditores, a manera de repositorio de habilidades y experiencia del staff de auditores, con la finalidad de que los altos ejecutivos de las empresas que deseen ser auditadas puedan seleccionar al personal idóneo.

La información del repositorio puede incluir lo siguiente:

- Perfiles generales y especializados.
- Puntos débiles generales y específicos.
- Valorización de desempeño.
- Áreas de oportunidad prioritarias.
- Planes de capacitación prioritarios.
- Carreras de avance de los auditores.

*Capacitación del personal.*

La administración de la auditoría debe reconocer la importancia de capacitar al personal en el uso de tecnología de información para asegurar la eficiencia de las aplicaciones, desarrollo e implementaciones a bajo costos. Adicionalmente, debe existir el compromiso de que la capacitación sea exitosa, ya que la oportunidad en que sea usada, formará nuevos perfiles dentro del staff de auditores.

Punto de control: Desarrollo y Mantenimiento de Políticas y Procedimientos Administrativos

Las políticas y procedimientos administrativos que proporcionan guías y directrices en la función de auditoría deben ser exactas, actuales y disponibles para todo el personal. La tecnología de información debe usarse para soportar el desarrollo y mantenimiento de políticas y procedimientos de lo siguiente:

*Procesamiento de palabras y almacenamiento electrónico de datos.*

Los procesadores de palabras pueden ser usados para desarrollar y mantener las políticas y procedimientos administrativos. Si el software es usado en una computadora portátil, los auditores deben cargar consigo las licencias de uso.

*Centro de información de auditoría en línea.*

En complemento al repositorio de información del staff de auditores, el centro de información de auditoría en línea representa el más avanzado uso de tecnología de información para soportar el desarrollo y mantenimiento de políticas y procedimientos administrativos, proporcionando acceso vía telecomunicaciones.

Punto de control: Planeación y Administración de la Auditoría

La planeación de la auditoría incluye las siguientes actividades, que pueden ser soportadas por la tecnología de información:

*Actualización de información de todos los planes y calendarios de auditoría.*

El proceso de actualización de información debe formar parte del plan y el calendario de auditoría, reevaluando riesgos e impactos de cambios derivados de rotación de personal o cambio de equipos de cómputo.

*Definición del alcance de la auditoría.*

La decisión de incluir o excluir una área especifica o función del alcance de la auditoría, debe estar soportada por información real, misma que debe ser obtenida de las siguientes fuentes:

- Valorización de riesgos.
- Resultados de auditorías prioritarias.
- Datos financieros y operacionales de las áreas o funciones a ser auditadas.
- *Materiales de referencia, tales como manuales técnicos y guías* reguladoras.

Punto de control: Uso de la Tecnología de Información para revisar los niveles de actividad del sistema

*Uso de Logs del Sistema.*

Muchos sistemas producen automáticamente un log de actividad, en donde se incluye, entre otros, los siguientes datos:

- *Jobs procesados.*
- Archivos usados.
- Fecha y hora de procesamiento.
- Tiempo de procesamiento.

Los auditores pueden usar los logs de actividad para una gran variedad de análisis, así como para confirmar lo siguiente:

- Solamente programas aprobados pueden accesar datos sensitivos para la organización.
- Uso correcto de utilerías capaces de alterar la información de los archivos.
- Los programas solamente son ejecutados de acuerdo a una calendarización de procesos.
- Los jobs de producción accesan los archivos correctos.
- Las terminaciones anormales de programas, violaciones de seguridad y otras anomalías son investigadas y resueltas.

El auditor puede usar las siguientes herramientas para analizar los logs de actividad:

- Software generalizado de auditoría.
- Software de regreso de información.
- Software especializado para analizar o auditar sistemas operativos.

Las consideraciones para el uso de logs de actividad, incluyen lo siguiente:

- Las estructuras de datos o layouts de archivos pueden ser complicadas y pueden existir muchos tipos de registros.
- Para disponer de datos reales tomados del log, el auditor debe verificar lo siguiente:
  - Que los datos están seguros.
  - Que los datos están respaldados.
  - Que la información no es propensa a perderse.

*Revisión del Control de Cambios a componentes.*

El control de cambios de componentes debe proporcionar lo siguiente:

- Seguridad para prevenir y detectar cambios accidentales o no autorizados.
- Pistas de auditoría de todos los cambios a los módulos, programas, lenguajes de control de tareas (jcl), incluyendo un registro con la fecha de cambio, personal responsable (user-id) y el estatus del cambio.
- Procedimientos de aseguramiento de calidad para confirmar la consistencia de los programas fuente y módulos de carga.

Una auditoría al control de cambios a componentes, involucra pruebas extensivas a todos los controles, incluyendo aprobación y aceptación de cambios y pruebas. Las herramientas computarizadas y técnicas deben incluir lo siguiente:

- Evaluaciones de los niveles de acceso a los programas y bibliotecas de jcl's.
- Utilería para listar la longitud de cada miembro de la biblioteca de carga en un momento específico, así como para identificar aquellos módulos que cambien de longitud después del primer listado.
- Herramientas para reportar la siguiente información:
  - Cambios a programas individuales.
  - Cambios por tipo.
  - Identificación del personal que realiza los cambios.
- Herramientas para comparar las versiones de un mismo programa en diferentes fechas de procesamiento.

Punto de control: Licencias de Software

Una licencia de software permite a un cliente usar una copia o un número indeterminado de copias de un producto en uno o más equipos. Los vendedores

pueden transferir derechos sobre el uso de software a los clientes de diversas maneras, incluyendo:

- Licencia sin derechos para reproducir, vender o sublicenciar el software en otras localidades de la organización.
- Licencia para reproducir, distribuir o venderlo a los usuarios.
- Venta de todos los derechos de un producto desarrollado por el vendedor.
- Venta de la mayoria de los derechos de un producto parcialmente desarrollado por otro proveedor, para la inclusión de otros módulos, ya sea de hardware o software.

Las licencias para reproducción de software, no necesariamente deben ser una reventa de los derechos de copia de un producto. Este tipo de licencias tienen uno de los siguientes acuerdos:

- Precio fijo.
- Cuota por derechos de autor.
- Combinación de precio fijo más una cuota por derechos de autor.

El contrato de soporte generalmente consiste de los siguientes elementos:

- Soporte telefónico.
- Corrección de errores (encontrar fallas de software).
- Nuevos de productos.

Punto de control: Seguridad Física

La información y los recursos de cómputo son activos que deben estar protegidos de accesos no autorizados, manipulación y destrucción. Un plan para contar con seguridad fisica debe diseñarse para:

- Prevenir accesos no autorizados a las áreas de operación de computadoras.
- Detectar intentos de accesos no autorizados, así como registrar todos los accesos válidos.

*Seguridad en Sitio.*

Existen muchas tendencias relacionadas con la instalación de equipos de cómputo y centros de información. Una de ellas se relaciona con la distribución de estaciones de trabajo y pc-lites en el departamento de los usuarios.

Por otro lado, una segunda tendencia se enfoca en consolidar centros de cómputo dentro de megacentros de información.

A pesar de estos controles, los factores de seguridad física implicados con la instalación de equipos de cómputo y centros de información deben incluir lo siguiente:

- Los centros de información no deben estar visibles para todo el personal de la organización.
- Para muchas organizaciones, el lugar ideal para un centro de información es un sitio apartado de conglomeraciones humanas.
- El sitio debe contar con todos los servicios de limpieza, así como tener servicio telefónico controlado.
- El acceso a personas no autorizadas debe estar controlado.
- La posibilidad de riesgos naturales debe ser minimizada.
- Las organizaciones deben evitar en lo posible, construir los centros de información en áreas que sean susceptibles a inundaciones, huracanes, terremotos, erupciones, incendios, etc.
- Deben desarrollarse planes de emergencia para actuar bajo desastres.
- Los arbustos, árboles y demás objetos que puedan ser usados como camuflaje para intrusos, deben ser apartados de la entrada del centro de información.
- El número de puertas y ventanas deben estar limitadas y el acceso a través de otras entradas, por ejemplo, tragaluces, conductos para deposito de basura, ranuras para correo, etc., deben ser clausurados.
- El cuarto de computadoras debe estar bien localizado en el interior del edificio, apartado de ventanas y paredes periféricas.
- Las paredes del cuarto de computadoras deben construirse con mampostería fuerte o con cualquier otro material de difícil penetración.
- El centro de información deberá contar con indicadores locales y nacionales contra incendios y el cuarto de computadoras deberá contar con el equipo necesario para prevenir incendios.
- El mobiliario que se encuentre en los centros de información tendrá que ser resistente a los incendios, así como el fumar deberá ser restringido.

*Detectores.*

Una gran variedad de detectores con alarma, pueden ser usados para brindar mayor seguridad, tales como los siguientes:

- Sensores de humo y calor.
- Detectores de agua y combustión de partículas.
- Controladores de temperatura y humedad.
- Sistemas para detección de intrusos.

Para contar con una cobertura amplia de seguridad física, los sensores no solamente deben estar instalados en los centros de información, sino también en las inmediaciones del edificio. Las alarmas deben ser automáticamente sensibles a cualquier incidente, debiendo ser monitoreadas por una persona que, al detectar el siniestro, pueda tomar las acciones correctivas pertinentes.

Una alarma contra incendio no solamente deberá sonar para avisar a un grupo de personas, sino que también deberá avisar al departamento de bomberos de lo que ocurre.

La experiencia dicta que los materiales comúnmente usados para la supresión de incendios en los centros de información, son el agua, el gas Halón y el dióxido de carbono ($CO_2$).

La producción de gas Halón se ha visto mermada debido a medidas ecológicas. El uso de ($CO_2$) ha declinado debido al alto riesgo de sofocación entre las personas, así como también su uso forma pequeñas capas de hielo en las superficies en donde se aplica.

Las principales ventajas y desventajas de usar sistemas de supresión de incendios basados en agua y gas se encuentran resumidas en la siguiente tabla:

| **Sistemas de supresión de incendios basados en agua** | |
|---|---|
| **Ventajas** | **Desventajas** |
| • Enfría los equipos.<br>• Seguridad para el personal y el ambiente.<br>• Normalmente es más barata su instalación y uso.<br>• Puede ser creado un sistema interconectado entre edificios.<br>• La liberación del agua puede estar localizada en el lugar que se necesite.<br>• Los modernos sistemas de entubamiento, minimizan las descargas accidentales. | • Contiene impurezas que pueden dañar al equipo y, por consiguiente, a los datos.<br>• Pueden generar daños eléctricos al no contar con interrupción automática de riego.<br>• Se requiere una alta temperatura para que puedan ser activados los sensores.<br>• El agua no puede alcanzar el fuego que se origine dentro de equipos o archiveros. |

| Sistemas de supresión de incendios basados en gas | |
|---|---|
| **Ventajas** | **Desventajas** |
| • No daña hardware.<br>• No conduce electricidad.<br>• Apaga incendios dentro de equipos o archiveros.<br>• El cuarto de computadoras o todo el centro de información, puede estar operando nuevamente después de dos horas de haber liberado el gas. | • El gas Halón contribuye a la destrucción de la capa de ozono.<br>• El gas Halón puede ser dañino para la salud, el $CO_2$ puede ser mortal.<br>• La fuerza de liberación de gas es altamente potente y puede ser peligrosa.<br>• Puede ser muy cara.<br>• El fuego puede reiniciarse si se desaloja inmediatamente el gas.<br>• Llena completamente el cuarto de computadoras; el $CO_2$ requiere la disponibilidad de un equipo de oxigeno de emergencia. |

*Controles de Acceso Físico.*

Los dispositivos de control de acceso deben cubrir los siguientes requerimientos:

- Teclados que permitan la entrada a personas que introduzcan correctamente la combinación de números requerida para el acceso.
- Sistemas basados en tarjetas electrónicas, los cuales usan tarjetas plásticas con una banda magnética que contiene información codificada.
- Sistemas biométricos, los cuales incluyen dispositivos que permiten el acceso mediante la identificación única de rasgos físicos, por ejemplo, huellas digitales, patrones de voz e identificación de patrones vasculares de los ojos.
- Guardias monitoreando la entrada mediante circuitos cerrados, a fin de complementar el controles de acceso.

*Ambiente del cuarto de computadoras.*

Los requerimientos ambientales del cuarto de computadoras, caen en las siguientes categorías:

- Requerimientos de espacio físico.
- Piso falso.
- Flujo de aire y requerimientos de acondicionamiento.
- Requerimientos eléctricos y misceláneos, por ejemplo, vibraciones, disturbios electromagnéticos, ruido, niveles de iluminación, etc.

Las especificaciones de instalación de piso falso, el cual soportará la instalación del equipo de cómputo, deben ser lo suficientemente claras para:

- Instalación de cableado.
- Distribución de componentes para enfriamiento por medio de agua y sistema de aire acondicionado.
- Instalación de detectores de fuego y agua debajo del piso falso.
- Drenaje.

*Distribución de energía y recuperación.*

Las variaciones en los voltajes y frecuencias son resultado tanto de condiciones externas e internas que afectan los equipos de cómputo. Algunos equipos contienen fuentes de poder internas que proveen de la energía necesaria para continuar procesando hasta que se normalice el suministro, o bien, presentan procedimientos para que se apague el sistema de manera ordenada interactuando con el usuario.

De no contar con un suministro alterno de energía, puede ocurrir lo siguiente:

- Cualquier variación fuerte de energía, puede hacer que el sistema se "caiga" y no será posible reprocesar la información en el punto de falla.
- La recuperación requiere la restauración del sistema, realmacenar archivos y bases de datos, tomándolos del último respaldo y comenzar el reprocesamiento desde ese punto.

Existe una gran variedad de dispositivos protectores de interrupciones momentáneas de energía. Las organizaciones cuentan con dos opciones básicas cuando se evalúa la adquisición de fuentes alternas de suministro de energía temporal:

- Suministro ininterrumpible de energía (Uninterruptible Power Supply UPS), el cual puede proveer de energía durante un tiempo limitado en caso de fallas de suministro eléctrico. Después de cinco o diez minutos de suministro, el administrador del centro de información puede iniciar el proceso ordenado de apagado o "shutdown". Esta estrategia elimina el impacto causado por las fallas y reduce significativamente el tiempo de restauración.

- Suministro emergente de energía (Emergency Power Supply EPS), el cual consiste de un motor a gasolina o diesel que proporciona energía por varias horas a los equipos de cómputo, luces de emergencia y dispositivos de control de acceso.

*Riesgos.*

Los riesgos asociados a una pobre planeación de instalación, son los siguientes:

- Robo o destrucción de equipo y/o datos.
- Perdida del centro de información, como resultado de desastres naturales.
- Interrupciones en el procesamiento, resultado de fallas en el suministro de energía eléctrica y agua.

Los riesgos asociados con la falta de instalación de dispositivos detectores, son los siguientes:

- Intromisiones no detectadas.
- Daños o perdida de equipos y/o datos, resultado de un incendio o inundación no detectada.

Los riesgos asociados con un inadecuado control de acceso físico, son los siguientes:

- Accesos no autorizados al equipo de cómputo.
- Posible perdida o destrucción de equipos.
- Accesos no autorizados a bibliotecas de programas, utilerías y bases de datos.
- Robo, copias no autorizadas, cambios no programadas o destrucción de datos.

Asimismo, los riesgos en los que se incurre con un control excesivo de acceso físico son los siguientes:

- Inconveniencia para la legitimación de empleados.
- Lentitud para atender emergencias y para evacuar rápidamente el lugar.

Por otro lado, los controles que se pueden emplear para mitigar estos riesgos son:

- Contar con plan de recuperación (probado y autorizado) en caso de desastres.
- Respaldo fuera de sitio de la información sensitiva para la organización.
- Pruebas periódicas al funcionamiento del equipo.

- Monitoreo del acceso al centro de información de la organización.
- Revisiones periódicas de listas de personas autorizadas para accesar a áreas restringidas.
- Elaboración de políticas y procedimientos para asegurar la pronta notificación de cambios en los roles de trabajo de los empleados.
- Elaboración de políticas y procedimientos que se refieran al cambio periódico de claves de acceso.
- Inculcar entre los empleados la cultura de seguridad de la información.

Punto de control: Planes de Respaldo/Reinicio y Recuperación en Caso de Desastres

*Plan de Respaldo/Reinicio.*

El resultado del procesamiento de una aplicación puede terminar anormalmente debido a una gran variedad de factores, entre los que se encuentran:

- Defectos de software.
- Errores o condiciones inusuales que el programa no puede soportar.
- Fluctuaciones o interrupciones en el suministro de energía eléctrica.
- Problemas de red.
- Mal funcionamientos de hardware.

Para los procesos batch que requieren un tiempo de procesamiento largo, es aconsejable usar la técnica de "punto de chequeo / reinicio" (checkpoint / restart), la cual requiere que el estatus de varios archivos y flujos de información sean registrados por el sistema en un punto de chequeo o checkpoint (por ejemplo, establecer un checkpoint cada 5,000 registros procesados). En caso de fallas, el programa y sus archivos pueden ser realmacenados desde el ultimo checkpoint y el procesamiento puede restablecerse. Esto puede ahorrar una cantidad significativa de tiempo de procesamiento, de tal manera que el job no tendrá que ser ejecutado desde el principio.

Si lo que falla es una aplicación en línea, particularmente cuando varios usuarios están ingresando información, el restablecimiento del proceso desde el punto de falla puede ser muy difícil, aun y cuando el estatus exacto de transacciones en línea pueda ser determinado. Las siguientes cuatro técnicas sobre recuperación en línea, son las más efectivas:

- Establecer un método de registro o log de transacciones, en el cual, un simple archivo journal (respaldado en cinta magnética) registre la secuencia de captura de las transacciones, así como la fecha y hora (en formato timestamp AAAAMMMDDHH:MM:SS:MSG) en que fueron ingresadas al sistema; esto en adición a un respaldo periódico del archivo maestro.

- Pre-actualizar el archivo de transacciones maestras, para lo cual se emplea una serie de registros pares (por ejemplo, una copia del registro de actividad del archivo maestro antes de la actualización y una copia de las transacciones que serán aplicadas al archivo maestro).
- Post-actualizar el archivo de transacciones maestras, para lo cual se emplea la técnica anterior, excepto que el archivo journal contenga una copia de cada registro maestro después de la actualización y que no contenga la imagen de la transacción.
- Efectuar un barrido completo de información (full trace), el cual provee la mejor pista de auditoría, pero incurre en significativas cargas de trabajo para el equipo, por ejemplo, requerir una copia de la pre-actualización y post-actualización del archivo maestro y del registro de transacciones.

Los riesgos en los que se puede incurrir en caso de no contar con un Plan de Respaldo/Reinicio adecuado son los siguientes:

- Incapacidad para restablecer los archivos y bases de datos a sus estatus iniciales, así como la nula reinicialización de procesos batch que consumen mucho tiempo máquina y recursos.
- Incapacidad de restablecer las aplicaciones en línea, al estatus que presentaban al inicio del día.

*Plan de Recuperación en caso de desastres.*

Las organizaciones se han vuelto cada vez más dependientes de las computadoras para realizar sus actividades día con día y por lo tanto, el impacto derivado de las fallas en los sistemas se convierte en un problema potencial. La falla puede generar un severo impacto financiero, por ejemplo, perdida de negocios, incapacidad para continuar con los procesos, etc., costando a menudo, mucho más dinero que solamente el tiempo máquina perdido.

Para contrarrestar estos efectos, es necesario que las organizaciones generen un Plan de Recuperación en caso de desastres, el cual debe considerar lo siguiente:

- Análisis de impactos al negocio, identificando las aplicaciones críticas y estimando los costos asociados con la caída o daño al sistema.
- Participación del área usuaria, para definir responsabilidades y acciones.
- Las copias de respaldo de los archivos, programas, bases de datos, etc., deberán ser almacenados fuera de sitio.
- Los jobs que se procesan deben estar categorizados con prioridad alta (aquellos que son críticos para la continuidad del negocio), de prioridad media (aquellos que se ejecutan cuando se cuenta con disponibilidad de recursos) y de prioridad baja.

- Para cada condición de falla, las acciones a seguir deberán ser exhaustivamente probadas antes de ser usadas.
- Los procedimientos de recuperación deberán ser monitoreados para asegurar que están siendo implementados.
- El plan debe ser probado periódicamente, modificando su estructura basándose en los resultados de las pruebas.
- Todo el plan en conjunto debe considerar los requerimientos de negocio, el diseño técnico del sistema y la capacidad de administración de recursos informáticos de la organización.

La mayoría de estas consideraciones aplican a los planes de recuperación en caso de desastres para una Red de Área Local.

Los riesgos asociados con un inadecuado plan de recuperación en caso de desastres, son los siguientes:

- Incapacidad para continuar procesando información, así como interrupción de procesos prioritarios para el negocio, mismos que derivan en cuantiosas pérdidas financieras.
- Dificultad de recuperación.

Punto de control: Seguridad Lógica

Los sistemas de software son un conjunto de programas diseñados para operar, controlar y extender las capacidades de procesamiento de los equipos de cómputo. Debido a que los desarrollos de software implican el manejo de información sensitiva para las organizaciones, se hace necesario contar con medidas para proteger este valioso activo.

Con respecto a lo anterior, se presenta un aspecto básico en la administración y uso de sistemas de software: la seguridad lógica de los sistemas, es decir, los controles que evitan que se ignore o modifiquen los sistemas mediante supuestos privilegios.

Los controles deben considerar lo siguiente:

- Instalación de software de seguridad que controle entradas y salidas a los sistemas, así como soporte de passwords de multinivel para protección de bibliotecas y datos.
- Incorporación de archivos que reporten los diferentes accesos de usuarios, registrando el USER-ID, password, fecha y hora de acceso.
- Utilizar un programa que monitoree el uso de los programas y recursos informáticos.
- Proveer pistas de auditoría detalladas procesadas por el sistema operativo.

- Instalar software de encriptación de información.
- Instalar un software para analizar el desempeño de la red de computadoras y monitoreo de telecomunicaciones.
- Asegurar la integridad de todos los reportes especiales y logs del sistema.
- Inculcar entre los empleados, la cultura de seguridad de la información.

Los riesgos asociados en los que se pueden incurrir en caso de no contar con controles para proteger los recursos sistemáticos (incluyendo programas, aplicaciones desarrolladas, especificaciones de programación, documentación dispositivos de almacenamiento y memoria principal de los equipos) son los siguientes:

- Perdida parcial o total de información vital para la organización, derivando con esto en fuertes impactos financieros.
- Mal uso de datos y especificaciones.

Con la finalidad de evaluar la seguridad lógica de los sistemas, el auditor debe analizar lo siguiente:

- Determinar como las organizaciones protegen la información, así como verificar la eficiencia de los controles implementados.
- Probar las funciones de los sistemas de seguridad de software para reportar el estatus de protección, a fin de verificar la integridad de los componentes del sistema operativo.
- Revisar la lista de programas de bibliotecas autorizadas para desarrollo de sistemas (estos programas presentan privilegios especiales de uso, por lo que pueden ser empleados erróneamente).
- Probar el software de control de acceso a programas y/o aplicaciones, tratando de violar la seguridad (se debe realizar esto con el apoyo y aprobación del administrador de seguridad).
- Probar el software de seguridad para determinar si contiene pruebas de programas en el ambiente de producción, en vez del ambiente de pruebas o preproducción.
- Obtener la lista de personas que tienen acceso a cada área en donde se encuentren equipos de cómputo, confirmando si dichos accesos están debidamente autorizados.
- Obtener la lista de todas las terminales y sus autoridades de acceso. Probar con esto si las terminales están bloqueadas o inaccesibles a personas no autorizadas.
- Verificar que solamente personas autorizadas poseen las llaves de entrada al cuarto de computadoras, las llaves de los gabinetes de los equipos y si se tienen resguardados los passwords de los usuarios y desarrolladores de sistemas.

Punto de Control: Usuario Final

Se refiere al uso de sistemas y aplicaciones que los usuarios crean, adquieren, mantienen y operan fuera de un sistema de información tradicional. Las categorías de hardware y software asociadas incluyen lo siguiente:

- Microcomputadoras, estaciones de trabajo, minicomputadoras y mainframe.
- Sistemas operativos, utilerías de software.
- Comunicaciones y control de software de red.
- Procesador de palabras, hojas de cálculo, bases de datos, lenguajes de cuarta generación, software para análisis gráfico, etc.

*Riesgos y Controles.*

Los riesgos asociados a los desarrollos del usuario final son:

- Los datos no son tan confiables como se espera, debido a que los usuarios que elaboran sistemas no siguen el desarrollo de controles de sistemas tradicionales.
- Los nuevos usuarios pueden estar desactualizados con los métodos para pronosticar requerimientos de sistemas y costos, desarrollando respaldos y procedimientos de contingencia y mantenimiento sin un análisis costo - beneficio adecuado.
- Establecer desarrollo de aplicaciones dentro de departamentos que puede resultar en duplicidad de esfuerzo y alto costo para la organización.
- La documentación puede ser limitada.
- La aplicación de controles puede ser inadecuada o no existir.

*Consideraciones a Auditar*

Una auditoría a los usuarios finales puede ser llevada a cabo en forma independiente de otros sistemas o como parte de un programa adicional, además de que puede ser periódica.

Punto de control: Telecomunicaciones

Las telecomunicaciones son definidas como las actividades mecánicas, eléctricas y electrónicas que habilitan a la gente y máquinas a comunicarse entre sí a determinadas distancias.

La función de las telecomunicaciones es transportar hacia el exterior de una organización, una variedad de medios de comunicación y son manejados por un portador de comunicaciones. Los mensajes son transportados por dispositivos

especiales, por ejemplo, alambre de cobre, cable coaxial, fibra óptica o microondas.

*Riesgos y Controles.*

Los riesgos asociados con la actividad en el área de telecomunicaciones, incluyen lo siguiente:

- Servicio no disponible o perdida de datos.
- El impacto al negocio puede resultar de una falla en los medios de comunicación que privan el manejo de los datos requeridos para tomar decisiones de negocio.
- Acceso de usuarios no autorizados a la red para envio, modificación o supresión de datos, así como negar el uso de servicios legítimos.
- El costo de la red puede ser demasiado alto para la actividad de negocios.

Existen también riesgos y controles asociados con usuarios quienes usan redes publicas switcheadas y que pueden tener acceso cuando marcan a la red. En estos casos se pueden mencionar los siguientes controles:

- Uso de módems síncronos en vez de módems asíncronos para conectarse a la red, así como dispositivos de protección de puertos.
- Uso de dispositivos de supresión de tonos sobre los puertos.
- Uso de servicios de verificación de autorización, desconectando usuarios después de un número determinado de intentos de accesos.

El control principal a considerar es el siguiente:

- Seguridad física y lógica de la red para impedir que los usuarios tengan acceso desde dispositivos físicos o medios de transmisión.

*Consideraciones a auditar.*

El paso lógico en la planeación de objetivos y alcances de la auditoría de telecomunicaciones, es determinar quién debe ser entrevistado al auditar la red. Los candidatos pueden ser los siguientes:

- El administrador de telecomunicaciones, quien controla la operación, el presupuesto y los planes de comunicación.
- El administrador de la red, quien tipicamente maneja el personal y el equipo.
- El administrador de las aplicaciones de comunicación, quien es responsable de los requerimientos de aplicaciones dentro de una realidad técnica.

Punto de control: Plan de Contingencias

El objetivo principal de la planificación de contingencias es proporcionar a la organización la habilidad de continuar con las operaciones críticas. La planificación de contingencias requiere de procedimientos adecuados y certificados en la recuperación de datos en caso de desastre.

La planificación de la contingencia es, en términos prácticos, un proceso que consta de las siguientes consideraciones:

- Metodología de planificación de contingencias y ciclo de vida.
- Apoyo a usuarios, para lograr una recuperación exitosa, ya que finalmente son responsables de asegurar la continuidad de negocio de la organización.

Una de las fases más críticas iniciales en la planeación de la contingencia es el análisis del riesgo, el cual identifica y prioriza las aplicaciones críticas que necesitan ser restauradas.

El éxito del plan de contingencia esta directamente relacionado con la calidad de su documentación, ya que si esta no refleja con precisión el estado presente de los medios, personas, hardware, software, comunicaciones y servicios del apoyo, se pudiese arriesgar el esfuerzo de recuperación.

*Riesgos y Controles.*

Los riesgos específicos y sus consecuencias para planificación de contingencias incluyen:

- Perdidas financieras y de información importante para la organización.
- Multas y sanciones.

*Consideraciones a auditar.*

- Desarrollo y documentación de una contingencia planeada basada en un análisis de riesgo adecuado.
- Involucramiento del usuario en los planes de desarrollo y mantenimiento.
- Comprobación periódica y revisiones para asegurar que se puede llevar a cabo el plan.
- El auditor interno debe evaluar la suficiencia del plan y proporcionar recomendaciones correctivas.

## 4.4 FFIEC (Consejo Examinador Federal de Instituciones Financieras).

### 4.4.1 Descripción general.

En 1996 el Consejo Federal Examinador de Instituciones Financieras (FFIEC) de los Estados Unidos de Norteamérica, conformado por los dirigentes del Sistema de la Reserva Federal, la Corporación del Seguro del Ingreso Federal, la Administración de la Unión de Crédito Nacional, la Oficina del Interventor del Dinero y la Oficina de Vigilancia de la Economía, crea un manual estructurado para apoyar a los profesionales encargados de auditar los sistemas de información en instituciones financieras y empresas independientes.

