

AUDITORÍA EN INFORMÁTICA

José Antonio Echenique García

Mc
Graw
Hill

edición **2**

AUDITORÍA EN INFORMÁTICA

Segunda edición

JOSÉ ANTONIO ECHENIQUE GARCÍA

Universidad Nacional Autónoma de México

Universidad Autónoma Metropolitana

McGraw-Hill

**MÉXICO • BUENOS AIRES • CARACAS • GUATEMALA • LISBOA • MADRID
NUEVA YORK • SAN JUAN • SANTAFÉ DE BOGOTÁ • SANTIAGO • SÃO PAULO
AUCKLAND • LONDRES • MILÁN • MONTREAL • NUEVA DELHI • SAN FRANCISCO
SINGAPUR • ST. LOUIS • SIDNEY • TORONTO**

CONTENIDO

AGRADECIMIENTOS	ix
INTRODUCCIÓN	xi
CAPÍTULO 1: Concepto de auditoría en informática y diversos tipos de auditorías	1
Concepto de auditoría y concepto de informática	2
Diversos tipos de auditoría y su relación con la auditoría en informática	5
Auditoría interna/externa y auditoría contable/financiera	5
Auditoría administrativa/operacional	9
Auditoría con informática	10
Definición de auditoría en informática	17
Concepto de auditoría en informática	17
Campo de la auditoría en informática	20
Auditoría de programas	22
CAPÍTULO 2: Planeación de la auditoría en informática	25
Fases de la auditoría	26
Planeación de la auditoría en informática	30
Revisión preliminar	32
Revisión detallada	33
Examen y evaluación de la información	34
Pruebas de consentimiento	35
Pruebas de controles del usuario	36
Pruebas sustantivas	36
Evaluación de los sistemas de acuerdo al riesgo	38
Investigación preliminar	39
Personal participante	42
CAPÍTULO 3: Auditoría de la función de informática	55
Recopilación de la información organizacional	56
Principales planes que se requieren dentro de la organización de informática	58
Evaluación de la estructura orgánica	61
Estructura orgánica	63
Funciones	67
Objetivos	72
Análisis de organizaciones	75
Evaluación de los recursos humanos	76
Entrevistas con el personal de informática	82
Situación presupuestal y financiera	84

Presupuestos	84
Recursos financieros	85
Recursos materiales	86
CAPÍTULO 4: Evaluación de los sistemas	89
Evaluación de sistemas	90
Evaluación del análisis	95
Análisis y diseño estructurado	97
Evaluación del diseño lógico del sistema	98
Programas de desarrollo	98
Bases de datos	99
El administrador de bases de datos	100
Comunicación	102
Informes	103
Análisis de informes	113
Ruido, redundancia, entropía	113
Evaluación del desarrollo del sistema	115
Sistemas distribuidos, Internet, comunicación entre oficinas	116
Control de proyectos	117
Control de diseño de sistemas y programación	119
Instructivos de operación	132
Forma de implantación	133
Equipo y facilidades de programación	133
Entrevistas a usuarios	133
Entrevistas	134
Cuestionario	134
Derechos de autor y secretos industriales	138
Internet	142
Protección de los derechos de autor	144
Secretos industriales	145
CAPÍTULO 5: Evaluación del proceso de datos y de los equipos de cómputo	155
Controles	156
Control de datos fuente y manejo de cifras de control	161
Control de operación	164
Control de salida	170
Control de asignación de trabajo	171
Control de medios de almacenamiento masivo	173
Control de mantenimiento	176
Orden en el centro de cómputo	182
Evaluación de la configuración del sistema de cómputo	183
Productividad	185
Puntos a evaluar en los equipos	186
CAPÍTULO 6: Evaluación de la seguridad	191
Seguridad lógica y confidencialidad	194

Seguri
Riesgo
Encr
Segurida
Segurida
Ubica
Piso ele
Aire ac
Instala
Seguri
Seguri
Detecc
Temper
Segurida
Protecc
Seguros
Condic
Segurida
Segurida
Plan de con
de desa
Plan de
Selecció

CAPÍTULO

Técnicas par
Análisis
Metodo
Evaluación
Análisis
Evaluación
Evaluaci
Evaluaci
Evaluaci
Controles
Presentación

Conclusiones

Bibliografía

Índice analít

84	Seguridad lógica	196
85	Riesgos y controles a auditar	205
86	Encriptamiento	216
89	Seguridad en el personal	218
90	Seguridad física	219
95	Ubicación y construcción del centro de cómputo	220
97	Piso elevado o cámara plena	221
98	Aire acondicionado	221
98	Instalación eléctrica y suministro de energía	222
99	Seguridad contra desastres provocados por agua	224
100	Seguridad de autorización de accesos	225
102	Detección de humo y fuego, extintores	226
103	Temperatura y humedad	227
113	Seguridad en contra de virus	236
113	Protecciones contra virus y elementos a auditar	237
115	Seguros	240
116	Condiciones generales del seguro de equipo electrónico	241
117	Seguridad en la utilización del equipo	247
119	Seguridad al restaurar el equipo	249
132	Plan de contingencia y procedimientos de respaldo para casos de desastre	251
133	Plan de contingencias	252
133	Selección de la estrategia	262
134	CAPÍTULO 7: Interpretación de la información	269
138	Técnicas para la interpretación de la información	270
142	Análisis crítico de los hechos	270
144	Metodología para obtener el grado de madurez del sistema	271
145	Evaluación de los sistemas	272
155	Análisis	272
161	Evaluación de los sistemas de información	276
164	Evaluación en la ejecución	277
170	Evaluación en el impacto	278
171	Evaluación económica	279
173	Evaluación subjetiva	280
176	Controles	281
182	Presentación	285
183	Conclusiones	289
185	Bibliografía	291
186	Índice analítico	293

INTRODUCCIÓN

En la actualidad el costo de los equipos de cómputo ha disminuido considerablemente, mientras que sus capacidades y posibilidades de utilización han aumentado en forma inversa a la reducción de sus costos. Aunque los costos unitarios han disminuido (el de una computadora personal, "microcomputadora"), los costos totales de la computación (de equipos, sistemas, paquetes, recursos humanos, consumibles, etc.) se han incrementado considerablemente. Ello se debe a que, si bien la relación precio/memoria es menor, el tamaño de la memoria de los equipos y sus capacidades son mucho mayores, con procesadores y dispositivos que permiten acceso de más datos en mucho menos tiempo y que procesan la información en forma más rápida (memorias RAM y ROM, discos fijos, etc.). Esto hace que, aunque se han reducido los costos, al aumentar sus capacidades y facilidades se ha incrementado el costo total, lo que ha tenido como consecuencia que los costos totales del uso no hayan disminuido en todos los casos. Las nuevas herramientas con que se cuenta (Internet, Extranet, comunicación, bases de datos, multimedia, etc.) hacen que también se pueda tener acceso a mayor información, aunque el costo total de los sistemas, así como la confiabilidad y seguridad con que se debe trabajar, sean muy altos.

En algunas ocasiones ha disminuido el costo de las aplicaciones, pero se tiene poca productividad en relación con la información y uso que se da a éstas. También se tiene poco control sobre la utilización de los equipos, existe un deficiente sistema de seguridad tanto física como lógica y se presenta una falta de confidencialidad de la información. Lo que se debe incrementar es la productividad, el control, la seguridad y la confidencialidad, para tener la información necesaria en el tiempo y en el lugar adecuados para poder tomar las mejores decisiones.

Los siguientes puntos de la tecnología de información son particularmente notables:

- Una gran disponibilidad de hardware de computadoras muy poderosos y baratos, incluyendo la incorporación, a través de la miniaturización de poderosas capacidades, en diferentes dispositivos diseñados para usos personales y profesionales.
- Una gran disponibilidad de software poderoso, barato y relativamente accesible, con interfaces de uso gráfico.
- A la medida del cliente, cambio de sistemas a software preempacado.
- Cambio de computadoras principales (*mainframe*) a computadoras de uso individual o aumentadas como parte de redes dedicadas a compartir información, así como computadoras corporativas con los correspondientes cam-

bios en la naturaleza, organización y localización de actividades de los sistemas de información, como el cambio a computadoras de usuario final.

- Incremento en la habilidad de las computadoras para acceder datos en tiempo real o demorado, ambos en forma local o a través de acceso a facilidades remotas, incluyendo vía Internet.
- Captura de nuevos datos y el liderazgo en tecnología en almacenamiento máximo para incrementar la computarización, datos/información en textos, gráficas y video, con énfasis en la administración, presentación y comunicación de información, utilizando aproximaciones de multimedia.
- La cobertura de información y las tecnologías de comunicación afectan la forma en que se trabaja y se compra.
- Incremento del uso de Internet para unir individuos, intraorganizaciones, a través de sistemas tales como correo electrónico (E-mail), Internet, incluyendo world y wide web.
- El incremento en el uso de Internet para conducir comunicación entre organizaciones e individuos, a través de sistemas de comercio electrónico, tales como intercambio electrónico de datos (EDI) y sistema de transferencia electrónica de fondos (EFTS).
- Mercadeo masivo y distribución de productos de tecnología de información y servicios, tales como computadoras, software preempacado, servicio de recuperación de datos en línea, correo electrónico y servicios financieros.
- Reducción de barreras de uso de sistemas, estimulando una gran penetración de sistemas de información dentro de organizaciones de todos los tamaños, de lucro o no lucrativas, para contadores y consejos de administración, y para propósitos estratégicos e incremento de papeles del usuario final de computadoras.
- Una amplia penetración de tecnología de información, tal como diseño de manufactura por medio de asistencia computarizada (CAD/CAM), sistema de imágenes por computadora, sistemas de información para ejecutivos (EIS) y sistemas de reuniones en forma electrónica (EMS).
- Nuevas técnicas de desarrollo de sistemas, basados en tecnologías de información, tales como software de ingeniería de asistencia computarizada (CASE), programación orientada a objetos y tecnología de flujos (WORKFLOW).
- Desarrollo continuo de soporte de sistemas inteligentes, incorporando sistemas expertos, redes neuronales, agentes inteligentes y otras ayudas de solución de problemas.
- Acceso a reingeniería de nuevos negocios, basado en la integración efectiva de tecnología de información y procesos de negocios.

Uno de los problemas más frecuentes en los centros de informática es la falta de una adecuada organización, que permita avanzar al ritmo de las exigencias de las organizaciones. A esto hay que agregar la situación que presentan los nuevos equipos en cuanto al uso de bases de datos, redes y sistemas de información. Lo anterior, combinado con la necesidad de una eficiente planeación estratégica y corporativa de las organizaciones, y con una descentralización de equipos y centralización de la información, ha provocado que la complejidad de las decisiones, y las dimensiones de los problemas en cuanto a la mejor for-

ma de organizar control y adminis-

En muchos pleo de herramien- puestos, finanzas repercute en una i- nes con las caract- hace que no se cue- desvíen de los obje-

La proliferaci- manda de control- vacidad de la infor- Además, hay una- dad de la continui- sistemas se caigan- incompatibles y el-

Los sistemas ti- de las herramient- Para poder evaluar- larlo desde su inici- electrónico, o bien- respaldos, segurida- No basta, pues, con- pos de cómputo, qu- ma total de inform-

La informática l- mos años. En una g- prendió hace algun- creación del horno- década hemos visto- era algo común la tar- remoto, y consideran- redes. Esto ha provo- mática. Ya no podem- con microcomputad- conocía en detalle so- de tener especialistas- informática, y en ella- rentes funciones que- de la informática y de-

El principal objeti- los siguientes puntos

- La parte administ
- Los recursos mate
- Los sistemas y pro- necesidades de la

ma de organizar el área de cómputo, requieran aplicar técnicas modernas de control y administración.

En muchos centros de informática también se desconoce el adecuado empleo de herramientas administrativas, contables / financieras, tales como presupuestos, finanzas, costos, recursos humanos, organización, control, etc. Esto repercute en una inadecuada área de informática que no permite tomar decisiones con las características que deben tener las organizaciones actuales, lo cual hace que no se cuente con los controles para asegurar que esas decisiones no se desvíen de los objetivos.

La proliferación de la tecnología de información ha incrementado la demanda de control de los sistemas de información, como el control sobre la privacidad de la información y su integridad, y sobre los cambios de los sistemas. Además, hay una preocupación sobre la caída de los sistemas y sobre la seguridad de la continuidad del procesamiento de la información, en caso de que los sistemas se caigan. Otra área de preocupación es la proliferación de subsistemas incompatibles y el ineficiente uso de los recursos de sistemas.

Los sistemas tienen diferentes etapas, y una de ellas puede ser la utilización de las herramientas que nos proporcionan los mismos sistemas electrónicos. Para poder evaluar un sistema de información es necesario conocerlo y controlarlo desde su inicio, siguiendo su proceso, que puede ser manual, mecánico, electrónico, o bien la combinación de éstos, hasta llegar a su almacenamiento, respaldos, seguridad y eficiencia en el uso de la información que proporcionan. No basta, pues, conocer una parte o fase del sistema, como pueden ser los equipos de cómputo, que tan sólo vienen a ser una herramienta dentro de un sistema total de información.

La informática ha sido un área que ha cambiado drásticamente en los últimos años. En una generación, la tecnología ha cambiado tanto que lo que sorprendió hace algunos años, como la llegada del hombre a la Luna, o bien la creación del horno de microondas, hoy nos parece algo muy familiar. En una década hemos visto el cambio en la organización de la informática: si hace poco era algo común la tarjeta perforada, hoy la vemos como algo de un pasado muy remoto, y consideramos como algo normal el uso de microcomputadoras y de redes. Esto ha provocado que se tengan especialistas dentro del área de la informática. Ya no podemos pensar en el personal de informática que podía trabajar con microcomputadores y con grandes computadoras, o bien en la persona que conocía en detalle sobre bases de datos y de comunicaciones. Ahora se deben de tener especialistas en cada una de las áreas. Una de éstas es la auditoría en informática, y en ella debemos de tener especialistas para cada una de las diferentes funciones que se realizarán. Esto sin duda depende del tamaño del área de la informática y de la organización.

El principal objetivo del libro es evaluar la función de la informática desde los siguientes puntos de vista:

- La parte administrativa del departamento de informática.
- Los recursos materiales y técnicos del área de informática.
- Los sistemas y procedimientos, y la eficiencia de su uso y su relación con las necesidades de la organización.

Es conveniente precisar y aclarar que la función de la auditoría en informática se ubica dentro del contexto de la organización, dependiendo de su tamaño y características. La profundidad con la que se realice, dependerá también de las características y del número de equipos de cómputo con que se cuente. El presente libro señala un panorama general, pero habrá que adecuar éste y profundizar de acuerdo a la organización de que se trate y de los equipos, software y comunicación que se auditen.

Para cualquier comentario sobre esta obra, los lectores pueden dirigirse a la dirección del autor en Internet: jaeg@correo.uam.mx

CAPÍTULO

OBJ

Al finaliz

1

CAPÍTULO

Concepto de auditoría en informática y diversos tipos de auditorías

OBJETIVOS

Al finalizar este capítulo, usted:

1. Analizará los conceptos de auditoría e informática.
2. Conocerá los diversos tipos de auditoría y su relación con la auditoría en informática.
3. Expondrá cuáles son las técnicas avanzadas que se utilizan en la auditoría con informática.
4. Describirá las habilidades fundamentales que debe tener todo auditor de informática.
5. Definirá cuál es el campo de la auditoría en informática.
6. Explicará cuáles son los principales objetivos de la auditoría en informática.

CONCEPTO DE AUDITORÍA Y CONCEPTO DE INFORMÁTICA

Auditoría. Con frecuencia la palabra auditoría se ha empleado incorrectamente y se le ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. Por eso se ha llegado a usar la frase "tiene auditoría" como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría es más amplio; no sólo detecta errores: es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos.

La palabra auditoría viene del latín *auditorius*, y de ésta proviene "auditor", el que tiene la virtud de oír; el diccionario lo define como "revisor de cuentas colegiado".¹ El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico, que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

Si consultamos nuevamente el diccionario encontramos que eficacia es: "virtud, actividad, fuerza, para poder obrar";² mientras que eficiencia es: "virtud y facultad para lograr un efecto determinado", es decir, es el poder lograr lo planeado con los menores recursos posibles, mientras que eficacia es lograr los objetivos.

El Boletín C de normas de auditoría³ del Instituto Mexicano de Contadores nos dice:

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 de seguirse y estimar los resultados obtenidos.

Así como existen normas y procedimientos específicos para la realización de auditorías contables, debe haber también normas y procedimientos para la realización de auditorías en informática como parte de una profesión. Éstas pueden estar basadas en las experiencias de otras profesiones, pero con algunas características propias y siempre guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, y que además la audito-

¹ Nuevo Diccionario Español Sopena.

² Idem.

³ Normas y procedimientos de auditoría, Instituto Mexicano de Contadores Públicos.

ría debe eva-
tivas de sol

Informática
equipos de
conferencia
tica de la Fa
Nacional A

No exist
palabra i
la conjur
fue estim
mecanici

En 1966,
del modo sig

Ciencia d
máquinas
humano y

Hacia pri
ción, sobre to
por redefinir
Interguberna
UNESCO. Es
ello, formuló

Aplicación
social y po

La IBI tan
ca que, aunqu

Ciencia de

En 1977,
Mexicana de l

Ciencia de

En alguna
proceso electro
más amplio, ya
la cual puede

⁴ Boletín del C

ría debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución.

Informática. El concepto de informática es más amplio que el simple uso de equipos de cómputo o bien de procesos electrónicos. Veamos lo que se dijo en la conferencia presentada del 5 al 9 de diciembre de 1983 en el Centro de Informática de la Facultad de Contaduría y Administración (CIFCA) de la Universidad Nacional Autónoma de México:⁴

No existe una sola concepción acerca de qué es informática; etimológicamente, la palabra informática deriva del francés *informatique*. Este neologismo proviene de la conjunción de *information* (información) y *automatique* (automática). Su creación fue estimulada por la intención de dar una alternativa menos tecnocrática y menos mecanicista al concepto de "proceso de datos".

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.

Hacia principios de los setenta ya eran claras las limitaciones de esta definición, sobre todo por el hincapié en el uso de las máquinas. El principal esfuerzo por redefinir el concepto de informática lo realizó en esa época la Oficina Intergubernamental de Informática (IBI), en aquel tiempo órgano asociado a la UNESCO. Este organismo, a través de los comités expertos convocados para ello, formuló en 1975 esta definición:

Aplicación racional, sistemática de la información para el desarrollo económico, social y político.

La IBI también dio en esa época una descripción del concepto de informática que, aunque no constituye una definición formal, resulta muy descriptiva:

Ciencia de la política de la información.

En 1977, con la intención de actualizar y afinar el concepto, la Academia Mexicana de Informática propuso la siguiente definición:

Ciencia de los sistemas inteligentes de información.

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

⁴ Boletín del Centro de Informática de la FCA de la UNAM, núm. 99, vol. 11, mayo de 1984.

Proceso de
información de
la información

Niveles de información

Esto es importante!
Distribución de
Información
Clasificación
de la información

Difusión 2

Parte jurídica (Criterio)

Planeación y Control
de la Información

Teoría de Sistemas
Bases de datos
Sistemas de Comunicación
Sistemas de Información

También es común confundir el concepto de dato con el de información. La información es una serie de datos clasificados y ordenados con un objetivo común. El dato se refiere únicamente a un símbolo, signo o a una serie de letras o números, sin un objetivo que dé un significado a esa serie de símbolos, signos, letras o números.

La información está orientada a reducir la incertidumbre del receptor y tiene la característica de poder duplicarse prácticamente sin costo, no se gasta. Además no existe por sí misma, sino que debe expresarse en algún objeto (papel, cinta, etc.); de otra manera puede desaparecer o deformarse, como sucede con la comunicación oral, lo cual hace que la información deba ser controlada debidamente por medio de adecuados sistemas de seguridad, confidencialidad y respaldo.

La información puede comunicarse, y para ello hay que lograr que los medios de seguridad sean llevados a cabo después de un adecuado examen de la forma de transmisión, de la eficiencia de los canales de comunicación [el transmisor, el receptor, el contenido de la comunicación, la redundancia y el ruido].

La información ha sido dividida en varios niveles. El primero es el nivel técnico, que considera los aspectos de eficiencia y capacidad de los canales de transmisión; el segundo es el nivel semántico, que se ocupa de la información desde el punto de vista de su significado; el tercero es el pragmático, el cual considera al receptor en un contexto dado, y el cuarto nivel analiza la información desde el punto de vista normativo y de la parte ética, o sea considera cuándo, dónde y a quién se destina la información o la difusión que se le dé.

La informática debe abarcar los cuatro niveles de información. En el cuarto nivel tenemos una serie de aspectos importantes, como la parte legal del uso de la información, los estudios que se han hecho sobre la parte jurídica de la informática y la creación de la ética en informática, que no sólo debe incluir a los profesionales técnicos y especialistas en informática, sino también a los usuarios tanto de grandes computadoras como de computadoras personales.

La información tradicional (oral y escrita) se ve afectada dentro de la informática cuando se introduce el manejo de medios electrónicos, lo cual la hace fácilmente modificable y adaptable a las características de cada receptor. La información también tiene la capacidad de manejarse en forma rápida y en grandes volúmenes, lo cual permite generar, localizar, duplicar y distribuir la información de modo sorprendente, a través de métodos, técnicas y herramientas como microcomputadoras, procesos distribuidos, redes de comunicación, bases de datos, etcétera.

La nueva tecnología permite que el usuario disponga de la información en cualquier momento, ya sea para su acceso, actualización, cambio o explotación o para que pueda distribuirse e intercambiarse entre tantos usuarios como se desee. Aunque al mismo tiempo se plantea un gran problema en cuanto al cuarto nivel de la información, que es su parte ética y el estudio de las posibilidades del buen o mal uso de la información por parte de personas no autorizadas.

La planeación y control de la información nos ofrece nuevos aspectos importantes a considerar, entre los que están la teoría de sistemas, las bases de datos, los sistemas de comunicación y los sistemas de información, que van a complementar el concepto de informática y su campo de acción.

DIVER Y SU R EN INF

AUDIT Y AUDI

El Boletín E
interno:

El estud
la norm
estudio
para det
permita
procedir
El o
procedir
guardar
financier
ticas pre

Objetivos b
tro objetivos

- La prote
- La obten
- La prom
- Lograr c
blecidas

Se ha es
troles intern
nistrativos.

Objetivos g
de el plan de
protección d

⁵ Boletín E
Públicos.

DIVERSOS TIPOS DE AUDITORÍA Y SU RELACIÓN CON LA AUDITORÍA EN INFORMÁTICA

DIVERSOS TIPOS DE
AUDITORÍA Y SU
RELACIÓN CON
LA AUDITORÍA EN
INFORMÁTICA

AUDITORÍA INTERNA/EXTERNA Y AUDITORÍA CONTABLE/FINANCIERA

El Boletín E-02 del Instituto Mexicano de Contadores⁵ señala respecto al control interno:

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 debe efectuar un estudio y evaluación adecuados del control interno existente, que le sirvan de base para determinar el grado de confianza que va a depositar en él, así mismo, que le permitan determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría.

El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración.

Definición y
objetivos del
control interno

Objetivos básicos del control interno. De lo anterior se desprende que los cuatro objetivos básicos del control interno son:

- La protección de los activos de la empresa.
- La obtención de información financiera veraz, confiable y oportuna.
- La promoción de la eficiencia en la operación del negocio.
- Lograr que en la ejecución de las operaciones se cumplan las políticas establecidas por los administradores de la empresa.

Se ha establecido que los dos primeros objetivos abarcan el aspecto de controles internos contables y los dos últimos se refieren a controles internos administrativos.

Objetivos generales del control interno. El control interno contable comprende el plan de organización y los procedimientos y registros que se refieren a la protección de los activos y a la confiabilidad de los registros financieros. Por lo

⁵ Boletín E-02. Normas y procedimientos de auditoría, Instituto Mexicano de Contadores Públicos.

tanto, está diseñado en función de los objetivos de la organización para ofrecer seguridad razonable de que las operaciones se realizan de acuerdo con las normas y políticas señaladas por la administración.

Cuando hablamos de los objetivos de los controles contables internos podemos identificar dos niveles:

- A) Objetivos generales de control interno aplicables a todos los sistemas
- B) Objetivos de control interno aplicables a ciclos de transacciones

⊗ Los objetivos generales de control aplicables a todos los sistemas se desarrollan a partir de los objetivos básicos enumerados anteriormente, y son más específicos, para facilitar su aplicación. Los objetivos de control de ciclos se desarrollan a partir de los objetivos generales de control de sistemas, para que se apliquen a las diferentes clases de transacciones agrupadas en un ciclo.

⊗ Los objetivos generales de control interno de sistemas pueden resumirse a continuación.

Objetivos de autorización

Todas las operaciones deben realizarse de acuerdo con autorizaciones generales o especificaciones de la administración.

Las autorizaciones deben estar de acuerdo con criterios establecidos por el nivel apropiado de la administración.

Las transacciones deben ser válidas para conocerse y ser sometidas oportunamente a su aceptación. Todas aquellas que reúnan los requisitos establecidos por la administración deben reconocerse como tales y procesarse a tiempo.

Los resultados del procesamiento de transacciones deben comunicarse oportunamente y estar respaldados por archivos adecuados.

Objetivos del procesamiento y clasificación de transacciones

Todas las operaciones deben registrarse para permitir la preparación de estados financieros en 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 en conformidad con los principios de contabilidad generalmente aceptados según el criterio de la administración.

Las transacciones deben quedar registradas en el mismo periodo contable, cuidando de manera específica que se registren aquellas que afectan más de un ciclo.

Objetivo

El acceso administr

Objetivo

Los datos se con los das aprop

Asimi periódica objetivo c

Estos todos los c cas de cor desarrollan que sean a

El área no. La prin interno, y l informática

En el p una organi en el logro auditoría. Informática. En decir, como adecuadam se obtenga mejore la ef y para que políticas est control inte

Al estud que, aunque tener en cue clo de trans

La audit ción, procesa da física, ver rencia entre financiero es zación media tivos del con

Objetivo de salvaguarda física

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

Objetivo de verificación y evaluación

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

Asimismo, deben existir controles relativos a la verificación y evaluación periódica de los saldos que se incluyen en los estados financieros, ya que este objetivo complementa en forma importante los mencionados anteriormente.

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 interactuar 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 el primer caso se lleva el control interno por medio de la evaluación de una organización, utilizando la computadora como herramienta que auxiliará en el logro de los objetivos, lo cual se puede hacer por medio de paquetes de auditoría. Esto debe ser considerado como parte del control interno con informática. En el segundo caso se lleva a cabo el control interno de 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, para que se mejore la eficiencia de la operación de la organización mediante la informática, y para que en la ejecución de las operaciones de informática se cumplan las políticas establecidas por la administración: todo ello debe ser considerado como control interno de informática.

Al estudiar los objetivos del control interno podemos ver en primer lugar que, aunque en auditoría en informática el objetivo es más amplio, se deben tener en cuenta los objetivos generales del control interno aplicables a todo ciclo de transacciones.

La auditoría en informática debe tener presentes los objetivos de autorización, procesamiento y clasificación de transacciones, así como los de salvaguarda física, verificación y evaluación de los equipos y de la información. La diferencia entre los objetivos de control interno desde un punto de vista contable financiero es que, mientras éstos están enfocados a la evaluación de una organización mediante la revisión contable financiera y de otras operaciones, los objetivos del control interno en informática están orientados a todos los sistemas en

general, al equipo de cómputo y al departamento de informática, para lo cual se requieren conocimientos de contabilidad, finanzas, recursos humanos, administración, etc., así como de experiencia y un saber profundo en informática.

La auditoría interna debe estar presente en todas y cada una de las partes de la organización. Ahora bien, la pregunta que normalmente se plantea es: ¿cuál debe ser su participación dentro del área de informática?

La informática es en primer lugar una herramienta muy valiosa que debe tener un adecuado control y es un auxiliar de la auditoría interna. Pero, según este concepto, la auditoría interna puede considerarse como un usuario del área de informática.

Se ha estudiado que los objetivos generales del control interno son:

- Autorización.
- Procesamiento y clasificación de las transacciones.
- Salvaguarda física.
- Verificación y evaluación.

Con base en los objetivos y responsabilidades del control interno podemos hacer otras dos preguntas: ¿De qué manera puede participar el personal de control interno en el diseño de los sistemas? ¿Qué conocimientos debe tener el personal de control interno para poder cumplir adecuadamente sus funciones dentro del área de informática?

Las respuestas a estas preguntas dependerán del nivel que tenga el control interno dentro de la organización. Sin embargo, en el diseño general y detallado de los sistemas se debe incluir a personal de la contraloría interna, que habrá de tener conocimientos de informática, aunque no se requerirá que sean especialistas, ya que sólo intervendrán en el diseño general del sistema, en el diseño de controles, en los sistemas de seguridad, en el respaldo y confidencialidad del sistema y en los sistemas de verificación. Se habrán de comprobar las fórmulas de obtención del impuesto sobre el producto del trabajo, el cálculo del pago del seguro social, etc., pero no deberán intervenir en la elaboración de los sistemas, bases de datos o programación. Tendrán que comprobar que lo señalado en el diseño general sea igual a lo obtenido en el momento de implantación, para que puedan dar su autorización a la corrida en paralelo.

El auditor interno, en el momento en que se están elaborando los sistemas, debe participar en estas etapas:

- Asegurarse de verificar que los requerimientos de seguridad y de auditoría sean incorporados, y participar en la revisión de puntos de verificación.
- Revisar la aplicación de los sistemas y de control tanto con el usuario como en el centro de informática.
- Verificar que las políticas de seguridad y los procedimientos estén incorporados al plan en caso de desastre.
- Incorporar técnicas avanzadas de auditoría en los sistemas de cómputo.

Los sistemas de seguridad no pueden llevarse a cabo a menos que existan procedimientos de control y un adecuado plan en caso de desastre, elaborados desde el momento en el que se diseña el sistema.

El auditor
planes a largo
de tal manera
dad sean incor

AUDITO

La tecnología e
están estructu
son dramático
administrativo
planeación ad
trol interno de
de la tecnologí
está soportado
nología.

William P.

El examen g
ción, una se
planes y ob
des humana

Se lleva a c
presa con el fir

- Pérdidas y
- Mejores me
- Mejores fo
- Operacione
- Mejor uso

La auditorí
del área de inf
auditoría en inf
aplicarlos al ár

El departa

- Objetivos,
- Organizaci
- Estructura
- Funciones

⁶ William P. I

El auditor interno desempeña una importante función al participar en los planes a largo plazo y en el diseño detallado de los sistemas y su implantación, de tal manera que se asegure que los procedimientos de auditoría y de seguridad sean incorporados a todas y cada una de las fases del sistema.

AUDITORÍA ADMINISTRATIVA/OPERACIONAL

La tecnología en información está afectando la forma en que las organizaciones están estructuradas, administradas y operadas. En algunos casos, los cambios son dramáticos. Cuando existe la necesidad de un nuevo diseño de sistemas administrativos para lograr una efectiva administración y control financiero, la planeación administrativa y el proceso de diseño y los requerimientos de control interno deberán cambiar o necesariamente se modificarán con los cambios de la tecnología de información. El incremento de la tecnología de información está soportado por una reestructuración organizacional alrededor de esta tecnología.

William P. Leonard⁶ define la auditoría administrativa como:

El examen global y constructivo de la estructura de una empresa, de una institución, una sección del gobierno o cualquier parte de un organismo, en cuanto a sus planes y objetivos, sus métodos y controles, su forma de operación y sus facilidades humanas y física.

Se lleva a cabo una revisión y consideración de la organización de una empresa con el fin de precisar:

- Pérdidas y deficiencias.
- Mejores métodos.
- Mejores formas de control.
- Operaciones más eficientes.
- Mejor uso de los recursos físicos y humanos.

La auditoría administrativa debe llevarse a cabo como parte de la auditoría del área de informática; se ha de considerar dentro del programa de trabajo de auditoría en informática, tomando principios de la auditoría administrativa para aplicarlos al área de informática.

El departamento de informática se deberá evaluar de acuerdo con:

- Objetivos, metas, planes, políticas y procedimientos.
- Organización.
- Estructura orgánica.
- Funciones y niveles de autoridad y responsabilidad.

⁶ William P. Leonard, *Auditoría administrativa*, editorial Diana.

7.1 { Estructura
Administrativa
Operativa

Hay 3 tipos de Auditoría:
- Operativa
- Financiera
- Integrada.

Además, es importante tener en cuenta los siguientes factores:

- Elemento humano.
- Organización (manual de organización).
- Integración.
- Dirección.
- Supervisión.
- Comunicación y coordinación.
- Delegación.
- Recursos materiales.
- Recursos técnicos.
- Recursos financieros.
- Control.

AUDITORÍA CON INFORMÁTICA

Concepto de auditoría con informática

Los procedimientos de auditoría con informática varían de acuerdo con la filosofía y técnica de cada organización y departamento de auditoría en particular. Sin embargo, existen ciertas técnicas y/o procedimientos que son compatibles en la mayoría de los ambientes de informática. Estas técnicas caen en dos categorías: métodos manuales y métodos asistidos por computadora.

Utilización de las técnicas de auditorías asistidas por computadora

En general, el auditor debe utilizar la computadora en la ejecución de la auditoría, ya que esta herramienta permitirá ampliar la cobertura del examen, reduciendo el tiempo/costo de las pruebas y procedimientos de muestreo, que de otra manera tendrían que efectuarse manualmente. Existen paquetes de computadora (software) que permiten elaborar auditorías a sistemas financieros y contables que se encuentran en medios informáticos. Además, el empleo de la computadora por el auditor le permite familiarizarse con la operación del equipo en el centro de cómputo de la institución. Una computadora puede ser empleada por el auditor en:

- Transmisión de información de la contabilidad de la organización a la computadora del auditor, para ser trabajada por éste, o bien acceso al sistema en red para que el auditor elabore las pruebas.

- Verificación de reportes de información almacenada.
- Pruebas de la validez de las operaciones.
- Clasificación de las operaciones.
- Selección de operaciones.
- Llevar a cabo las acciones de control de la computadora.

Con fines para:

- Utilización de los datos de software.
- Supervisión de la auditoría.
- Utilización del equipo, que el auditor o mi-

Todos los datos deben estar bajo estricta documentación, además de los datos.

En aquellas organizaciones, los programas de protección de las instrucciones desde la biblioteca de objetos de hacer finir sus propósitos.

Cuando los datos internos deberán ser controlados adecuadamente.

- Mantener los datos en el sistema.
- Observar el sistema.
- Desarrollar el sistema de control.
- Mantener el sistema y control.

- Verificación de cifras totales y cálculos para comprobar la exactitud de los reportes de salida producidos por el departamento de informática, de la información enviada por medios de comunicación y de la información almacenada.
- Pruebas de los registros de los archivos para verificar la consistencia lógica, la validación de condiciones y la razonabilidad de los montos de las operaciones.
- Clasificación de datos y análisis de la ejecución de procedimientos.
- Selección e impresión de datos mediante técnicas de muestreo y confirmaciones.
- Llevar a cabo en forma independiente una simulación del proceso de transacciones para verificar la conexión y consistencia de los programas de computadora.

Con fines de auditoría, el auditor interno puede emplear la computadora para:

- Utilización de paquetes para auditoría; por ejemplo, paquetes provenientes del fabricante de equipos, firmas de contadores públicos o compañías de software.
- Supervisar la elaboración de programas que permitan el desarrollo de la auditoría interna.
- Utilización de programas de auditoría desarrollados por proveedores de equipo, que básicamente verifican la eficiencia en el empleo del computador o miden la eficiencia de los programas, su operación o ambas cosas.

*Análisis de un
software para
automatización
de auditorías*

Todos los programas o paquetes empleados en la auditoría deben permanecer bajo estricto control del departamento de auditoría. Por esto, toda la documentación, material de pruebas, listados fuente, programas fuente y objeto, además de los cambios que se les hagan, serán responsabilidad del auditor.

En aquellas instalaciones que cuentan con bibliotecas de programas catalogados, los programas de auditoría pueden ser guardados utilizando contraseñas de protección, situación que sería aceptable en tanto se tenga el control de las instrucciones necesarias para la recuperación y ejecución de los programas desde la biblioteca donde están almacenados. Los programas desarrollados con objeto de hacer auditoría deben estar cuidadosamente documentados para definir sus propósitos y objetivos y asegurar una ejecución continua.

Cuando los programas de auditoría estén siendo procesados, los auditores internos deberán asegurarse de la integridad del procesamiento mediante controles adecuados como:

- Mantener el control básico sobre los programas que se encuentren catalogados en el sistema y llevar a cabo protecciones apropiadas.
- Observar directamente el procesamiento de la aplicación de auditoría.
- Desarrollar programas independientes de control que monitoreen el procesamiento del programa de auditoría.
- Mantener el control sobre las especificaciones de los programas, documentación y comandos de control.

- Controlar la integridad de los archivos que se están procesando y las salidas generadas.

Técnicas avanzadas de auditoría con informática

Cuando en una instalación se encuentren operando sistemas avanzados de computación, como procesamiento en línea, bases de datos y procesamiento distribuido, se podría evaluar el sistema empleando técnicas avanzadas de auditoría. Estos métodos requieren un experto y, por lo tanto, pueden no ser apropiados si el departamento de auditoría no cuenta con el entrenamiento adecuado. Otra limitante, incluyendo el costo, puede ser la sobrecarga del sistema y la degradación en el tiempo de respuesta. Sin embargo, cuando se usan apropiadamente, estos métodos superan la utilización en una auditoría tradicional.

Pruebas integrales. Consisten en el procesamiento de datos de un departamento ficticio, comparando estos resultados con resultados predeterminados. En otras palabras, las transacciones iniciadas por el auditor son independientes de la aplicación normal, pero son procesadas al mismo tiempo. Se debe tener especial cuidado con las particiones que se están utilizando en el sistema para prueba de la contabilidad o balances, a fin de evitar situaciones anormales.

Simulación. Consiste en desarrollar programas de aplicación para determinada prueba y comparar los resultados de la simulación con la aplicación real.

Revisiones de acceso. Se conserva un registro computarizado de todos los accesos a determinados archivos; por ejemplo, información de la identificación tanto de la terminal como del usuario.

Operaciones en paralelo. Consiste en verificar la exactitud de la información sobre los resultados que produce un sistema nuevo que sustituye a uno ya auditado.

Evaluación de un sistema con datos de prueba. Esta verificación consiste en probar los resultados producidos en la aplicación con datos de prueba contra los resultados que fueron obtenidos inicialmente en las pruebas del programa (solamente aplicable cuando se hacen modificaciones a un sistema).

Registros extendidos. Consisten en agregar un campo de control a un registro determinado, como un campo especial a un registro extra, que pueda incluir datos de todos los programas de aplicación que forman parte del procesamiento de determinada transacción, como en los siguientes casos.

Totales aleatorios de ciertos programas. Se consiguen totales en algunas partes del sistema para ir verificando su exactitud en forma parcial.

Selección de d
de un archivo
parcial el archi
car en forma to

Resultados de
demos compar

Las técnica
una metodolog
ción, empleand
actualmente se
nan los problem
venir en las act
al departament
dencia al audit
auditor puede e
redes de comun

El empleo
mienta que faci

- Trasladar l
- Llevar a cal
- Verificar l
- Visualizaci
- Ordenamie

El auditor i
sistemas, con e
con las polític

A continua
dencia que exis
puede cambiar

Transacciones
ceso. En las apl
Por ejemplo, el
cuando el inve
computadora s
orden de repos
blecido.

El registro man
En las aplicaci
do la informaci
nómina puede
través de la red
tener una clave

Selección de determinado tipo de transacciones como auxiliar en el análisis de un archivo histórico. Por medio de este método podemos analizar en forma parcial el archivo histórico de un sistema, el cual sería casi imposible de verificar en forma total.

Resultados de ciertos cálculos para comparaciones posteriores. Con ellos podemos comparar en el futuro los totales en diferentes fechas.

Las técnicas anteriormente descritas ayudan al auditor interno a establecer una metodología para la revisión de los sistemas de aplicación de una institución, empleando como herramienta el mismo equipo de cómputo. Sin embargo, actualmente se han desarrollado programas y sistemas de auditoría que eliminan los problemas de responsabilidad del departamento de auditoría, al intervenir en las actividades e información cuyo control corresponde estrictamente al departamento de informática, lo cual proporciona una verdadera independencia al auditor en la revisión de los datos del sistema. En la actualidad, el auditor puede estar desarrollando algunas de sus funciones al intervenir en las redes de comunicación interna.

El empleo de la microcomputadora en la auditoría constituye una herramienta que facilita la realización de actividades de revisión como:

- Trasladar los datos del sistema a un ambiente de control del auditor.
- Llevar a cabo la selección de datos.
- Verificar la exactitud de los cálculos: muestreo estadístico.
- Visualización de datos.
- Ordenamiento de la información. Producción de reportes e histogramas.

El auditor interno debe participar en el diseño general y específico de los sistemas, con el fin de asegurar que se tengan todos los controles de acuerdo con las políticas internas antes de que se comience la programación del sistema.

A continuación se muestran ejemplos de las formas tradicionales de evidencia que existen en un proceso manual y las maneras en que la computadora puede cambiarlas:

Transacciones originadas por personas y accesadas a un sistema para su proceso. En las aplicaciones computarizadas, pueden generarse automáticamente. Por ejemplo, el sistema puede emitir automáticamente una orden de reposición cuando el inventario esté a un nivel por debajo del punto de reorden. Sin la computadora se requeriría que una persona estuviera revisando y elaborara la orden de reposición cuando el inventario estuviera abajo del mínimo ya establecido.

El registro manual de la información necesaria para originar una transacción. En las aplicaciones computarizadas no se producen documentos impresos cuando la información es accesada. Por ejemplo, un cambio hecho a las tarifas de nómina puede ser accesado a un archivo maestro de nóminas computarizado a través de la red interna, sin dejar registro impreso del cambio, aunque se debe tener una clave de seguridad para poder accederlo y llevar un registro histórico

en el que se tenga la información sobre la persona y terminal en la que se accedió la información.

La revisión de transacciones por el personal, que deja constancia con sus firmas, iniciales o sellos en los documentos para indicar la autorización del proceso. En las aplicaciones computarizadas la autorización puede ser automática. Por ejemplo, una venta a crédito puede ser automáticamente aprobada si el límite de crédito previamente determinado no está excedido. Otros métodos de autorización electrónica incluyen el acceso mediante claves de seguridad.

Anteriormente se tenían firmas en donde ahora sólo se tiene una clave o llave de acceso, que es equivalente a la autorización, dejando únicamente un registro (en el mejor de los casos) de la llave de acceso utilizada, el lugar donde se tuvo acceso y la hora y día en que fue autorizada.

El transporte de documentos de una estación de trabajo a otra por personas, correo o servicios similares de un lugar del negocio a otro sitio completamente distinto. Por estos medios se moviliza un documento físicamente. En aplicaciones computarizadas, los datos pueden ser enviados electrónicamente. La información es transcrita, codificada, frecuentemente condensada y entonces enviada electrónicamente por líneas de comunicaciones, y al final queda un registro de cuándo recibió la información el receptor.

Procesamiento manual. Generalmente, los documentos de las transacciones contienen espacio de trabajo para ejecutar el proceso necesario. En las aplicaciones computarizadas, el proceso se efectúa electrónicamente dentro de la memoria del computador mediante procedimientos programados y siguiendo reglas predeterminadas.

Proceso simplificado que facilita las ejecuciones repetitivas sin alta probabilidad de error. En las aplicaciones computarizadas, el proceso puede ser extremadamente complejo debido a la velocidad y exactitud del computador. Por ejemplo, una compañía puede utilizar su computadora para calcular la efectividad de cientos de posibles horarios o cédulas de producción a fin de seleccionar el más adecuado, mientras que en los métodos manuales esto sería casi imposible.

Mantenimiento en manuales de información de naturaleza fija que es necesaria para el proceso, como tarifas de nóminas o precios de productos. En las aplicaciones computarizadas, esta información se almacena en medios computarizados o bien por medio de catálogos; en los métodos manuales es difícil tener catálogos muy amplios y con actualización inmediata.

Listado de los resultados del proceso en documentos impresos, como cheques y reportes. Frecuentemente, estos documentos contienen resultados de procesos intermedios. En las aplicaciones computarizadas el proceso puede no dar por resultado documentos impresos. Por ejemplo, los fondos pueden ser transferidos electrónicamente. En algunos sistemas, la información rutinaria es

retenida de
ren acción.

Almacenam
archivo o si
recobrase n
computariza
ben utilizars
dios, los cual
de bases de

Uso de docu
nuales estos
métodos de
suficiente pa
partir de ésto
las pistas de
rre en un aml
serviría de pi
dos. Las pista
reglas del pro
ejecutaron, en

Uno o más m
a las transac
ción y proces
den ser inclui

Revisión de
minar su razo
nes computai
mente media
difícil para la
tacionales est
acorta; al mis
ción es mayor

La división de
la distribución
pleados, sino t
zado. Por ejen
partes de una
tengan sistema
en el caso de l

Proceso de gra
cruzamiento d
difícil y costoso

retenida de manera que sólo se recibe noticia de aquellas partidas que requieren acción.

Almacenamiento de documentos de entrada, proceso y salida en registro de archivo o similares. Cuando la información es necesaria, puede localizarse y recobrase manualmente del área de almacenamiento físico. En las aplicaciones computarizadas, la mayoría de los archivos están en medios magnéticos. Deben utilizarse programas extractivos para recobrar la información de tales medios, los cuales son normalmente muy rápidos y exactos, por ejemplo, en el caso de bases de datos.

Uso de documentos impresos para construir el proceso. En los procesos manuales estos documentos contienen información fuente, firmas de autorización, métodos de proceso y resultados de salida. Esta información usualmente es suficiente para construir la transacción y rastrearla hacia totales de control o, a partir de éstos, hasta el documento fuente. En las aplicaciones computarizadas, las pistas de auditoría pueden verse fragmentadas, como frecuentemente ocurre en un ambiente de base de datos. Además, gran parte de la información que serviría de pista de auditoría puede estar almacenada en medios computarizados. Las pistas de auditoría computarizadas a menudo requieren entender las reglas del proceso del sistema y no siempre es obvio cuáles pasos del proceso se ejecutaron, en especial cuando el proceso computacional es complejo.

Uno o más manuales de procedimientos que contienen información relativa a las transacciones del sistema. Estos manuales guían a la gente en la circulación y proceso de las transacciones. En las aplicaciones computarizadas, pueden ser incluidos en los sistemas mediante ayudas (*help*).

Revisión de procesos por personas, generalmente supervisores, para determinar su razonabilidad, exactitud, totalidad y autorización. En las aplicaciones computarizadas, gran parte de este monitoreo es ejecutado automáticamente mediante una lógica de programa predeterminada. Cada vez es más difícil para la gente monitorear los procesos, conforme los sistemas computacionales están más integrados y son más complejos y el ciclo del proceso se acorta; al mismo tiempo, el número de usuarios y responsables de la información es mayor.

La división de tareas entre los empleados. En las aplicaciones computarizadas, la distribución de deberes implica no sólo la división de tareas entre los empleados, sino también la división de tareas entre los pasos del proceso automatizado. Por ejemplo, los programas computarizados pueden procesar diferentes partes de una transacción en diversos lugares, y en ocasiones se requiere que tengan sistemas de seguridad de acceso a nivel sistema, dato o programa, como en el caso de los sistemas bancarios.

Proceso de grandes cantidades de datos que pueden requerir la repetición o cruzamiento de diversos elementos de la información. Esto es frecuentemente difícil y costoso en un sistema manual y sólo se realiza cuando es necesario. En

las aplicaciones computarizadas, grandes cantidades de datos pueden ser almacenadas en una base de datos. La velocidad y capacidades de proceso del computador hacen que esta información esté disponible en el formato deseado. En un ambiente computarizado, son posibles los más complejos análisis y los usos secundarios de los datos.

Planeación de los procedimientos de auditoría con informática

El propósito principal de la planeación de las medidas de auditoría es incluir dentro de las aplicaciones las facilidades que permitan realizar las actividades de auditoría de la manera más fluida.

La planeación de los servicios establece las facilidades tanto actuales como futuras que ofrece la dirección de informática. El auditor debe examinar este plan para establecer los requerimientos de auditoría necesarios.

Para el funcionamiento de dichos procedimientos se requieren dentro de los programas rutinas que permitan acceder la información y sistemas independientes para la selección, sumarización, comparación y emisión de reportes.

El poder planear y realizar estas tareas implica un trabajo complicado pero que es necesario hacer. La computarización de las organizaciones ha dado por resultado una concentración de datos y funciones, que son seleccionados, correlacionados, resumidos y diseminados. En un ambiente computarizado típico, normalmente un dato puede actualizar muchos archivos. Es necesario que el auditor cuente con las herramientas adecuadas para poder seguir el rastro del mismo y también verificar que el sistema esté realizando las funciones que supuestamente debe ejecutar; estas herramientas computarizadas le deben permitir detectar los errores y corregirlos posteriormente.

Es comprensible pensar que el auditor no es un programador especializado, por lo que es obligación de este grupo de proceso planear el desarrollo de estas herramientas de cómputo, atendiendo las solicitudes y recomendaciones de los auditores y aportando su propia experiencia.

También debe participar en las pruebas en paralelo y en la implantación del sistema, para asegurarse de que todos los procedimientos, entradas y salidas son los solicitados por el usuario en el momento del diseño detallado, así como para evaluar que los cálculos realizados sean los correctos y, en general, para dar la aprobación del sistema una vez verificado que cumpla con los objetivos, flujo de información, controles y políticas del usuario y de la organización.

La participación del auditor interno en el diseño e implementación de un sistema es de suma importancia. Por ejemplo, la clasificación de la evidencia que se venía utilizando tradicionalmente, como la firma del funcionario para autorizar una transacción, se ve reemplazada por una clave de seguridad de acceso o la firma electrónica, aunque la introducción de un computador no necesariamente cambia las formas de la evidencia de auditoría.

El auditor interno debe estar presente en el desarrollo del sistema para evaluar que la información requerida por el usuario quede cubierta y se cumpla

con el grado de acuerdo con lo

Existen cie
 las mínimas qu

- Habilidad
- Habilidad
- Habilidad
- Habilidad
- Habilidad

Como eval
 tre los proceso
 piadas para en
 área de trabajo
 mientos de los
 contexto de la
 y prácticas que
 tribución poter
 específico.

Las habilid
 implantar, ejec
 de la tecnología
 gobiernen el ob

DEFINICIÓN

CONCEPTO

Después de ana
 tipos de audito
 ponder las sigu
 campo de acció

Ésta es la d
 Practice sobre au

Es una funci
 vos de los sis
 los objetivos

Mientras qu

Auditoría en
 áreas de la or

con el grado de control que necesita la información procesada por el sistema, de acuerdo con los objetivos y políticas de la organización.

Existen ciertas habilidades fundamentales que deben ser consideradas como las mínimas que todo auditor de informática debe tener:

- Habilidad para manejar paquetes de procesadores de texto.
- Habilidades para manejo de hojas de cálculo.
- Habilidad para el uso del E-mail y conocimiento de Internet.
- Habilidad para manejo de bases de datos.
- Habilidad para el uso de al menos un paquete básico de contabilidad.

Como evaluador, el auditor de informática debe ser capaz de distinguir entre los procesos de evaluación de sistemas y las aproximaciones que son apropiadas para encauzar los propósitos específicos de evaluación relevante para el área de trabajo. En este sentido, el auditor en informática debe tener los conocimientos de los pasos requeridos para aplicar una evaluación particular en el contexto de la tecnología de la información. Debe poseer estándares relevantes y prácticas que gobiernen la conducción de una evaluación particular. Su contribución potencial a una evaluación particular puede ser hecha en un contexto específico.

Las habilidades técnicas requeridas por el auditor en informática son las de implantar, ejecutar y comunicar los resultados de la evaluación en el contexto de la tecnología de información, de acuerdo con estándares profesionales que gobiernen el objetivo de la auditoría.

DEFINICIÓN DE AUDITORÍA EN INFORMÁTICA

CONCEPTO DE AUDITORÍA EN INFORMÁTICA

Después de analizar los conceptos de auditoría y de informática, los diferentes tipos de auditoría, así como su interrelación con la informática, debemos responder las siguientes preguntas: ¿Qué es auditoría en informática? ¿Cuál es su campo de acción?

Ésta es la definición de Ron Weber en *Auditing Conceptual Foundations and Practice* sobre auditoría informática:

Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente.

Mientras que la definición de Mair William es la siguiente:

Auditoría en informática es la verificación de los controles en las siguientes tres áreas de la organización (informática):

- Aplicaciones (programa de producción).
- Desarrollo de sistemas.
- Instalación del centro de proceso.

Por tanto, podemos decir que auditoría en informática es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones.

La información contenida depende de la habilidad de reducir la incertidumbre alrededor de las decisiones. El valor de la reducción de la incertidumbre depende del pago asociado con la decisión que se realiza.

Los factores que pueden influir en una organización a través del control y la auditoría en informática son:

- Necesidad de controlar el uso evolucionado de las computadoras.
- Controlar el uso de la computadora, que cada día se vuelve más importante y costosa.
- Los altos costos que producen los errores en una organización.
- Abuso en las computadoras.
- Posibilidad de pérdida de capacidades de procesamiento de datos.
- Posibilidad de decisiones incorrectas.
- Valor del hardware, software y personal.
- Necesidad de mantener la privacidad individual.
- Posibilidad de pérdida de información o de mal uso de la misma.
- Toma de decisiones incorrectas.
- Necesidad de mantener la privacidad de la organización.

La información es un recurso necesario para la organización y para la continuidad de las operaciones, ya que provee de una imagen de su ambiente actual, su pasado y su futuro. Si la imagen de la organización es apropiada, ésta crecerá adaptándose a los cambios de su entorno.

En el proceso de la información se deben detectar sus errores u omisiones, y evitar su destrucción por causas naturales (temblores, inundaciones) o cualquier contingencia que pudiera suscitarse.