Este manual contiene una apreciación global de conceptos de los sistemas de información, prácticas, ejemplos y programas de trabajo aplicables a la auditoria de sistemas de información.

El manual se ha enfocado en la creación y promoción de:

- Guías para mejorar la supervisión y el análisis.
- Capacitación para nuevos auditores en sistemas de información.
- Referencia y búsqueda de excepciones.
- Evaluación de recursos técnicos.

Gran parte del manual ha sido reorganizado y revisado para reflejar con más exactitud los cambios de información en el ambiente. Los cambios más significativos incluyen el desarrollo de varios capítulos con nuevos programas de trabajo.

El manual establece que las instituciones financieras deben establecer controles internos efectivos, así como desarrollar sistemas de administración para salvaguarda de información y medidas operativas avanzadas y confiables. Plantea también revisiones y evaluaciones del control interno en los sistemas de información, cubriendo la integridad, realidad y veracidad de los datos, así como la calidad de la información para toma de decisiones.

Las revisiones consisten en identificar los riesgos que pueden originarse, sondeando las operaciones de inseguridad que pueden derivar, entre otros puntos, en:

- Manejo inadecuado de la información de aplicaciones prioritarias para la organización.
- Contratos ineficientes de desarrollo y mantenimiento con proveedores.
- Violaciones a la seguridad de los sistemas.
- Compras y adquisiciones fuera de presupuesto.

### 4.4.2 Objetivos de Control.

Punto de control: Administración de la red

1. Si en la institución la red LAN presenta arquitectura cliente/servidor y usa un sistema de telecomunicaciones para el transporte de información, entonces el auditor deberá enfocarse a la evaluación de:

   - Operación de terminales remotas.
   - Operaciones remotas cliente/servidor haciendo uso de proceso distribuido y/o impresión/operación de servicio.

2. Determinar si el sistema operacional de la red cuenta con un plan de recuperación en caso de desastre y plan de contingencia.

Punto de Control: Seguridad

1. Determinar si la organización usa un sistema de seguridad on-line, evaluando si este es adecuado y efectivo.

2. Evaluar, si existen, las políticas de seguridad de datos basándose en:

   - Periodicidad de revisión por un funcionario.
   - Niveles de autorización de acceso.
   - Procedimientos de cambio de password y su composición.
   - Responsable de mantener la seguridad del archivo de passwords.
   - Violaciones al sistema (monitoreo y rastreo).
   - Actividad de logs de violaciones a la seguridad.

*Consideraciones a auditar.*

1. Evaluar los controles de entrada de datos desde el punto de origen.

2. Identificar controles durante los procesos de entrada, proceso y salida.

3. Evaluar políticas, procedimientos o prácticas estándar que describan las aplicaciones y la programación de los sistemas, determinando si estos procedimientos son usados y adecuados.

4. Identificar:

   - Deficiencias significativas de control interno.
   - Acciones correctivas para corrección de deficiencias.

Punto de Control: Seguridad Física y Lógica

Los sistemas de información determinan que la seguridad es la estructura de control establecida para proteger la integridad, confiabilidad y viabilidad de los datos y recursos de la computadora.

Hay dos tipos básicos de seguridad usados para proteger los sistemas de información: seguridad física de sistemas y redes y seguridad lógica de los datos y recursos.

*Riesgos y Controles.*

De no contar con un proceso de seguridad de información, se podría incurrir en los siguientes riesgos:

- Desventaja competitiva de la organización en el mercado, ya que la importancia estratégica de guardar y administrar los datos es de vital importancia.
- Incapacidad de la organización para toma de decisiones en operaciones importantes.

Los principales controles asociados a la seguridad son:

- Determinar las líneas de acción de la organización respecto a los sistemas de información, estableciendo políticas para alinear los objetivos de la organización a los procesos de seguridad.
- Involucrar a los procedimientos rutinarios y los planes estratégicos de la organización en los procesos de seguridad.
- Políticas basadas en recursos humanos y prácticas estándar de seguridad.
- Establecer un departamento encargado de generar políticas y procedimientos de seguridad de información, así como vigilar que los integrantes de la organización se apeguen a los mismos.
- Establecer los niveles de protección que los datos requieren.
- Proteger el centro de cómputo contra daños potenciales de fuego, agua y otros riesgos medio - ambientales.
- Limitar el acceso físico a recursos e instalar sistemas de alarma.
- Implementación de controles de acceso de software.

*Consideraciones a Auditar.*

1. Seguridad Física. Lo más común respecto a la seguridad física, es determinar cuáles son las áreas sensibles relacionadas con los sistemas de información, incluyendo las operaciones de computadoras y el trabajo general de las áreas. Estas áreas deben estar acondicionadas para que soporten el equipo (ejemplo: aire acondicionado, paneles de control, etc.).

2. Seguridad Lógica. Los sistemas de información requieren de seguridad lógica, estableciendo controles que permitan a la organización monitorear usuarios, datos y recursos para controlarlos y producir o hacer auditorías de la actividad del sistema. La identificación de usuarios y el acceso que tienen a los recursos informáticos de la organización, son elementos críticos en la seguridad lógica. La identificación de usuarios debe estar acompañada de un password o bien, empleando otros procedimientos (identificación de huellas digitales, retina y firmas). El desarrollo de controles lógicos debe evaluar los caminos de acceso de los datos y la información. Es recomendable usar múltiples niveles de seguridad que garanticen que los datos están siendo accesados por los usuarios autorizados.

La evaluación al proceso de seguridad se puede desarrollar seleccionando los aspectos apropiados en materia de seguridad física y lógica, personalizando aquellos que encajan en los planes operativos, tácticos y estratégicos de la arquitectura tecnológica de la organización.

Punto de Control: Plan de Contingencia

El objetivo principal de la planificación de contingencias es proporcionar a la organización la continuidad del servicio de las aplicaciones críticas. La planificación de contingencias requiere de procedimientos adecuados y probados para recuperación de datos en caso de desastre.

*Riesgos y Controles.*

Los riesgos específicos y sus consecuencias para planificación de contingencias incluyen:

- Perdida de ventaja competitiva en el mercado.
- Incapacidad para entregar productos o servicios a clientes.
- Multas y/o sanciones por parte de instancias privadas o gubernamentales.

Dentro del proceso de planificación de la contingencia, se deben considerar los siguientes controles:

- Contar con el apoyo del usuario para lograr una recuperación exitosa. Los usuarios dependen de los sistemas de información para manipulación y proceso de datos, ya que son responsables de asegurar la continuidad de la organización cuando ocurre una contingencia.
- Asegurar la calidad del plan, estableciendo una metodología de la planificación y aplicación de planes de contingencias.
- La metodología mencionada debe incluir un ciclo de vida que contemple a su vez análisis del riesgo, documentación, comprobación y mantenimiento.
- Contar con procedimientos de mantenimiento y actualización del plan.
- Llevar a cabo un análisis del riesgo, identificando y priorizando las aplicaciones críticas que necesitan ser restauradas, a fin de establecer el tiempo ideal en el que se deben restablecer las aplicaciones.
- Contar la documentación del plan de contingencia, el cual refleje con precisión el estado presente de los medios informáticos, personas, hardware, software, comunicaciones y servicios de apoyo.

*Consideraciones a auditar.*

- Desarrollo y documentación de un plan de contingencia basado en un análisis del riesgo adecuado.
- Involucramiento del usuario en los planes de desarrollo y mantenimiento.
- Revisiones periódicas para asegurar que se puede llevar a cabo el plan.
- Evaluación de la suficiencia del plan, identificando debilidades y proporcionando recomendaciones preventivas y correctivas.
- Evaluación de la metodología de uso y aplicación del plan.
- Asegurar que el plan incluya una lista de distribución autorizada entre todo el personal de la organización.

## 4.5 EXPERIENCIA DE AUDITORÍA EN INFORMÁTICA EN UNA INSTITUCIÓN FINANCIERA.

### 4.5.1 Descripción general.

De acuerdo con la experiencia profesional adquirida en una institución financiera en el área de auditoria en informática, podemos definir que la misión de ésta es vigilar que la institución cuente con un sistema de control interno que permita la protección de los activos informáticos, a través de la evaluación de los sistemas de información y la tecnología en que se soportan, apegándose a políticas, normas y estándares establecidos.

Objetivos

- Evaluar el apego al sistema de control interno, promoviendo la optimización constante de sus componentes.
- Identificar riesgos que impacten los intereses de la institución por la información contenida en los sistemas e infraestructura en que se soportan, así como en la administración, a efecto de que se tomen las medidas de control necesarias.
- Sugerir el establecimiento de controles preventivos, detectivos y correctivos en tecnologías de información.
- Verificar y evaluar la auditabilidad, seguridad, integridad, eficiencia y vigencia de los sistemas automatizados en los que la institución soporta su operación.

Funciones y Responsabilidades Genéricas

- Vigilar el cumplimiento de políticas, normas y procedimientos establecidos por la institución para las funciones informáticas.
- Evaluar el sistema de control interno en tecnologías de información, seleccionando áreas críticas de operación que involucren riesgos importantes.
- Evaluar el proceso de desarrollo de sistemas a efecto de garantizar la implementación de controles que aseguren la integridad de la información e incrementen la eficiencia en la operación.
- Informar a diferentes niveles las observaciones al control interno detectadas en las revisiones, así como las recomendaciones para corregirlas.
- Ejercer seguimiento sobre las acciones tomadas en el incumplimiento a políticas y procedimientos institucionales, en la corrección de errores y desviaciones y en el tratamiento de casos por excepción o especiales.

**Objetivos de control.**

Sistemas en desarrollo

La Auditoría en Informática a un sistema en desarrollo se divide en dos etapas:

**Cualitativa** Comprende el conocimiento de los procesos clave del negocio, la identificación de riesgos críticos, los controles previstos para el desarrollo del sistema y la evaluación de la estructura del Control Interno, mediante el análisis de la documentación del proyecto (acuerdos, diseños, manuales, circulares, contratos, políticas, procedimientos, ciclo del negocio, entre otros) que permite al consultor en informática, ubicarse en la operación y necesidades del negocio, desarrollando recomendaciones a las definiciones del nuevo sistema o a la misma operación.

**Cuantitativa** Implica evaluar el funcionamiento del Control Interno definido en el sistema mediante la aplicación de matrices de prueba, poniendo en práctica los conocimientos adquiridos durante la etapa cualitativa y participando activamente en las juntas de trabajo que se deriven del desarrollo.

- Los informes de auditoria parciales o finales que son discutidos con los auditados, invariablemente promoverán el reforzamiento del Control Interno antes de llevar el sistema a producción, previendo riesgos innecesarios al cliente y/o institución.

  El seguimiento a los informes y comprobación de correcciones es una actividad que debe formar parte del plan de auditoria, dependiendo de los compromisos establecidos con el propietario del sistema o usuario aplicativo.

Factores de Riesgo Sistemas en Desarrollo.

| Fase | Factores de Riesgo | Puntos Mínimos de Control que debe cubrir cualquier desarrollo |
|---|---|---|
| **Análisis Preliminar**<br><br>1. Requerimiento / Necesidades de negocio.<br>2. Alcance del proyecto.<br>3. Situación actual.<br>4. Ciclo de negocio.<br>5. Ámbito legal.<br>6. Análisis costo / beneficio del proyecto. | • Justificación inadecuada del proyecto.<br>• Deficiencias en alcances y limites del desarrollo.<br>• Desapego a lineamientos oficiales.<br>• Desviación a tendencias tecnológicas en la institución.<br>• Desapego a lineamientos establecidos en el Manual de Prácticas Estándar Corporativas. | • Estudio de Factibilidad.<br>• Ciclo de Negocio.<br>• Ámbito legal.<br>• Contratos con proveedores. |

| Fase | Factores de Riesgo | Puntos Mínimos de Control que debe cubrir cualquier desarrollo |
|---|---|---|
| **Diseño Conceptual**<br><br>1. Acuerdo admvo.<br>2. Especificaciones del producto o servicio.<br>3. Diagrama estructural.<br>4. Alternativas de desarrollo.<br>5. Selección de proveedores y contratos.<br>6. Fases de desarrollo.<br>7. Plan de desarrollo. | • Deficiencias en la definición del proyecto.<br>• Definición inadecuada de responsabilidades de auditoría en informática.<br>• Insuficiencia de responsabilidades por área.<br>• Plan de desarrollo inadecuado.<br>• Impedimentos operativos para el desarrollo del proyecto. | • Acuerdo administrativo.<br>• Diseño de productos y servicios.<br>• Diagrama estructural de funciones y modelo de datos. |

| Fase | Factores de Riesgo | Puntos Mínimos de Control que debe cubrir cualquier desarrollo |
|---|---|---|
| **Diseño Funcional**<br><br>1. Diagrama estructural de funciones.<br>2. Diagrama de flujo de datos.<br>3. Diseño de pantallas inventario, lay-out, definición de grupos, uso, definición teclas de función, mensajes.<br>4. Diseño de reportes, inventario, lay-out, uso.<br>5. Detalle de impactos a la organización: personal, equipos.<br>6. Políticas y procedimientos operativos. | • Insuficiencia de validaciones a la entrada de datos, por parámetros inadecuados o inexistencia de referencias cruzadas.<br>• Carencia de cifras control en el procesamiento de información.<br>• Definición de transacciones de riesgo.<br>• Niveles de acceso no acorde a funciones y montos. | • Diseño Funcional.<br>• Plataforma de seguridad para control de acceso al sistema.<br>• Campos para uso de auditoría en los archivos maestros del sistema.<br>• Módulo de auditoría para seguimiento a usuarios o transacciones o ambas, incluso por combinación de transacciones.<br>• Perfiles de acceso específicos para auditoría. |

| | | |
|---|---|---|
| 7. Políticas y procedimientos del sistema.<br>8. Definición y descripción de proceso línea, batch e interfaces.<br>9. Descripción del esquema de seguridad.<br>10. Definición de Niveles de Servicio.<br>11 Cifras de control. | • Visualizar información sensitiva y claves de acceso al sistema.<br>• Ausencia de políticas y procedimientos para administración de la seguridad.<br>• Indefinición de reportes financieros o de tipo gerencial.<br>• Insuficiencia de información histórica para rastreo del origen de las transacciones.<br>• Inconsistencia en la longitud/definición de campos conforme a estándares. | |

| **Fase** | **Factores de Riesgo** | **Puntos Mínimos de Control que debe cubrir cualquier desarrollo** |
|---|---|---|
| **Diseño Técnico**<br><br>1. Definición de plataforma de comunicaciones y procesamiento de datos.<br>2. Inventario de los programas línea y batch.<br>3. Definición del diccionario de datos.<br>4. Especificaciones de rendimiento del sistema y recursos a utilizar.<br>5. Políticas y procedimientos de emergencia y contingencia. | • Desviaciones en la normalización de la base de datos.<br>• Truncamiento o rebasamiento de datos.<br>• Inconsistencias en los valores de las tablas de equivalencia. | • Diseño de base de datos.<br>• Diccionario de elementos.<br>• Campos para uso de auditoria en los archivos maestros del sistema.<br>• Módulo de auditoría para seguimiento de usuarios o transacciones o ambas, incluso por combinación de transacciones.<br>• Procedimientos para encriptación de datos sensitivos. |

| | | |
|---|---|---|
| 6. Especificaciones del esquema de seguridad.<br>7. Prioridades de proceso, definición del negocio.<br>8. Procedimientos de conversión.<br>9. Plan de Pruebas. | | |

| Fase | Factores de Riesgo | Puntos Mínimos de Control que debe cubrir cualquier desarrollo |
|---|---|---|
| **Desarrollo**<br><br>1. Crear ambiente.<br>2. Estandar programas y documentación técnica.<br>3. Procedimientos de respaldo / recuperación.<br>4. Manejar programas auxiliares (RACF, encriptación, etc.).<br>5. Manuales, políticas y procedimientos de usuario, de sistema, seguridad y verificación de procesos.<br>6. Capacitación en operaciones, negocio y sistemas.<br>7. Cambios al alcance del proyecto, priorización.<br>8. Plan de Pruebas. | • Entrega de programas sin ejecución de pruebas unitarias o modulares. | • Plan de capacitación.<br>• Archivos para auditoría (extracto de archivos maestros). |

| Fase | Factores de Riesgo | Puntos Mínimos de Control que debe cubrir cualquier desarrollo |
|---|---|---|
| **Pruebas**<br><br>1. Creación de ambiente.<br>2. Plan de ejecución.<br>3. Casos y tipos de prueba.<br>4. Bitácora de pruebas.<br>5. Criterios de aceptación.<br>6. Uso herramientas automatizadas.<br>7. Emergencia y contingencia.<br>8. Conversión.<br>9. Estrategia Piloto.<br>10. Autorización operaciones, negocio, sistemas. | • Inconsistencias en manejo de información aplicando matrices de pruebas (integración, regresión, volumen, seguridad, integridad, comunicaciones, etc.).<br>• Insuficiencia de información para control del sistema y contabilidad.<br>• Incumplimiento con requerimientos de usuario.<br>• Falta de control sobre transacciones de riesgo.<br>• Deficiencias en los procesos para mantenimiento a parámetros.<br>• Indefinición de políticas y procedimientos para el usuario, operación y sistema. | • Establecimiento de puntos de control conforme a la metodología de sistemas<br>• Proceso de pruebas.<br>• Elaboración y aplicación de matrices de prueba (funcionalidad, seguridad, emergencia y contingencia).<br>• Afinación del sistema y niveles de servicio.<br>• Documentación inherente al sistema y operación autorizada por la unidad de negocio, operaciones y sistemas. |

| Fase | Factores de Riesgo | Puntos Mínimos de Control que debe cubrir cualquier desarrollo |
|---|---|---|
| **Instalación**<br><br>1. Niveles de servicio negociados y autorizados. | • Impactos al servicio por condiciones no previstas en pruebas. | • Aprobación control de cambios.<br>• Plan de instalación y matriz de escalamiento. |

| | | |
|---|---|---|
| 2. Circulares.<br>3. Pilotos.<br>4. Definición puntos de control y Plan de *retorno.*<br>5. Acuerdo de liberación. | • Falta de difusión del material de capacitación.<br>• Instalación piloto/ *expansión no* controlada.<br>• Manejo de versiones inadecuado.<br>• Ausencia de plan de retorno. | • Niveles de servicio.<br>• Plan Piloto y de expansión.<br>• Difusión, capacitación y soporte.<br>• *Administración de la* seguridad. |

| Fase | Factores de Riesgo | Puntos Mínimos de Control que debe cubrir cualquier desarrollo |
|---|---|---|
| **Post-instalación**<br><br>1. Resumen de aspectos no cubiertos en diseño vs. Instalación.<br>2. Comportamiento del desempeño.<br>3. Impactos al servicio.<br>4. Control de cambios y *reportes problema.*<br>5. Definición desarrollo siguientes fases u optimizaciones. | • Incumplimiento de compromisos *contractuales.*<br>• Desviaciones en los niveles de servicio comprometidos. | • Bitácora de incidencia de problemas en periodo de *garantía.*<br>• Plan de auditoría a aspectos observados durante el desarrollo y para revisión de fases subsecuentes. |

Basándose en el *análisis* de "Factores de Riesgo", podemos *determinar* que los *puntos mínimos* de control son:

Puntos de Control Interno para Sistemas en Desarrollo

1. Requerimientos de usuario y/o necesidades impuestas por organismos oficiales, característicos del servicio o producto a automatizar, alcance y *factores críticos del proyecto.*

2. Análisis del ámbito legal, contable y fiscal que pudieran determinar condiciones de impacto al cliente o institución.

3. Definición de la base de datos que identifique el origen de las operaciones y diccionario de datos que indique validación de información contra archivos paramétricos institucionales o propios, incluyendo referencias cruzadas entre campos en la entrada y actualización.

4. Especificación de funciones, transacciones y procesos a habilitar, diagrama estructural del sistema, detalle de productos a generar, cifras de control en número de registros e importes en cada punto de procesamiento y envío/recepción de datos con otros sistemas por interface automatizada.

5. Información financiera y estadística consolidada a nivel Institución en número de registros e importes, que permitan comprobar los cálculos efectuados por el sistema, el arrastre de cifras y la conciliación contable.

6. Archivos históricos que permitan efectuar la reconstrucción de las operaciones y deslindar responsabilidades de usuario, aún cuando hayan existido depuraciones de datos.

7. Procedimientos automatizados que eviten duplicidades a la entrada de datos y validen la confiabilidad de los resultados del proceso.

8. Políticas y procedimientos de seguridad para administración de usuarios y acceso a datos, definiendo perfiles y facultades de usuario de acuerdo a funciones y puestos.

9. Plataforma de seguridad para control de acceso al sistema y bases de datos, que contemple bloqueo/desbloqueo de usuarios, encriptación/desencriptación de información sensitiva y procesos automatizados para el mantenimiento de usuarios en las diferentes plataformas de seguridad.

10. Plan de pruebas contemplando los diferentes tipos de proceso, reformateo de datos, todas las transacciones manuales y automatizadas propias y de interfaces, estableciendo criterios de aceptación y riesgos de su incumplimiento.

11. Procesos automatizados para respaldo y recuperación de la base de datos en caso de emergencia o contingencia, incorporando el espejeo de archivos maestros con el centro de cómputo fuera de sitio, así como al plan de contingencia institucional.

12. Documentación inherente al sistema y operación con políticas y procedimientos autorizados por la unidad de negocio/operaciones/sistemas, incluyendo niveles de servicio y capacitación a usuarios.

13. Informe de productos no instalados y compromisos para desarrollo de fases complementarias.

Responsabilidades de Auditoría en Informática

| Punto Mínimo de Control Interno | Responsabilidades |
|---|---|
| 1. Requerimiento de usuario / organismos oficiales. | • Comprobar que el proyecto justifica su desarrollo por obtención de beneficios a la Institución y muestra apego a sus directrices. |
| 2. Análisis del ámbito legal, contable y fiscal. | • Comprobar que el proyecto contempla regulaciones que no impiden su desarrollo o riesgos al cliente/institución. |
| 3. Definición de la base de datos y validaciones. | • Comprobar la consistencia de campos y criterios de validación |
| 4. Especificación de funciones, transacciones y procesos. | • Comprobar que las definiciones funcionales muestran consistencia en el procesamiento de datos. |
| 5. Información financiera y estadística. | • Comprobar que la información sea suficiente, confiable y consistente respecto a lo procesado por el sistema. |
| 6. Archivos históricos. | • Comprobar la definición de elementos para identificar origen de operaciones o reconstrucción de eventos. |
| 7. Procedimientos automatizados que validen el proceso. | • Comprobar habilitación de políticas y procedimientos para control del sistema y la operación. |
| 8. Administración de accesos al sistema. | • Comprobar que el módulo de seguridad permite controlar usuarios, facultades y accesos. |
| 9. Plataforma de seguridad, encriptación / desencriptación de información. | • Comprobar que el sistema encripta información sensitiva del cliente y servicio, así como que el módulo de seguridad impida y reporte intentos de violación. |
| 10. Proceso de pruebas. | • Comprobar la consistencia, confiabilidad e integridad del procesamiento de datos, elaborando y aplicando matrices de auditoría a todas las transacciones habilitadas en el sistema, revisando resultados y determinando condiciones de riesgo. |
| 11. Respaldo y recuperación de base de datos. | • Comprobar la definición de procesos para respaldo y recuperación de archivos maestros que permitan la continuidad del negocio. |

| | |
|---|---|
| 12. Documentación inherente al sistema y operación. | • Comprobar que las políticas y procedimientos correspondan a la funcionalidad del sistema, operación y marco normativo. |
| 13. Informe de productos no instalados. | • Comprobar que los requerimientos del negocio y operación han sido cubiertos conforme a expectativas del proyecto (presupuestado, pagado e instalado). |

Sistemas en Producción

La Auditoría en Informática a un sistema en producción se divide en dos etapas:

**Cualitativa** Comprende el conocimiento de procesos claves del negocio, la identificación y evaluación de riesgos y controles críticos, mediante el análisis de documentación que soporte al sistema y operación (diseños, manuales, circulares, políticas, procedimientos, administración de la seguridad y asignación de responsabilidades, entre otros) y que permita al consultor en informática calificar la estructura del control interno.

**Cuantitativa** Implica evaluar el funcionamiento y suficiencia del Control Interno definido en el sistema mediante la aplicación de matrices de prueba a transacciones de riesgo y muestreos de información de archivos maestros, determinando áreas de oportunidad que eviten impactos en el patrimonio del cliente y/o institución.

Puntos de Control Interno para Sistemas en Producción

1. Seguridad Lógica.

| Factores del Control Interno | Responsabilidades |
|---|---|
| a) Administración de seguridad. | • Comprobar la existencia, funcionalidad y suficiencia de procedimientos automatizados y/o manuales para control de usuarios, facultades y montos.<br>• Revisar que la información emitida por el sistema permita monitorear la actividad de los usuarios, sus perfiles y facultades definidas en las diferentes plataformas de seguridad. |
| b) Perfiles y atributos. | • Comprobar la correcta definición y asignación de niveles de acceso de acuerdo a funciones, puestos y facultades del usuario. |

| | |
|---|---|
| c) Manuales, políticas y procedimientos. | • Revisar la existencia, funcionalidad y suficiencia de políticas y procedimientos para administración de usuarios y acceso a datos. |
| d) Control de acceso a datos y programas. | • Comprobar la existencia y suficiencia de procedimientos automatizados que impidan accesos no autorizados.<br>• Verificar la funcionalidad del módulo para mantenimiento de usuarios en las diferentes interfaces.<br>• Verificar la suficiencia de información histórica que permita rastrear el origen de las transacciones. |
| e) Seguimiento a reportes violación y sanciones. | • Revisar la existencia y actualización de políticas que sancionen violaciones o intentos de violación.<br>• Comprobar la correcta aplicación de sanciones en apego a políticas definidas. |
| f) Apego a lineamientos para control de usuarios y facultades. | • Revisar que los procedimientos de alta, mantenimiento y baja de claves de usuario se efectúen en apego a los procedimientos definidos y bajo el esquema de función de puesto y facultades.<br>• Verificar la existencia de cartas responsivas personalizadas. |

2. Seguridad Física.

| Factores del Control Interno | Responsabilidades |
|---|---|
| a) Manuales, políticas y procedimientos para acceso al equipo. | • Revisar la existencia de políticas y procedimientos para control de acceso a equipo de cómputo en áreas restringidas.<br>• Comprobar que existan dispositivos físicos que impidan el acceso a personal no autorizado y que sean suficientes para detectar la actividad en sitio. |
| b) Ubicación y localización del equipo. | • Comprobar que el equipo de cómputo se encuentre instalado de acuerdo a especificaciones definidas por el proveedor (suministro eléctrico, condiciones ambientales, sistema de enfriamiento, entre otros).<br>• Verificar la existencia de bitácoras que registren los mantenimientos preventivos efectuados y la programación de su próxima inspección. |
| c) Pólizas de seguro | • Revisar que los componentes críticos cuenten con pólizas de seguro de cobertura amplia y se encuentren vigentes. |

3. Gestión.

| Factores del Control Interno | Responsabilidades |
|---|---|
| a) Contratos y pagos realizados en apego a estándares | • Revisar que las contrataciones de servicios y adquisiciones de bienes informáticos y sus pagos, se lleven a cabo en apego a Prácticas Estándar Corporativas vigentes. |
| b) Justificación de adquisición de bienes informáticos. | • Comprobar que el estudio de factibilidad se haya elaborado con apego a necesidades del negocio. |
| c) Alternativas de solución. | • Comprobar que la solución definida haya sido la mejor, habiendo concursado diversas alternativas (reutilizar o adaptar un sistema, comprar o desarrollar uno nuevo) y criterios obligatorios para desarrollos internos o contratación de proveedores. |
| d) Análisis Costo/ Beneficio. | • Comprobar que la justificación cuantitativa considere tiempo de recuperación de la inversión, de acuerdo con los costos presupuestados frente a los beneficios esperados por cada alternativa de solución identificada. |
| e) Cumplimiento de productos y servicios | • Comprobar que los productos y servicios contratados se encuentren instalados y cumplan con la calidad y eficiencia requerida por los estándares institucionales, cubriendo íntegramente las necesidades del negocio.<br>• Existencia de cartas de aceptación autorizadas por la unidad de negocio y sistemas que amparen los pagos efectuados.<br>• Comprobar que los pagos efectuados no rebasen el presupuesto destinado al proyecto. |

4. Uso y aprovechamiento de la plataforma.

| Factores del Control Interno | Responsabilidades |
|---|---|
| a) Políticas, parámetros, criterios de validación y actualización. | • Verificar que los parámetros y criterios de validación y actualización se encuentren definidos en apego a estándares institucionales.<br>• Comprobar que el sistema procese información validando los datos contra parámetros y referencias cruzadas. |

| | |
|---|---|
| b) Transacciones y condiciones de riesgo. | • Comprobar que el procesamiento de datos se ejecute conforme a las especificaciones, políticas y parámetros del sistema. |
| c) Cálculo. | • Comprobar que los datos calculados correspondan a las políticas y parámetros definidos en el sistema. |
| d) Interfaces. | • Comprobar la existencia y funcionalidad de procedimientos automatizados que controlen el envío y recepción de datos con otros sistemas, en número de registros e importe tanto por aceptados como rechazados. |
| e) Reportes de Control y Financieros. | • Comprobar existencia y funcionalidad de procedimientos automatizados que impidan el procesamiento erróneo de datos, así como suficiencia, consistencia y calidad de información generada para control del sistema, sus interfaces y excepciones. |
| f) Información Histórica y Medios de Consulta. | • Comprobar que la información generada se encuentre disponible para consulta y permita identificar el origen de las operaciones. |

5. Uso y aprovechamiento de recursos de cómputo.

| Factores del Control Interno | Responsabilidades |
|---|---|
| a) Discos, cintas, programas y procedimientos. | • Evaluar el correcto aprovechamiento de recursos de hardware y software detectando subutlización de espacio, obsolescencia en componentes instalados, programas no utilizados, saturación de usuarios, entre otros. |

6. Emergencia / Contingencia.

| Factores del Control Interno | Responsabilidades |
|---|---|
| a) Manuales, políticas, procedimientos para recuperación. | • Comprobar la existencia, suficiencia y actualización de políticas y procedimientos para respaldo y recuperación de sistemas en sitio y fuera de sitio.<br>• Verificar que se encuentre incluido en el plan de recuperación institucional, definiendo la prioridad para el negocio.<br>• Comprobar la existencia de estrategia de pruebas que contemple su ejecución con cierta periodicidad y en diferentes escenarios. |

| | |
|---|---|
| b) Planes de contingencia o desastre. | • Comprobar la localización de un centro de cómputo alterno en caso de emergencia o contingencia, en un lugar físico distinto al centro de cómputo principal.<br>• Comprobar el cumplimiento de la estrategia de pruebas y evaluación de resultados obtenidos registrados en bitácoras que muestren la aplicación de medidas correctivas en caso de haber existido problemas en la recuperación parcial o total del sistema. |
| c) Tiempos de proceso y niveles de servicio. | • Comprobar la existencia de niveles de servicio comprometidos con el negocio (disponibilidad, tiempo de respuesta, calidad de la información, estabilidad en sus diferentes plataformas) y su permanente actualización.<br>• Verificar que las mediciones efectuadas correspondan a lo estipulado en el acuerdo de niveles de servicio, llevando a cabo las medidas para su cumplimiento. |

7. Control de Cambios y Problemas.

| Factores del Control Interno | Responsabilidades |
|---|---|
| a) Antecedentes y alternativas de solución. | • Comprobar la existencia de análisis de impactos a la continuidad de negocio que justifique las necesidades del cambio, ya sea por mejora al servicio o cumplimiento de requerimiento legal.<br>• Verificar su correcta categorización, basándose en el sistema afectado y en las necesidades de su instalación.<br>• Comprobar que se haya identificado el origen del problema y determinado estrategias para su corrección dentro del margen establecido para minimizar los impactos al cliente y/o servicio.<br>• Evaluar la incidencia, registro y atención de problemas a sistemas vitales. |
| b) Proceso de pruebas. | • Comprobar que los programas a instalar hayan cubierto el Proceso de Pruebas definido en la Metodología de Sistemas y los criterios de aceptación definidos por la unidad de negocio.<br>• Verificar que se hayan generado respaldo de archivos críticos, emitiendo cifras de control antes y después de la corrección. |

| | |
|---|---|
| c) Planes de instalación y retorno. | • Verificar que la estrategia de instalación contemple pruebas, cifras de control y criterios de aceptación que en su caso, determinen el retorno a programas anteriores.<br>• Comprobar la elaboración de pruebas en producción como punto de control antes de la apertura del servicio. |
| d) Autorización de usuarios. | • Comprobar que la instalación cuente con la autorización de la unidad de negocio, áreas operativas y otras áreas involucradas, habiendo cubierto el Proceso de Pruebas y los criterios de aceptación definidos. |

# PROPUESTA DE ASPECTOS A CONSIDERAR PARA AUDITAR EL AMBIENTE DE REDES DE ÁREA LOCAL

## 5.1 CONTROLES A AUDITAR.

Introducción

El objetivo de esta propuesta es ejecutar una auditoría al ambiente de redes de área local identificando y evaluando el apego a normas, políticas y procedimientos definidos para la administración y operación, así como la detección de riesgos, promoviendo el desarrollo de controles y medidas de seguridad que eviten impactos en el patrimonio de la institución.

Una vez que la red de área local ha sido puesta en marcha, es importante monitorear su operación para asegurar un proceso continúo y correcto. Esta auditoría, por lo tanto, será direccionada no solamente a la verificación de controles, sino también a la revisión de procedimientos adecuados para mantener un ambiente de producción estable, con la finalidad de cumplir con los requerimientos y compromisos contraídos con los usuarios y la institución.

Dado que cada institución tiene su propia estructura organizacional, en esta guía las áreas que se consideran dentro del proceso de administración de la red son:

- Soporte técnico.
- Operación, cuyas funciones pueden estar en diferentes áreas y que de forma general son:
  - Operación del equipo de cómputo.
  - Control de la red de comunicaciones.
  - Preparación de datos.
  - Administración de archivos.
  - Administración de documentación.
  - Monitoreo de performance.
- Niveles de servicio.

Objetivos Generales

- Asegurarse que existan los controles necesarios para evitar daños en el equipo, operación, directorios, archivos, etc.

- Asegurarse que existe una segregación de funciones y rotación de éstas, verificando que no solamente una persona ejecute una función desde el inicio hasta el fin o sea responsable de checar la precisión de su propio trabajo. Asimismo revisar que exista personal capacitado para actuar en caso de emergencia.
- Respecto a la rotación de funciones, verificar que ésta se realice con el fin de capacitar a cada operador para las tareas de operación y evitar que sólo ciertas personas manejen una función indefinidamente.
- Revisar que se realice el mantenimiento preventivo y correctivo a los equipos.
- Verificar la existencia y actualización de manuales para operación de equipos.
- Revisar la periodicidad de los backups para el sistema operativo, programas aplicativos, archivos maestros, archivos de transacciones, etc.
- Evaluar la continuidad de la operación en caso de problemas mayores, tales como pérdida del área donde se encuentra el equipo de cómputo y conmuto por terremotos, incendios, etc.
- Asegurarse que existan procedimientos para monitorear el rendimiento del equipo, detectando posibles degradaciones para que las acciones correctivas puedan ser tomadas a tiempo.
- Verificar la eficiencia de procesos administrativos, considerando cambios a la infraestructura y/o sistemas, así como los reportes de problemas y la atención y solución a estos para mantener la continuidad de la operación.

Principales Riesgos

- Organización y personal.
- Administración de la red.
- Inventario de equipo y licencias de software.
- Seguridad física.
- Seguridad lógica.
- Respaldo/Recuperación.
- Cambios a componentes.
- Reporte y seguimiento de problemas.
- Uso y aprovechamiento de la plataforma.

Los riesgos anteriores no se encuentran clasificados en orden de importancia, sin embargo, cualquiera puede afectar la disponibilidad de las aplicaciones.

Es necesario que antes de efectuar la auditoría a una red de área local, se haga una evaluación de los riesgos, ya que cubrirlos todos implica que entre más grande y compleja sea la infraestructura de red, se requerirá invertir mayor tiempo.

### 5.1.1 Organización y personal.

Los administradores deben implementar políticas y procedimientos para la segregación y rotación de funciones. El tamaño de la red influenciará los tipos de políticas implementadas para la división de funciones.

En toda las áreas de una empresa que cuente con una red de computadoras, la segregación de funciones es el mejor control contra empleados deshonestos o que intencionalmente desean causar daño al equipo, documentación o archivos.

#### 5.1.1.1 Objetivos.

- Determinar si es adecuada la estructura organizacional de la institución, de acuerdo a la segregación de funciones y a las aplicaciones que se procesan en el servidor de la red.
- Determinar si el personal conoce las funciones y responsabilidades de su puesto y reconoce la importancia del mismo.
- Verificar que el personal se encuentra capacitado para el desarrollo de sus funciones y que exista un plan de capacitación para mantenerlos actualizados.

#### 5.1.1.2 Riesgos específicos.

- Personal no capacitado para el desarrollo de sus funciones.
- Segregación de funciones inadecuada.
- Funciones y responsabilidades mal definidas.

#### 5.1.1.3 Evidencia disponible.

- Organigramas y descripciones de puestos.
- Plan de capacitación.
- Políticas, procedimientos y estándares que normen el funcionamiento y actividades en la red.

#### 5.1.1.4 Procedimiento de Auditoría.

1. Verificar que las políticas sean conocidas por el personal, que se actualicen periódicamente, que se supervise su aplicabilidad y que se de seguimiento a su cumplimiento.

2. Revisar que el organigrama este autorizado por el área de recursos humanos.

3. Determinar si la organización actual coincide con la oficial, en caso de encontrar desviaciones o diferencias, evaluar si son o no razonables.

4. Verificar que no exista personal sindicalizado en puestos clave.

5. Identificar si existen descripciones de puestos, si están autorizadas por el área de recursos humanos y si el personal conoce las funciones de su puesto.

6. Entrevistar a una muestra del personal para constatar sus funciones operativas y el grado de comprensión de objetivos y descripción de puesto, cruzando dicha información con la descrita en la descripción del puesto.

7. Determinar si están correctamente delimitadas las funciones y responsabilidades entre el personal administrador de la red y áreas usuarias.

8. Revisar si existen controles adecuados para llevar un seguimiento de vacaciones y tiempo extra.

9. Verificar la razonabilidad del tiempo extra y el procedimiento para su autorización, revisando el pago por este concepto, comparado con meses anteriores y determinando las causas de variación.

10. Identificar si se conservan expedientes para registrar eventos como faltas injustificadas, faltas al reglamento, indisciplinas y otras irregularidades relacionadas con la actuación del personal.

11. Revisar que los planes de capacitación y la rotación de funciones se encuentren calendarizados.

12. Determinar si el personal clave como soporte técnico y operación cuenta con la capacidad y habilidad suficiente para desarrollar sus funciones.

13. En caso de despidos de personal, analizar el procedimiento verificando que se documenten las causas más comunes y la cancelación de claves de acceso en forma oportuna.

### 5.1.2 Administración de la red (adquisición / instalación).

#### 5.1.2.1 Objetivos.

Adquisición de la red

El principal objetivo de este punto es determinar si la compra de software y/o hardware fue la adecuada y si las políticas y procedimientos actuales son

suficientes para reducir los riesgos legales involucrados, especialmente los relacionados con el uso de software.

Asimismo, deberán existir claramente políticas, procedimientos y estándares para ejercer el presupuesto asignado a cómputo y tener justificados los montos que requieren ser autorizados por los altos niveles directivos.

Instalación de la red

Bajo esta área de control, se establecen los criterios para asegurarse que se cuenta con las instalaciones adecuadas para el uso y manejo de las computadoras, tanto físicas primeramente, como lógicas (cableado, lugar, sistemas, personal, etc.) y en general de todo lo que cae en torno a la LAN, dentro de la seguridad requerida.

### 5.1.2.2 Riesgos específicos.

Adquisición de la red

- Metodología de adquisición de equipos y/o software pobre o deficiente.
- Adquisiciones de hardware y software:
  - no autorizados por una mala definición de políticas y procedimientos de adquisición de equipos,
  - no útiles para el negocio por una planeación mal definida,
  - inadecuada por convocatoria de proveedores de equipos no reconocidos profesionalmente en el mercado,
  - con protocolos de comunicación no compatibles con otros sistemas instalados previamente,
  - con incompatibilidad de conexión física con otros equipos requeridos para cumplir con alguna función importante para el negocio.
- Virus informáticos que afectan al software de la red debido a adquisiciones de dudosa procedencia.
- Gastos ejercidos sin soporte o autorización.
- Gastos adicionales de adquisición no presupuestados, debido a crecimientos no planeados de la red.
- Graves impactos financieros por un control inadecuado de los gastos realizados.
- Bajos niveles de servicio por falta de capacitación en el uso y administración de la red.

Instalación de la red

- Pérdida total o parcial de información vital, debida a la falta de procedimientos de seguridad lógica en la red.
- Destrucción y/o daños accidentales de las instalaciones por una mala distribución de los componentes de la red.
- Pérdida o destrucción de información o equipos al no contar con sistemas de seguridad física para ingreso al centro de cómputo.
- Destrucción total o parcial de las instalaciones al no considerar dispositivos contra incendios o inundaciones.
- Pérdida de información vital, graves impactos financieros para la organización por falta de supervisión al instalar los componentes de la red (cableado, software de comunicaciones, flujo de señales, transmisión satelital, etc.).
- Suspensión de servicios de la red al no contar con planes de emergencia bien definidos para recuperar el servicio.
- Retraso en el restablecimiento del servicio al no contar con un adecuado servicio de mantenimiento por parte de los proveedores.
- Retraso en la instalación de la red, debido a un reanálisis de parámetros técnicos mal dimensionados.

### 5.1.2.3 Evidencia disponible.

Adquisición de la red

- Metodología de adquisición de equipos y/o software.
- Normatividad vigente para convocar proveedores de equipos y software.
- Políticas y procedimientos elaborados para adquirir equipos y software.
- Plan de adquisición de la red, el cual como mínimo deberá contener:

  - Antecedentes sobre la necesidad de adquisición de red.
  - Presupuesto destinado para adquisiciones.
  - Convocatorias y ofertas de proveedores.
  - Resultado del concurso de proveedores.

- Gastos generados por la adquisición.
- Contratos celebrados con proveedores para efectos de revisión de servicios de mantenimiento a la red.
- Adquisición de la red y de sus componentes por parte del personal autorizado.
- Conocimiento y aplicación de las políticas y procedimientos sobre el correcto uso del software por parte del administrador de la red y los usuarios de la misma.

- Pruebas de laboratorio y de servicio.
- Programas de capacitación y actualización elaborados para el administrador de la red y los usuarios de la misma.

Instalación de la red

- Número de estaciones de trabajo requeridas y futuras (crecimiento).
- Porcentaje de utilización de aplicaciones.
- Necesidades de almacenamiento de información e impresión.
- Necesidades de comunicación remota con todas sus implicaciones (protocolos adecuados).
- Plano del centro de cómputo y localización del equipo.
- Procedimientos de emergencia.
- Políticas y procedimientos de seguridad lógica y física.
- Costos de instalación.

### 5.1.2.4 Procedimiento de Auditoría.

Adquisición de la red

- Determinar si las adquisiciones se ejercen de acuerdo al presupuesto asignado.
- Comparar lo ejercido contra lo presupuestado, evaluando apego a presupuesto y distribución por área o departamento.
- Verificar que existan controles para dar seguimiento al gasto ejercido y a las desviaciones reflejadas en el control presupuestal.
- Determinar si los controles existentes para el pago de facturas están diseñados para evitar pagos improcedentes, apegándose a las políticas establecidas.
- Investigar si existen criterios definidos para la selección de proveedores.
- Cerciorarse que las propuestas de los proveedores cuenten con toda la documentación necesaria para tomar una decisión.
- Verificar que los pedidos de hardware y software estén por escrito y apegados a las políticas y procedimientos para tal fin, además de estar aprobados por personal autorizado.
- Comprobar que los contratos con proveedores contemplen el soporte y mantenimiento periódico a los equipos adquiridos.
- Identificar que en los contratos con proveedores existan penalizaciones en caso de incumplimiento.
- Identificar la necesidad de compartir información, recursos, programas, bases de datos, etc.
- Determinar los canales de comunicación requeridos entre los diferentes departamentos a los que brindará servicio la red.

- Identificar problemas físicos en el establecimiento de los canales de comunicación.
- Revisar y, de ser posible, participar en las pruebas de laboratorio y de servicio.
- Verificar que se cuente con programas periódicos de capacitación para el administrador de la red y los usuarios de la misma.

Instalación de la red

- Verificar que se tenga un control vigente para identificar físicamente los equipos comprados y el departamento o área donde están localizados.
- Revisar que la asignación de responsables para la custodia y cuidado del equipo de cómputo y software, se encuentre actualizada y apegada a la normatividad.
- Verificar que se lleve a cabo un seguimiento periódico a los movimientos contables que se efectúan al centro de cómputo, con el fin de identificar partidas que no le corresponden o que presenten irregularidades.
- Identificar la posible destrucción y/o daños accidentales de las instalaciones.
- Asegurarse que se cuente con instalaciones adecuadas para los equipos, mismas que garanticen el buen funcionamiento y servicio de la red.
- Verificar que los componentes de la red estén instalados de acuerdo con las necesidades definidas.
- Revisar si existen grupos de soporte técnico y mantenimiento de la red y, de ser así, evaluar las funciones y responsabilidades de los mismos.
- Verificar que sea implantado un proceso de mejora continua para que los niveles de servicio de la red sean cada vez más satisfactorios.
- Identificar y evaluar los planes de expansión de la red.

### 5.1.3 Inventario de equipo y licencias de software.

Deberán existir claramente definidas políticas y procedimientos para el control de software y equipo de cómputo.

#### 5.1.3.1 Objetivos.

- Determinar que se tenga un control adecuado y actualizado sobre la existencia y custodia del equipo, software y suministros para el sistema.
- Verificar que los inventarios asociados al centro de cómputo sean razonables y que se apeguen a políticas y procedimientos definidos.

#### 5.1.3.2 Riesgos específicos.

- Inventarios inexistentes o desactualizados.

- Control inadecuado del software y equipo de cómputo.
- Control inadecuado de suministros de cómputo (papel, cintas, otros).

#### 5.1.3.3 Evidencia disponible.

- Inventario de mobiliario, equipo de cómputo y software en el centro de cómputo.
- Asignación de responsables de mobiliario, equipo y software.
- Políticas para adquisición de mobiliario, equipo de cómputo y software.

#### 5.1.3.4 Procedimiento de Auditoría.

1. Políticas para asegurar que el software cubra los siguientes puntos:

   - Adquisición o instalación de software.
   - Cuantificación del software (original y copia).
   - Registro del software instalado, dado de baja o en proceso de adquisición.
   - Descripción del software (por original).
   - Software por legalizar.
   - Autorización de su uso.
   - Uso del software (tipo de uso, responsables de uso).
   - Reemplazo del software actual por otro nuevo.
   - Análisis costo/beneficio del software adquirido.
   - Autorización por medio de la justificación de reemplazo.
   - Implicaciones de control en la implantación y uso del software nuevo.
   - Verificar que los pedidos de software estén por escrito y apegados a las políticas y procedimientos definidos para tal fin.

2. El inventario de software comprado debe considerar:

   - Fecha de compra.
   - Nombre del fabricante y del producto.
   - Identificar si fue adquirido con un acuerdo de licencia o de única vez.
   - Costo, versión y número de serie.
   - Localización y número de copias o productos instalados por máquina.

3. El inventario de hardware debe incluir:

   - Nombre del fabricante y modelo.
   - Número de serie.
   - Costo.
   - Fecha de compra.

- Localización actual.
- Responsable o usuario.
- Políticas y procedimientos relativos al control y protección de hardware.

4. Verificar que se tenga vigente un control para identificar físicamente los equipos comprados o arrendados.

5. Distribución del hardware (ubicación física).

6. Cerciorarse que los equipos comprados o arrendados estén conciliados con el inventario de activo fijo de la institución.

7. Cuantificación del hardware.

8. Actualización del hardware.

9. Con respecto a la adquisición o renta de bienes informáticos:

   - Identificar y evaluar procedimientos para obtención de suministros de sistemas, determinando si se tiene un adecuado control del inventario.
   - Investigar si existen criterios definidos para la selección de proveedores.
   - Verificar que los pedidos de hardware estén por escrito y apegados a las políticas y procedimientos definidos para tal fin.
   - Identificar en los contratos que existan cláusulas de penalización en caso de incumplimiento por parte de los proveedores.
   - Aprobación formal de la adquisición del hardware.
   - Contrato legal de la compra de hardware que proteja a la institución.

### 5.1.4 Seguridad física.

Para tener una operación ininterrumpida hay que tomar acciones para prevenir, detectar, minimizar y recuperar pérdidas por daño o uso no autorizado de equipo, software o datos.

Las medidas de protección contra daños accidentales, fortuitos o intencionales deben ser incluidas en las políticas y procedimientos de seguridad.

#### 5.1.4.1 Objetivos.

- Verificar que los controles implantados sean los adecuados para salvaguardar los bienes y evitar fugas de equipos y materiales.
- Verificar que se cumplan los planes de mantenimiento a equipos contra cualquier siniestro.

- Determinar si el centro de cómputo cuenta con las facilidades necesarias para la seguridad y operación del equipo, por ejemplo: detectores de humo, equipo de enfriamiento, señalizaciones, etc.
- Revisar que existan procedimientos adecuados para restringir el acceso al centro de cómputo a personas ajenas a éste.
- Verificar que existan y se cumplan las condiciones especificadas en los contratos de seguros para que éstos sean validos.

### 5.1.4.2 Riesgos específicos.

- Accesos al centro de cómputo sin control.
- Condiciones físicas inadecuadas para la operación del centro de cómputo.
- Equipo insuficiente o inadecuado en casos de daño físico.

### 5.1.4.3 Evidencia disponible.

- Políticas y procedimientos de seguridad del centro de cómputo.
- Diagramas del centro de cómputo.
- Diagrama unifilar (diseño de instalaciones eléctricas).
- Contratos de pólizas de seguros.
- Facturas pagadas por mantenimiento.
- Bitácoras de Entrada/Salida del centro de cómputo.
- Bitácoras de mantenimiento a extinguidores, tableros, detectores, etc.

### 5.1.4.4 Procedimiento de Auditoría.

1. Obtener el plano actualizado de las instalaciones del centro de cómputo y verificar si cumple con la distribución descrita y con las especificaciones de instalación en cuanto a equipos de cómputo, alarmas, equipos de seguridad, piso y plafón falso, luces de emergencia, etc.

2. Verificar que la ubicación física del equipo de cómputo en el edificio sea la más adecuada, pensando en diversos desastres o contingencias que se puedan presentarse (manifestaciones o huelgas, inundaciones, incendios, otros).

3. Revisión de protección contra fuego, verificando:

   - Ubicación de alarmas contra incendio.
   - Existencia de extinguidores manuales y automáticos en puntos estratégicos, conteniendo el material apropiado (halón, dióxido de carbono, agua, otros).
   - Que los extinguidores y salidas de emergencia estén claramente señalizadas y libres de obstáculos y que las salidas de emergencia cuenten con indicaciones y dispositivos de apertura inmediata.

- Que el personal haya recibido pláticas o cursos de capacitación en caso de siniestros.
- Las gráficas de sensibilidad en cada uno de los detectores y determinar si se vigilan periódicamente las condiciones de funcionamiento.
- Que la alarma contra incendios tenga comunicación a una estación de bomberos.

4. Revisión de protección contra daños por agua, verificando:

- Que exista un adecuado sistema de drenaje y que no crucen tuberías de agua o drenaje el área del centro de cómputo.
- Que exista un sistema de desagüe.
- Que existan alarmas o dispositivos de detección de agua instalados en puntos estratégicos.

5. Revisión de entradas no autorizadas, verificando:

- Que el procedimiento para el control de entrada/salida del personal o visitantes incluya registro y comprobación de identidad por gafetes.
- Si se cuenta con controles para revisar la entrada/salida de materiales, paquetes, maletines, cajas, etc.
- Existencia de un directorio de personal facultado para autorizar el ingreso a personas ajenas al centro de cómputo, identificando nombre, área a la que pertenece, puesto y extensión telefónica.
- Accesos al centro de cómputo en días y horas inhábiles.
- Los lineamientos y controles existentes para efectuar servicios de limpieza y mantenimiento a los equipos.

6. Revisión de suministros, verificando:

- Existencia, localización, mantenimiento y funcionamiento de medidores de humedad, sistemas no-break, termómetros, detectores de humo y rociadores.
- Las especificaciones operativas y ambientales de cada uno de los equipos de cómputo instalados, evaluando su cumplimiento.
- El procedimiento en caso de presentarse fallas en el acondicionamiento ambiental.
- La bitácora de fallas de unidades de acondicionamiento ambiental y de todos los equipos de detección y control instalados. Las bitácoras de falla al menos deben contener:

  - Fecha y persona que reporta la falla.
  - Tipo de falla.
    Fecha y hora en que se presentan a repararla.

Detalle de la reparación efectuada.
Fecha y hora de finalización de reparación.
Nombre y firma de la persona que efectúo la reparación.
Fecha y hora en que se realizaron los mantenimientos preventivos.
Nombre y firma del responsable del mantenimiento preventivo.
Nombre y firma del responsable que da por cumplido el mantenimiento preventivo.

- Que el suministro eléctrico hacia el centro de cómputo sea independiente y regulado.
- La identificación del cableado eléctrico y la cama de soporte desde la cometida principal hasta el centro de cómputo.
- El monitoreo del comportamiento del suministro eléctrico.
- El diagrama unifilar de la instalación eléctrica en el centro de cómputo, en el cual se puede localizar el suministro alterno.
- El tipo y polarización de los contactos eléctricos.
- La configuración eléctrica y capacidad del equipo UPS y planta de emergencia, su funcionamiento y tiempo de respuesta.
- El ambiente en que opera el UPS (ventilación, ubicación, protección, limpieza).
- El plan de contingencias de los equipos UPS, identificando el plan de respaldo en caso de fallas de equipos y plan de recuperación.
- La ubicación, trayectoria, estado y tipo de canaletas eléctricas.
- La periodicidad y mantenimiento de la instalación eléctrica, revisando los planes de mantenimiento preventivo/correctivo para los equipos del sistema de energía tales como: UPS, tierras físicas, pararrayos, subestaciones y centros de carga. Estos planes deben contener al menos:

  - Fecha y lugar de mantenimiento.
  - Periodicidad.
  - Duración.
  - Empresa que presta el servicio.

- Los contratos de mantenimiento, identificando:

  - Duración de contrato y equipo que ampara.
  - Cláusulas especiales.
  - Si el contrato es total o parcial.
  - Procedimiento de mantenimiento.
  - Número de mantenimientos amparados por el contrato.

7. El procedimiento para dar mantenimiento a la instalación.

8. Los controles existentes en las áreas de almacenamiento magnético.

9. Que el cableado tanto de equipo como de telecomunicaciones se encuentre en orden, abajo del piso falso y perfectamente identificado y etiquetado.

10. La existencia de otras áreas operativas dentro del centro de cómputo y evaluando el riesgo/impacto que pudiera surgir por su estancia en tal lugar.

11. La existencia de pólizas de seguros vigentes que cubran la pérdida total o parcial de los activos informáticos con que cuenta la institución (hardware, software, etc.).

12. El procedimiento para obtener la papelería.

### 5.1.5 Seguridad lógica.

El software y los datos son valiosos activos por lo que daños considerables e inclusive pérdidas financieras pueden presentarse si éstos se pierden, son robados o modificados sin control. Implementando y forzando controles de seguridad en la información, se evita cualquier revelación accidental o intencional a personas no autorizadas a modificarla o destruirla.

#### 5.1.5.1 Objetivos.

- Asegurarse que los perfiles de seguridad definidos para el personal encargado de administrar la red sean congruentes con las funciones del puesto.
- Verificar que los perfiles de usuario estén definidos de acuerdo a sus funciones.
- Revisar que programadores y analistas de sistemas no tengan la posibilidad de pasar por alto los controles de seguridad implementados en los servidores de red.
- Verificar que los archivos vitales se encuentren protegidos.
- Evaluar el control de acceso a los recursos de la red y dispositivos magnéticos.
- Evaluar el apego a políticas y procedimientos de seguridad definidos.
- Verificar que los datos sean auditables para una rápida detección de pérdida o manipulación accidental o intencional.

#### 5.1.5.2 Riesgos específicos.

- Administración deficiente de usuarios, grupos, directorios y archivos.
- Perfiles de seguridad no acordes a funciones realizadas.

- Otorgamientos descontrolados de accesos a información sensitiva.
- Información sensitiva no encriptada.
- Inexistencia de software detector y eliminador de virus.

#### 5.1.5.3 Evidencia disponible.

- Políticas y procedimientos de seguridad para otorgar acceso a la información.
- Logs del sistema.
- Usuarios registrados en los servidores.
- Software de seguridad.
- Funciones y responsabilidades del personal encargado de la administración de la red.
- Perfiles estándar definidos.

#### 5.1.5.4 Procedimiento de Auditoria.

1. Evaluar la existencia de políticas y procedimientos formalizados y completos para otorgar claves de acceso a la información.

2. Cerciorarse que dentro de los procedimientos exista carta responsiva firmada por el usuario, en la que lo comprometa a responder por el uso que se le de a la clave que tenga asignada.

3. Determinar dentro de las políticas el nivel requerido para dar de alta usuarios para uso de recursos informáticos de la institución. Validar el nivel de cumplimiento y si es correcto el nivel de autorización conforme a la confidencialidad de la información.

4. Verificar que el personal conozca las políticas respecto a la seguridad de la información y las sanciones en caso de falta a éstas.