La toma de decisiones incorrectas, producto de datos erróneos proporcionados por los sistemas, trae como consecuencia efectos significativos, que afectan directamente a la organización.

El mayor estímulo para el desarrollo de la auditoría en informática dentro de la organización normalmente está dado por el abuso en el uso de las computadoras. El abuso en computadoras es cualquier incidente asociado con la tecnología en computación, en el cual la víctima sufra o pueda sufrir una pérdida y un daño hechos intencionalmente o para obtener una ganancia. El problema más serio está en los errores u omisiones que causan pérdidas a la organización. En seguida está el desastre de las computadoras debido a causas naturales, tales como fuego, agua o fallas en el suministro de energía. Las técnicas de control

Influencia de la auditoría

que manejan
aquellas que

El control
bido a lo in-
inadecuado
mas, debido
na, y sólo la
a la informa-

El abuso en
informática
nización es
de informát
ción del equ
información
robos horm
también son

La auditi
equipos de c
más habrá c
das, proced
(desarrollad
ben incluir l
ner una info
cómputo, de
y el persona

Además
son recursos
versiones en
seguro adecu
daños consi
inversión im
la organizaci
recobrado. S
dencial a la
pérdidas en
pre un recur
estrenado.

Las comp
nuestra socie
den ir desde
bertad o de la

Además
siderado la p
es responsab
redes de com
integrada y e
queridas. Exi
que la inform

que manejan estos dos tipos de problemas han sido mejor desarrolladas que aquellas que se relacionan con el abuso en las computadoras.

El control en el abuso de las computadoras es normalmente más difícil debido a lo inadecuado de las leyes. Es más difícil condenar a alguien que hizo un inadecuado uso del tiempo de las computadoras, o copias ilegales de programas, debido a que las leyes no consideran a las computadoras como una persona, y sólo las personas pueden ser declaradas como culpables, o bien considerar a la información como un bien tangible y un determinado costo.

El abuso tiene una importante influencia en el desarrollo de la auditoría en informática, ya que en la mayoría de las ocasiones el propio personal de la organización es el principal factor que puede provocar las pérdidas dentro del área de informática. Los abusos más frecuentes por parte del personal son la utilización del equipo en trabajos distintos a los de la organización, la obtención de información para fines personales (Internet), los juegos o pasatiempos, y los robos hormiga, además de los delitos informáticos que en muchas ocasiones también son llevados a cabo por el propio personal de la organización.

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 habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, comunicación, controles, archivos, seguridad, personal (desarrollador, operador, usuarios) y obtención de información. En esto se deben incluir los equipos de cómputo, por ser la herramienta que permite obtener una información adecuada y una organización específica (departamento de cómputo, departamento de informática, gerencia de procesos electrónicos, etc.), y el personal que hará posible el uso de los equipos de cómputo.

Además de los datos, el hardware de computadora, el software y personal son recursos críticos de las organizaciones. Algunas organizaciones tienen inversiones en equipo de hardware con un valor multimillonario. Aun con un seguro adecuado, las pérdidas intencionales o no intencionales pueden causar daños considerables. En forma similar, el software muchas veces constituye una inversión importante. Si el software es corrompido o destruido, es posible que la organización no pueda continuar con sus operaciones, si no es prontamente recuperado. Si el software es robado, se puede proporcionar información confidencial a la competencia, y si el software es de su propiedad, pueden tenerse pérdidas en ganancias o bien en juicios legales. Finalmente, el personal es siempre un recurso valioso, sobre todo ante la falta de personal de informática bien entrenado.

Las computadoras ejecutan automáticamente muchas funciones críticas en nuestra sociedad. Consecuentemente, las pérdidas pueden ser muy altas y pueden ir desde pérdidas multimillonarias en lo económico, hasta pérdidas de libertad o de la vida en el caso de errores en laboratorios médicos o en hospitales.

Además de los aspectos constitucionales y legales, muchos países han considerado la privacidad como parte de los derechos humanos. Consideran que es responsabilidad de las personas que están con las computadoras y con las redes de comunicación, asegurar que el uso de la información sea recolectada, integrada y entregada rápidamente y con la privacidad y confidencialidad requeridas. Existe una responsabilidad adicional en el sentido de asegurarse de que la información sea usada solamente para los propósitos que fue elaborada.

DEFINICIÓN DE AUDITORÍA EN INFORMÁTICA

Pérdida de información

Campo
de la auditoría

En este caso se encuentran las bases de datos, las cuales pueden ser usadas para fines ajenos para los que fueron diseñadas o bien entrar en la privacidad de las personas.

La tecnología es neutral, no es buena ni mala. El uso de la tecnología es lo que puede producir problemas sociales. Por ejemplo, el mal uso de la tecnología en Internet no es problema de la tecnología, sino de la forma y características sobre las cuales se usa esa tecnología. Es una función del gobierno, de las asociaciones profesionales y de los grupos de presión evaluar el uso de la tecnología; pero es bien aceptado el que las organizaciones en lo individual tengan una conciencia social, que incluya el uso de la tecnología en informática.

Deberá de existir una legislación más estricta en el uso de la tecnología, en la que se considere el análisis y la investigación para evitar el mal uso de Internet y otras tecnologías, para evitar situaciones como el suicidio colectivo de sectas religiosas, como sucedió en Estados Unidos. También se requiere de una ética por parte de las organizaciones y de los individuos que tienen en sus manos todo tipo de tecnología, no sólo la de informática.

CAMPO DE LA AUDITORÍA EN INFORMÁTICA

El campo de acción de la auditoría en informática es:

- La evaluación administrativa del área de informática.
- La evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información. La evaluación de la eficiencia y eficacia con la que se trabaja.
- La evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, bases de datos, comunicaciones).
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Para lograr los puntos antes señalados se necesita:

- A) Evaluación administrativa del departamento de informática. Esto comprende la evaluación de:
- Los objetivos del departamento, dirección o gerencia.
 - Metas, planes, políticas y procedimientos de procesos electrónicos estándares.
 - Organización del área y su estructura orgánica.
 - Funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos.
 - Integración de los recursos materiales y técnicos.
 - Dirección.
 - Costos y controles presupuestales.
 - Controles administrativos del área de procesos electrónicos.

B) Evaluación de la eficiencia que se tiene

- Ev
- Ev
- Ev
- Fa
- Co
- Co
- Ins
- For
- Seg
- Co
- Co
- Ut
- Pre
- cup
- Pro
- Der

C) Evaluación de la eficiencia que se tiene

- Con
- Con
- Con
- Con
- Con
- Con
- Con
- Con
- Orde

D) Seguridad

- Segu
- Conf
- Resp
- Segu
- Segu
- Segu
- Plan
- sastre
- Resta

Los princ

- Salvaj
- ware
- Integr

B) Evaluación de los sistemas y procedimientos, y de la eficiencia y eficacia que se tienen en el uso de la información, lo cual comprende:

- Evaluación del análisis de los sistemas y sus diferentes etapas.
- Evaluación del diseño lógico del sistema.
- Evaluación del desarrollo físico del sistema.
- Facilidades para la elaboración de los sistemas.
- Control de proyectos.
- Control de sistemas y programación.
- Instructivos y documentación.
- Formas de implantación.
- Seguridad física y lógica de los sistemas.
- Confidencialidad de los sistemas.
- Controles de mantenimiento y forma de respaldo de los sistemas.
- Utilización de los sistemas.
- Prevención de factores que puedan causar contingencias; seguros y recuperación en caso de desastre.
- Productividad.
- Derechos de autor y secretos industriales.

C) Evaluación del proceso de datos y de los equipos de cómputo que comprende:

- Controles de los datos fuente y manejo de cifras de control.
- Control de operación.
- Control de salida.
- Control de asignación de trabajo.
- Control de medios de almacenamiento masivos.
- Control de otros elementos de cómputo.
- Control de medios de comunicación
- Orden en el centro de cómputo.

D) Seguridad:

- Seguridad física y lógica.
- Confidencialidad.
- Respaldos.
- Seguridad del personal.
- Seguros.
- Seguridad en la utilización de los equipos.
- Plan de contingencia y procedimiento de respaldo para casos de desastre.
- Restauración de equipo y de sistemas.

Los principales objetivos de la auditoría en informática son los siguientes:

- Salvaguardar los activos. Se refiere a la protección del hardware, software y recursos humanos.
- Integridad de datos. Los datos deben mantener consistencia y no duplicarse.

- Efectividad de sistemas. Los sistemas deben cumplir con los objetivos de la organización.
- Eficiencia de sistemas. Que se cumplan los objetivos con los menores recursos.
- Seguridad y confidencialidad.

Para que sea eficiente la auditoría en informática, ésta se debe realizar también durante el proceso de diseño del sistema. Los diseñadores de sistemas tienen la difícil tarea de asegurarse que interpretan las necesidades de los usuarios, que diseñan los controles requeridos por los auditores y que aceptan y entienden los diseños propuestos.

La interrelación que debe existir entre la auditoría en informática y los diferentes tipos de auditoría es la siguiente: el núcleo o centro de la informática son los programas, los cuales pueden ser auditados por medio de la auditoría de programas. Estos programas se usan en las computadoras de acuerdo con la organización del centro de cómputo (personal).

La auditoría en informática debe evaluar todo (informática, organización del centro de cómputo, computadoras, comunicación y programas), con auxilio de los principios de auditoría administrativa, auditoría interna, auditoría contable/financiera y, a su vez, puede proporcionar información a esos tipos de auditoría. Las computadoras deben ser una herramienta para la realización de cualquiera de las auditorías.

La adecuada salvaguarda de los activos, la integridad de los datos y la eficiencia de los sistemas solamente se pueden lograr si la administración de la organización desarrolla un adecuado sistema de control interno.

El tipo y características del control interno dependerán de una serie de factores, por ejemplo, si se trata de un medio ambiente de minicomputadoras o macrocomputadoras, si están conectadas en serie o trabajan en forma individual, si se tiene Internet y Extranet. Sin embargo, la división de responsabilidades y la delegación de autoridad es cada vez más difícil debido a que muchos usuarios comparten recursos, lo que dificulta el proceso de control interno.

Como se ve, la evaluación que se debe desarrollar para la realización de la auditoría en informática debe ser hecha por personas con un alto grado de conocimiento en informática y con mucha experiencia en el área.

La información proporcionada debe ser confiable, oportuna, verídica, y debe manejarse en forma segura y con la suficiente confidencialidad, pero debe estar contenida dentro de parámetros legales y éticos.

AUDITORÍA DE PROGRAMAS

La auditoría de programas es la evaluación de la eficiencia técnica, del uso de diversos recursos (cantidad de memoria) y del tiempo que utilizan los programas, su seguridad y confiabilidad, con el objetivo de optimizarlos y evaluar el riesgo que tienen para la organización.

La auditoría de programas tiene un mayor grado de profundidad y de detalle que la auditoría en informática, ya que analiza y evalúa la parte central del

uso de las con-
parte de la au-

Para log-
realicen han c-
temas de adm-
bases de dato-
el programa.
ción del mism-
mas se necesi-
tengan los res-
general se ca-
optimizar un)

Para optin-
ción del sisten-
mentación del

uso de las computadoras, que es el programa, aunque se puede considerar como parte de la auditoría en informática.

Para lograr que la auditoría de programas sea eficiente, las personas que la realicen han de poseer conocimientos profundos sobre sistemas operativos, sistemas de administración de base de datos, lenguajes de programación, utilerías, bases de datos, medios de comunicación y acerca del equipo en que fue escrito el programa. Asimismo, se deberá comenzar con la revisión de la documentación del mismo. Para poder llevar a cabo una auditoría adecuada de los programas se necesita que los sistemas estén trabajando correctamente, y que se obtengan los resultados requeridos, ya que al cambiar el proceso del sistema en general se cambiarán posiblemente los programas. Sería absurdo intentar optimizar un programa de un sistema que no está funcionando correctamente.

Para optimizar los programas se deberá tener pleno conocimiento y aceptación del sistema o sistemas que usan ese programa, y disponer de toda la documentación detallada del sistema total.

OBJETIVOS

Al finalizar este capítulo, usted:

1. Comprenderá los distintos tipos que comprende la auditoría en informática.
2. Comprenderá la importancia en el trabajo de auditoría de la planeación, examen y la evaluación de la información, la comunicación de los resultados y el seguimiento.
3. Explicará el valor de la evaluación de los sistemas de acuerdo al tiempo.
4. Describirá las fases que deben seguirse para realizar una adecuada investigación preliminar.
5. Definirá cuáles son las principales características que requiere el personal que habrá de participar en una auditoría.
6. Conocerá cómo se elige una lista correcta de servicios profesionales de auditoría.

2

CAPÍTULO

Planeación de la auditoría en informática

OBJETIVOS

Al finalizar este capítulo, usted:

1. Conocerá las distintas fases que comprende la auditoría en informática.
2. Comprenderá la importancia en el trabajo de auditoría de la planeación, el examen y la evaluación de la información, la comunicación de los resultados y el seguimiento.
3. Explicará el valor de la evaluación de los sistemas de acuerdo al riesgo.
4. Describirá las fases que deben seguirse para realizar una adecuada investigación preliminar.
5. Definirá cuáles son las principales características que requiere el personal que habrá de participar en una auditoría.
6. Conocerá cómo se elabora una carta-convenio de servicios profesionales de auditoría.

Auditoría interna

FASES DE LA AUDITORÍA

La auditoría en informática es el proceso de recolección y evaluación de evidencias para determinar cuándo son salvaguardados los activos de los sistemas computarizados, de qué manera se mantiene la integridad de los datos y cómo se logran los objetivos de la organización eficazmente y se usan los recursos consumidos eficientemente. La auditoría en informática sigue los objetivos tradicionales de la auditoría: aquellos que son de la auditoría externa, de salvaguarda de los activos y la integridad de datos, y los objetivos gerenciales, aquellos propios de la auditoría interna que no sólo logran los objetivos señalados sino también los de eficiencia y eficacia.

La auditoría interna es una función independiente de la evaluación que se establece dentro de una organización para examinar y evaluar sus actividades. El objetivo de la auditoría interna consiste en apoyar a los miembros de la organización en el desempeño de sus responsabilidades. Para ello, proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

Los auditores internos son responsables de proporcionar información acerca de la adecuación y efectividad del sistema de control interno de la organización y de la calidad de la gestión.

El manual de organización deberá establecer claramente los propósitos del departamento de auditoría interna, especificar que el alcance del trabajo no debe tener restricciones y señalar que los auditores internos no tendrán autoridad y/o responsabilidad respecto de las actividades que auditan.

El auditor interno debe ser independiente de las actividades que audita. Esta independencia permite que el auditor interno realice su trabajo libre y objetivamente, ya que sin esta independencia no se pueden obtener los resultados deseados.

Las normas de auditoría interna comprenden:

- Las actividades auditadas y la objetividad de los auditores internos.
- El conocimiento técnico, la capacidad y el cuidado profesional de los auditores internos con los que deben ejercer su función. En el caso de la auditoría en informática es de suma importancia el que el auditor cuente con los conocimientos técnicos actualizados y con la experiencia necesaria en el área.
- El alcance del trabajo de auditoría interna en el área de informática.
- El desarrollo de las responsabilidades asignadas a los auditores internos responsables de la auditoría a informática.

Los auditores internos deben ser independientes de las actividades que auditan, y deben de tener un amplio criterio para no tomar decisiones subjetivas basadas en preferencias personales sobre determinado equipo o software, sin analizar a profundidad las opiniones. Los auditores internos son independientes cuando pueden desempeñar su trabajo con libertad y objetividad. La independencia permite a los auditores internos rendir juicios imparciales, esen-

ciales para una adecuada

La objetividad de los auditores internos debe sub

La objetividad de tal manera que no haya auditores interesados en las posibilidades

Los resultados de la auditoría interna y el respectivo informe de que el tra

El auditor interno debe ser independiente de las actividades que audita

El departamento de auditoría interna debe ser una disciplina profesional que asegure que los auditores sean

Asimismo, los auditores internos deben de tener un amplio criterio para no tomar decisiones subjetivas basadas en preferencias personales sobre determinado equipo o software, sin analizar a profundidad las opiniones. Los auditores internos son independientes cuando pueden desempeñar su trabajo con libertad y objetividad. La independencia permite a los auditores internos rendir juicios imparciales, esen-

El departamento de auditoría interna debe ser una disciplina profesional que asegure que los auditores sean

El departamento de auditoría interna debe ser una disciplina profesional que asegure que los auditores sean

- Que las actividades auditadas y la objetividad de los auditores internos.
- Que los auditores internos cuenten con los conocimientos técnicos actualizados y con la experiencia necesaria en el área.
- Que los auditores internos sean independientes de las actividades que auditan.
- Que los auditores internos sean independientes de las actividades que auditan.
- Que los auditores internos sean independientes de las actividades que auditan.
- Que los auditores internos sean independientes de las actividades que auditan.
- Que los auditores internos sean independientes de las actividades que auditan.
- Que los auditores internos sean independientes de las actividades que auditan.

Cada auditor interno debe ser independiente de las actividades que auditan, y deben de tener un amplio criterio para no tomar decisiones subjetivas basadas en preferencias personales sobre determinado equipo o software, sin analizar a profundidad las opiniones. Los auditores internos son independientes cuando pueden desempeñar su trabajo con libertad y objetividad. La independencia permite a los auditores internos rendir juicios imparciales, esen-

- Se requiere que los auditores internos sean independientes de las actividades que auditan.

ciales para la adecuada conducción de las auditorías; esto se logra a través de una adecuada objetividad y criterio.

La objetividad es una actitud de independencia mental que los auditores internos deben mantener al realizar las auditorías. Los auditores internos no deben subordinar sus juicios en materia de auditoría al de otros.

La objetividad requiere que los auditores internos realicen sus auditorías de tal manera que tengan una honesta confianza en el producto de su trabajo y que no hayan creado compromisos significativos en cuanto a la calidad. Los auditores internos no deben colocarse en situaciones en las que se sientan imposibilitados para hacer juicios profesionales objetivos.

Los resultados del trabajo de auditoría deben ser revisados antes de emitir el respectivo informe de auditoría, para proporcionar una razonable seguridad de que el trabajo se realizó objetivamente.

El auditor en informática debe contar con los conocimientos técnicos requeridos y con capacidad profesional.

El departamento de auditoría interna deberá asignar a cada auditoría a aquellas personas que en su conjunto posean los conocimientos, la experiencia y la disciplina necesarios para conducir apropiadamente la auditoría. También deberá asegurarse que la experiencia técnica y la formación académica de los auditores sean las apropiadas para realizar las auditorías en informática.

Asimismo, se deberá obtener una razonable seguridad sobre las capacidades y pericias de cada prospecto para auditor en informática.

El departamento de auditoría interna deberá contar u obtener los conocimientos, experiencias y disciplinas necesarias para llevar a cabo sus responsabilidades de auditoría en informática. Deberá tener personal o emplear consultores calificados en las disciplinas de informática necesarias para cumplir con las responsabilidades de auditoría; sin embargo, cada miembro del departamento no necesita estar calificado en todas las disciplinas.

El departamento de auditoría interna deberá asegurarse:

- Que las auditorías sean supervisadas en forma apropiada. La supervisión es un proceso continuo que comienza con la planeación y termina con el trabajo de auditoría.
- Que los informes de auditoría sean precisos, objetivos, claros, concisos, constructivos y oportunos.
- Que se cumplan los objetivos de la auditoría.
- Que la auditoría sea debidamente documentada y que se conserve la evidencia apropiada de la supervisión.
- Que los auditores cumplan con las normas profesionales de conducta.
- Que los auditores en informática posean los conocimientos, experiencias y disciplinas esenciales para realizar sus auditorías.

Cada auditor interno requiere de ciertos conocimientos y experiencias:

- Se requiere pericia en la aplicación de las normas, procedimientos y técnicas de auditoría interna para el desarrollo de las revisiones. Se entiende por pericia la habilidad para aplicar los conocimientos que se poseen a las si-

**Habilidades
de los auditores**

tuaciones que posiblemente se encuentren, ocupándose de ellas sin tener que recurrir en exceso a ayudas o investigaciones técnicas.

- Tener habilidad para: aplicar amplios conocimientos a situaciones que posiblemente se vayan encontrando, reconocer las desviaciones significativas y poder llevar a cabo las investigaciones necesarias para alcanzar soluciones razonables.

Entre las habilidades que deben tener los auditores están:

- Habilidad para comunicarse efectivamente y dar un trato adecuado a las personas. Los auditores internos deben tener habilidad para comunicarse tanto de manera oral como escrita, de tal manera que puedan transmitir clara y efectivamente asuntos como: los objetivos de la auditoría, las evaluaciones, las conclusiones y las recomendaciones.
- Los auditores en informática son responsables de continuar su desarrollo profesional para poder mantener su pericia profesional. Deberán mantenerse informados acerca de las mejoras y desarrollos recientes.
- Los auditores en informática deben ejercer el debido cuidado profesional al realizar sus auditorías. El cuidado profesional, deberá estar de acuerdo con la complejidad de la auditoría que se realiza. Los auditores deben estar atentos a la posibilidad de errores intencionales, de errores omisiones, de la ineficiencia, del desperdicio, de la ineffectividad y del conflicto de intereses. También deberán estar alertas ante aquellas condiciones y actividades en donde es más probable que existan irregularidades. Además, deberán de identificar los controles inadecuados y emitir recomendaciones para promover el cumplimiento con procedimientos y prácticas aceptables.

El debido cuidado implica una razonable capacidad, no infalibilidad ni acciones extraordinarias. Requiere que el auditor realice exámenes y verificaciones con un alcance razonable, pero no requiere auditorías detalladas de todas las operaciones. Por consiguiente, el auditor no puede dar una absoluta seguridad de que no existan incumplimientos o irregularidades. Sin embargo, la posibilidad de que existan irregularidades materiales o que no se cumplan las disposiciones debe ser considerada siempre que el auditor emprende una auditoría. Cuando el auditor detecte una irregularidad que va en contra de lo establecido deberá informarlo a las autoridades adecuadas de la organización. El auditor puede recomendar cualquier investigación que considere necesaria en esas circunstancias. Posteriormente, el auditor deberá efectuar su seguimiento para verificar que se ha cumplido con lo señalado.

El ejercicio del debido cuidado profesional significa el uso razonable de las experiencias y juicios en el desarrollo de la auditoría.

Para este fin el auditor deberá considerar:

- El alcance del trabajo de auditoría necesario para lograr los objetivos de la auditoría.
- La materialidad o importancia relativa de los asuntos a los que se aplican los procedimientos de la auditoría.

Cuidado profesional

- La adecuación
- El costo

El cuidado profesional determina los procedimientos. Cuando se realiza una auditoría, el alcance de la auditoría y el efecto de la auditoría en el control interno de la organización, se revisa la auditoría del sistema establecida y metas de la auditoría.

Los objetivos de la auditoría son:

- La confianza en la información financiera para la toma de decisiones.
- El cumplimiento de los objetivos.
- La salvaguarda de los recursos.
- El uso eficiente de los recursos.
- El logro de los objetivos.

El sistema de control y el control interno deben examinarse.

- Que los recursos sean utilizados, como se debe.
- Que los recursos sean utilizados, como se debe.

Los auditores deben cumplir con los objetivos de la auditoría que pueden tener. Los auditores deben determinar los objetivos de la auditoría.

La gerencia debe diseñar políticas, planes y procedimientos. Los auditores son responsables de si las actividades se cumplen o no.

Los auditores deben:

- La corrección de la existencia de los recursos.

- La adecuación y efectividad de los controles internos.
- El costo de la auditoría en relación con los posibles beneficios.

El cuidado profesional incluye la evaluación de los estándares establecidos, determinando en consecuencia si tales estándares son aceptables y si son cumplidos. Cuando éstos son vagos deberán solicitarse interpretaciones autorizadas.

El alcance de la auditoría debe abarcar el examen y evaluación de la adecuación y efectividad del sistema de control interno de la organización y la calidad en el cumplimiento de las responsabilidades asignadas. El propósito de revisar la adecuación del sistema de control interno es el de cerciorarse si el sistema establecido proporciona una razonable seguridad de que los objetivos y metas de la organización se cumplirán eficiente y económicamente.

Los objetivos elementales del control interno son para asegurar:

- La confiabilidad e integridad de la información. Los auditores deben revisar la confiabilidad e integridad de la información y los métodos empleados para identificar, medir, clasificar y reportar dicha información
- El cumplimiento de las políticas, planes, procedimientos, leyes y reglamentos.
- La salvaguarda de los activos.
- El uso eficiente y económico de los recursos.
- El logro de los objetivos y metas establecidos para las operaciones o programas.

El sistema de información proporciona datos para la toma de decisiones, el control y el cumplimiento con requerimientos externos. Por ello, los auditores deben examinar los sistemas de información y cuando sea apropiado asegurarse:

- Que los registros e informes contengan información precisa, confiable, oportuna, completa y útil.
- Que los controles sobre los registros e informes sean adecuados y efectivos.

Los auditores deben revisar los sistemas establecidos para asegurarse del cumplimiento de las políticas, planes y procedimientos, leyes y reglamentos que pueden tener un impacto significativo en las operaciones e informes, y deben determinar si la organización cumple con ellos.

La gerencia de informática es responsable del establecimiento de los sistemas diseñados para asegurar el cumplimiento de requerimientos tales como políticas, planes, procedimientos y leyes y reglamentos aplicables. Los auditores son responsables de determinar si los sistemas son adecuados y efectivos y si las actividades auditadas están cumpliendo con los requerimientos apropiados.

Los auditores deberán revisar:

- La corrección de los métodos de salvaguarda de los activos y verificar la existencia de estos activos.

**Uso eficiente
 de recursos**

- Los métodos empleados para salvaguardar los activos de diferentes tipos de riesgos tales como: robo, incendios, actividades impropias o ilegales, así como de elementos naturales como terremotos, inundaciones, etcétera.

Los auditores deberán evaluar si el empleo de los recursos se realiza en forma económica y eficiente.

La administración es responsable de establecer estándares de operación para medir la eficiencia y economía en el uso de los recursos. Los auditores internos son responsables de determinar si:

- Los estándares para medir la economía y eficiencia en el uso de los recursos son los adecuados.
- Los estándares de operación establecidos han sido entendidos y se cumplen.
- Las desviaciones a los estándares de operación se identifican, analizan y se comunican a los responsables para que tomen las medidas correctivas.
- Se toman las medidas correctivas.

Las auditorías relacionadas con el uso económico y eficiente de los recursos deberán identificar situaciones tales como:

- Subutilización de instalaciones.
- Trabajo no productivo.
- Procedimientos que no justifican su costo.
- Exceso o insuficiencia de personal.
- Uso indebido de las instalaciones.

Los auditores deberán revisar las operaciones o programas para cerciorarse si los resultados son consistentes con los objetivos y metas establecidos y si las operaciones o programas se llevan a cabo como se planearon.

PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA

Para hacer una adecuada planeación de la auditoría en informática hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo. Con ello podremos determinar el número y características del personal de auditoría, las herramientas necesarias, el tiempo y costo, así como definir los alcances de la auditoría para, en caso necesario, poder elaborar el contrato de servicios.

Dentro de la auditoría en general, la planeación es uno de los pasos más importantes, ya que una inadecuada planeación provocará una serie de proble-

mas que p
 efectúe co

El trab
 men y la e
 seguimien
 La plan

- El estal
- La obte
- La dete
- El estal
- involuc
- La reali
- familiar
- ción de
- promov
- La prep
- La deter
- dos de l
- La obten

En el ca
 pues habrá c

- Evaluaci
- Evaluaci
- Evaluaci
- Evaluaci
- to (softw
- Segurida
- Aspectos

Para logr
 información g
 evaluar. Para
 entrevistas prev
 deberá inclui
 solicitar o for

El proces

- Metas.
- Program
- Planes de
- Informes

Las metas
 plimiento, sob

mas que pueden impedir que se cumpla con la auditoría o bien hacer que no se efectúe con el profesionalismo que debe tener cualquier auditor.

El trabajo de auditoría deberá incluir la planeación de la auditoría, el examen y la evaluación de la información, la comunicación de los resultados y el seguimiento.

La planeación deberá ser documentada e incluirá:

- El establecimiento de los objetivos y el alcance del trabajo.
- La obtención de información de apoyo sobre las actividades que se auditarán.
- La determinación de los recursos necesarios para realizar la auditoría.
- El establecimiento de la comunicación necesaria con todos los que estarán involucrados en la auditoría.
- La realización, en la forma más apropiada, de una inspección física para familiarizarse con las actividades y controles a auditar, así como identificación de las áreas en las que se deberá hacer énfasis al realizar la auditoría y promover comentarios y la promoción de los auditados.
- La preparación por escrito del programa de auditoría.
- La determinación de cómo, cuándo y a quién se le comunicarán los resultados de la auditoría.
- La obtención de la aprobación del plan de trabajo de la auditoría.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de varios objetivos:

- Evaluación administrativa del área de procesos electrónicos.
- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.
- Evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, bases de datos, comunicaciones).
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Para lograr una adecuada planeación, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, y con base en esto planear el programa de trabajo, el cual deberá incluir tiempos, costos, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la auditoría.

El proceso de planeación comprende el establecer:

- Metas.
- Programas de trabajo de auditoría.
- Planes de contratación de personal y presupuesto financiero.
- Informes de actividades.

Las metas se deberán establecer de tal manera que se pueda lograr su cumplimiento, sobre la base de los planes específicos de operación y de los presu-

Objetivos de la planeación

puestos, los que hasta donde sea posible deberán ser cuantificables. Deberán acompañarse de los criterios para medirlas y de fechas límite para su logro.

Los programas de trabajo de auditoría deberán incluir: las actividades que se van a auditar, cuándo serán auditadas, el tiempo estimado requerido, tomando en consideración el alcance del trabajo de auditoría planeado y la naturaleza y extensión del trabajo de auditoría realizado por otros. Los programas de trabajo deberán ser lo suficientemente flexibles para cubrir demandas imprevistas.

Los planes de contratación de empleados y los presupuestos financieros —incluyendo el número de auditores, su conocimiento, su experiencia y las disciplinas requeridas para realizar su trabajo—, deberán contemplarse al elaborar los programas de trabajo de auditoría, así como las actividades administrativas, la escolaridad y el adiestramiento requeridos, la investigación sobre auditoría y los esfuerzos de desarrollo.

REVISIÓN PRELIMINAR

El primer paso en el desarrollo de la auditoría, después de la planeación, es la revisión preliminar del área de informática. El objetivo de la revisión preliminar es el de obtener la información necesaria para que el auditor pueda tomar la decisión de cómo proceder en la auditoría. Al terminar la revisión preliminar el auditor puede proceder en uno de los tres caminos siguientes.

- Diseño de la auditoría. Puede haber problemas debido a la falta de competencia técnica para realizar la auditoría.
- Realizar una revisión detallada de los controles internos de los sistemas con la esperanza de que se deposite la confianza en los controles de los sistemas y de que una serie de pruebas sustantivas puedan reducir las consecuencias.
- Decidir el no confiar en los controles internos del sistema. Existen dos razones posibles para esta decisión. Primero, puede ser más eficiente desde el punto de vista de costo-beneficio el realizar pruebas sustantivas directamente. Segundo, los controles del área de informática pueden duplicar los controles existentes en el área del usuario. El auditor puede decidir que se obtendrá un mayor costo-beneficio al dar una mayor confianza a los controles de compensación y revisar y probar mejor estos controles.

La revisión preliminar significa la recolección de evidencias por medio de entrevistas con el personal de la instalación, la observación de las actividades en la instalación y la revisión de la documentación preliminar. Las evidencias se pueden recolectar por medio de cuestionarios iniciales, o bien por medio de entrevistas, o con documentación narrativa. Debemos considerar que ésta será sólo una información inicial que nos permitirá elaborar el plan de trabajo, la cual se profundizará en el desarrollo de la auditoría.

La revisión preliminar es una actividad normal en la parte gerencial de la auditoría; el auditor debe familiarizarse con las causas de la revisión; el auditor debe considerar si el auditor puede garantizar de proceder con la fase de los controles internos.

REVISIÓN

Los objetivos de la revisión preliminar para que el auditor pueda tomar la decisión dentro del área de informática.

El auditor debe tener un conocimiento, con el fin de control interno de las compensaciones, puede, después de la revisión preliminar, los controles internos se tienden a ser alternos de la revisión preliminar.

En la fase de la revisión preliminar, las causas de la revisión para reducir la revisión detallada de los controles internos pueden reducir la atención de la revisión preliminar, usados en la revisión preliminar con que se obtiene la información preliminar.

Como en la revisión preliminar de lograr los objetivos de la auditoría interna, la eficiencia y eficacia de la revisión preliminar suficientes para la revisión preliminar interno debe ser sobrecontrol, los controles internos de la revisión preliminar controles internos de la revisión preliminar procedimientos de los sistemas.

La revisión preliminar elaborada por un auditor interno difiere de la realizada por un auditor externo en tres aspectos. En primer lugar, el auditor interno normalmente requiere de menos revisiones y trabajos, especialmente en la parte gerencial y de organización, ya que él es parte de la organización y está familiarizado con la misma. En segundo, el auditor externo se enfoca más en las causas de las pérdidas y en los controles necesarios para justificar sus decisiones; el auditor interno tiene una amplia perspectiva, la cual incorpora en sus consideraciones sobre la eficiencia y la eficacia con la que se trabaja. En tercero, si el auditor interno supone serias debilidades en los controles internos, en lugar de proceder directamente con las pruebas sustantivas, deberá continuar con la fase de revisión detallada para señalar recomendaciones para mejorar los controles internos.

REVISIÓN DETALLADA

Los objetivos de la fase detallada son los de obtener la información necesaria para que el auditor tenga un profundo entendimiento de los controles usados dentro del área de informática.

El auditor debe decidir si debe de continuar elaborando pruebas de consentimiento, con la esperanza de obtener mayor confianza por medio del sistema de control interno, o proceder directamente a la revisión con los usuarios (pruebas compensatorias), o a las pruebas sustantivas. En algunos casos el auditor puede, después de hacer un análisis detallado, decidir que con los controles internos se tiene suficiente confianza, y en otros casos que los procedimientos alternos de auditoría pueden ser más apropiados.

En la fase de evaluación detallada es importante para el auditor identificar las causas de las pérdidas existentes dentro de la instalación y los controles para reducir las pérdidas y los efectos causados por éstas. Al terminar la revisión detallada el auditor debe evaluar en qué momento los controles establecidos reducen las pérdidas esperadas a un nivel aceptable. Los métodos de obtención de información al momento de la evaluación detallada son los mismos usados en la investigación preliminar, y lo único que difiere es la profundidad con que se obtiene la información y se evalúa.

Como en el caso de la investigación preliminar, se tienen diferentes formas de lograr los objetivos desde el punto de vista del auditor interno o externo. El auditor interno debe considerar las causas de las pérdidas que afectan la eficiencia y eficacia, además de evaluar por qué los controles escogidos son o no suficientes para reducir las pérdidas esperadas a un nivel aceptable. El auditor interno debe evaluar si los controles escogidos son óptimos, si provocan un sobrecontrol, o bien si se logra un satisfactorio nivel de control usando menos controles o controles menos costosos. Si el auditor interno considera que los controles internos del sistema no son satisfactorios, en lugar de proceder directamente a revisar, a probar controles alternos o a realizar pruebas sustantivas y procedimientos, debe señalar las recomendaciones para mejorar los controles de los sistemas.

EXAMEN Y EVALUACIÓN DE LA INFORMACIÓN

Los auditores internos deberán obtener, analizar, interpretar y documentar la información para apoyar los resultados de la auditoría.

El proceso de examen y evaluación de la información es el siguiente:

- Se debe obtener la información de todos los asuntos relacionados con los objetivos y alcances de la auditoría.
- La información deberá ser suficiente, competente, relevante y útil para que proporcione bases sólidas en relación con los hallazgos y recomendaciones de la auditoría. La información suficiente significa que está basada en hechos, que es adecuada y convincente, de tal forma que una persona prudente e informada pueda llegar a las mismas conclusiones que el auditor. La información competente significa que es confiable y puede obtenerse de la mejor manera, usando las técnicas de auditoría apropiadas. La información relevante apoya los hallazgos y recomendaciones de auditoría y es consistente con los objetivos de ésta. La información útil ayuda a la organización a lograr sus metas.
- Los procedimientos de auditoría, incluyendo el empleo de las técnicas de pruebas selectivas y el muestreo estadístico, deberán ser elegidos con anterioridad, cuando esto sea posible, y ampliarse o modificarse cuando las circunstancias lo requieran.
- El proceso de recabar, analizar, interpretar y documentar la información deberá supervisarse para proporcionar una seguridad razonable de que la objetividad del auditor se mantuvo y que las metas de auditoría se cumplieron.
- Los documentos de trabajo de la auditoría deberán ser preparados por los auditores y revisados por la gerencia de auditoría. Estos documentos deberán registrar la información obtenida y el análisis realizado, y deben apoyar las bases de los hallazgos de auditoría y las recomendaciones que se harán.

Los auditores deberán reportar los resultados del trabajo de auditoría. El auditor deberá discutir las conclusiones y recomendaciones en los niveles apropiados de la administración antes de emitir su informe final. Los informes deberán ser objetivos, claros, concisos, constructivos y oportunos. Los informes presentarán el propósito, alcance y resultados de la auditoría y, cuando se considere apropiado, contendrán la opinión del auditor.

Los informes pueden incluir recomendaciones para mejoras potenciales y reconocer el trabajo satisfactorio y las medidas correctivas. Los puntos de vista de los auditados respecto a las conclusiones y recomendaciones pueden ser incluidos en el informe de auditoría.

Los auditores internos realizarán el seguimiento de las recomendaciones, para asegurarse que se tomaron las acciones apropiadas sobre los hallazgos de auditoría reportados.

El director
selecciona

- Descripción
- Selección
- Entrenamiento
- Todos los
- Evaluación
- Año.
- Asesoramiento
- Sional.

El trabajo
la adecuación

El director
ner un pro
tamento de
una seguridad
normas ap
Un pro

- Supervisión
- Revisión
- Revisión

La supervisión
cabo contin
las normas,

Las revisiones
del departa
auditoría re
ra que cual

Para ev
practicarse

P

El objetivo
controles in
determinar
jan confiabl

Además
cuentamente
asistidas por

El director de auditoría en informática deberá establecer un programa para seleccionar y desarrollar los recursos, el cual debe contemplar:

- Descripciones de puestos por cada nivel de auditoría en informática.
- Selección de individuos calificados y competentes.
- Entrenamiento y oportunidad de capacitación profesional continua para todos y cada uno de los auditores.
- Evaluación del trabajo de cada uno de los auditores por lo menos una vez al año.
- Asesoría a los auditores en lo referente a su trabajo y a su desarrollo profesional.

El trabajo de auditoría interna y externa deberá coordinarse para asegurar la adecuada cobertura y para minimizar la duplicidad de esfuerzos.

El director de auditoría interna en informática deberá establecer y mantener un programa de control de calidad para evaluar las operaciones del departamento de auditoría interna. El propósito de este programa es proporcionar una seguridad razonable de que el trabajo de auditoría está de acuerdo con las normas aplicables.

Un programa de control de calidad deberá incluir los siguientes elementos:

- Supervisión.
- Revisiones internas.
- Revisiones externas.

La supervisión del trabajo de los auditores en informática deberá llevarse a cabo continuamente para asegurarse de que están trabajando de acuerdo con las normas, políticas y programas de auditoría en informática.

Las revisiones internas deberán realizarse periódicamente por el personal del departamento de auditoría interna para evaluar la calidad del trabajo de auditoría realizado. Estas revisiones deberán llevarse a cabo de la misma manera que cualquier otra auditoría.

Para evaluar la calidad del trabajo de auditoría en informática deberán practicarse revisiones externas.

P RUEBAS DE CONSENTIMIENTO

El objetivo de la fase de prueba de consentimiento es el de determinar si los controles internos operan como fueron diseñados para operar. El auditor debe determinar si los controles declarados en realidad existen y si realmente trabajan confiablemente.

Además de las técnicas manuales de recolección de evidencias, muy frecuentemente el auditor debe recurrir a técnicas de recolección de información asistidas por computadora, para determinar la existencia y confiabilidad de los

Programa
de control
de calidad

Tipos de pruebas

controles. Por ejemplo, para evaluar la existencia y confiabilidad de los controles de un sistema en red, se requerirá el entrar a la red y evaluar directamente al sistema.

PRUEBAS DE CONTROLES DEL USUARIO

En algunos casos el auditor puede decidir el no confiar en los controles internos dentro de las instalaciones informáticas, porque el usuario ejerce controles que compensan cualquier debilidad dentro de los controles internos de informática. Estas pruebas que compensan las deficiencias de los controles internos se pueden realizar mediante cuestionarios, entrevistas, vistas y evaluaciones hechas directamente con los usuarios

PRUEBAS SUSTANTIVAS

El objetivo de la fase de pruebas sustantivas es obtener evidencia suficiente que permita al auditor emitir su juicio en las conclusiones acerca de cuándo pueden ocurrir pérdidas materiales durante el procesamiento de la información. El auditor externo expresará este juicio en forma de opinión sobre cuándo puede existir un proceso equivocado o falta de control de la información. Se pueden identificar ocho diferentes pruebas sustantivas:

- Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad.
- Pruebas para asegurar la calidad de los datos.
- Pruebas para identificar la inconsistencia de los datos.
- Pruebas para comparar con los datos o contadores físicos.
- Confirmación de datos con fuentes externas.
- Pruebas para confirmar la adecuada comunicación.
- Pruebas para determinar falta de seguridad.
- Pruebas para determinar problemas de legalidad.

Debemos cuestionarnos el beneficio de tener un excesivo control o bien evaluar el beneficio marginal de tener mayor control contra el costo que representa éste. Para ello es necesario evaluar el costo por falla del sistema, y sus repercusiones para determinar el grado de riesgo y confianza necesarios contra el costo de implantación de controles y el costo de recuperación de la información o eliminación de las repercusiones.

El au

- Dura
- Dura
- Dura

En ge
sideran q
pendencia
nar esto:

- Aume
- Asign
- poster
- Crear
- audito
- Obten

Realiz
lograr los
subsistema
cas de cad
subsistema
evaluación
sin olvidar

La sum
sistema,

Los pas
llos que se
investigació
de cómo es
que son pro
controles in
ro, el audito
troles que s
dimientos. I
sos el audito
der con pas

Durante
ciles. Cada
quiere de ev
cias obtenid

El auditor debe participar en tres estados del sistema:

- Durante la fase de diseño del sistema.
- Durante la fase de operación.
- Durante la fase posterior a la auditoría.

En general, la opinión del gerente de informática y de la alta gerencia consideran que el que el auditor participe en la fase de diseño disminuye la independencia del auditor, pero existen varias formas en las cuales se puede eliminar esto:

- Aumentando los conocimientos en informática del auditor.
- Asignar diferentes auditores a la fase de diseño, al trabajo de auditoría y al posterior a la auditoría.
- Crear una sección de auditoría en informática dentro del departamento de auditoría interno, especializado en auditoría en informática.
- Obtener mayor soporte de la alta gerencia.

Realizar una auditoría en informática es un trabajo complejo. Por ello, para lograr los objetivos, el auditor necesita dividir los sistemas en una serie de subsistemas, identificando los componentes que realizan las actividades básicas de cada subsistema, evaluar la confianza de cada componente, y la de los subsistemas, y en forma agregada evaluar cada subsistema hasta llegar a una evaluación global sobre la confianza total del sistema. Esto se deberá realizar sin olvidar el postulado de investigación de operaciones, que nos señala que:

La suma de los óptimos parciales de los subsistemas no es igual al óptimo del sistema, pero nos da una buena aproximación.

Los pasos que involucran una auditoría en informática son similares a aquellos que se realizan para auditar un sistema manual. Primero se realiza una investigación preliminar del área de informática, para lograr un entendimiento de cómo está siendo administrada la instalación y de los principales sistemas que son procesados. En segundo lugar, si el auditor determina confiar en los controles internos del sistema, se realiza una investigación detallada. En tercero, el auditor, de acuerdo con su juicio, prueba la confianza sobre aquellos controles que son críticos. En cuarto, se realizan pruebas sustantivas de los procedimientos. Finalmente, el auditor debe dar una opinión. Después de estos pasos el auditor evalúa los controles internos del sistema y decide si debe proceder con pasos alternativos.

Durante la auditoría en informática deben tomarse muchas decisiones difíciles. Cada evaluación sobre la confianza de los sistemas de control interno requiere de evaluaciones complejas realizadas en forma conjunta con las evidencias obtenidas.

EVALUACIÓN DE LOS SISTEMAS DE ACUERDO AL RIESGO

Una de las formas de evaluar la importancia que puede tener para la organización un determinado sistema, es considerar el riesgo que implica el que no sea utilizado adecuadamente, la pérdida de la información o bien el que sea usado por personal ajeno a la organización. Para evaluar el riesgo de un sistema con mayor detalle véase el apartado "Plan de contingencia y procedimientos de respaldo para casos de desastre", en el capítulo 6.

Algunos sistemas de aplicaciones son de más alto riesgo que otros debido a que:

- Son susceptibles a diferentes tipos de pérdida económica.

Ejemplo

Fraudes y desfalcos entre los cuales están los sistemas financieros.

El auditor debe de poner especial atención a aquellos sistemas que requieran de un adecuado control financiero.

Ejemplo

Flujo de caja, inversiones cuentas por pagar y cobrar, nómina.

- Las fallas pueden impactar grandemente a la organización.

Ejemplo

Una falla en el procesamiento de la nómina puede tener como consecuencia el que se tenga una huelga.

- Interfieren con otros sistemas, y los errores generados permean a otros sistemas.
- Potencialmente, alto riesgo debido a daños en la competencia. Algunos sistemas le dan a la organización un nivel competitivo muy alto dentro de un mercado.

Ejemplo

Sistema de planeación estratégica. Patentes, derechos de autor, los cuales son las mayores fuentes de recursos de la organización. Otros a través de los cuales su pérdida puede destruir la imagen de la organización.

- Sistemas de tecnología de punta o avanzada. Si los sistemas utilizan tecnología avanzada o de punta.

Ejemplo

Sistemas de bases de datos, sistemas distribuidos o de comunicación, tecnología sobre la cual la organización tenga muy poca experiencia o respaldo, la cual es más probable que sea una fuente de problemas de control.

- Sistemas de alto costo. Sistemas que son muy costosos de desarrollar, los cuales son frecuentemente sistemas complejos que pueden presentar muchos problemas de control.

INVE

Es ne
que p
rápid
nismo

La in
trol ger
troles ger
prácticas
de la insta
los contro
dos sobre
aplicacion
Se del
mento po
document
programa
Se deb

dentro de
ria y la fec
En el c
ción prelin
pos de cón
nar se deb
áreas, basá

Administ
departame
de docume

La efici
objetivos es
adapta a lo

Esta ad
usuarios de
dirección y
dicho sist
cutivos y us

Asimism
que el perso
dos que se e
trol, únicam

¹ "The Spr

INVESTIGACIÓN PRELIMINAR

INVESTIGACIÓN PRELIMINAR

Es necesario iniciar el trabajo de obtención de datos con un contacto preliminar que permita una primera idea global. El objeto de este primer contacto es percibir rápidamente las estructuras fundamentales y diferencias principales entre el organismo a auditar y otras organizaciones que se hayan investigado.¹

La investigación preliminar debe incorporar fases de evaluación del control gerencial y del control de las aplicaciones. Durante la revisión de los controles gerenciales el auditor debe entender a la organización y las políticas y prácticas gerenciales usadas en cada uno de los niveles, dentro de la jerarquía de la instalación en que se encuentran las computadoras. Durante la revisión de los controles de las aplicaciones, el auditor debe entender los controles ejercidos sobre el mayor tipo de transacciones que fluyen a través de los sistemas de aplicaciones más significativos dentro de la instalación de computadoras.

Se debe recopilar información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitudes de documentos; la finalidad es definir el objetivo y alcance del estudio, así como el programa detallado de la investigación.

Se deberá observar el estado general del departamento o área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

En el caso de la auditoría en informática debemos comenzar la investigación preliminar con una visita al organismo, al área de informática y a los equipos de cómputo, y solicitar una serie de documentos. La investigación preliminar se debe hacer solicitando y revisando la información de cada una de las áreas, basándose en los siguientes puntos:

Administración. Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

La eficiencia en el departamento de informática sólo se puede lograr si sus objetivos están integrados con los de la institución y si permanentemente se adapta a los posibles cambios de éstos.

Esta adaptación únicamente puede ser posible si los altos ejecutivos y los usuarios de los sistemas toman parte activa en las decisiones referentes a la dirección y utilización de los sistemas de información, y si el responsable de dicho sistema constantemente consulta y pide asesoría y cooperación a los ejecutivos y usuarios.

Asimismo el control de la dirección de informática no es posible, a menos que el personal responsable aplique la misma disciplina de trabajo y los métodos que se exigen normalmente a los usuarios. Podemos hablar de tener el control, únicamente cuando se contemplaron los objetivos, se estableció un presu-

¹ "The Spreading Darger of Computer Crime", en *Business Week*, 20 de abril de 1981.

puesto y se registraron correctamente los costos en el desarrollo de la aplicación, y cuando ésta contempla el nivel de servicio en términos de calidad y tiempos mínimos de entrega de resultados de la operación del computador.

El éxito de la dirección de informática dentro de una organización depende finalmente de que todas las personas responsables adoptan una actitud positiva respecto a su trabajo y evalúen constantemente la eficiencia en su propio trabajo, así como el desarrollado en su área, estableciendo metas y estándares que incrementen su productividad.

La dirección de informática, según las diferentes áreas de la organización, es evaluada desde diferentes puntos de vista.

Los usuarios a nivel operativo generalmente la ven como una herramienta para incrementar su eficiencia en el trabajo. Para estos usuarios, la dirección de informática es una función de servicio. Cada grupo de usuarios tiene su propia expectativa del tipo y nivel de servicio, sin considerar el costo del mismo y normalmente sin tomar en cuenta las necesidades de otros grupos de usuarios.

Los altos ejecutivos consideran a la dirección de informática como una inversión importante, que tiene la función de participar activamente en el cumplimiento de los objetivos de la organización. Por ello, esperan un máximo del retorno de su inversión; esperan que los recursos destinados a la dirección de informática proporcionen un beneficio máximo a la organización y que ésta participe en la administración eficiente y en la minimización de los costos mediante información que permita una adecuada toma de decisiones. Los directivos, con toda la razón, consideran que la organización cada día depende más del área de informática y consecuentemente esperan que se deba administrar lo más eficiente y eficaz posible.

Esencialmente, la meta principal de los administradores de la dirección de informática es la misma que inspira cualquier departamento de servicio: combinar un servicio adecuado con una operación económica.

El problema estriba en balancear el nivel de servicio a los usuarios, que siempre puede ser incrementado a costa de un incremento del factor económico o viceversa.

Para poder analizar y dimensionar la estructura a auditar se debe solicitar:

A nivel organización total:

- Objetivos a corto y largo plazos.
- Manual de la organización.
- Antecedentes o historia del organismo.
- Políticas generales.

A nivel del área de informática:

- Objetivos a corto y largo plazos.
- Manual de organización del área que incluya puestos, funciones, niveles jerárquicos y tramos de mando.
- Manual de políticas, reglamentos internos y lineamientos generales.
- Número de personas y puestos en el área.

Requerimientos
de una auditoría

- Proc
- Pres
- Recu
- Solic
- local
- prog
- Estuc
- Fecha
- Cont
- Cont
- Conv
- Confi
- Confi
- locali
- Plane
- Ubica
- Polític
- Polític
- Polític
- extern
- Sistem
- Descri
- larse, c
- Manua
- Manua
- Descri
- Diagra
- Fecha
- Proyec
- Bases c
- Proced
- Sistema
- En el m
- ción, deben
- Se solic
- No
- No
- Se tiene
- No
- Es i

- Procedimientos administrativos del área.
- Presupuestos y costos del área.

Recursos materiales y técnicos:

- Solicitar documentos sobre los equipos, así como el número de ellos, su localización y sus características (de los equipos instalados, por instalar y programados).
- Estudios de viabilidad.
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.
- Configuración de los equipos y capacidades actuales y máximas.
- Configuración de equipos de comunicación (redes internas y externas) y localización de los equipos.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.
- Políticas de seguridad física y prevención contra contingencias internas y externas.

Sistemas:

- Descripción general de los sistemas instalados y de los que estén por instalarse, que contengan volúmenes de información.
- Manual de formas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de entrada, archivos, salida.
- Fecha de instalación de los sistemas.
- Proyecto de instalación de nuevos sistemas.
- Bases de datos, propietarios de la información y usuarios de la misma.
- Procedimientos y políticas en casos de desastre.
- Sistemas propios, rentados y adquiridos.

En el momento de hacer la planeación de la auditoría o bien en su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

- Se solicita la información y se ve que:

- No se tiene y se necesita.
- No se tiene y no se necesita.

- Se tiene la información pero:

- No se usa.
- Es incompleta.

Uso
de información

- No está actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de que no se disponga de la información y se considere que no se necesita, se debe evaluar la causa por la que no es necesaria, ya que se puede estar solicitando un tipo de información que debido a las características del organismo no se requiera. Eso nos dará un parámetro muy importante para hacer una adecuada planeación de la auditoría.

En el caso de que no se tenga la información pero que sea necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar.

En el caso de que se tenga la información pero que no se utilice, se debe analizar por qué no se usa. El motivo puede ser que esté incompleta, que no esté actualizada, que no sea la adecuada, etc. Hay que analizar y definir las causas para señalar alternativas de solución, lo que nos lleva a la utilización de la información.

En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa; de ser así, se considerará dentro de las conclusiones de la evaluación, ya que como se dijo la auditoría no sólo debe considerar errores, sino también señalar los aciertos.

Antes de concluir esta etapa no se olvide que el éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento). Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

PERSONAL PARTICIPANTE

Una de las partes más importantes en la planeación de la auditoría en informática es el personal que deberá participar.