5. Identificar si existe un criterio de unicidad para la asignación de claves de usuario y, si son reasignados, evaluar el impacto.

6. Evaluar si la administración se realiza a través de la definición de grupos que contengan a los usuarios que tienen las mismas funciones y un mismo perfil de operación.

7. Verificar que se cuente con el soporte requerido de documentación en torno al otorgamiento de acceso a los recursos informáticos.

8. Determinar si se cuenta con los elementos que permitan relacionar las claves de acceso del personal, con el perfil de facultades y restricciones de acceso a la información.

9. Checar que las claves de acceso se encuentren personalizadas.

10. Verificar que se requiera cambio periódico de password, que no se permitan espacios en blanco y que se valide la longitud mínima y máxima del password de acuerdo con las políticas de seguridad definidas.

11. Verificar que se bloquee la clave de acceso después de varios intentos de acceso fallidos en apego a políticas establecidas

12. Monitorear la actividad del personal que administra la red evaluando su efectividad.

13. Evaluar que sólo personal autorizado cuente con el perfil de administrador para crear, modificar, borrar usuarios y grupos de usuarios, administración de políticas de seguridad, impresoras y permisos de acceso a recursos.

14. Verificar permisos a grupos creados por default por parte del sistema operativo.

15. Comprobar la existencia de procedimientos de ejecución periódica para revocar aquellas claves de usuario que en un período determinado no hayan sido utilizadas y que se efectúe un seguimiento para su cancelación definitiva en caso de no proceder su permanencia.

16. Revisar si los recursos y la información son protegidos en forma genérica y/o específica. Identificar y evaluar los criterios utilizados.

17. Verificar que el personal de desarrollo no tenga acceso a directorios y archivos de producción.

18. Verificar los accesos de los archivos y directorios sensitivos que se hacen fuera de producción.

19. Evaluar el control de altas, bajas y cambios de las claves de acceso, que la asignación de perfiles este centralizado en un administrador y que este verifique el uso adecuado de los elementos de seguridad.

20. Verificar que las claves de acceso dadas de alta no pertenezcan a personal que ya no labora en la institución o que haya cambiado de área.

21. Verificar que los operadores no tengan acceso a programas fuente y que el acceso a otra documentación no requerida para el proceso de aplicaciones

esté restringida con lo que se evitan modificaciones sin control por operadores con conocimiento de programación.

22. Verificar la existencia y habilitación de controles que permitan monitorear la seguridad a través de:

- Software de monitoreo de estaciones de trabajo.
- Utilerías para estadísticas de errores, accesos no permitidos, etc.
- Utilerías para auditar el tiempo de uso de recursos de la red.
- Log de seguridad propio del sistema operativo de red.

23. Verificar si se autentifican los usuarios de la red.

24. Verificar la existencia de controles para el uso de módems.

25. Comprobar la existencia de procedimientos de actualización de software para detectar virus en la red.

### 5.1.6 Respaldo / Recuperación.

La importancia de efectuar periódicamente los respaldos, estriba en el riesgo de que siempre se está expuesto a desastres de tipo natural: inundaciones, terremotos, incendios, etc.; los cuales podrían en determinado momento acabar por completo con el centro de cómputo y por tanto, si no se cuenta con los respaldos correspondientes, con la continuidad de operación.

Simplemente hay que considerar el hecho de no tener respaldo de información y que el servidor de archivos de una LAN sufra un daño en la fuente de poder y que las cabezas del o de los discos duros se aterricen, ocasionando con esto la destrucción total de los discos y por consecuencia, de la información existente en ellos.

No solamente las situaciones referidas anteriormente podrían dañar la información, también los errores de operación por parte del elemento humano llegan a causar estragos que afectan directamente el funcionamiento del hardware y/o software.

Es muy frecuente que las personas cometan errores o que debido a falta de capacitación, lleguen a borrar información de manera accidental e incluso a formatear discos duros de la red.

Otro factor a considerar es el fallo que puede llegar a ocurrir en el equipo de cómputo, pues éste no está exento de sufrir desperfectos; sobre todo puede

ocurrir en los discos duros debido a que tienen un tiempo promedio de fallas que no hay que dejar de tomar en cuenta.

Por lo general, los errores de hardware se deben en muchas ocasiones al mal manejo del equipo, golpes, derrames de líquidos, polvo y condiciones ambientales, entre otros.

El software también es susceptible de fallo. En algunas ocasiones existen errores tanto en los programas de aplicación como en los sistemas operativos, capaces de ocasionar alteraciones en los archivos y pérdida de información, esto sin tomar en cuenta que los virus son hoy en día, una de las principales causas de daño y de pérdida de información.

Considerando lo anterior, resulta difícil pensar en el hecho de administrar una red sin contar con medios y técnicas de respaldo. En realidad, como ya se ha mencionado antes, un buen respaldo es aplicable desde una PC hasta un mainframe.

### 5.1.6.1 Objetivos.

- Verificar que los datos cuenten con una forma de recuperarlos en caso de daño o pérdida intencional o accidental.
- Verificar que los procedimientos de backup consideren:

  - El sistema operativo actual.
  - La infraestructura de cómputo y conmuto necesaria.
  - Códigos de los programas aplicativos.
  - Utilerías más utilizadas, por ejemplo, editores de texto, compiladores, programas externos, etc.
  - Archivos maestros y transaccionales.
  - Archivos de desarrollo y de preproducción, en caso de existir.
  - Documentación que soporte los puntos anteriores.

- Revisar que los respaldos se efectúen con la periodicidad requerida para asegurar la recuperación en caso de impacto.
- Determinar si se realizan pruebas periódicas acerca del funcionamiento de los procedimientos de recuperación.
- Verificar el tipo de respaldo utilizado en los servidores.
- Evaluar el Plan de Contingencia existente.

### 5.1.6.2 Riesgos específicos.

- Respaldos inadecuados o incompletos que eviten una recuperación.

- Respaldos mal identificados, implicando problemas en la recuperación y desperdicio de recursos (espacio, cintas, cartuchos, etc.).
- Rotación inadecuada de respaldos.
- Procedimientos de recuperación erróneos.
- Plan de Contingencia incompleto o poco funcional.

**5.1.6.3 Evidencia disponible.**

- Procedimientos documentados de respaldo/recuperación.
- Catálogos y/o bitácora de respaldos.
- Cintas cartuchos, diskettes.
- Plan de Contingencia y resultado de las pruebas realizadas.

**5.1.6.4 Procedimiento de Auditoría.**

1. Revisar que los procedimientos indiquen de forma clara y comprensible:

   - Archivos vitales que deban respaldarse.
   - Archivos que se respaldan en sitio y fuera de sitio, la forma en que los envían y el lugar de almacenamiento.
   - Periodicidad con que se realizan los respaldos, retención y rotación de éstos.
   - Marcos de tiempo del restablecimiento del sistema o servicio.

2. Revisar que los controles eviten algunos de los siguientes aspectos:

   - Respaldos no actualizados o hechos en forma esporádica.
   - Que los medios magnéticos no se encuentren identificados claramente.
   - Que no se tengan los respaldos de las últimas versiones de los sistemas de producción.

3. Identificar el medio magnético utilizado para respaldar información:

   - Cintas o cartuchos.
   - Discos flexibles o duros.
   - Discos ópticos, compactos.

4. Verificar la existencia e implantación de técnicas para mantener en línea un nivel de respaldo tolerante a fallas:

   - Disco en espejo (disk mirroring) y servidores en espejo (backup server).
   - Duplicidad de discos (disk duplexing) y sistema de arreglo de archivos en disco.

5. Asegurar que se verifique la autenticidad del personal que realiza el traslado de los respaldos al sitio alterno y que éstos llegan en el tiempo estipulado.

6. Verificar la existencia de manuales y procedimientos documentados que indiquen como restablecer un servidor en caso de que éste falle.

7. Verificar que exista un medio alterno para dar continuidad a la operación si los servidores fallan.

8. Verificar que el plan de contingencia cuente con:

   - Objetivo y alcance.
   - Estructura organizacional y definición de responsabilidades en casos de contingencia.
   - Definición de directorio de los responsables del plan, el cual debe de contener:

     - Nombres de los responsables y personal sustituto.
     - Direcciones y teléfonos particulares.

   - Establecer los medios formales de comunicación que permitan difundir el plan de contingencia al personal de la institución.
   - Supuestos bajo los cuales fueron desarrollados.
   - Infraestructura de cómputo:

     - Inventario y características de componentes de hardware y software críticos.
     - Configuración de sistema operativo requerido.
     - Copia del contrato con la empresa que proporcionará el centro de respaldo en caso de contingencia.
     - Directorio de proveedores de hardware y software para asesoría y soporte.

   - Aplicaciones clasificadas por importancia para el negocio.
   - Especificación de los marcos de tiempo de restablecimiento.
   - Plan general, el cual debe contener un panorama global de los procesos vitales a restablecer para el hardware, software y comunicaciones.
   - Plan detallado de las actividades a realizar hora por hora en caso de contingencia en el hardware, software y comunicaciones.
   - Procedimiento para mantener actualizado y funcional el plan.
   - Autorizaciones.

9. Evaluar el plan de contingencia, cuestionándose respecto a su funcionalidad y alcances necesarios para minimizar impactos, considerando:

- Que el departamento de sistemas de información y sus principales usuarios, cuentan con planes implantados para enfrentar eventos de baja frecuencia y gran potencial de consecuencias, tales como tormentas, terremotos, bombas o pérdida de los servicios más importantes como: energía eléctrica, aire acondicionado, comunicaciones, transporte, etc.
- Que los planes están documentados y han sido comunicados de una manera adecuada a todas las personas que deben conocerlos.
- Que el plan del departamento de sistemas ha sido desarrollado en conjunto con los usuarios.
- Que los usuarios están informados de que aún en el evento de pérdida de la capacidad de proceso, ellos mantienen la responsabilidad principal para las funciones del negocio.
- Que existan acuerdos acerca de las bases sobre las cuales trabajar, así como la frecuencia, severidad y duración de tales caídas y de las estrategias de recuperación y respaldo.
- Que los planes (de los usuarios y sistemas de información) han sido revisados y aceptados por un nivel de gerencia común.
- Que los planes han sido probados con simulacros, ejercicios o revisiones de terceros.
- Que los planes indiquen que se almacene en un sitio apartado una copia actualizada de los datos fundamentales para que la operación del negocio continúe "fuera de sitio".
- Que todas las responsabilidades que contempla el plan han sido documentadas y comunicadas adecuadamente.
- Que se han tomado medidas para monitorear todas las fuentes de alarma, incluyendo incendios, malfuncionanientos de temperatura, etc.
- Que se han asignado claramente las responsabilidades individuales de la gerencia para aplicar los planes de contingencia y toma de decisiones en las acciones correctivas necesarias.
- Que se han tomado medidas para notificar a todo el personal (ej. evacuación) que acciones deben realizar.
- Que se ha capacitado a los empleados en procedimientos de emergencia, (ej. uso de extinguidores, apagar el equipo, etc.).
- Que se llevan simulacros de evacuación por incendio sobre una base periódica.
- Que se han identificado y otorgado prioridades a todos los procesos críticos (ej. los relacionados con el flujo de efectivo tal como facturación, los relacionados con los productos de recepción y embarque o aquellos vinculados con un servicio cobrable).
- Que se ha identificado la configuración mínima para todos esos procesos críticos.
- Que se han identificado alternativas adecuadas de capacidad de proceso requerida para los procesos críticos.

- Que se ha demostrado la habilidad de correr los procesos críticos en las facilidades alternas de procesamiento.

### 5.1.7 Cambios a componentes.

#### 5.1.7.1 Objetivos.

Cualquier tipo de cambio acarrea la posibilidad de un error y la generación de problemas. Los cambios en los sistemas de información deben ser vigilados y tener un procedimiento para su integración a producción, asegurando que estos satisfagan las solicitudes de negocio con la oportunidad requerida.

Para llevar a efecto los cambios a los sistemas de información, es importante considerar lo siguiente:

- Asegurar que cualquier modificación a los sistemas de información este sujeta a un procedimiento de cambios, el cual incluya un seguimiento.
- Verificar que el procedimiento de control de cambios al menos incluya los siguientes elementos:

  - Registro de cambios requeridos.
  - Cambios priorizados y agrupados basándose en las necesidades de negocio y una revisión técnica.
  - Cambios programados, diferidos y rechazados.
  - Monitoreo de pruebas.
  - Monitoreo de la instalación en producción.
  - Control y reporte de todos los cambios registrados.

- Verificar que exista y se encuentre actualizado el inventario de recursos (componentes del sistema y de la aplicación).

**Políticas Generales del Proceso de Cambios.**

En todo proceso de cambios a componentes de sistemas de información, deben existir políticas que normen éste importante rubro. A continuación, se presentan aquellas políticas que son consideradas primordiales para el éxito dentro del proceso de cambios en una organización:

1. Cualquier modificación a las especificaciones de ejecución o funcionamiento de los procesos y recursos de producción y distribución de los servicios que presta el sistema de información, es un cambio.

2. El proceso de cambios es único y de aplicación general para todas las modificaciones que afecten a los recursos de cómputo y comunicaciones, mismas que se proporcionan a los usuarios de los sistemas de información.

3. El alcance de los cambios es aplicado a procesos y recursos en producción y distribución con los que se prestan servicios.

4. Los siguientes rubros son considerados como motivos de cambio a los componentes en producción:

   - **Solución a problemas**
     Son todos los cambios que en forma emergente solucionan los problemas de producción y que quedan enmarcados en alguno de los siguientes puntos:

     El problema impide continuar con la producción.
     Prevenir fallas en producción en el siguiente proceso diario.
     No se cuenta con procedimientos autorizados de recuperación.
     - El riesgo de no corregir el problema es alto.
     - Riesgo inminente de una recuperación en línea.
     - Degradación extrema en el servicio de línea.
     - Mal funcionamiento de una aplicación/transacción relevante en línea.
     - Corrección de procedimientos desactualizados.

   - **Nuevas funciones**
     Son todos los cambios que apoyan a los usuarios para generar nuevos productos que no están contemplados en los sistemas que residen en producción y son necesarios para cumplir a corto plazo las demandas de las unidades de negocio.

     Generalmente provienen de requerimientos de usuarios y de tipo legal, o bien, por disposiciones de la dirección del negocio.

   - **Mantenimiento**
     Son todos los cambios que apoyan la correcta funcionalidad de los sistemas, derivados de la instalación de nuevas herramientas de cómputo, conmuto o comunicaciones, de las interrelaciones con otros sistemas o mejoras técnicas por uso de nuevos productos.

     Generalmente provienen de proyectos internos y no afectan la funcionalidad de las aplicaciones.

- **Optimización**
  Son todos los cambios que apoyan a los sistemas, derivados de las solicitudes de usuarios o reportes internos de malos comportamientos de los procesos justificando modificaciones a la funcionalidad de las aplicaciones.

  Generalmente provienen de la acumulación de reportes de problemas levantados por los usuarios y/o producción.

- **Otros**
  Son todos los cambios que por su esencia abarcan dos o más de los conceptos anteriores. Generalmente provienen de solicitudes internas y de usuarios.

5. Es necesario contar con un sistema automatizado como única fuente autorizada para el registro y seguimiento de cambios y el proceso debe ser coordinado por los involucrados en el mismo, de acuerdo a los procedimientos autorizados para el manejo y operación de los cambios.

6. Cada cambio en función de su visibilidad, magnitud y riesgo, recibirá a su entrada al proceso una calificación denominada categoría, la cual definirá la profundidad con la que cada etapa deberá cubrirse, a saber:

   **Categoría A.** Cambios sin pruebas y sin retornos, que impliquen interrupción total del servicio, instalaciones en días críticos, legales de alto riesgo que afecten la funcionalidad de múltiples sistemas críticos o de la organización.
   - **Categoría B.** Línea y batch de aplicaciones críticas que dejen algo de línea, nuevos sistemas, nuevas liberaciones, reingenierías e instalaciones estratégicos.
   - **Categoría C.** Con retorno probado y ágil de ejecutar, con impacto menor a 30 minutos y cierre de transacciones no críticas, retraso en la entrega de productos no críticos.
   - **Cambios Estratégicos.** Son los cambios que se efectúan en diferentes fechas y/o por uno a más líderes promotores y/o para uno o más componentes o aplicaciones, en los que se debe presentar la estrategia general del proyecto.
   - **Cambios en Modo Release.** Son aquellos que en días previamente establecidos se instalarán a las aplicaciones agrupando más de una modificación a la vez. Para este caso, se tendrá un calendario anual por cada sistema.

7. Debe asignarse la categoría del cambio al término de la fase de análisis de la iniciativa, proyecto o problema; con el fin de terminar anticipadamente los

requerimientos del proceso de cambios y evitar contratiempos en el cumplimiento del trámite.

8. Las categorías de los cambios se distribuirán de acuerdo a sus componentes por grupo, de la siguiente manera:

| GRUPO | COMPONENTES | CATEGORIA A | B | C |
|---|---|---|---|---|
| Sistemas aplicativos línea y batch. *(También están categorizados como cambios Estrategicos y Modo Release).* | Programas, archivos, bases de datos, transacciones, etc., interactúan entre sí o que son independientes, a fin de lograr los objetivos de negocio. | | X | X |
| Equipo Central de Proceso. | Canales, cintas, discos, procesador, controlador de cintas y de discos, diskettes, Impresoras, grabador de microfichas, etc. | X | X | X |
| Equipo Central de Conmutadores. | Conmutador central. | X | | |
| Equipo de la Red de Teleproceso. | Controlador de comunicaciones y terminales, hardware de comunicaciones, terminales, módems, servidores, hubs, mini y/o microcomputadoras, impresoras de red, enlaces, satélite, routers, cableado. | | X | X |
| Sistemas Operativos Centrales. | Assembler, COBOL, DB2, JES2, MARK IV, MVS, NDM, RACF, OS/2, TSO, UCC, Utilerías, VSAM, VTAM. | | X | X |
| Sistemas Operativos de la Red. | CICS, NCP. | | | X |
| Instalaciones Físicas. | Control de acceso a CPD, agua para enfriamiento, sistema de aire acondicionado, energía eléctrica, sistemas de detección y extinción de incendios, instrumentos de medición. | | X | X |

Fig. 5.1

9. Todo cambio, independientemente de su categoría y de su ejecución, contará con una persona quien fungirá como líder promotor para su ejecución y este será responsable de que el producto a instalar funcione de acuerdo a los requerimientos de los usuarios.

10. Todos los cambios deberán pasar por los evaluadores técnico/aplicativos para ser revisados y aprobados.

11. Las áreas y personas responsables de los servicios de información que tengan a su cargo la custodia, funcionamiento u operación de recursos de cómputo y/o comunicaciones, fungirán como receptores de los cambios a dichos recursos.

12. Todo cambio registrado debe estar aprobado por los evaluadores/aprobadores que sean designados de acuerdo a la categoría del cambio antes de ser instalado.

13. El objetivo de la evaluación técnica/aplicativa es la revisión del plan de instalación de todos los cambios, retornos e impactos a los cambios programados obteniendo las recomendaciones correspondientes.

14. El objetivo de la función de aprobación de negocio o gerencial es revisar el plan de los cambios, pruebas o instalación de los mismos y autorizar los riesgos de las instalaciones y posibles impactos, pudiendo cambiar el plan de acuerdo a necesidades de negocio.

15. Para decidir la retorno de cambios instalados con anterioridad, es necesaria la determinación conjunta de las áreas receptora y promotora.

16. Se cerrarán los cambios de acuerdo con el siguiente criterio:

    - **Éxito**: los cambios que no hayan ocasionado problemas en producción.
    - **Fracaso**: los cambios que hayan ocasionado problemas en producción y que no se apeguen al plan.

17. Las áreas receptoras de cambios en conjunto con los promotores se encargarán de calificar los cambios, apegándose a la política anterior y registrándolas en la base de datos que haya sido designada para dar seguimiento al proceso.

18. El área receptora de cambios solicitará al usuario de la aplicación que sufrió el fracaso de un cambio, el impacto financiero ocasionado.

19. Es responsabilidad de los participantes el monitoreo y resultado de la etapa de pruebas, recomendar el proceder o no con la instalación de un cambio a partir de los resultados de esta etapa, sin tener en ningún caso, autoridad para detener o suspender un cambio.

20. Se suspenderá la instalación de un cambio si por especificaciones erróneas se presentan problemas, calificando al responsable del error.

21. Todo cambio suspendido de acuerdo al punto anterior, se reprogramará basándose en el análisis de concurrencia de cambios y manejo de prioridades de los mismos.

### 5.1.7.2 Riesgos específicos.

Todo cambio lleva asociado uno o varios riesgos que pueden impactar la continuidad de los procesos o representar impactos financieros para el negocio.

A continuación se presentan algunos de los riesgos potenciales que tienen lugar en el proceso de cambios:

1. Modificaciones a los sistemas sin una evaluación riesgo/impacto eficiente.
2. Documentación inadecuada para efectuar la modificación y seguir con la operación normal después del cambio.
3. Cambios con prerequisitos sin control.
4. Alto porcentaje de cambios rechazados.
5. Cambios sin planes de retorno que impactan el servicio.
6. Aplicación inadecuada de controles por políticas mal definidas.
7. Alto número de instalaciones no exitosas por revisiones y aprobaciones inadecuadas a planes de cambio.
8. Fuga de información vital para el negocio al registrar datos de aplicaciones en sistemas no autorizados para el registro y seguimiento de cambios.
9. Instalación deficiente de cambios al no dar seguimiento adecuado a la etapa de pruebas.
10. Impacto a otras aplicaciones importantes para el negocio por no elegir correctamente o dejar de invitar a participantes clave del proceso.
11. Instalaciones no exitosas al designar incorrectamente a los evaluadores/aprobadores de acuerdo a la categoría del cambio.
12. Pagos no programados a proveedores de servicios de informática para corrección de programas, derivado de una planeación incorrecta para efectuar los cambios.

13. Servicio deficiente a usuarios al tener una catalogación incorrecta de componentes en producción, debido a la ausencia de revisión de instalación en producción.

14. Retraso y/o fracaso en la instalación del cambio, por habilidades y capacitación pobres entre el personal encargado de dar soporte, así como ausencia en el dominio del manejo de la complejidad del cambio.

15. Impacto en la capacidad de recursos y equipos de cómputo por una demanda no planeada.

16. Solución a requerimientos de usuario no cumplida, por ausencia de planes de retorno, recuperación y seguridad de la información.

17. Alto riesgo de impactos financieros para el negocio y retraso en el servicio a usuarios por falta de priorización de cambios concurrentes a componentes de una misma aplicación, así como no contemplar antecedentes y/o dependencias.

18. Atención deficiente a problemas que requieran cambio en producción al no contar con una categorización de cambios adecuada y bien estructurada.

**5.1.7.3 Evidencia disponible.**

Para llevar a efecto la revisión a este control, se deben considerar las siguientes evidencias:

1. Sistema automatizado estándar para el registro y seguimiento de cambios.

2. Políticas y procedimientos para cambios a los sistemas y equipos en producción.

3. Logs del sistema.

4. Estadísticas de los cambios efectuados, incluyendo resultados e impactos.

5. Establecimiento de niveles de servicio.

6. Calendario de cambios.

7. Matriz de participantes en los cambios por grupo de componente.

8. Documentación generada por el retorno de cambios.

9. Recomendaciones generadas por el comité técnico/aplicativo al revisar los planes de cambios.

10. Documentación generada por reportes problema levantados para generación de cambios en producción.

11. Requerimientos funcionales elaborados, revisados y validados con el usuario para generar cambios a componentes.

12. Requerimientos estructurales o de recursos de cómputo elaborados, revisados y validados con personal de soporte, necesarios para llevar a cabo los cambios.

13. Bitácoras de pruebas y visto bueno del usuario responsable.

14. Matriz de pruebas antes de la instalación del cambio.

15. Revision del resultado de las pruebas.

16. Monitoreo del cambio en producción.

17. Aprobaciones del cambio por todos los involucrados.

#### 5.1.7.4 Procedimiento de Auditoría.

Dentro del procedimiento de auditoría, se deberán considerar los siguientes puntos:

1. Verificar que el registro del cambio incluya al menos la siguiente información:

   - Reporte problema levantado o análisis de cambio a componentes de la aplicación.
   - Descripción del cambio y clasificación del mismo por impacto.
   - Fecha de registro e instalación del cambio.
   - Prerequisitos para efectuar el cambio (ej. tiempo máquina o soporte en sitio).
   - Existencia de líder promotor del cambio.
   - Nombre de la aplicación y componentes a afectar o modificar de la misma.
   - Documentación sobre posibles riesgos e impactos.
   - Detalle de actividades a realizar y responsables de llevarlas a cabo.
   - Puntos de control que indiquen cuando debe suspenderse el cambio.
   - Existencia de planes de retorno en caso de cambios fracasados, a fin de dejar a la aplicación o infraestructura como estaban.
   - Matriz de responsables de autorizar el cambio.

- Matriz de escalamiento en caso de problemas.
- Requerimientos funcionales y estructurales debidamente documentados.
- Casos de pruebas unitarias, modulares, de sistema y de retorno analizados y aprobados por el líder promotor del cambio y el usuario de la aplicación a afectar.
- Autorización para utilizar los ambientes de pruebas y preproducción para modificar y llevar a cabo las pruebas a los componentes de la aplicación antes de la instalación.

2. Verificar la existencia de un log o base de datos que refleje el estatus actual y la historia de los cambios realizados por periodos

3. Revisar la calendarización y priorización de los cambios.

4. Verificar que sólo un área efectúe la planeación de los cambios.

5. Revisar que se generen y revisen reportes que incluyan los cambios realizados en un periodo, los exitosos y los rechazados por categoría, componente afectado, líder promotor, etc.

6. Asegurar que los componentes que se encuentren en producción estén en bibliotecas protegidas y que solamente personal autorizado pueda efectuar cambios a un mismo módulo o programa.

7. Determinar si los programas se encuentran en el inventario propio de la aplicación, cerciorándose que éste se encuentre actualizado.

8. Verificar que, para llevar a efecto un cambio, existan debidamente documentadas las funciones y obligaciones del líder promotor, del comité técnico/aplicativo, del área de administración de cambios; así como guías y procedimientos para posibles emergencias y contingencias.

9. Determinar si los niveles de servicio son adecuados para dar atención oportuna al desarrollo del proceso de cambio.

### 5.1.8 Reporte y seguimiento a problemas.

Para un control eficiente de los problemas presentados es conveniente tener definido un proceso, que se inicie cuando ocurre el problema y termina cuando se resuelve. Existen problemas que se solucionan en el momento por medio de procedimientos de emergencia y otros que requieren de un diagnostico y proyectos de mantenimiento o afinación.

### 5.1.8.1 Objetivos.

1. Verificar que el procedimiento para reporte/solución de problemas cubra al menos los siguientes puntos:

   - Reconocimiento y reporte/registro del problema.
   - Identificación de la naturaleza, impacto y extensión real del problema.
   - Existencia de procedimientos de "bypass" y recuperación.
   - Acciones controladas y coordinadas en la solución del problema.
   - Control y reporte de todos los problemas tanto abiertos como cerrados.

2. Asegurar que los problemas presentados son registrados, atendidos, cerrados o resueltos y que se apegan al procedimiento establecido para reporte y solución de problemas.

3. Verificar la calidad de la solución a los problemas presentados.

### 5.1.8.2 Riesgos específicos.

1. Problemas recurrentes debido a una baja calidad en la solución de problemas.

2. Impactos constantes en el servicio sin la posibilidad de identificarlos debido a que no se cuenta con un registro de problemas.

### 5.1.8.3 Evidencia disponible.

1. Políticas y procedimientos para el registro y cierre de problemas.

2. Base de datos o bitácora de problemas registrados.

3. Estadísticas de problemas recurrentes.

### 5.1.8.4 Procedimiento de Auditoría.

1. Revisar que se cuente con una matriz de escalamiento de problemas, la cual contenga los niveles de soporte (administrador, proveedores, gerentes, etc.) nombre y teléfono, así como los límites para que se escale el problema si este no ha sido resuelto.

2. Revisar que el reporte problema contenga como mínimo la siguiente información:

   - Fecha, hora y componente en que se presentó el problema.
   - Nombre de quien recibe y reporta el problema.

- Número de reporte asignado.
- Breve descripción del problema.
- Impacto ocasionado.
- Procedimiento de bypass aplicado.
- En caso de no funcionar el procedimiento de bypass, describir las acciones tomadas para activar nuevamente el componente y a quién se escala el problema.
- Checar que al cierre de un problema se describan brevemente las acciones que lo solucionaron.

3. Determinar la calidad de solución a través de la identificación de problemas recurrentes y soluciones aplicadas.

4. Verificar las estadísticas de problemas abiertos y cerrados y enfatizar en aquellos que aún no se han cerrado y llevan abiertos un tiempo no razonable.

### 5.1.9 Uso y aprovechamiento de la plataforma.

En la actualidad la mayoría de las empresas donde se utilizan computadoras, se tiene ya el uso de un ambiente de red o la tendencia a su instalación. Por tal motivo es importante evaluar cómo está operando esta red.