En este punto no veremos el número de personas que deberán participar, ya que esto depende de las dimensiones de la organización, de los sistemas y de los equipos; lo que se deberá considerar son las características del personal que habrá de participar en la auditoría.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervenga esté debidamente capacitado, que tenga un alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases debemos considerar los conocimientos, la práctica profesional y la capacitación que debe tener el personal que intervendrá en la auditoría.

En primer zación, que de la auditoría, p las reuniones

Éste es un dirección, ni c una o varias p ción en el mor

También s en el momento de comprobac do, y comple sólo el punto d del sistema.

Para comp de la auditoría

- Técnico en
- Conocimie
- Experiencia
- Experiencia
- Conocimie
- Conocimie
- Conocimie
- Conocimie

En el caso d mientos y exper caciones, etcéte

Lo anterior y experiencias s con las caracter

Una vez pla bilidad de prese de auditores ext

La carta con su confirmación auditoría, las lin dad y los inform

Una vez que do en la figura 2. Este formato de cuado control de de formulación, l dad, el número c minación, el núm

En primer lugar, debemos pensar que hay personal asignado por la organización, que deba tener el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionarnos toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, será casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información, o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se está solicitando, y complementen el grupo multidisciplinario, ya que debemos analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para complementar el grupo, como colaboradores directos en la realización de la auditoría, se deben tener personas con las siguientes características:

- Técnico en informática.
- Conocimientos de administración, contaduría y finanzas.
- Experiencia en el área de informática.
- Experiencia en operación y análisis de sistemas.
- Conocimientos y experiencia en psicología industrial.
- Conocimiento de los sistemas operativos, bases de datos, redes y comunicaciones, dependiendo del área y características a auditar.
- Conocimientos de los sistemas más importantes.

Características del personal

En el caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, comunicaciones, etcétera.

Lo anterior no significa que una sola persona deba tener los conocimientos y experiencias señaladas, pero sí que deben intervenir una o varias personas con las características apuntadas.

Una vez planeada la forma de llevar a cabo la auditoría, estaremos en posibilidad de presentar la carta —convenio de servicios profesionales (en el caso de auditores externos)— y el plan de trabajo.

La carta convenio es un compromiso que el auditor dirige a su cliente para su confirmación de aceptación. En ella se especifican el objetivo y alcance de la auditoría, las limitaciones y la colaboración necesaria, el grado de responsabilidad y los informes que se han de entregar.

Una vez que se ha hecho la planeación, se puede utilizar el formato señalado en la figura 2.1, el cual servirá para resumir el plan de trabajo de la auditoría. Este formato de programa de auditoría nos servirá de base para llevar un adecuado control del desarrollo de la misma. En él figuran el organismo, la fecha de formulación, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días-hombre estimados.

Programa de auditoría

El control del avance de la auditoría lo podemos llevar mediante el formato de la figura 2.2, el cual nos permite cumplir con los procedimientos de control y asegurarnos que el trabajo se está llevando a cabo de acuerdo con el programa de auditoría, con los recursos estimados y en el tiempo señalado en la planeación.

El hecho de contar con la información del avance permite que el trabajo elaborado pueda ser revisado por cualquiera de nuestros asistentes.

Como ejemplo de propuesta de auditoría en informática, véase la figura 2.3, y como ejemplo de contrato de auditoría en informática consúltese la figura 2.4.

Figura 2.1.

ORGANISMO:

FASE

PERSONAL PARTICIPANTE

ORGANISMO: _____ NÚM. _____ HOJA NÚM.: _____ DE _____

PERIODO QUE REPORTA _____

[illegible]

EDENTES

ntecedentes específicos del proyecto de auditoría.)

OS DE LA AUDITORÍA EN INFORMÁTICA

jetivo específico de la auditoría.)

ES DEL PROYECTO

el proyecto comprende:

ón de la dirección de informática en lo que corresponde a:

rganización.

iones.

tivos.

ectura.

rsos humanos.

as y políticas.

citación.

es de trabajo.

roles.

ndares.

iciones de trabajo.

ción presupuestal y financiera.

on de los sistemas:

ación de los diferentes sistemas en operación (flujo, procedi-
os, documentación, organización de archivos, estándares de
amación, controles, utilización de los sistemas, opiniones de
suarios).

ación de avances de los sistemas en desarrollo y congruencia
l diseño general, control de proyectos, modularidad de los siste-

ridad lógica de los sistemas, confidencialidad y respaldos

- Análisis de la seguridad lógica y confidencialidad.
 - Evaluación de los proyectos en desarrollo, prioridades y personal asignado.
 - Evaluación de la participación de auditoría interna.
 - Evaluación de controles.
 - Evaluación de las licencias, la obtención de derechos de autor y de la confidencialidad de la información.
 - Entrevistas con usuarios de los sistemas.
 - Evaluación directa de la información obtenida contra las necesidades y requerimientos de los usuarios.
 - Análisis objetivo de la estructuración y flujo de los programas.
 - Análisis y evaluación de la información compilada.
 - Elaboración de informe.
3. Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:
- Solicitud de los estudios de viabilidad, costo/beneficio y características de los equipos actuales, proyectos sobre adquisición o ampliación de equipo y su actualización.
 - Solicitud de contratos de compra o renta de los equipos.
 - Solicitud de contratos de mantenimiento de los equipos.
 - Solicitud de contratos y convenios de respaldo.
 - Solicitud de contratos de seguros.
 - Bitácoras de los equipos.
 - Elaboración de un cuestionario sobre la utilización de equipos, archivos, unidades de entrada/salida, equipos periféricos, y su seguridad.
 - Visita a las instalaciones y a los lugares de almacenamiento de archivos magnéticos.
 - Visita técnica de comprobación de seguridad física y lógica de las instalaciones.
 - Evaluación técnica del sistema eléctrico y ambiental de los equipos, del local utilizado y en general de las instalaciones.
 - Evaluación de los sistemas de seguridad de acceso.
 - Evaluación de la información recopilada, obtención de gráficas, porcentajes de utilización de los equipos y su justificación.
 - Elaboración de informe.
4. Elaboración del informe final, presentación y discusión del mismo, y presentación de conclusiones y recomendaciones.

V. TIEMPO Y COSTO

(Poner el tiempo en que se realizará el proyecto, de preferencia indicando el tiempo de cada una de las etapas; el costo del mismo, que incluya el personal participante en la auditoría y sus características, y la forma de pago.)

Figura 2.4. Ejemplo de contrato de auditoría en informática

Contrato de prestación de servicios profesionales de auditoría en informática que celebran por una parte _____,

representado por _____, en su carácter de _____ y que en lo sucesivo se denominará "el cliente", por otra parte _____, representada por _____ a quien se denominará "el auditor", de conformidad con las declaraciones y cláusulas siguientes:

DECLARACIONES

I. El cliente declara:

- a) Que es una _____
- b) Que está representado para este acto por _____ y que tiene como su domicilio _____
- c) Que requiere obtener servicios de auditoría en informática, por lo que ha decidido contratar los servicios del auditor.

II. Declara el auditor:

- a) Que es una sociedad anónima, constituida y existente de acuerdo con las leyes y que dentro de sus objetivos primordiales está el de prestar auditoría en informática _____
- b) Que está constituida legalmente según escritura número _____ de fecha _____ ante el notario público núm. _____ del _____ Lic. _____
- c) Que señala como su domicilio _____

III. Declaran ambas partes:

- a) Que habiendo llegado a un acuerdo sobre lo antes mencionado, lo formalizan otorgando el presente contrato que se contiene en las siguientes:

CLÁUSULAS

Primera. Objeto

El auditor se obliga a prestar al cliente los servicios de auditoría en informática para llevar a cabo la evaluación de la dirección de informática del cliente, que se detallan en la propuesta de servicios anexa que, firmada por las partes, forma parte integrante del contrato.

Segunda. Alcance del trabajo

El alcance de los trabajos que llevará a cabo el auditor interno dentro de este contrato son:

a) Evaluaciones de la dirección de informática en lo que corresponde a:

- Su organización.
- Funciones.
- Estructura.
- Cumplimiento de los objetivos.
- Recursos humanos.
- Normas y políticas.
- Capacitación.
- Planes de trabajo.
- Controles.
- Estándares.
- Condiciones de trabajo.
- Situación presupuestal y financiera.

b) Evaluación de los sistemas:

- Evaluación de los diferentes sistemas en operación (flujo, procedimientos, documentación, organización de archivos, estándares de programación, controles, utilización de los sistemas).
- Opiniones de los usuarios.
- Evaluación de avances de los sistemas en desarrollo y congruencia con el diseño general, control de proyectos, modularidad de los sistemas.
- Evaluación de prioridades y recursos asignados (humanos y equipos de cómputo).
- Seguridad lógica de los sistemas, confidencialidad y respaldos.
- Derechos de autor y secretos industriales, de los sistemas propios y los utilizados por la organización.
- Evaluación de las bases de datos.

c) Evaluación de los equipos:

- Adquisición, estudios de viabilidad y costo-beneficio.
- Capacidades.
- Utilización.
- Estandarización.
- Controles.
- Nuevos proyectos de adquisición.
- Almacenamiento.
- Comunicación.
- Redes.
- Equipos adicionales.
- Respaldos de equipos.

- Contratos de compra, renta o renta con opción a compra.
- Planes y proyecciones de adquisición de nuevos equipos.
- Mantenimientos.

d) Evaluación de la seguridad:

- Seguridad lógica y confidencialidad.
- Seguridad en el personal.
- Seguridad física.
- Seguridad contra virus.
- Seguros.
- Seguridad en la utilización de los equipos.
- Seguridad en la restauración de los equipos y de los sistemas.
- Plan de contingencia y procedimientos en caso de desastre.

e) Elaboración de informes que contengan conclusiones y recomendaciones por cada uno de los trabajos señalados en los incisos a, b, c, d de esta cláusula.

Tercera. Programa de trabajo

El cliente y el auditor convienen en desarrollar en forma conjunta un programa de trabajo en el que se determinen con precisión las actividades a realizar por cada una de las partes, los responsables de llevarlas a cabo y las fechas de realización.

Cuarta. Supervisión

El cliente o quien designe tendrá derecho a supervisar los trabajos que se le han encomendado al auditor dentro de este contrato y a dar por escrito las instrucciones que estime convenientes.

Quinta. Coordinación de los trabajos

El cliente designará por parte de la organización a un coordinador del proyecto, quien será el responsable de coordinar la recopilación de la información que solicite el auditor, y de que las reuniones y entrevistas establecidas en el programa de trabajo se lleven a cabo en las fechas establecidas.

Sexta. Horario de trabajo

El personal del auditor dedicará el tiempo necesario para cumplir satisfactoriamente con los trabajos materia de la celebración de este contrato, de acuerdo al programa de trabajo convenido por ambas partes, y gozará de libertad fuera del tiempo destinado al cumplimiento de las actividades, por lo que no estará sujeto a horarios y jornadas determinadas.

Séptima. Personal asignado

El auditor designará para el desarrollo de los trabajos objeto de este contrato a socios del despacho, quienes, cuando consideren necesario, incorporarán personal técnico capacitado de que dispone la firma, en el número que se requieran y de acuerdo a los trabajos a realizar.

Octava. F

El personal que queda expuesto que el auditor se derive cualquier

Novena. I

El auditor de este contrato se firme e estimado por la calidad con que cumplimentará por las partes del cliente, el cual deberá el program

Décima. H

El cliente por honorarios por el impuesto siguiente:

- a) _____
b) _____
c) _____
trato
info

Undécima.

El importe de los honorarios, honorarios de auditoría, pr

Duodécima

En caso de incumplimiento, demora en la entrega de los trabajos al cliente, se señalará

Decimotercera

De ser necesario, el cliente, las

Octava. Relación laboral

El personal del auditor no tendrá ninguna relación laboral con el cliente y queda expresamente estipulado que este contrato se suscribe en atención a que el auditor en ningún momento se considera intermediario del cliente respecto al personal que ocupe para dar cumplimiento de las obligaciones que se deriven de las relaciones entre él y su personal, y que exime al cliente de cualquier responsabilidad que a este respecto existiere.

Novena. Plazo de trabajo

El auditor se obliga a terminar los trabajos señalados en la cláusula segunda de este contrato en _____ días hábiles después de la fecha en que se firme el contrato y sea cobrado el anticipo correspondiente. El tiempo estimado para la terminación de los trabajos está con relación a la oportunidad con que el cliente entregue los documentos requeridos por el auditor y al cumplimiento de las fechas estipuladas en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de usuarios de los sistemas repercutirá en el plazo estipulado, el cual deberá incrementarse de acuerdo a las nuevas fechas establecidas en el programa de trabajo, sin perjuicio alguno para el auditor.

Décima. Honorarios

El cliente pagará al auditor por los trabajos objeto del presente contrato, honorarios por la cantidad de _____ más el impuesto al valor agregado correspondiente. La forma de pago será la siguiente:

- a) _____ % a la firma del contrato.
- b) _____ % a los _____ días hábiles después de iniciados los trabajos.
- c) _____ % a la terminación de los trabajos y presentación del informe final.

Undécima. Alcance de los honorarios

El importe señalado en la cláusula décima compensará al auditor por sueldos, honorarios, organización y dirección técnica propia de los servicios de auditoría, prestaciones sociales y laborales de su personal.

Duodécima. Incremento de honorarios

En caso de que se tenga un retraso debido a la falta de entrega de información, demora o cancelación de las reuniones, o cualquier otra causa imputable al cliente, este contrato se incrementará en forma proporcional al retraso y se señalará el incremento de común acuerdo.

Decimotercera. Trabajos adicionales

De ser necesaria alguna adición a los alcances o productos del presente contrato, las partes celebrarán por separado un convenio que formará parte

Decimocuarta. Viáticos y pasajes

Decimoquinta. Gastos generales

Decimosexta. Causas de rescisión

Decimoséptima. Jurisdicción

Enteradas las partes del contenido y alcance legal de este contrato, lo rubrican y firman de conformidad, en original y tres copias, en la ciudad de _____, el día _____.

EL AUDITOR

3

CAPÍTULO

Auditoría de la función de informática

OBJETIVOS

Al finalizar este capítulo, usted:

1. Explicará la importancia de la recolección de información sobre la organización que se va a auditar.
2. Describirá los pasos a seguir para realizar una adecuada evaluación de la estructura orgánica de la organización a auditar.
3. Definirá los elementos a tomar en cuenta en la evaluación del personal de una organización.
4. Manejará una guía para entrevistar adecuadamente al personal de informática.
5. Conocerá la importancia de evaluar los recursos financieros y materiales de una organización.

RECOPILACIÓN DE LA INFORMACIÓN ORGANIZACIONAL

Una vez elaborada la planeación de la auditoría, la cual servirá como plan maestro de los tiempos, costos y prioridades, y como medio de control de la auditoría, se debe empezar la recolección de la información. Para ello se procederá a efectuar la revisión sistematizada del área, a través de los siguientes elementos:

A) Revisión de la estructura orgánica:

- Jerarquías (definición de la autoridad lineal, funcional y de asesoría).
- Estructura orgánica.
- Funciones.
- Objetivos.

B) Se deberá revisar la situación de los recursos humanos.

C) Entrevistas con el personal de procesos electrónicos:

- Jefatura.
- Análisis.
- Programadores.
- Operadores.
- Personal de bases de datos.
- Personal de comunicación y redes.
- Personal de mantenimiento.
- Personal administrativo.
- Responsable de comunicaciones.
- Responsable de Internet e Intranet.
- Responsable de redes locales o nacionales.
- Responsable de sala de usuarios.
- Responsable de capacitación.

D) Se deberá conocer la situación en cuanto a:

- Presupuesto.
- Recursos financieros.
- Recursos materiales.
- Mobiliario y equipo.
- Costos.

E) Se hará un levantamiento del censo de recursos humanos y análisis de situación en cuanto a:

- Número de personas y distribución por áreas.
- Denominación de puestos y personal de confianza y de base (sindicalizado y no sindicalizado).
- Salario y conformación del mismo (prestaciones y adiciones).
- Movimientos salariales.
- Capacitación (actual y programa de capacitación).
- Conocimientos.
- Escolaridad.
- Experiencia profesional.
- Antigüedad (en la organización, en el puesto y en puestos similares fuera de la organización).
- Historial de trabajo.
- Índice de rotación del personal.
- Programa de capacitación (vigente y capacitación otorgada en el último año).

F) Por último, se deberá revisar el grado de cumplimiento de los documentos administrativos:

- Organización.
- Normas y políticas.
- Planes de trabajo.
- Controles.
- Estándares.
- Procedimientos.

La información nos servirá para determinar:

- Si las responsabilidades en la organización están definidas adecuadamente.
- Si la estructura organizacional está adecuada a las necesidades.
- Si el control organizacional es el adecuado.
- Si se tienen los objetivos y políticas adecuadas, si se encuentran vigentes y si están bien definidas.
- Si existe la documentación de las actividades, funciones y responsabilidades.
- Si los puestos se encuentran definidos y señaladas sus responsabilidades.
- Si el análisis y descripción de puestos está de acuerdo con el personal que los ocupa.
- Si se cumplen los lineamientos organizacionales.
- Si el nivel de salarios está de acuerdo con el mercado de trabajo.
- Si se tiene un programa de capacitación adecuado y si se cumple con él.
- Si los planes de trabajo concuerdan con los objetivos de la empresa.
- Si se cuenta con los recursos humanos necesarios que garanticen la continuidad de la operación o si se cuenta con los "indispensables".
- Si se evalúan los planes y se determinan las desviaciones.
- Si se cumple con los procedimientos y controles administrativos.

Funciones
de la gerencia

La organización debe estar estructurada de tal forma que permita lograr eficiente y eficazmente los objetivos, y que esto se logre a través de una adecuada toma de decisiones.

Una forma de evaluar la forma en que la gerencia de informática se está desempeñando es mediante la evaluación de las funciones que la alta gerencia debe realizar:

- **Planeación.** Determinar los objetivos del área y la forma en que se van a lograr estos objetivos.
- **Organización.** Proveer de las facilidades, estructura, división del trabajo, responsabilidades, actividades de grupo y personal necesario para realizar las metas.
- **Recursos humanos.** Seleccionando, capacitando y entrenando al personal requerido para realizar las metas.
- **Dirección.** Coordinando las actividades, proveyendo liderazgo y guía, y motivando al personal.
- **Control.** Comparando lo real contra lo planeado, como base para realizar los ajustes necesarios.

PRINCIPALES PLANES QUE SE REQUIEREN DENTRO DE LA ORGANIZACIÓN DE INFORMÁTICA

Estudio de viabilidad

Investiga los costos y beneficios de los usos a largo plazo de las computadoras, y recomienda cuándo debe o no usarse. En caso de requerirse el uso de la computación, sirve para definir el tipo de hardware, el software y el equipo periférico y de comunicación necesarios para lograr los objetivos de la organización.

El estudio de viabilidad consiste en la evaluación para determinar, primero, si la computadora puede resolver o mejorar un determinado procedimiento, y, segundo, cuál es la mejor alternativa. Para lograr esto se deben de contestar una serie de preguntas, entre las cuales están las siguientes:

- ¿La computadora resolverá o mejorará los procedimientos, funciones o actividades que se realizan?
- ¿La computadora mejorará la información para lograr una adecuada toma de decisiones?

- ¿El o
- (En e
- ¿Cuá
- ¿Cuá
- ¿Se d
- o bien
- que s
- ¿Se d
- cuaci
- ¿Se d
- ¿Se d
- creme
- ¿Qué
- ¿Qué
- ¿Cuál
- ¿Cuál
- ¿Cuál
- ¿Cuál
- ¿Cuál
- ¿Cuál

Despu
cificacione
asesores, p
y como gu

Planeaci modificac

Especifica l
y modificac
do la organ
hardware, c
Alguna

- Especific
- periféri
- Evaluac
- Planeac
- Pruebas
- Envío e
- Particip
- Diseño

- ¿El costo de la informática proporcionará una adecuada tasa de retorno? (En este caso, uno de los mayores problemas es el de evaluar los intangibles.)
- ¿Cuál es el periodo de recuperación de la inversión?
- ¿Cuál es la relación costo-beneficio que se obtendrá?
- ¿Se debe desarrollar un nuevo sistema o adquirir una nueva computadora, o bien hacer cambios al sistema actual o actualizar el sistema de cómputo que se tiene?
- ¿Se debe comprar o elaborar internamente los nuevos sistemas o las adecuaciones?
- ¿Se deben comprar los equipos, rentar o rentar con opción a compra?
- ¿Se deben hacer cambios estructurales en la organización para lograr el incremento en las capacidades de procesamiento?
- ¿Qué prioridad tiene el proyecto y para cuándo debe ser realizado?
- ¿Qué características tiene el sistema actual?
- ¿Cuáles son las áreas potenciales en que se usará el nuevo sistema?
- ¿Cuáles son las fortalezas y debilidades del sistema actual?
- ¿Cuáles son los recursos adicionales que se requerirán?
- ¿Cuál es el impacto a informática a largo plazo?
- ¿Cuáles son las restricciones que se deben considerar?
- ¿Cuál es el proyecto (PERT) que se tiene para su implementación?

Después de contestar estas preguntas, se debe elaborar un manual de especificaciones para ser distribuido al personal de informática, a los vendedores o asesores, para que les sirva de base para la contratación, elaboración o compra, y como guía de referencia y control del proyecto.

Planeación de cambios, modificaciones y actualización

Especifica las metas y actividades que se deben realizar para lograr los cambios y modificaciones, su independencia, tiempos, responsables y restricciones, cuando la organización toma la decisión de hacer cambios sustanciales de software, hardware, comunicación o equipos periféricos.

Algunas de las actividades típicas en este plan son:

- Especificación completa de hardware, software, comunicación, equipos periféricos.
- Evaluación y selección.
- Planeación física y preparación del lugar.
- Pruebas finales de aceptación.
- Envío e instalación.
- Participación del auditor interno y de los usuarios.
- Diseño de la estructura organizacional en caso de que se vea afectada.

Plan maestro

El plan maestro o plan estratégico de una instalación informática define los objetivos a largo plazo y las metas necesarias para lograrlo.

Una de las principales obligaciones del área de gerencia en informática es la construcción de un plan maestro. El plan maestro debe contener los objetivos, metas y actividades generales a realizar durante los siguientes años, incluyendo los nuevos sistemas que se pretenden implementar. Puede comprender un periodo corto o largo, dependiendo de las características y necesidades de la organización, y de lo cambiante de los sistemas. Una organización consolidada posiblemente requiera un plan maestro a más largo plazo que una organización de reciente creación.

El plan maestro puede comprender cuatro subplanes:

- A) El plan estratégico de organización. Incluye los objetivos de la organización a largo plazo, el medio ambiente, los factores organizacionales que serán afectados, así como sus prioridades, el personal requerido, su actualización, desarrollo y capacitación.
- B) El plan estratégico de sistemas de información. Se debe elaborar el plan estratégico y los objetivos planteados a largo plazo dentro de un plan estratégico de información, y las implicaciones que tendrá dentro de la organización en general y en la organización de informática.
- C) El plan de requerimientos. Define la arquitectura necesaria para lograr los objetivos planteados.
- D) El plan de aplicaciones de sistemas de información. Define los sistemas de aplicaciones que se desarrollarán, asociados con las prioridades y con el periodo en que serán implantados:
 - Adquisición o desarrollo de sistemas y su programa de trabajo.
 - Planeación de desarrollo y capacitación del personal necesario, o bien su contratación.
 - Recursos financieros que se necesitarán.
 - Requerimiento de facilidades.
 - Requerimientos de cambios en la organización.

Plan de proyectos

Consiste en el plan básico para desarrollar determinado sistema y para asegurarse que el proyecto es consistente con las metas y objetivos de la organización y con aquellos señalados en el plan maestro. Es importante que este plan no sólo contemple los sistemas, sino también las prioridades y el momento en el cual se desarrollarán los sistemas.

Un plan
grar un det
cadas dent

- Identifi
- Identifi
- Determ
- Determ
- Determ
- Determ

Plan de s continge en caso

Una instal
razones: h
mas del ec
ocurrencia
nización. S
deben tene
de recuper
encuentre
to para la c

EVAL

Para logra
de organiz

- Organ
- Funcio
- Objeti
- Anális
- Manua
- Manua
- Instru

Un plan de proyectos debe contener las actividades básicas para poder lograr un determinado proyecto. Las principales tareas que deben estar especificadas dentro de un plan de proyecto son:

- Identificar las tareas a realizar.
- Identificar las relaciones entre tareas.
- Determinar las restricciones de tiempo de cada tarea del proyecto.
- Determinar los recursos necesarios para cada tarea.
- Determinar cualquier otra restricción que se tenga.
- Determinar la secuencia de actividades.

Plan de seguridad: seguros, contingencias y recuperación en caso de siniestro

Una instalación de informática está expuesta a sufrir un desastre por muchas razones: huracanes, fuego, inundaciones, terremotos, sabotaje, fraude, problemas del equipo. Se debe tener un plan que permita eliminar en lo posible la ocurrencia de un desastre o de pérdida por causas internas o externas a la organización. Se debe contar con una adecuada planeación sobre los seguros que se deben tener en caso de que ocurra un desastre. También se debe tener un plan de recuperación para que en caso de que ocurra un desastre la instalación se encuentre en funcionamiento en el menor tiempo posible y con el menor impacto para la organización.

EVALUACIÓN DE LA ESTRUCTURA ORGÁNICA

Para lograr la evaluación de la estructura orgánica se deberá solicitar el manual de organización de la dirección, el cual deberá comprender, como mínimo:

- Organigrama con jerarquías.
- Funciones.
- Objetivos y políticas.
- Análisis, descripción y evaluación de puestos.
- Manual de procedimientos.
- Manual de normas.
- Instructivos de trabajo o guías de actividad.

También se deben solicitar:

- Objetivos de la dirección.
- Políticas y normas de la dirección.
- Planeación.

El director de informática y aquellas personas que tengan un cargo directivo deben llenar los cuestionarios sobre estructura orgánica, funciones, objetivos y políticas.

Básicamente, el departamento de informática puede estar dentro de alguno de estos tipos de dependencia:

A) Depende de alguna dirección o gerencia, la cual, normalmente, es la dirección de finanzas. Esto se debe a que inicialmente informática, o departamento de procesamiento electrónico de datos, nombre con que se le conocía, procesaba principalmente sistemas de tipo contable, financiero o administrativo; por ejemplo, la contabilidad, la nómina, ventas o facturación.

El que informática dependa del usuario principal, normalmente se presenta en estructuras pequeñas o bien que inician en el área de informática. La ventaja que tiene es que no se crea una estructura adicional para el área de informática y permite que el usuario principal tenga un mayor control sobre sus sistemas.

La desventaja principal es que los otros usuarios son considerados como secundarios y normalmente no se les da la importancia y prioridad requerida. Otra desventaja es que, como la información es poder, a veces hace que un área tenga un mayor poder. También, en ocasiones, sucede que el gerente o director del área usuaria del cual depende informática tiene muy poco conocimiento de informática; ello ocasiona que el jefe de informática cree una isla dentro de la gerencia y que acuerde directamente con otras gerencias usuarias, lo que da lugar a problemas con las líneas de autoridad. Este tipo de organización se usaba cuando comenzó el área de informática, y en la actualidad sólo es recomendable para instalaciones muy pequeñas.

B) La segunda posibilidad es que la dirección de informática dependa de la gerencia general; esto puede ser en línea o bien en forma de asesoría.

La ventaja de alguna de estas organizaciones es que el director de informática podrá tener un nivel adecuado dentro de la organización, lo cual le permitirá lograr una mejor comunicación con los departamentos usuarios y, por lo tanto, proporcionarles un mejor servicio y asignar las prioridades de acuerdo con los lineamientos dados por la gerencia general.

La desventaja es que aumentan los niveles de la organización, lo que eleva el costo de la utilización de los sistemas de cómputo.

C) La tercera posibilidad es para estructuras muy grandes, en las que hay bases de datos, redes o bien equipos en diferentes lugares.

En esta estructura se considera la administración corporativa. La dirección de informática depende de la gerencia general, y existen departamentos de informática dentro de las demás gerencias, las cuales reciben todas las normas, políticas, procedimientos y estándares de la dirección de informática, aunque funcionalmente dependan de la gerencia a la cual están adscritas. La dirección de informática es la responsable de las políticas, normatividad y controles.

Dirección de informática

Las f
perfectar
lugares d
en un lug
otro lugar
ciones que
tener bien

La ve
centraliza
se debe te
departame
zos o la d

En la a
ción de rec
utilizadas
nización se
muy claro
es el respo
zación del

Dentro
de tener un
los sistema
te la creaci
pero con la
sistema der

La resp
y en qué gr
tralizada o
mación ocu
minicompu
el desarrollo
tener polític
ción de equi
sición de eq
cual hace ne
mas y plata

D) La c
pendiente q

ESTRU

Uno de los el
Un personal
repercute dir

Las funciones, organización y políticas de los departamentos deben estar perfectamente definidas para evitar la duplicidad de mando y el que en dos lugares diferentes se estén desarrollando los mismos sistemas, o bien que sólo en un lugar se programe y no se permita usar los equipos para programar en otro lugar que no sea la dirección de informática. Esto se puede dar en instalaciones que tengan equipo en varias ciudades o lugares, y para evitarlo se deben tener bien definidas las políticas y funciones de todas las áreas.

La ventaja principal de esta organización consiste en que se puede tener centralizada la información (base de datos) y descentralizados los equipos; pero se debe tener una adecuada coordinación entre la dirección de informática y los departamentos de informática de las áreas usuarias para evitar duplicar esfuerzos o la duplicidad de mando.

En la actualidad, con la proliferación de computadoras personales y la creación de redes tanto internas como externas, así como de bases de datos que son utilizadas por diferentes usuarios a diversas profundidades, este tipo de organización se puede considerar como la más recomendable. Lo que hay que tener muy claro es que en este tipo de organización el departamento de informática es el responsable de las normas y políticas de adquisición de equipo y de utilización del mismo.

Dentro de esta misma forma de organización se debe evaluar la posibilidad de tener una estructura por proyectos, lo cual permitirá que los diseñadores de los sistemas estén más cerca de las áreas usuarias. Esto se puede lograr mediante la creación de una fuerza de trabajo independiente, con todos los recursos, pero con la obligación de cumplir con los objetivos y metas señalados para un sistema dentro de los diferentes planes.

La respuesta a si un tipo de organización corporativa es la más conveniente y en qué grado está en función de la decisión sobre tener una organización centralizada o descentralizada. La descentralización del procesamiento de la información ocurre en la actualidad como algo natural, debido al incremento de las minicomputadoras y a los sistemas en redes. Sin embargo, si se desea controlar el desarrollo, implementación y adquisición de equipos y de software, se deben tener políticas de descentralización muy bien definidas, para evitar la proliferación de equipo y de software que impida la adecuada comunicación y la adquisición de equipo no compatible, y que dificulte la integridad de los datos, lo cual hace necesario que el personal sea entrenado en diferentes equipos, sistemas y plataformas.

D) La cuarta forma de organización es la creación de una compañía independiente que dé servicio de informática a la organización.

ESTRUCTURA ORGÁNICA

Uno de los elementos más críticos es el relativo al personal y a su organización. Un personal calificado, motivado, entrenado y con la adecuada remuneración, repercute directamente en el buen desempeño del área de informática.

**Bases jurídicas (principalmente
en el sector público)**

A continuación ofrecemos unos cuestionarios que servirán para evaluar la estructura orgánica y las bases jurídicas:

¿Se ajusta la estructura orgánica actual a las disposiciones jurídicas vigentes?

SÍ NO

No, ¿por qué razón?

¿Cuáles son los ordenamientos legales en que se sustenta la dirección?

OBJETIVO DE LA ESTRUCTURA

¿La estructura actual está encaminada a la consecución de los objetivos del área? Explique en qué forma.

¿Permite la estructura actual que se lleven a cabo con eficiencia:

- | | | |
|----------------------------------|----|----|
| • Las atribuciones encomendadas? | SÍ | NO |
| • Las funciones establecidas? | SÍ | NO |
| • La distribución del trabajo? | SÍ | NO |
| • El control interno? | SÍ | NO |

Si alguna de las respuestas es negativa, explique cuál es la razón.

NIVELES JERÁRQUICOS

Es conveniente conocer los niveles jerárquicos para poder evaluar si son los necesarios y si están bien definidos.

¿Los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área?

SÍ NO

¿Cuáles y por qué son sus recomendaciones?

¿Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la:

- | | | |
|----------------|----|----|
| • Operación? | SÍ | NO |
| • Supervisión? | SÍ | NO |
| • Control? | SÍ | NO |

¿Permiten los niveles actuales que se tenga una ágil:

- | | | |
|-----------------------------|----|----|
| • Comunicación ascendente? | SÍ | NO |
| • Comunicación descendente? | SÍ | NO |
| • Toma de decisiones? | SÍ | NO |

Si alguna de las respuestas es negativa, explique cuál es la razón.

¿Considera que algunas áreas deberían tener:

- | | | |
|--------------------|----|----|
| • Mayor jerarquía? | SÍ | NO |
| • Menor jerarquía? | SÍ | NO |

¿Por qué razón?

DEPARTAMENTALIZACIÓN

¿Se consideran adecuados los departamentos, áreas y oficinas en que está dividida actualmente la estructura de la dirección?

SÍ NO

No, ¿por qué razón?

¿El área y sus subáreas tienen delimitadas con claridad sus responsabilidades?

SÍ NO

No, ¿qué efectos provoca esta situación?

PUESTOS

Se debe tener cuidado de que estén bien definidas las funciones de cada puesto, ya que desafortunadamente existe mucha confusión en los nombres que se dan a los puestos dentro del medio de la informática.

¿Los puestos actuales son adecuados a las necesidades que tiene el área para llevar a cabo sus funciones?

SÍ NO

No, ¿por qué razón?

¿El número de empleados que trabaja actualmente es adecuado para cumplir con las funciones encomendadas?

SÍ NO

Solicite el manual de descripción de puestos de:

- Análisis.
- Programación.

- Técnicos.
- Operación.
- Captura.
- Administrador de bases de datos.
- Comunicación y redes.
- Dirección.
- Administrativos.
- Otros.

Pida la plantilla del personal. Se debe especificar el número de personas que reportan a las personas que a su vez reportan a cada puesto, ya sea:

- Director.
- Subdirector.
- Jefes de departamento.
- Jefes de sección.
- Jefes de área.

¿El número de personas es el adecuado en cada uno de los puestos?

SÍ NO

¿Sí? ¿Por qué?

No, ¿cuál es el número de personal que consideraría adecuado? Señale el puesto o los puestos.

EXPECTATIVAS

Dentro de las expectativas se pueden detectar, en algunas ocasiones, deficiencias y frustraciones de las personas.

¿Considera que debe revisarse la estructura actual, a fin de hacerla más eficiente?

SÍ NO

¿Sí? ¿Por qué razón?

¿Cuál es la estructura que propondría?

De realizar una modificación a la estructura, ¿cuándo considera que debería hacerse?

¿Se encuen

¿No, por que

¿Su autorida

¿No, por qué

¿En su área

Sí, explique e

¿Existe en el

FUNCION

Las funciones e
designen con el
una organizació
nuación un cues

¿Se han estat

¿Por qué no?

¿Las funciones

¿Por qué no es

¿Están por esc

¿Cuál es la cau

¿Cuál es la for

AUTORIDAD

¿Se encuentra definida adecuadamente la línea de autoridad? SÍ NO

¿No, por qué razón?

¿Su autoridad va de acuerdo a su responsabilidad? SÍ NO

¿No, por qué razón?

¿En su área se han presentado conflictos por el ejercicio de la autoridad?

SÍ NO

Sí, explique en qué casos.

¿Existe en el área algún sistema de sugerencias y quejas por parte del personal?

SÍ NO

FUNCIONES

Las funciones en informática pueden diferir de un organismo a otro, aunque se designen con el mismo nombre; por ejemplo, la función del programador en una organización puede ser diferente en otra organización. Ofrecemos a continuación un cuestionario para evaluar las funciones.

EXISTENCIA

¿Se han establecido funciones del área? SÍ NO

¿Por qué no?

¿Las funciones están de acuerdo con las atribuciones legales?

SÍ NO

¿Por qué no están de acuerdo?

¿Están por escrito en algún documento las funciones del área? SÍ NO

¿Cuál es la causa de que no estén por escrito?

¿Cuál es la forma de darlas a conocer?

¿Quién elaboró las funciones?

¿Participó el área en su formulación?

¿Por qué causas no participó?

¿Quién las autorizó o aprobó?

COINCIDENCIAS

Se debe tener cuidado en que se conozcan las funciones del área.

¿Las funciones están encaminadas a la consecución de los objetivos institucionales e internos? SÍ NO

No, ¿por qué?

¿Las funciones del área están acordes al reglamento interior? SÍ NO

No, ¿en qué considera que difieren?

¿A qué nivel se conocen las funciones del área?

¿Conocen otras áreas las funciones del área? SÍ NO

No, ¿por qué?

¿Considera que se deben dar a conocer? SÍ NO

No, ¿por qué?

ADECUADAS

Debemos tener cuidado, ya que en esta área podemos detectar malestares del personal, debido a que si las funciones no son adecuadas a las necesidades, pueden existir problemas de definición de funciones o bien de cargas de trabajo.

¿Son adecuadas a la realidad las funciones? SÍ NO

En caso negativo, ¿por qué no son adecuadas?

¿Son adecuadas?

En caso negativo

¿Cuáles son sus

¿Son adecuadas?

¿Existen conflictos?

¿De qué tipo?

¿Se tiene control?

No, ¿por qué?

¿Cómo afecta la

¿Qué funciones

¿Participó la dirección?

No, ¿por qué?

Esta sección no
del personal.

¿Están delimitadas?

¿A nivel de departamento?

¿A nivel de puesto?

No, ¿por qué?

¿Las actividades
asignadas?

¿Son adecuadas a las necesidades actuales? SÍ NO

En caso negativo, ¿por qué no?

¿Cuáles son sus principales limitaciones?

¿Son adecuadas a las cargas de trabajo? SÍ NO

¿Existen conflictos por las cargas de trabajo desequilibradas? SÍ NO

¿De qué tipo?

¿Se tiene contemplada la desconcentración? SÍ NO

No, ¿por qué?

¿Cómo afecta la desconcentración a las funciones?

¿Qué funciones se van a desconcentrar?

¿Participó la dirección de informática en su elaboración? SÍ NO

No, ¿por qué?

CUMPLIMIENTO

Esta sección nos sirve para evaluar el grado de cumplimiento de las funciones del personal.

¿Están delimitadas las funciones? SÍ NO

¿A nivel de departamento? SÍ NO

¿A nivel de puesto? SÍ NO

No, ¿por qué?

¿Las actividades que realiza el personal son acordes a las funciones que tiene asignadas? SÍ NO

No, ¿qué tipo de actividades realiza que no están acordes a las funciones asignadas?

¿Cuál es la causa?

¿Quién las ordena?

¿Las actividades que realiza actualmente cumplen en su totalidad con las funciones conferidas? SÍ NO

No, ¿cuál es su grado de cumplimiento?

La falta de cumplimiento de sus funciones es por:

- | | | |
|-------------------------------------|----|----|
| • Falta de personal. | SÍ | NO |
| • Personal no capacitado. | SÍ | NO |
| • Cargas de trabajo excesivas. | SÍ | NO |
| • Porque realiza otras actividades. | SÍ | NO |
| • La forma en que las ordena. | SÍ | NO |

¿Cuáles funciones realiza en forma:

- Periódica?
- Eventual?
- Sistemática?
- Otras?

¿Tienen programas y tareas encomendadas? SÍ NO

No, ¿por qué?

¿Permiten cumplir con los programas y tareas encomendadas (necesidades de operación)? SÍ NO

No, ¿por qué causas?

¿Quién es el responsable de ordenar que se ejecuten las actividades?

En caso de realizar otras actividades, ¿quién las ordena y autoriza?

En caso de no encontrarse el jefe inmediato, ¿quién lo puede realizar?

APOYOS

71

EVALUACIÓN DE
LA ESTRUCTURA
ORGÁNICA

¿Para cumplir con sus funciones requiere de apoyos de otras áreas?

SÍ NO

¿De qué tipo?

¿Cuál es el área que proporciona el apoyo?

¿Se lo proporcionan con oportunidad?

SÍ NO

No, ¿qué le ocasiona?

No, ¿cómo resuelve esa falta de apoyo?

¿Con qué frecuencia lo solicita?

Para cumplir con sus funciones, ¿proporciona apoyos a otras áreas?

SÍ NO

Sí, ¿qué tipo de apoyo proporciona?

¿A cuántas áreas?

¿Cuáles son?

DUPLICIDAD

¿Existe duplicidad de funciones en la misma área?

SÍ NO

Sí, ¿qué conflictos ocasiona y cuáles funciones?

¿Existe duplicidad de funciones en otras áreas?

SÍ NO

Sí, ¿cuáles y dónde?

¿Qué conflictos ocasiona?

¿La duplicidad de funciones se debe a que el área no puede realizarlas?

SÍ NO

Sí, ¿cuál es la razón?

No, ¿cuál es su opinión al respecto?

¿Se pueden eliminar funciones? SÍ NO

Sí, ¿cuáles?

¿Se pueden transferir funciones? SÍ NO

Sí, ¿cuáles y adónde?

¿Permite la duplicidad que se dé el control interno? SÍ NO

No, ¿por qué?

OBJETIVOS

Uno de los posibles problemas o descontentos que puede tener el personal es el desconocimiento de los objetivos de la organización, lo cual puede deberse a una falta de definición de los objetivos; esto provoca que no se pueda tener una planeación adecuada.

Ofrecemos un cuestionario que sirve para evaluar los objetivos.

EXISTENCIA

¿Se han establecido objetivos para el área? SÍ NO

¿Quién los estableció?

¿Cuál fue el método para el establecimiento de los objetivos?

¿Participó el área en su establecimiento? SÍ NO

¿Cuáles fueron las principales razones de la selección de los objetivos?

¿Los objetivos establecidos son congruentes con:

- | | | |
|--|----|----|
| • Los de la dirección? | SÍ | NO |
| • Los de la subdirección? | SÍ | NO |
| • Los del departamento/oficina? | SÍ | NO |
| • Los de otros departamentos/oficinas? | SÍ | NO |

¿Por qué no se han establecido objetivos para el área?

Nadie le exige establecerlos. SÍ NO

Considera importante que se establezcan. SÍ NO

Es responsabilidad de otra área establecer los objetivos. SÍ NO

¿Cuál?

¿De qué manera planea el trabajo del área?

¿Cómo afecta la operación del área el no tener establecidos los objetivos?

FORMALES

¿Se han definido por escrito los objetivos del área? SÍ NO

¿En qué documentos? (Recabarlos.)

¿Por qué no están definidos por escrito?

¿Qué problemas se han derivado de esta situación?

CONOCIMIENTO

¿Se han dado a conocer los objetivos? SÍ NO

¿A quién se han dado a conocer?

¿Quién más debería conocerlos?

¿Qué método se ha utilizado para dar a conocer los objetivos?

¿Por qué no se han dado a conocer los objetivos?

¿Considera importante que los conozca el personal? SÍ NO

¿Cómo afecta a la operación del área el hecho de que los objetivos no se hayan dado a conocer o que su conocimiento sea parcial?

ADECUADOS

¿Abarcan los objetivos toda la operación del área? SÍ NO

¿Qué aspectos no se cubren?

¿Los objetivos son claros y precisos? SÍ NO

¿Son realistas? SÍ NO

¿Se pueden alcanzar? SÍ NO

¿Por qué?

¿Están de acuerdo con las funciones del área? SÍ NO¿Señalan cuáles son las realizaciones esperadas? SÍ NO¿Son congruentes con los objetivos institucionales? SÍ NO¿Sirven de guía al personal? SÍ NO¿Sirven para motivar al personal? SÍ NO¿Se han establecido para el corto, mediano y largo plazos? SÍ NO

¿Qué adecuaciones puede sugerir para los objetivos actuales?

CUMPLIMIENTO

¿En qué grado se cumplen los objetivos?

¿Existen mecanismos para conocer el grado de cumplimiento de los objetivos?
SÍ NO

Sí, ¿cuáles?

No, ¿de qué manera se establece el grado de cumplimiento?

¿Se elabora algún reporte sobre el grado de avance en el cumplimiento de los objetivos?
SÍ NO

¿Para quién y con qué frecuencia? (Recabar datos.)

¿Quién elabora este reporte?

¿Qué se hace en caso de desviación en el cumplimiento de los objetivos?

¿Qué sugerencia puede hacer para lograr el cumplimiento total de los objetivos?

ACTUALIZACIÓN¿Se revisan los objetivos? SÍ NO

¿Por sistema?

¿Quién rev

¿De qué m

¿Participa

¿Cuándo s

¿De qué m

¿Por qué

¿Qué sug

ANÁL

Entre las d
informática
ésta. Las fu
mador, en
se han divi
mador I, p

Esto h
niveles, fu
ellos consi
nido el gra
las que co
analizar la
funciones
niveles de

Si no
actual pla
imagen ge
Criter

- Agrup
- Agrup
- Local
- Local
- Local

¿Quién revisa los objetivos?

¿De qué manera se lleva a cabo la revisión?

¿Participa el área en la actualización de los objetivos? SÍ NO

¿Cuándo se hizo la última revisión de los objetivos?

¿De qué manera se incorporan las modificaciones derivadas de las revisiones?

¿Por qué no se revisan los objetivos?

¿Qué sugerencias tiene para que la actualización de los objetivos sea más eficaz?

ANÁLISIS DE ORGANIZACIONES

Entre las diferentes formas de la estructura organizacional de la dirección de informática no existe una evaluación concreta y aceptada de las funciones de ésta. Las funciones que en una organización son consideradas como de programador, en otra pueden ser de analista o de analista programador, y en algunas se han dividido ciertas funciones con diferentes niveles, por ejemplo, programador I, programador II, etcétera.

Esto ha dado por resultado que, al no existir una definición clara de los niveles, funciones y conocimientos, las personas se designen con el título que ellos consideran pertinente; por ejemplo, ingeniero en sistemas (sin haber obtenido el grado), analista de sistemas, o bien que en algunos países existan escuelas que confieran grados académicos que no son reconocidos oficialmente. Al analizar las organizaciones debemos tener muy en cuenta si están definidas las funciones y la forma de evaluar a las personas que ingresan a los diferentes niveles de la organización.

Si no existe un organigrama, el auditor debe elaborar uno que muestre el actual plan de organización, ya que esto facilita el estudio y proporciona una imagen general de la organización.

Criterios para analizar organigramas:

- Agrupar funciones similares y relacionarlas entre sí.
- Agrupar funciones que sean compatibles.
- Localizar la actividad cerca de la función a la que sirva.
- Localizar la actividad cerca o dentro de la función mejor preparada para realizarla.

Elaboración
del organigrama

- No asignar la misma función a dos personas o entidades diferentes.
- Separar las funciones de control y aquellas que serán objeto del mismo.
- Ningún puesto debe tener dos o más líneas de dependencia jerárquica.
- El tramo de control no debe ser exagerado, ni muy numerosos los niveles jerárquicos.

Cuando se estudia la estructura orgánica es importante hacer algunas anotaciones sobre las tareas asignadas a cada puesto y responder las siguientes preguntas:

- ¿Existen líneas de autoridad justificadas?
- ¿Hay una extralimitación de funciones?
- ¿Hay demasiada supervisión de funcionarios?
- ¿Es excesiva la supervisión en general?
- ¿Hay agrupamientos ilógicos en las unidades?
- ¿Hay uniformidad en las asignaciones?

EVALUACIÓN DE LOS RECURSOS HUMANOS

El desarrollo del personal implica:

- Establecer promociones y oportunidades de desarrollo.
- Educación y capacitación. Estas actividades mantienen la moral y las habilidades de los empleados en un nivel adecuado para cumplir con los objetivos y metas encomendadas, y les permitirá tener mayor motivación y mejores remuneraciones. En el área de informática es muy importante la capacitación para tener actualizado a nuestro personal en una disciplina en la que puede quedarse rezagado muy rápidamente, aunque, por otro lado, debido a la presión de tiempo con la que se trabaja, en muchas ocasiones no se le da al personal la oportunidad para capacitarse.

Se deberá obtener información sobre la situación del personal del área, para lo cual se puede utilizar la tabla de recursos humanos y la tabla de proyección de recursos humanos. A continuación un ejemplo de cuestionario para obtener información sobre los siguientes aspectos:

- Desempeño y comportamiento.
- Condiciones de ambiente de trabajo.
- Organización en el trabajo.
- Desarrollo y motivación.
- Capacitación y supervisión.

DESEMPEÑO Y CUMPLIMIENTO

¿Es suficiente el número de personal para el desarrollo de las funciones del área?

SÍ NO

¿Se deja

¿Está cap

No, ¿por c

¿Es eficaz

No, ¿por q

¿Es adecu

No, ¿por q

¿Es frecue

¿El persona

No, anote r

En general,
cidos?

No, ¿por qu

¿Alguna de
trabajo?

Si, ¿qué se

¿Respeto el

No, ¿por qu

¿Existe coop

No, ¿por qué

¿El personal

¿Presenta el

¿Se deja de realizar alguna actividad por falta de personal? SÍ NO

¿Está capacitado el personal para realizar con eficacia sus funciones? SÍ NO

No, ¿por qué?

¿Es eficaz en el cumplimiento de sus funciones? SÍ NO

No, ¿por qué?

¿Es adecuada la calidad del trabajo del personal? SÍ NO

No, ¿por qué?

¿Es frecuente la repetición de los trabajos encomendados? SÍ NO

¿El personal es discreto en el manejo de información confidencial? SÍ NO

No, anote repercusiones.

En general, ¿acata el personal las políticas, sistemas y procedimientos establecidos? SÍ NO

No, ¿por qué?

¿Alguna de las situaciones anteriores provoca un desequilibrio de las cargas de trabajo? SÍ NO

Si, ¿qué se hace al respecto?

¿Respeta el personal la autoridad establecida? SÍ NO

No, ¿por qué?

¿Existe cooperación por parte del personal para la realización del trabajo? SÍ NO

No, ¿por qué?

¿El personal tiene afán de superación? SÍ NO

¿Presenta el personal sugerencias para mejorar el desempeño actual? SÍ NO

¿Cómo considera las sugerencias?

¿Qué tratamiento se les da?

¿Se toman en cuenta las sugerencias de los empleados? SÍ NO

¿En qué forma?

¿Cómo se les da respuesta a las sugerencias?

CAPACITACIÓN

Uno de los puntos que se deben evaluar con más detalle dentro del área de informática es la capacitación; esto se debe al proceso cambiante y al desarrollo de nuevas tecnologías en el área.

Los programas de capacitación incluyen al personal de:

- Dirección. ()
- Análisis. ()
- Programación. ()
- Operación. ()
- Administración. ()
- Administrador de bases de datos. ()
- Comunicaciones redes. ()
- Captura. ()
- Otros (especifique). ()

¿Se han identificado las necesidades actuales y futuras de capacitación del personal del área? SÍ NO

No, ¿por qué?

¿Se desarrollan programas de capacitación para el personal del área? SÍ NO

No, ¿por qué?

¿Apoya la superioridad la realización de estos programas? SÍ NO

¿Se evalúan los resultados de los programas de capacitación? SÍ NO

No, ¿por qué?

Solicite el plan de capacitación para el presente año.

SUPERVISIÓN

79

EVALUACIÓN DE
LOS RECURSOS
HUMANOS

¿Cómo se lleva a cabo la supervisión del personal?

En caso de no realizarse, ¿por qué no se realiza?

¿Cómo se controlan el ausentismo y los retardos del personal?

¿Por qué no se llevan controles?

¿Cómo se evalúa el desempeño del personal?

¿Por qué no se evalúa?

¿Cuál es la finalidad de la evaluación del personal?

LIMITANTES

¿Cuáles son los principales factores internos que limitan el desempeño del personal?

¿Cuáles son los principales factores externos que limitan el desempeño del personal del área?

¿Cuál es el índice de rotación de personal en:

- Análisis? ()
- Operación? ()
- Administración? ()
- Captura? ()
- Programación? ()
- Dirección? ()
- Administración de bases de datos? ()
- Comunicaciones redes? ()
- Técnicos? ()
- Otros? (especifique). ()

En términos generales, ¿se adapta el personal al mejoramiento administrativo (resistencia al cambio)?

SÍ NO

¿Cuál es el grado de disciplina del personal?

¿Cuál es el grado de asistencia y puntualidad del personal?

¿Existe una política uniforme y consistente para sancionar la indisciplina del personal? SÍ NO

¿Se lleva a efecto esta política? SÍ NO

¿Puede el personal presentar quejas y/o problemas? SÍ NO

Sí, ¿cómo se solucionan?

¿Otras áreas externas presentan quejas sobre la capacidad y/o atención del personal del área? SÍ NO

Sí, ¿qué tratamiento se les da?

¿Cómo se otorgan los ascensos, promociones y aumentos salariales?

¿Cómo se controlan las faltas y ausentismos?

¿Cuáles son las principales causas de faltas y ausentismo?

CONDICIONES DE TRABAJO

Para poder trabajar se requiere que se tenga una adecuada área de trabajo, con mayor razón en un área en la que se debe hacer un trabajo de investigación e intelectual.

¿Conoce el reglamento interior de trabajo el personal del área? SÍ NO

¿Se apoyan en él para solucionar los conflictos laborales? SÍ NO

No, ¿por qué?

¿Cómo son las relaciones laborales del área con el sindicato?

¿Se presentan problemas con frecuencia? SÍ NO

Sí, ¿en qué aspectos?

¿Cómo se resuelven?

REMUNERACIONES

81

EVALUACIÓN DE
LOS RECURSOS
HUMANOS

Normalmente las personas están inconformes con su remuneración. Es importante evaluar que tan cierta es esta inconformidad o si está dada por otros malestares aunque sean señalados como inconformidad en las remuneraciones, o bien puede deberse a que se desconoce cómo se evalúa a la persona para poder darle una mejor remuneración.

¿Está el personal adecuadamente remunerado con respecto a:

- | | | |
|--|----|----|
| • Trabajo desempeñado? | SÍ | NO |
| • Puestos similares en otras organizaciones? | SÍ | NO |
| • Puestos similares en otras áreas? | SÍ | NO |

Sí, ¿cómo repercute?

No, ¿cómo repercute?

Conseguir información sobre los sueldos de los mismos niveles en otras organizaciones.

AMBIENTE

El ambiente en el área de informática, principalmente en programación, es muy importante para lograr un adecuado desarrollo.

¿El personal está integrado como grupo de trabajo? SÍ NO

No, ¿por qué?

¿Cuál es el grado de convivencia del personal?

¿Cómo se aprovecha esto para mejorar el ambiente de trabajo?

¿Son adecuadas las condiciones ambientales con respecto a:

- | | | |
|----------------------------------|----|----|
| • Espacio del área? | SÍ | NO |
| • Iluminación? | SÍ | NO |
| • Ventilación? | SÍ | NO |
| • Equipo de oficina? | SÍ | NO |
| • Mobiliario? | SÍ | NO |
| • Ruido? | SÍ | NO |
| • Limpieza y/o aseo? | SÍ | NO |
| • Instalaciones sanitarias? | SÍ | NO |
| • Instalaciones de comunicación? | SÍ | NO |

ORGANIZACIÓN DEL TRABAJO

¿Participa en la selección del personal? SÍ NO

No, ¿por qué?

¿Qué repercusiones tiene?

¿Se prevén las necesidades de personal con anterioridad:

En cantidad? SÍ NO

En calidad? SÍ NO

No, ¿por qué?

¿Está prevista la sustitución del personal clave? SÍ NO

No, ¿por qué?

DESARROLLO Y MOTIVACIÓN

¿Cómo se lleva a cabo la introducción y el desarrollo del personal del área?

En caso de no realizarse, ¿por qué no se realiza?

¿Cómo se realiza la motivación del personal del área?

¿Cómo se estimula y se recompensa al personal del área?

¿Existe oportunidad de ascensos y promociones? SÍ NO

¿Qué política hay al respecto?

ENTREVISTAS CON EL PERSONAL DE INFORMÁTICA

Se deberán efectuar entrevistas con el personal de informática, para lo cual puede entrevistarse a un grupo de personas elegidas, sin dejar de señalar que quienes

deseen ext
nados. En a
poder hace
que las opi
Esto no

- Grado
- Grado
- Satisfac
- Capaci
- Observ

Ofrecen

1. Nor
2. Pue
3. Pue
4. Pue
5. Núm
6. Des
7. Acti
8. Acti
9. ¿Co
10. ¿Cu
11. Señ
12. En
- esta
13. ¿Có
14. ¿Có
15. ¿Có
16. ¿Co
17. ¿So
18. Men
- año.
19. ¿Có
20. Obs

NOTA: En c
informática
iniciales. E
nes y com

SITUACIÓN PRESUPUESTAL Y FINANCIERA

PRESUPUESTOS

Se obtendrá información presupuestal y financiera del departamento, así como del número de equipos y características para hacer un análisis de su situación desde un punto de vista económico. Entre esta información se encuentra:

- Costos del departamento, desglosado por áreas y controles.
- Presupuesto del departamento, desglosado por áreas.
- Características de los equipos, número de ellos y contratos.

NOTA: Se deberán pedir los costos, presupuestos y características de los equipos señalados en los puntos anteriores, además de contestar el cuestionario, del cual se ofrece un ejemplo a continuación:

1. ¿Cuál es el gasto total anual del área de informática incluyendo renta del equipo y administración del centro de cómputo (gastos directos o indirectos)?

2. ¿Existe un sistema de contabilidad de costos por:
 - Usuario? ()
 - Por aplicación? ()
3. ¿Conocen los usuarios los costos de sus aplicaciones? sí NO
4. ¿Los reportes de costo permiten la comparación de lo gastado en la dirección de informática contra lo presupuestado? sí NO
5. Cite a los principales proveedores de su dirección en materia de:

Proveedor

Volumen anual

Mobiliario en general
Consumibles
Equipo
Software
Mantenimiento
Equipo auxiliar
Papelería
Cintas, discos, etcétera

6. ¿P

U
S
C
A
G
In
S
O

7. ¿U

C
R
R
R
M
O

8. ¿C

C
R
E
E
M
OPueden
este caso

RECU

A continua
recursos fin

¿Quién in

¿Se resp

No, ¿en c

6. ¿Cuáles cargos adicionales se manejan por separado fuera del contrato?
Ponga una X en ellos.

Utilización del equipo.	()
Servicio de mantenimiento.	()
Capacitación del personal.	()
Asesoría en sistemas de cómputo.	()
Gastos de instalación del equipo.	()
Impuestos federales, estatales, municipales y especiales.	()
Seguros de transporte y compra de equipo.	()
Otros (especifíquelos).	()

7. ¿Cuál es la situación jurídica del equipo (especificar por equipo)?

Compra del equipo.	()
Renta del equipo.	()
Renta con opción a compra.	()
Renta de tiempo máquina.	()
Maquila.	()
Otro, ¿cuál?	()

8. ¿Cuál es la situación jurídica del software (especificar por software)?

Compra.	()
Renta.	()
Elaborado internamente.	()
Maquila.	()
Otro, ¿cuál?	()

Pueden existir diferentes situaciones jurídicas de los equipos y del software; en este caso se debe especificar la situación de cada uno.

RECURSOS FINANCIEROS

A continuación, se ofrecen algunas preguntas útiles para abordar el tema de los recursos financieros.

FORMULACIÓN

¿Quién interviene en la formulación del presupuesto del área?

¿Se respetan los planteamientos presupuestales del área? SÍ NO

No, ¿en qué partidas no se ha respetado y en qué monto?

ADECUACIÓN

¿Los recursos financieros con que cuenta el área, son suficientes para alcanzar los objetivos y metas establecidos? SÍ NO

No, ¿qué efectos se han tenido en el área al no contar con suficientes recursos financieros?

RECURSOS MATERIALES

PROGRAMACIÓN

¿Existe un programa sobre los requerimientos del área? SÍ NO

¿Qué personas del área intervienen en su elaboración?

¿Se respetan los planteamientos del área? SÍ NO

No, ¿en qué aspectos no se respetan?

ADECUACIÓN

¿Los recursos materiales que se le proporcionan al área, son suficientes para cumplir con las funciones encomendadas? SÍ NO

No, ¿en qué no son suficientes?

¿Los recursos materiales se proporcionan oportunamente? SÍ NO

¿Cuáles son las principales limitaciones que tiene el área en cuanto a los recursos materiales?

¿Qué sugerencias harían para superar las limitaciones actuales?

SERVICIOS GENERALES

¿Existe un programa sobre los servicios generales que requiere el área? SÍ NO

¿Considera los servicios generales que se proporcionan al área:

- | | |
|----------------|-------|
| • Adecuados? | SÍ NO |
| • Suficientes? | SÍ NO |
| • Oportunos? | SÍ NO |

En caso de que alguna de las respuestas sea negativa especifique cuál es la deficiencia.

¿Qué sugerencias harían para superar las limitaciones actuales?

MOBILIARIO Y EQUIPO

¿Se cuenta con el equipo y mobiliario adecuados y en cantidad suficiente para desarrollar su trabajo?

SÍ NO

¿Por qué?

¿Están adecuadamente distribuidos en el área de trabajo?

¿Actualmente se están dejando de realizar actividades por falta de material y equipo?

SÍ NO

¿Qué se hace para solucionar este problema?

¿Conoce esta situación el jefe de la unidad?

¿Qué medidas se han tomado?

¿Existe el servicio de mantenimiento del equipo?

¿Existen medidas de seguridad?

SÍ NO

¿Cuáles?

No, ¿por qué?

¿Qué se hace con el equipo en desuso?

¿Sobre quién recae la responsabilidad del equipo?

¿Con qué frecuencia se renuevan el equipo y mobiliario?

¿Se recogen opiniones y sugerencias que nos permitan establecer las medidas correctivas con las cuales lograr un mejor funcionamiento de estos recursos?

4

CAPÍTULO

Evaluación de los sistemas

OBJETIVOS

Al finalizar este capítulo, usted:

1. Evaluará si las organizaciones que se van a auditar cuentan con los sistemas necesarios para cumplir con sus funciones.
2. Explicará la importancia de la evaluación del diseño lógico de un sistema y de su desarrollo.
3. Definirá las características principales del control de proyectos, ya que de esto depende el adecuado desarrollo de un sistema.
4. Conocerá el contenido mínimo que deben tener los instructivos de operación de los sistemas.
5. Describirá cuáles son los trabajos que se deben realizar para iniciar la operación de un sistema.
6. Explicará la importancia de las entrevistas a los usuarios para comparar los datos con los proporcionados por la dirección de informática.
7. Conocerá los señalamientos principales relacionados con los derechos de autor y la informática.

EVALUACIÓN DE SISTEMAS

Existen diversas formas por medio de las cuales las organizaciones pueden contar con el software necesario para cumplir con sus requerimientos; entre ellas se encuentran:

Elaborado por el usuario, o bien un software comercial. El que el usuario elabora un determinado software tiene las siguientes ventajas: normalmente es desarrollado para cubrir todas las necesidades del usuario; puede ser modificado de acuerdo a las necesidades de la organización; contiene sistemas de seguridad propios. Aunque tiene estas desventajas: es más costoso; su tiempo de implementación es más largo, su mantenimiento y actualización, normalmente no se hacen sobre una base periódica.

Software compartido o regalado. Normalmente se trata de un software sencillo elaborado para computadoras personales, que puede ser conseguido a bajo costo vía Internet. El peligro de este tipo de software es que puede no cumplir con todas nuestras necesidades, además de que se debe tener cuidado con los programas pirata o con virus.

Se debe considerar la librería de programas de aplicación. Sin importar la forma de desarrollo, los programas siempre son escritos para correr en un determinado sistema operativo. Un elemento importante del sistema operativo es la cantidad y diversidad de programas de aplicación que son escritas en él, lo cual se conoce como la librería de programas de aplicación. Es importante tomar en cuenta el sistema operativo utilizado, ya que puede ser un tipo de sistema operativo conocido como "propietario", el cual sólo puede ser usado en máquinas de un determinado proveedor.

Software transportable (portability). Se considera que un software es portable o transportable cuando 1) tiene diferentes versiones para diferentes sistemas operativos, cuando 2) puede cambiarse entre dos o más sistemas operativos, o cuando 3) puede ser fácilmente convertido de un sistema operativo a otro. Un software que es transportable permite, aparentemente, usar el mismo programa de aplicación sin importar el sistema computacional. Se puede usar en una gran computadora (*mainframe*) o en una minicomputadora, o cambiar entre diferentes tipos de minicomputadoras. Una organización que obtiene un software que tiene diferentes versiones, pero que en esencia es el mismo, lo cual significa que es transportable, ahorra tiempo en entrenamiento y en personal, y permite el que fácilmente se mueva de un trabajo a otro o bien en diferentes lugares.

Un solo usuario o multiusuario. Como en el caso de los sistemas operativos, los programas de aplicación pueden ser para un solo usuario o para una variedad de usuarios.

Categorización del software de aplicación por usuario. El software puede ser catalogado como: de propósitos generales, de funciones específicas o específico de la industria.

Software
bien puede
paquetes
Por ejemplo
diseñados
tes indivi
puede ten
paquete d
por dos d
cual pued
ware que
mandos y
usar paqu
tener el ir
mientos d

Al de
de adquiri
zación se
bien "casa
pero requ
La ela
lle, para l
mas hasta

- Existe
- gram
- Existe
- están
- vos.
- Los re
- efier

El pla
futuro, co

- ¿Cuál
- ¿Cuár
- ¿Qué
- ¿Cuár

La est
cursos qu
estarán fu

- ¿Qué
- ¿Qué
- ¿Qué
- ¿Qué

Software a la medida de la oficina. El software comercial puede ser vendido, o bien puede ser elaborado internamente como paquetes individuales o como paquetes integrales y compatibles que son diseñados para trabajar en conjunto. Por ejemplo, un paquete elaborado en Cobol, o una hoja de cálculo, pueden ser diseñados para trabajar sólo con un determinado sistema operativo. Los paquetes individuales pueden ocasionar muchos problemas, ya que por ejemplo se puede tener un magnífico paquete de presupuestos que sea incompatible con el paquete de contabilidad. Si dos paquetes son diseñados en forma individual por dos diferentes compañías, es muy probable que no sean compatibles, lo cual puede repercutir en aumento de tiempo, costo y entrenamiento. Un software que es compatible e integrado permite que sus menús, apuntadores, comandos y ayudas sean iguales y que las salidas del sistema sean compatibles. El usar paquetes de software compatible, tiene grandes beneficios, aunque puede tener el inconveniente de que no todos los paquetes cumplan con los requerimientos de los usuarios.

Al desarrollar un determinado sistema se debe cuidar si habrá necesidad de adquirir sistemas o lenguajes propiedad de una compañía, que para su utilización se requiera de una licencia específica, lo cual puede ser muy costoso, o bien "casarnos" con un determinado proveedor, lo cual puede ser conveniente pero requiere de una evaluación muy detallada.

La elaboración o adquisición de sistemas debe evaluarse con mucho detalle, para lo cual se debe revisar desde la planeación y elaboración de los sistemas hasta su desarrollo e implementación. Se deberá evaluar si:

- Existen realmente sistemas entrelazados como un todo o bien si existen programas aislados.
- Existe un plan estratégico para la elaboración de los sistemas o bien si se están elaborando sin el adecuado señalamiento de prioridades y de objetivos.
- Los recursos son los adecuados y si se están utilizando en forma eficaz y eficiente.

El plan estratégico deberá establecer los servicios que se prestarán en un futuro, contestando preguntas como las siguientes:

- ¿Cuáles servicios se implementarán?
- ¿Cuándo se pondrán a disposición de los usuarios?
- ¿Qué características tendrán?
- ¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones y recursos que proporcionará la dirección de informática y la arquitectura en que estarán fundamentados:

- ¿Qué aplicaciones serán desarrolladas y cuándo?
- ¿Qué tipo de archivos se desarrollarán y cuándo?
- ¿Qué bases de datos serán desarrolladas y cuándo?
- ¿Qué lenguajes se utilizarán y en qué software?

- ¿Qué tecnología será utilizada y cuándo se implementará?
- ¿Cuántos recursos se requerirán aproximadamente?
- ¿Cuál es aproximadamente el monto de la inversión en hardware y software?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la organización:

- ¿Qué estudios van a ser realizados al respecto?
- ¿Qué metodología se utilizará para dichos estudios?
- ¿Quién administrará y realizará estos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos.

Por último, el plan estratégico determina la planeación de los recursos.

- ¿Contempla el plan estratégico las ventajas de la nueva tecnología?
- ¿Cuáles serán los conocimientos requeridos por los recursos humanos planeados?
- ¿Se contemplan en la estructura organizacional los nuevos niveles jerárquicos requeridos por el plan estratégico?
- ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

El proceso de planeación de sistemas deberá asegurarse de que todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos.

Estos recursos (hardware, software y comunicaciones) deberán ser compatibles con la estrategia de la arquitectura de la tecnología con que se cuenta actualmente.

Para identificar los problemas de los sistemas primero debemos detectar los síntomas, los cuales son un reflejo del área problemática; después de analizar los síntomas podremos definir y detectar las causas, parte medular de la auditoría.

Se deben reunir todos los síntomas y distinguirlos antes de señalar las causas, evitando tomar los síntomas como causas y dejando fuera todo lo que sean rumores sin fundamento.

Los sistemas deben ser evaluados de acuerdo con el ciclo de vida que normalmente siguen. Para ello, se recomiendan los siguientes pasos:

- Definición del problema y requerimientos del usuario. Examinar y evaluar los problemas y características del sistema actual, sea manual, mecánico o electrónico, así como los requerimientos por parte del usuario.
- Estudio de factibilidad:
 - Desarrollo de los objetivos y del modelo lógico del sistema propuesto.
 - Análisis preliminar de las diferentes alternativas, incluyendo el estudio de factibilidad técnico y económico de cada alternativa.

- Desarrollo de recomendaciones para el proyecto de sistema, incluyendo los tiempos y costos del proyecto.

C) Diseño general y análisis del sistema:

- Estudio detallado del sistema actual, incluyendo los procedimientos, diagramas de flujo, métodos de trabajo, organización y control.
- Desarrollo del modelo lógico del sistema actual.

D) Diseño del sistema:

- Desarrollo de los objetivos para el sistema propuesto.
- Desarrollo del modelo lógico del sistema propuesto, incluyendo la definición lógica de los procesos, diccionario lógico de datos y diseño lógico de las bases de datos.
- Evaluación de las diferentes opciones de diseño.
- Desarrollo del análisis costo-beneficio para evaluar las implicaciones económicas de cada alternativa.

E) Diseño detallado:

- Desarrollo de las especificaciones para el sistema físico, incluyendo el diseño de reportes, archivos, entradas, pantallas y formas.
- Diseño de las especificaciones del programa.
- Diseño de la implementación y el tiempo y forma de llevar a cabo las pruebas.

F) Implementación y desarrollo físico:

- Codificación y documentación del programa.
- Evaluación y selección del equipo de cómputo.
- Desarrollo de sistemas de auditoría, control y seguridad, y desarrollo de los procedimientos de prueba.
- Desarrollo de los programas de entrenamiento.

G) Pruebas del sistema, evaluación y aceptación por parte del usuario y de contraloría interna:

- Modificaciones y adecuaciones.
- Instalación.
- Carga de datos.

H) Soporte cotidiano, cambios y mejoras al sistema. Después de esto, se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el estudio de factibilidad.

También se debe evaluar que un error o corrección en el momento del diseño lógico es de fácil solución y bajo costo, pero que los errores o modificaciones

entre más adelantado esté el desarrollo del sistema son más costosos y de más difícil implementación. Hay ocasiones en que un sistema en su fase de implementación tiene tantas modificaciones, que es preferible hacer uno nuevo, en lugar de usar el diseñado con demasiadas modificaciones.

La primera etapa a evaluar en el sistema es el estudio de factibilidad, el cual debe analizar si el sistema es susceptible de realizarse, cuál es su relación beneficio-costos y si es conductualmente favorable.

Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como de los que estén en la fase de análisis para evaluar:

- La disponibilidad y características del equipo.
- Los sistemas operativos y los lenguajes disponibles.
- Las necesidades de los usuarios.
- Las formas de utilización de los sistemas.
- El costo y los beneficios que reportará el sistema.
- El efecto que producirá en quienes lo usarán.
- El efecto que éstos tendrán sobre el sistema.
- La congruencia de los diferentes sistemas.
- La congruencia entre los sistemas y la organización.
- Si están definidos los procesos administrativos, la normatividad y las políticas para la utilización de los sistemas.
- Su seguridad y confidencialidad.

En el caso de los sistemas que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados, y comparar con la realidad lo especificado en el estudio de factibilidad.

Por ejemplo, en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cuál fue su costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), el tiempo, el personal y la operación. En la práctica, debemos de considerar los costos directos, indirectos y de operación involucrados en un sistema, para poderlos comparar con los beneficios obtenidos.

Los beneficios que justifican el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema, una mayor exactitud, un mejor servicio, una mejoría en los procedimientos de control, una mayor confiabilidad y seguridad, una mejor comunicación y en forma más eficiente.

Entre los problemas más comunes en los sistemas están los siguientes:

- Falta de estándares en el desarrollo, en el análisis y en la programación.
- Falta de participación y de revisión por parte de la alta gerencia.
- Falta de participación de los usuarios.
- Inadecuada especificación del sistema al momento de hacer el diseño detallado.

- Deficiencia
- Nueva
- Inexper
- Diseño
- Proyec
- Control
- sobre el
- Problema
- mento c
- Inadecu
- Falta de
- gramas
- Docu
- Dificult
- docume
- ma.
- Problema
- Procedi

EVALU

En esta etapa
para llevar a
Se debe
cuatro fuentes

- La plane
- nados en
- prender
- ción, inc
- justificac
- Los requ
- El inven
- bios que
- Los requ

La situac

- Planeada
- En desar
- En proce
- En proce

- Deficiente análisis costo-beneficio.
- Nueva tecnología no usada o usada incorrectamente.
- Inexperiencia por parte del personal de análisis y del de programación.
- Diseño deficiente.
- Proyección pobre de la forma en que se realizará el sistema.
- Control débil o falta de control sobre las fases de elaboración del sistema y sobre el sistema en sí.
- Problemas de auditoría (poca participación de auditoría interna en el momento del diseño del sistema).
- Inadecuados procedimientos de seguridad, de recuperación y de archivos.
- Falta de integración de los sistemas (elaboración de sistemas aislados o programas que no están unidos como sistemas).
- Documentación inadecuada o inexistente.
- Dificultad de dar mantenimiento al sistema, principalmente por falta de documentación o por excesivos cambios y modificaciones hechos al sistema.
- Problemas en la conversión e implementación.
- Procedimientos incorrectos o no autorizados.

EVALUACIÓN DEL ANÁLISIS

En esta etapa se evaluarán las políticas, procedimientos y normas que se tienen para llevar a cabo el análisis.

Se deberá evaluar la planeación de las aplicaciones que pueden provenir de cuatro fuentes principales:

- La planeación estratégica: agrupando las aplicaciones en conjuntos relacionados entre sí y no como programas aislados. Las aplicaciones deben comprender todos los sistemas que puedan ser desarrollados en la organización, independientemente de los recursos que impliquen su desarrollo y justificación en el momento de la planeación.
- Los requerimientos de los usuarios.
- El inventario de sistemas en proceso al recopilar la información de los cambios que han sido solicitados, sin importar si se efectuaron o se registraron.
- Los requerimientos de la organización y de los usuarios.

La situación de una aplicación puede ser alguna de las siguientes:

- Planeada para ser desarrollada en el futuro.
- En desarrollo.
- En proceso, pero con modificaciones en desarrollo.
- En proceso con problemas detectados.

- En proceso sin problemas.
- En proceso esporádicamente.

NOTA: Se deberá documentar detalladamente la fuente que generó la necesidad de la aplicación. La primera parte será evaluar la forma en que se encuentran especificadas las políticas, los procedimientos y los estándares de análisis, si es que se cumplen y si son los adecuados para la organización.

Es importante revisar la situación en que se encuentran los manuales de análisis y ver si están acordes con las necesidades de la organización. En algunas ocasiones se tiene una microcomputadora con sistemas sumamente sencillos y se solicita que se lleve a cabo una serie de análisis que después hay que plasmar en documentos señalados en los estándares, lo cual hace que esta fase sea muy compleja y costosa. Los sistemas y su documentación deben estar acordes con las características y necesidades de una organización específica; no se deberá tener la misma documentación para un sistema que se va a usar en computadoras personales, el cual debe de ser documentado en forma más sencilla (el usuario no necesariamente debe de saber de computación) que un sistema en red. También deben de existir diferentes niveles de documentación (documentación para usuarios, para responsables de la información técnica).

Se debe evaluar la obtención de datos sobre la operación, el flujo, el nivel, la jerarquía de la información que se tendrá a través del sistema, así como sus límites e interfases con otros sistemas. Se han de comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la ejecución deseada corresponde al actual.

La auditoría en informática debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas (pantallas, las cuales deben tener una estructura "amigable") y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, las bases de datos, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuente a usarse.

Dentro del estudio de los sistemas en uso se deberá solicitar:

- Manual del usuario.
- Descripción de flujo de información.
- Descripción y distribución de información.
- Manual de formas.
- Manual de reportes.
- Lista de archivos y especificación.
- Definición de bases de datos.
- Definición de redes.

Con la información obtenida podremos dar respuesta a las siguientes preguntas:

- ¿Se está ejecutando en forma correcta y eficiente el proceso de información?
- ¿Puede ser simplificado para mejorar su aprovechamiento?

- ¿Se de
- ¿Se ti
- ¿Está
- ¿Se d
- ¿Los i
- ¿Las p

ANÁL

El mayor o
mientos e)
turado em
análisis de
error que
tras que e
pruebas de
sistemas d
que los err
los sistema
da o simpl
mientras q
sobre proc
decisiones
usando he

El diag
requerimie
gráfico del
sarrollar lo

Las mo
de informa
rias para lo
son descri
del nuevo

El diag
la base par
nuevo siste
tadora pri
computado
soporte est
tes de prog
sus caracte
comenzar e
involucra e
vos y los pr

- ¿Se debe tener una mayor interacción con otros sistemas?
- ¿Se tiene propuesto un adecuado control y seguridad sobre el sistema?
- ¿Está en el análisis la documentación adecuada?
- ¿Se debe usar otro tipo de técnicas o de dispositivos (redes, bases de datos)?
- ¿Los informes de salida son confiables y adecuados?
- ¿Las pantallas y el sistema son amigables?

ANÁLISIS Y DISEÑO ESTRUCTURADO

El mayor objetivo del análisis y diseño estructurado es determinar los requerimientos exactos, de tal forma que se diseñe el sistema correcto. El diseño estructurado emplea una serie de herramientas gráficas y técnicas que permiten el análisis de tal forma que sea posible conocer errores antes de que ocurran. Un error que ocurre durante la operación puede tener un costo de 30 a 90%, mientras que en la fase de aceptación puede tener un costo de 5 a 10%, en la fase de pruebas del diseño, de 4 a 7%, en la de codificación, de 5%, en la de diseño de sistemas de 3 a 6%, y en la de análisis de 1 a 4%, por lo cual es muy conveniente que los errores sean detectados y eliminados en las fases iniciales. En el caso de los sistemas tradicionales la información puede estar incompleta, no actualizada o simplemente imprecisa, y estos problemas pueden que no sean detectados, mientras que en la programación estructurada el analista recolecta información sobre procedimientos actuales, flujos de información, procesos de toma de decisiones y reportes, y así construye un modelo lógico de la situación actual, usando herramientas conocidas como diagramas lógicos de flujo de datos.

El diagrama de flujo es muy útil porque detecta los procesos lógicos, los requerimientos de información, el flujo de información, y provee un modelo gráfico del sistema actual, que puede ser utilizado para detectar mejoras y desarrollar los objetivos del nuevo sistema.

Las modificaciones mayores en los procedimientos actuales, necesidades de información y de los procesos de toma de decisiones, las cuales son necesarias para lograr los objetivos, son construidas dentro del nuevo modelo lógico y son descritas gráficamente dentro de la propuesta del diagrama lógico de flujo del nuevo sistema.

El diagrama lógico de flujo de datos del sistema propuesto se convierte en la base para desarrollar y evaluar las diferentes alternativas de diseño para el nuevo sistema. Las alternativas de diseño pueden incluir las bases para la computadora principal (*batch*), para el sistema en línea o distribuido, para las computadoras dedicadas o minicomputadoras, y para el rango de software que soporte estas configuraciones, incluyendo el desarrollo de software, los paquetes de programas, usando lenguajes de cuarta generación, las bases de datos y sus características. Una vez que son seleccionadas estas alternativas se puede comenzar el diseño detallado y la implementación del sistema. Este proceso involucra el diseño de las salidas y de las entradas, los requerimientos de archivos y los procedimientos de control.

**Diagrama
de flujo de datos**

EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA

En esta etapa se deberán analizar las especificaciones del sistema:

- ¿Qué deberá hacer?
- ¿Cómo lo deberá hacer?
- ¿Cuál es la justificación para que se haga de la manera señalada?
- ¿Cuál es la secuencia y ocurrencia de los datos?
- La definición del proceso.
- Los archivos y bases de datos utilizados.
- Las salidas y reportes.

Una vez que hemos analizado estas partes se deberá estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión.

Al tener el análisis del diseño lógico del sistema debemos compararlo con lo que realmente se está obteniendo: como en el caso de la administración, en la cual debemos evaluar lo planeado, cómo fue planeado y lo que realmente se está obteniendo (lo real).

PROGRAMAS DE DESARROLLO

Los programas de desarrollo incluyen software que sólo puede ser usado por el personal que ha tenido entrenamiento y experiencia; este software incluye:

A) Lenguajes de programación:

- Lenguaje de máquina.
- Ensambladores.
- De tercera generación.
- De cuarta generación:
 - 4GLS.
 - Query languages.
 - Generadores de reportes.
 - Lenguajes naturales.
 - Generadores de aplicaciones.

B) CASE (*computer aided software engineering*).

C) Programación orientada a objetos.

Al utilizar

- Interfases c...
- dables y vi...
- Enlace de...
- determina...
- procesador...
- un prograr...
- Capacidad...
- Capacidad...
- Licencias...
- múltiple, c...
- Transporte...
- Compatibl...
- Compatibl...
- Fácil de us...
- Grado de...
- Capacidad...
- De fácil in...
- Demanda...
- Requerimi...
- Costo.
- Seguridad

BASES

El banco de d...
temática indej

La cantida...
grande, del or

Se conside...
vos de datos...
están relacion...
cirse que una...
estructurado

El DBMS...
de datos) es u...
base de datos

El conjunt...
mación de

Al utilizar un determinado software se debe evaluar lo siguiente:

99

EVALUACIÓN DEL
DISEÑO LÓGICO
DEL SISTEMA

- Interfases de usuario gráfico, para poder diseñar pantallas y reportes agradables y visuales.
- Enlace de objetos en los sistemas de información. Esto nos permite unir determinados objetos dentro de un documento, por ejemplo, unir un procesador de palabra con una hoja de cálculo, o bien unir información de un programa o sistema a otro programa o sistema.
- Capacidad de trabajar en multiplataformas.
- Capacidad de trabajar en redes.
- Licencias. Verificar el tipo de licencia que se puede contratar (individual, múltiple, corporativa).
- Transportable.
- Compatible con otro software.
- Compatible con periféricos.
- Fácil de usar.
- Grado de sofisticación.
- Capacidad de utilización en red.
- De fácil instalación.
- Demanda de hardware.
- Requerimientos de memoria.
- Costo.
- Seguridad y confidencialidad.

BASES DE DATOS

El banco de datos es el conjunto de datos que guardan entre sí una coherencia temática independiente del medio de almacenamiento.

La cantidad de información que contiene un banco de datos suele ser muy grande, del orden de millones de datos.

Se considera que una base de datos es la organización sistemática de archivos de datos para facilitar su acceso, recuperación y actualización, los cuales están relacionados unos con otros y son tratados como una entidad. Puede decirse que una base de datos es un banco de datos organizado como un tipo estructurado de datos.

El DBMS (*data base management system* = sistema de administración de bases de datos) es un conjunto de programas que permite manejar cómodamente una base de datos, o sea:

El conjunto de facilidades y herramientas de actualización y recuperación de información de una base de datos.¹

Base de datos

¹ Antonio Vaquero y Luis Jopnes, *Informática: glosario de términos y siglas*, McGraw-Hill.

En las bases de datos se debe evaluar:

- La independencia de los datos. Muchos de los programas elaborados internamente eran dependientes de los archivos creados por ellos mismos, o sea que carecían de independencia. La falta de independencia significa que cada vez que un archivo es cambiado, todo programa que accesa a ese archivo debe ser cambiado.
- Redundancia de los datos. Se deben evitar las redundancias en las bases de datos.

Ejemplo

Si tuviésemos el nombre completo de los alumnos en cada una de las bases de datos en las que se accese, la cantidad de datos redundantes sería muy alta.

- Consistencia de los datos. El problema de redundancia en los datos no sólo provoca que se ocupe demasiado espacio en los discos, sino que también puede causar el problema de inconsistencia en los datos, ya que se puede cambiar en un archivo pero omitirse en algún otro de los archivos.

Un sistema de bases de datos es un conjunto de programas que:

- Almacena los datos en forma uniforme y de manera consistente.
- Organiza los datos en archivos en forma uniforme y consistente.
- Permite el acceso a la información en forma uniforme y consistente.
- Elimina la redundancia innecesaria en los archivos.

Los componentes a evaluar dentro de una base de datos son:

- Diccionario/directorio de datos.
- Lenguajes de datos (lenguajes de descripción de datos: DDL; lenguajes de manipulación de datos: DML).
- Monitoreo de teleproceso.
- Herramientas de desarrollo de aplicaciones.
- Software de seguridad.
- Sistemas de almacenamiento, respaldo y recuperación.
- Reportadores.
- *Query languages (structured query language: SQL; natural language queries, query by example: QBE).*
- Bases de datos de multiplataformas.
- *Web server software (world wide web: www).*

EL ADMINISTRADOR DE BASES DE DATOS

El desarrollo de las bases de datos ha creado la necesidad dentro de la organización de contar con un organismo encargado de administrar las bases de datos,

cuyas funciones son dar soporte a los

Dentro de la alta administración, los usuarios, los usuarios

Los modelos

- Jerárquicos.
- De redes.
- Relacionales.
- Orientados

Entre las ve

- Compartir
- Reducción
- Mejora de l
- Independen
- Incrementa
- Mejora el c
- Incrementa
- cia de la in

Problemas de administración

Cuando varios no fue diseñado no existe un control más usuarios por momento, y nosotros. Este tipo de computadoras actualizaciones

También por lo, lo cual se a de datos.

Problemas de control para que se debe definir el acceso a los datos del tario de la base

cuyas funciones son las de planear, diseñar, organizar, operar, entrenar, así como dar soporte a los usuarios, seguridad y mantenimiento.

Dentro de las funciones de este organismo están las de tener relaciones con la alta administración, los analistas de sistemas, los programadores de aplicaciones, los usuarios y los programadores de sistemas.

Los modelos de bases de datos pueden ser:

- Jerárquicos.
- De redes.
- Relacionales.
- Orientados a objetos.

Entre las ventajas del sistema de bases de datos se encuentran:

- Compartir datos.
- Reducción de redundancia de datos.
- Mejora de la consistencia de los datos.
- Independencia de datos.
- Incrementa la productividad del programador de aplicaciones y de usuarios.
- Mejora el control y la administración de los datos.
- Incrementa el énfasis de los datos como un recurso. Aumenta la importancia de la información como parte fundamental de la administración.

Problemas de los sistemas de administración de bases de datos

Cuando varios usuarios utilizan una base de datos, pueden existir problemas si no fue diseñada para usuarios múltiples. Uno de estos problemas surge cuando no existe un control sobre la actualización inmediata. Esto significa que dos o más usuarios pueden estar elaborando cambios al mismo archivo en el mismo momento, y no existe control sobre la actualización inmediata de los archivos. Este tipo de problemas existe principalmente en las bases de datos de computadoras personales, ya que los grandes sistemas tienen control sobre las actualizaciones inmediatas.

También pueden existir problemas en el uso de recursos excesivos de cómputo, lo cual se agrava si no se tiene un mantenimiento constante sobre las bases de datos.

Problemas de seguridad. Las bases de datos deben de tener suficiente control para que se asegure que sólo personal autorizado pueda acceder datos, y se debe definir el tipo de usuario que pueda adicionar, dar de baja, actualizar o acceder datos dependiendo de su llave de entrada, así como el usuario propietario de la base de datos.

COMUNICACIÓN

Se debe evaluar el modo de comunicación y el código empleado. Los diferentes modos de comunicación varían dependiendo del tipo de información que transmitimos y el costo del medio empleado.

El medio de comunicación es también un factor importante a evaluar, y éste dependerá de la velocidad y capacidad de transmisión, lo cual está directamente relacionado con el costo (cables trenzados, cable coaxial, fibra óptica, microondas, ondas de radio, infrarrojas).

Los componentes más comunes dentro de un sistema de comunicación son:

- Servidor y huésped.
- Terminal o estación de trabajo.
- Convertidores de protocolo.
- Módem.
- Equipo de conexión de terminales.
- Modo de comunicación.
- Medio de comunicación.
- Topología de las redes:
 - De punto a punto o estrella y topología jerárquica.
 - Mutidrop o bus y ring.
 - Mesh.
 - Sin cables (*wireless*).
- Tipo de redes:
 - Local.
 - Wide area networks (WAN).
 - Enterprise.
 - Internacional.

En general las redes pueden ser caras y pueden crear complicaciones en el sistema de información, pero pueden ser justificables por alguna o varias de las siguientes razones:

- Compartir periféricos.
- Compartir archivos.
- Compartir aplicaciones.
- Reducir costos de adquisición, instalación y mantenimiento de software.
- Conexión con otras redes.
- Captura de datos en lugares que son de información.
- Aumentar productividad.
- Permitir expansión.
- Disminuir tiempo de comunicación.
- Aumentar control.
- Seguridad.

- Los
- Con
 - "caí
 - ción
 - Tier
 - que
 - ocas
 -
 -
 -
 -
 - Cost
 - Cor
 - Segu
 - Los j
 - Entr
 - Salic
 - Proc
 - Espe
 - Espe
 - Méto
 - Ope
 - Man
 - tos).
 - Proc
 - Ident
 - Proc
 - Frec
 - Siste
 - Siste
 - Resp
 - la inf
 - Núm
 - Soft
 - Bases
 - En ca

INFO

Cuando s
mente en

Los puntos a revisar en las redes son:

- Confiabilidad de las redes. Un sistema con redes que estén constantemente "caídas", o que no sea confiable, provoca muchos problemas a la organización y cuestiona su funcionamiento.
- Tiempo de respuesta. Una red que sea lenta en sus operaciones, provoca que los usuarios la eviten o no la utilicen. Entre los problemas que puede ocasionar esta lentitud están:
 - La distancia que tiene que recorrer y la forma en que se transmite.
 - La cantidad de tráfico en la red.
 - La capacidad de los canales de comunicación.
 - Factores externos a la red, como puede ser la estructura de las bases de datos.
- Costo de la red.
- Compatibilidad con otras redes.
- Seguridad en las redes.

Los puntos a evaluar en el diseño lógico del sistema son:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulaciones de datos (antes y después del proceso electrónico de datos).
- Proceso lógico (necesario para producir informes).
- Identificación de archivos, tamaño de los campos y registros.
- Proceso en línea o lote y su justificación.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.
- Sistemas de control.
- Responsables (tipos de usuarios, identificando los usuarios propietarios de la información).
- Número de usuarios.
- Software necesario.
- Bases de datos requeridos.
- En caso de redes determinar su tipo y características.

INFORMES

Cuando se analiza un sistema de informática es muy común pensar exclusivamente en la parte relacionada con la informática, olvidándonos de que un siste-

ma comprende desde el momento en que se genera un dato, así como su procesamiento, retroalimentación y salida. Es muy común que solamente se evalúe el procesamiento de la información y su almacenamiento dejando fuera la evaluación de aquello que es el inicio del sistema, el seguimiento administrativo y la obtención de los reportes y salidas de información.

Lo que debemos determinar en el sistema es:

- En el procedimiento:
 - ¿Quién hace la función, cuándo y cómo?
 - ¿Qué formas se utilizan en el sistema?
 - ¿Son necesarias, se usan, están duplicadas?
 - ¿El número de copias es el adecuado?
 - ¿Existen puntos de control o faltan?
- En la gráfica de flujo de información:
 - ¿Es fácil de usar?
 - ¿Es lógica?
 - ¿Se encontraron lagunas?
 - ¿Hay faltas de control?
- En las formas de diseño:
 - ¿Cómo está usada la forma en el sistema?
 - ¿Qué tan bien se ajusta la forma al procedimiento?
 - ¿Cuál es el propósito, por qué se usa?
 - ¿Se usa y es necesaria?
 - ¿El número de copias es el adecuado?
 - ¿Quién lo usa?

Entre los elementos a revisar en el diseño de formas están:

Numeración. ¿Está numerada la forma? ¿Es necesaria su numeración? ¿Está situada en un solo lugar fácil de encontrar? ¿Cómo se controlan las hojas numeradas y su utilización?

Título. ¿Da el título de la forma una idea clara sobre su función básica?

Espacio. Si la forma va ser mecanografiada, ¿hay suficiente espacio para escribir a máquina rápidamente, con exactitud y eficiencia? Si la forma se llenará a mano, ¿hay el espacio adecuado para que se escriba en forma legible?

Tabulación. Si la forma va ser mecanografiada, ¿permite su tabulación llenarla uniformemente? ¿Es la tabulación la mínima posible? Una excesiva tabulación disminuye la velocidad y eficiencia para llenarla. Además le da una apariencia desigual y confusa.

Zonas. ¿Están juntos los datos relacionados entre sí? Si los datos similares están agrupados por zonas, todas las personas que usan la forma ahorran tiempo. La

informa
grafía r
verifica
situada

Rayado
uso cor

Instruc
autoins
que el p
De no s
para ve
excesiv
sión y l

Firmas.
dament
como u
firmanc

Nombr
duo en
rotación

Encabe
qué firm

Rótulos
adecuac
ubicación

Ubicaci
donde s
nógrafa
para esc

Casiller
cación r
cesivos?

Tipo de
Use pap
un man
para rec

Tamaño
ajusta a
jo, tiemp

información similar reunida por zonas hace más fácil su referencia, se mecanografía más eficientemente y se revisa con más rapidez. Posteriormente, se debe verificar que las zonas de las formas que sean utilizadas para captura estén situadas de manera congruente con el diseño de las pantallas de captura.

Rayado. ¿Da la forma una apariencia desordenada y difícil de entender por el uso confuso y excesivo de líneas delgadas, gruesas o de doble raya?

Instrucciones. ¿Se le dice al usuario cómo debe llenar la forma? Formas autoinstruccionales o que suministran la información de cómo llenarlas permiten que el personal nuevo y los otros trabajen con supervisión y errores mínimos. De no ser así, existe un manual de llenado de formas, el cual se debe revisar para ver si las instrucciones son claras, si son congruentes con la forma y si son excesivas, ya que un diseño excesivo de instrucciones puede provocar confusión y hacer que éstas sean poco claras.

Firmas. ¿Existe suficiente espacio para una firma legible? ¿Está el espacio debidamente identificado respecto a la firma que se solicita? ¿La firma se utiliza como un mero trámite o realmente controla la persona que firma lo que se está firmando?

Nombres. ¿Se usan los nombres de los puestos en lugar del nombre del individuo en la forma? No es conveniente imprimir nombres de personas debido a la rotación de personal.

Encabezados ambiguos. ¿Se indica con exactitud qué fechas, qué números o qué firmas se requieren? Se deben evitar encabezados dudosos o ambiguos.

Rótulos. ¿Son demasiados llamativos? ¿Son demasiado discretos? ¿Existe un adecuado contraste entre los rótulos y los textos respecto a su tamaño, color y ubicación, para que los datos solicitados sean identificados fácilmente?

Ubicación de los rótulos. ¿Están los rótulos o encabezados debajo de la línea en donde se debe mecanografiar? Esto causa pérdida de tiempo, porque la mecanógrafa tiene que mover el carro para ver el rótulo y acomodarlo nuevamente para escribir la información deseada.

Casilleros. ¿Se usan pequeños espacios enmarcados () para con una sola indicación reducir escritos largos o repetitivos? ¿Los espacios son suficientes o excesivos?

Tipo de papel. ¿Son el peso y calidad del papel apropiados para esa forma? Use papel más pesado y de mejor calidad para aquellas formas que requieren un manejo excesivo. Use papel de menor peso con formas que se usen poco, para reducir costo y espacio en los archivos.

Tamaños estándar. ¿Tiene la forma un tamaño estándar? El tamaño estándar se ajusta a sobres y archivos estándar. Además reduce existencias de papel, manejo, tiempo y costo de impresión. Se debe considerar que el costo del papel que

Figura 4.1. Descripción de informes

FECHA

SISTEMA

NOMBRE DEL INFORME

PROPÓSITO

CLAVE

QUIÉN LO FORMULA

PERIODICIDAD

VOLUMEN EN HOJAS

EN VIGOR

FECHA EN QUE DEBE PRESENTARSE

DESDE

OPORTUNIDAD CONFIABILIDAD COMPLETO

NÚM. COPIAS

COPIA	USUARIO	USO
ORIGINAL		
1a.		
2a.		
3a.		
4a.		

NÚM.	DESCRIPCIÓN DEL PROCEDIMIENTO

*ANEXAR COPIA FOTOSTÁTICA DEL INFORME Y DEL DIAGRAMA DE FLUJO.

ANALIZÓ

PÁG. DE

FUNCIÓN

NOMBRE DEL INFORME _____

PROPÓSITO DEL INFORME _____

QUIÉN LO FORMULA _____

QUÉ LO ORIGINA _____

VOLUMEN DE HOJAS O REGISTROS _____

FORMA DE HACERLO _____

PRINCIPAL USUARIO _____

FECHA TEÓRICA DE PRESENTACIÓN _____ PERIODICIDAD _____

FECHA DE PRESENTACIÓN _____ PERIODICIDAD _____

NIVEL DE INFORMACIÓN _____

EN VIGOR DESDE _____

MODIFICACIONES _____

OTROS DATOS _____

[illegible][illegible]

FECHA	RECOPILO	REVISÓ	ÍNDICE
			PÁGINA DE

Figura 4.3. Evaluación de formas				
NOMBRE DE LA FORMA.		FRECUENCIA DE USO		
ELABORADO POR		NÚM. DE FORMA	NÚM. DE COPIAS	
USUARIOS		CANT. IMPRESA	CANT. INV.	
		PERIODO ESTIMADO DE USO		
OBSERVACIONES				
FACTORES A EVALUAR				
INFORMACIÓN EMPRESA		IMAGEN		
TERMINOLOGIA ESTÁNDAR	SÍ NO	PROFESIONAL Y CORRECTA	SÍ NO	
EXISTE MANUAL DE OPERACIÓN	SÍ NO	CALIDAD APROPIADA DE PAPEL	SÍ NO	
AUTODESCRIPTIVA	SÍ NO	BUENA CALIDAD DE IMPRESIÓN	SÍ NO	
FUENTE DE INFORMACIÓN DEBIDAMENTE IDENTIFICADA	SÍ NO	COSTO		
REQUIERE OTROS DATOS DE REFERENCIA	SÍ NO	MÁXIMO APROVECHAMIENTO DE PAPEL	SÍ NO	
TIENE SUFICIENTES ESPACIOS	SÍ NO	MÁXIMO APROVECHAMIENTO DE IMPRESIÓN	SÍ NO	
DATOS QUE CONTIENE		CUMPLE CON LAS NECESIDADES	SÍ NO	
NECESITA DATOS ADICIONALES	SÍ NO	DUPLICA DATOS DE OTRAS FORMAS	SÍ NO	
TIENE DATOS INNECESARIOS	SÍ NO			
EN CASO DE HABER CONTESTADO "NO" A ALGUNA PREGUNTA, ANOTE LAS OBSERVACIONES.				

EN CASO D

Figura 4.5. Evaluación de formas

A. ¿CONOCE LA PERSONA QUE FORMULA EL DOCUMENTO, EL OBJETIVO Y LA IMPORTANCIA DEL MISMO? Sí _____ NO _____

B. ¿QUÉ OPINIÓN TIENE EL EMPLEADO DEL MANEJO DE ESTE DOCUMENTO?

C. ¿QUÉ PROBLEMAS EXISTEN EN SU ELABORACIÓN?

D. ¿EXISTE RETRASO EN SU FORMULACIÓN? Sí _____ NO _____

MOTIVO _____

E. SE USA LA FORMA NO PARCIAL- EN FORMA EN FORMA
 MENTE INCORRECTA CORRECTA

¿EL USO QUE SE DA A LA FORMA EN LOS DIFERENTES LUGARES ES EL ADECUADO? Sí _____ NO _____

¿EN QUÉ CASO Y POR QUÉ? _____

F. ¿CONSIDERA QUE SE PUEDEN HACER CAMBIOS A LA FORMA PARA SIMPLIFICAR TRABAJO Y PROCEDIMIENTO? Sí _____ NO _____

¿CUÁLES SON, POR QUÉ Y CUÁLES SERÍAN LOS BENEFICIOS?

G. OPINIÓN GENERAL

FECHA _____

AUDITOR _____

SI

FORMA _____

ELABORAD

AUTORIZA

FUENTE

OBJETIVO

DESTINO

ORDEN

ORIGINAL

1a. COPIA

2a. COPIA

3a. COPIA

4a. COPIA

5a. COPIA

6a. COPIA

7a. COPIA

Figura 4.6. Descripción de formas

SISTEMA _____

FORMA _____

ELABORADA: NOMBRE _____

PUESTO _____

AUTORIZADA: NOMBRE _____

FUENTE DE INFORMACIÓN

OBJETIVO

DESTINO

ORDEN	DESTINO	USO
ORIGINAL		
1a. COPIA		
2a. COPIA		
3a. COPIA		
4a. COPIA		
5a. COPIA		
6a. COPIA		
7a. COPIA		

Figura 4.7. Descripción de formas de papelería

<div style="display: flex; justify-content: space-between; margin: 0;"> <div style="border: 1px solid black; padding: 2px 10px;">SISTEMA</div> <div style="border: 1px solid black; padding: 2px 10px;">FECHA</div> </div>			
NOMBRE _____			
OBJETIVO _____		FRECUENCIA _____	
QUIÉN FORMULA _____		VOLUMEN MENSUAL _____	
FORMA DE LLENARLA _____		EN VIGOR DESDE _____	
FOLIO IMPRESO	SÍ NO	NÚM. DE COPIAS _____	
QUÉ LA ORIGINA _____ _____			
A QUÉ DA ORIGEN _____ _____			
RECOMENDACIONES AL IMPRIMIR _____			

COPIA NÚM.	COLOR	PROCEDIMIENTO, USO Y DESTINO DE CADA COPIA	FIRMA NECESARIA
ORIGINAL			

OBSERVACIONES	
ANALIZÓ	PÁGINA DE

no es de
estándar.

Color. ¿Pe
mas en col
ros, son dif
sión (negro
cuidado tan
estar identi

Como
descripción

ANÁL

Una vez q
informes p
la encuesta
se la figura
cribir el cor
ción.

RUIDO

En la audito
que tiene ca
En prim

La trans
prenda.²

El ruido
solamente lo
Koontz/O'D

Cualquier
za la con

² Koontz y

no es de tamaño estándar es considerablemente mayor que el de tamaño estándar.

Color. ¿Permite el contraste del color del papel una lectura eficiente? Las formas en colores, como el anaranjado, el verde, el azul, el gris, etc., en tonos oscuros, son difíciles de leer porque no ofrecen suficiente contraste entre la impresión (negro) y el papel. Ciertos colores brillantes cansan la vista. Se debe tener cuidado tanto en el color del papel como en el color de la tinta. Las copias deben estar identificadas de acuerdo con el color.

Como ejemplo de análisis de formas véase las figuras 4.3, 4.4 y 4.5; para la descripción de formas véase las figuras 4.6 y 4.7.

ANÁLISIS DE INFORMES

Una vez que se han estudiado los formatos de entrada debemos analizar los informes para posteriormente evaluarlos con la información proporcionada por la encuesta a los usuarios. Como ejemplo de la descripción de los informes véase la figura 4.1, y para el análisis de los informes la figura 4.2. Después de describir el contenido de los informes se debe tener el análisis de datos e información.

RUIDO, REDUNDANCIA, ENTROPÍA

En la auditoría de sistemas hay que estudiar la redundancia, el ruido y la entropía que tiene cada uno de los sistemas.

En primer lugar, debemos considerar como comunicación:

La transferencia de información del emisor al receptor de manera que éste la comprenda.²

El ruido es todo aquello que interfiere en una adecuada comunicación; no solamente los sonidos sino todo aquello que impida la adecuada comunicación. Koontz/O'Donnel definen el ruido como:

Cualquier cosa (sea en el emisor, en la transmisión o en el receptor) que obstaculiza la comunicación.

² Koontz y O'Donnel, *Administración*, McGraw-Hill.

Así, por ejemplo, si una persona se encuentra jugando, sin hacer necesariamente algún sonido, en el momento que otra esté hablando, se considera como tipo de ruido para el sistema.

En el caso de un sistema computarizado, el error en una captura, una pantalla de la terminal demasiado llena de información y poco entendible o un reporte inadecuado se deben considerar como ruido en el sistema, ya que impiden una buena comunicación de la información. En el caso de los sistemas se debe evaluar lo que se conoce como "sistema amigable", lo cual significa:

- Que tenga las ayudas necesarias para el caso de alguna duda (*help*).
- Que contenga los catálogos necesarios para el caso de referencias.
- Que tenga las ligas automáticas con otros sistemas para obtener información o para consulta (conexiones automáticas a otras bases de datos o redes).
- Que la información sea solicitada en forma secuencial y lógica.
- Que sea de fácil lectura y, en su caso, escritura.
- Que sea rápido, ágil, y que contenga una limpieza que permita una fácil visualización.

La redundancia es toda aquella duplicidad que tiene el sistema con la finalidad de que, en caso de que exista ruido, permita que la información llegue al receptor en forma adecuada.

Podemos enviar un mensaje de la forma siguiente:

Ejemplo

Llegó por avión el día martes 31 de octubre de 2000 del presente año, a las 16:00 hrs. de la tarde a la ciudad de Cancún, Quintana Roo, México.

En el mensaje anterior tenemos excesiva redundancia debido a que el 31 de octubre de 2000 es martes y si estamos en 2000 es del presente año. Las 16:00 hrs. siempre serán de la tarde y la ciudad de Cancún está sólo en el estado de Quintana Roo, México. En cambio puede ser incompleta, ya que no se especifica la línea aérea ni el vuelo en que llegará.

Función de la redundancia

La redundancia puede ser conveniente en el caso de que haya que cerciorarse de que la información se recibe correctamente. Esto estará en función de lo delicada que sea la información y del riesgo que se corre en caso de una pérdida total o parcial de la misma.

Un ejemplo de redundancia dentro de las máquinas es el BIT de paridad, el cual permite que en caso de pérdida de un BIT, se pueda recuperar la información que contiene el byte.

La redundancia es una forma de control que permite que, aunque exista ruido, la comunicación pueda llevarse a cabo en forma eficiente; deberá haber mayor redundancia entre más arriesgada, costosa o peligrosa sea la pérdida de información, aunque, a la vez, debemos estar conscientes de que el exceso de redundancia puede provocar ruido.

Ejemplo

Es el caso de un profesor que por desear ser muy claro, se dedica a dar demasiados ejemplos; puede provocar ruido en el sentido que llega a confundir o a aburrir a sus alumnos y que el número excesivo de ejemplos impida una adecuada comunicación.