La planeación de carga de trabajo en el uso de la red es de suma importancia para eficientar la operación de la empresa, por lo que debe darse un mantenimiento preventivo y correctivo por parte del vendedor de la red.

#### 5.1.9.1 Objetivos.

- Verificar la existencia y apego a los contratos de mantenimiento preventivo y/o correctivo.
- Verificar que dentro de las funciones del encargado se incluya la limpieza del servidor y periféricos y que ésta se haga de acuerdo a las recomendaciones del fabricante.
- Asegurar que el encargado esté autorizado para efectuar reparaciones a la red.
- Revisar que los contratos de mantenimiento estén vigentes.
- Revisar que el mantenimiento se haga de acuerdo a un plan y no en forma aleatoria.
- Verificar que el encargado cuente con la documentación y procedimientos necesarios para la operación de la red.
- Evaluar la administración y supervisión de la red.

#### 5.1.9.2 Riesgos específicos.

- Falta de contrato de mantenimiento.
- Equipo sin mantenimiento preventivo debido a que no se respetan los planes.
- Mantenimiento no realizado que haya sido pagado.
- Mantenimiento aparentemente realizado.
- Documentación faltante o inadecuada para la operación.
- Actividad del encargado no definida.
- Actividad del usuario no definida.
- Plan de operación ineficiente.
- Falta de capacidad del operador.
- Fallas constantes en la red.

#### 5.1.9.3 Evidencia disponible.

- Documento de la capacidad óptima de operación de la red del encargado.
- Relación de usuarios y nivel de operación.
- Bitácoras de mantenimiento externo/interno.
- Estadísticas de problemas y los impactos causados por la aplicación.
- Contratos de mantenimiento.
- Relación de equipos, accesorios y diagrama de la red.

#### 5.1.9.4 Procedimiento de Auditoría.

- Verificar que existan políticas y procedimientos para integrar aplicaciones en la instalación y funcionamiento de la red.
- Revisar que la bitácora de mantenimiento se encuentre correctamente autorizada y que todos los mantenimientos planeados en un período se encuentren registrados.
- Verificar que en los contratos de compra/renta del equipo se encuentre incluido el mantenimiento.
- Verificar que el contrato de mantenimiento ampare o contenga:

  - Servicios de reparación.
  - Detalle de mantenimiento preventivo a ser cumplido.
  - Plan de mantenimiento.
  - Tiempo de respuesta.
  - Penalización en caso de incumplimiento.
  - Vigencia de garantías.
  - Parámetros que determinen la razonabilidad de los cobros.

- Verificar que los operadores tengan identificados a los proveedores a contactar en caso de presentarse problemas con el equipo.
- Revisar el registro de los problemas de hardware y el tiempo que el equipo esta fuera de servicio entre cada sesión de mantenimiento.
- Comprobar que los operadores no ejecuten programas que alteren información sin autorización.
- Verificar el procedimiento de planeación, monitoreo y administración de la red, en aspectos como espacio en disco, capacidad de procesamiento y almacenaje de información, uso de memoria, spool de impresión, etc., evaluando su funcionalidad, cerciorándose que las estadísticas se obtienen de los archivos del servidor de la red.
- Verificar que existan pruebas de funcionamiento de la red.

# PLAN DE AUDITORÍA, INFORME DE AUDITORÍA Y SEGUIMIENTO

## 6.1 PLAN DE AUDITORÍA.

Objetivo

*Definir el alcance de la revision y elaborar el plan de trabajo*

En esta actividad debe analizarse el entorno del proyecto para conocer como esta organizado, dimensionarlo e identificar las áreas involucradas en la revisión de la unidad auditable, con el propósito de definir el alcance y elaborar el plan de trabajo correspondiente.

Cabe mencionar que el nivel de información existente hasta este momento es de tipo general; sin embargo, es importante considerar los siguientes aspectos:

- Políticas directivas.
- Información preliminar existente.
- Enfoque y conocimiento general.

**A) Definición de objetivos y alcance.**

Con base en el análisis y estudio previo de la unidad auditable, se establecen en forma clara y concreta los objetivos de la revisión, así como la cobertura y el nivel de profundidad de la misma.

Como parte de esta actividad debe elaborarse la carta inicial de revisión, a fin de presentar a las áreas involucradas el grupo de auditoria que estará a cargo de la revisión.

Productos finales

- Lista de objetivos y alcances.
- Carta inicial de revisión.

**B) Levantamiento de información básica.**

Consiste en acudir directamente con los responsables de las áreas involucradas para solicitar la información, tanto administrativa como técnica, indispensable para llevar a cabo la revisión, considerando que independientemente del volumen de

información recabada sólo se analice lo necesario para cubrir los objetivos de esta fase y realizar un análisis profundo en las fases posteriores.

Asimismo, se tiene que revisar la información obtenida a fin de contar con una perspectiva general para conocer las principales características de la unidad auditable.

Durante el desarrollo de esta actividad es necesario hacer un programa de entrevistas, definiendo para ello el perfil de cada una de las mismas con base en la naturaleza de las funciones que realicen las personas entrevistadas y a efecto de prever el nivel de información que se solicitará.

Es importante documentar y resumir la información obtenida como resultado de las entrevistas.

La inclusión de nuevas entrevistas debe ser considerada en virtud de que existe la posibilidad de identificar áreas que originalmente no habían sido contempladas en la revisión.

Productos finales

- Lista de requerimientos de información básica.
- Programa de entrevistas iniciales.
- Resumen de entrevistas.

**C) Análisis de información.**

Debe efectuarse un examen minucioso de la información obtenida, con el propósito de identificar y seleccionar los aspectos primarios, secundarios y no relevantes, así como la determinación de la información adicional o complementaria que debe ser requerida.

Asimismo, es recomendable la elaboración de un flujo operativo que describa gráficamente las funciones del área o sistema a auditar, ya que constituye un elemento de apoyo para evaluaciones posteriores.

Productos finales

- Descripción narrativa de las características principales.
- Resumen del análisis de la información inicial.
- Flujo de la operación.

**D) Diagnóstico de viabilidad.**

Considerar en esta actividad los elementos de información identificados en el análisis, con el objeto de hacer un examen previo de la unidad auditada y decidir si se realiza la revisión o no, estableciendo las causas que justifiquen ambas situaciones y los siguientes aspectos:

1. Importancia e impacto de la unidad auditable (Nivel de riesgo).

- Cobertura de servicio.
- Tecnología existente.
- Interacción con otros sistemas.
- Costo financiero de la función.
- Dimensión del sistema en términos de programas o procesos.
- Número de personas involucradas.
- Áreas participantes.
- Nivel de autorización.

2. Situación de control.

- Determinar cual es la situación que presenta la unidad auditable en cuanto a: suficiencia, debilidades de control y probabilidad de riesgo.

3. Beneficios esperados de la revisión.

- Identificar los factores de riesgo, determinando los aspectos relevantes que pudieran afectar a la institución en términos financieros, de operación o administrativos.
- Con base en el diagnóstico de los aspectos citados, elaborar la propuesta para efectuar la revisión o indicar cuáles son las causas que justifican la suspensión de la misma.

Producto final

- Resumen de Viabilidad.

**E) Planeación del desarrollo.**

Elaborar el programa de trabajo, asignando tiempos y responsables a las actividades de las siguientes fases de la metodología.

Producto final

- Plan de Desarrollo de la Revisión.

**Desarrollo de la Auditoría**

**A) Obtención de información detallada.**

Con base en el resultado del análisis de la información y el conocimiento adquirido hasta ahora de la unidad que estamos revisando, podemos determinar que información adicional requerimos para satisfacer nuestras necesidades.

Producto final

- *Documentación de Auditoría.*

**B) Detallar plan original.**

Siguiendo el plan de desarrollo en donde se identificaron las macroactividades, se *procederá a desglosar aquellas* que requieran mayor detalle para obtener programas de revisión de acuerdo con las características de la función auditada.

Producto final

- *Programa de Trabajo.*

**C) Evaluación de controles**

En esta actividad se evaluarán los puntos de control determinados en el programa de revisión, con el propósito de conocer la eficiencia en el *manejo de información* y en la generación de resultados, vigilando el cumplimiento de los objetivos determinados en el programa de revisión.

Producto final

- Lista de controles.
- Matrices de evaluación.
- *Resumen de la situación del Control Interno.*

**D) Diseño de pruebas de auditoría.**

En esta actividad se deberá diseñar y realizar el programa de pruebas de aquellas funciones y procedimientos que por su *nivel de riesgo sea necesario validar.*

Producto final

- Programa de Pruebas de Auditoria.

**E) Aplicación de pruebas de auditoría.**

En esta actividad se deberá aplicar el programa de pruebas de la unidad auditada para validar aquellos controles que, de acuerdo con sus características, es necesario revisar a través de pruebas de auditoría.

Productos finales

- Papeles de trabajo de las pruebas.
- Lista de observaciones.
- Resumen de hallazgos.

## 6.2 INFORME DE AUDITORÍA.

**Introducción**

La presentación de un informe con grado de excelencia es el producto básico de la auditoria en general. Dentro del contexto general del campo de la auditoría, se involucra el levantamiento de información, la evaluación, la comprobación y es precisamente la acción de informar la que queda a la vista, al escrutinio y a la opinión - muchas veces crítica - de los auditados.

La preparación de un informe constituye un proceso interesante, pero a la vez complejo de sintetizar. La síntesis es la integración ordenada de las partes de una unidad. Es un método que procede de lo simple a lo compuesto. Es la suma, es el compendio, es el extracto, es la sinopsis. Es la combinación lógica de premisas y conclusiones. La calidad de la síntesis depende de la calidad del proceso de análisis.

Los informes de auditoría reflejan un amplio conocimiento del negocio, conocimiento tecnológico y de los procesos administrativos y técnicos que estamos evaluando, además de mostrar con claridad el enfoque de las situaciones observadas, las conclusiones y las acciones que deben ser llevadas a cabo.

Es importante mencionar que, además de cumplir satisfactoriamente con los objetivos de evaluar, comprobar e informar sobre debilidades, se aporten ideas

que se traduzcan en un valor agregado para la consecución de los principales objetivos del negocio u organización.

Para ello, se depende de la efectividad con que se hayan despejado, principalmente, las siguientes incógnitas:

- ¿ Se planeó adecuadamente el trabajo ?
- ¿ Se definió claramente el enfoque de la revisión ?
- ¿ Se documentaron suficientemente las pruebas efectuadas ?
- ¿ Se cuenta con un conocimiento a fondo de lo que se está auditando ?
- ¿ Los hechos observados son relevantes ?
- ¿ Las conclusiones son claras y significativas ?

Si la respuesta a cada una de las interrogantes anteriores es afirmativa, entonces se está en condiciones de entregar un buen producto. En caso contrario, el informe podrá ser severamente cuestionado y terceras personas podrán tener evidencia de omisiones y aseveraciones que no están debidamente sustentadas.

**Objetivos**

Elaborar el Informe Final con la Carpeta de Apoyo que lo sustente, así como la aprobación por parte de los ejecutivos de auditoría para emitirlo.

Establecer compromisos para la atención de las observaciones.

**A) Evaluación y documentación de resultados.**

Con base en el resultado de las pruebas y apoyándose en el resumen de la situación del Control Interno el auditor determinará los riesgos debidos a controles deficientes, inexistentes o duplicados. Lo anterior servirá para facilitar el análisis de las observaciones, el establecimiento de recomendaciones y el cumplimiento con los objetivos de la revisión.

Posteriormente, el auditor deberá analizar y evaluar las observaciones a fin de estructurar el "Borrador de Observaciones", determinando el impacto de cada una de ellas en cuanto al riesgo que representan para el negocio o institución.

Como resultado de esta etapa el auditor deberá generar el "Borrador de Observaciones" para la elaboración del Informe, en donde cada una de las observaciones deberá ser sustentada con evidencias suficientes y papeles de trabajo competentes, con lo que se formará la carpeta de apoyo.

Se presentará el "Borrador de Observaciones" a los auditados y se obtendrán los compromisos y firmas correspondientes que los ratifiquen.

Productos finales

- Borrador de observaciones y recomendaciones.
- Carpeta de apoyo actualizada.
- Compromisos de las áreas auditadas para cada observación del informe.

B) Elaboración del informe.

El auditor redactará el informe ponderando y seleccionando aquellas observaciones que impliquen alto nivel de riesgo para la organización, tomando en cuenta para su estructura el siguiente formato:

**Fecha del informe.** Deberá fecharse preferiblemente en el momento de su entrega.

**Destinatario.** El informe será dirigido de acuerdo a la importancia de hallazgos y a juicio del Subdirector y/o Director de Auditoría, procurando que sea al titular de la Dirección del área involucrada con responsabilidad de coordinación de participantes de la función auditada.

**Obtención de compromisos.** Incluir quienes se comprometieron a solucionar las situaciones especiales detectadas, considerando nombre, puesto y área.

**Dictamen.** Indicar el propósito de la revisión y sus alcances considerando lo establecido en la Planeación de Auditoría.

**Estado actual del proyecto o unidad auditada, sustentado con papeles de trabajo.** Esta situación deberá reflejar los efectos de los antecedentes y su posible relación con las observaciones, en términos de riesgo y problemática general, incluyendo la conclusión de Auditoría derivada del análisis integral de los resultados obtenidos.

**Comentarios de los auditados.** Cuando no exista compromiso formal en alguna observación, incluir textualmente los comentarios de los auditados.

**Firma.** El informe debe ir firmado en el dictamen por el Director o el Subdirector de Auditoría.

**Distribución.** Marcar copia del Informe a los titulares y usuarios directos de todas las áreas involucradas en la revisión.

Recomendaciones adicionales

- Es importante cuidar la redacción y la ortografía.
- Preparar anticipadamente los lineamientos de argumentación para facilitar el análisis del informe con los involucrados en la Auditoría.
- Revisar que el informe incluya comentarios que eviten posibles malas interpretaciones en cuanto a críticas que pudieran parecer tendenciosas.

Producto final

- Informe definitivo.

A continuación se detallan las condiciones que permiten la elaboración y presentación exitosa de informes.

### 6.2.1 Enfoque.

En la preparación del informe es fundamental definir de antemano cual debe ser el mejor enfoque. Para ello conviene tener respuesta a las siguientes preguntas:

- ¿ Las situaciones detectadas son ordinarias, extraordinarias, significativas o graves ?
- ¿ La naturaleza de las situaciones o irregularidades detectadas nos indica que son omisiones, errores, irregularidades o fraudes ?
- ¿ Las situaciones observadas representan un grave peligro al sistema de control interno ?
- ¿ Pueden representar un quebranto significativo para el negocio ?

Basándose en la respuesta de cada uno de los aspectos anteriores, se puede definir con toda seguridad el enfoque del informe a entregar.

El enfoque puede presentarse en el sentido de que no se han detectado situaciones que ameriten profundidad o detalle en la investigación, o bien, que no son significativas.

Asimismo, se pueden detectar u observar fallas críticas a las políticas y procedimientos establecidos en los diversos controles que rodean a la unidad auditable, mismos que pueden provocar o han provocado quebrantos significativos al negocio.

En caso de que se hayan efectuado operaciones irregulares o fraudulentas, el enfoque tendrá que ser formulado de acuerdo a la naturaleza de la falta.

### 6.2.2 Respaldo.

Para la formulación y presentación de los informes, es imprescindible contar con todo el respaldo necesario para cada una de las aseveraciones ahí comentadas. Esto es de gran utilidad al estar revisando el informe con el auditado, ya que así es posible demostrar las fallas en las que se incurren.

De manera más completa, se requiere el respaldo para:

- Afirmar que se ha llevado a cabo la revisión en los términos que se indican en el informe.
- Afirmar que se ha tenido un alcance previamente determinado.
- Señalar las observaciones, fallas o posibles fraudes detectados.
- Evaluar los efectos que pueden provocar dichas situaciones en la unidad auditada o en el negocio en general.
- Proponer las medidas preventivas y/o correctivas para tratar de eliminar o prevenir los riesgos potenciales que se hayan detectado.
- Apoyar a futuras auditorías, o bien, a alguna auditoría realizada por una entidad externa al negocio.

El respaldo se encuentra principalmente en:

- Planes de auditoría.
- Políticas y procedimientos escritos.
- Programas.
- Cuestionarios, flujogramas, memorándums, formatos y papeles de trabajo.
- Impresiones de pantallas.
- Notas de observaciones.
- Catálogos (de equipos, proveedores, programas, listados, cuentas contables, activo fijo, etc.).
- Planes y resultado de pruebas.

### 6.2.3 Estructura.

Para facilitar la presentación del informe al auditado y para que el mensaje que contiene sea debidamente captado, es primordial que tenga una adecuada estructura.

La estructura del informe en general se compone de tres grandes capítulos:

- Introducción.
- Desarrollo.
- Conclusiones.

Dentro de cada uno de estos rubros, se señalan los siguientes aspectos:

**Introducción**

- Objeto de la revisión. Indicar los antecedentes y el objetivo de la auditoría.
- Alcance de la auditoría. Indicar los componentes a evaluar de la entidad auditable.
- Procedimientos aplicados. Mostrar la metodología aplicada para la evaluación.

**Desarrollo**

- Situaciones relevantes detectadas. Presentar observaciones, fallas o desviaciones que no se apegan a la normatividad de la unidad auditable.
- Efectos en la organización. Explicar los riesgos y/o impactos que pueden provocar o que están provocando salir de balance al negocio u organización.
- Medidas sugeridas. Mostrar las recomendaciones preventivas y correctivas que minimizaran o eliminaran tales desviaciones.

**Conclusión**

- Confiabilidad del sistema de control interno. Indicar la importancia de contar con un control interno dentro de la entidad auditada. Por otro lado, reforzar los puntos débiles si es que se cuenta con el control interno.
- Trascendencia en los hallazgos. Hacer énfasis en las desviaciones detectadas para eliminarlas o minimizarlas.
- Acciones a emprender. Desarrollar en conjunto con el auditado un plan para poner en práctica las sugerencias preventivas y correctivas.

La estructura del informe en si debe tener un equilibrio. La parte introductoria no debe estar desproporcionada con respecto a la parte de desarrollo. Asimismo, el capítulo de conclusiones debe ser congruente en contenido y extensión con los capítulos introductorio y de desarrollo.

### 6.2.4 Procedimientos aplicados.

En esta parte del informe se procede a comunicar en forma resumida los procedimientos de revisión que fueron aplicados y el alcance de las pruebas de auditoría llevadas a efecto. Es de suma importancia el basarse en los papeles de trabajo para poder explicar tales procedimientos.

### 6.2.5 Observaciones.

Las observaciones son el resultado de la aplicación de los procedimientos de revisión y son la parte medular de los informes. Son también los puntos en los que en ocasiones, se detecta que el alcance de la auditoría no fue el adecuado por una planeación pobre. Por tanto, se puede **(1)** detener la auditoría, ampliar el alcance y continuar o **(2)** seguir con lo planeado y llevar a efecto una segunda auditoría con un alcance que cubra los aspectos que no fueron planeados.

A continuación se mencionan algunos de los aspectos que conviene considerar al informar sobre los hechos detectados:

- Las observaciones deben ser congruentes con el propósito de la revisión y los procedimientos aplicados
- Las observaciones deben ser significativas.
- Deben basarse en hechos comprobados.
- Se debe contar con todo el respaldo de los hechos reportados.
- Deben estar plenamente identificadas las condiciones en que se realizaron las operaciones.

### 6.2.6 Recomendaciones.

Una vez señaladas las principales fallas o debilidades al sistema de control interno de la entidad auditada, es importante indicar las acciones correctivas y preventivas que deben emprenderse.

Al efectuar el proceso de análisis y de síntesis en la auditoría, se tiene una posición privilegiada para conocer los problemas y las áreas de oportunidad.

Algunos aspectos que deben ser tomados en consideración al determinar las medidas más apropiadas para la organización, son los siguientes:

- Experiencia.
- Amplio conocimiento de la operación y del proceso operativo que se trate.
- Contar con el respaldo necesario sobre las operaciones efectuadas.
- Conocer la perspectiva de los responsables de los procesos administrativos y técnicos.
- Tener presentes las premisas y objetivos del plan estratégico y los principales programas para su realización.

### 6.2.7 Valor agregado.

Partiendo de la premisa de que el éxito de las instituciones depende de la calidad de sus integrantes y de las ideas que ellos aporten, el valor agregado a las recomendaciones es un aspecto de gran importancia en la elaboración y presentación de los informes, ya que es la imagen de conocimiento para con los auditados sobre la entidad auditada.

Dentro de los aspectos claves a tratar en este rubro, se puede mencionar a los auditados que la implantación de las recomendaciones que se les plantean, han dado buenos resultados en otras entidades auditadas. Es recomendable contar con tales resultados a fin de poder mostrarlos y lograr así que las recomendaciones sean tomadas y puestas en práctica con más interés.

Otro aspecto a considerar, es hacer especial énfasis en los riesgos e impactos en los que incurriría el negocio o institución si no se ponen en práctica las recomendaciones dadas.

Para los altos directivos que lean el informe, es importante ver los resultados del mismo en materia estadística, ya que es más fácil para ellos entender tendencias negativas o positivas en el desarrollo del negocio y por tanto, también será más sencillo y rápido poner en práctica las recomendaciones.

## 6.3 SEGUIMIENTO.

**Objetivo**

Certificar que las deficiencias y problemas d... ...tados durante la revisión han sido corregidos y evaluar el estado de control. Para esto se elaborará el programa de seguimiento y con base en él se verificará que las actividades contempladas dentro del Plan de Acción se efectúen de acuerdo a lo establecido, generando un informe que permita conocer los resultados de las medidas correctivas.

Al determinar el grado de avance de las soluciones, se desarrollarán actividades de la fase de desarrollo, con lo cual se dará continuidad al proceso de Auditoría.

Son objeto de seguimiento todas las revisiones que se encontraron en un estado de control deficiente, regular o bueno con posibilidades de optimizarse.

**A) Programación del seguimiento.**

Con base en el Plan de Acción, recurrir a la estructura del Informe, áreas afectadas y compromisos anticipados obtenidos, a efecto de generar un programa de revisión al seguimiento, con actividades y fechas tentativas de realización, considerando para ello alguna otra observación que se deba incluir.

Producto final

- Programa de Seguimiento y Pruebas.

**B) Desarrollo del seguimiento.**

Los auditores deberán hacer el seguimiento correspondiente para cerciorarse de la suficiencia de las medidas adoptadas para corregir las debilidades de control reportadas. La auditoría deberá determinar si la medida correctiva tomada logra los resultados deseados o si el área auditada asumió la responsabilidad de no tomar ninguna medida correctiva.

Durante el desarrollo del seguimiento se aprovechará que, a juicio del auditor o superiores, se revisen aspectos adicionales cuando por su importancia lo ameriten o por su relación con los resultados de la auditoría, con el fin de tener una continuidad en la permanencia de la función de Auditoría en el proyecto o unidad auditada.

**C) Informe de resultados.**

Dependiendo de la importancia de los avances en la solución a las observaciones, la aplicación de las medidas correctivas, la desatención de los compromisos contraídos o cualquier otro factor que se juzgue relevante, se emitirá el informe del seguimiento con las características definidas en el punto **6.2 INFORME DE AUDITORÍA**.

Productos finales

- Resumen de observaciones.
- Informe de seguimiento.
- Carpeta de apoyo del informe de resultados.

# APLICACIÓN DE LA METODOLOGÍA EN UNA INSTITUCIÓN FINANCIERA

## 7.1 PLANEACIÓN DE LA REVISIÓN.

| No. | Actividad | Días |
|---|---|---|
| 1 | **Auditoría al ambiente de la red de Sistemas de una Institución Financiera.** | 28 |
| 2 | **Administración y operación.** | 5 |
| 3 | Entrevistas con las áreas de sistemas y usuaria | |
| 4 | Evaluación de funciones del administrador de la red | |
| 5 | Análisis de documentación | |
| 6 | **Uso y aprovechamiento de la plataforma.** | 5 |
| 7 | Evaluación de políticas y procedimientos para integración de aplicaciones. | |
| 8 | Evaluación de bitácora de mantenimiento | |
| 9 | Evaluación de contratos y cotizaciones | |
| 10 | Análisis de procedimientos de planeación, monitoreo y administración de la red | |
| 11 | Evaluación de pruebas de funcionamiento de la red. | |
| 12 | **Soporte y mantenimiento.** | 5 |
| 13 | Evaluación de políticas y procedimientos definidas para el administrador de la red | |
| 14 | Evaluación de niveles de servicio de la red y del administrador | |
| 15 | Análisis de documentación de apoyo | |
| 16 | **Seguridad física.** | 5 |
| 17 | Evaluación de políticas y procedimientos definidos. | |
| 18 | Análisis de contratos de seguros para los equipos | |
| 19 | Evaluación de controles implantados. | |
| 20 | Evaluación de bitácoras | |
| 21 | **Seguridad lógica.** | 5 |
| 22 | Evaluación de políticas y procedimientos para control de usuarios y facultades. | |
| 23 | Análisis de log's de auditoría | |
| 24 | Evaluación de asignación de niveles de acceso a funciones/facultades para usuarios. | |
| 25 | Evaluación de protección de archivos y programas. | |
| 26 | **Emergencia y contingencia.** | 3 |
| 27 | Evaluar políticas y procedimientos para respaldo de información y recuperación en y fuera de sitio. | |
| 28 | Evaluar los resultados de pruebas efectuadas | |
| 29 | Análisis de r de servicio comprometidos | |

## 7.2 DESARROLLO DE LA AUDITORÍA.

El desarrollo de la auditoria contempló los siguientes puntos:

**Administración y operación.**

- Entrevistas con los administradores de la red y con usuarios.
- Vigilancia de apego a políticas y procedimientos dictados por la institución.
- Análisis de funciones y responsabilidades del administrador de la red de acuerdo con la documentación oficial de la institución.
- Evaluación de documentación de soporte.
- Revisión de inventarios.
- Evaluación de estándares y planes de capacitación.

**Uso y aprovechamiento de la plataforma.**

- Evaluación del correcto aprovechamiento de recursos de hardware y software para detectar, entre otros aspectos, subutilización de espacio y obsolescencia en componentes instalados.

**Soporte y mantenimiento.**

- Análisis de políticas y procedimientos estipulados para el administrador de la red.
- Evaluación de los niveles de servicio negociados con el administrador de la red y con el área de soporte de la institución.

**Seguridad física.**

- Verificación de la existencia de controles automatizados para control de acceso a los equipos.
- Revisión de la existencia de políticas y procedimientos para control de acceso a equipos de cómputo en áreas restringidas.
- Evaluación de instalaciones eléctricas, cableado, ventilación e iluminación.
- Verificación de la existencia de bitácoras de acceso a áreas restringidas.
- Análisis de contratos de seguros para los equipos.

**Seguridad lógica.**

- Verificación de la existencia, funcionalidad y suficiencia de procedimientos automatizados y/o manuales para control de usuarios y facultades.
- Evaluación de la información emitida por el sistema, a fin de monitorear la actividad de los usuarios, sus perfiles y facultades.

- Verificación de la correcta definición y asignación de niveles de acceso de acuerdo a funciones, puestos y facultades del usuario.
- Evaluación de procedimientos para alta, mantenimiento y baja de claves de acceso, a fin de que se efectúen en apego a los procedimientos definidos por la institución.

**Emergencia y contingencia.**

- Verificación de la existencia, suficiencia y actualización de políticas y procedimientos para respaldo y recuperación de sistemas en sitio y fuera de sitio.
- Comprobación de la existencia de estrategia de pruebas que contemple su ejecución con cierta periodicidad y en diferentes escenarios.
- Evaluación del cumplimiento de la estrategia de pruebas y de los resultados obtenidos.
- Análisis de bitácoras de aplicación de medidas correctivas por recuperación parcial o total del sistema.
- Evaluación de niveles de servicio comprometidos con el negocio y su permanente actualización.

## 7.3 ELABORACIÓN DE INFORME.

**Antecedentes.**

Actualmente, en una área de sistemas de una institución bancaria, se cuenta con una red de área local cuya función principal es establecer comunicación con el equipo central de la institución para extraer información específica de una aplicación prioritaria y llevar a cabo el análisis, desarrollo y pruebas a los diferentes programas, transacciones y tablas propios de la aplicación, migrando estos datos posteriormente al equipo central e instalándolos en producción. Este procedimiento esta fundamentado en el **Offloading de Aplicaciones**[1].

La red está instalada bajo topología Ethernet y el sistema operativo con el que cuenta es Windows NT versión 4.0. Presenta 36 nodos, 85 usuarios y cuenta con dos responsables de la operación y mantenimiento de la misma. La paquetería instalada es la propia para realizar las funciones antes mencionadas.

[1] El Offloading de aplicaciones se fundamenta en la obtención de todos los componentes o programas fuente que se encuentran en ambiente de producción. Estos serán transmitidos desde el mainframe hasta el entorno PC-LAN, donde serán catalogados y compilados, asimismo, se transmiten los archivos de prueba de la aplicación para su ejecución en el nuevo ambiente.

En el ambiente PC-LAN se lleva a cabo el mantenimiento y desarrollo de las aplicaciones. Una vez depurados y probados los programas, serán transmitidos hacia el mainframe, donde serán catalogados y compilados para su ejecución, verificación de volúmenes de información e integración definitiva en la plataforma mainframe.