En l
ro adecu
mita una
redunda
Tam
incremen
de contr
bien que
requiere

Entropía

El diccion

Canti

La er
el cual es
del sisten

En la
entra

En un
entropía,
nera que
otro syster

Al cap
de info

EVAL

En esta et
guaje utili
hardware

Al eva
debe propi
eficaz y op
obtener un
se contará

³ Nuevo a

En la auditoría se debe considerar que todo sistema ha de ofrecer un número adecuado de redundancia, según su nivel de importancia, de modo que permita una buena comunicación, aun en el caso de que exista ruido, pero sin ser la redundancia de tal magnitud que a su vez provoque ruido.

También debemos considerar que con un mayor control y redundancia se incrementa también el costo de los sistemas. Hay que tener un adecuado nivel de control y redundancia, que no sea de tal magnitud que provoque ruido o bien que no sea demasiado costoso en relación con el nivel de seguridad que requiere el sistema.

Entropía

El diccionario la define como:

Cantidad de energía que por su degradación no puede aprovecharse.³

La entropía en un sistema, por ejemplo de un motor, es el calor que genera, el cual es energía que por sus características no puede aprovecharse. En el caso del sistema llamado motor se utiliza esta entropía.

En la calefacción del automóvil o bien para calentar el aire y la gasolina que entra al motor (en el caso de motores turbo).

En un sistema computarizado debemos procurar reducir al máximo esta entropía, y una de las formas de reducirla es interconectar sistemas, de tal manera que esa cantidad de energía no usada en un sistema pueda ser utilizada en otro sistema.

Al capturar el catálogo de clientes para el sistema de cobranzas, con un poco de información adicional lo podemos utilizar en contabilidad.

Ejemplo**Ejemplo**

EVALUACIÓN DEL DESARROLLO DEL SISTEMA

En esta etapa del sistema se deberán auditar los programas, su diseño, el lenguaje utilizado, la interconexión entre los programas y las características del hardware empleado (total o parcial) para el desarrollo del sistema.

Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, así como para reducir la duplicidad de datos y de reportes, y obtener una mayor seguridad en la forma más económica posible. De ese modo se contará con los mejores elementos para una adecuada toma de decisiones.

³ Nuevo diccionario español ilustrado Sopena.

SISTEMAS DISTRIBUIDOS, INTERNET, COMUNICACIÓN ENTRE OFICINAS

Los sistemas distribuidos se pueden definir como el sistema en el cual las computadoras y los datos están en más de un lugar (*site*), así como los programas de aplicación. Ejemplos de esto son las redes WAN, PBX, LAN, Internet.

Las razones para implementar un sistema distribuido son:

- Mejora del tiempo de respuesta.
- Reducción de costos.
- Mejora de exactitud en la actualización.
- Reducción del costo de la computadora principal (*mainframe*) y la dependencia a una sola computadora.
- Puede tenerse un crecimiento planeado. En lugar de grandes equipos que dificultan su administración, organización, y que requieren de espacios muy amplios, se tienen equipos descentralizados que son más fáciles de administrar y de controlar su crecimiento.
- Incremento de confianza, ya que si falla el equipo principal no significa que falle todo el sistema.
- Compartir recursos.
- Aumenta la satisfacción de los usuarios, ya que las computadoras y el desarrollo pueden estar más cerca del usuario.
- En bases de datos se puede usar el concepto cliente/servidor y *Structured Query Language* (SQL).

Los puntos que se deben considerar al evaluar un sistema distribuido son:

- Falta de personal calificado en todos los puntos del sistema.
- Estandarización.
- Documentación.
- Pérdida de datos.
- Seguridad.
- Consistencia de los datos.
- Mantenimiento del sistema.

Al tener un proceso distribuido es preciso considerar la seguridad del movimiento de la información entre nodos. El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, recordando que el plan de aplicaciones proporciona información de la ubicación planeada de las terminales, los tipos de mensajes requeridos, el tráfico esperado en las líneas de comunicación y otros factores que afectan el diseño.

Es importante considerar las variables que afectan a un sistema: ubicación en los niveles de la organización, tamaño y recursos que utiliza.

Las características que deben evaluarse en los sistemas son:

- Dinámicos (susceptibles de modificarse).

• Tran
rent
• Estr
actu
• Inte
lació
• Acco
• Neco
• Com
• Opo
• Func
• Está
nive
• Mod
• Jerár
• Segu
• Únic

En r
ma que p
aislados.
Se de
ésta no s

CON

Debido a
frecuente
una perso
ridades e
de inform
de una ac
la técnica

¿Qué
del presu
del mismo
mente o p
porque ex
esta cuali
porcionar

Para p
el analista
el cual se
plan debe
para evalu

- Transportables (que puedan ser usados en diferentes máquinas y en diferentes plataformas).
- Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo).
- Integrados (un solo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
- Accesibles (que estén disponibles).
- Necesarios (que se pruebe su utilización).
- Comprensibles (que contengan todos los atributos).
- Oportunos (que esté la información en el momento que se requiere).
- Funcionales (que proporcionen la información adecuada a cada nivel).
- Estándar (que la información tenga la misma interpretación en los distintos niveles).
- Modulares (facilidad para ser expandidos o reducidos).
- Jerárquicos (por niveles funcionales).
- Seguros (que sólo las personas autorizadas tengan acceso).
- Únicos (que no dupliquen información).

En relación con otros sistemas deben de estar interconectados de tal forma que permitan un sistema integral, y no una serie de programas o sistemas aislados.

Se deben de tener sistemas que tengan la necesaria redundancia, pero que ésta no sea tan grande que provoque que el sistema sea lento o ineficiente.

CONTROL DE PROYECTOS

Debido a las características propias del análisis y de la programación es muy frecuente que la implantación de los sistemas se retrase, y llega a suceder que una persona trabaje varios años en un sistema o bien que se presenten irregularidades en las que los programadores realizan actividades ajenas a la dirección de informática. Para poder controlar el avance de los sistemas, ya que se trata de una actividad intelectual de difícil evaluación, se recomienda que se utilice la técnica de administración por proyectos para su adecuado control.

¿Qué significa que un sistema sea liberado en el plazo establecido y dentro del presupuesto? Pues sencillamente que el grado de control en el desarrollo del mismo es el adecuado o tal vez el óptimo. Pero esto no se consigue gratuitamente o porque la experiencia o calidad del personal de desarrollo sea alta, sino porque existe un grado de control durante su desarrollo que permite obtener esta cualidad. Cabe preguntar aquí: ¿quién es el elemento adecuado para proporcionar este grado de control?

Para poder tener una buena administración por proyectos se requiere que el analista o el programador y su jefe inmediato elaboren un plan de trabajo en el cual se especifiquen actividades, metas, personal participante y tiempos. Este plan debe ser revisado periódicamente (semanal, mensual o bimestralmente) para evaluar el avance respecto a lo programado.

La estructura estándar de la planeación de proyectos deberá incluir la facilidad de asignar fechas predefinidas de terminación de cada tarea. Entre estas fechas debe estar el calendario de reuniones de revisión, las cuales tendrán diferentes niveles de detalle. Son necesarias las reuniones a nivel técnico con la participación del personal especializado de la dirección de informática, para definir la factibilidad de la solución y los resultados planeados. Son muy importantes las reuniones con los usuarios finales, para verificar la validez de los resultados esperados.

La evaluación de proyectos y su control puede realizarse de acuerdo con diferentes autores. A manera de ejemplo presentamos el siguiente cuestionario:

1. ¿Existe una lista de proyectos de sistema de procesamiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?
2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?
3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?
4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?

- Poner la lista de proyectos a corto y a largo plazos.
- Poner una lista de sistemas en proceso de periodicidad y de usuarios.

5. ¿Quién autoriza los proyectos?
6. ¿Cómo se asignan los recursos?
7. ¿Cómo se estiman los tiempos de duración?
8. ¿Quién interviene en la planeación de los proyectos?
9. ¿Cómo se calcula el presupuesto del proyecto?
10. ¿Qué técnicas se usan en el control de los proyectos?
11. ¿Quién asigna las prioridades?
12. ¿Cómo se asignan las prioridades?
13. ¿Cómo se controla el avance del proyecto?
14. ¿Con qué periodicidad se revisa el reporte de avance del proyecto?
15. ¿Cómo se estima el rendimiento del personal?
16. ¿Con qué frecuencia se estiman los costos del proyecto para compararlo con lo presupuestado?
17. ¿Qué acciones correctivas se toman en caso de desviaciones?
18. ¿Qué pasos y técnicas se siguen en la planeación y control de los proyectos? Enumérelas secuencialmente.

- () Determinación de los objetivos.
- () Señalamiento de las políticas.
- () Designación del funcionario responsable del proyecto.
- () Integración del grupo de trabajo.
- () Integración de un comité de decisiones.
- () Desarrollo de la investigación.
- () Documentación de la investigación.
- () Factibilidad de los sistemas.
- () Análisis y valuación de propuestas.
- () Selección de equipos.

19. ¿Se lle
aún cu

De análisis
De programa
Observacion

Incluir el p
que el departa
cia, según la si

Como ejer
calendario de
sables del siste
figura 4.12; de
los informes d
avance de pro

Se deberán
tran en proces
cumple con su

CONTR Y PROGR

El objetivo de
cificaciones fu
para su mane

Las revisi
gramación, y

Etapas de análisis
objetivo del s
las especifica

Etapas de estudio
rollando el m
incluyendo el

Etapas de desarrollo
lógico; evalua
omisiones, an
que el costo
que se detecta
el costo que s
nar la descrip
vista del usua
lógica de cad

19. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos para los cuales fueron diseñados?

De análisis	sí ()	NO ()
De programación	sí ()	NO ()
Observaciones		

Incluir el plazo estimado de acuerdo con los proyectos que se tienen para que el departamento de informática satisfaga las necesidades de la dependencia, según la situación actual.

Como ejemplo de formato de control de proyectos véase la figura 4.8; del calendario de actividades véase las figuras 4.9 y 4.10; del reporte de los responsables del sistema, véase la figura 4.11; del control de programadores, véase la figura 4.12; de planeación de la programación, véase las figuras 4.13 y 4.14; de los informes de avance de la programación, véase la figura 4.15; de control de avance de programación véase figuras 4.16 y 4.17.

Se deberán revisar tanto los proyectos terminados como los que se encuentran en proceso, para verificar si se ha cumplido con el plan de trabajo o si cumple con su función de medio de control.

CONTROL DE DISEÑO DE SISTEMAS Y PROGRAMACIÓN

El objetivo de esto es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación.

Las revisiones se efectúan en forma paralela, desde el análisis hasta la programación, y sus objetivos son los siguientes:

Etapas de análisis y definición del problema. Identificar con claridad cuál es el objetivo del sistema, eliminando inexactitudes, ambigüedades y omisiones en las especificaciones.

Etapas de estudio de factibilidad. Elaborar el costo/beneficio del sistema, desarrollando el modelo lógico, hasta llegar a la decisión de elaborarlo o rechazarlo, incluyendo el estudio de factibilidad técnico y las recomendaciones.

Etapas de diseño. Desarrollar los objetivos del sistema; desarrollar el modelo lógico; evaluar diferentes opciones de diseño, y descubrir errores, debilidades, omisiones, antes de iniciar la codificación. Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento en que se detectan: si se descubren en el momento de programación será más alto el costo que si se detectan en la etapa de análisis. El análisis deberá proporcionar la descripción del funcionamiento del sistema funcional desde el punto de vista del usuario, indicando todas las interacciones del sistema, la descripción lógica de cada dato, las estructuras que éstos forman, el flujo de información

COORDINADOR _____ FECHA _____

(anotar en la primera línea las fechas estimadas y en la segunda las reales)

[illegible][illegible]

Figura 4.9. Calendario de actividades

ANÁLISIS Y PROGRAMACIÓN

RESPONSABLE
APLICACIÓN

FECHA _____

HOJA DE

[illegible]

Figura 4.10. Control de actividades del programador

SISTEMA _____

PROGRAMA _____ IDENTIF. _____

PROGRAMADOR _____

ACTIVIDAD	PLANEADO			REAL			DIF.
	INICIO	TÉRMINO	DIF.	INICIO	TÉRMINO	DIF.	
1. ANÁLISIS							
2. DIAGRAMA LÓGICO							
3. CREAC. DE PRUEBAS							
4. PRUEB. ESCRITORIO							
5. CODIFICACIÓN							
6. CAPTURA							
7. COMPILACIÓN							
8. GENER. PRUEBAS							
9. DEPURACIÓN							
10. PRUEBAS							
11. VERIF. PRUEBAS							
12. CORRECCIONES							
13. DOCUMENTACIÓN							
FINAL							

ESPECIFICAR EL NÚMERO
DE COMPILACIONES REALIZADAS _____

PRUEBAS REALIZADAS _____

OBSERVACIONES

DIF.

DIF.

DIF.

DIF.

Figura 4.12. Control de programadores

[illegible][illegible]

Figura 4.13. Planeación de programación

[illegible]

Figura 4.14. Hoja de planeación de actividades

[illegible]

U.	REAL
----	------

[illegible]

Figura 4.16. Control de avance de programación

SISTEMA _____ FECHA _____

PROGRAMADOR _____

[illegible]

OBSERVACIONES _____

- 1000 05

HOJA DE

Figura

SISTEMA

PROGRAMA

PROGRAM

CLAVE
ACTI-
VIDAD

HOJA DE

[illegible]

que tiene lugar en el sistema. Asimismo, se indicará lo que el sistema tomará como entradas, los procesos que serán realizados, las salidas que deberá proporcionar, los controles que se efectuarán para cada variable y los procedimientos.

Etapas de programación. Buscar la claridad, modalidad y verificar con base en las especificaciones.

Etapas de implementación y pruebas del sistema. Desarrollar la implementación del sistema con datos de prueba y la carga de datos definitivos, evaluando el sistema, su seguridad y confidencialidad y dando entrenamiento a los usuarios. Las pruebas del sistema tratan de garantizar que se cumplan los requisitos de las especificaciones funcionales, verificando datos estadísticos, transacciones, reportes, archivos, anotando las fallas que pudieran ocurrir y realizando los ajustes necesarios. Los niveles de prueba pueden ser agrupados en módulos, programas y sistema total.

Esta función tiene una gran importancia en el ciclo de evaluación de aplicaciones de los sistemas de información y busca comprobar que la aplicación cumple las especificaciones del usuario, que se haya desarrollado dentro de lo presupuestado, que tenga los controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados.

Un cambio hecho a un sistema existente, como la creación de uno nuevo, presupone necesariamente cambios en la forma de obtener la información y un costo adicional. Ambos deberán ser evaluados.

Se debe evaluar el cambio (si lo hay) de la forma en que se ejecutan las operaciones; se debe comprobar si mejora la exactitud de la información generada, si la obtención de los reportes efectivamente reduce el tiempo de entrega o si es más completa. Se debe determinar cuánto afecta las actividades del personal usuario o si aumenta o disminuye el personal de la organización, así como los cambios entre las interacciones entre los miembros de la organización. Todo ello, a fin de saber si aumenta o disminuye el esfuerzo realizado y su relación costo/beneficio para generar la información destinada a la toma de decisiones, con objeto de estar en condiciones de determinar la productividad y calidad del sistema.

Como ejemplo de cuestionario para la evaluación del diseño y prueba de los sistemas presentamos el siguiente:

1. ¿Quiénes intervienen al diseñar un sistema?

- Usuario.
- Analista.
- Gerente de departamento.
- Administradores de bases de datos.
- Personal de comunicaciones y redes.
- Auditores internos.
- Asesores.
- Otros.

2. ¿Qué lenguaje o lenguajes conocen los analistas?

3. ¿Cuántos analistas hay y qué experiencia tienen?

4. ¿Cómo se controla el trabajo de los analistas?

5. Indique qué pasos se siguen en el desarrollo de un sistema:

- | | |
|--|-----|
| • Definición del problema | () |
| • Desarrollo de objetivos del sistema | () |
| • Estudio de factibilidad | () |
| • Estudio costo/beneficio | () |
| • Estudio de factibilidad técnico | () |
| • Definición de tiempos y costo del proyecto | () |
| • Desarrollo del modelo lógico | () |
| • Propuesta de diferentes alternativas | () |
| • Especificaciones para el sistema físico | () |
| • Especificaciones de programas | () |
| • Diseño de implementación | () |
| • Diseño de carga de datos | () |
| • Codificación | () |
| • Programa de entrenamiento | () |
| • Estudio de la definición | () |
| • Discusión con el usuario | () |
| • Elaborar datos de prueba | () |
| • Revisión de resultados | () |
| • Documentación | () |
| • Someter resultados de prueba | () |

6. ¿Qué documentación acompaña al programa cuando se entrega?

Es muy frecuente que no se libere un sistema, esto es, que alguien continúe dándole mantenimiento y que sea el único que lo conozca. Ello puede deberse a amistad con el usuario, falta de documentación, mal análisis preliminar del sistema, resistencia a cambiar a otro proyecto, o bien a una situación que es muy grave dentro del área de informática: la aplicación de "indispensables", que son los únicos que tienen la información y, por lo tanto, son inamovibles.

¿Qué sucede respecto al mantenimiento o modificación de un sistema cuando éste no ha sido bien desarrollado (analizado, diseñado, programado, probado) e instalado? La respuesta es sencilla: necesitará cambios frecuentes por omisiones o nuevos requerimientos.

En el caso de sistemas, muchas organizaciones están gastando cerca de 80% de sus recursos de cómputo en mantenimiento.

El mantenimiento excesivo es consecuencia de falta de planeación y control del desarrollo de sistemas; la planeación debe contemplar los recursos disponibles y técnicos apropiados para el desarrollo.

Por su parte, el control debe tener como soporte el establecimiento de normas de desarrollo que han de ser verificadas continuamente en todas las etapas del desarrollo de un sistema. Estas normas no pueden estar aisladas, primero, del contexto particular de la dirección de informática (ambiente) y, segundo, de los lineamientos generales de la organización, para lo cual es necesario contar con personal en desarrollo que posea suficiente experiencia en el establecimiento de normas de desarrollo de sistemas. Estas mismas características deben existir en el personal de auditoría de sistemas.

Es poco probable que un proyecto llegue a un final feliz cuando se ha iniciado sin éxito.

Difícilmente estaremos controlando realmente el flujo de la información de un sistema que desde su inicio ha sido mal analizado, mal diseñado, mal programado e incluso mal documentado.

El excesivo mantenimiento de los sistemas generalmente es ocasionado por un mal desarrollo. Esto se inicia desde que el usuario establece sus requerimientos (en ocasiones sin saber qué desea) hasta la instalación del sistema, sin que se haya establecido un plan de prueba de éste para medir su grado de confiabilidad en la operación que se efectuará.

Para verificar si existe esta situación, se debe pedir a los analistas las actividades que están desarrollando en el momento de la auditoría y evaluar si están efectuando actividades de mantenimiento o si se están realizando nuevos proyectos. En ambos casos se deberá evaluar el tiempo que llevan dentro del mismo sistema, la prioridad que se le asignó y cómo está el tiempo real en relación con el tiempo estimado en el plan maestro.

El que los analistas, los programadores, o unos y otros, tengan acceso en todo momento a los sistemas en operación puede ser un grave problema y ocasionar fallas de seguridad.

INSTRUCTIVOS DE OPERACIÓN

Debemos evaluar los instructivos de operación de los sistemas para evitar que los programadores tengan acceso a los sistemas en operación. El contenido mínimo de los instructivos de operación deberá comprender:

- Diagrama de flujo por cada programa.
- Diagrama particular de entrada-salida.
- Mensaje y su explicación.
- Parámetros y su explicación.
- Diseño de impresión de resultados.
- Cifras de control.
- Fórmulas de verificación.
- Observaciones.
- Instrucciones en caso de error.
- Calendario de proceso y resultados.

FORMA

La finalidad de un sistema es la aceptación por parte del usuario. Para ello se debe considerar:

1. Indicar

- Pruebas de aceptación.
- Pruebas de integración.
- Pruebas de rendimiento.
- Pruebas de seguridad.
- Pruebas de compatibilidad.
- Otros.

2. En la inicialización del sistema se debe indicar la forma de operar las actividades.

En el caso de inicio de nuevos puestos de trabajo se debe indicar la forma de operar las actividades.

3. También se debe considerar la forma de operar las actividades.

EQUIPO

La selección de número de equipos de sistema operativo de producción de información de equipos (biomédicos) en relación con el número de usuarios.

ENTREVISTA

Las entrevistas se deben realizar en la situación de trabajo.

FORMA DE IMPLANTACIÓN

La finalidad es la de evaluar los trabajos que se realizan para iniciar la operación de un sistema; esto comprende: prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento de los responsables del sistema. Para ello deben de considerarse los siguientes aspectos:

1. Indicar cuáles puntos se toman en cuenta para la prueba de un sistema:

- Prueba particular de cada programa.
- Prueba por fase, validación, actualización.
- Prueba integral del paralelo.
- Prueba en sistema paralelo.
- Pruebas de seguridad y confidencialidad.
- Otros (especificar).

2. En la implantación se debe de analizar la forma en que se van a cargar inicialmente los datos del sistema, lo cual puede ser por captura o por transferencia de información. Estos datos pueden ser de todo el sistema, o bien en forma parcial. Lo que es necesario evaluar es la forma en que se van a cargar las cifras de control o bien los datos acumulados.

En el caso de una nómina, los días trabajados por los empleados a la fecha de iniciación del sistema, o bien sus acumulados en percepciones y en impuestos retenidos.

3. También se debe de hacer un plan de trabajo para la implantación, el cual debe contener las fechas en que se realizarán cada uno de los procesos.

Ejemplo

EQUIPO Y FACILIDADES DE PROGRAMACIÓN

La selección de la configuración de un sistema de cómputo incluye la interacción de numerosas y complejas decisiones de carácter técnico. El impacto en el rendimiento de un sistema de cómputo debido a cambios trascendentales en el sistema operativo o en el equipo, puede ser determinado por medio de un paquete de pruebas (*benchmark*) que haya sido elaborado para este fin en la dirección de informática. Es conveniente solicitar pruebas y comparaciones entre equipos (*benchmark*) para evaluar la situación del equipo y del software en relación con otros que se encuentran en el mercado.

ENTREVISTAS A USUARIOS

Las entrevistas se deberán llevar a cabo para comparar los datos proporcionados y la situación de la dirección de informática desde el punto de vista de los usuarios.

Su objeto es conocer la opinión que tienen los usuarios sobre los servicios proporcionados, así como la difusión de las aplicaciones de la computadora de los sistemas en operación.

Las entrevistas se deberán hacer, en caso de ser posible, a todos los usuarios, o bien en forma aleatoria a algunos de ellos, tanto a los más importantes como a los de menor importancia en cuanto al uso del equipo.

ENTREVISTAS

Aunque la entrevista es una de las fuentes de información más importante para saber cómo opera un sistema, no siempre tiene la efectividad que se desea, ya que en ocasiones las personas entrevistadas pueden ser presionadas por los analistas de sistemas, o piensan que si se hacen algunos cambios, éstos podrían afectar su trabajo. El gerente debe de hacer del conocimiento de los entrevistados el propósito del estudio.

Una guía para la entrevista puede ser la siguiente:

- Prepárese para la entrevista estudiando los puestos de las personas que van a ser entrevistadas y sus funciones dentro de la organización.
- Preséntese y dé un panorama del motivo de la entrevista.
- Comience con preguntas generales sobre las funciones, la organización y los métodos de trabajo.
- Haga preguntas específicas sobre los procedimientos que puedan dar como resultado el señalamiento de mejoras.
- Siga los temas tratados en la entrevista.
- Limite el tomar notas a lo más relevante, para evitar distractores.
- Al final de la entrevista, ofrezca un resumen de la información obtenida y pregunte cómo se le podrá dar seguimiento.

CUESTIONARIO

El diseño de un cuestionario debe tener una adecuada preparación, elaboración, preevaluación y evaluación. Algunas guías generales son:

1. Identificar el grupo que va a ser evaluado.
2. Escribir una introducción clara, para que el investigado conozca los objetivos del estudio y el uso que se le dará a la información.
3. Determine qué datos deben ser recopilados.
4. Elabore las preguntas con toda precisión (no haga preguntas en negativo), de tal forma que la persona que las responda lo pueda hacer con toda claridad. Estructure las preguntas en forma lógica y secuencial de tal forma que

el tiempo
tas las ob
objetivo c

5. Limite el
contestaci
 6. Implemen
sean clara
 7. Diseñe e
 8. Determin
 9. Distribuy
tas desea
- Procure c

- ¿Qué
- ¿Qué
- ¿Qué
- ¿Qué
- ¿Cón
- ¿Exis
- ¿Cón

Desde el

1. Cumplir
2. Cubrir to
3. No exced
4. Ser fácil
5. Ser confi
6. Poderlos
7. Ser amig

Para que
una comuni
ma. En ella
rio, las neces
mación de s

En esta
que será pro
ma y la form
cuados, esta
quién tiene

Esta eta
especialista
logró una a
trol satisfact

Para ve
requeridos
será preciso

el tiempo de respuesta y de escritura sea breve (aunque se deben dejar abiertas las observaciones). Elimine todas aquellas preguntas que no tengan un objetivo claro, o que sean improcedentes.

5. Limite el número de preguntas para evitar que sea demasiado el tiempo de contestación y que se pierda el interés de la persona.
6. Implemente un cuestionario piloto, para evaluar que todas las preguntas sean claras y que las respuestas sean las esperadas.
7. Diseñe e implemente un plan de recolección de datos.
8. Determine el método de análisis que será usado.
9. Distribuya los cuestionarios y déles seguimiento para obtener las respuestas deseadas; asimismo, analice los resultados.

Procure que su cuestionario responda a las siguientes preguntas:

- ¿Qué áreas pueden ser mejoradas?
- ¿Qué información necesita que actualmente no tiene o que es difícil de obtener?
- ¿Qué cuellos de botella ocurren durante el día? ¿Cómo se pueden eliminar?
- ¿Cómo se puede cambiar el procedimiento para eliminarlos?
- ¿Existe un procedimiento que sea redundante o repetitivo?
- ¿Cómo se podría eliminar esta repetición?

Desde el punto de vista del usuario los sistemas deben:

1. Cumplir con los requerimientos totales del usuario.
2. Cubrir todos los controles necesarios.
3. No exceder las estimaciones del presupuesto inicial, en tiempo y costo.
4. Ser fácilmente modificables.
5. Ser confiables y seguros.
6. Poderlos usar a tiempo, y con el menor tiempo y esfuerzo posible.
7. Ser amigables.

Para que un sistema cumpla con los requerimientos del usuario se necesita una comunicación completa entre éste y el responsable del desarrollo del sistema. En ella se deben definir claramente los elementos con que cuenta el usuario, las necesidades del proceso de información y los requerimientos de información de salida, almacenada o impresa.

En esta misma etapa debió haberse definido la calidad de la información que será procesada por la computadora, estableciéndose los riesgos de la misma y la forma de minimizarlos. Para ello se debieron definir los controles adecuados, estableciéndose además los niveles de acceso a la información, es decir, quién tiene privilegio de consultar, modificar o incluso borrar información.

Esta etapa habrá de ser cuidadosamente verificada por el auditor interno especialista en sistemas y por el auditor en informática, para comprobar que se logró una adecuada comprensión de los requerimientos del usuario y un control satisfactorio de información.

Para verificar si los servicios que se proporcionan a los usuarios son los requeridos y que se están proporcionando en forma adecuada, cuando menos será preciso considerar la siguiente información:

**Requerimientos
del usuario**

- Descripción de los servicios prestados.
- Criterios que utilizan los usuarios para evaluar el nivel del servicio prestado.
- Reporte periódico del uso y concepto del usuario sobre el servicio.
- Registro de los requerimientos planteados por el usuario.
- Tiempo de uso.

Con esta información se puede comenzar a realizar la entrevista para determinar si los servicios proporcionados y planeados por la dirección de informática cubren las necesidades de información de la organización.

A continuación se presenta una guía de cuestionario para aplicarse durante la entrevista con el usuario.

1. ¿Considera que la dirección de informática le da los resultados esperados?

SÍ NO

¿Por qué?

2. ¿Cómo considera usted, en general, el servicio proporcionado por la dirección de informática?

A. Deficiente B. Aceptable C. Satisfactorio D. Excelente

¿Por qué?

3. ¿Cubre sus necesidades de procesamiento?

A. No las cubre B. Parcialmente C. La mayor parte D. Todas

¿Por qué?

4. ¿Cómo considera la calidad del procesamiento que se le proporciona?

A. Deficiente B. Aceptable C. Satisfactorio D. Excelente

¿Por qué?

5. ¿Hay disponibilidad de procesamiento para sus requerimientos?

A. Generalmente no existe B. Ocasionalmente

C. Regularmente D. Siempre

¿Por qué?

6. ¿Conoce los costos de los servicios proporcionados? SÍ NO

7. ¿Qué opina del costo del servicio proporcionado por el departamento de procesos electrónicos?

A. Excesivo B. Mínimo C. Regular D. Adecuado E. No lo conoce

¿Por qué?

8. ¿Son entregados con puntualidad los trabajos?

- A. Nunca B. Rara vez C. Ocasionalmente
D. Generalmente E. Siempre

¿Por qué?

9. ¿Qué piensa de la presentación de los trabajos solicitados?

- A. Deficiente B. Aceptable C. Satisfactoria D. Excelente

¿Por qué?

10. ¿Qué piensa de la atención brindada por el personal de procesos electrónicos?

- A. Insatisfactoria B. Satisfactoria C. Excelente

¿Por qué?

11. ¿Qué piensa de la asesoría que se imparte sobre informática?

- A. No se proporciona B. Es insuficiente
C. Satisfactoria D. Excelente

¿Por qué?

12. ¿Qué piensa de la seguridad en el manejo de la información proporcionada para su procesamiento?

- A. Nula B. Riesgosa C. Satisfactoria
D. Excelente E. Lo desconoce

¿Por qué?

13. ¿Existen fallas de exactitud en los procesos de información? sí NO

¿Cuáles?

14. ¿Cómo utiliza los reportes que se le proporcionan?

15. ¿Cuáles no utiliza?

16. De aquellos que no utiliza, ¿por qué razón los recibe?

17. ¿Qué sugerencias hace en cuanto a la eliminación de reportes: modificación, fusión, división de reporte?

18. ¿Se cuenta con un manual del usuario por sistema? SÍ NO

19. ¿Es claro y objetivo el manual del usuario? SÍ NO

20. ¿Qué opinión tiene sobre el manual?

NOTA: Pida el manual del usuario para evaluarlo.

21. ¿De su departamento, quién interviene en el diseño de sistemas?

22. ¿En qué sistemas tiene actualmente su servicio de computación?

23. ¿Qué sistemas desearía que se incluyeran?

24. Observaciones.

DERECHOS DE AUTOR Y SECRETOS INDUSTRIALES

En relación con las disposiciones jurídicas adecuadas para la actividad informática, la Cámara de Diputados y el Instituto Nacional de Estadística, Geografía e Informática (INEGI) organizaron un foro de consulta sobre derecho e informática. Como resultado, se recopilaron opiniones, propuestas y experiencias relacionadas con diversos aspectos, entre los que destacan: las garantías para la información personal almacenada en bases de datos y la protección jurídica de datos de carácter estratégico; la tipificación de delitos informáticos; el valor probatorio del documento electrónico, y la protección de derechos de autor para quienes desarrollan programas para computadora.

Dentro del concepto de propiedad intelectual, uno de los aspectos más importantes es el que se refiere a los derechos de autor, el cual involucra la parte más importante del desarrollo intelectual de las personas, ya que se refiere a las ramas literaria, científica, técnica, jurídica, musical, pictórica, escultórica, arqui-

tectónica, fotogra-

to, las bases de
En la mayo
les que produ
escultores, y
tadora y las ba
nes celebran c
a los autores.

En primer
vecho de su tr
gida del públi
son, en cierto

En segund
se verá estim
literatura, el t
país. Nadie d
mismo modo
yen a la elabo
mente remun

En tercer
cesarias, por
fáciles de obt

En cuarto
del pensamie
derecho a dec
y derecho a o

En quint
obras de los
mejor sus co
patrimonio c

El progr
en francés co
dor, es un co
ble por máq
miento de la
dos determi

Cada ve
obras acreec
últimas adic
porar entre

Artículo
todo crea
en virtuo
privilegi

La legis
catálogo de

tectónica, fotográfica, cinematográfica, televisiva, así como los programas de cómputo, las bases de datos y los medios de comunicación, entre las más importantes.

En la mayoría de los países existen leyes protectoras de las obras intelectuales que producen los poetas, los novelistas, los compositores, los pintores, los escultores, y de manera reciente se han protegido los programas de computadora y las bases de datos. Pero además de su legislación doméstica, las naciones celebran compromisos unas con otras para dar una protección internacional a los autores. En general, se admite que son cinco las razones de la protección.

En primer lugar, por una razón de justicia social: el autor debe obtener provecho de su trabajo. Los ingresos que perciba, deben estar en función de la acogida del público a sus obras y de sus condiciones de explotación: las "regalías" son, en cierto modo, los salarios de los trabajadores intelectuales.

En segundo, por una razón de desarrollo cultural; si está protegido, el autor se verá estimulado para crear nuevas obras, enriqueciendo de esta manera la literatura, el teatro, la música, los programas de computación elaborados en su país. Nadie debe realizar un trabajo sin que sea debidamente remunerado; del mismo modo, los que, por su trabajo, su inteligencia, su experiencia, contribuyen a la elaboración de programas y sistemas de cómputo, deben de ser debidamente remunerados.

En tercero, por una razón de orden económico; las inversiones que son necesarias, por ejemplo, para la elaboración de un sistema de cómputo serán más fáciles de obtener si existe una protección efectiva.

En cuarto, por una razón de orden moral; al ser la obra la expresión personal del pensamiento del autor, éste debe tener derecho a que se respete, es decir, derecho a decidir si puede ser reproducida o ejecutada en público, cuándo y cómo, y derecho a oponerse a toda deformación o mutilación cuando se utiliza la obra.

En quinto lugar, por una razón de prestigio nacional: el conjunto de las obras de los autores de un país refleja el alma de la nación y permite conocer mejor sus costumbres, sus usos, sus aspiraciones. Si la protección no existe, el patrimonio cultural será escaso y no se desarrollarán las artes.

El programa de computación, conocido en inglés como *computer program* y en francés como *programme d'ordinateur*, y también llamado programa de ordenador, es un conjunto de instrucciones que, cuando se incorpora a un soporte legible por máquina, puede hacer que una máquina con capacidad para el tratamiento de la información indique, realice o consiga una función, tarea o resultados determinados.

Cada vez se acepta con mayor frecuencia que los programas originales son obras acreedoras a la protección que otorga el derecho de autor. Una de las últimas adiciones de que fue objeto la precedente ley autoral, consistió en incorporar entre las obras protegidas a los programas de computación.

Artículo 11. El derecho de autor es el reconocimiento que hace el Estado a favor de todo creador de obras literarias y artísticas previstas en el artículo 13 de esta Ley, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial.

La legislación actual, además de conservar dichos programas en un similar catálogo de las obras para las que se reconocen los derechos de autor (art. 13,

LFDA), les dedica un capítulo especial (capítulo IV del título IV) con reglas particulares también sobre protección.

Artículo 13. Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas:

[...]

XI. Programas de cómputo;

[...]

Las demás obras que por analogía puedan considerarse obras literarias o artísticas se incluirán en la rama que les sea más afín a su naturaleza.

Artículo 83. Salvo pacto en contrario, la persona física o moral que comisione la producción de una obra o que la produzca con la colaboración remunerada de otras, gozará de la titularidad de los derechos patrimoniales sobre la misma y le corresponderán facultades relativas a la divulgación, integridad de la obra y de colección sobre este tipo de creaciones.

La persona que participe en la realización de la obra, en forma remunerada, tendrá el derecho a que se le mencione expresamente su calidad de autor, artista, intérprete o ejecutante sobre la parte o partes en cuya creación haya participado.

Artículo 84. Cuando se trate de una obra realizada como consecuencia de una relación laboral establecida a través de un contrato individual de trabajo que conste por escrito, a falta de pacto en contrario, se presumirá que los derechos patrimoniales se dividen por partes iguales entre empleador y empleado.

El empleador podrá divulgar la obra sin autorización del empleado, pero no al contrario. A falta de contrato individual de trabajo por escrito, los derechos patrimoniales corresponderán al empleado.

Capítulo IV

DE LOS PROGRAMAS DE COMPUTACIÓN Y LAS BASES DE DATOS

Artículo 101. Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, en un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102. Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 103. Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104. Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aun después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 105. El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o
II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no puede utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106. El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir.

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y

IV. La descompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 107. Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108. Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109. El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110. El titular del derecho patrimonial sobre una base de datos tendrá derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111. Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112. Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113. Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114. La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite y otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

Artículo 231. Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:

I. Comunicar o utilizar públicamente una obra protegida por cualquier medio y de cualquier forma, sin la autorización previa y expresa del autor, de sus legítimos herederos o del titular del derecho patrimonial de autor;

II. Utilizar la imagen de una persona sin su autorización o la de sus causahabientes;

III. Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros, protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley;

IV. Ofrecer en venta, almacenar, transportar o poner en circulación obras protegidas por esta Ley que hayan sido deformadas, modificadas o mutiladas sin autorización del titular del derecho de autor;

V. Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación;

VI. Retransmitir, fijar, reproducir y difundir al público emisiones de organismos de radiodifusión y sin la autorización debida, y

VII. Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular.

Artículo 232. Las infracciones en materia de comercio previstos en la presente Ley serán sancionadas por el Instituto Mexicano de la Propiedad Industrial con multa:

I. De cinco mil hasta diez mil días de salario mínimo en los casos previstos en las fracciones I, III, IV, V, VII, VIII y IX del artículo anterior;

II. De mil hasta cinco mil días de salario mínimo en los casos previstos en las fracciones II y VI del artículo anterior, y

III. De quinientos hasta mil días de salario mínimo en los demás casos a que se refiere la fracción X del artículo anterior.

Se aplicará multa adicional de hasta quinientos días de salario mínimo general vigente por día a quien persista en la infracción.

Artículo 233. Si el infractor fuese un editor, organismo de radiodifusión, o cualquier persona física o moral que explote obras a escala comercial, la multa podrá incrementarse hasta en un cincuenta por ciento respecto de las cantidades previstas en el artículo anterior.

INTERNET

El Internet, considerado como una colección de redes interconectadas o como un conjunto de computadoras unidas entre sí, no ha sido tomado en cuenta entre las disposiciones que se acaban de mencionar.

Para obtener acceso a Internet se requiere un equipo que está al alcance del público en general, por lo que cualquier persona puede entrar a la red de redes de comunicación si contrata los servicios de un proveedor de acceso.

Recientemente han surgido empresas proveedoras de servicios dedicados a ofrecer en renta conexiones a Internet, ya sea de manera directa, indirecta o parcial, siendo las propias empresas las que proporcionan el equipo necesario para tener acceso.

Los proveedores de servicios son los responsables de la información que ponen al servicio de sus usuarios, ya que dichas compañías son encargadas de divulgar y controlar la información transmitida por Internet.

Son muchas las llevadas a cabo infracción a la norma de comercio electrónico de modificación de obra bajo e violaciones les en forma pública de

También utiliza la protección, por cuestiones que pueden sobre tela artista pre

El debate polémica sobre el instrumento Internet. El disco duro Internet. E una o vari

Cuando atribuye ge pues, extra cookies", c

Esto p visitantes y entre vari que perm electrónic anunciand

El coc todo en ca línea, la co to de paga grabando

Teóric un servid

Las re nes han al verdadera ción de da do su nav den borra programa

La sit determina de Intern

Son muy complejos los aspectos técnicos que implica conocer las acciones llevadas a cabo en Internet para determinar cuáles pudieran constituir alguna infracción a los derechos de autor. No obstante, se puede pensar que este sistema de comunicación puede originar las siguientes violaciones: al derecho moral de modificar la obra; al derecho moral de inédito; al derecho de publicar la obra bajo el propio nombre o de manera anónima. También pueden producirse violaciones a los derechos patrimoniales cuando se transmiten obras intelectuales en forma de archivos por medio de Internet, ya que se realiza una utilización pública de una obra sin la remuneración para el autor de la creación intelectual.

También puede ser fácilmente violado el derecho de autor cuando la red utiliza la propia imagen, de la que son titulares los artistas, intérpretes y ejecutantes, por cuanto que en Internet es posible encontrar un gran número de imágenes que pueden ser reproducidas imprimiéndolas sobre papel, como carteles, o sobre tela para obtener prendas de vestir (como playeras con la imagen del artista preferido).

El debate sobre la protección de los datos personales en Internet reabre la polémica sobre el papel desempeñado por los cookie, que sirven más como instrumento de mercadotecnia que como medio para espiar a los usuarios de Internet. El término cookie se aplica a un simple archivo de datos situado en el disco duro del computador de una persona o compañía que ofrece servicios de Internet. El cookie y su contenido son creados por un servidor que almacena una o varias páginas Internet.

Cuando un visitante accede a una página web por primera vez, el servidor le atribuye generalmente un número de identificación con atributos, el cookie. Después, extrae su nombre de un fichero empleado en las plataformas Unix, los "magic cookies", con lo que el visitante será identificado en sus visitas ulteriores.

Esto permite al propietario de la página analizar el comportamiento de sus visitantes y personalizar sus visitas. El desplazamiento de los usuarios de Internet entre varias páginas de una dirección se puede identificar a la perfección, lo que permite "tomar nota" del recorrido utilizado más a menudo. La dirección electrónica podrá ser modificada para satisfacer a la vez al visitante y a los anunciantes, que pueden colocar su publicidad en el lugar más adecuado.

El cookie sirve también para grabar lo que ocurre en estas visitas, sobre todo en caso de compra. Si se elige, por ejemplo, un libro en una librería en línea, la compra queda grabada en un cookie, antes de reaparecer en el momento de pagar la factura en la caja virtual. La visita también puede ser personalizada grabando en el archivo cookie las informaciones facilitadas por el usuario.

Teóricamente la seguridad de estas informaciones está garantizada, ya que un servidor sólo puede obtener la información del cookie que ha producido.

Las redes de publicidad en línea sí tienen esta capacidad. Estas innovaciones han alarmado a algunas asociaciones, para quienes este sistema supone una verdadera intrusión en la vida privada de los usuarios de Internet. Esta captación de datos se realiza sin que el usuario lo sepa, a menos que haya configurado su navegador para ser advertido. Los que no disponen de este sistema pueden borrar periódicamente el fichero cookie de su disco duro o recurrir a un programa especial.

La situación de los cookie debe ser evaluada dentro de la auditoría, para determinar si se considera como una intromisión la privacidad de los usuarios de Internet de una compañía.

PROTECCIÓN DE LOS DERECHOS DE AUTOR

Las obras protegidas por la ley deberán ostentar la expresión "Derechos Reservados" o su abreviatura D.R., seguida por el símbolo c dentro de un círculo: ©. Sin embargo, la omisión de estos requisitos no implica la pérdida de los derechos de autor, aunque sujeta al responsable a las sanciones establecidas en la ley.

La reserva de los derechos de autor es la facultad para usar y explotar en forma exclusiva títulos, nombres, denominaciones, características físicas y psicológicas distintivas o características de operación originales. Ahora bien, para proteger los derechos de autor se han establecido diversos procedimientos, el primero relacionado con los delitos que pueden cometerse al invadirse un derecho de autor, por lo cual se estableció el artículo 215 de la Ley de Derechos de Autor, que corresponde conocer a los tribunales de la Federación, sobre los delitos relacionados con el derecho de autor, los cuales deberán estar previstos en el Código Penal para el Distrito Federal, que regula los delitos en materia del fuero común y para toda la República en materia del fuero federal.

Independientemente de solicitar el ejercicio de la acción penal, la persona afectada por un derecho protegido por la Ley de Derechos de Autor, podrá optar entre hacer valer las acciones judiciales que le correspondan o sujetarse al procedimiento de avenencia.

El procedimiento de avenencia tiene por objeto dirimir de manera amistosa un conflicto surgido con motivo de la interpretación o aplicación de la ley, y se inicia con la queja, que se presenta directamente ante el Instituto Nacional del Derecho de Autor.

Mediante la aplicación del artículo 2o. de la Ley de Derechos de Autor, corresponde al Instituto Nacional del Derecho de Autor su aplicación administrativa, y en los casos previstos por dicha ley al Instituto Mexicano de la Propiedad Industrial.

Mediante el arbitraje las partes podrán resolver todas las controversias que hayan surgido en materia de derechos de autor, y podrán someterse por medio de cláusula compromisoria o compromiso arbitral.

Es de señalar que el artículo 223 de la Ley de Derechos de Autor señala que para ser árbitro se requiere el ser licenciado en derecho, pero no es requisito el ser especialista en el área en que se va a arbitrar, como sería el ser experto en programación, informática o bases de datos.

Las penalidades en caso de delitos se han incrementado notablemente de acuerdo con lo señalado en el:

CÓDIGO PENAL PARA EL DISTRITO FEDERAL EN MATERIA DE FUERO COMÚN Y PARA TODA LA REPÚBLICA EN MATERIA DE FUERO FEDERAL

"TÍTULO VIGÉSIMO SEXTO" DE LOS DELITOS EN MATERIA DE DERECHOS DE AUTOR

Artículo 424. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días de multa:

I. Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Pública;

II. Al ed
ejemplares c
autorizados

III. A q
venta o arr
por la Ley F
la autorizac
derechos de

IV. Las
comercial y
da ley; y

V. A qu
sea desactiv
tación.

Artículo
tres mil día
interpretaci

Artículo
a tres mil d

I. A qu
descifrar u
del distribu

II. A q
frar una se
distribuido

Artículo
tres mil día
del autor p

Artículo
carán sin p
cuarenta p
ción de se

tutelados p

Artículo
parte ofen
guido de c

SECRE

Artículos d
en Materia

Art. 82. Se
o comerci
signifique

II. Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos;

III. A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa; a escala comercial y sin la autorización que en los términos de la citada ley deba otorgar el titular de los derechos de autor o de los derechos conexos;

IV. Las mismas sanciones se impondrán a quien use en forma dolosa, a escala comercial y sin la autorización correspondiente, obras protegidas por la mencionada ley; y

V. A quien fabrique con fines de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 425. Se impondrá prisión de seis meses a dos años o de trescientos a tres mil días multa, al que a sabiendas y sin derecho explote con fines de lucro una interpretación o una ejecución.

Artículo 426. Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:

I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Artículo 427. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa, a quien publique a sabiendas una obra sustituyendo el nombre del autor por otro nombre.

Artículo 428. Las sanciones pecuniarias previstas en el presente título se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor al cuarenta por ciento del precio de venta al público de cada producto o de la prestación de servicios que impliquen violación a alguno o algunos de los derechos tutelados por la Ley Federal del Derecho de Autor.

Artículo 429. Los delitos previstos en este título se perseguirán por querrela de parte ofendida, salvo el caso previsto en el artículo 424, fracción I, que será perseguido de oficio.

SECRETOS INDUSTRIALES

Artículos de la Ley de la Propiedad Industrial en Materia de Secretos Industriales

Art. 82. Se considera secreto industrial a toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terce-

ros en la relación de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o a los medios o formas de distribución o comercialización de productos o prestación de servicios.

No se considerará secreto industrial aquella información que sea del dominio público la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial. No se considerará que entra al dominio público o que es divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporción es para el efecto de obtener licencias, permisos, autorizaciones, registros, o cualesquiera otros actos de autoridad.

Se considera secreto industrial "toda información de aplicación industrial o comercial". En principio, respecto de la aclaración de que la información puede ser de carácter industrial o comercial, la cual, aun y cuando parece elemental, da lugar a que en ciertos casos la voluntad del legislador pretendiera interpretarse en un sentido restrictivo, limitando la protección exclusivamente a la información estrictamente de carácter industrial.

Por otro lado, especial peso debe concederse al término "aplicación" que incluye el precepto al referirse a los secretos industriales, ya que la información deberá satisfacer ese particular requisito. De hecho, en este punto podemos encontrar una relativa equivalencia con el requisito que al efecto se establece en materia de patentes, consistente en que las invenciones sean susceptibles de aplicación industrial.

Es claro que la expresión "aplicable", en este particular contexto, debe ser interpretada en su forma más amplia, ya que pudiera presentarse el caso de que cierta información que aun y cuando en la práctica aún no hubiese sido puesta en práctica, sus posibilidades de ser implementada le ubiquen como información merecedora de la tutela de este régimen.

En aras de que el régimen tutelar de los secretos industriales verdaderamente constituya un medio de protección de información confidencial que se estima como bien económicamente valioso, la limitación que el precepto realiza del tipo de información que califica como constitutiva de secretos industriales, incorpora la palabra "referida a", con lo que el legislador parece establecer que basta que la información guarde cierta liga o esté asociada a las actividades fundamentales del agente económico o bien una ventaja competitiva para poder ser considerada como apta para constituir un secreto industrial, lo cual puede ser cuestionable, ya que no todas las copias, por ejemplo, de programas, tienen una finalidad de beneficio económico o una ventaja competitiva.

Entre la información típicamente considerada como constitutiva de secretos industriales se cuenta la relativa a listas de clientes y proveedores, formulaciones, procesos industriales, estrategias de mercado, lanzamiento de productos, resultados de estudios comerciales y de mercado, sueldos, procesos legales, listas de precios, bases de datos, y en general, cualquier información sensible que represente un valor económico para la empresa, este tipo de información la podemos considerar directamente ligada con bases de datos.

Respecto de la condición de que el secreto industrial sea guardado por una persona física o moral con carácter confidencial, puede considerarse que sin duda constituye ésta el núcleo fundamental que imprime a este tipo de información la característica que le califica como secreto industrial.

Es importante considerar que el precepto no establece condición alguna respecto del origen de la información que guarda su poseedor, es decir, no se establece como condición el que la información hubiese sido generada por su poseedor, o bien, que la misma hubiese sido obtenida por algún título legal como pueda ser su transmisión por parte de un tercero, por lo que la información contenida en una base de datos, es considerada como un secreto industrial, sin importar si ésta fue o no creada por la persona que la posee y que la pueden difundir.

Obviamente se abre aquí el planteamiento de si la información que eventualmente ha sido obtenida de manera ilegal, en caso de seguir cumpliendo las condiciones de confidencialidad exigidas por el precepto, debe ser merecedora de la protección conferida a los secretos industriales. Sería el caso, por ejemplo, de información que indebidamente revele un ex empleado a su nuevo patrón, y que éste pretenda conservar y proteger como secreto industrial propio, o bien copias de programas que posea un empleado y que las proporcione a su nuevo empleador.

En términos del tercer párrafo de este mismo artículo, se establece que no se considera que entra al dominio público o que es divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando se proporcione para el objeto de obtener licencias, permisos, autorizaciones, registros, o cualesquiera otros actos de autoridad.

Las bases de datos que son del dominio público, pero que son modificadas, mejoradas o ampliadas, para lo cual se emplean tiempo y recursos, se convierten en propiedad industrial. Es el caso, por ejemplo, de múltiples bases de datos que son obtenidas a partir de información accesible para el público, pero que al imprimirse una dosis significativa de recursos, tiempo y talento, la información es tratada y depurada hasta el grado de convertirla en un producto nuevo y diferente, que por ese solo hecho merece la protección que la legislación confiere a los secretos industriales, siempre que, desde luego, se satisfagan las otras condiciones exigidas para esta figura.

Este mismo criterio puede aplicarse a ciertos programas de computación que para su conformación han requerido de la participación de especialistas que han invertido en la investigación cantidades notables de esfuerzo y erudición, de manera que el resultado puede ser considerado como secreto industrial.

Un aspecto que es conveniente destacar es que en este punto la disposición parece apartarse del texto del Tratado de Libre Comercio entre México, Estados Unidos y Canadá, en su artículo 1711, únicamente requiere que quien posee el secreto hubiere tomado "medidas a su alcance". El punto parece mínimo, pero es claro que existe una gran distancia entre haber tomado "medidas al alcance" que haber tomado "las medidas necesarias", tal como la Ley de Propiedad Industrial lo determina.

Resulta imprescindible para las empresas modernas contar con un reglamento interno de trabajo, en el que se especifiquen las políticas de la empresa en materia de información confidencial. Dicho reglamento debe ser conocido por todos los empleados y funcionarios de la empresa, y su puesta en práctica debe ser un asunto prioritario para cumplir con los requerimientos que la ley determina para la constitución y preservación del secreto industrial. Entre las políticas que deben observarse como mínimas en materia de secretos industriales se cuentan enunciativamente las consistentes en la identificación de los materiales considerados como secreto de negocios, la prohibición de la duplicación de documentos sensibles sin autorización, el control de ingreso a las áreas en que la información se concentra, la utilización de sistemas de seguridad y control, la implementación de claves de acceso a las computadoras, la firma de convenios de confidencialidad con empleados y proveedores, etc. Estos puntos son tratados con mayor amplitud en el tema relacionado a la seguridad.

Entre otras disposiciones aplicables se encuentran las de la Ley Federal de Responsabilidades de los Servidores Públicos, que en su artículo 47 determina que todo servidor público tendrá la obligación de custodiar y cuidar la documentación e información que por razón de su empleo, cargo o comisión, conserve bajo su cuidado o a la cual tenga acceso, impidiendo o evitando el uso, la sustracción, destrucción, ocultamiento o inutilización indebida de la misma.

En relación con el llamado "know how", cabe también hacer la distinción de que no toda la información de este tipo es necesariamente confidencial, ya que este concepto se dirige a referir aquel conjunto de conocimientos y habilidades que permiten a una persona o grupo de personas desarrollar, producir, distribuir o comercializar un bien o un servicio con ventajas frente a otros competidores, pero con la característica de que dicha información bien puede estar en el dominio público, y en su caso son elementos como la experiencia y la destreza lo que permite consolidar la ventaja de ese "saber hacer". Es decir, en el caso del "know how" podemos considerar que una de sus diferencias básicas con los secretos industriales es que no necesariamente es información que deba considerarse como confidencial.

La definición de la "Uniform Trade Secrets Act", legislación que en Estados Unidos habla sobre los secretos industriales es la siguiente:

"Un secreto industrial podrá consistir en cualquier fórmula, patrón, dispositivo o compilación de información que se usen en una empresa y que den al empresario la oportunidad de obtener una ventaja sobre los competidores que no lo conocen o no lo usa. Puede ser la fórmula de un compuesto químico, un proceso de manufactura, de tratamiento o de conservación de materiales, el patrón para una máquina u otro dispositivo, o una lista de clientes."

Art. 83. La información a que se refiere el artículo anterior, deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares.

Es importante considerar que este precepto adiciona un elemento más, y es el hecho de que la información respectiva debe constar en un soporte material. Un problema que se tiene está en que para que los documentos que contienen el secreto industrial sean registrados ante el Registro Nacional de Derecho de Autor, dependiente del Instituto Nacional del Derecho de Autor, deben ser presentados en un soporte material, y al tratarse de un registro público la información se hace accesible a terceros perdiendo, precisamente por ese hecho, cualquier tipo de protección legal que como secreto industrial le hubiere correspondido.

Art. 84. La persona que guarde un secreto industrial podrá transmitirlo o autorizar su uso a un tercero. El usuario autorizado tendrá la obligación de no divulgar el secreto industrial por ningún medio.

En los convenios por los que se transmitan conocimiento técnicos, asistencia técnica, provisión de ingeniería básica o de detalle, se podrán establecer cláusulas de confidencialidad para proteger los secretos industriales que contemplen, los cuales deberán precisar los aspectos que comprenden como confidenciales.

Art. 85. Toda aquella persona que, con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a un secreto industrial del cual se haya prevenido sobre su confidencialidad, deberá abstenerse de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado.

Todas las personas mencionadas en el precepto parecen cubrir las diversas opciones de quienes pueden tener legal acceso a los secretos industriales de su poseedor, esto es, trabajadores, empleados, asesores, y en general, cualquiera que tenga acceso a los secretos por virtud de sostener una relación de negocios con el que guarda el secreto. De acuerdo con las fracciones III, IV y V del artículo 223 de la Ley de Propiedad Industrial, no sólo la revelación del secreto está vedada, sino también su utilización y aprovechamiento.

Consi
el em
frente

Las po
dose d
enorm
ción d
exclus

Lo
que de
sistem
conect

La
do Ne

admir
de Int
solicit

sión e
asigna
puedo

E
fronta

sitios
domi

D
intern

da, p
y, po

Art. 86. La persona física o moral que contrate a un trabajador que esté laborando o haya laborado o a un profesionista, asesor o consultor que preste o haya prestado sus servicios para otra persona, con el fin de obtener secretos industriales de ésta, será responsable del pago de daños y perjuicios que le ocasione a dicha persona.

También será responsable del pago de daños y perjuicios la persona física o moral que por cualquier medio ilícito obtenga información que contemple un secreto industrial.

El artículo 223 de la Ley de Propiedad Industrial define y sanciona las conductas delictivas en relación con secretos industriales. Al propio tiempo, el artículo incurre en otra intrascendencia por obviedad, al señalar que quien reciba secretos industriales de terceros por vía de contratar a sus empleados o ex empleados, asesores o ex asesores, será responsable de los daños y perjuicios que ocasione, siendo que dicha obligación deviene de cualquier hecho ilícito que lesione a una persona, tal como lo prescribe el artículo 1910 del Código Civil.

Consideraciones legales sobre el empleo de nombres de dominio frente al régimen de marcas

Las posibilidades de la comunicación vía Internet son inagotables, comprendiéndose dentro de ellas la posibilidad de ofertar productos y prestar servicios al enorme mercado potencial que acude a los sitios en la red, mediante la obtención de un nombre de dominio que refiera a los usuarios de la red a un sitio exclusivo destinado a promover sus bienes y/o servicios.

Los nombres de dominio son denominaciones únicas asignadas a personas que desean tener un domicilio que pueda ser visitado por usuarios en la red. El sistema de dominio interpreta los nombres como números y cada computadora conectada a la red cuenta con un número único.

La concesión de nombres de dominio es coordinada por un organismo llamado Network Solutions Inc, a través de InterNIC, quien trabaja en conjunto con administradores de dominio, coordinadores de redes y proveedores de servicio de Internet. Los nombres de dominio son registrados a través de una forma de solicitud estándar disponible en la red y el único criterio seguido para su concesión es el de verificar que no exista un nombre de dominio, idéntico, previamente asignado. Lo anterior, resulta necesario desde el punto de vista técnico, ya que no pueden existir dos rutas de acceso idénticas de sitios distintos en la red.

El comercio de bienes y servicios a través de la red ha propiciado la confrontación de los intereses de titulares de marcas registradas con dueños de sitios en la red que adoptan marcas propiedad de terceros como nombres de dominio.

Desde fines de 1995 los gobiernos de los estados y distintas organizaciones internacionales han encaminado sus esfuerzos a balancear de manera adecuada, por un lado, la necesidad de proteger los derechos de propiedad intelectual y, por otro, las innegables ventajas del acceso a la información vía Internet.

Mantiene el liderazgo de dicha empresa Network Solutions, Inc (NSI), que es el brazo operativo de la US National Science Foundation, autoridad que regula la asignación de dominios en Internet.

En el décimo Congreso de las Naciones Unidas sobre prevención del delito y tratamiento de delincuentes celebrado en Viena del 10 al 17 de octubre del 2000, se llegó a la conclusión sobre los delitos relacionados con las redes informáticas: "Para combatir eficazmente los delitos cibernéticos es necesario un enfoque internacional coordinado a diferentes niveles. A nivel nacional, la investigación de esos delitos requiere personal, conocimientos especializados y procedimientos adecuados. Se alienta a los Estados a que consideren la posibilidad de crear mecanismos que permitan obtener de manera oportuna datos exactos de los sistemas y redes informáticas cuando estos datos se requieran como prueba en los procedimientos judiciales. A nivel internacional, la investigación eficaz de los delitos cibernéticos requiere una adecuación oportuna, facilitada por la coordinación entre los organismos nacionales de aplicación de la ley y la institución de la autoridad legal pertinente."

Como ejemplo de legislaciones relacionadas con informática en Latinoamérica tenemos el caso de Colombia:

Poder Público - Rama Legislativa
LEY 527 DE 1999 (agosto 18)

por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

PARTE I
PARTE GENERAL

CAPÍTULO I. Disposiciones generales

Artículo 2o. Definiciones. Para los efectos de la presente ley se entenderá por:

- a) **Mensaje de datos.** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;
- b) **Comercio electrónico.** Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

- c) **Firma digital.** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;
- d) **Entidad de certificación.** Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;
- e) **Intercambio Electrónico de Datos (EDI).** La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;
- f) **Sistema de información.** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

CAPÍTULO II. Aplicación de los requisitos jurídicos de los mensajes de datos

Artículo 9o. Integridad de un mensaje de datos.

Artículo 10. Admisibilidad y fuerza probatoria de los mensajes de datos.

Artículo 11. Criterio para valorar probatoriamente un mensaje de datos.

Artículo 12. Conservación de los mensajes de datos y documentos.

CAPÍTULO III. Comunicación de los mensajes de datos

Artículo 17. Presunción del origen de un mensaje de datos.

Artículo 18. Concordancia del mensaje de datos enviado con el mensaje de datos recibido.

Artículo 19. Mensajes de datos duplicados.

Artículo 20. Acuse de recibo.

Artículo 21. Presunción de recepción de un mensaje de datos.

PARTE II COMERCIO ELECTRÓNICO EN MATERIA DE TRANSPORTE DE MERCANCÍAS

PARTE III FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACIÓN

CAPÍTULO I. Firmas digitales

Artículo 28. Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

CAPÍTULO II. Entidades de certificación

CAPÍTULO III. Certificados

CAPÍTULO IV. Suscriptores de firmas digitales

CAPÍTULO V. Superintendencia de Industria y Comercio

Artículo 42. Sanciones.

DECRETO NÚMERO 1747 DE 2000
(septiembre 11)

por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

CAPÍTULO I. Aspectos generales

Artículo 1o. Definiciones. Para efectos del presente decreto se entenderá por:

1. **Iniciador:** persona que actuando por su cuenta, o en cuyo nombre se haya actuado, envíe o genere un mensaje de datos.
2. **Suscriptor:** persona a cuyo nombre se expide un certificado.
3. **Repositorio:** sistema de información utilizado para almacenar y recuperar certificados y otra información relacionada con los mismos.
4. **Clave privada:** valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.
5. **Clave pública:** valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador.
6. **Certificado en relación con las firmas digitales:** mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la clave pública de éste.
7. **Estampado cronológico:** mensaje de datos firmado por una entidad de certificación que sirve para verificar que otro mensaje de datos no ha cambiado en un periodo que comienza en la fecha y hora en que se presta el servicio y termina en la fecha en que la firma del mensaje de datos generado por el prestador del servicio, de estampado, pierde validez.
8. **Entidad de certificación cerrada:** entidad que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.

9. **Entidad de certificación abierta:** la que ofrece servicios propios de las entidades de certificación, tales que:
- a) Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o
 - b) Recibe remuneración por éstos.
10. **Declaración de Prácticas de Certificación (DPC):** manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

CAPÍTULO II. De las entidades de certificación y certificados digitales

Sección I. De las entidades de certificación cerradas

Sección II. De las entidades de certificación abiertas

Artículo 60. Declaración de Prácticas de Certificación (DPC). La Superintendencia de Industria y Comercio definirá el contenido de la Declaración de Prácticas de Certificación, DPC, la cual deberá incluir, al menos lo siguiente:

1. Identificación de la entidad de certificación.
2. Política de manejo de los certificados.
3. Obligaciones de la entidad y de los suscriptores del certificado y precauciones que deben observar los terceros.
4. Manejo de la información suministrada por los suscriptores.
5. Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.
6. Límites de responsabilidad por el ejercicio de su actividad.
7. Tarifas de expedición y revocación de certificados.
8. Procedimientos de seguridad para el manejo de los siguientes eventos:
 - a) Cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida;
 - b) Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado;
 - c) Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio;
 - d) Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratados por el suscriptor.
9. El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación.
10. Modelos y minutas de los contratos que utilizarán con los usuarios.
11. Política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.

Artículo 11. Informe de Auditoría.

Artículo 12. Requisitos de las firmas auditoras.

Artículo 14. Certificaciones recíprocas. El reconocimiento de los certificados de firmas digitales emitidos por entidades de certificación extranjeras, realizado por entidades de certificación autorizadas para tal efecto en Colombia, se hará constar en un certificado expedido por estas últimas.

Artículo 15. Uso del certificado digital.

Artículo 16. Unicidad de la firma digital.

Sección III. De la decisión y las responsabilidades

Sección IV. De los certificados digitales

Artículo 24. Registro de certificados. Toda entidad de certificación autorizada deberá llevar un registro de público, acceso que contenga todos los certificados emitidos y sus fechas de emisión, expiración o revocación.

Artículo 25. Información. Las entidades de certificación estarán obligadas a respetar las condiciones de confidencialidad y seguridad, de acuerdo con las normas vigentes respectivas.

Salvo la información contenida en el certificado, la suministrada por los suscriptores a las entidades de certificación se considerará privada y confidencial.

CAPÍTULO III. Facultades de la Superintendencia de Industria y Comercio

Artículo 27. Estándares. La Superintendencia de Industria y Comercio determinará los estándares admisibles con respecto a los cuales las entidades de certificación deberán acreditar el cumplimiento de los requisitos relativos a:

1. La generación de pares de claves.
2. La generación de firmas.
3. Los certificados.
4. Los sistemas de cifrado.
5. Las comunicaciones.
6. La seguridad de los sistemas de información y de las instalaciones, o
7. Cualquier otro aspecto que redunde en la confiabilidad y seguridad de los certificados, o de la información que repose en la entidad de certificación.

Para la determinación de los estándares admisibles, la superintendencia deberá adoptar aquellos que tengan carácter internacional y que estén vigentes tecnológicamente o los desarrollados por el organismo nacional de normalización o los que sean ampliamente reconocidos para los propósitos perseguidos. En todo caso, deberá tener en cuenta su aplicabilidad a la luz de la legislación vigente.

5

CAPÍTULO

Evaluación del proceso de datos y de los equipos de cómputo

OBJETIVOS

Al finalizar este capítulo, usted:

1. Explicará por qué los datos de las organizaciones son valiosos recursos y por qué es necesario tener estrictos controles sobre ellos.
2. Conocerá los distintos tipos de control que deben ejercerse sobre los datos de las organizaciones.
3. Describirá las reglas relativas al orden y cuidado que deben observarse en el centro de cómputo.
4. Explicará la importancia de evaluar el grado de eficiencia del sistema operativo para satisfacer las necesidades de una instalación.
5. Conocerá los puntos principales que deberán ser evaluados en los equipos de cómputo de una organización.

CONTROLES

Los datos son uno de los recursos más valiosos de las organizaciones, y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

- La responsabilidad de los datos es compartida conjuntamente por alguna función determinada de la organización y la dirección de informática.
- Un problema que se debe considerar es el que se origina por la duplicidad de los datos, el cual consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.
- Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.
- Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

En todo centro de informática se debe contar con una serie de políticas que permitan la mejor operación de los sistemas. Estas políticas son evaluadas durante el transcurso de la auditoría, por lo que sólo son mencionadas en esta sección, pero se encuentran estudiadas en detalle en diferentes capítulos.

Entre las políticas de operación del computador se encuentran las siguientes:

Políticas de respaldos

Los respaldos de la información deben realizarse mensual, semanal o diario, y se deben observar los siguientes puntos:

- Contar con políticas formales por escrito para efectuar los respaldos mensuales, semanales y diarios de la información.
- Todos los medios magnéticos de respaldo no deben estar almacenados en un mismo lugar, aunque se tengan los medios magnéticos de operación en el *site*, por lo que si hubiera una contingencia grave (incendio, inundación) no se tendría el riesgo de perder parte o la totalidad de la información, ya que se cuenta en otro lugar con los respaldos.
- Debe tenerse acceso restringido al área en donde se tienen almacenados los medios magnéticos, tanto de operación como de respaldo.
- Se deben tener identificadas las cintas por fecha, concepto y consecutivo, y es conveniente elaborar y actualizar una relación sobre las cintas, el contenido de los datos de registro y los responsables de efectuarlos.
- Se debe contar con una política que indique los procedimientos a seguir en cuanto al almacenamiento de las cintas de respaldo en un lugar diferente al

de la ubicación del *site*, en donde se pueda tener acceso las 24 horas del día y donde se designen responsables de mantener actualizada la información vital de la organización.

El hecho de no contar con estas políticas de respaldo que contemplen los puntos anteriores puede provocar que no se sigan los procedimientos adecuados para realizar los respaldos, que haya riesgo de pérdida de información en caso de alguna contingencia y no tener una disponibilidad inmediata de la información de respaldo para recuperar la información y conseguir una continuidad en la organización.

Se debe elaborar por escrito una serie de políticas y procedimientos para la elaboración de los respaldos, contemplando los pasos a seguir, la información que debe de ser respaldada, según el periodo correspondiente (mensual, semestral o anual), así como al personal asignado para cada caso.

También se debe especificar la forma de etiquetación, nomenclatura, pruebas, rotación de cintas, los nombres de los responsables de efectuar los respaldos y las cintas que serán designadas para ser resguardadas fuera de las instalaciones. También se debe tener una relación por escrito de la ubicación y el contenido de las cintas, que debe ser entregada al responsable de la seguridad del *site*, así como al gerente del área de informática.

Dentro de las políticas de respaldo, se debe contar con un punto que indique los procedimientos a seguir en cuanto al almacenamiento de las cintas de respaldo en un lugar diferente al de la ubicación del *site*, donde se pueda tener acceso las 24 horas del día y donde se designen responsabilidades de mantener actualizada la información vital de la organización.

Políticas para el computador

Políticas y procedimientos

Las políticas existentes deben estar actualizadas en todas las actividades, estar debidamente documentadas y ser del conocimiento del personal.

No contar con políticas y procedimientos actualizados que rijan la administración del área de sistemas podría ocasionar:

- Administración inadecuada de la operación.
- Relajamiento en el cumplimiento de las obligaciones del personal.
- Inadecuada división de labores.

Las políticas y procedimientos deben incluir los siguientes puntos:

- Seguridad de la información (física y lógica).
- Adquisición de hardware y software.
- Operación de centro de cómputo.

Es recomendable que se documenten todos los procedimientos de las diversas actividades. Éstos, al igual que las normas y políticas, se manifestarán por escrito en manuales de operación.

Al proceder de esta manera, se obtendrían las siguientes ventajas:

- Se tiene una base uniforme, estable y formal para capacitación, consulta y supervisión, y se fomenta la eficiencia del personal en sus funciones.
- Ante la rotación del personal, se evita el desvirtuamiento de las normas y procedimientos originales creados.
- Se precisa la responsabilidad individual de los participantes en una operación, en caso de errores y omisiones.

Además, dichas políticas y procedimientos a desarrollar, deberán ser del conocimiento del personal.

Política de revisión de bitácora (soporte técnico)

Deben existir bitácoras de operación en las que se registren los procesos realizados, los resultados de su ejecución, la concurrencia de errores, los procesos ejecutados en el equipo y la manera en que concluyeron.

No contar con una política de revisión de las bitácoras de operación de los diferentes procesos puede ocasionar problemas como:

- Carecer de bases para el rastreo de errores de procesamiento.
- Falta de parámetros de evaluación respecto al funcionamiento del equipo y del departamento de sistemas.
- Ausencia de controles en cuanto a registro de seguimiento de problemas.
- Falta de parámetros para determinar las causas de una falla significativa en el sistema y dar seguimiento a su corrección.
- Dependencia del personal para solución de errores.
- Los errores pueden presentarse en forma recurrente y no ser detectados, lo cual causa pérdidas de tiempo en la corrección.
- Puede presentarse una pérdida de tiempo al no programarse adecuadamente las funciones, lo que tiene como consecuencia una confusión en el área respecto a los procesos que ya se han realizado y los que se deban realizar.

Es necesario establecer una política de revisión de las bitácoras de operación, asignando responsables por proceso y función, lo que traería como beneficio detectar y corregir a buen tiempo los errores recurrentes y poder tomar medidas preventivas para que éstos ya no se presenten.

Para la adquisición, mantenimiento y desarrollo de sistemas se deben considerar:

Control de las licencias del software

Todas las organizaciones deben de tener un inventario de las licencias del software actualizado, que asegure que toda la paquetería y software en general sea

legal y
por pag

Al
provee
contar c
número
en una
muy fác
Por

- Act
- que
- esté
- En
- del
- más
- Elab
- paq
- Des
- ten
- Pro
- se i
- apli

Polític

Las inst
namien
y proce
deben c
Por
siguien

- El a
- una
- trol
- así
- tar
- Se c
- tade
- Deb
- mín
- El p
- tam
- No
- pot

legal y esté amparada por una licencia, para evitar posibles problemas legales por pago de derechos de uso y explotación del software.

Al no contar con las licencias correspondientes, no se le puede exigir al proveedor el servicio de soporte o actualización de software, ya que para poder contar con estos servicios es necesario presentar las licencias de adquisición o el número de serie instalado dentro de la licencia, el cual se encuentra clasificado en una base de datos dentro de los equipos del proveedor. Por tal motivo es muy fácil detectar si la licencia es pirata o ya venció.

Por ello, es muy importante:

- Actualizar el inventario de hardware y software, señalando los paquetes que se tienen instalados por máquina y verificando que cada uno de éstos esté amparado por una licencia.
- En caso de no contar con las licencias, es necesario contactar al proveedor del software o del paquete en cuestión para actualizarlas o adquirirlas lo más pronto posible.
- Elaborar un plan verificador de software, para revisar que no se instale paquetería pirata.
- Designar a una persona responsable del área de informática para guardar y tener actualizadas las licencias.
- Promover un plan de concientización entre el personal con el fin de que no se instale paquetería pirata en las máquinas propiedad de la empresa, y aplicar sanciones al personal que no acate estas medidas.

Políticas de seguridad física del *site*

Las instalaciones del *site* deben ser las adecuadas para asegurar el buen funcionamiento y la continuidad necesaria en las operaciones. Deben existir políticas y procedimientos que describan los aspectos de seguridad física mínimos que deben de regir dentro del departamento de sistemas.

Por tal motivo, durante la visita a las instalaciones se deben observar los siguientes puntos:

- El acceso al *site* debe estar restringido por una puerta, la cual contará con una chapa adecuada de seguridad, o con un dispositivo electrónico de control de acceso. Se deben tener dispositivos adecuados de detección de humo, así como aspersores de calor para la extinción de incendios, además de contar con extintores.
- Se debe tener protección en los servidores para que no puedan ser desconectados accidental o intencionalmente y provocar así serios daños al equipo.
- Deben existir documentos o carteles que indiquen las normas de seguridad mínima que deben de observarse al estar en el *site*.
- El personal operativo no debe permitir el acceso a personal ajeno al departamento.
- No debe tenerse papel para impresión dentro del *site*, el cual es un objeto potencial de algún desastre.

Cuidado del *site*

- Los equipos que se utilizan para la limpieza dentro del *site* no deben de estar directamente conectados a la toma de corriente en la que están conectados los equipos de cómputo y los servidores.
- Los equipos eléctricos, interruptores o de comunicación, no deben estar al alcance de cualquier persona.

Hay que elaborar políticas formales de seguridad y diseñar las características para el *site*, por lo que se recomienda lo siguiente:

- Seguridad física del centro de cómputo. Diseñar un lugar exclusivo y adecuado para los equipos centrales. Implementar dispositivos adecuados para la prevención y extinción de incendios que garanticen la salvaguarda del equipo e información que se encuentre dentro del *site*.
- Acceso al centro de cómputo. El acceso al centro de cómputo debe estar restringido por llaves electrónicas, chapas magnéticas, etc.; además, es necesario que se implemente algún procedimiento de control de acceso para personal no autorizado a las instalaciones. Asimismo, se debe de realizar una distribución correcta de las políticas y procedimientos de seguridad física, con el objetivo de que el personal conozca las responsabilidades y acciones que les corresponde, y con el fin de promover el cumplimiento de los objetivos y metas.
- Plan de contingencias. Debe existir un plan de contingencias que permita que los sistemas sigan funcionando en caso de algún siniestro o en caso de alguna huelga. Debe verificarse que se cumplan con todas las características que un documento de esta importancia requiere. Un plan de contingencias puede asegurar que se está preparado para enfrentar imprevistos y desastres de cualquier índole, asegurando una continuidad en la operación de los sistemas de cómputo. Ejemplos de contingencias pueden ser: incendios, tormentas, inundaciones y actos vandálicos, los cuales pueden ocasionar una disminución en el aprovechamiento de la computadora por un periodo considerable. Con la importancia y dependencia que se tiene de la computadora, una pérdida de información o la imposibilidad potencial para procesarla originada por una contingencia puede ser muy significativa. Se sugiere la revisión del plan de contingencias para que contenga los siguientes controles:
 - Delegación de funciones y entrenamiento de personal.
 - Resumen de actividades a seguir en caso de contingencias.
 - Estudio detallado de las que, de acuerdo con la zona geográfica, tienen más probabilidad de ocurrir y los impactos que cada una de éstas ocasionaría.
 - Realizar un estudio de tiempo estimado de restablecimiento de operaciones de acuerdo a una determinada contingencia, así como un estudio de consecuencias potenciales que se desprenderían por la inoperatividad de los sistemas.
 - Identificar las aplicaciones y archivos de datos críticos para la operación de los servicios computacionales, así como determinar las prioridades de restablecimiento de éstos. Se deben incluir especificaciones de hardware y software, tiempo de procesamiento, programa, archivos y documentación de programas y operación.

- Proveer los lineamientos necesarios para el restablecimiento de operaciones a partir de los respaldos de información.
- Desarrollo de pruebas periódicas del plan de contingencia, así como el establecimiento de niveles de autoridad y responsabilidades para garantizar el buen resultado de la prueba.
- Establecer procedimientos y responsabilidades para mantener el plan de contingencias.
- Procedimientos o planes para la reconstrucción de los *site* después de una contingencia.
- Establecimiento de procedimientos manuales de operación por parte de los usuarios para restablecer operaciones mientras se recuperan los sistemas.
- Lineamientos para garantizar que dicho plan sea probado y actualizado periódicamente.

El plan de contingencias, revisado y aprobado, debe ser distribuido a cada una de las áreas de la división de informática de la empresa y será dado a conocer a todo el personal que labora en ellas.

CONTROL DE DATOS FUENTE Y MANEJO DE CIFRAS DE CONTROL

La mayoría de los delitos por computadora son cometidos por modificaciones de datos fuente al:

- Suprimir u omitir datos.
- Adicionar datos.
- Alterar datos.
- Duplicar procesos.

Esto es de suma importancia en el caso de sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información. Por ello, se debe tener un adecuado control con señalamiento de responsables de los datos (uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a niveles.

El primer nivel es en el que se pueden hacer únicamente consultas; el segundo nivel es aquel en el que se puede hacer captura, modificaciones y consultas, y el tercer nivel es aquel en el que se puede hacer todo lo anterior y además se pueden realizar bajas.

NOTA: Debido a que se denomina de diferentes formas la actividad de transcribir la información del dato fuente a la computadora, sugerimos llamarla captura o captación, por considerarla considerándola como sinónimo de digitalizar (capturista, digitalizadora), anteriormente la responsabilidad de captura era del área de informática; en la actualidad es principalmente responsabilidad del usuario, pero esto no elimina la posibilidad de errores y consecuentemente la necesidad de auditar sus controles. Ahora existen diversas formas de captura de la

información, por ejemplo, scanners, pero debe existir una persona que sea responsable del control de esta información y asegúrese que es confiable y oportuna.

Lo primero que debemos evaluar es la entrada de la información y que se tengan las cifras de control necesarias para determinar la veracidad de ésta, para lo cual se puede utilizar el siguiente cuestionario, el cual está dirigido a la captura en el área de informática, independientemente de la captura que sea responsabilidad del usuario:

1. ¿Existen normas que definan el contenido de los instructivos de captación de datos?

2. Indique el porcentaje de datos que se reciben en el área de captación y verifique si contiene su instructivo correspondiente. En caso de que el usuario sea el responsable de la captura, debe existir un manual del usuario, o bien ayuda (*help*) dentro del sistema.

3. Indique el contenido de la orden de trabajo que se recibe en el área de captación de datos del área de informática:

Número de folio.	()	Fecha y hora de entrega de	
Fecha y hora de recepción.	()	documentos y registros	
Nombre del documento.	()	captados.	()
Volumen aproximado de	()	Clave del capturista.	()
registros.	()	Número(s) de formato(s).	()
Clave de cargo (número de		Nombre, departamento, usuario.	()
cuenta).	()	Nombre del responsable.	()
Número de registros.	()	Fecha estimada de entrega.	()

4. Indique cuál(es) control(es) interno(s) existe(n) en el área de captación de datos:

Firmas de autorización.	()	Verificación de cifras de	
Recepción de trabajos.	()	control de entrada con las	
Revisión del documento fuente		de salida.	()
(legibilidad, verificación de		Control de trabajos atrasados.	()
datos completos, etc.).	()	Avance de trabajos.	()
Prioridades de captación.	()	Verificación.	()
Producción de trabajo.	()	Errores por trabajo.	()
Costo mensual por trabajo.	()	Corrección de errores.	()
		Entrega de trabajos.	()

5. ¿Existe un programa de trabajo de captación de datos?

A) ¿Se elabora ese programa para cada turno?

Diariamente ()
Semanalmente ()
Mensualmente ()

B) La elaboración del programa de trabajo se hace:

Internamente ()
Se les señala a los usuarios las prioridades ()
Se les señala a los usuarios la posible fecha de entrega ()

C) ¿El programa de trabajo es congruente con el calendario de producción?
Sí () NO ()

D) Indique el contenido del programa de trabajo de captación.

Nombre de usuario.	()	Hora programada de entrega.	()
Clave de trabajo.	()	Volumen estimado de	
Fecha programada de		registros por trabajo.	()
recepción.	()	Fecha programada de	
Hora programada de recepción.	()	entrega.	()

E) ¿Qué acción(es) se toma(n) si el trabajo programado no se recibe a tiempo?

6. Cuando la carga de trabajo supera la capacidad instalada se requiere:

Tiempo extra. ()

Se subcontrata. ()

7. ¿Quién controla las entradas de documentos fuente?

8. ¿En qué forma las controla?

9. ¿Qué cifras de control se obtienen?

Sistema	Cifras que se obtienen	Observaciones
---------	---------------------------	---------------

10. ¿Qué documentos de entrada se tienen?

Sistemas	Documentos	Depto. que proporciona el documento	Periodicidad	Observaciones
----------	------------	---	--------------	---------------

11. ¿Se anota qué persona recibe la información y su volumen?

SÍ NO

12. ¿Se anota a qué capturista se entrega la información, el volumen y la hora?

SÍ NO

13. ¿Se verifica la calidad de la información recibida para su captura?

SÍ NO

14. ¿Se revisan las cifras de control antes de enviarlas a captura?

SÍ NO

15. ¿Para aquellos procesos que no traigan cifras de control se han establecido criterios a fin de asegurar que la información es completa y válida?

SÍ NO

16. ¿Existe un procedimiento escrito que indique cómo tratar la información inválida? (Sin firma, ilegible, no corresponden las cifras de control.) SÍ NO
17. En caso de resguardo de información de entrada en sistemas, ¿se custodian en un lugar seguro? SÍ NO
18. Si se queda en el departamento de sistemas, ¿por cuánto tiempo se guarda?

19. ¿Existe un registro de anomalías en la información debido a mala codificación? SÍ NO
20. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen? SÍ NO
21. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada? SÍ NO
22. ¿Se hace una relación de cuándo y a quién fueron distribuidos los listados? SÍ NO
23. ¿Se controlan separadamente los documentos confidenciales? SÍ NO
24. ¿Se aprovecha adecuadamente el papel de los listados inservibles? SÍ NO
25. ¿Existe un registro de los documentos que entran a captura? SÍ NO
26. ¿Se hace un reporte diario, semanal o mensual de captura? SÍ NO
27. ¿Se hace un reporte diario, semanal o mensual de anomalías en la información de entrada? SÍ NO
28. ¿Se lleva un control de la producción por persona? SÍ NO
29. ¿Quién revisa este control?

30. ¿Existen instrucciones escritas para capturar cada aplicación o, en su defecto, existe una relación de programas? SÍ NO

Véase en la figura 5.1 un ejemplo del formato de mesa de control.

Los sistemas en línea, redes y comunicación son evaluados en la sección de sistemas, y esta evaluación debe ser confirmada con el usuario.

CONTROL DE OPERACIÓN

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para

Figura 5.1. Mesa de control

FECHA	HOJA	DE
SISTEMA		
DIRECCIÓN		FORMULÓ

NÚM.	DOCUMENTOS FUENTE	ORIGEN	FRECUENCIA	RECEPCIÓN HORA LÍMITE

OPERACIÓN: REVISAR, CAPTURAR, PROCESAR, ETC.	TIEMPO	PERSONAL	HORA SAL

INSPECCIÓN DE REVISIÓN

REPORTE	REPORTE	REPORTE
DISTRIBUC. DÍA__ HORA __	DISTRIBUC. DÍA__ HORA __	DISTRIBUC. DÍA__ HORA __

Sistemas en lote

el proceso en la computadora. Los instructivos de operación proporcionan al operador información sobre los procedimientos que debe seguir en situaciones normales y anormales del procesamiento, y si la documentación es incompleta o inadecuada lo obliga a improvisar o suspender los procesos mientras investiga lo conducente, generando probablemente errores, reprocesos, desperdicio de tiempo de máquina; se incrementan, pues, los costos del procesamiento de datos.

Debemos de considerar la operación de los sistemas en línea, los cuales deben de estar residentes en todo momento, con su correspondiente sistema de comunicación, mientras que en cuanto a los sistemas en lote (*batch*) se debe planear y programar su operación. Para lograr esto existen instalaciones que tienen equipos de computación y comunicación dedicados exclusivamente a los sistemas en línea, y otros equipos dedicados únicamente a proceso en lotes (*batch*).

El objetivo del siguiente ejemplo de cuestionario es señalar los procedimientos e instructivos formales de operación de sistemas en lote (*batch*), analizar su estandarización y evaluar el cumplimiento de los mismos.

1. ¿Existen procedimientos formales para la operación del sistema de cómputo? SÍ NO
2. ¿Esos procedimientos describen detalladamente tanto la organización de la sala de máquinas como la operación del sistema de cómputo? SÍ NO
3. ¿Están actualizados los procedimientos? SÍ NO
4. Indique la periodicidad de la actualización de los procedimientos:

Semestral	()
Anual	()
Cada vez que haya cambio de equipo	()
5. Observe la forma en que está operando la máquina, ¿cómo se distribuyen los trabajos en lotes? ¿Cuál es el límite de trabajos en lotes y si se tiene un adecuado orden y control en los procesos por lotes? SÍ NO
6. Indique el contenido de los instructivos de operación para cada aplicación:

Identificación del sistema.	()
Periodicidad y duración de la corrida.	()
Especificación de formas especiales.	()
Etiquetas de archivos de salida, nombre del archivo lógico y fechas de creación y expiración.	()
Instructivo sobre materiales de entrada y salida.	()
Altos programados y las acciones requeridas.	()
Instructivos específicos para los operadores en caso de falla del equipo.	()
Puntos de reinicio, procedimientos de recuperación para proceso de gran duración o criterios.	()

Identificación de todos los dispositivos de la máquina a ser usados. ()
 Especificaciones de resultados (cifras de control, registros de salida por archivo, etc.). ()
 Instructivos de plan de contingencia. ()
 Instructivos de procedimientos de recuperación. ()

7. ¿Existen órdenes de proceso para cada corrida en computadora (incluyendo pruebas, compilaciones y producción)? SÍ NO
8. ¿Son suficientemente claras para los operadores estas órdenes? SÍ NO
9. ¿Existe una estandarización de las órdenes de proceso? SÍ NO
10. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están trabajando estén autorizados y tengan una razón de ser procesados. SÍ NO
11. ¿Cómo programan los operadores los trabajos dentro de la sala de máquinas?
- Primero que entra, primero que sale. ()
 Se respetan las prioridades. ()
 Otra (especifique).
12. ¿Los retrasos o incumplimiento del programa de operación diaria, se revisa y analiza? SÍ NO
13. ¿Quién revisa este reporte en su caso?
14. ¿Cómo controlan los operadores las versiones correctas y cómo se identifican las que son de prueba?
15. Analice la eficiencia con que se ejecutan los trabajos dentro de la sala de máquinas, tomando en cuenta equipo y operador, mediante una inspección visual, y describa sus observaciones.
16. ¿Existen procedimientos escritos para la recuperación del sistema en caso de fallas? SÍ NO
17. ¿Cómo se actúa en caso de errores?
18. ¿Existen instrucciones específicas para cada proceso, con las indicaciones pertinentes? SÍ NO
19. ¿Se tienen procedimientos específicos que indiquen al operador qué hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso? SÍ NO

- | | | |
|--|-----|----|
| 20. ¿Puede el operador modificar los datos de entrada? | SÍ | NO |
| 21. ¿Se prohíbe a analistas y otro personal ajeno al área la operación de la máquina? | SÍ | NO |
| 22. ¿Se prohíbe al operador modificar información de archivos o biblioteca de programas? | SÍ | NO |
| 23. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran? | SÍ | NO |
| 24. ¿Las intervenciones de los operadores: | | |
| Son muy numerosas? | SÍ | NO |
| Se limitan a los mensajes esenciales? | SÍ | NO |
| Otras? (especifique). | SÍ | NO |
| <hr/> | | |
| 25. ¿Se tiene un control adecuado sobre los sistemas que están en operación? | SÍ | NO |
| 26. ¿Cómo se controlan los trabajos dentro de la sala de máquinas? | | |
| <hr/> | | |
| 27. ¿Se rota al personal del control de información con los operadores, procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos? | SÍ | NO |
| 28. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos? | | |
| SI | | |
| Por máquina | () | |
| Escrita manualmente | () | |
| NO | | |
| 29. ¿Verifican que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software? | SÍ | NO |
| 30. ¿Existen procedimientos para evitar las corridas de programas no autorizados? | SÍ | NO |
| 31. ¿Existe un plan definido para el cambio de turno de operación que evite el descontrol y discontinuidad de la operación? | SÍ | NO |
| 32. ¿Verifican que sea razonable el plan para coordinar el cambio de turno? | SÍ | NO |
| 33. ¿Se hacen inspecciones periódicas de muestreo? | SÍ | NO |
| 34. Enuncie los procedimientos mencionados en el inciso anterior. | | |

35. ¿Se controla estrictamente el acceso a la documentación de aplicaciones rutinarias? SÍ NO

¿Cómo?

36. ¿Verifican que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador? SÍ NO

37. ¿Existen procedimientos formales que se deban observar antes de que se hayan aceptado en operación, sistemas nuevos o modificaciones a los mismos? SÍ NO

38. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores? SÍ NO

39. ¿Durante cuánto tiempo?
-

40. ¿Qué precauciones se toman durante el periodo de implantación?
-

41. ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación?
-

42. Mencione qué instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.
-

43. Indique qué tipo de controles se tienen sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.
-

44. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo? SÍ NO

45. Indique cómo está organizado este archivo de bitácora.

Por fecha	()
Por fecha y hora	()
Por turno de operación	()
Otros	()

46. ¿Cuál es la utilización sistemática de las bitácoras?
-

47. ¿Además de las mencionadas anteriormente, qué otras funciones o áreas se encuentran en la sala de máquinas actualmente?
-

48. ¿Se verifica que se lleve un registro de utilización del equipo diario, sistemas en línea y *batch*, de tal manera que se pueda medir la eficiencia del uso del equipo? sí NO

49. ¿Se tiene un inventario actualizado del total de los equipos, de su localización? sí NO

50. ¿Cómo se controlan los procesos en línea?

51. ¿Se tienen seguros sobre todos los equipos? sí NO

¿Con qué compañía?

Solicitar pólizas de seguros y verificar tipo de seguro y montos.

52. ¿Cómo se controlan las llaves de acceso (*password*)?

Se debe verificar que el instructivo de operación contenga los siguientes datos:

- Diagramas.
- Mensajes y su explicación.
- Parámetros y su explicación.
- Fórmulas de verificación.
- Observaciones e instrucciones en caso de error.
- Calendario de proceso y de entrega de resultados.

CONTROL DE SALIDA

Se ofrece el siguiente cuestionario en relación con el control de salida:

1. ¿Se tienen copias de los archivos magnéticos en otros locales?

sí NO

2. ¿Dónde se encuentran esos locales?

3. ¿Qué seguridad física se tiene en esos locales?

4. ¿Qué confidencialidad se tiene en esos locales?

5. ¿Quién entrega los documentos de salida de los procesos en lotes (*batch*)?

6. ¿En qué forma se entregan?

7. ¿Qué documentos?

Sistema	Documentos	A quién se entregan	Periodicidad	Observaciones
---------	------------	---------------------	--------------	---------------

8. ¿Qué controles se tienen?

Sistema	Control	Observaciones	Comentarios
---------	---------	---------------	-------------

9. ¿Se tiene un responsable (usuario) de la información de cada sistema en línea y en lotes (*batch*)?

SI NO

10. ¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?

11. ¿Se destruye la información no utilizada, o bien qué se hace con ella?

Destruye () Vende () Tira () Otro ()

CONTROL DE ASIGNACIÓN DE TRABAJO

Esta parte se relaciona con la dirección de las operaciones de la computadora en términos de la eficiencia y satisfacción del usuario. Esta sección debe ser comparada con la opinión del usuario. La función clave del personal de cargas de máquina está relacionada con el logro eficiente y efectivo de varios aspectos:

- Satisfacer las necesidades de tiempo del usuario.
- Ser compatible con los programas de recepción y transcripción de datos.
- Permitir niveles efectivos de utilización de los equipos y sistemas de operación.
- Volver la utilización de los equipos en línea.
- Entregar a tiempo y correctamente los procesos en lotes (*batch*).

La experiencia muestra que los mejores resultados se logran en organizaciones que utilizan sistemas formales de programación de actividades, los cuales intentan balancear los factores y medir resultados.

Se deberán evaluar los procedimientos de programación de cargas de máquina para determinar si se ha considerado atenuar los picos de los procesos generados por cierres mensuales, o bien los picos de los sistemas en línea, y poder

balancear las cargas de trabajo de lotes (*batch*) y línea, dando prioridad a los procesos en línea, o contar con equipos que permitan en forma independiente cumplir con las necesidades de procesos en línea, con su comunicación, y con procesos en lote.

En relación con los programas de trabajo proponemos el siguiente cuestionario:

1. ¿Opera la sala de máquinas sobre la base de programas de trabajo?

SÍ NO

2. Indique los periodos que abarcan los programas de trabajo.

3. Indique el puesto o departamento responsable de la elaboración de los programas de trabajo.

4. ¿Se cambian frecuentemente los programas de trabajo?

SÍ NO

5. ¿Cuál es la causa principal?

6. ¿Se comunica oportunamente a los usuarios las modificaciones a los programas de trabajo?

SÍ NO

¿Cómo se comunican?

7. Dentro del programa de trabajo de la máquina, ¿se tienen previstas:

- Demandas inesperadas? ()
- Fallas de la máquina? ()
- Soporte de los usuarios? ()
- Mantenimiento preventivo? ()
- Otras? (especifique). ()

8. ¿Con qué frecuencia se asigna la computadora, en su totalidad o en un gran porcentaje, para una sola aplicación (la de mayor utilización)?

9. Especifique los elementos que sirven como base para programar las cargas de máquina.

Se deberá procurar que la distribución física del equipo sea funcional, que la programación de las cargas de máquina satisfaga en forma eficaz al usuario. Asimismo, se tendrá cuidado con los controles que se tengan para la utilización de equipo y que el mantenimiento satisfaga las necesidades.

CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes, cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia en la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Además, se deben tener perfectamente identificados físicamente los archivos para reducir la posibilidad de utilización errónea o destrucción de la información.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de proceso.

El siguiente cuestionario puede ser extensivo a todo tipo de almacenamiento magnético; como ejemplo de formato para el análisis de archivos, véase figura 5.2.

1. Los locales asignados a almacenamientos magnéticos tienen:

- | | |
|-----------------------------------|-----|
| Aire acondicionado. | () |
| Protección contra el fuego | () |
| (señalar qué tipo de protección). | () |
| Cerradura especial. | () |
| Otro. | () |

2. ¿Tienen el almacén de archivos protección automática contra el fuego?

SÍ NO

(Señalar qué tipo.)

3. ¿Qué información mínima contiene el inventario de la cintoteca y la disco-teca?

- | | |
|-----------------------------------|-----|
| Número de serie o carrete. | () |
| Nombre o clave del usuario. | () |
| Nombre del archivo lógico. | () |
| Nombre del sistema que lo genera. | () |
| Fecha de generación del archivo. | () |
| Fecha de expiración del archivo. | () |
| Número de volumen. | () |
| Otras. | () |

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?

SÍ NO

5. En caso de existir discrepancia entre archivos y su contenido, ¿se resuelven y explican satisfactoriamente las discrepancias? SÍ NO

6. ¿Qué tan frecuentes son estas discrepancias?

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta o disco, el cual fue inadvertidamente destruido? SÍ NO

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso? SÍ NO

¿Cómo?

9. ¿Existe un control estricto de las copias de estos archivos? SÍ NO

10. ¿Qué medio se utiliza para almacenarlos?:

Mueble con cerradura. ()

Bóveda. ()

Otro (especifique).

11. Este almacén está situado:

En el mismo edificio de la dirección de informática. ()

En otro lugar. ()

Ambos. ()

12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan éstos? SÍ NO

¿Cuáles?

13. ¿Se certifica la destrucción o baja de los archivos defectuosos? SÍ NO

14. ¿Se registran como parte del inventario los nuevos elementos magnéticos que se reciben en la biblioteca? SÍ NO

15. ¿Se tiene un responsable, por turno, de los archivos magnéticos? SÍ NO

16. ¿Se realizan auditorías periódicas a los medios de almacenamiento? SÍ NO

¿Con qué periodicidad?

CONTROLES

17. ¿Qué medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, a cargo de personal autorizado? sí NO

19. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales? sí NO

20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán? sí NO

21. ¿Se lleva control sobre los archivos prestados por la instalación? sí NO

22. En caso de préstamo, ¿con qué información se documentan?

FORMATO PARA PRÉSTAMO

Nombre de la institución a quien se hace el préstamo.

Fecha de recepción	()
Fecha en que se debe devolver	()
Archivos que contiene	()
Formatos	()
Cifras de control	()
Código de grabación	()
Nombre del responsable que los prestó	()
Otros	()

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros.

24. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura? sí NO

25. ¿La operación de reemplazo es controlada por el cintotecario? sí NO

26. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo? sí NO

27. En los procesos que manejan archivos en línea, ¿existen procedimientos para recuperación de archivos? sí NO

28. ¿Estos procedimientos los conocen los operadores? sí NO

¿Cómo los consigue?

29. ¿Con qué periodicidad se revisan estos procedimientos?

- | | |
|------------|-----|
| Mensual. | () |
| Anual. | () |
| Semestral. | () |
| Otra. | () |

30. ¿Existe un responsable en caso de falla? SÍ NO

31. Explique qué políticas se siguen para la obtención de archivos de respaldo.

32. ¿Existe un procedimiento para el manejo de la información de la cintoteca? SÍ NO

33. ¿Lo conoce y lo sigue el cintotecario? SÍ NO

34. ¿Se distribuyen en forma periódica entre los jefes de sistemas informes de archivos para que liberen los dispositivos de almacenamiento? SÍ NO

¿Con qué frecuencia?

El objetivo del cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección. Al señalar archivos magnéticos nos referimos a cintas, discos, disquetes, CD, DVD y cualquier otro medio de almacenamiento masivo de información.

CONTROL DE MANTENIMIENTO

Existen básicamente tres tipos de contrato de mantenimiento. El contrato de mantenimiento total, que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no las incluye. El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente el más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización de los equipos. (Este tipo de mantenimiento normalmente se emplea en equipos grandes.)

El segundo tipo de mantenimiento es "por llamada", en el cual se llama al proveedor en caso de descompostura y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerla (casi todos los proveedores incluyen en la cotización de compostura el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer
aquel en el
una cotizac
refacciones
tadoras per

Al eval
pos es el qu
con detalle
tividad y q
tos que sea

Para p
control sob
Para ev
pueden uti

1. Espe
del c

2. ¿Exis
sister

3. ¿Se l

4. ¿Exis

5. Si los
¿qué

6. Solic
por e

7. ¿Exi
auto

¿Cu

¿Có

¿Có

1. ¿Se
siste
ene
(Sol

El tercer tipo de mantenimiento es el que se conoce como "en banco", y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y éste hace una cotización de acuerdo con el tiempo necesario para su compostura, más las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento debemos primero analizar cuál de los tres tipos es el que más nos conviene, y en segundo lugar pedir los contratos y revisar con detalle que las cláusulas estén perfectamente definidas, que no exista subjetividad y que haya penalización en caso de incumplimiento, para evitar contratos que sean parciales hacia el proveedor.

Para poder exigir el cumplimiento del contrato se debe tener un estricto control sobre las fallas, la frecuencia y el tiempo de reparación.

Para evaluar el control que se tiene sobre el mantenimiento y las fallas se pueden utilizar los siguientes cuestionarios:

1. Especifique el tipo de contrato de mantenimiento que se tiene (solicitar copia del contrato).

2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo? SÍ NO

3. ¿Se lleva a cabo tal programa? SÍ NO

4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos? SÍ NO

5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿qué acciones correctivas se toman para ajustarlos a lo convenido?

6. Solicite el plan de mantenimiento preventivo, que debe ser proporcionado por el proveedor.

7. ¿Existe algún tipo de mantenimiento preventivo que pueda dar el operador autorizado por el proveedor? SÍ NO

¿Cuál?

¿Cómo se notifican las fallas?

¿Cómo se les da seguimiento?

CONTROL DE FALLAS

1. ¿Se mantienen registros actualizados de las fallas de los dispositivos del sistema de cómputo y servicios auxiliares (aire acondicionado, sistema de energía ininterrumpida, etcétera)? SÍ NO
(Solicitar los registros de los últimos seis meses.)

- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

Eva
Cuan
dad
to pr
lació
que
trol
sión

2. ¿Es posible identificar por medio de estos registros los problemas más recurrentes o las fallas mayores que afectan en forma determinante el funcionamiento de la sala de máquinas? SÍ NO

¿Cómo se identifican?

3. Tiempo de respuesta promedio que se ha tenido con el contrato de mantenimiento (tiempo de respuesta es el periodo entre la notificación o aviso de la existencia de un problema y la llegada del personal técnico que realizó las reparaciones del equipo).

4. ¿Cuáles son las actitudes de los ingenieros de servicio que mantienen sus equipos?

5. ¿Cuál considera que es la competencia técnica de los ingenieros de servicio que dan mantenimiento a sus equipos? ¿Por qué?

6. ¿Cuál es el tiempo promedio que toma investigar y resolver el problema?

7. ¿Cuál es la disponibilidad de refacciones necesarias para dar mantenimiento a sus equipos?

8. ¿Cuál es la efectividad del proveedor para resolver sus problemas de mantenimiento?

9. ¿Cuáles son las medidas de mantenimiento preventivo realizadas al dar servicio a su equipo?

10. ¿Cuál es en general la calidad de los servicios ofrecidos bajo su "Contrato de mantenimiento"?

Evaluación del mantenimiento

Cuando se evalúa la capacidad de los equipos, no se debe olvidar que la capacidad bruta disponible se deberá disminuir por las actividades de mantenimiento preventivo, fallas internas y externas no previstas, y mantenimiento e instalación de nuevos sistemas.

El enfoque de esta sección se orienta a evaluar, mediante los controles que se tengan en la dirección, la utilización del sistema de cómputo. Un control adecuado permitirá sustentar sólidamente cualquier solicitud de expansión de la configuración presente. Se debe tener control de las fallas y del

mantenimiento no sólo del equipo central, sino del total de los equipos, incluyendo computadoras personales, impresoras, equipo de comunicación y periféricos.

El siguiente cuestionario sirve para evaluar el mantenimiento:

1. Indique los registros que se llevan de la utilización del sistema de cómputo (especificando la periodicidad).

Tiempo de prueba de programas.	()
Tiempo dedicado a producción.	()
Tiempo dedicado a mantenimiento correctivo del sistema operativo.	()
Tiempo dedicado a mantenimiento preventivo.	()
Tiempo de falla de los dispositivos del sistema de cómputo.	()
Tiempo de uso de cada unidad de cinta.	()
Tiempo ocioso.	()
Tiempo de uso de impresora.	()
Tiempo de reproceso.	()
Tiempo de la computadora utilizado en demostraciones.	()
Tiempo de falla por servicios auxiliares.	()

2. Anote los siguientes datos:

Tiempo promedio de operaciones por día. _____ hrs.

Tiempo promedio de respuesta para programas de producción. _____ hrs.

Número promedio al día que se consideran como horas de producción.

Número promedio de trabajos en cola de espera de ejecución en horas pico.

Número promedio de trabajos en cola de espera de impresión en horas pico.

Número promedio de trabajos de ejecución en horas pico.

3. Evalúe la relación de uso de impresoras respecto a la mezcla de trabajo. Determine si se debe:

• Incrementar el número de impresoras.	()
• Restaurar las cargas de trabajo.	()
• Utilizar otro tipo de salidas (diferentes a impresoras).	()
• Utilizar impresora de mayor velocidad.	()
• ¿Es excesivo el volumen de impresión?	SÍ NO

En caso de contestar sí, señale las causas:

Reportes muy largos.	()
Reportes no utilizados.	()
Procesos en lote que deben estar en línea.	()
Otros (especificar cuáles).	()

CONTROLES

- Especificar si existen procesos que deben cambiarse de *batch* a línea o viceversa.

4. Evalúe la utilización del sistema de cómputo a través de las siguientes relaciones:

Si el tiempo ocioso excede el 35%.

El equipo instalado puede estar sobrado de capacidad para la carga de trabajo actual.

Si el tiempo de mantenimiento al equipo sobrepasa el 5%.

Se deberá exigir al proveedor que mejore la calidad de soporte de mantenimiento.

Si el tiempo de falla del sistema de cómputo es mayor al 5%.

Se le deberá exigir la reparación y disminución de los tiempos de falla al proveedor.

NOTA: Éstos son solamente ejemplos de factores que pueden obtenerse, los cuales pueden ser ampliados, y los porcentajes dependerán del tipo de equipo y la experiencia que se tenga.

(Esta sección está orientada a revisar las acciones que realiza la dirección de informática para evaluar, mantener y auditar los sistemas implantados.)

5. Indique qué tipo de evaluación se realiza a los sistemas implantados:

Ninguna.	()	De objetivos.	()
Económica.	()	De oportunidad.	()
De beneficios.	()	De operación.	()
Otros (especificar).	()		

6. Indique qué instructivos se elaboran:

Interno del sistema (<i>help</i>).	()	De captación.	()
Del usuario.	()	De operación.	()
Otros (especificar).	()		

7. ¿Qué porcentaje del personal de programación se dedica a dar mantenimiento a los sistemas existentes?

8. ¿El responsable del área de producción formula las estadísticas de utilización de equipos, mostrando la frecuencia de fallas de los mismos y las estadísticas de producción por aplicación? (Especifique cómo se realiza y dé un ejemplo.)

SI NO

9. ¿En qué porcentaje se cumplen los calendarios de producción?