**Objetivo.**

Con la finalidad de fortalecer el Sistema de Control Interno del área de sistemas en cuestión, se presenta informe con observaciones y recomendaciones derivadas de la auditoria llevada a cabo a la red instalada en dicha área.

**Alcance.**

La revisión se llevó a cabo evaluando los siguientes aspectos:

- Administración y operación.
- Uso y aprovechamiento de la plataforma.
- Soporte y mantenimiento.
- Seguridad física.
- Seguridad lógica.
- Emergencia y contingencia.

**Procedimientos.**

Para llevar a cabo la evaluación, se aplicaron los siguientes procedimientos:

- Entrevistas con administradores y usuarios de la red.
- Explotación de información generada por la propia operación de la red y su interrelación con las aplicaciones de los usuarios.
- Aplicación de planeación de la revisión.

**Observaciones.**

Con base en la información proporcionada por el administrador de la red, así como trabajos realizados en sitio, se presentan las siguientes observaciones de acuerdo al alcance mostrado:

***Administración y operación.***

**Funciones del administrador de la red**

La Subdirección cuenta con los servicios del administrador de la red a través de un contrato de administración, soporte y mantenimiento que celebró con la compañía IDS Comercial, S.A. de C.V. Dicho contrato es renovado cada seis meses.

La Subdirección cuenta además con un administrador de red interno quien dirige, coordina y evalúa al administrador externo en todas las actividades que lleva a cabo.

De acuerdo al documento **Estrategia de Servicios de Red** de la Institución, en donde se detallan el Modelo de Perfiles, Funciones y Responsabilidades para Administradores de Servicios de Red y comentado con el *administrador de la red* quien se encuentra como responsable desde el 14 de octubre de 1996, se determina que las *funciones principales del administrador son:*

- *Administración local de la red. Apoyo a áreas corporativas.*

    1. Administración de fallas.
        - Monitoreo preventivo.
        - Detección y corrección de problemas.
        - Disponibilidad/Niveles de servicio.

    2. Administración de configuraciones.
        - Inventario de la red actualizado permanentemente.
        - Control de versiones y distribución de software.

    3. Administración de desempeño.
        - Estadísticas de uso.
        - Planeación de capacidad.

    4. *Administración de la Seguridad.*
        - Respaldo y recuperación.
        - Passwords, privilegios y acceso a recursos.
        - Detección y limpieza de virus en archivos.

Además de las funciones detalladas, el encargado de la administración de la red tiene a su cargo las siguientes actividades:

- Dar de alta nuevos usuarios y accesos a los recursos del servidor.
- Proporcionar soporte, *asesoría, pláticas, capacitación y apoyo a los usuarios* de la infraestructura instalada.
- *Dar soporte y mantenimiento al servidor y a las workstations instaladas.*
- Hacer solicitudes de requerimientos de servicio para el soporte interno y/o externo en áreas de oportunidad detectadas.
- Administrar el almacenamiento y respaldo de información en el servidor.
- Administrar los datos contenidos en las tablas DB/2 de cada workstation.
- Controlar la actualización de componentes de cada usuario en el servidor.

**Fallas**

Ausencia de un *formato estándar para notificación de fallas en la red o en los* equipos, lo que ha provocado que el administrador no registre los reportes de falla.

Sin embargo, toma nota de los problemas en su bitácora diaria de actividades, lo que implica no contar con un control de problemas formal.

Por otro lado, el administrador de la red elaboró un formato para el reporte de problemas de software, sin embargo, desde el 11 de enero de 1997 a la fecha de la auditoría ya no se registran, debido a diversos cambios estructurales en la Subdirección.

Sin embargo, al analizar los reportes de problema registrados en la bitácora, se observó que se documentaba la información suficiente para control, seguimiento y solución.

**Inventario**

*Hardware*

El inventario de hardware proporcionado por el administrador de la red se encontró actualizado a la fecha de la auditoría y apegado a los estándares establecidos. **(Véase anexo I, pág. 181)**.

*Software*

De acuerdo a la información proporcionada por el administrador de la red, el inventario de software instalado en los equipos de cómputo se encuentra debidamente actualizado. **(Véase anexo II, págs. 182 - 184)**.

El software adquirido y la distribución de éste y de los archivos de usuarios, se encuentra distribuido en seis particiones del disco duro. Sin embargo, en algunos subdirectorios del servidor se detectó la existencia de software no autorizado, mismo que no se encuentra dentro del inventario proporcionado ni tampoco apegado a estándares. **(Véase anexo III, pág. 185)**.

**Estándares**

La definición y estructuración del nombre y dominio del servidor y nombres de impresoras, están dadas por uso / aplicación, tal como está indicado en el documento Políticas de Instalación.

Con relación a los nombres de los grupos definidos en el servidor, ninguno se apega a estándares, además de que existen algunos de ellos que no contienen ningún usuario y/o no son utilizados. **(Véase Anexo IV, pág. 186)**.

Los nombres de los subdirectorios que contienen paqueteria están bajo estándares, sin embargo, los subdirectorios de usuario de la partición **H** presentan anomalías a este respecto, ya que de acuerdo a los nombres que tienen

asignados, no es posible identificar de primera instancia al responsable de la información contenida en los mismos. Solamente uno de ellos presenta como nombre el user-id del responsable, sin embargo, esta persona ya no labora en la institución.

Las direcciones IP asignadas se encuentran bajo la estructura estándar definida para la red de la Institución.

A los archivos CONFIG.SYS, AUTOEXEC.BAT y PROTOCOL.INI contenidos en el servidor y en las workstations, se les han cambiado los atributos a sólo lectura y oculto (read only y hidden), tal como se estipula en las **Políticas de Instalación en Estaciones de Trabajo**.

**Capacitación**

El administrador de la red fue capacitado en la administración de servidores Windows NT, servidores OS/2, servidores Lan Manager y estaciones de trabajo, asimismo se le capacitó en lo referente a la instalación y actualización de hardware en el servidor, por lo que para cualquier cambio y/o instalación de nuevos dispositivos o nuevo software, él es quién se encarga de llevarla a cabo bajo la supervisión del administrador interno.

El programa de capacitación del administrador de la red se compone de varios cursos de actualización semestrales, los cuales son impartidos por personal de su misma empresa.

El administrador interno no cuenta con un programa de capacitación definido, por lo que su campo de acción dentro de la operación de la red se ve disminuido en caso de que el otro administrador no estuviera disponible.

***Uso y aprovechamiento de la plataforma.***

El intercambio de información (archivos, programas, tablas, etc.) entre el equipo mayor y los diferentes usuarios de la red, se realiza con ayuda del administrador, empleando para ello la herramienta **MicroFocus XCHANGE**, misma que se encuentra inventariada y con licencia autorizada de uso.

En el servidor, el administrador ha creado subdirectorios para cada usuario con el fin de almacenar información correspondiente a las migraciones de datos que se lleven a cabo, o bien datos correspondientes a los diversos proyectos de la Subdirección. Sin embargo, estos subdirectorios no son depurados con regularidad, hecho que provoca contar con mucho espacio desperdiciado en el disco duro.

A este respecto, existen 11 subdirectorios que no han sido utilizados desde hace mes y medio de acuerdo con la fecha de la realización de la auditoria. **(Véase Anexo V, págs. 187 - 188)**.

***Soporte y mantenimiento.***

Dentro de las funciones estipuladas en el contrato del administrador externo, se encuentran el soporte y mantenimiento a la red, para lo cual cuenta con la documentación y manuales requeridos. Cabe hacer notar que no se ha establecido un calendario formal de mantenimiento para equipos y dispositivos de la red.

En cuanto a solicitudes de soporte y mantenimiento que se le hacen al administrador de la red, solamente se registran y documentan un 10% de ellas, ya que el resto se llevan a cabo verbalmente entre el administrador de la red y el solicitante y en algunas ocasiones es notificado el administrador interno. Todo esto se realiza sin que quede rastro alguno del requerimiento y sin el visto bueno del administrador interno.

Por otro lado, el administrador interno no cuenta con el manual de Políticas de Instalación actualizado. Esta situación ha provocado que se desconozcan las políticas evolutivas en cuanto a instalación, configuraciones, actualizaciones y nomenclaturas estándar.

Finalmente, a la fecha de la auditoria, no se habian estipulado formalmente los niveles de servicio para la red, sin embargo, de acuerdo a la opinión de los usuarios con respecto a los servicios de mantenimiento proporcionados por el área de soporte de la institución, han sido satisfactorios.

***Seguridad física.***

El sitio donde se encuentra ubicado el servidor carece de control de acceso, debido a que no existe un sitio específico para la operación del mismo. El servidor se encuentra instalado dentro del mismo módulo donde labora todo el personal del área. A este módulo tienen acceso libre, además de los empleados, personal ajeno a la Dirección de Sistemas, personal usuario, personal de vigilancia y de limpieza.

Las workstations se encuentran también al alcance de cualquier persona, ya que al igual que el servidor, no cuentan con un sitio especifico con medidas de seguridad para salvaguarda física.

El almacenamiento y custodia de manuales, diskettes, discos compactos, cartuchos de respaldo y documentación en general de la red y su operación, no

cuenta con medidas de seguridad, ya que estos elementos se encuentran al alcance de cualquier persona sin que se tenga un control de préstamo.

Las situaciones mencionadas han provocado lo siguiente:

- Suspensión temporal de la operación del servidor debido a un shutdown accidental por personal ajeno a la Subdirección, impactando el servicio durante tres horas.
- Extravío de dos cartuchos con información respaldada.
- Extravío de una caja con 8 cartuchos vírgenes para respaldo de información.
- Extravío de un teclado de workstation.
- Sustitución no programada de cuatro monitores de workstation por monitores de equipos ajenos a la red.
- Reconfiguración de dos workstations por eliminación de archivos vitales.
- Descomposturas graves en teclados y monitores de las workstations.
- Dispersión de manuales de operación en todo el módulo.

El lugar cuenta con alarmas para detectar fuego, sin embargo, solo se cuenta con un extinguidor que resulta insuficiente debido a la cantidad de equipo y papelería existente (listados, toner de impresoras, manuales, etc.).

Cabe mencionar que el extinguidor no se encuentra a la mano, ya que en caso de ser utilizado, es necesario salir del módulo y dirigirse al pasillo para poder llegar hasta él.

Por otro lado, las instalaciones eléctricas, el cableado y la iluminación del lugar son las adecuadas, no siendo así lo referente a la ventilación, ya que no se cuenta con los equipos idóneos para su operación.

Cabe mencionar que la única ventilación que se proporciona, se da a través de un ventilador, mismo que se encuentra colocado encima de un escritorio cercano al servidor.

Por último, a la fecha de la auditoría no se habían celebrado contratos con ninguna compañía aseguradora que ampare los equipos y dispositivos de la red en caso de desastre.

***Seguridad lógica.***

Existen 85 claves de usuario dadas de alta en el servidor **(véase Anexo VI, pág. 188)**, de las cuales se desprende el siguiente análisis:

- Solamente 51 de ellas se apegan a los estándares de la nomenclatura para asignación de user-id.

- Existen 13 usuarios con perfil de administrador de la red, donde 2 de ellos cuentan con 2 user-id diferentes, 5 no pertenecen a la Subdirección, 2 no deben tener este perfil de acuerdo a sus funciones, aun siendo integrantes de la Subdirección y 1 no cuenta con la información suficiente para determinar quien es el responsable.
- Existen 6 claves con perfil de usuario, mismas que no tienen asignado formalmente a un responsable.
- Se detectaron 25 claves con perfil de usuario, mismas que pertenecen a personal que ya no labora en la Subdirección (personal interno y externo).
- Existen 3 personas quienes tienen asignadas dos claves diferentes con perfil de usuario y una más con tres claves de las mismas características.
- Se detectaron las siguientes anomalías en algunos de los atributos de todos los usuarios de la red:

| | |
|---|---|
| Expiración del user-id. | Nunca |
| Expiración del password. | Nunca |
| Uso máximo de espacio en disco duro. | Ilimitado |

Los atributos especificados para los subdirectorios del servidor se encuentran apegados a estándares, sin embargo, a la fecha de la auditoría no se había delimitado el número máximo de usuarios que pueden accesar de manera concurrente a los subdirectorios con paquetería y aplicaciones de más demanda.

La asignación de las workstations a usuarios no se lleva de forma administrada, ya que no hay priorización para uso de las mismas. Algunos usuarios las emplean por tiempos prolongados sin dar oportunidad a los demás de aprovecharlas, permaneciendo en ocasiones firmados en su sesión aún y cuando ellos no se encuentren presentes.

El servidor y las workstations cuentan con un password de arranque personalizado. El utilizado en el servidor sólo lo conocen el administrador de la red, el administrador interno y el subdirector del área y el de las workstations es conocido por todos los usuarios de la red.

Sin embargo, los passwords de encendido de las workstations no se han cambiado desde que éstas se instalaron.

El servidor y las workstations se inhabilitan después de no recibir instrucción alguna por un periodo de tres minutos.

Por otro lado, el administrador de la red inhabilitó el uso de las unidades de discos de 3½" tanto del servidor como de las workstations, con la finalidad de evitar la carga de software no autorizado o copia ilegal de archivos del disco duro.

***Emergencia y contingencia.***

La unidad de cinta para respaldo de información se encuentra dañada desde enero de 1998, hecho que ha provocado que los respaldos se hagan a través de la unidad de cinta de otro servidor ajeno a la red.

Por otro lado, a la fecha de la auditoría la red no se encontraba alineada al Procedimiento de Emergencia y Contingencia Institucional. Esto se refleja en el hecho de que no se cuenta con procedimientos de respaldo de información fuera de sitio, por lo que en caso de alguna contingencia, no se estaría en posibilidad de recuperar el servicio y/o información.

Finalmente, se cuenta con procedimientos que apoyan al administrador de la red a restablecer el servicio en caso de que el servidor sufra alguna "caída" no imputable a una contingencia.

**RECOMENDACIONES.**

***Administración y operación.***

<u>Fallas</u>

Establecer y difundir un formato estándar para control de fallas en la red, el cual se sugiere que contenga:

- Fecha y hora de la falla.
- Fecha y hora de atención y solución.
- Breve descripción de la falla.
- Impacto ocasionado.
- Descripción de la solución.
- Nombre de la persona que reporta la falla.
- Nombre y firma del administrador.
- Vo. Bo. del administrador interno de la red una vez arreglada la falla.

Desarrollar y difundir entre todos los usuarios el uso del formato para reportar problemas con el software de la red mediante correos electrónicos.

Implementar bitácora automatizada de fallas de hardware y software de la red para mantener la historia de las mismas e identificar aquellas que sean repetitivas, a fin de establecer procedimientos de mejora continua en la operación.

**Inventario**

Normalizar en cuanto a licencias de software se refiere, toda aquella paqueteria que sea requerida para la operación de la red.

De acuerdo a lo estipulado en las Políticas de Instalación, se deberán eliminar todos los juegos que se tienen instalados en el servidor, ya que representan un foco de distracción para el administrador y los usuarios, además de proyectar una mala imagen en el desempeño del personal de la Subdirección.

**Estándares**

Llevar a cabo los cambios pertinentes a los grupos del servidor conforme a los estándares establecidos en el manual de Políticas de Instalación.

Depurar aquellos grupos que se encuentren vacios o que no son utilizados, previa evaluación y autorización del administrador interno de la red y del subdirector.

Establecer procedimientos internos para asignación de nombres a los diferentes subdirectorios de usuarios de la partición **H**, a fin de identificar de manera más rápida y eficiente a los responsables de la información contenida en los mismos.

**Capacitación**

Determinar las necesidades actuales de instrucción técnica para el administrador interno de la red y establecer un plan de capacitación que se apegue a las necesidades requeridas.

***Uso y aprovechamiento de la plataforma.***

Establecer, difundir y poner en práctica políticas internas de depuración y vigencia de información para los subdirectorios de usuarios de la red, con el fin de mantener únicamente los datos que sean útiles y eliminar la información obsoleta. De esta manera, se optimiza y administra mejor el espacio en el disco duro del servidor.

Establecer y responsabilizar a los administradores sobre un sistema de monitoreo permanente de la actividad de los subdirectorios del servidor.

***Soporte y mantenimiento.***

Definir y difundir los niveles de servicio para la red con el objeto de comprometerlos con los administradores y los usuarios.

Elaborar un procedimiento administrado que permita medir y calificar periódicamente los niveles de servicio que se establezcan, a fin de llevar la operación de la red hacia un proceso de mejora continua.

Establecer un procedimiento para atención de requerimientos de usuarios contando con el visto bueno del administrador interno, con el fin de evitar malos manejos de la información, así como dejar rastro de las actividades realizadas en caso de algún problema.

Dotar a los administradores de la red del manual actualizado de Políticas de Instalación, así como establecer periodos de revisión del mismo, con el fin de mantenerse apegado a los estándares establecidos.

***Seguridad física.***

Con el fin de mantener la integridad de los equipos y periféricos de la red:

- Diseñar e instalar un espacio dedicado a la operación del servidor, al que solo tengan acceso los administradores y el subdirector, implementando para ello un dispositivo electrónico que valide la identidad de dichas personas.
- Diseñar e instalar un espacio dedicado a la operación de las workstations, al que solo tengan acceso los usuarios autorizados de la red, implementando para ello un dispositivo electrónico que valide la identidad de dich personas.
- Los espacios dedicados para la operación de servidor y workstations, deberán contar con todas las instalaciones necesarias para:

  - Detectar y sofocar incendios.
  - Monitorear temperatura y humedad.
  - Proporcionar ventilación y/o iluminación adecuadas.
  - Mantener en óptimas condiciones las instalaciones eléctricas.
  - Asegurar que no se extraigan manuales o equipos periféricos.

- Diseñar e instalar muebles específicos para almacenamiento de manuales de operación de la red, de políticas y procedimientos y de software, diskettes, discos compactos, cartuchos de respaldo, etc. Estos muebles deberán contar con las medidas de seguridad que permitan proteger los elementos mencionados contra malos manejos y/o destrucción.
- Adquirir pólizas de seguro en caso de desastre para todos los equipos y dispositivos de la red con compañías aseguradoras.

***Seguridad lógica.***

Con el fin de mantener la integridad de la información:

- Completo apego a los estándares para asignación de user-id's, de acuerdo a lo estipulado en el manual de Políticas de Instalación.
- Reasignar perfiles a los user-id's de usuarios independientes a las funciones del administrador.
- Eliminar todos aquellos user-id's de usuarios internos y de proveedores que ya no laboren en la Subdirección.
- Otorgar únicamente un user-id por persona de acuerdo a lo estipulado en el manual de Políticas de Instalación.
- Implementar un procedimiento automatizado para expiración de user-id's y password de usuarios, así como establecer en los atributos de los usuarios el espacio máximo de utilización del espacio en disco duro de acuerdo a las necesidades de los usuarios.
- Desarrollar y difundir un procedimiento automatizado para asignar sesiones de trabajo y períodos de utilización en las workstations.
- Delimitar el número máximo de usuarios que accesen de manera concurrente a la paquetería de la red.
- Definir y establecer periodos para cambio de passwords en las workstations.

***Emergencia y contingencia.***

Reparar y poner en funcionamiento la unidad de cinta para respaldo de información, a fin de evitar pérdida y malos manejos de la misma al efectuar los respaldos por medio de otro servidor ajeno a la red.

Definir y establecer entre los administradores procedimientos periódicos de respaldo de información fuera de sitio, con el fin de proteger la información generada contra posibles pérdidas o malos manejos.

Alinear la operación de la red al Procedimiento de Emergencia y Contingencia Institucional, a fin de estar en posibilidades de recuperar el servicio y/o información ante cualquier eventualidad.

Asimismo, se recomienda integrar a la red en los planes de pruebas periódicas de contingencia institucional, contemplando a su vez, los planes de las diferentes aplicaciones con las que se tiene interfase e involucrando a los usuarios pertinentes para llevar a cabo las acciones que se detallen en los planes mencionados.

Eduardo Gomora Ramírez

Luis Miguel Sánchez González

Armando Godínez Díaz

Juan Molina Pérez

José Ramón Morales González

## ANEXO I

**Inventario de hardware proporcionado por el administrador de la red.**

**Servidor (Compaq Proliant 2000).**
**Cantidad: 1**

Procesador Pentium Intel 100 MHz.
Memoria RAM de 128 MB.
Disco duro de 11.4 GB.
Unidad de respaldo cinta 8mm Hewlett Packard.
Unidad de CD-ROM Compaq CR-503BCQ.
Unidad de Disquetes 3½" de 1.44 Mb.
Monitor Compaq 1024 14" SVGA.
Tarjetas de red Compaq Netflex-3 Network Controller 3Com TokenLink.
Unidad de Respaldo de corriente (UPS).

**Estaciones de Trabajo.**
**Cantidad: 6**

HP Vectra N2 486 / 66 Mhz.
Memoria RAM de 16 MB.
Tarjeta de red Ethernet RJ-45.
Disco Duro de 1GB.

**PC-Lites.**
**Cantidad: 30**

IBM 386 / 33 Mhz.
Memoria RAM de 4 MB.
Tarjeta de red Ethernet RJ-45.
Disco Duro de 120 MB.
Centinela de Hardware para Cobol II.

**Total: 37 equipos.**

## ANEXO II

**Inventario de software proporcionado por el administrador de la red.**

***Servidor (Compaq Proliant 2000).***

**Windows NT.**
Windows NT V.4.0 con Windows 95.
Partición de arranque tipo FAT de 211 MB.
El resto de particiones tipo HPFS.

**LAN Server.**
LAN Server V. 4.0.
Driver Token Ring instalado.
Driver Ethernet instalado.
Protocolo TCP/IP instalado.
Protocolo NETBIOS sobre TCP/IP instalado.
*Default Router configurado.*

**LAN Requester.**
LAN Requester V. 4.0.
Driver Ethernet instalado.
Protocolo TCP/IP instalado.
Protocolo NETBIOS sobre TCP/IP instalado.
Default Router configurado.

**DB2/2.**
DB2/2 V. 1.20.1
Query Manager instalado.
DB2/2 On Line Help instalado.

**ADMVS.**
ADMVS V3.1.12 instalado.
Microfocus CICS Option V. 3.043 instalado.
Microfocus CICS Option V. 3.050 instalado
Host Compatibility Option V. 2.0.20 instalado.
SPF/PC V. 4.0 instalado.

## ANEXO II (Continuación)

**Communications Manager/2.**
Servicios APPC.
Servicios LU 6.2.
Sesiones 3270 definidas.

**MicroFocus X CHANGE V. 2.1.1**

Estaciones de Trabajo.

**Windows NT.**
Windows NT V.4.0 con Windows 95.
Partición de arranque tipo FAT de 125 MB.
El resto de particiones tipo HPFS.

**LAN Requester.**
LAN Requester V. 4.0.
Driver Ethernet instalado.
Protocolo TCP/IP instalado.
Protocolo NETBIOS sobre TCP/IP instalado.
Default Router configurado.

**DB2/2.**
DB2/2 V. 1.20.1
Query Manager instalado.
DB2/2 On Line Help instalado.

**ADMVS.**
ADMVS V3.1.12 instalado.
Microfocus CICS Option V. 3.043 instalado.
Microfocus CICS Option V. 3.050 instalado.
Host Compatibility Option V. 2.0.20 instalado.
SPF/PC V. 4.0 instalado.

**Communications Manager/2.**
Servicios APPC.
Servicios LU 6.2.
Sesiones 3270 definidas.

## ANEXO III

**Distribución de software y archivos de usuario en el disco duro.**

| Partición | Espacio asignado | Contenido |
|---|---|---|
| C: | 206 MB | Sistema operativo y archivos de arranque. |
| D: | 810 MB | Software de red, bibliotecas de paso y paqueteria |
| E: | 4.2 GB | Bibliotecas de componentes y Base de Inspect. |
| F: | 1.03 GB | Archivos y directorios de usuario. |
| G: | 1.02 GB | Workstation modelo, archivos y directorios de usuario. |
| H: | 2.13 GB | Archivos y directorios de usuario. |
| I: | 2.05 GB | Archivos y directorios de usuario. |
| J: | - o - | Unidad asignada al CD-ROM. |

**Software no autorizado ni apegado a estándares.**

| Partición | Subdirectorio | Software | Tipo |
|---|---|---|---|
| E | \Inspect | Base de datos Inspect | Aplicación |
| F | \PARTCNS<br>\PYIDS<br>\Quake | Quake | Juego |
| H | \Alex | Pool<br>SB<br>Stars<br>Ugn<br>Winbowl | Juego<br>Juego<br>Juego<br>Juego<br>Juego |
| | \EDS<br>\Admon<br>\Alfonso<br>\Junio | Arquero<br><br>PKZIP | Juego<br><br>Aplicación |
| | \Riesgos | PKZIP | Aplicación |

## ANEXO IV

**Grupos definidos en el servidor.**

| Nombre | Descripción | Estatus | No. usuarios |
|---|---|---|---|
| ADMINS | Grupo de administración. | Activo | 13 |
| ANDERSEN | Grupo de trabajo de Andersen Consulting, S.A. de C.V. | No se utiliza | 2 |
| BANCO | Usuarios Banco. | Activo | 70 |
| BANCOPH | Usuarios Banco Prestamos. | Activo | 45 |
| BANCOPM | Usuarios Banco Promotores. | Activo | 5 |
| IDS | Grupo de trabajo para IDS Comercial, S.A. de C.V. | No se utiliza | 3 |
| ROBOHELP | Usuarios Banco. | Activo | 8 |
| SOFTTEK | Grupo de trabajo para SOFTTEK, S.A. de C.V. | No se utiliza | 0 |
| TECNOSYS | Grupo de trabajo para TECNOSYS, S.A. de C.V. | No se utiliza | 0 |
| USERS | Usuarios Banco. | Activo | 72 |
| USGAAP | Usuarios Proyectos. | No se utiliza | 8 |

## ANEXO V

**Subdirectorios con anomalías contenidos en el servidor.**

| Nombre | Contenido | Tamaño (Mb.) | Fecha de creación | Fecha de última modificación |
|---|---|---|---|---|
| ALEX | Subdirectorios: 7<br>Archivos: 129 | 7.11 | 30 de octubre de 1997. | 13 de mayo de 1998. |
| ALTMRA | Subdirectorios: 0<br>Archivos: 2 | 3.10 | 28 de octubre de 1997. | 11 de noviembre de 1997. |
| ANIBAL | Subdirectorios: 2<br>Archivos: 13 | 14.0 | 28 de octubre de 1997. | 25 de marzo de 1998. |
| ARCHADEL | Subdirectorios: 0<br>Archivos: 15 | 1.12 | 17 de noviembre de 1997. | 17 de noviembre de 1997. |
| COTA | Subdirectorios: 0<br>Archivos: 0 | 0 | 27 de marzo de 1998. | 14 de mayo de 1998. |
| EDS | Subdirectorios: 29<br>Archivos: 751 | 183.0 | 28 de octubre de 1997. | 17 de marzo de 1998. |
| ENRIQUE | Subdirectorios: 0<br>Archivos: 31 | 48.4 | 28 de octubre de 1997. | 25 de febrero de 1998. |
| HRH | Subdirectorios: 0<br>Archivos: 3 | 0.36 | 28 de octubre de 1997. | 28 de octubre de 1997. |
| LAOCA | Subdirectorios: 2<br>Archivos: 86 | 2.12 | 28 de octubre de 1997. | 8 de mayo de 1998. |
| LIPP | Subdirectorios: 14<br>Archivos: 244 | 29.2 | 28 de octubre de 1997. | 14 de abril de 1998. |
| LMSG | Subdirectorios: 6<br>Archivos: 58 | 7.68 | 17 de marzo de 1998. | 12 de mayo de 1998. |
| MARTIN | Subdirectorios: 0<br>Archivos: 3 | 35.6 | 28 de octubre de 1997. | 6 de mayo de 1998. |
| MEJIA | Subdirectorios: 0<br>Archivos: 26 | 56.8 | 28 de octubre de 1998. | 15 de mayo de 1998. |
| MEXMSME | Subdirectorios: 0<br>Archivos: 1 | 1.87 | 28 de octubre de 1997. | 28 de octubre de 1997. |
| MONY | Subdirectorios: 0<br>Archivos: 10 | 7.58 | 11 de febrero de 1998. | 3 de abril de 1998. |
| POLANSKY | Subdirectorios: 0<br>Archivos: 2 | 0.42 | 19 de noviembre de 1997. | 23 de diciembre de 1997. |
| RIESGOS | Subdirectorios: 0<br>Archivos: 5 | 3.46 | 13 de mayo de 1998. | 14 de mayo de 1998. |
| TERE | Subdirectorios: 5<br>Archivos: 59 | 14.5 | 28 de octubre de 1998. | 13 de mayo de 1998. |

La tabla anterior arroja las siguientes cifras: 416.32 Mb. de espacio ocupado por los subdirectorios de algunos de los usuarios de la red, 75 sub-subdirectorios y 1,438 archivos de diferente tipo.