10. Existen:

- Programadores que utilizan el equipo o el tiempo para aplicaciones ajenas a la organización.
- Personal que utiliza la computadora para trabajos personales, trabajos no autorizados o juegos.
- Programas que, por estar mal elaborados (generalmente cuando se usan grandes archivos), degradan la máquina.
- Degradación del equipo por fallas en equipos periféricos. La computadora puede considerarse como un proceso en línea el cual, al fallar alguna de las unidades principales (*memoria, unidad central*), *no permite la utilización del resto del equipo*. Pero existen unidades secundarias (cintas, impresoras, terminales, discos) que al fallar provocan que se vea reducida la posibilidad de utilización del equipo.

Ejemplo

Si tenemos una impresora y se descompone, un alto porcentaje de utilización del equipo se ve disminuida, aunque el proveedor considere que sólo una unidad secundaria fue la dañada. Lo mismo sucede si se tienen dos unidades de disco y se descompone una (en caso de tener sólo una unidad de discos, la falla es total).

Para controlar este tipo de degradación se puede tener un reporte que contenga:

- Dispositivo que integra la configuración del equipo (por ejemplo, cinta, disco, impresora).
- Número del dispositivo; si tenemos por ejemplo 2 cintas, se anota 1 y 2, dependiendo de cuál fue la que falló.
- Tipo de falla. Se anotará una buena descripción del tipo de falla, para lo cual se puede elaborar un catálogo.
- Porcentaje de degradación. Este dato deberá ser anotado por los responsables de la dirección de informática basándose en la experiencia y en las implicaciones que tenga en el sistema total (por ejemplo, si se tienen 2 unidades de disco la degradación es del 50%, si se descomponen las dos es el 100% y si se tiene sólo una, también el 100%; en el caso de la impresora si se tiene sólo una puede ser el 66.6%, etc.).
- Número de horas que duró la falla, desde el momento de la descompostura hasta el momento en que la entregue reparada el proveedor.

ORDEN EN EL CENTRO DE CÓMPUTO

Una dirección de informática bien administrada debe tener y observar reglas relativas al orden y cuidado de la sala de máquinas. Los dispositivos del sistema de cómputo y los archivos magnéticos pueden ser dañados si se manejan en forma inadecuada, lo que puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Por ello, se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro de la sala de máquinas.

El siguiente cuestionario ayuda a evaluar el orden que existe en la sala de máquinas.

Cuidado de la sala de máquinas

1. Indique la periodicidad con que se hace la limpieza de la sala de máquinas y de la cámara de aire que se encuentra abajo del piso falso y los ductos de aire:

Semanalmente.	()	Quincenalmente.	()
Mensualmente.	()	Bimestralmente.	()
No hay programa.	()	Otro (especifique).	()

2. ¿Existe un lugar asignado a las cintas y discos magnéticos? SÍ NO
3. ¿Se tiene asignado un lugar específico para papelería y utensilios de trabajo? SÍ NO
4. ¿Son funcionales los muebles asignados para la cintoteca y discoteca? SÍ NO
5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etcétera? SÍ NO
6. Indique la periodicidad con que se limpian las unidades de cinta:
- | | | | |
|---------------------|-----|---------------------|-----|
| Al cambio de turno. | () | Cada semana. | () |
| Cada día. | () | Otra (especificar). | () |
7. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en la sala de máquinas? SÍ NO
8. ¿Se cuenta con carteles en lugares visibles que recuerden dicha prohibición? SÍ NO
9. ¿Se tiene restringida la operación del sistema de cómputo únicamente al personal especializado de la dirección de informática? SÍ NO
10. Mencione los casos en que personal ajeno al departamento de operación opera el sistema de cómputo.
11. Evalúe los niveles de iluminación y ruido y señale cuando estén fuera del rango estipulado en los estándares.

EVALUACIÓN DE LA CONFIGURACIÓN DEL SISTEMA DE CÓMPUTO

Los objetivos son evaluar la configuración actual, tomando en consideración las aplicaciones y el nivel de uso del sistema, evaluar el grado de eficiencia con el cual el sistema operativo satisface las necesidades de la instalación y revisar las

políticas seguidas por la unidad de informática en la conservación de su programación.

Esta sección está orientada a:

- Evaluar posibles cambios en el hardware a fin de nivelar el sistema de cómputo (computadoras, unidades periféricas, redes, sistemas de comunicación) con la carga de trabajo actual, o de comparar la capacidad instalada con los planes de desarrollo a mediano y largo plazos.
- Evaluar las posibilidades de modificar el equipo para reducir el costo o bien el tiempo de proceso.
- Evaluar la utilización de los diferentes dispositivos periféricos.

Ofrecemos el siguiente cuestionario, que sirve para hacer esas evaluaciones:

1. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo:

Con poco uso?	SÍ	NO
Ocioso?	SÍ	NO
Capacidad superior a la necesaria?	SÍ	NO

Describa cuál es:

2. ¿El equipo mencionado en el inciso anterior puede reemplazarse por otro más rápido y de menor costo?

SÍ NO

3. ¿El sistema de cómputo tiene capacidad de red?

SÍ NO

4. ¿Se utiliza la capacidad de red?

SÍ NO

5. En caso negativo, exponga los motivos por los cuales no se utiliza la red.

6. Especifique qué sistema de comunicación se tiene.

7. ¿Cuántas terminales, computadoras personales, periféricas, se tienen conectadas al sistema de cómputo?

Cantidad _____
Tipo _____

8. ¿Se ha investigado si el tiempo de respuesta satisface a los usuarios?

SÍ NO

9. Indique si existen políticas para aplicaciones soportadas en red:

Tamaño máximo de programas.	SÍ	NO
Número de archivos.	SÍ	NO
Tamaño máximo para cada archivo.	SÍ	NO
Nivel de acceso.	SÍ	NO

10. ¿El almacenamiento máximo del sistema de cómputo es suficiente para atender el proceso por lotes y en línea?

SÍ NO

El objetivo del siguiente cuestionario es evaluar la eficiencia con que opera el área de captación y producción.

1. Verifique que se cuente con una descripción completa de los trabajos que se corren y la descripción de las características de carga.
2. Verifique la existencia de un pronóstico de cargas o trabajos que se efectuarán durante el año, con el objeto de que se prevean los picos en las cargas de trabajo y se puedan distribuir adecuadamente estas cargas.
3. ¿Se tiene un programa de trabajo diario? ¿Semanal? ¿Anual?

SÍ NO
4. En caso de que no se tenga la programación diaria, ¿cómo se realiza la producción?

5. Verifique que se contemplen dentro de los planes de producción periodos de mantenimiento preventivo.
6. Verifique que se disponga de espacio y tiempo para realizar corridas especiales, corridas de prueba de sistemas en desarrollo y corridas que deben repetirse.
7. Verifique que se tengan definidos el espacio y el tiempo para el respaldo de la información.
8. Verifique el equipo de comunicación, características, número de usuarios y tiempo de respuesta que se obtiene en un proceso normal.
9. ¿Se tiene una programación del mantenimiento previo?

SÍ NO
10. ¿Se tiene un plan definido de respaldo de la información?

SÍ NO
11. ¿Se revisa el cumplimiento de los programas de producción establecidas?

SÍ NO
12. Verifique que se tenga conocimiento de los próximos sistemas que entrarán en producción, con objeto de que se programe su incorporación.

SÍ NO
13. ¿Quién revisa estos planes?

14. ¿Se cumplen generalmente estos planes? Si no, explique por qué.

SÍ NO

15. ¿Se repiten con frecuencia corridas por anomalías?

SÍ NO

16. Indique los estándares de producción que se tienen en la dirección de informática.

Por tipo de equipo ()

Por plataforma ()

17. ¿Existen índices de error aceptables para cada tipo de trabajo?

SÍ NO

18. ¿Cuándo fue la última revisión de esos estándares?

19. ¿El personal de captación conoce esos estándares?

SÍ NO

20. Indique los medios utilizados para medir la eficiencia de los operadores de captación.

Estadísticas mensuales de producción por trabajo y por operador. ()

Estadísticas mensuales de error por trabajo y por operador. ()

Estadísticas mensuales de producción por trabajo. ()

Estadísticas mensuales de error por trabajo. ()

Estadísticas de producción por trabajo y operador por hora. ()

Otros (especificar). ()

21. Indique qué medida(s) se toma(n) cuando el rendimiento para un trabajo está abajo del estándar:

Se consulta a los operadores sobre los problemas observados en el trabajo. ()

Se capacitan los operadores sobre el manejo del equipo. ()

Se imparten pláticas sobre el trabajo. ()

Otros. ()

22. ¿Se tienen incentivos para el personal que tenga un rendimiento superior al estándar?

SÍ NO

23. ¿Cada cuánto se imparten cursos de capacitación sobre la operación del equipo?

24. ¿Se registran los tiempos de respuesta a las solicitudes?

SÍ NO

25. ¿Cuál es el tiempo de respuesta promedio?

PUNTOS A EVALUAR EN LOS EQUIPOS

El equipo que se adquiere dentro de una organización debe de cumplir con el esquema de adquisición de toda la organización. En lo posible, se deben tener equipos estándares dentro de la organización, a menos que por requerimientos específicos se necesite un equipo con características distintas. Esto no implica que los equipos tengan que ser del mismo proveedor, aunque sí deben tener la misma

filoso
gan c
probl
E
cada
los c
requ
tador
equip
tador
facto
T
de da
incre
requi
tes p
L
evalu
equip
depe
tal en
tador
E
publi
ren e
con p
venta
así co
E
costo
tador
pode
sas a
estar
nefici
actua

Rent

Las c
pra, c
jas y
espec
super
E

- ¿I
- ¿C
- ¿E

filosofía. Las compras por impulso u oportunistas pueden provocar que se tengan diferentes equipos, modelos, estructuras y filosofías. Esto puede provocar problemas de falta de compatibilidad, expansión y de confianza.

Si no se tienen políticas y estándares de compra de equipos de cómputo, cada departamento o empleado puede decidir el adquirir diferentes equipos, los cuales pueden no ser compatibles, o bien el conocimiento y entrenamiento requerirá de mayor tiempo y costo. La conexión de un tipo de terminal o computadora personal a una computadora principal (*mainframe*) puede requerir de equipo o de software adicional. Los sistemas elaborados para un tipo de computadora pueden no servir en otro tipo de máquina. El mantenimiento es otro factor que puede incrementarse en caso de no tener compatibilidad de equipos.

Tener diferentes plataformas de programación, sistemas operativos, bases de datos, equipos de comunicación y lenguajes propietarios, provoca que se incrementen los costos, que se haga más problemático el mantenimiento, que se requiera personal con diferente preparación técnica, y que se necesiten diferentes programas de capacitación.

La posibilidad de que se pueda expandir un equipo es otro de los factores a evaluar. Al crecer una organización, es muy probable que se requiera que los equipos también crezcan y sean más rápidos. Esto es de mayor importancia dependiendo del tamaño de las computadoras, ya que es un factor fundamental en los grandes equipos y de relativamente poca importancia en las computadoras personales, debido a que no es tan alto su costo de reemplazo.

En muchas ocasiones se cambia o se compra una computadora por el factor publicitario, sin que se tenga la evaluación real de los equipos, o bien se adquieren equipos (principalmente computadoras personales) que son ensamblados con partes de diferentes proveedores a costos muy bajos. Se deberá evaluar la ventaja de adquirir lo último en tecnología, contra el costo que esto representa, así como el tener equipos muy baratos pero con baja confianza en el proveedor.

En la actualidad cada día las computadoras son más poderosas y menos costosas, y las organizaciones también cada día dependen más de las computadoras, así es que existe la tendencia de comprar cada día computadoras más poderosas, sin considerar que en el futuro existirán computadoras más poderosas a menor precio. La decisión de adquirir o cambiar una computadora deberá estar basada en un estudio muy detallado que demuestre el incremento de beneficios en relación con su costo, y en la relación costo/beneficio de los equipos actuales.

Renta, renta con opción a compra o compra

Las computadoras y el software pueden rentarse, rentarse con opción a compra, comprarse, y en el caso del software, producirse. Cada una tiene sus ventajas y desventajas, y es función del auditor el evaluar en cada instalación en específico por qué se escogió una opción, y si las ventajas que se obtienen son superiores a sus desventajas.

El auditor deberá evaluar:

- ¿Existe un comité de compra de equipo?
- ¿Quién participa en el comité?
- ¿Existen políticas de adquisición de equipos?

Adquisición
de equipos

- ¿Cómo se determina el proveedor del equipo?
- ¿Cómo se evalúan las propuestas de instalación, mantenimiento y entrenamiento?
- ¿Cómo se evalúa el costo de operación y el medio ambiente requerido para cada equipo?
- ¿Se evalúan las opciones de compra, renta y renta con opción a compra?

Los factores a considerar dentro de estas opciones son los siguientes:

Ventajas

- Renta:
 - Compromiso a corto plazo.
 - Menor riesgo de obsolescencia.
 - No requiere de inversión inicial.
- Renta con opción a compra:
 - Menor riesgo de obsolescencia.
 - No requiere de inversión inicial.
 - Se puede ejercer la opción de compra.
 - Los pagos normalmente incluyen servicios.
 - Menor costo que renta.
- Compra:
 - Se puede tener valor de recuperación.
 - Normalmente es menor su costo que el de compra a largo plazo.

Desventajas

- Renta:
 - Más caro que compra o renta con opción a compra.
 - El equipo puede ser usado.
 - Algunos vendedores de equipo no lo rentan.
- Renta con opción a compra:
 - Es más caro que compra.
 - No tiene valor de recuperación para el comprador.
- Compra:
 - Requiere de inversión inicial o de préstamo.
 - Amarra al comprador a su decisión.
 - El comprador debe conseguir u obtener servicio de mantenimiento.

Centralización vs. descentralización

El tener equipos en forma centralizada o descentralizada puede tener ventajas y desventajas, dependiendo del tipo de organización. El auditor deberá evaluar

a la organ
organizac
este punto
computad
usuario

Centraliz

- Venta
 - E
 - A
 - O
 - A
 - S
 - U
 - U
 - m
 - C
 - E
- Desv
 - F
 - si
 - L
 - se
 - P
 - l

Descentr

- Vent
 - A
 - M
 - F
 - A
 - I
 - c
 - C
 - c
 - C
 - t
- Desv
 - l
 -
 -
 -

a la organización y la justificación que se tiene para que en una determinada organización se tengan equipos en forma centralizada o descentralizada. En este punto se evalúan las grandes computadoras e instalaciones, eliminando las computadoras personales, ya que éstas deberán estar descentralizadas para cada usuario.

Centralización

- Ventajas:
 - Economía de escala.
 - Acceso a grandes capacidades.
 - Operaciones y administración más profesionales.
 - Accesos múltiples a datos comunes.
 - Seguridad, control y protección de los datos.
 - Un mejor reclutamiento y entrenamiento del personal especializado.
 - Una mejor planeación de la carrera profesional del personal de informática.
 - Control de los gastos de informática.
 - Estandarización de equipos y de software.
- Desventajas:
 - Falta de control de los usuarios sobre el desarrollo y operación de los sistemas.
 - La responsabilidad del desarrollo de los proyectos está limitada a un selecto personal.
 - Posible frustración dentro de la organización por desconocimiento de los cambios en los servicios de informática.

Descentralización de procesamiento de datos

- Ventajas:
 - Autonomía local y control por parte de los usuarios.
 - Mayor responsabilidad ante las necesidades de los usuarios.
 - Reducción de los costos de telecomunicación.
 - Acceso inmediato a las bases de datos descentralizadas.
 - Los analistas de sistemas locales tienen mayor atención a las necesidades de los usuarios.
 - Oportunidad de crear una carrera profesional dentro de las áreas funcionales de los usuarios.
 - Consistente con la descentralización establecida dentro de una estructura corporativa.
- Desventajas:
 - Pérdida de control gerencial central.
 - Posibilidad de incompatibilidad de datos, equipos y software.
 - Posibles errores para seguir los estándares de sistemas dentro de las prácticas de desarrollo.
 - Duplicación de personal y de esfuerzo.

6

CAPÍTULO

Evaluación de la seguridad

OBJETIVOS

Al finalizar este capítulo, usted:

1. Conocerá la importancia de salvaguardar la integridad de la información que se almacena en una computadora.
2. Explicará por qué es importante conservar la integridad, confidencialidad y disponibilidad de los sistemas de información.
3. Entenderá que un buen centro de cómputo depende, en gran medida, de la integridad, estabilidad y lealtad del personal.
4. Describirá las políticas, procedimientos y prácticas necesarios para mantener la seguridad física de un centro de cómputo.
5. Conocerá los distintos tipos de daños que provocan los virus en las computadoras, y las maneras de evitarlos.
6. Definirá las características de los seguros existentes para enfrentar los riesgos relacionados con los equipos de cómputo.
7. Explicará qué elementos deberán considerarse para tener una adecuada seguridad en el uso de los equipos y sistemas, así como en su restauración.

**Delitos
por computadora**

Las computadoras son un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Ante esta situación, en el transcurso de este siglo el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y derecho.

Imagínese que, por una u otra razón, el centro de cómputo o las librerías sean destruidos o usados inapropiadamente, ¿cuánto tiempo pasaría para que esta organización estuviese nuevamente en operación? El centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

En la situación actual de criminología, en los delitos de "cuello blanco" se incluye la modalidad de los delitos hechos mediante la computadora o los sistemas de información, de los cuales 95% de los detectados han sido descubiertos por accidente, y la gran mayoría no han sido divulgados para evitar dar ideas a personas mal intencionadas. Es así como la computadora ha modificado las circunstancias tradicionales del crimen. Muestra de ello son los fraudes, falsificaciones y venta de información hechos a las computadoras o por medio de éstas. Existen diferentes estimaciones sobre el costo de los delitos de cuello blanco, las cuales dependerán de la fuente que haga estas estimaciones, pero en todos los casos se considera que los delitos de cuello blanco en Estados Unidos superan los miles de millones de dólares.

Durante mucho tiempo se consideró que los procedimientos de auditoría y seguridad eran responsabilidad de la persona que elabora los sistemas, sin considerar que son responsabilidad del área de informática en cuanto a la elaboración de los sistemas, del usuario en cuanto a la utilización que se le dé a la información y a la forma de accederla, y del departamento de auditoría interna en cuanto a la supervisión y diseño de los controles necesarios.

La seguridad del área de informática tiene como objetivos:

- Proteger la integridad, exactitud y confidencialidad de la información.
- Proteger los activos ante desastres provocados por la mano del hombre y de actos hostiles.
- Proteger a la organización contra situaciones externas como desastres naturales y sabotajes.
- En caso de desastre, contar con los planes y políticas de contingencias para lograr una pronta recuperación.
- Contar con los seguros necesarios que cubran las pérdidas económicas en caso de desastre.

Los motivos de los delitos por computadora normalmente son por:

- Beneficio personal. Obtener un beneficio, ya sea económico, político social o de poder, dentro de la organización.
- Beneficios para la organización. Se considera que al cometer algún delito en otra computadora se ayudará al desempeño de la organización en la cual se trabaja, sin evaluar sus repercusiones.

- Síndrome de Robin Hood (por beneficiar a otras personas). Se están haciendo copias ilegales por considerar que al infectar a las computadoras, o bien al alterar la información, se ayudará a otras personas.
- Jugando a jugar. Como diversión o pasatiempo.
- Fácil de desfalcar.
- El individuo tiene problemas financieros.
- La computadora no tiene sentimientos. La computadora es una herramienta que es fácil de desfalcar, y es un reto poder hacerlo.
- El departamento es deshonesto.
- Odio a la organización (revancha). Se considera que el departamento o la organización es deshonesto, ya que no ha proporcionado todos los beneficios a los que se tiene derecho.
- Equivocación de ego (deseo de sobresalir en alguna forma).
- Mentalidad turbada. Existen individuos con problemas de personalidad que ven en elaborar un virus un reto y una superación, los cuales llegan a ser tan cínicos que ponen su nombre y dirección en el virus, para lograr ese reconocimiento.

En la actualidad, principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente en paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Se trata de pequeñas subrutinas escondidas en los programas que se activan cuando se cumple alguna condición, por ejemplo, haber obtenido una copia en forma ilegal, y puede ejecutarse en una fecha o situación predeterminada. El virus normalmente es puesto por los diseñadores de algún tipo de programa (software) para "castigar" a quienes lo roban o copian sin autorización o bien por alguna actitud de venganza en contra de la organización. (En la actualidad existen varios productos para detectar los virus.)

Existen varios tipos de virus pero casi todos actúan como "caballos de Troya", es decir, se encuentran dentro de un programa y actúan con determinada indicación.

Un ejemplo es la destrucción de la información de la compañía USPA & IRA de Forth Worth. Cuando despidieron a un programador en 1985, éste dejó una subrutina que destruía mensualmente la información de las ventas. Este incidente provocó el primer juicio en Estados Unidos contra una persona por sabotaje a una computadora.

Al auditar los sistemas, se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. También se debe cuidar que en ocasiones se toma como pretexto el virus y se producen efectos psicológicos en los usuarios, ya que en el momento de una falla de la computadora o del sistema, lo primero que se piensa es que están infectados.

Se considera que hay cinco factores que han permitido el incremento en los crímenes por computadora:

- El aumento del número de personas que se encuentran estudiando computación.

Los virus

- El aumento del número de empleados que tienen acceso a los equipos.
- La facilidad en el uso de los equipos de cómputo.
- El incremento en la concentración del número de aplicaciones y, consecuentemente, de la información.
- El incremento de redes y de facilidades para utilizar las computadoras en cualquier lugar y tiempo.

Estos cinco factores, aunque son objetivos de todo centro de cómputo, también constituyen una posibilidad de uso con fines delictivos.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos al de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor, hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos. Estos delitos pueden ser cometidos por personas que no desean causar un mal.

En la actualidad las compañías cuentan con grandes dispositivos para la seguridad física de las computadoras, y se tiene la idea que los sistemas no pueden ser violados si no se entra al centro de cómputo, olvidando que se pueden usar terminales y sistemas remotos de teleproceso. Se piensa, como en el caso de la seguridad ante incendio o robo, que "eso no me puede suceder a mí o es poco probable que suceda aquí".

Algunos gerentes creen que las computadoras y sus programas son tan complejos que nadie fuera de su organización los va a entender y no les van a servir. Pero en la actualidad existe un gran número de personas que puede captar y usar la información que contiene un sistema y considerar que hacer esto es como un segundo ingreso. También se ha detectado que el mayor número de fraudes, destrucción de información o uso ilegal de ésta, provienen del personal interno de una organización. También se debe considerar que gran parte de los fraudes hechos por computadora o el mal uso de ésta son realizados por personal de la misma organización.

En forma paralela al aumento de los fraudes hechos a los sistemas computarizados, se han perfeccionado los sistemas de seguridad tanto física como lógica; la gran desventaja del aumento en la seguridad lógica es que se requiere consumir un número mayor de recursos de cómputo para lograr tener una idónea seguridad, lo ideal es encontrar un sistema de acceso adecuado al nivel de seguridad requerido por el sistema con el menor costo posible. En los desfalcos por computadora (desde un punto de vista técnico), hay que tener cuidado con los "caballos de Troya" que son programas a los que se les encajan rutinas que serán activadas con una señal específica.

SEGURIDAD LÓGICA Y CONFIDENCIALIDAD

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de una compu-

tadora, así como de controlar el mal uso de la información. Estos controles reducen el riesgo de caer en situaciones adversas.

Se puede decir entonces que un inadecuado control de acceso lógico incrementa el potencial de la organización para perder información, o bien para que ésta sea utilizada en forma inadecuada; asimismo, esto hace que se vea disminuida su defensa ante competidores, el crimen organizado, personal desleal y violaciones accidentales.

La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el software de desarrollo y por los programas en aplicación; identifica individualmente a cada usuario y sus actividades en el sistema, y restringe el acceso a datos, a los programas de uso general, de uso específico, de las redes y terminales.

La falta de seguridad lógica o su violación puede traer las siguientes consecuencias a la organización:

- Cambio de los datos antes o cuando se le da entrada a la computadora.
- Copias de programas y/o información.
- Código oculto en un programa.
- Entrada de virus.

La seguridad lógica puede evitar una afectación de pérdida de registros, y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.

El tipo de seguridad puede comenzar desde la simple llave de acceso (contraseña o *password*) hasta los sistemas más complicados, pero se debe evaluar que cuanto más complicados sean los dispositivos de seguridad más costosos resultan. Por lo tanto, se debe mantener una adecuada relación de seguridad-costeo en los sistemas de información.

Los sistemas de seguridad normalmente no consideran la posibilidad de fraude cometida por los empleados en el desarrollo de sus funciones. La introducción de información confidencial a la computadora puede provocar que ésta esté concentrada en manos de unas cuantas personas, por lo que existe una alta dependencia en caso de pérdida de los registros. El más común de estos delitos se presenta en el momento de la programación, en el cual por medio de ciertos algoritmos se manda borrar un archivo. Por ejemplo, al momento de programar un sistema de nómina se puede incluir una rutina que verifique si se tiene dentro del archivo de empleados el registro federal de causantes del programador. En caso de existir, continúa el proceso normalmente; si no existe significa que el programador que elaboró el sistema renunció o fue despedido y en ese momento pudo borrar todos los archivos. Esta rutina, aunque es fácil de detectar, puede provocar muchos problemas, en caso de que no se tenga los programas fuente o bien que no se encuentren debidamente documentados. También en el caso de programadores honestos, en ocasiones en forma no intencional, se pueden tener fallas o negligencia en los sistemas. La dependencia de ciertos individuos clave, algunos de los cuales tienen un alto nivel técnico, comúnmente pone a la organización en manos de unas cuantas personas, las cuales suelen ser las únicas que conocen los sistemas debido a que no los documentan.

**Control
de acceso**

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho de manera simple, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden al usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de los clientes alguno de estos paquetes. Sin embargo, los paquetes de control de acceso basados en contraseñas pueden ser eludidos por delincuentes sofisticados en computación, por lo que no es conveniente depender de esos paquetes por sí solos para tener una seguridad adecuada.

El sistema integral de seguridad debe comprender:

- Elementos administrativos.
- Definición de una política de seguridad.
- Organización y división de responsabilidades.

SEGURIDAD LÓGICA

Uno de los puntos más importantes a considerar para poder definir la seguridad de un sistema es el grado de actuación que puede tener un usuario dentro de un sistema, ya sea que la información se encuentre en un archivo normal o en una base de datos, o bien que se posea una minicomputadora, o un sistema en red (interna o externa). Para esto podemos definir los siguientes tipos de usuarios:

Tipos de usuarios

- *Propietario.* Es, como su nombre lo indica, el dueño de la información, el responsable de ésta, y puede realizar cualquier función (consultar, modificar, actualizar, dar autorización de entrada a otro usuario). Es responsable de la seguridad lógica, en cuanto puede realizar cualquier acción y puede autorizar a otros usuarios de acuerdo con el nivel que desee darles.
- *Administrador.* Sólo puede actualizar o modificar el software con la debida autorización, pero no puede modificar la información. Es responsable de la seguridad lógica y de la integridad de los datos.
- *Usuario principal.* Está autorizado por el propietario para hacer modificaciones, cambios, lectura y utilización de los datos, pero no puede dar autorización para que otros usuarios entren.
- *Usuario de consulta.* Sólo puede leer la información pero no puede modificarla.
- *Usuario de explotación.* Puede leer la información y utilizarla para explotación de la misma, principalmente para hacer reportes de diferente índole, los cuales, por ejemplo, pueden ser contables o estadísticos.
- *Usuario de auditoría.* Puede utilizar la información y rastrearla dentro del sistema para fines de auditoría.

Los usuarios pueden ser múltiples, y pueden ser el resultado de la combinación de los antes señalados. Se recomienda que exista sólo un usuario propietario, y que el administrador sea una persona designada por la gerencia de informática.

Para conservar la integridad, confidencialidad y disponibilidad de los sistemas de información se debe tomar en cuenta lo siguiente:

- La *integridad* es responsabilidad de los individuos autorizados para modificar datos o programas (usuario administrador) o de los usuarios a los que se otorgan accesos a aplicaciones de sistema o funciones fuera de sus responsabilidades normales de trabajo (usuario responsable y principal).
- La *confidencialidad* es responsabilidad de los individuos autorizados para consultar (usuario de consulta) o para bajar archivos importantes para microcomputadoras (usuario de explotación).
- La *disponibilidad* es responsabilidad de individuos autorizados para alterar los parámetros de control de acceso al sistema operativo, al sistema manejador de base de datos, al monitoreo de teleproceso o al software de telecomunicaciones (usuario administrador).

El control implantado para minimizar estos riesgos debe considerar los siguientes factores:

- El valor de los datos siendo procesados.
- La probabilidad de que ocurra un acceso no autorizado.
- Las consecuencias para la organización si ocurre un acceso no autorizado.
- El riesgo y repercusiones en caso de que un usuario no autorizado utilice la información.

La seguridad lógica abarca las siguientes áreas:

- Rutas de acceso.
- Claves de acceso.
- Software de control de acceso.
- Encriptamiento.

Rutas de acceso

El acceso a la computadora no significa tener una entrada sin restricciones. Limitar el acceso sólo a los niveles apropiados puede proporcionar una mayor seguridad.

El objetivo de la seguridad de los sistemas de información es controlar las operaciones y su ambiente mediante el monitoreo del acceso a la información y a los programas, para poder darle un seguimiento y determinar la causa probable de desviaciones. Por ello es conveniente al utilizar algún tipo de software dentro de un sistema, contar con una ruta de acceso.

Control
de acceso

Cada uno de los sistemas de información tiene una ruta de acceso, la cual puede definirse como la trayectoria seguida en el momento de acceso al sistema.

Como se ha señalado, un usuario puede pasar por uno o múltiples niveles de seguridad antes de obtener el acceso a los programas y datos. Los tipos de restricciones de acceso son:

- Sólo lectura.
- Sólo consulta.
- Lectura y consulta.
- Lectura y escritura, para crear, actualizar, borrar, ejecutar o copiar.

El esquema identifica a los usuarios del sistema, los tipos de dispositivos por los cuales se accesa al sistema, el software usado para el acceso al sistema, los recursos que pueden ser accedidos y los sistemas donde residen estos recursos. Los sistemas pueden ser en línea, fuera de línea, en *batch*, y rutas de telecomunicación.

El esquema de las rutas de acceso sirve para identificar todos los puntos de control que pueden ser usados para proteger los datos en el sistema. El auditor debe conocer las rutas de acceso para la evaluación de los puntos de control apropiados.

Claves de acceso

Un área importante en la seguridad lógica es el control de las claves de acceso de los usuarios. Existen diferentes métodos de identificación para el usuario:

- Un *password* o código.
- Una credencial con banda magnética.
- Algo específico del usuario (características propias).

La identificación es definida como el proceso de distinción de un usuario de otros. La identificación de entrada proporcionará un reconocimiento individual; cada usuario debe tener una identificación de entrada única que debe ser reconocida por el sistema.

Password, código o llaves de acceso. La identificación de los individuos es usualmente conocida y está asociada con un *password* o clave de acceso. Las claves de acceso pueden ser usadas para controlar el acceso a la computadora, a sus recursos, así como definir nivel de acceso o funciones específicas.

Las llaves de acceso deben tener las siguientes características:

- El sistema debe verificar primero que el usuario tenga una llave de acceso válida.
- La llave de acceso debe ser de una longitud adecuada para ser un secreto.
- La llave de acceso no debe ser desplegada cuando es tecleada.

Identificación
del usuario

- Las llaves de acceso deben ser encriptadas, ya que esto reduce el riesgo de que alguien obtenga la llave de acceso de otras personas.
- Las llaves de acceso deben de prohibir el uso de nombres, palabras o cadenas de caracteres difíciles de retener, además el *password* no debe ser cambiado por un valor pasado. Se recomienda la combinación de caracteres alfabéticos y numéricos. No debe ser particularmente identificable con el usuario, como su nombre, apellido o fecha de nacimiento.

Credenciales con banda magnética. La banda magnética de las credenciales es frecuentemente usada para la entrada al sistema. Esta credencial es como una bancaria, pero se recomienda que tenga fotografía y firma.

La ventaja más importante de la credencial es prevenir la entrada de impostores al sistema. Una credencial ordinaria es fácil de falsificar, por lo que se debe elaborar de una manera especial, que no permita que sea reproducida.

Validación por características. Es un método para la identificación del usuario, que es implantado con tecnología biométrica. Consiste en la verificación y reconocimiento de la identidad de las personas, basándose en características propias. Algunos de los dispositivos biométricos son:

- Las huellas dactilares.
- La retina.
- La geometría de la mano.
- La firma.
- La voz.

Software de control de acceso

Éste puede ser definido como el software diseñado para permitir el manejo y control del acceso a los siguientes recursos:

- Programas de librerías.
- Archivos de datos.
- *Jobs*.
- Programas en aplicación.
- Módulos de funciones.
- Utilerías.
- Diccionario de datos.
- Archivos.
- Programas.
- Comunicación.

Controla el acceso a la información, grabando e investigando los eventos realizados y el acceso a los recursos, por medio de la identificación del usuario.

El software de control de acceso, tiene las siguientes funciones:

- Definición de usuarios.
- Definición de las funciones del usuario después de acceder el sistema.
- Establecimiento de auditoría a través del uso del sistema.

El software de seguridad protege los recursos mediante la identificación de los usuarios autorizados con las llaves de acceso, que son archivadas y guardadas por este software.

Esto puede ser efectuado a través de la creación de archivos o tablas de seguridad. Los paquetes de seguridad frecuentemente incluyen facilidades para encriptar estas tablas o archivos.

A cada usuario se le debe asignar un alcance en el acceso y por cada recurso un grado de protección, para que los recursos puedan ser protegidos de un acceso no autorizado.

Algunos paquetes de seguridad pueden ser usados para restringir el acceso a programas, librerías y archivos de datos; otros pueden además limitar el uso de terminales o restringir el acceso a bases de datos, y existen otros más para confirmar y evaluar la autorización de la terminal remota para utilizar determinada información. Éstos pueden variar en el nivel de la seguridad brindada a los archivos de datos. La seguridad puede estar basada en el tipo de acceso: usuarios autorizados para agregar registros a un archivo o los que únicamente leen registros.

La mayor ventaja del software de seguridad es la capacidad para proteger los recursos de accesos no autorizados, incluyendo los siguientes:

- Procesos en espera de modificación por un programa de aplicación.
- Accesos por los editores en línea.
- Accesos por utilerías de software.
- Accesos a archivos de las bases de datos, a través de un manejador de base de datos (DBMS).
- Acceso de terminales o estaciones no autorizadas.

Estos paquetes pueden restringir el acceso a los recursos (archivos de datos), reduciendo así el riesgo de los accesos no autorizados.

En el caso de terminales de compra de boletos de pronósticos, se puede restringir la entrada a terminales no autorizadas o en tiempo no autorizado.

Otra característica de estos paquetes es que se pueden detectar las violaciones de seguridad, tomando las siguientes medidas:

- Terminaciones de procesos.
- Forzar a las terminales a apagarse.
- Desplegar mensajes de error.
- Escribir los registros para la auditoría.

La bitácora de auditoría es seleccionada durante la implementación.

La bitácora puede consistir en registrar los accesos no exitosos, sólo los intentos, un registro de todos los accesos válidos y los recursos protegidos.

Paquetes de seguridad

Ejemplo

Ejemplo

Algunos paquetes contienen datos específicos para ser incluidos en la bitácora de auditoría.

Cada bitácora debe incluir la identificación del usuario: si el acceso es exitoso, deben consignarse los recursos accedidos, día, hora, terminal y un dato específico de lo que fue modificado durante el acceso; si el acceso no fue exitoso la mayor información posible sobre día, hora, terminal y claves de intento usadas.

Otros tipos de software de control de acceso

Algunos tipos de software son diseñados con características que pueden ser usadas para proveerles seguridad. Sin embargo, es preferible usar un software de control de acceso para asegurar el ambiente total y completar las características de seguridad con un software específico.

Como existen diferentes tipos de software, explicaremos las características de seguridad de los siguientes:

- Sistemas operativos.
- Manejadores de bases de datos.
- Software de consolas o terminales maestras.
- Software de librerías.
- Software de utilerías.
- Telecomunicaciones.

A) Sistemas operativos

Se trata de una serie de programas que se encuentran dentro de los sistemas operativos, los cuales manejan los recursos de las computadoras y sirven como interfase entre el software de aplicaciones y el hardware.

Estos programas proporcionan seguridad ya que, internamente, dentro de los sistemas operativos manejan y controlan la ejecución de programas de aplicación y proveen los servicios que estos programas requieren, dependiendo del usuario y del sistema que se esté trabajando. Cada servicio debe incluir un calendario de trabajo (*Job Schedule*), manejador de equipos periféricos, un contador de trabajo y un compilador de programas, pruebas y *debugs* (depuraciones). El grado de protección sobre estos servicios depende de los sistemas operativos.

Los elementos de seguridad de los sistemas operativos incluyen lo siguiente:

- Control de salidas de los programas al modificarse códigos. Éstos usualmente tienen accesos a los elementos más importantes del sistema, y sus actividades deben ser monitoreadas.
- Los sistemas operativos usan claves de acceso (*passwords*, ID) para prevenir usuarios no autorizados a funciones y utilerías del sistema operativo. Muchas veces, estas claves de acceso están definidas en una tabla del sistema

que es activada cuando un sistema es utilizado. Las claves de acceso deben ser cambiadas inmediatamente por las nuevas claves de acceso.

- Algunos sistemas operativos proveen una característica que puede limitar el número de accesos no autorizados y autorizar usuarios a los recursos protegidos, si este número es excedido, el usuario no autorizado es prevenido para el nuevo acceso a estos recursos.
- Los sistemas operativos permiten una instalación para la implementación opcional de características de seguridad cuando el sistema es instalado. Algunos sistemas operativos contienen sus propias características de seguridad y muchas veces éstas no son adecuadas; en este caso es aconsejable integrar al sistema operativo un software de seguridad para proteger los recursos. El valor de éstos es un factor determinante cuando se decide qué tanta protección es necesaria.
- Los sistemas operativos tienen un completo control sobre las actividades de todas las aplicaciones que están corriendo en el sistema. Si un usuario no autorizado puede lograr acceder a los recursos del sistema operativo, puede hacer modificaciones que alteren el proceso normal del flujo del sistema. El sistema operativo tiene autoridad para dar facilidades de seguridad y para acceder recursos confidenciales. Esto implica que en algunas ocasiones se requerirá del uso de algún producto de seguridad adicional. El software de funciones de control del sistema operativo debe proveer una bitácora de auditoría.
- Tanto el administrador del sistema o el administrador de la seguridad de datos establecen sus privilegios a través del sistema operativo. Individualmente, con estos privilegios tienen completo control sobre el sistema operativo y su ambiente; ellos pueden otorgar la autoridad para modificar usuarios y acceder secciones, alterar la generación de procedimientos del sistema y modificar las prioridades de trabajos (*jobs*) que corren dentro del control del sistema. Debe existir una bitácora de las actividades del administrador del sistema o del administrador de la seguridad de datos.
- Los sistemas operativos permiten la definición de consolas o terminales maestras desde las cuales los operadores pueden introducir comandos al sistema operativo. Las consolas no requieren una señal en proceso para la emisión de comandos. Por lo tanto, el acceso a áreas físicas en donde están las consolas debe ser restringido. Además, las características del sistema que permiten a una terminal ser asignada con el estatus de consola deben ser guardadas a prueba de accesos no autorizados.

B) Software manejador de base de datos

Es un software cuya finalidad es la de controlar, organizar y manipular los datos. Provee múltiples caminos para acceder los datos en una base de datos. Maneja la integridad de datos entre operaciones, funciones y tareas de la organización.

Cuando un usuario inicialmente requiere del uso del sistema de administración de bases de datos (*Data Base Management System, DBMS*) se establece un identificador para el usuario y la sesión. Inmediatamente, el usuario puede ser identificado por el ID-usuario, ID-terminal, y por una aplicación o función.

En espera del modo de modificaciones, el usuario podrá ser identificado por el trabajo (*job*), por la aplicación o por la función.

El identificador del usuario será usado para rastrear todos los accesos a los archivos de datos a través del administrador de la base de datos (DBMS).

Las características de seguridad del software DBMS pueden ser usadas para restringir el acceso a un usuario específico, a un cierto archivo o a vistas lógicas, los accesos a procedimientos, funciones o software en aplicaciones limitado a usuarios autorizados con el propósito de ejecutar sus tareas asignadas. Las vistas de datos lógicos están colocadas en archivos para usuarios particulares, funciones o aplicaciones, y puede ser representado todo o parte del archivo de datos físicos o una combinación de campos de múltiples archivos de datos físicos. Estas características son usadas para controlar funciones únicas en el administrador de la base de datos (DBMS).

Las utilerías de la base de datos proveen funciones de mantenimiento, como respaldos y restauración de la base de datos, reorganización de datos, reportes estadísticos de las bases de datos y sus relaciones. Éstos pueden ser usados además para adicionar o borrar datos y proveer seguridad.

El diccionario de datos (DD) es un software que guía y provee un método para documentar elementos de la base de datos, así como un método de seguridad de datos en un administrador de bases de datos (DBMS).

Todas las modificaciones al directorio de datos (DD) deben producir una bitácora de auditoría, como un registro automático de todos los cambios y un medio de recuperación después de alguna interrupción que hubiese ocurrido.

C) Software de consolas o terminales maestras

El software de consolas o terminales maestras puede ser definido como varios programas del sistema operativo que proveen soporte y servicio para que las terminales en línea accesen a los programas en aplicación.

Las consolas incluyen funciones de seguridad para restringir el acceso a los datos, vía programas en aplicación.

Estas funciones frecuentemente están basadas en una serie de tablas que definen a los usuarios autorizados, así como los recursos y programas en aplicación que ellos pueden acceder. Generalmente las consolas pueden sólo limitar el acceso al usuario para entrar a un programa en aplicación, no para el uso de funciones específicas de un programa.

La mayor parte de las consolas mantienen un registro de uso de llaves de acceso (*password*) diario válidas o no válidas.

D) Software de librerías

El software de librerías consta de datos y programas específicos escritos para ejecutar una función en la organización.

Los programas en aplicación (librerías) pueden ser guardados en archivos en el sistema, y el acceso a estos programas puede ser controlado por medio del software (software de control de acceso general) usado para controlar el acceso a estos archivos.

El software de manejo de librerías puede ser usado para mantener y proteger los recursos de programas de librerías, la ejecución de *jobs*, y en algunas instancias, los archivos de datos pueden ser utilizados por éstas.

Estas librerías deben ser soportadas por un adecuado control de cambios y procedimientos de documentación.

Una importante función del software controlador de librerías es controlar y describir los cambios de programas en una bitácora. El software de librerías provee diferentes niveles de seguridad, los cuales se reflejan en las bitácoras de auditoría.

Los controles de cambios de emergencia deben estar en algún lugar debido a la naturaleza de estos cambios (frecuentemente son realizados fuera de horas de trabajo normal, son cortos, no se comunican):

- Accesos de emergencia. Pueden ser concedidos con el propósito de resolver el problema, y ser inmediatamente revocados después de que el problema es resuelto.
- Todas las acciones realizadas durante la emergencia deberán ser automáticamente registradas.

Cuando se instala el software de librerías se definen las librerías y sus respectivos niveles de protección.

Los tipos de acceso a la librería pueden ser restringidos durante la instalación. Por ejemplo, un programador deberá ser autorizado para leer o modificar un programa.

E) Software de utilerías

Existen dos tipos de software de utilerías. El primero es usado en los sistemas de desarrollo para proveer productividad. El desarrollo de programas y los editores en línea son los ejemplos de este tipo de software. El segundo es usado para asistir en el manejo de operaciones de la computadora. Monitoreos, calendarios de trabajo, sistema manejador de disco y cinta son ejemplos de este tipo de software.

El software de utilerías tiene privilegios de acceso todo el tiempo, algún tiempo o nunca. Los accesos privilegiados se otorgan a programadores o a usuarios que ejecutan funciones que sobrepasan la seguridad normal.

Entre los ejemplos de utilerías de software están:

- Utilerías de monitores.
- Sistemas manejadores de cinta.
- Sistemas manejadores de disco.
- Calendarios de *jobs*.
- Editores en línea.
- *Debuggers*.
- Scanner de virus.
- Software de telecomunicaciones.

Ciertos tipos de software de telecomunicaciones pueden restringir el acceso a las redes y a aplicaciones específicas localizadas en la red.

El software de telecomunicaciones provee la interfase entre las terminales y las redes y tiene la capacidad para:

- Controlar la invocación de los programas de aplicación.
- Verificar que todas las transacciones estén completas y sean correctamente transmitidas.
- Restringir a los usuarios para actuar en funciones seleccionadas.
- Restringir el acceso al sistema a ciertos individuos.

RIESGOS Y CONTROLES A AUDITAR

Los controles de software de seguridad general y de software específico pueden ser implantados para minimizar el riesgo de la seguridad lógica.

Controles del software de seguridad general. Los controles del software de seguridad general aplican para todos los tipos de software y recursos relacionados y sirven para:

- El control de acceso a programas y a la información.
- Vigilar los cambios realizados.
- Las bitácoras de auditoría.
- Control de acceso a programas y datos. Este control de acceso se refiere a la manera en que cada software del sistema tiene acceso a los datos, programas y funciones. Los controles son usualmente a través del ID (identificador) o del *password* para identificar a usuarios no autorizados y para controlar el acceso inicial al software.
- Cambios realizados. Deben ser probados y revisados para ser autorizados, y una vez autorizados se asignan a los programas en aplicación y datos. Dependiendo de la aplicación, el ambiente y el potencial del efecto de los cambios, éste puede ser muy informal o extremadamente rígido. Los procedimientos a seguir para los cambios realizados pueden ser los siguientes:
 - Diseño y código de modificaciones.
 - Coordinación con otros cambios.
 - Asignación de responsabilidades.
 - Revisión de estándares y aprobación.
 - Requerimientos mínimos de prueba.
 - Procedimientos del respaldo en el evento de interrupción.

La bitácora de auditoría debe registrar cambios en el software antes de la implementación. Los procedimientos de cambios de software deben además incluir notificaciones escritas para el departamento apropiado de cada cambio. Los cambios realizados deben incluir independientemente una fase de pruebas realizadas por un grupo fuera del ambiente de desarrollo.

- Bitácoras de auditoría. Las bitácoras de auditoría son usadas para monitorear los accesos permitidos y negados. El software debe contener una bitácora de auditoría del uso de las funciones que el software ejecuta, particularmente si cambian las funciones o se modifican datos. Esta bitácora de auditoría posiblemente sea mantenida en un archivo separado, y puede ser manejada por las actividades del sistema, o tal vez sea una parte del registro. El tipo de bitácoras de auditoría varía gradualmente de acuerdo al software y al vendedor; por ejemplo, un software puede guardar antes y después imágenes de los cambios, mientras que otros solamente tienen una técnica de recuperación que puede ser usada para seguridad en casos necesarios.

Las bitácoras de auditoría generalmente están relacionadas con el sistema operativo o con el software de control de acceso.

Estas bitácoras de auditoría registran las actividades y opcionalmente muestran el registro de los cambios hechos en el archivo o programa. Son importantes para el seguimiento de los cambios.

Controles de software específico. A continuación presentamos algunos de los controles usados por los diferentes tipos de software específico:

- El acceso al sistema debe ser restringido para individuos no autorizados.
- Se debe controlar el acceso a los procesos y a las aplicaciones permitiendo a los usuarios autorizados ejecutar sus obligaciones asignadas y evitando que personas no autorizadas logren el acceso.
- Las tablas de acceso o descripciones deberán ser establecidas de manera que se restrinja a los usuarios ejecutar funciones incompatibles o más allá de sus responsabilidades.
- Se deberá contar con procedimientos para que los programadores de aplicaciones tengan prohibido realizar cambios no autorizados a los programas.
- Se limitará tanto a usuarios como a programadores de aplicaciones a un tipo específico de acceso de datos (por ejemplo: lectura y modificación).
- Para asegurar las rutas de acceso deberá restringirse el acceso a secciones o tablas de seguridad, mismas que deberán ser encriptadas.
- Las bitácoras de auditoría deberán ser protegidas de modificaciones no autorizadas.

Deberán restringirse las modificaciones o cambios al software de control de acceso, y éstos deberán ser realizados de acuerdo a procedimientos autorizados:

- Software de sistemas operativos. Entre los controles se incluyen los siguientes:
 - Los *password* e identificadores deberán ser confidenciales. Los usuarios no autorizados que logran acceder al sistema pueden causar modificaciones no autorizadas.
 - El acceso al software de sistema operativo deberá ser restringido.

- Los administradores de la seguridad deberán ser los únicos con autoridad para modificar funciones del sistema, incluyendo procedimientos y tablas de usuarios.
 - El acceso a utilerías del sistema operativo será restringido.
 - Las instalaciones de sistemas y las reinstalaciones deben ser monitoreadas porque la realización no autorizada puede resultar inválida.
 - El uso de todas las funciones del software (editores de línea, consolas) es restringido a individuos autorizados.
 - Deberán revisarse las bitácoras de auditoría para determinar si ocurre un acceso no autorizado o si se realizan modificaciones.
- Software manejador de base de datos. Los controles incluyen lo siguiente:
 - El acceso a los archivos de datos deberá ser restringido en una vista de datos lógica, a nivel de tipo de campo. La seguridad en el campo será dada de acuerdo al contenido del campo (validación de campos).
 - Deberá controlarse el acceso al diccionario de datos.
 - La base de datos debe ser segura y se usarán las facilidades de control de acceso construidas dentro del software DSMS.
 - La bitácora de auditoría debe reportar los accesos al diccionario de datos.
 - Las modificaciones de capacidades desde el DBMS para las bases de datos deberán limitarse al personal apropiado.
 - Software de consolas o terminales maestras. Estos controles incluyen lo siguiente:
 - Los cambios realizados al software de consolas o terminales maestras deberán ser protegidos y controlados.
 - Software de librerías. Los controles incluyen los siguientes:
 - El software de librerías mantiene una bitácora de auditoría de todas las actividades realizadas. La información provista en la bitácora incluye el nombre del programa, el número de la versión, los cambios específicos realizados, la fecha de mantenimiento y la identificación del programador.
 - El software de librerías tiene la facilidad de comparar dos versiones de programas en código fuente y reportar las diferencias.
 - Deben limitarse el acceso a programas o datos almacenados por el software de librerías.
 - Deberá impedirse el acceso a *password* o códigos de autorización a individuos no autorizados.
 - Los cambios realizados al software de librerías tendrán que ser protegidos y controlados.
 - Las versiones correctas de los programas de producción deben corresponder a los programas objeto.

- Software de utilerías. Los controles incluyen lo siguiente:
 - Deberá restringirse el acceso a archivos de utilerías.
 - Algunas utilerías establecen niveles de utilización por cada función y verifican cada nivel de autorización del usuario antes de darle acceso, utilizando *password* para prever accesos no autorizados.
 - El software de utilerías genera una bitácora de auditoría de usos y actividades. Algunas proveen bitácoras detalladas de actividades con datos protegidos, librerías y otros recursos. Estas bitácoras de auditoría proveen información de cada identificador (ID), fecha y hora de acceso, recursos accedidos y tipo de acceso.
 - Esta bitácora sirve como un registro de eventos, incluyendo violaciones a la seguridad y accesos no autorizados. Cada paquete de software puede tener diferentes capacidades de control.
 - Tomar precauciones para asegurar la manipulación de datos (copiar, borrar, etc.), los protege de un uso no autorizado.
 - Asegurar que únicamente personal autorizado tenga acceso a correr aplicaciones.
 - Las utilerías no deben ser mantenidas en el ambiente de producción y se debe asegurar que únicamente usuarios autorizados tengan acceso a ellas.
 - Las bitácoras de auditoría producidas por utilerías deben ser cuidadosamente revisadas para identificar alguna violación a la seguridad.
- Software de telecomunicaciones. Los controles incluyen lo siguiente:
 - Controlar el acceso a datos sensibles y recursos de la red de la siguiente forma:
 - Verificación de *login* de aplicaciones.
 - Control de las conexiones entre sistemas de telecomunicaciones y terminales.
 - Restricción al uso de aplicaciones de la red.
 - Protección de datos sensibles durante la transmisión, terminando la sesión automáticamente.
 - Los comandos del operador que pueden dar *shoutdown* a los componentes de la red sólo pueden ser usados por usuarios autorizados.
 - El acceso diario al sistema debe ser monitoreado y protegido.
 - Asegurar que los datos no sean accedidos o modificados por un usuario no autorizado, ya sea durante la transmisión o mientras está en almacenamiento temporal.

Consideraciones al auditar

Cuando se realiza una revisión de seguridad lógica, el auditor interno deberá evaluar y probar los siguientes tres controles implantados para minimizar riesgos:

- Control de acceso a programas y a la información.
- Control de cambios.
- Bitácoras de auditoría.

La evaluación de todos los tipos de software deberá asegurar que los siguientes objetivos sean cumplidos:

- El acceso a funciones, datos y programas asociados con el software debe estar restringido a individuos autorizados y debe ser consistente con documentos esperados.
- Todos los cambios del software deben ser realizados de acuerdo con el manejo del plan de trabajo y con la autorización del usuario.
- Se debe de mantener una bitácora de auditoría de todas las actividades significativas.

Una auditoría de seguridad lógica puede ser realizada de diferentes formas. La auditoría puede enfocarse en áreas de seguridad que son aplicables a todo tipo de software y pueden cubrir la instalación, el mantenimiento y la utilización del software.

También debe tomarse en cuenta las características de seguridad del software, incluyendo el control de acceso, la identificación del usuario y el proceso de autenticación del usuario, ejecutado por el software.

Entre las consideraciones específicas al auditar están:

- Software de control de acceso.
- Software de telecomunicaciones.
- Software manejador de librerías.
- Software manejador de bases de datos.
- Software de utilerías.
- Software de sistema operativo.

Durante el ciclo de vida del software deben ser evaluadas su instalación, mantenimiento y operación. Se debe utilizar la auditoría para asegurar que algún cambio hecho al software no comprometa la integridad, confidencialidad o aprovechamiento de los datos o recursos del sistema.

El software de auditoría especializado puede ser usado para revisar todos los cambios y asegurarse que son ejecutados de acuerdo con los procedimientos aprobados por la gerencia.