## ANEXO VI

**Claves de usuario actuales en el servidor (Datos a la fecha de la auditoría).**

| | | |
|---|---|---|
| ADMDEM | EXT496 | MEXDLS |
| ADMDERG | EXT502 | MEXECA |
| ADMMC[illegible] | EXT584 | MEXFRV |
| ADMOCC | EXT646 | MEXFSMO |
| B0160841 | EXT647 | MEXGGGA |
| B0194659 | EXT712 | MEXGRH |
| B0336573 | EXT713 | MEXGSFO |
| B0338199 | EXT788 | MEXHRH |
| B0456660 | EXT790 | MEXHRM |
| B0518048 | EXT810 | MEXJAFE |
| B0519251 | EXT857 | MEXJFF |
| B0520507 | EXT858 | MEXJLP |
| B0524822 | EXT918 | MEXJMPU |
| B0529763 | EXT956 | MEXJPB |
| B0531116 | GDB2DA | MEXLSG |
| B0532262 | GDB2DB | MEXMCCA |
| B0535760 | GDB2DE | MEXMIJ |
| B0536107 | HIPOTEC-SRV | MEXMJC |
| B0559372 | IBM-APP | MEXMRLO |
| B0560084 | MEXABM | MEXMSME |
| CBANCO | MEXACACO | MEXMVGO |
| EXT160 | MEXACZ | MEXMVMA |
| EXT164 | MEXAFB | MEXRCJA |
| EXT233 | MEXAGR | MEXSDF |
| EXT259 | MEXAHG | MEXSRE |
| EXT261 | MEXAHU | TIDSRGS |
| EXT322 | MEXAMAL | USERID |
| EXT323 | MEXCVS | |
| EXT363 | MEXDJC | |

# CONCLUSIONES

En el presente trabajo se ha mostrado el beneficio que representa contar con una red de área local como elemento vital en la evolución de las organizaciones y desarrollo de sistemas de información.

Implantar una red LAN en las organizaciones permite incrementar la productividad de las empresas en cuestión de información, mejorar los procesos de negocio y operativos, así como brindar nuevas perspectivas de crecimiento estratégico, todo para cumplir con un fin común: procesar y utilizar la información generada por los diferentes entes de la organización como una herramienta eficiente para la toma de decisiones.

Sin embargo, es primordial invertir eficientemente en la infraestructura que se instale, ya que frecuentemente se realizan análisis y planeaciones que no reflejan las necesidades prioritarias de manejo y uso de información en las organizaciones, ni se dimensionan las metas a cubrir a mediano y largo plazo.

Se debe de tomar en cuenta que este trabajo, consideró los principales aspectos que abarca una auditoría en informática al ambiente de redes de área local, proporcionando un plan de trabajo y guías de auditoría que mejoren el control interno con la finalidad de hacer más eficiente el uso de los recursos y brindar una seguridad al negocio.

A este respecto, es de suma importancia mencionar que han sido tomadas en cuenta y aplicadas las recomendaciones plasmadas en el informe, poniendo especial énfasis en los puntos de control referidos a la seguridad y los planes de contingencia y emergencia.

Se logró que se llevasen a cabo acciones para normalizar todas las claves de usuario activas en el servidor de la red, eliminando aquellas que ya no están vigentes. También se pusieron en marcha varios proyectos que permitirán optimizar la seguridad física y lógica de todos los componentes de la red, así como mejorar los planes de contingencia y emergencia e integrar a la red en los planes de Emergencia y Contingencia Institucional.

Cabe mencionar que las recomendaciones incluidas en el informe, fueron evaluadas en conjunto con los administradores y el dueño de la red, resultando ser viables y costeables de acuerdo al presupuesto asignado para mejora continua en la operación de la misma.

El desarrollo y recopilación de la información se realizó por inquietud grupal, pretendiendo servir de apoyo a la Dirección de Sistemas de la Institución en donde

se llevó a cabo la auditoría, así como también en la operación de redes de área local que se encuentren instaladas o bien, que estén en planes de instalación.

De esta manera, también se apoya a los ingenieros interesados en este ramo, ya que no existen técnicas y herramientas bien definidas para auditar específicamente este ambiente.

Por otro lado, el aplicar los conocimientos que fueron adoptados durante la carrera y la experiencia laboral adquirida, nos permitió contar con un panorama más amplio sobre el tema desarrollado, logrando discernir entre diversas situaciones que se presentaron durante la aplicación de la auditoría.

Por todo lo anterior, concluimos que actualmente en México la Auditoría en Informática sólo existe en las grandes empresas, por esto, un Ingeniero en Computación, quien posiblemente será el encargado de alguna Dirección o Subdirección de Sistemas en la que se use un ambiente de red de área local, deberá manejar los conceptos de auditoría en informática que lo apoyarán a realizar una productiva y adecuada administración y así poder implementar esta función en las pequeñas y medianas empresas sin afectar los costos de operación de las mismas.

# APÉNDICES

## APÉNDICE 1. GUÍA DE AUDITORÍA.

Se ha preparado esta guía con el objetivo de brindar apoyo a los profesionales que se desenvolverán en este medio, poniendo especial énfasis en los controles que permiten reunir evidencias para generar recomendaciones acerca del buen funcionamiento de la entidad auditada.

### 1. Datos generales.

1.1 Proporcionar los siguientes datos:

a) Nombre de Depto./Entidad. _____
b) Dirección. _____
c) Teléfono. _____

¿ Cuántas redes existen en el Departamento/Entidad ?

¿ Cuántos servidores tiene cada red ?

| | | | |
|---|---|---|---|
| Red 1 | _____ | Red 6 | _____ |
| Red 2 | _____ | Red 7 | _____ |
| Red 3 | _____ | Red 8 | _____ |
| Red 4 | _____ | Red 9 | _____ |
| Red 5 | _____ | Red 10 | _____ |

1.2 Proporcionar los siguientes datos por servidor.

| Nombre del servidor | Red a la que Pertenece | No. de usuarios dados de alta | Nombre del administrador |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**2. Configuración de la red.**

**Nota**: Por cada una de las redes que se indicaron en el punto 1.1, requisitar esta sección.

2.1 Proporcionar los siguientes datos como administrador de la red.

Nombre o número de la red. _____
Puesto según tabulador. _____
Antigüedad en el puesto. _____
Experiencia como administrador de redes (años). _____
Tabulador y sueldo mensual. _____

Nivel máximos de estudios.

1. Profesional ☐
2. Preparatoria ☐
3. Secundaria ☐
4. Otro ☐ Especificar. _____

2.2 Indicar que topología tiene la red en donde se encuentra el servidor.

Arcnet ☐ Ethernet ☐ Token Ring ☐

2.3 Indicar cuántas estaciones de trabajo están conectadas a la red.

Más de 80 ☐ de 61 a 80 ☐ de 41 a 60 ☐

de 21 a 40 ☐ de 1 a 20 ☐

2.4 ¿ Cuentan con disco duro las estaciones de trabajo ?

Si ☐ No ☐

2.4.1 ¿ Qué porcentaje representan del total ?

Más de 80 % ☐ de 61 % a 80 % ☐ de 41 % a 60 % ☐

de 21 % a 40 % ☐ de 0 % a 20 % ☐

2.4.2 ¿ Qué capacidad tienen los discos duros de las estaciones de trabajo ?

Más de 110 Mb ☐ Menos de 110 Mb ☐

2.5 ¿ La red está conectada a otra red ?

Si ☐ No ☐

2.6 ¿ La red está conectada a un Host ?

Si ☐ No ☐

2.7 ¿ Cómo están conectados los componentes de comunicación al Host ?

Serie ☐ Paralelo ☐

**3. Uso del servidor.**

**Nota**: Por cada una de las redes que se indicaron en el punto 1.1, requisitar esta sección.

3.1 Proporcionar el nombre del servidor a evaluar. _____

3.2 Indicar los datos del servidor.

Marca. _____ Nombre de sistema operativo y versión. _____
Modelo. _____ Capacidad de disco duro. _____

3.3 El servidor se usa como:

Servidor de archivos ☐ Servidor de comunicaciones ☐

Servidor de bases de datos ☐

3.4 ¿ Qué tipo de servicio presta ?

Comunicación con la red de la empresa. ☐

Manejo de las operaciones del usuario. ☐

Aplicación con afectaciones contables. ☐

Desarrollo de sistemas. ☐

Uso departamental. ☐

Correo electrónico / fax. ☐

Otro. ☐ Especificar. _____

3.5 Número de usuarios del servidor. _____

3.6 ¿ Qué tipo de usuarios trabajan con el servidor ?

Programadores ☐ Usuarios de paquetes ☐

Operadores de aplicaciones ☐ Otros ☐ Especificar. _____

3.7 Fecha de inicio de funcionamiento. _____

3.8 ¿ Se tiene instalado en el servidor algún software para protección de virus ?

Si ☐ Especificar. _____ No ☐

3.9 ¿ Se realizan revisiones en la red para detectar paquetería no autorizada ?

Si ☐ No ☐

3.10 ¿ Existe control de acceso en el área donde se encuentra el servidor ?

Si ☐ No ☐

3.11 ¿ En que tipo de área de trabajo se encuentra el servidor ?

Pública ☐ Cubículo aislado ☐ Oficina privada ☐

Acceso restringido ☐ Otra ☐ Especificar. _____

3.12 ¿ El servidor se encuentra cerca de una ventana ?

Si ☐ No ☐

3.13 ¿ Existen señalizaciones preventivas en el área donde se encuentra el servidor, por ejemplo: no fumar, no consumir alimentos ni bebidas, etc. ?

Si ☐ No ☐

3.14 ¿ Se cuenta con extinguidores en el área donde se encuentra el servidor ?

Si [ ] No [ ]

3.15 ¿ De qué tipo ?

Polvo químico [ ] Bióxido de carbono [ ] Gas halón [ ]

**4. Respaldo de información.**

4.1 ¿ Se cuenta con una unidad de respaldo de información ?

Si [ ] No [ ]

4.2 ¿ Se llevan a cabo respaldos de información del disco duro ?

Si [ ] No [ ]

4.3 ¿ Con qué frecuencia se respalda la información ?

Mensual [ ] Diaria [ ]

Semanal [ ] Otra [ ] Especificar. _____

4.4 ¿ Las cintas y/o discos de respaldo del servidor se encuentran en un lugar donde sólo tengan acceso a personas autorizadas ?

Si [ ] No [ ]

4.5 ¿ Los dispositivos de respaldo se encuentran identificados con una etiqueta que contenga fecha de su realización, contenido y versión ?

Si [ ] No [ ]

4.6 ¿ Se cuenta con un calendario de respaldo y se mantiene actualizado ?

Si [ ] No [ ]

4.7 ¿ Existen políticas para la administración de espacio en disco ?

Si [ ] No [ ]

4.8 ¿ Existen procedimientos para la depuración del disco duro del servidor ?

Si ☐ No ☐

4.9 ¿ Con qué periodicidad se depura el disco duro del servidor ?

Más de tres meses ☐ De uno a tres meses ☐

De dos semanas a un mes ☐ Otra ☐ Especificar. _____

**5. Estructura de directorios.**

5.1 ¿ Existen grupos funcionales de usuarios en la red ?

Si ☐ No ☐

5.2 ¿ Existen restricciones respecto al acceso de archivos en general ?

Si ☐ No ☐

**6. Administración de usuarios.**

6.1 ¿ Cuál es la longitud de los user-id's en el servidor ?

*Menos de 8 caracteres* ☐ *8* caracteres ☐ Más de 8 caracteres ☐

6.2 ¿ Son dados de baja los user-id's de los usuarios que dejan de pertenecer a la organización ?

Si ☐ No ☐

6.3 ¿ Es requerido un password por usuario para accesar al servidor ?

Si ☐ No ☐

6.4 ¿ Existen *cambios automáticos y/o* periódicos en los passwords de usuarios ?

Si ☐ No ☐

6.5 ¿Con qué periodicidad se realizan los cambios ?

Tres meses o más ☐ Bimestral ☐ Mensual ☐ Semanal ☐

6.6 ¿ En cuántas estaciones de trabajo puede estar dado de alta un mismo usuario ?

Una ☐ Dos a más ☐

6.7 ¿ Se tienen establecidos parámetros para definir atributos de acceso a usuarios ?

Si ☐ No ☐

6.8 ¿ Se monitorea periódicamente la utilización de recursos de la red ?

Si ☐ No ☐

**7. Mantenimiento.**

7.1 ¿ Se da mantenimiento preventivo a los componentes de la red ?

Si ☐ No ☐

7.2 ¿ Se encuentra actualizado el calendario de mantenimiento preventivo para todos los equipos de la red ?

Si ☐ No ☐

7.3 ¿ Se conserva la documentación que respalda el mantenimiento dado ?

Si ☐ No ☐

7.4 ¿ Se mantiene actualizada la bitácora de problemas de hardware ?

Si ☐ No ☐

7.5 ¿ Existen planes de contingencia documentados ?

Si ☐ No ☐

7.6 ¿ Existen procedimientos para reinicio de operaciones después de fallas ?

Si ☐ No ☐

**8. Bienes y servicios informáticos.**

8.1 ¿ Se sabe a quién dirigirse para solicitar bienes y/o servicios informáticos ?

Si [ ] No [ ]

8.2 ¿ Se sabe a quién dirigirse en caso de recibir un bien informático defectuoso o incompleto ?

Si [ ] No [ ]

8.3 ¿ Cuál es el plazo de tiempo establecido para atender fallas en los equipos ?

Tres días [ ] Dos días [ ] Un día [ ] Otro [ ] Especificar ____

8.4 ¿ Se notifica a la Dirección cuando se sustituye un equipo ?

Si [ ] No [ ]

8.5 ¿ Existen partidas presupuestales autorizadas por la Dirección dirigidas a la compra de bienes informáticos ?

Si [ ] No [ ]

**9. Administración de la documentación.**

9.1 ¿ En que porcentaje se encuentran actualizados los manuales de operación de cada aplicación instalada en el servidor ?

0% [ ] 25% [ ] 50% [ ] 75% [ ] 100% [ ]

9.2 ¿ Se conservan ejemplares de manuales del sistema operativo y de cada uno de los paquetes que se tienen instalados en el servidor ?

Si [ ] No [ ]

9.3 ¿ Se conservan ejemplares de manuales de cada uno de los dispositivos conectados al servidor como estaciones de trabajo, unidades de respaldo, tarjetas de red, unidades de disco óptico, etc. ?

Si [ ] No [ ]

9.4 ¿ En donde se almacena la paqueteria original ?

Escritorio [ ] Gabetas [ ] Otros [ ] Especificar. _____

## 10. Adecuaciones electrónicas.

10.1 ¿ Se conecta más de un equipo en un contacto dúplex ?

Si [ ] No [ ]

10.2 ¿ Están conectados el CPU y el monitor del servidor a un sistema de soporte ininterrumpido de energía (UPS) ?

Si [ ] No [ ]

10.3 ¿ Son del conocimiento del administrador de la red las acciones a seguir cuando se activa la alarma del UPS ?

Si [ ] No [ ]

## 11. Inventarios de equipo.

11.1 ¿ Se cuenta con un inventario actualizado de todos los equipos y dispositivos de la red ?

Si [ ] No [ ]

11.2 ¿ Se tiene identificada la ubicación física de todos los equipos y dispositivos de la red ?

Si [ ] No [ ]

11.3 ¿ Existen procedimientos para actualizar el inventario del equipo y dispositivos de la red?

Si [ ] No [ ]

11.4 ¿ Existen registros de consumo de diskettes, papel para impresoras, etc. ?

Si [ ] No [ ]

## APENDICE 2. LEVANTAMIENTO DE INFORMACIÓN DE REDES LOCALES EN UNA ORGANIZACIÓN.

**Folio** ☐ **Fecha** ☐

**Datos generales.**

Dirección. _____
División. _____
Responsable. _____
Ubicación. _____ Teléfono. _____ Fax. _____

Administrador de la red. Ubicación. _____
Teléfono. _____

### 1. Sistema de cableado.

- Sistema Operativo de Red.

  Lan Manager ☐ Netware ☐ OS/2 ☐

  Otros ☐ Especificar. _____

  Versión. _____

- Tipo de Topología.

  Ethernet ☐ Token Ring ☐ Arcnet ☐

- Tipos de Cables.

  Coaxial Delgado ☐ Coaxial Grueso ☐ Teléfono ☐

  Velocidad de Transmisión. _____

1.1 *Distribución del cable.*

Edificio ☐ Ubicación cuarto de cable ☐

| Controlador | Puerto origen | Puerto destino | Long. del cable |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**2. Conectividad.**

**2.1 Conectividad con host.**

- Tipo de enlace.

  Coaxial ☐ Solo ☐ Token Ring ☐

- Software de comunicaciones.

  Com Server ☐ WsLan ☐ SNA Services ☐

  Otro ☐ Especificar. _____

- Tipo de comunicación.

  LU 2 ☐ LU 6.2 ☐

- Número de sesiones. _____

- Si la comunicación es LU 6.2, ¿ qué producto y aplicación maneja ?

  _____

- Equipo utilizado como Gateway.

  Marca y modelo. _____RAM. _____

  Disco Duro. _____ Marca de las tarjetas de comunicación. _____

**2.2 Conectividad con minicomputadoras y/o redes.**

- Sistema operativo.

Netware ☐ Lan Manager ☐ Windows for Groups ☐

Otro ☐ Especificar. _____

- Si el sistema operativo es UNIX, ¿ qué producto TCP/IP se utiliza y cuál aplicación está manejando ?

**2.3 Conexión entre redes (Internetworking)**

2.3.1 Datos de la red.

| Área (red) | Ubicación | Hardware de enlace | Razón de conexión |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

2.3.2. Datos del servidor.

- ¿ Qué tipo de servicios presta ?

Administración de archivos ☐ Administración base de datos ☐

Comunicaciones ☐ Impresión ☐

Correo Electrónico ☐ Otro ☐

Especificar. _____

| Nombre del Servidor | Número de red | Dominio | Marca y Modelo | Procesador | Velocidad | RAM |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Nombre del Servidor | Video | Número de disco | Bus del disco | Capacidad | Tarjeta de red | Tipo de cable | Uso del servidor |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

3. **Estaciones de trabajo.**

- Número de estaciones de trabajo. ___
- Tipo de cable.

  Teléfono [ ] Coaxial [ ] Otro [ ] Especificar. _____

- Características.

| Marca y modelo | Procesador | Velocidad | RAM | Disco duro |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

4. **Administración de redes.**

- Tolerancias a fallas

  Disk Mirroring [ ] Disk Duplexing [ ] Disk Array [ ]

  Backup Server [ ] UPS [ ]

- Unidad de respaldo.

  Capacidad de los cartuchos. _____ Frecuencia de respaldo. _____

- Personal.

  Indicar la cantidad de personas asignadas a las siguientes funciones:

  Administradores de red. ____
  Administradores de Bases de Datos. ____
  Administradores de comunicaciones e instalaciones. ____

- Carpeta de administración:

  - [ ] Diagrama de la red.
  - [ ] Datos técnicos del sistema de cableado.
  - [ ] Datos técnicos del servidor.
  - [ ] Datos técnicos de las estaciones de trabajo.
  - [ ] Datos técnicos de periféricos compartidos.
  - [ ] Inventario de periféricos y accesorios.
  - [ ] Responsabilidades del administrador de la red.
  - [ ] Inventario de paquetería.
  - [ ] Políticas y procedimientos a seguir en caso de fallas.
  - [ ] Calendario de soporte técnico.
  - [ ] Bitácora de fallas.
  - [ ] Calendario de respaldos.

**5. Soporte de red.**

| Tipo de soporte | Encargado | Area y/o proveedor |
|---|---|---|
| Planeación. | | |
| Configuración. | | |
| Conectividad (Host, Minis, Redes e instalación de cableado). | | |
| Adquisiciones. | | |
| Control de fallas. | | |

## APENDICE 3. FORMATOS PARA LEVANTAMIENTO DE INFORMACIÓN TÉCNICA.

### 1. Servidor de red.

Dirección. _____ Área. _____

Responsable. _____ Teléfono. _____ Fax. _____

1.1 Información técnica.

Nombre del servidor. _____ Procesador. _____ Coprocesador. _____

Modelo. _____ No. de discos. _____ Capacidad de discos. _____

Velocidad. _____ RAM. _____ Memoria. _____ Puertos. _____

BIOS. _____ Slots. _____ Arquitectura. _____ Tarjeta de red. _____

Tarjeta adicional. _____ Sistema operativo. _____ Versión. _____

### 2. Estaciones de trabajo.

Dirección. _____ Área. _____

Responsable. _____ Teléfono. _____ Fax. _____

2.1 Información técnica.

Nombre del servidor. _____ Procesador. _____ Coprocesador. _____

Modelo. _____ No. de discos. _____ Capacidad de discos. _____

Velocidad. _____ RAM. _____ Memoria. _____ Puertos. _____

BIOS. _____ Slots. _____ Arquitectura. _____ Tarjeta de red. _____

Tarjeta adicional. _____ Sistema operativo. _____ Versión. _____

### 3. Software de la red.

3.1. Aplicaciones y/o paquetes instalados.

| Número de serie del servidor. | Número de serie del monitor. | Número de serie del teclado. |
|---|---|---|
| _____ | _____ | _____ |

| Nombre del sistema o paquete | Versión | Número de serie del paquete | No. de licencia | Fecha de instalación | Instalado por |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

3.2. Directorio de proveedores y/o departamentos de asesoría y soporte.

| Área, compañía o razón social | Dirección ó ubicación | Teléfono | Responsable | Dirigirse a | Horario |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**4. Sistema de cableado.**

Dirección. _____ _____ Área. _____

Responsable. _____ Teléfono. _____ Fax. _____

4.1. Información técnica.

Tipo de red. _____ Topología. _____ Tipo de cable _____
Velocidad de transmisión. _____ Repetidores. _____ Cantidad ___
Fuente de poder. _____ Distancia total. _____

4.2. Distribución del cable.

Edificio. _____ Piso. _____ Cuarto de cableado. _____
Fecha de último registro. _____

| Cable No. | Pto. Origen | Pto. Destino | Distancia | Información |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

5. Bitácora de fallas (Comunicaciones, hardware y/o software).

| Fecha | Reportado por | Teléfono | Tipo de error | Solución | Comentarios |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## APÉNDICE 4. CUESTIONARIO PARA LEVANTAMIENTO DE INFORMACIÓN.

| EMPRESA AUDITADA | | FECHA. | |
|---|---|---|---|
| ÁREA. | | REF. | |
| NOMBRE DEL AUDITOR. | | | |
| **Seguridad** | **Si** | **No** | **Observaciones** |
| 1 ¿ Existe un responsable de la seguridad tanto física como lógica en el área ? | | | |
| 2 ¿ Existen restricciones básicas para:<br>• el acceso a documentos que contienen información original o vital ?<br>• que el acceso a la red durante la producción se limite a los operadores ?<br>• *que el acceso a archivos y programas en uso se limite a los operadores* ?<br>• que el personal del departamento de informática no ejecute transacciones o cambios en los archivos maestros ?<br>• el acceso a la parte central de la red ? | | | |
| 3 ¿ Se tienen identificadas las áreas de alto riesgo en la red ? | | | |
| 4 ¿ Se tiene protegido el servidor o servidores de la red contra accesos no autorizados? | | | |
| 5. ¿ Las instalaciones de cableado están ocultas ? | | | |
| 6. ¿ Se cuenta con elementos que controlen las fallas de energía eléctrica ? | | | |
| 7. ¿ Se tienen instalados detectores contra incendios ? | | | |
| 8. ¿ Se revisan regularmente los detectores para asegurar su buen estado ? | | | |
| 9 ¿ *Se tienen instaladas alarmas contra robos o accesos físicos no autorizados* ? | | | |
| 10 ¿ Se cuenta con controles de acceso a los sistemas de la red ? | | | |
| 11. ¿ Los usuarios cuentan con password de acceso ? | | | |
| 12 ¿ Los passwords son temporales o fijos ? | | | |
| 13. ¿ Se hacen respaldos periódicos de archivos ? | | | |
| 14 ¿ *Existen planes de seguridad para el personal, instalaciones y datos* ? | | | |
| 15 ¿ Se cuenta con técnicas y procedimientos para análisis y evaluación de riesgos ? | | | |
| 16 ¿ Se cuenta con un plan de contingencias estructurado ? | | | |
| 17 ¿ Se hacen pruebas periódicas del plan de contingencias ? | | | |
| 18 ¿ Se han establecido técnicas para evaluar dicho plan ? | | | |

| Administración de la red | Si | No | Observaciones |
|---|---|---|---|
| 19 ¿ Se cuenta con una estructura formal para la administración de la red ? | | | |
| 20 ¿ Los administradores cuentan con el software adecuado para este fin ? | | | |
| 21 ¿ El administrador de la red cuenta con conocimientos amplios en lo que refiere a su función ? | | | |
| 22 ¿ Se tiene documentado el perfil del administrador de la red ? | | | |
| 23 ¿ Se encuentran definidas y documentadas las funciones y responsabilidades del administrador de la red ? | | | |

# GLOSARIO

| | |
|---|---|
| 10Base2 | Estándar de IEEE 802 3 basado en Ethernet (método CSMA/CD a 10 Mb). Trabaja con segmentos de 200 m de cable coaxial. |
| 10Base5 | Estándar de IEEE 802 3. Opera sobre cable ancho coaxial con segmentos de 500 m. |
| 10BaseT | Estándar de IEEE 802 3. Opera sobre cable telefónico no blindado (UTP). |

## A

| | |
|---|---|
| AdvancedNET | Solución de red de área local de Hewlett Packard, basada en Ethernet. |
| Algoritmo | Secuencia finita de pasos, dirigidos a realizar una tarea específica, (método de solución). |
| ANSI | Siglas de "American National Standar Institute", Institución voluntaria que ayuda a definir estándares y que representA a los E.U. en la Organización Internacional de Estándares (ISO). |
| Archive Server | Es un servidor (server) enfocado a realizar en forma automática respaldos de información de uno a más servidores. |
| Arcnet Plus | Propuesta de un nuevo tipo de ARCnet para trabajar a 20 Mbps. Espera ser avalado por IEEE y/o ANSI. Es interoperable con ARCnet de 2 5 Mbps. |
| ARPANET | Red de área amplia que utiliza protocolos de paquetes diferidos (tipo X.25). La red fue creada por ARPA junto con el Departamento de Defensa de E.U. para dar soporte a las comunidades militares.<br><br>ARPANET se divide en dos partes interconectadas: Milnet, para uso militar y para uso comercial y académico. |

ASCII — Siglas de "American Standar Code for Information Interchange" Forma estándar de codificar los caracteres en un patrón de 7 bits El ASCII extendido utiliza 8 bits y logra codificar patrones (2 8). en lugar de 128 (2 7).

Atenuación — Reducción de la potencia de una señal eléctrica durante la transmisión Medida en decibeles. Opuesto a ganancia. Los decibeles son medidos logaritmicamente.

## B

BackBone — Generalmente se denomina de esta manera a la conexión entre varias redes de área local.

Backup Server — Un producto, habitualmente software, que asegura que al menos las dos últimas versiones de un archivo sean almacenadas continuamente.

Balun — Del inglés "balanced-unbalanced". Dispositivo de tamaño reducido utilizado para conectar un medio balanceado (par trenzado) con un medio no balanceado (cable coaxial).

Baseband — Las redes de área local, de acuerdo a su utilización de canal, pueden ser de tipo Baseband o Broadband. En el primer caso, todo lo ancho de banda del canal se utiliza para enviar datos.

Batch — Un método de procesamiento de datos en donde todos los trabajos se agrupan primero para después enviarse en forma secuencial a la computadora para su procesamiento.

Baudio — Medida de velocidad de transmisión de datos. La velocidad en baudios es igual al número de veces que cambia la condición de la línea por segundo. A velocidades bajas, los baudios y los bits-por-segundo, son lo mismo. Sin embargo, cuando la velocidad aumenta, por cada baudio son codificados varios bits, por lo que dejan de ser sinónimos.

BIOS — Siglas de "Basic Input/Output System". Servicios de software y/o firmware que definen la forma en que interactúan las aplicaciones y todos los puertos seriales y paralelos de entrada/salida.

| | |
|---|---|
| Bit de paridad | Método sencillo para detectar errores en la transmisión. Se agrega un bit en 0 ó 1 dependiendo del número de unos que tenga el patrón a enviar (por ejemplo, si se trabaja en paridad par y en el patrón original existen 3 unos, el bit de paridad irá en 1 para completar un número par). |
| Blindaje | Es el proceso de proteger un cable con un metal aterrizado, de tal forma que las señales eléctricas no pueden interferir con la transmisión dentro del cable. |
| Boot | Proceso de carga de los programas básicos para encender la computadora. Bajo términos de IBM, se denomina IPL (Initial Program Load). |
| Bootp | Protocolo que se utiliza para transferencia de información (booting), entre un Boot-Server y el dispositivo. |
| Boot Remoto | En una red, proceso de encender una estación de trabajo haciendo el "boot" desde el servidor de red. |
| Bps | Abreviación de bits por segundo. La medida de velocidad de transmisión más utilizada. En redes de área local, lo más frecuente es hablar de Mbps. (Mega bits por segundo). Es importante hacer notar que la abreviación de bit es una **b** minúscula, mientras que Byte es una **B** mayúscula. |
| Bridge | Dispositivo que permite enviar datos de una red de área local a otra (en español es un "Puente"). |
| Broadband | En este tipo de red de área local en ancho de banda se divide en canales de voz, datos y video. Esto se logra a través del manejo de varias frecuencias en un mismo canal. |
| Brouter | Un bridge que puede llevar a cabo funciones de ruteador (yuxtaposición de un bridge y router). |
| BSC | Siglas de "Binary Synchronous". Es un método arcaico de transmitir datos, creados por IBM en 1964. |
| Buffer | Es un espacio donde se almacenan datos temporalmente mientras se les puede enviar a su destino final. |

BUS — Es un circuito de transmisión eléctrica que sirve para transportar información entre varios dispositivos de una computadora.

## C

Cable Coaxial — Es un tipo de cable eléctrico en el cual un alambre sólido de metal está cubierto por un aislante, todo es protegido por una malla de metal cuyo eje de curvatura coincide con el del alambre, de ahí el nombre de coaxial (eje común).

Canal — Un camino físico o lógico que permite la transmisión de información. En algunos casos, puede ser sinónimo de bus.

CMIP — Siglas de "Common Management Internet Protocol". Es el protocolo propuesto por OSI para realizar la administración de redes.

Colisión — El resultado de que dos o más estaciones traten de usar simultáneamente un medio de transmisión (cable) común. Después de una colisión la transmisión se corrompe y hay que reintentarla.

Compatibilidad — Estado que permite la transmisión precisa desde el origen hasta el destino (esto no implica que el destino entenderá la información).

Concentrador — Para fines generales, dispositivo que concentra (de ahí su nombre) segmentos de cable de una red de área local para su mejor distribución y administración.

Conectividad — Estado que permite la transferencia de señales eléctricas desde un origen hasta un destino.

Conector — Es un accesorio al final de un alambre o conjunto de alambres que facilitan su conexión a un recurso.

Convenio de nivel de servicio (CNS) — Un convenio de nivel de servicio es un contrato entre el proveedor de un servicio y el consumidor de dicho servicio. La palabra "contrato" no tiene una connotación legal, sino que se usa en el sentido de que los convenios se ponen por escrito y quedan sujetos a mediciones.

El propósito del CNS es establecer objetivos medibles convenidos de desempeño. Su objetivo es el logro de un desempeño que sea aceptable para el cliente del servicio y al mismo tiempo realista para el proveedor.

CPU — Siglas de "Central Processing Unit". Generalmente se utiliza este término para definir el Procesador Central de una computadora. Es la base de una computadora digital.

CSMA/CD — Siglas de "Carrier Sense Múltiple Access/Collission Detectión". Técnica utilizada para enviar señales dentro de una red de área local. El cable se utiliza por "competencia" y cuando una tarjeta detecta sólo la portadora, empieza a transmitir, pero debe seguir escuchando por si ocurre alguna colisión. De ser así, requiere hacer una retransmisión.

## D

DAS — Siglas de "Dual-Attachment Station". Dispositivo utilizado en las redes Token-Ring que permite el acceso a dos sistemas de cableado al mismo tiempo, ofreciendo protección a los cables dañados.

DCE — Siglas de "Data Comunication Equipment". En la terminologia común es sinónimo de módem.

DIP Switch — Siglas de "Dual In Package". Grupo de pequeños switches que normalmente vienen en dispositivos o tarjetas para ayudar en su configuración.

Direccion — Conjunto de números que identifican de manera única "algo". Puede ser una estación de trabajo en una red, una localidad de memoria, un paquete de datos viajando en una red, una tarjeta de red, etc.

DNA — Sigla de "Digital Network Architecture". Arquitectura de comunicaciones de Digital Equipment Corporation (DEC).

## E

**Emulación** La imitación que hace un dispositivo de otro. Típicamente una PC actuando como terminal de un equipo mayor.

**Encripción** Proceso matemático donde los datos de un mensaje por seguridad son codificados para protegerlos de accesos no deseados.

**Estacion de trabajo** Cualquier equipo conectado a una red, con capacidad propia de proceso.

**Estación remota** En general, nombre que se le da a las PC´s que se conectan a una red de área local a través de un módem.

**Estación sin disco** Estación de trabajo que no posee unidades de diskette ni discos duros y que por lo tanto hace un "boot" remoto (Diskless Workstation).

**Ethernet** El estándar de tarjetas de red más conocido y sólido. Define una velocidad de transmisión de 10 Mbps, utilizando protocolo CSMA/CD.

## F

**FAT** Siglas de "File Allocation Table". Tabla del sistema operativo, que se encuentra en las primeras pistas de los diskettes y discos duros, cuyo objetivo es llevar la relación de los sectores usados por cada archivo (a través de listas encadenadas).

**FAT Indexing** Característica del Sistema Operativo Netware V2.1 y mayores, bajo la cual cada vez que se abre cualquiera de los archivos especificados por el supervisor. Netware "carga" a memoria toda la tabla de sectores que le corresponde, agilizando con esto, las búsquedas a los bytes más alejados del inicio del archivo.

**FDDI** Siglas de "Fiber Distributed Interface". El estándar para transmisión de datos en redes de área local utilizando fibra óptica, a una velocidad de 100 Mbps.

| | |
|---|---|
| | Utiliza un doble anillo en una topología similar a Token Ring, incluso en la definición del frame, igualmente usa un protocolo de Token Passing para control de la red. |
| Fibra Óptica | Medio de transmisión de datos que consisten en una fibra de vidrio. Una fuente luminosa (LED´s o Lassers) emite un haz de luz que se va reflejando dentro del cable gracias a los diferentes grados de retracción entre el material de la fibra y una cubierta de material similar. Aunque el costo de la fibra ha bajado, todavía resulta costoso y complejo el instalar fibra óptica en redes de área local. Generalmente se utiliza para construir Back Bones (conexión entre redes). |
| File Server | Servidor de archivos. Computadora dedicada a compartir información de los archivos que tiene almacenados en su(s) disco(s), entre los usuarios de una red de área local. |
| Firmware | Conjunto de programas requeridos para implementar una función especifica. Estos programas se encuentran almacenados en ROM (Memoria de sólo lectura). |
| Frecuencia | Número de ciclos por unidad de tiempo normalmente medida en Hertz (Hz.). |
| FTP | Siglas de "File Transfer Protocol". Servicio de alto nivel bajo ambiente TCP que permite y controla el proceso de transferencia de archivos a través de una red. |

## G

| | |
|---|---|
| GAN | Siglas de "Global Area Network". Red que involucra comunicación remota y sin embargo posee una administración centralizada. |
| Ganancia | Incremento en la potencia de una señal, normalmente como resultado de una ampliación. |
| Gateway | Dispositivo que permite conectar dos redes (locales o geográficas) con diferentes protocolos. Un gateway cambia al menos, por los protocolos de los primeros 4 niveles del modelo ISO/OSI. |
| Gigabyte | Equivalencia de 1000 Megabytes. |

H

Handshake — Procedimiento preliminar, normalmente parte de un protocolo, para establecer una conexión entre dos dispositivos.

Hertz (Hz) — Unidad de frecuencia, equivalente a un ciclo por segundo.

Host — Computadora local o remota en donde se lleva a cabo el procesamiento batch y linea de las aplicaciones de una organización. Normalmente es una minicomputadora o un mainframe.

Hub — Utilizado como sinonimo de repetidor o concentrador.

I

IEEE — Siglas de "Institute of Electrical and Electronics Enginers". El comité 802 del IEEE ha establecido los estándares para las redes de área local.

IEEE 802.1 — Define un algoritmo de enrrutamiento de "frames" llamado Spanning-tree.

IEEE 802.2 — Define dentro del nivel 2 las tareas de interfase con el nivel 3 (denominado LLC Logical Link Control).

IEEE 802.3 — Basado en Ethernet, define una forma de protocolo referido en CSMA/CD. Posee diversas variantes cable grueso, delgado, par trenzado y broadband).

IEEE 802.4 — Define un tipo de red Token-Bus, Similar a Arcnet.

IEEE 802.5 — Define un tipo de red Token-Ring. Aunque IBM patrocinó gran parte de este comité, el Token-Ring que lanza al mercado, es un superconjunto del 802.4.

Integridad — Característica de la información de reflejar datos congruentes con la realidad.

Internet — Red de información mundial basada en computadoras. La Internet se compone de un gran número de pequeñas redes interconectadas, las cuales a su vez, pueden tener conectadas cientos o miles de computadoras, permitiendo

compartir información y recursos tales como poderosas supercomputadoras y bases de datos. La Internet ha hecho posible que miles de personas alrededor del mundo se comuniquen entre sí con gran eficiencia.

IPX — Protocolo "puerto a puerto", propio de Novell, que actúa en el nivel 3 del modelo OSI (nivel de red). Entre sus ventajas esta el contar con direcciones de tres campos nodos, red y socket, que le permiten tener enlaces entre redes y varios procesos corriendo en diferentes servidores. Está basado en el protocolo de nivel 3 del XNS.

ISO — Siglas de "International Standard Organization". Institución internacional que se encarga de especificar estándares en diversas áreas.

## J

J-Bit — Un bit de transmisión codificada, que no representa datos y se utiliza solamente para el control de transmisión.

JCL — Job Control Languaje (Lenguaje de Control de Procesos). I enguaje especifico de Main Frame, empleado esencialmente para ejecutar y compilar programas, así como para efectuar operaciones básicas de abrir, cerrar, buscar y eliminar archivos y programas de aplicaciones desarrolladas en equipo mayor.

Jumper — Pieza pequeña que permite unir dos terminales (pins) de algún conector de hardware. En general, conector que une dos extremos.

## K

K-Bit — Un bit de transmisión codificada que representa datos y se utiliza únicamente para el control de transmisión.

Kilobit — Medida que significa bits, se representa por la abreviación Kb.

## L

**LAN** — Siglas de "Local Area Network". La abreviación más común al hablar de Redes de Area Local.

**LAN Manager** — El Sistema Operativo para redes de área local creado por Microsoft, basado en OS/2. También se denomina LAN-Manager a cierto software de IBM, utilizado para monitorear el estado de una red.

**LAN Manager / UNIX** — Versión de LAN Manager desarrollada inicialmente por Hewlett-Packard y SCO para UNIX. En la actualidad existen versiones de diferentes UNIX. La responsabilidad del código original recae ahora en la compañía AT&T.

**LAN Server** — La versión de LAN-Manager, muy particular de IBM soporta entre otros protocolos, APPC de manera nativa.

**Login** — Acción de entrar a utilizar un host o servidor de red, establecer una sesión de trabajo y ser reconocido como usuario por el Sistema Operativo.

**LPT** — Siglas de "Lan Performance Test". Herramienta de software, desarrollado por Smart Soft Inc. para medir en forma relativa, la eficiencia de una red.

**LU** — Siglas de "Logical Unit" (Unidad Lógica) en léxico IBM. En forma sencilla, LU es un "puerto" de software que se establece para llevar a cabo una sesión.

## M

**Mainframe** — Computadora mayor o equipo mayor del centro de cómputo. Normalmente, en este equipo se llevan a cabo las operaciones de mayor volumen, así como los procesos línea y batch.

**MAO** — Siglas de "Manufacturing Automation Protocol", una red de bus, con protocolo de acceso token-passing, diseñada para ambientes de fábricas, patrocinadas por General Motors.

MAU o MSAU — Siglas de "Multistation Access Unit". Dispositivo fundamental para cableado de Token-Ring. Su función es cerrar el anillo entre todos los dispositivos que se le conecta.

Menú — Carátula en la cual se presenta por pantalla el desglose general de una aplicación.

Método de acceso — Forma en que la tarjeta de red "accesa" el cable o canal de comunicación. Existen dos variantes importantes CSMA/CD (Ethernet) y Token Passing (Token Ring).

MICE — Siglas de "Management Information Control and Exchange". Protocolo de nivel de aplicación del modelo OSI, que utiliza DEC en la fase V de su DNA para implementar funciones de administración de redes.

Microondas — Transmisiones de ondas de radio en el rango de los Gigahertz (GHz). Las microondas se utilizan en g[illegible]da para la transmisión de datos en distancias cortas, desde 35 hasta 65 Km. Este tipo de enlace requiere de línea de vista para su funcionamiento.

Microsegundo — La millonésima parte de un segundo.

Milisegundo — La milésima parte de un segundo. Se representa por la abreviación ms.

Módem — Yuxtaposición de Modulador/Demodulador. Dispositivo que convierte señales digitales desde una terminal (PC) a una señal adecuada para transmitirse en un canal telefónico (analógico). En el otro extremo, otro módem reconvierte la señal analógica en digital y la transmite a la computadora de ese extremo.

Modulación — Proceso por medio del cual la señal de transmisión se modifica para llevar algún tipo de información.

Monitor — Hardware o software que recibe información sobre el rendimiento y operación de una red, para su almacenamiento o para toma de decisiones.

Motherboard — La tarjeta principal (con circuitos integrados) que contiene toda computadora personal.

Normalmente posee diversas ranuras (slots) para agregar otro tipo de tarjetas como son de memoria, controladores de disco, tarjetas de red, etc.

Multiplexar — Enviar señales por un mismo medio, variando en cada una de estas señales algún parámetro para diferenciarla de las restantes (ej. la frecuencia). Es posible también separarlas en el tiempo, lo cual se denomina multiplexaje por división de tiempo.

Multitasking — Capacidad de un sistema operativo para realizar más de una tarea en forma simultánea. OS/2, por ejemplo es un sistema operativo que brinda capacidades de multitasking (multitareas).

N

Nanosegundo — Millonésima parte de un segundo. Para su representación se utiliza la nomenclatura ns.

Netbios — Interfase estándar (hasta hoy) para comunicar dos estaciones de trabajo en una red de área local. Definido por IBM y Sytek en 1984-1985. Dentro del contexto de MS DOS son los servicios de software y firmware que implementan la interfase entre las aplicaciones y la tarjeta de red.

Netview — Producto de software desarrollado por IBM que permite controlar redes complejas como aquellas que se forman utilizando SNA y redes de área local Netview. Sólo puede operar con productos de red definidos por IBM.

Netware — Sistema Operativo de red (en sus diferentes versiones), desarrollado por Novell Inc.

Nivel de servicio — Satisfacción de las necesidades de los usuarios de servicios de cómputo y conmuto, basados en la cultura de servicio, calidad y rentabilidad.

Nodo — Este término se utiliza generalmente para referirse a una estación de trabajo dentro de una red Punto computacional bajo una red de comunicaciones

Novell — Uno de los principales fabricantes de productos para redes Desde 1988 se ha enfocado preponderantemente al mercado de sistemas operativos, desligando casi totalmente del hardware para redes de área local.

## O

Offloading de aplicaciones — El Offloading de aplicaciones se fundamenta en la obtención de todos los componentes o programas fuente que se encuentran en ambiente de producción Estos mismos, serán transmitidos desde el mainframe hasta el entorno PC-LAN, donde serán catalogados y compilados, asimismo, se transmiten los archivos de prueba de la aplicación para su ejecución en el nuevo ambiente.

Open View — Arquitectura para administracion de redes, desarrollada y usada por HP.

OSI — Siglas de "Open Systems Interconnect". Estructura lógica y estándar de 7 niveles de protocolos definida por ISO para facilitar la comunicación en ambientes heterogéneos.

OS/2 — Sistema Operativo desarrollado por IBM-Microsoft para la línea de computadoras personales PS/2 (Personal System 2).

## P

Par Trenzado — Se forma con dos cables aislados que se tuercen entre si (de ahí el nombre de par trenzado). Existen dos variantes básicas blindado o no blindado. El blindado permite mayores distancias y es mucho más inmune al ruido El no blindado (UTP) es más económico, pero tiene limitantes de distancias y ruido.

PDN — Siglas de "Public Data Network". Termino internacional con que se define a las redes públicas que operan utilizando conmutación de paquetes.

PDU — Siglas de "Protocol Data Unit". Forma en la deben aparecer los datos definidos por un protocolo.

Peer to Peer — Una comunicación peer - to - peer (puerto - a - puerto) se establece cuando las dos computadoras pueden iniciar una conversación y no se requiere "permiso" de la otra.

## Q

Q-Bit — Bit calificador en un paquete X.25 que el DTE utiliza para indicar que quiere transmitir datos a más de un nivel.

Q-Bus — Estructura de interconexión interna de la familia de computadoras VAX de DEC.

QLLC — Siglas de "Qualified Logical l ink Control". Protocolo de control para el nivel de datos del modelo OSI que permite a los sistemas SNA operar sobre redes de paquetes conmutados CCITT X.25.

Queue — Literalmente cola de espera. Normalmente referida a las colas de espera de la impresora.

## R

Radio frecuencia — Cualquier radiación electromagnética coherente. La mínima frecuencia de dicha radiación es aproximadamente 15khz.

RAM — Siglas de "Random Access Memory". Memoria que puede ser escrita y leida de manera dinámica. Puede ser accesada por el usuario en cualquier punto con facilidad y sin tener que leer grabaciones anteriores.

RARP — "Reverse Address Resolution Protocol". Protocolo que descubre una dirección desconocida y otorga una dirección conocida y un servidor RARP para proveer una respuesta.

Red de área local — Conjunto de computadoras, enlazadas por algún tipo de cable y en distancias relativamente cercanas (dentro de un mismo edificio o campus). También conocida como LAN (Local Area Network).

| | |
|---|---|
| Redirector | Conjunto de servicios de software de alto nivel que rutea peticiones de programas del usuario hacia recursos tales como archivos, impresoras y programas a través de una red. |
| Repetidor | Dispositivo que transmite y amplifica la señal recibida. Actúa solamente en el nivel I del Modelo OSI. |
| ROM | Siglas de "Read Only Memory". Memoria no-volátil que puede ser leída pero no modificarse. |
| RS-232C | Interfase estándar para conectar un DTE a un CDE. La especificación técnica ha sido publicada por la EIA. Tradicionalmente usa 25 pins (o terminales). |
| Ruido | Señales eléctricas que distorsionan una transmisión, introduciendo errores. El ruido puede provenir de cables de corriente, motores eléctricos, etc. |
| Ruteador | Dispositivo que toma un paquete (Nivel III del Modelo OSI) y lo envía del punto A al punto B, después de analizar cuál es el camino óptimo para llegar a su destino. Esto se logra gracias a la información que cada ruteador almacena sobre todos los nodos de la red. |

**S**

| | |
|---|---|
| S/F | Store and Forward. Servicio de transmisión donde los mensajes son recibidos en un punto intermedio en la red y después retransmitidos a otro punto en ella. |
| SAA | Siglas de "Systems Application Architecture". Grupo de estándares definido por IBM, enfocado a lograr que las aplicaciones que se desarrollen en un cierto tipo de equipo (micro, mini o mainframe) puedan ser transportadas a otros ambientes sin ningún cambio importante a nivel programación. |
| Satélite | Dispositivo de recepción y transmisión que se encuentra orbitando la tierra (en órbita geoestacionaria) utilizado para enviar señales sobre grandes distancias. |
| Secuenciamiento | Proceso de dividir un mensaje de datos, en piezas más pequeñas, para su transmisión. |

| | |
|---|---|
| Servidor | Dispositivo de hardware o rutina de software que provee uno o más servicios predefinidos a una población de entidades usuarias, tales como nodos de una red. |
| Sesión | En terminología IBM, es la plática entre dos Logical Units (LU's). |
| SLIP | Siglas de "Serial Line Internet Protocol". Protocolo que controla el proceso de transferir paquetes de TCP/IP a través de una línea serial. |
| SNA | Siglas de "Systems Network Architecture". La arquitectura de protocolos para redes creada por IBM. |
| SNMP | Siglas de "Simple Network Management Protocol". Protocolo estándar de la familia TCP/IP, enfocado al manejo, administración y control de redes que utilicen TCP/IP. |
| SPOOL | Siglas de "Simultaneous Peripheral Operations On Line". Comúnmente el software encargado de controlar las colas de espera en una impresora. |
| SPX | Siglas de "Sequenced Packet Exchange". Protocolo propio de Netware para el nivel IV del Modelo OSI. Apoya a IPX brindando servicios de secuenciamiento de paquetes y garantía de llegada. |
| SQL | Siglas de "Structure Query Language". El lenguaje de consulta y acceso a la base de datos más común en la actualidad, definido como estándar por IBM, ANSI e ISO. |
| SQL-Server | Servidor de bases de datos desarrollado por Microsoft y Sybase (hasta 1989 fue comercializado por Ashton-Tate). Se liberó en mayo de 1989. Posee características sumamente poderosas en manejo de transacciones, integridad de la información y control de concurrencia. |
| Starlan | Red de área local creada por AT&T. Transmite a 1Mbps, aunque tiene una variante de 10 Mbps. Utiliza cable telefónico. Sus frames son muy similares a Ethernet. |

Windows — Ambiente operativo (complemento a MS-DOS) desarrollado por Microsoft para tener una interfase sencilla y amigable con el usuario, pero muy poderosa.

Windows NT — Windows New Technology. Nuevo sistema operativo de Microsoft. Ya no es un ambiente sobre DOS, sino un Sistema Operativo completo de 32 bit[illegible] que incluir[illegible]rios servicios básicos de red y una arquitectura diferente.

## X

X.3 — Estándar de comunicaciones ANSI. No debe confundirse con las especificaciones CCITT X.3 para montar y desmontar dispositivos.

X.25 — Estándar del CCITT que define el protocolo de comunicaciones por el que una computador[illegible]de accesar una red de conmutación en paquetes (packe[illegible]ning). En general, cuando se menciona X.25 se habla de una familia de protocolos que son X.3, X.28, etc.

XENIX — Versión de UNIX desarrollada para computadoras Zenith, Data Systems, que pertenece a Group Bull Company

XMODEM — Un protocolo asíncrono de control del nivel de "data-link" del Modelo OSI. Este protocolo es de dominio público.

X/WINDOWS — Protocolo Cliente/Servidor orientado al desarrollo de interfases gráficas. Desarrollado originalmente en el Instituto Tecnológico de Massachusetts (MIT) para el proyecto ATHENA.

**Transceiver** — En redes IEEE 802.3 es un dispositivo a través del cual se conecta la tarjeta de red al cable de transmisión. Se usa también para designar cualquier dispositivo que transmite y recibe.

**Transmisión Síncrona** — Forma de transmisión en la que los dos extremos deben tener un mismo pulso de reloj y con base en éste, ambos conocen en que momento pueden transmitir. Aunque en la transmisión síncrona no se necesitan bits de inicio y final por cada carácter, el hardware requerido para sincronizar los pulsos de reloj, la hace más cara que la asíncrona.

## U

**UPS** — Siglas de "Uninterruptible Power Supply". Fuente de poder alterna que sirve de respaldo para que cuando se presenta una falla o suspensión de energía eléctrica, no se interrumpa el suministro en los dispositivos que se encuentran conectados a éste.

**UTP** — Siglas de "Unshielded Twisted Pair". Par trenzado no blindado.

## V

**VAN** — Siglas de "Value Added Network". Una red que provee algunos servicios adicionales a los básicos. Ejemplos de este tipo de red: TelNet y TymNet.

**VINES** — Siglas de "Virtual Networking System". Sistema Operativo de Red desarrollado por Banyan Systems. VINES esta basado en el Sistema Operativo UNIX.

**Virtual Circuit** — Circuito Virtual. Es una conexion que se comporta como si existiera una conexión física entre la fuente y el destino.

## W

**WAN** — Siglas de "Wide Area Network". Nombre que se da a la red extendida sobre distancias muy grandes y que generalmente depende de líneas de comunicación para su funcionamiento correcto.

Windows — Ambiente operativo (complemento a MS-DOS) desarrollado por Microsoft para tener una interfase sencilla y amigable con el usuario, pero muy poderosa.

Windows NT — Windows New Technology. Nuevo sistema operativo de Microsoft. Ya no es un ambiente sobre DOS, sino un Sistema Operativo completo de 32 bit. que incluir: rios servicios básicos de red y una arquitectura diferente.

## X

X.3 — Estándar de comunicaciones ANSI. No debe confundirse con las especificaciones CCITT X.3 para montar y desmontar dispositivos.

X.25 — Estándar del CCITT que define el protocolo de comunicaciones por el que una computador· · te accesar una red de conmutación en paquetes (packe· . ·ing). En general, cuando se menciona X.25 se habla de una familia de protocolos que son X.3, X.28, etc.

XENIX — Versión de UNIX desarrollada para computadoras Zenith, Data Systems, que pertenece a Group Bull Company

XMODEM — Un protocolo asincrono de control del nivel de "data-link" del Modelo OSI. Este protocolo es de dominio público.

X/WINDOWS — Protocolo Cliente/Servidor orientado al desarrollo de interfases gráficas. Desarrollado originalmente en el Instituto Tecnológico de Massachusetts (MIT) para el proyecto ATHENA.

# BIBLIOGRAFÍA

1. **ASERCOM.**
Asesoría en Redes y Telecomunicaciones.
Cursos Datos 01.
México, 1996

2. **Arter, Dennis R.**
Quality Audits for Improved Performance.
Second edition, ASQC Quality Press.
Wisconsin, 1994

3. **Ayala Rodiles, Sara Isabel.**
Auditoria de aplicaciones computarizadas.
México, 1991

4. Ayala Rodiles, Sara Isabel.
Revisión del ciclo de vida del desarrollo de sistemas.
México, 1991

5. Cabrera Molina, José.
Seminario Ejecutivo Modelo de Madurez en
Procesos del Software Engineering Institute.
Quality Assurance Institute / Instituto Tecnológico de Informática.
México, 1996

6. Cabrera Molina, José.
Seminario Establecimiento de Convenios de Servicio.
Quality Assurance Institute / Instituto Tecnológico de Informática.
México, 1994

7. Chiavenato, Idalberto.
Introduccion a la teoria de la administración.
Ed Mc Graw Hill
México, 1987

8. **De la Cámara Cordero, Ana María.**
Seminario de redes locales.
Novellco de México, S.A. de C.V.
*México, 1990*

9. **Deitel, Harvey M.**
Introducción a los sistemas operativos.
Ed. Addison Wesley Iberoamericana.
México, 1987

10. **Echenique García, José Antonio.**
Auditoría en Informática.
Ed. Limusa.
*México, 1996*

11. **Hammer, Michael & Champy, James.**
Reingeniería.
Grupo Editorial Norma.
México, 1994

12. **Holm[illegible] Arthur W.**
Prin[illegible]sicos de auditoría.
Ed. Diana.
México, 1994

13. **IBM Centro Latinoamericano de Desarrollo.**
Auditoría, seguridad y control en informática.
México, 1996

14. **Information Systems Audit and Control Foundation.**
Control Objectives for Information and Related Technology (COBIT).
USA, april 1996

15. **Instituto Mexicano de Contadores Públicos.**
*Boletines C y E-02. Normas y procedimientos de auditoría.*
México, 1996

16. **Leonard, William P.**
Auditoría administrativa.
Ed. Diana.
México, 1991

17. **Mancera, S.C.**
Conferencia Informes de Auditoría.
Cuernavaca, Mor., marzo 3, 1997

18. **Márquez, Pablo Enrique.**
El papel de la Auditoría en la organización.
México, 1991

19. **Matcheti, Noel D.**
Seguridad de redes.
Technology Training S. de R.L. de C.V.
México, 1993

20. Microsoft Corporation.
Managing Microsoft Windows NT.
'Advanced Server'.
USA, 1993

21. MIS Training Institute.
Área local de la red.
'Cuestionario de seguridad y auditoría
USA, 1995

22. Mora, José Luis y Molina, Enzo.
Introducción a la informática
Ed. Diana
México, 1994

23. Newnan, Donald G.
Análisis económico en ingeniería
Ed. Mc Graw Hill
México, 1985

24. **Nolan, Richard L.**
Como administrar las crisis en el procesamiento de datos.
*Biblioteca Harvard de Administración de Empresas.*
México, 1980

25. **Novellco de México S.A. de C.V.**
Seminario de Conectividad de Redes LAN.
México, 1990

26. **Ogata, Katsuhiko.**
*Ingenieria de control moderna.*
*Ed. Prentice-Hall Hispanoamericana.*
México, 1991

27. **Petit, Robert.**
Diccionario de la lengua francesa.
Ed. Promexa.
México, 1985

28. **Reyes Ponce, Agustín.**
Administración de empresas. Teoria y práctica.
Ed. Limusa.
México, 1990

29. **Revista Informática.**
México, noviembre 1996 Núm. 27.

30. **Tanenbaum, Andrew S.**
Computer Networks.
Ed. Prentice Hall.
México, 1991

31. **The Federal Reserve Bank.**
FFIEC Examination Handbook.
USA, 1997

32. **The Information Systems Audit and Control Association.**
Manual de Revisión CISA 1997.
USA 1997

33. **The Institute of Internal Auditors, Inc.**
Systems Auditability and Control (SAC).
USA, 1996

34. **The Institute of Internal Auditors Research Foundation.**
Auditability and Control Report.
Altamonte Springs.
Florida USA, 1991

35. **Universidad Nacional Autónoma de México.**
Apuntes escolares de la carrera Ingeniería en Computación.
México, 1988 -1992