Instalación y mantenimiento. Es la primer fase del ciclo de vida del software, en la cual el auditor debe revisar lo siguiente:

- Procedimientos para nuevas pruebas o modificaciones al software, incluyendo al personal responsable, ejecución de pruebas, respaldo de software existente, pruebas de funciones, documentación de cambios, notificación de cambios, revisión y redención de pruebas de salida y aprobación de prioridades para la implementación.

Ciclo de vida
del software

- Procedimientos para iniciación, documentación, pruebas y aprobación de modificaciones al software.
- Procedimientos para la generación y modificación al software.
- Procedimientos usados para ejecutar software y mantenimiento del diccionario de datos para un mayor grado de modificación.
- Procedimientos de emergencia usados para dar solución a un problema específico de software.
- Mantenimiento y contenido de las bitácoras de auditoría de todos los DBMS y modificaciones del diccionario de datos.
- Bitácoras a los parámetros del software y de las sentencias del lenguaje de aplicaciones en ejecución.
- Acceso a librerías de programas.

Operación. En la segunda fase del ciclo de vida del software deberán revisarse:

- Controles de acceso para los programas, librerías, parámetros, secciones o archivos de software asociados.
- Procedimientos diseñados para asegurar que el sistema no es instalado (carga inicial del programa) sin el software original, creando así un procedimiento de seguridad.
- Disponibilidad y control de acceso a los comandos que pueden ser usados para desactivar el software.
- Áreas de responsabilidad para el control del software, operación y consistencia de capacidad de acceso.
- Horas durante las cuales el software está disponible.
- Procedimientos para la iniciación y terminación del uso del software.
- Control de acceso sobre consolas y terminales maestras.
- Procedimientos para registrar terminación anormal o errores, los cuales pueden indicar problemas en la integridad del software y documentar los resultados en programas de seguridad.
- Controles de acceso sobre escritura de programas y lenguajes de librerías y de aplicaciones en ejecución.
- Bitácoras de auditoría sobre las actividades del software.
- Dependencia de otro software para continuar la operación, operaciones automatizadas o dependencia del calendario de actividades.

Software de control de acceso. Entre las consideraciones de auditoría para el software de control de acceso están:

- Diseño y administración.
- Procedimientos de identificación del usuario.
- Procedimientos de autenticación del usuario.
- Recursos para controlar el acceso.
- Reportes y vigilancia del software de control de acceso reportando y vigilando.

El software de control de acceso usualmente provee utilerías que pueden ser usadas en la ejecución de una auditoría. Los eventos pueden ser registrados en un archivo de auditoría (cambios en el sistema, así como la ocurrencia de

otras numerosas actividades: *login*, archivos de acceso, recursos de acceso, violaciones y cambios de acceso). Los reportadores y otras utilerías pueden ser usadas para presentar esta información continuamente.

- Diseño y administración. En estos aspectos los auditores internos deben revisar lo siguiente:

- Localización de archivos de seguridad y tablas para asegurar que los archivos del software de control de acceso están protegidos.
- Uso de recursos o controles de acceso a nivel del usuario para asegurar que el software de control de acceso protege datos y recursos en un nivel correcto.
- Archivos de seguridad o encriptación de tablas usadas para prohibir la vista de tablas individuales.
- Limitaciones de acceso para archivos de seguridad que contienen descripciones y *passwords*.
- Limitaciones de acceso a archivos de seguridad a través de la administración de comandos de seguridad en línea o utilerías.
- La jerarquía de seguridad.
- Los usuarios encargados de la administración de la seguridad pueden tener gran capacidad para cierto software.
- Métodos y limitaciones sobre archivos de seguridad o modificación de tablas.
- Responsabilidades del usuario para la administración de la seguridad, particularmente en un ambiente descentralizado, para asegurar que las capacidades definidas son consistentes con las responsabilidades.
- Definición de parámetros de seguridad, como los recursos definidos, reglas de *password*, *default* de niveles de acceso y opciones de *login* con aprobación de la gerencia, considerando pruebas de protección para acceder recursos protegidos.

- Procedimientos de identificación del usuario. Los auditores deberán revisar y aprobar los métodos usados para definir usuarios para el software.

Las siguientes situaciones deberán ser revisadas por un apropiado nivel de dirección:

- Las identificaciones del usuario para corroborar que sean individuales y no compartidas.
- Probar la revocación de usuarios inactivos.
- El despliegue de la última fecha y hora en que algún ID específico fue usado. Esta información podrá ayudar para identificar actividades ilícitas.
- Revocación o desconexión de identificaciones del usuario siguiendo un número específico de acceso inválido. Este control puede también limitar actividades ilícitas.
- El uso de comienzo y fin de fechas para ID de usuario de empleados contratados.

- El uso de grupos de usuarios para el recurso de acceso a los archivos. Los usuarios deberán ser asignados a los grupos apropiados.
- Propietarios de datos y recursos para asegurar que ellos son los responsables apropiados.
- Procedimientos de autenticación del usuario. Los auditores internos revisarán lo siguiente:
 - Deberá ser evaluado el uso de *passwords* o información personal durante la sesión.
 - Deberá ser identificada la disponibilidad de automatizar funciones una vez identificado el usuario, así como la autenticación de procedimientos.
 - Deberá ser identificado el uso de *passwords* por otro personal que no sean usuarios autorizados.
 - Los procedimientos para el uso de *passwords* para asegurarse que éste está protegido cuando es usado por el usuario.
 - La máscara del *password* para asegurarse que el área donde los caracteres son tecleados no se despliegan.
 - La sintaxis del *password*. Algún software de control de acceso puede restringir el uso de ciertas palabras o cadenas de caracteres.
 - El mantenimiento de la historia del *password*. Éste puede ser usado para prevenir a usuarios que reutilizan un *password* por un periodo específico.
 - Procedimientos para suplir identificaciones de usuarios y *passwords* por procesos *batch*.
- Los recursos para controlar el acceso. Los auditores internos deberán revisar lo siguiente:
 - Posibles niveles de acceso.
 - Niveles de acceso por *default*, particularmente para usuarios o *jobs* que no tienen un ID de usuario.
 - El acceso del usuario a archivos de seguridad.
 - Que la seguridad sea implantada en el nivel correcto.
 - Procedimientos para asegurar la protección automática.
 - Procedimientos para la protección de recursos.
 - Uso de rutas rápidas o funciones aceleradas a través de controles.
 - Controles de acceso sobre aplicaciones locales o remotas.
 - Restricciones de acceso sobre recursos críticos del sistema, tales como sistemas, programas y aplicaciones en ejecución, librerías del lenguaje, catálogos del sistema y directorios, diccionarios de datos, *logs* y archivos de *password*, tablas de definición de privilegios, algoritmos de encriptación y tablas de datos.
- Reportes y vigilancia del software de control de accesos. El auditor interno deberá revisar:
 - *Login*, identificación del acceso autorizado al sistema y el uso de recursos.

- Las identificaciones de acceso no autorizado.
- La identificación de archivos de seguridad, mantenimiento a tabla y el uso de comandos sensibles.
- El *login* de usuarios privilegiados y sus actividades.
- Las restricciones de acceso a archivos de *log* del sistema. Estos archivos frecuentemente contienen las bitácoras de auditoría del control de acceso.
- Sistema operativo o software de control de acceso existente.
- Las violaciones a la seguridad.
- Los archivos de seguridad y la generación de reportes de las actividades del usuario para asegurar que los propietarios de datos y recursos son notificados de los eventos de seguridad en un periodo determinado.

Sistemas operativos. El auditor deberá revisar, evaluar y probar el uso y procedimientos que gobiernan programas, usuarios y funciones del sistema operativo, especialmente los siguientes:

- Las facilidades del sistema operativo, como son la supervisión y privilegios para programas y usuarios.
- Controles de acceso sobre tablas que definen privilegios de usuarios, programas y funciones.
- Controles de acceso sobre consolas o terminales maestras y privilegios asociados.
- Bitácoras de auditoría.
- Posibilidad y uso del control de acceso sobre los *default* de inicio de ID de usuarios y *passwords*.
- Comandos de software o funciones que son consideradas importantes, como mantenimiento de seguridad al archivo de descripciones.
- Diagnóstico de utilerías del sistema operativo que pueden ser usados para leer o almacenar áreas que contienen información importante.

Software del sistema manejador de bases de datos. En relación con las funciones del *software* que restringen el acceso a datos y recursos, y los procedimientos que gobiernan el uso de estas funciones, el auditor deberá revisar, evaluar y probar lo siguiente:

- Procedimientos usados por el software de control de acceso para restringir el acceso a la base de datos y al diccionario de datos.
- El diseño de una restricción de acceso en los archivos por niveles, incluyendo restricciones sobre archivos físicos y lógicos en el DBMS y en el diccionario de datos.
- Seguridad de campos, uso de secciones de usuarios y *passwords* y restricciones de acceso.
- Si el software ejecuta la función de identificación del usuario y procedimientos de autenticación.
- Comandos y funciones del diccionario de datos (utilerías del administrador de la base de datos, comandos para modificar DSMS, archivos o definiciones de archivo).

- Accesos de los programadores, acceso a DBMS y comandos o funciones del directorio de datos.
- Bitácoras de auditoría.
- El software de desarrollo que afecta a la seguridad del DBMS.

El manejador de la base de datos y el diccionario de datos usualmente proveen utilerías para revisar e imprimir las capacidades de acceso, información del usuario y bitácoras de auditorías.

Software del manejo de librerías. Las funciones del software restringen el acceso a librerías críticas; los procedimientos que gobiernan el uso de esas funciones deberán ser revisados, evaluados y probados. El auditor deberá revisar, evaluar y probar lo siguiente:

- Documentación de librerías.
- Programas fuentes y ejecutables.
- *Jobs* en ejecución y lineamientos de control.
- Parámetros de corrida.
- Uso de software para restringir el acceso a librerías.
- Restricción del acceso a librerías de producción.
- Restricciones de funciones que pueden ser usadas para modificar el estado de un programa (pruebas a producción).
- Acceso a librerías en prueba.
- Convenciones para dar nombre a librerías que son usadas para facilitar la seguridad.
- Métodos para clasificar y restringir el acceso a librerías por tipo (fuentes, objeto, carga y control de *job*).
- Si el software ejecuta funciones de identificación de usuario y procedimientos de autenticación.
- Procedimientos inusuales de las librerías.
- Capacidades de la bitácora de auditoría.
- Los números de versión del software.

Los reportes escritos pueden ser usados para organizar las actividades de las librerías de *logs* de acceso al software manejador de librerías o bitácoras de auditoría.

Software de utilerías. El auditor deberá evaluar, revisar y probar los siguientes procedimientos diseñados para limitar el acceso a comandos de utilerías o funciones:

- Funciones o comandos de utilerías.
- Los controles de acceso sobre comandos o funciones de utilerías.
- Seguridad de acceso a los programadores para la utilización de funciones o comandos de utilerías.
- Si el software ejecuta las funciones de identificación del usuario y procedimientos de autenticación.
- Capacidades de uso de utilería para cada grupo de usuarios.
- Bitácoras de auditorías.

El software de utilerías no provee bitácoras de auditoría, por ello debe usarse el reporte escrito del software, para lo cual puede utilizarse el software de control de acceso, si éste está integrado al software. Deberán usarse reportes para monitorear el control de acceso.

Software de telecomunicaciones. El auditor deberá revisar, evaluar y probar si es posible usar las funciones del software que restringe el acceso en las redes de telecomunicaciones y los procedimientos que gobiernan su uso, especialmente los siguientes:

- Restricciones al acceso de la red basados en tiempo, día, usuario, lugar y terminal.
- Apagado automático de terminales inactivas en un tiempo específico (terminales que pueden ser usadas).
- Facilidad de acceso no autorizado basada en protocolos de transmisión y líneas para la conexión rápida.
- Número de seguridad de entrada (revisar la posibilidad de este número para acceso local o tableros de boletín nacional.)
- "Autorrespuesta", facilidad de uso sobre módem.
- Horas durante las cuales la línea está disponible.
- Recursos y funciones posibles a través del acceso de entrada.
- Uso de identificación de la terminal físicamente.
- Controles de acceso sobre los recursos de la red.
- Controles de acceso sobre tablas de configuración de red.
- Controles de acceso a funciones de la red.
- Seguridad física sobre líneas telefónicas y telecomunicaciones.
- El uso de red de área local y la conectividad para otras LAN, WAN o redes en otro lugar.
- Si el software ejecuta las funciones de la identificación del usuario y procedimientos de autenticación.
- Procedimientos para la protección de comunicaciones (desde las conexiones hasta la recepción no autorizada).
- Posibilidad y uso de encriptación de datos o mensajes técnicos de identificación.

Los reportes escritos pueden ser usados para reportar las actividades de la red, de logs de acceso a software de telecomunicaciones o bitácoras de auditoría. Éstos pueden además hacerlo con el software de control de acceso.

Los reportes especiales de auditoría deberán contener lo siguiente:

- Personal registrado por el sistema en el que no corresponde el *password* con su identificador, o el que ha intentado más de dos veces entrar al sistema sin un *password* autorizado.
- Identificaciones de usuarios no usados hace seis meses.
- Identificaciones de usuarios con privilegios especiales.
- Un reporte de referencias cruzadas que debe mostrar a los ID usuarios con cada acceso a las aplicaciones.
- Listar todos los ID usuarios por grupos.

ENCRIPTAMIENTO

Definición

Encriptar es el arte de proteger la información transformándola con un determinado algoritmo dentro de un formato para que no pueda ser leída normalmente. Sólo aquellos usuarios que posean la clave de acceso podrán "desencriptar" un texto para que pueda ser leído. Las tecnologías modernas de encriptamiento hacen casi imposible que una persona no autorizada utilice la información.

Encriptar es la transformación de los datos a una forma en que no sea posible leerla por cualquier persona, a menos que cuente con la llave de desencriptación. Su propósito es asegurar la privacidad y mantener la información alejada de personal no autorizado, aun de aquellos que la puedan ver en forma encriptada.

Debido a que Internet y otras formas de comunicación electrónica se han convertido en algo normal y rutinario, la seguridad se ha convertido en un factor muy importante. El encriptamiento se usa para proteger mensajes de correo electrónico (E-mail), firmas electrónicas, llaves de acceso, información de tipo financiero e información confidencial. Existen en el mercado diferentes paquetes y formas para encriptar la información.

Los sistemas de encriptamiento pueden ser clasificados en sistemas de llave simétrica, los cuales usan una llave común para el que envía información y para el que la recibe, y sistemas de llave pública, el cual utiliza dos llaves, una que es pública, conocida por todos, y otra que solamente conoce el receptor.

Para generar una firma digital, se usan algunos algoritmos públicos. La firma digital es un conjunto de datos que son creados usando una llave secreta, aunque existe una llave pública que es usada para verificar que la firma fue realmente generada usando la llave privada correspondiente. El algoritmo usado para generar la firma electrónica es de tal naturaleza, que si no se usa la llave secreta no es posible usar la firma electrónica.

La autenticación en sentido digital es el proceso por medio del cual el emisor y/o receptor de un mensaje digital confidencial tiene una identificación válida para enviar o recibir un mensaje. Los protocolos de autenticación pueden estar basados en sistemas convencionales de encriptamiento de llaves secretas, o en sistemas públicos de encriptamiento. En la autenticación de sistemas de llaves públicas se usan las firmas digitales.

La firma digital tiene la misma función que la firma escrita en cualquier documento. La firma digital es un fragmento de información confidencial y propia de cada usuario que asegura a la persona que envía o autoriza un documento. El receptor o terceras personas pueden verificar que el documento y la firma corresponden a la persona que lo firma, y que el documento no ha sido alterado.

La firma digital es usada para verificar que el mensaje realmente viene de la persona que se señala como la que lo envía. También puede ser usada para certificar que una persona envió un documento o una autorización en un tiempo determinado. Existe una serie de firmas digitales que identifican y certifican desde el usuario inicial hasta el último usuario.

Firma digital

En el caso de envío de documentos pueden certificar la organización que envía el documento, su departamento y la persona que lo manda o autoriza.

Un sistema seguro de firmas digitales debe comprender dos partes: un método para firmar el documento que sea de tal manera confiable que no pueda ser usado por otras personas, y otro que verifique que la firma fue realmente generada por el que ella representa, de tal forma que posteriormente no pueda ser cuestionada.

El resultado de un conjunto de datos encriptados es la firma digital. Normalmente, junto con la información, la llave pública que es usada para firmar. Para verificar la información, el receptor primero determina si la llave pertenece a la persona a la cual debe pertenecer, y después de desencriptarla verifica si la información corresponde al mensaje; entonces la firma es aceptada como válida.

Criptografía es el arte de desencriptar comunicaciones sin conocer las llaves apropiadas. Existen muchas técnicas para lograrlo, y entre las más comunes están:

- Ataque a textos encriptados. Ésta es una situación en la cual el atacante no conoce nada acerca del contenido del mensaje, y debe de trabajar únicamente en el contenido del mensaje. En la práctica es muy posible adivinar el contenido de algún texto, ya que normalmente tienen encabezados fijos.
- Ataque conociendo el texto original. El atacante conoce o puede adivinar el contenido del texto debido a algunas partes del texto encriptado. El objetivo es desencriptar el resto del texto usando esta información. Esto también puede ser hecho al determinar la llave usada para encriptar.
- Ataque hecho por medio de escoger un texto encriptado. El atacante tiene el objetivo de determinar la llave con la cual se encriptó el texto.
- Atacar en la parte central. Este tipo de ataque es relevante para la comunicación criptografiada y para los protocolos clave de intercambio. La idea es que cuando dos personas están intercambiando llaves de seguridad para lograr la comunicación, el atacante se pone en medio de la línea de comunicación. El atacante realiza un intercambio separado de llaves. Posteriormente, el atacante, con las llaves de acceso, puede realizar cualquier función. Una forma de prever este tipo de ataques es encriptar la llave de acceso al momento de enviar; así, una vez enviada, el emisor y receptor verifican la firma digital para realizar las operaciones necesarias.
- Ataque en el tiempo. Éste es un nuevo tipo de ataque y está basado en la medición repetitiva de los tiempos exactos de ejecución.

Aunque existen diversas formas para atacar la información encriptada, es conveniente que el programador conozca las formas de encriptamiento, sus ventajas y desventajas, así como su costo, para determinar la mejor para cada uno de los sistemas, y que el auditor verifique la forma de encriptamiento y su seguridad de acuerdo con los requerimientos de seguridad de cada sistema.

Existen diferentes protocolos y estándares para la criptografía, entre los cuales están:

- DNSSEC (*Domain Name Server Security*). Éste es un protocolo para servicio seguro de distribución de nombres.

- GSSAPI (*Generic Security Services, API*). Provee una autenticación genérica, llaves de intercambio e interfases de encriptamiento para diferentes sistemas y métodos de autenticación.
- SSL (*Secure Socket Layer*). Es uno de los dos protocolos para una conexión segura de web.
- SHTTP (*Secure Hypertext Transfer Protocol*). Protocolo para dar más seguridad a las transacciones de web.
- E-Mail (*Security and Related Services*).
 - MSP (*Message Security Protocol*).
- PKCS (*Public Key Encryption Standards*).
- SSH2 (*Protocol*).
- Algoritmos de encriptamiento:
 - DIFFIE HELLMAN.
 - DSS (*Digital Signature Standard*).
 - ELGAMAL.
 - LUC.
 - ◆ Symetricos.
 - ◆ DES.
 - ◆ BLOWFISH.
 - ◆ IDEA (*International Data Encryption Algorithm*).
 - ◆ RC4.
 - ◆ SAFER.
- Varios algoritmos de llave pública, algunos con promisorio futuro; sin embargo, el más popular es el RSA (*Rivest Shamir Adelman*). En algoritmos simétricos el más famoso es el denominado DES y su variante DES-CBC, pero el más reciente es RC4.

SEGURIDAD EN EL PERSONAL

Un buen centro de cómputo depende, en gran medida, de la integridad, estabilidad y lealtad del personal, por lo que al momento de reclutarlo es conveniente hacerle exámenes psicológicos y médicos, y tener muy en cuenta sus antecedentes de trabajo.

Se debe considerar sus valores sociales y, en general, su estabilidad, ya que normalmente son personas que trabajan bajo presión y con mucho estrés, por lo que importa mucho su actitud y comportamiento.

El personal de informática debe tener desarrollado un alto sistema ético y de lealtad, pero la profesión en algunas ocasiones cuenta con personas que subestiman los sistemas de control, por lo que el auditor tiene que examinar no solamente el trabajo del personal de informática, sino la veracidad y confiabilidad de los programas de procesamiento.

Características
del personal

E
gran
depe
crean
riesgo
vacac
y evit
zo en
pued
zación
T
posib
bia a
sabría
Esto s
aunqu
mite,
Se
do no
lidad
la mo
así co
El
ligro l
audite
fraude
En
está d
nal lea
citado
ver la
contro
palme
ciente
person

SE

El obje
interru
bido a
terrem
sea res

En los equipos de cómputo es normal que se trabajen horas extra, con gran presión, y que no haya una adecuada política de vacaciones debido a la dependencia que se tiene de algunas personas, lo cual va haciendo que se crean "indispensables", que son muy difíciles de sustituir y que ponen en gran riesgo a la organización. Se debe verificar que existan adecuadas políticas de vacaciones (lo cual nos permite evaluar la dependencia de algunas personas, y evitar esta dependencia) y de reemplazo. La adecuada política de reemplazo en caso de renuncia de alguna persona permitirá que, en caso necesario, se pueda cambiar a una persona sin arriesgar el funcionamiento de la organización.

También se debe tener políticas de rotación de personal que disminuyan la posibilidad de fraude. Si un empleado está cometiendo un fraude y se le cambia a otra actividad al mes, sería muy arriesgado cometer un fraude porque sabría que la nueva persona que esté en su lugar puede detectarlo fácilmente. Esto se debe hacer principalmente en función de un alto nivel de confianza, aunque implique un alto costo. Este procedimiento de rotación de personal permite, además, detectar quiénes son indispensables y quiénes no.

Se deberá evaluar la motivación del personal, ya que un empleado motivado normalmente tiene un alto grado de lealtad, con lo que disminuirá la posibilidad de ataques intencionados a la organización. Una de las formas de lograr la motivación es darle al personal la capacitación y actualización que requiere, así como proporcionarle las retribuciones e incentivos justos.

El programador honesto en ocasiones elabora programas que ponen en peligro la seguridad de la empresa, ya que no se considera un procedimiento de auditoría dentro de los programas para disminuir o limitar las posibilidades de fraude.

En muchas ocasiones el mayor riesgo de fraude o mal uso de la información está dentro del mismo personal, y la mayor seguridad está en contar con personal leal, honesto y con ética. Para lograr esto se debe contar con personal capacitado, motivado y con remuneraciones adecuadas. Pero también se debe prever la posibilidad de personal mal intencionado, para lo cual se debe tener los controles de seguridad señalados, los cuales deben de ser observados principalmente por el personal del área de informática. El auditor debe de estar consciente que los primeros que deben implantar y observar los controles son los del personal de informática.

SEGURIDAD FÍSICA

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de información, debido a contingencias como incendio, inundación, huelgas, disturbios, sabotaje, terremotos, huracanes etc., y continuar en un medio de emergencia hasta que sea restaurado el servicio completo.

UBICACIÓN Y CONSTRUCCIÓN DEL CENTRO DE CÓMPUTO

En el pasado se acostumbraba colocar los equipos de cómputo en un lugar visible, con grandes ventanales, ya que constituían el orgullo de la organización y se consideraba necesario estuviesen a la vista del público, incluso había gran cantidad de invitados para conocerlos. Esto ha cambiado de modo radical, principalmente por el riesgo de terrorismo o sabotaje. Piénsese que una persona que desea perjudicar a la organización querrá dañar el 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, o bien en un lugar cercano a la calle o con un alto número de invitados, además, el excesivo flujo de personal interfiere con la eficiencia en el trabajo y disminuye la seguridad.

Otros elementos referentes al material y construcción del edificio del centro de cómputo con los que se debe tener precaución son los materiales altamente inflamables, que despiden humos sumamente tóxicos, o las paredes que no quedan perfectamente selladas y despiden polvo (por ejemplo, el tirol planchado, a menos que tenga sellador), los cuales deben ser evitados.

En lo posible también se debe tomar precauciones en cuanto a la orientación del centro de cómputo (por ejemplo, lugares sumamente calurosos a los que todo el día les está dando el sol), y se debe evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol, pueden ser riesgosos para la seguridad del centro de cómputo.

Las dimensiones mínimas del centro de cómputo deben determinarse por la cantidad de componentes del sistema, el espacio requerido para cada unidad, para su mantenimiento, el área de operación. Por ello, las paredes y paneles removibles pueden ser utilizados para facilitar ampliaciones futuras. En general, aunque los equipos de cómputo se han reducido en tamaño, se debe considerar el incremento en el número de éstos y en equipos periféricos.

Además, en el centro de cómputo se debe prever espacio para lo siguiente:

- Almacenamiento de equipos magnéticos.
- Formatos y papel para impresora.
- Mesas de trabajo y muebles.
- Área y mobiliario para mantenimiento.
- Equipo de telecomunicaciones.
- Área de programación.
- Consolas del operador.
- Área de recepción.
- Microcomputadoras.
- Fuentes de poder.
- Bóveda de seguridad. Los archivos maestros y/o registros deberán ser guardados en una bóveda antiincendio bajo máxima protección.

PISO O CÁM

En la anti
pisos elev
de compu
tadoras, p
con pisos
cuenta co

Una c
y protecc
Además,
cerca de l
rejillas de

Un pi
do con las
dad de se

Se rec
que la su
cámara p
terminad
poder se
sistema y

AIRE

El equipo
tipo de c
cual se r
ma, así c

Los c
las princ

Las i
frecuent
ductos. S
to exterio
indiquer

Se re
superior
sucieda

PISO ELEVADO O CÁMARA PLENA

En la antigüedad era un requerimiento en todos los centros de cómputo tener pisos elevados o pisos falsos. En la actualidad, con los cambios de los sistemas de cómputo, este requerimiento sólo es necesario o deseable para macrocomputadoras, por lo que habrá que verificar con el proveedor la necesidad de contar con pisos elevados, o bien la conveniencia de tener una mejor instalación que cuente con el cableado dentro del piso elevado.

Una de las ventajas de los pisos falsos es que permiten organizar el tendido y protección del cableado del sistema, y facilitan el reacomodo del sistema. Además, proveen de un excelente método para llevar el aire acondicionado cerca de las unidades del sistema, permitiendo la adición o recolocación de las rejillas de aire cuando son agregadas o recolocadas máquinas en la sala.

Un piso elevado debe ser capaz de soportar una carga uniforme, de acuerdo con las especificaciones del proveedor; también debe considerarse la capacidad de soportar unidades adicionales según el potencial de crecimiento.

Se recomienda que el acabado del piso sea hecho con plástico antiestático y que la superficie del piso elevado tenga 45 cm de alto, cuando es usado como cámara plena de aire acondicionado. La altura del plafón, desde el piso falso terminado, debe ser de 2.4 m. Asimismo, los paneles del piso elevado deben poder ser removidos fácilmente para permitir la instalación del cableado del sistema y ser de fácil limpieza con trapo húmedo o aspiradora.

AIRE ACONDICIONADO

El equipo de aire acondicionado es otro de los dispositivos que dependerán del tipo de computadora que se utilice y del lugar donde está instalado, para lo cual se recomienda verificar con el proveedor la temperatura mínima y máxima, así como la humedad relativa en la que deberán trabajar los equipos.

Los ductos de aire acondicionado deben estar limpios, ya que son una de las principales causas de polvo.

Las instalaciones del aire acondicionado son una fuente de incendio muy frecuente, son susceptibles de ataques físicos, especialmente a través de los ductos. Se deben instalar redes de protección en todo el sistema de ductos, tanto exteriores como interiores, y deberá de contarse con detectores de humo que indiquen la posible presencia de fuego.

Se recomienda que la presión de aire en la sala de cómputo sea ligeramente superior a la de las áreas adyacentes, para reducir así la entrada de polvo y suciedad.

INSTALACIÓN ELÉCTRICA Y SUMINISTRO DE ENERGÍA

Uno de los dispositivos que deben de ser evaluados y controlados con mayor cuidado es la instalación eléctrica, ya que no solamente puede provocar fallas de energía que pueden producir pérdidas de información y de trabajo, sino que es uno de los principales provocadores de incendios.

El auditor debe auxiliarse de un especialista para evaluar el adecuado funcionamiento del sistema eléctrico y el suministro de energía.

Protección del sistema eléctrico

Los cables del sistema eléctrico deben estar perfectamente identificados (positivos, negativos y tierra física); lo más frecuente es identificarlos por medio de colores (positivo, rojo). Deben de existir conexiones independientes para los equipos de cómputo; este cuidado se debe tener en las oficinas donde hay conectadas terminales o microcomputadoras, y además deben estar identificadas, contar con tierra física, lo cual protegerá a los equipos contra un cortocircuito en caso de una descarga. Se debe revisar que se cuente con los planos de instalación eléctrica debidamente actualizados.

Es común en las oficinas que, al no tener identificados los contactos para las computadoras, éstos sean utilizados para equipos que pueden producir picos, ya que utilizan grandes cargas de corriente, como fotocopiadoras o aires acondicionados.

Las variaciones de energía en una línea pueden ser causados por el encendido o apagado de máquinas eléctricas, tales como motores, ascensores, equipos de soldadura, sistemas de aire acondicionado, etc. El flujo de corriente de un sistema de iluminación puede producir "picos de ruidos" que podrían exceder el nivel de energía aceptable para alguna unidad del sistema. Por ello es altamente recomendado que el sistema eléctrico utilizado en los equipos de informática cuente con tierra física, y de ser posible sistemas de corriente continua (*no-break*) y estén aislados con contactos independientes y perfectamente identificados. En zonas grandes con cargas eléctricas industriales o con condiciones de entrada de potencia marginales puede ser necesario un aislamiento adicional para prevenir interrupciones de energía en el sistema.

La tierra física debe estar perfectamente instalada de acuerdo con las especificaciones del proveedor, dependiendo de la zona en que esté instalado el equipo y de las características de éste.

Se debe tener una protección contra roedores o fauna nociva en los cables de sistema eléctrico y de comunicaciones. Es común que los roedores se coman el plástico de los cables, por lo que se debe tener cuidado de combatir esta fauna nociva, y tener la precaución de que el veneno o el fumigante que se use para combatirla no provoque problemas al personal.

Los reguladores son dispositivos eléctricos que reducen el riesgo de tener un accidente por los cambios de corriente. Dichos protectores son comúnmente contruidos dentro de un sistema de corriente ininterrumpido UPS (*Uninterruptible Power Supply System*).

Los reguladores que existen en el mercado pueden funcionar para varios equipos, o bien estar limitados para un reducido número (parecidos a los reguladores existentes para las casas). Si se tiene un regulador para toda la instalación de informática (incluyendo terminales y microcomputadoras), se debe verificar y controlar que el número de equipos conectados sean acordes con las cargas y especificaciones del regulador. Si son equipos pequeños se debe verificar que el regulador sea suficiente para el número de equipos conectados, ya que es muy frecuente en las oficinas que se conecte al regulador no solamente la computadora personal, sino otros dispositivos periféricos, como impresora o fax, y que se llegue hasta conectar otro tipo de equipo eléctrico como radios o televisores. Esto puede provocar dos problemas: el primero es que el regulador no proteja a todos los equipos, ya que el requerimiento eléctrico sobrepasa sus capacidades, y el otro es que se puede provocar una sobrecarga en los contactos y consecuentemente una posibilidad de incendio.

También se debe tener cuidado en adquirir reguladores que tengan un nivel máximo y un mínimo, ya que existen algunos que en caso de una sobrecarga la disminuyen hasta el nivel aceptable, pero si existe una baja de corriente no la elevan a niveles mínimos aceptables. En ocasiones perjudica más a un equipo una baja de energía prolongada, que no es detectada y provoca que el equipo continúe prendido en un nivel bajo, que una sobrecarga, que hace que automáticamente el regulador o equipo se apague.

Una forma para asegurarnos de que un regulador actuará en una sobrecarga o en bajos niveles, es contar con un regulador que tenga un sistema no interrumpido (*no-break*), ya que en caso de que exista una variación que pase los niveles mínimos y máximos, automáticamente entrará el sistema no interrumpido.

Un sistema de energía no interrumpido (UPS) consiste en un generador, ya sea de batería o de gas, que hace interfase entre la energía eléctrica y el dispositivo de entrada de energía eléctrica a la computadora. Dar una consistencia a la corriente eléctrica que hace funcionar a la computadora en caso de haber una falla en el abastecimiento de energía eléctrica. El sistema de energía no interrumpible (UPS) provee de energía eléctrica a la computadora por un cierto periodo; dependiendo de lo sofisticado que sea, la corriente eléctrica puede ser de horas o de algunos minutos, de tal forma que permita respaldar la información.

Es conveniente evaluar la probabilidad de que no se tenga corriente en la zona en la que se trabaja, para determinar el tiempo que necesita el sistema no interrumpido. También se deben evaluar los problemas que puede provocar el no contar con electricidad y las prioridades y necesidades que se tienen. En la mayoría de los casos se necesita un determinado periodo para respaldar los archivos de computadoras personales, y se puede esperar para utilizar la impresora.

En el caso de sistemas de alto riesgo o costosos, como por ejemplo un sistema bancario, no solamente se debe contar con sistemas de reguladores y eléctricos no interrumpidos, sino también con plantas de luz de emergencia, para cuando se pierda la energía eléctrica por un periodo prolongado.

En algún momento tal vez exista la necesidad de apagar la computadora y sus dispositivos periféricos en caso de que el centro de cómputo donde se en-

cuentre la computadora se incendie o si hubiera una evacuación. Los switch de emergencia sirven para este propósito: uno en el cuarto de máquinas y el otro cerca, pero afuera del cuarto. Éstos deben ser claramente identificados con un letrero, accesibles e inclusive estar a salvo de gente que no tiene autorización para utilizarlos. Los switch deben estar bien protegidos de una activación accidental.

Los incendios a causa de la electricidad son siempre un riesgo. Para reducirlo, los cables deben ser puestos en paneles y canales resistentes al fuego. Estos canales y paneles generalmente se encuentran en el piso del centro de cómputo. Los cables deben estar adecuadamente aislados y fuera de los lugares de paso del personal. Se debe cuidar no sólo que los cables estén aislados sino también que los cables no se encuentren por toda la oficina.

Los circuitos ramificados para la iluminación y los sistemas de aire no deberán estar conectados a los tableros de potencia utilizados por el sistema.

El proveedor debe proporcionar un tablero de distribución, el que deberá contar con interruptor general, voltímetro, amperímetro, frecuentímetro e interruptor individual por cada una de las unidades que configuren en el sistema. El tablero debe ubicarse en un lugar accesible y cada interruptor debe estar debidamente rotulado para su fácil localización.

SEGURIDAD CONTRA DESASTRES PROVOCADOS POR AGUA

Los centros de cómputo no deben colocarse en sótanos o en áreas de planta baja, sino de preferencia en las partes altas de una estructura de varios pisos, aunque hay que cuidar que en zonas sísmicas no queden en lugares donde el peso ocasionado por equipos o papel pueda provocar problemas.

Se debe evaluar la mejor opción, dependiendo de la seguridad de acceso al centro de cómputo, cuando en la zona existen problemas de inundaciones o son sísmicas. En caso de ser zona de inundaciones o con problemas de drenaje la mejor opción es colocar el centro de cómputo en áreas donde el riesgo de inundación no sea evidente.

Algunas causas de esto pueden ser la ruptura de cañerías o el bloqueo del drenaje, por lo tanto, la ubicación de las cañerías en un centro de cómputo es una decisión importante, así como considerar el nivel del manto freático.

Debe considerarse el riesgo que representa el drenaje cuando el centro de cómputo se localiza en un sótano. Deben instalarse, si es el caso, detectores de agua o inundación, así como bombas de emergencia para resolver inundaciones inesperadas.

Otro de los cuidados que se deben tener para evitar daños por agua es poseer aspersores contra incendio especiales que no sean de agua.

SEGURIDAD DE AUTORIZACIÓN DE ACCESOS

Es importante asegurarse que los controles de acceso sean estrictos durante todo el día, y que éstos incluyan a todo el personal de la organización, en especial durante los descansos y cambios de turno.

El personal de informática, así como cualquier otro ajeno a la instalación, se debe identificar antes de entrar a ésta. El riesgo que proviene de alguien de la organización es tan grande como el de cualquier otro visitante. Solamente el personal autorizado por medio de una llave de acceso o por la gerencia debe ingresar a dichas instalaciones.

En los centros de cómputo se pueden utilizar los siguientes recursos:

- Puerta con cerradura. Requiere de la tradicional llave de metal, la cual debe ser difícil de duplicar.
- Puerta de combinación. En este sistema se usa una combinación de números para permitir el acceso. La combinación debe ser cambiada regularmente o cuando el empleado sea transferido o termine su función laboral dentro de ese centro de cómputo. Esto reduce el riesgo de que la combinación sea conocida por gente no autorizada.
- Puerta electrónica. El sistema más común es el que usa una tarjeta de plástico magnética como llave de entrada. Un código especial interno en la tarjeta es leído por un sensor activando el seguro de la puerta.
- Puertas sensoriales. Son activadas por los propios individuos con alguna parte de su cuerpo, como puede ser la huella dactilar, voz, retina, geometría de la mano o bien por la firma.
- Registros de entrada. Todos los visitantes deben firmar el registro de visitantes indicando su nombre, su compañía, la razón para la visita, la persona a la que visita. El registro se encuentra en la recepción del centro de cómputo. Es importante que el visitante proporcione una identificación con foto (licencia de manejo o credencial), ya que de otra forma podría inventar el nombre y no se tendría seguridad. Los empleados deben de portar la credencial de la empresa con foto, la cual además de servir de identificación, se utilizará para señalar las áreas de informática a las cuales tiene autorización de entrar.
- Videocámaras. Éstas deben ser colocadas en puntos estratégicos para que se pueda monitorear el centro. Los casetes deben ser guardados para su posible análisis.
- Escolta controladora para el acceso de visitantes. Todos los visitantes deben ser acompañados por un empleado responsable. Se consideran visitantes: amigos, proveedores, ingenieros de mantenimiento y auditores externos.
- Puertas dobles. Este equipo es recomendable para lugares de alta seguridad: se trata de dos puertas, donde la segunda sólo se pueda abrir cuando la primera está cerrada.
- Alarmas. Todas las áreas deben estar protegidas contra robo o accesos físicos no autorizados. Las alarmas contra robo deben ser usadas hasta donde sea posible en forma discreta, de manera que no se atraiga la atención hacia este dispositivo de alta seguridad. Tales medidas no sólo se deben aplicar en el centro de cómputo sino también en áreas adyacentes.

**Puertas
de seguridad**

DETECCIÓN DE HUMO Y FUEGO, EXTINTORES

Los detectores de fuego y humo se deben colocar tomando en cuenta la cercanía o no con los aparatos de aire acondicionado, ya que éstos pueden difundir el calor o el humo y no permitir que se active el detector.

El que se elija deberá ser capaz de detectar los distintos tipos de gases que desprenden los cuerpos en combustión. Algunos no detectan el humo o el vapor que proviene del plástico quemado que se usa como aislante en electricidad, y en consecuencia los incendios ocasionados por un cortocircuito tal vez no sean detectados.

Los detectores de humo y calor se deben instalar en el centro de cómputo, en las áreas de oficina, incluyendo el depósito de papelería y el perímetro físico de las instalaciones. Es necesario colocar detectores de humo y de calor bajo el piso y en los conductos de aire acondicionado.

Las alarmas contra incendios deben estar conectadas con la alarma central del lugar, o bien directamente con el departamento de bomberos.

La organización se debe cerciorar que los controles de seguridad contra incendios satisfagan los estándares mínimos del departamento de bomberos.

La documentación sobre los sistemas, la programación y las operaciones necesitan una protección contra incendios y debe tenerse un sistema de respaldo específico en el plan de contingencias. Se deben establecer procedimientos de respaldo que garanticen la actualización de toda la documentación de manera rutinaria; las copias de seguridad se deben almacenar en un lugar alejado, así como las copias de seguridad de los programas y los archivos, los cuales deben estar debidamente actualizados, documentados y fechados, para cuando sean requeridos.

Debe existir un sistema de detección de humo por ionización para aviso anticipado. Este sistema debe hacer sonar una alarma e indicar la situación del detector activado. El sistema de detección no debe interrumpir la corriente de energía eléctrica al equipo de cómputo. Se debe contar con un dispositivo manual de emergencia para cortar el sistema eléctrico y el aire acondicionado y deben instalarse en cada salida del centro de cómputo.

Se deben colocar en lugares estratégicos del centro de cómputo extintores portátiles de CO (recomendable para equipo eléctrico). El equipo para poder respirar debe estar a la mano, tanto en el área de cómputo como para el uso de los bomberos en caso de incendio. Se deben señalizar las salidas de emergencia (es conveniente que este señalamiento se encuentre en la parte inferior, cercano al piso, ya que en caso de humo sólo podrán ser visibles en la parte inferior).

En cuanto a los extintores, se debe revisar el número de éstos, su capacidad, fácil acceso, pesos y tipo de producto que utilizan. Es muy frecuente que se tengan extintores, pero puede suceder que no se encuentren recargados o bien que sean de tan difícil acceso o de un peso tal que sea difícil utilizarlos. Los extintores deben estar a la altura o tener un peso proporcional al de una mujer para que pueda utilizarlos.

Detectores
de humo

Equipos contra
incendio

Se debe
vocar may
gases tóx

Tamb
dio y si ha
das de em

Los m
producen

Los d
falso, repa
control co
de 0 a 60
boquillas
permitir l
que el ma
los equip

Es ne
en caso c
mente pr
de su usc
deben ha

Las c
debe con
Esta sala
cesarias,
propio e
en arma
dos hora

TEM

Algunos
persona
sistema
base en

- Dis
- Ma
- Mo
- Cúb
- Pér
- cal
- la i
- áre

Se debe cuidar que los de extintores no sean inadecuados, que puedan provocar mayor perjuicio a las máquinas (extintores líquidos) o que produzcan gases tóxicos.

También se debe evaluar si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su empleo; que existan suficientes salidas de emergencia, debidamente controladas para evitar robos.

Los materiales más peligrosos son las cintas magnéticas que, al quemarse, producen gases tóxicos, y el papel carbón, que es altamente inflamable.

Los detectores de ionización del aire deben colocarse en el techo y en el piso falso, repartirse de manera uniforme y estar conectados al tablero del equipo de control contra incendio. En este tablero se localiza un reloj que puede calibrarse de 0 a 60 segundos; para provocar un disparo de gas debe jalararse a través de boquillas de aspersión estratégicamente colocadas en el techo de la sala, para permitir la evacuación del personal y desconectar el sistema. Se debe verificar que el material utilizado para extinguir los incendios no provoque problemas a los equipos electrónicos.

Es necesario definir y documentar los procedimientos que se deben seguir en caso de incendio. Los planes de evacuación del centro deben estar plenamente probados y documentados. Además, se debe entrenar al personal acerca de su uso, ya que con frecuencia muchos empleados no saben exactamente qué deben hacer en caso de incendio.

Las cintas y discos magnéticos deben almacenarse en una sala aparte y se debe contar con un acceso al área en donde se localiza el equipo de cómputo. Esta sala debe contar con todas las condiciones ambientales y de seguridad necesarias, ya que la información almacenada ahí tiene más importancia que el propio equipo de cómputo. Las cintas y discos magnéticos deben almacenarse en armarios con paredes fabricadas especialmente para resistir por lo menos dos horas de fuego.

TEMPERATURA Y HUMEDAD

Algunos equipos grandes de cómputo (mainframes), o bien las computadoras personales que son usadas en zonas muy cálidas o desérticas, necesitan de un sistema de aire acondicionado diseñado para estar en operación constante, con base en los siguientes parámetros:

- Disipación térmica (BTU). La disipación térmica de cada unidad de sistemas es mostrada en unidades térmicas británicas por hora.
- Movimiento de aire (CFM). Los movimientos de aire se muestran en pies cúbicos por minuto.
- Pérdidas por transferencia de calor. Existen pérdidas por transferencia de calor, por las siguientes curvas: a) A través de paredes, pisos y techos, o por la iluminación; b) diferencias en temperatura entre la sala de cómputo y áreas adyacentes, y c) ventanas expuestas a los rayos del sol.

Los cambios de temperatura durante la operación del computador deben ser disminuidos. La variación cíclica de temperatura sobre el rango completo de operación no debe realizarse en menos de ocho horas.

La disipación térmica, el movimiento de aire, así como los mínimos y máximos de temperatura y humedad permitidos deben ser especificados por el proveedor del equipo, aunque la temperatura ideal recomendada es de 22°C. Generalmente la humedad debe ser agregada, ya que al enfriar el aire se remueve la mayoría del vapor de agua por condensación.

Se recomienda que se instalen instrumentos registradores de temperatura y humedad. Dichos instrumentos son necesarios para proveer un continuo registro de las condiciones ambientales en el área del equipo.

Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas de polvo, y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.

Tomando en cuenta lo anterior, en el siguiente cuestionario se consignan las características necesarias para evaluar una adecuada seguridad física:

UBICACIÓN Y CONSTRUCCIÓN DEL CENTRO DE CÓMPUTO

1. ¿El edificio donde se encuentra la computadora está situado a salvo de:

- | | |
|-------------|-----|
| Inundación? | () |
| Terremoto? | () |
| Fuego? | () |
| Sabotaje? | () |

2. ¿El centro de cómputo da al exterior? SI NO

3. Describa brevemente la construcción del centro de cómputo; de preferencia tomando en cuenta el material con que fue construido, así como el equipo (muebles, sillas, etc.) del centro.

4. ¿Tiene el cuarto de máquinas una instalación de escaparate y, si es así, pueden ser rotos los vidrios con facilidad? SI NO

5. ¿Está el centro de cómputo en un lugar de alto tráfico de personas? SI NO

6. ¿Se tiene materiales o paredes inflamables dentro del centro de cómputo? SI NO

7. ¿Se tiene paredes que despiden polvo? SI NO

8. ¿Se tiene paredes que no están adecuadamente selladas? SI NO

9. ¿Se tiene grandes ventanales orientados a la entrada o salida del sol? SI NO

10. ¿Existe lugar suficiente para los equipos? SI NO

11. ¿Está sobresaturada la instalación? sí NO

12. ¿Se tiene lugar previsto? Éste es el adecuado para:

- | | | |
|---|----|----|
| • Almacenamiento de equipos magnéticos. | sí | NO |
| • Formatos y papel para impresora. | sí | NO |
| • Mesas de trabajo y muebles. | sí | NO |
| • Área y mobiliario para mantenimiento. | sí | NO |
| • Equipo de telecomunicaciones. | sí | NO |
| • Área de programación. | sí | NO |
| • Consolas del operador. | sí | NO |
| • Área de recepción. | sí | NO |
| • Microcomputadoras. | sí | NO |
| • Fuentes de poder. | sí | NO |
| • Bóveda de seguridad (bóveda antiincendio bajo máxima protección). | sí | NO |

PISO ELEVADO O CÁMARA PLENA

13. ¿Se tiene piso elevado? sí NO

En caso afirmativo:

- | | | |
|-----------------------------------|----|----|
| 14. ¿Está limpia la cámara plena? | sí | NO |
| 15. ¿Es de fácil limpieza? | sí | NO |
| 16. ¿El piso es antiestático? | sí | NO |

AIRE ACONDICIONADO

17. ¿La temperatura en la que trabajan los equipos es la recomendada por el proveedor? sí NO

18. ¿Los ductos del aire acondicionado cuentan con alarmas contra intrusos? sí NO

19. ¿Los ductos de aire acondicionado están limpios? sí NO

20. ¿Se controla la humedad de acuerdo con las especificaciones del proveedor? sí NO

21. ¿De qué forma?

22. ¿Con qué periodicidad?

INSTALACIÓN ELÉCTRICA Y SUMINISTRO DE ENERGÍA

23. ¿Se cuenta con tierra física? sí NO

24. ¿La tierra física cumple con las disposiciones del proveedor de equipos de cómputo? sí NO

25. ¿El cableado se encuentra debidamente instalado? sí NO

26. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)? SÍ NO
27. ¿Los contactos de equipo de cómputo están debidamente identificados? SÍ NO
28. ¿En los contactos, está identificado el positivo, negativo y tierra física? SÍ NO
29. ¿Se cuenta con los planos de instalación eléctrica actualizados? SÍ NO
30. ¿Se tiene conectado a los contactos de equipo de cómputo otro equipo electrónico? SÍ NO
31. ¿Se tiene instalación eléctrica de equipo de cómputo independiente de otras instalaciones eléctricas? SÍ NO
32. ¿Se tiene precaución contra fauna nociva? SÍ NO
33. ¿El equipo contra fauna nociva está debidamente protegido y cuidado para no producir problemas al personal? SÍ NO
34. ¿Se utiliza material antiestático? SÍ NO
35. ¿Se tienen reguladores para los equipos de cómputo? SÍ NO
36. ¿Se verifica la regulación de las cargas máximas y mínimas? SÍ NO
En caso positivo, ¿con qué periodicidad?
-
37. ¿Se tiene equipo ininterrumpible? SÍ NO
38. ¿Dura el tiempo suficiente para respaldar los archivos o para continuar el proceso? SÍ NO
39. ¿Se tiene generadores de corriente ininterrumpida? SÍ NO
En caso positivo, ¿de qué tipo?
-
40. ¿Se prueba su funcionamiento? SÍ NO
En caso positivo, ¿con qué periodicidad?
-
41. ¿Se tiene switch de apagado en caso de emergencia en lugar visible? SÍ NO
42. ¿Los cables están dentro de paneles y canales eléctricos? SÍ NO
43. ¿Existen tableros de distribución eléctrica? SÍ NO

SEGURIDAD CONTRA DESASTRES PROVOCADOS POR AGUA

44. ¿Se cuenta con alarmas contra inundaciones? sí NO

SEGURIDAD DE AUTORIZACIÓN DE ACCESOS

45. ¿Se han adoptado medidas de seguridad en la dirección de informática? sí NO
46. ¿Existe una persona responsable de la seguridad? sí NO
47. ¿Existe personal de vigilancia en la institución? sí NO
48. ¿Se investiga a los vigilantes cuando son contratados directamente? sí NO
49. ¿Se controla el trabajo fuera de horario? sí NO
50. ¿Se registran las acciones de los operadores para evitar que realicen alguna que pueda dañar el sistema? sí NO
51. ¿Se identifica a la persona que ingresa? sí NO
52. ¿De qué forma?
-
53. ¿Cómo se controla el acceso?
- Vigilante. ()
 - Recepcionista. ()
 - Tarjeta de control de acceso. ()
 - Puerta de combinación. ()
 - Puerta con cerradura. ()
 - Puerta electrónica. ()
 - Puerta sensorial. ()
 - Registro de entradas. ()
 - Puertas dobles. ()
 - Escolta controlada. ()
 - Alarmas. ()
 - Tarjetas magnéticas. ()
 - Control biométrico. ()
 - Identificación personal. ()
54. ¿Existe vigilancia en el cuarto de máquinas las 24 horas? sí NO
55. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización? sí NO
56. ¿Son controladas las visitas y demostraciones en el centro de cómputo? sí NO
- ¿Cómo son controladas?
-

SEGURIDAD
FÍSICA

57. ¿Se registra el acceso al cuarto de personas ajenas a la dirección de informática? SÍ NO

DETECCIÓN DE HUMO Y FUEGO. EXTINTORES

58. ¿Existe alarma para:

- Detectar fuego (calor o humo) en forma automática? ()
- Avisar en forma manual la presencia del fuego? ()
- Detectar una fuga de agua? ()
- Detectar magnetos? ()
- No existe? ()

59. ¿Estas alarmas están:

- En el cuarto de máquinas? ()
- En la cintoteca y discoteca? ()
- En las bodegas? ()
- En otros lados? ()

60. ¿Existe alarma para detectar condiciones anormales del ambiente:

- En el cuarto de máquinas? ()
- En la cintoteca y discoteca? ()
- En la bodega? ()
- En otros lados? ()

¿Cuáles ?

61. ¿La alarma es perfectamente audible? SÍ NO

62. ¿La alarma está conectada:

- Al puesto de guardias? ()
- A la estación de bomberos? ()
- A algún otro lado? ()
- Otro. ()

63. ¿Existen extintores de fuego:

- Manuales? ()
- Automáticos? ()
- No existen. ()

64. ¿Se ha adiestrado el personal en el manejo de los extintores? SÍ NO

65. Los extintores, manuales o automáticos, funcionan a base de:

- Agua. ()
- Gas. ()
- Otros. ()

66. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?

SÍ NO

(NOTA: Verifique el número de extintores y su estado.)

67. Si es que existen extintores automáticos, ¿son activados por los detectores automáticos de fuego?

SÍ NO

68. Si los extintores automáticos son a base de agua, ¿se han tomado medidas para evitar que el agua cause más daño que el fuego?

SÍ NO

69. Si los extintores automáticos son a base de gas, ¿se han tomado medidas para evitar que el gas cause más daño que el fuego?

SÍ NO

70. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos, para que el personal:

- Corte la acción de los extintores por tratarse de falsa alarma?

SÍ NO

- Pueda cortar la energía eléctrica?

SÍ NO

- Pueda abandonar el local sin peligro de intoxicación?

SÍ NO

- ¿Es inmediata su acción?

SÍ NO

71. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

SÍ NO

72. ¿Saben qué hacer los operadores del cuarto de máquinas en caso de que ocurra una emergencia ocasionada por fuego?

SÍ NO

73. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?

SÍ NO

74. ¿Existe salida de emergencia?

SÍ NO

75. ¿Esta puerta sólo es posible abrirla:

- Desde el interior?

()

- Desde el exterior?

()

- Por ambos lados?

()

76. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?

SÍ NO

77. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?

SÍ NO

78. ¿Se han tomado medidas para minimizar la posibilidad de fuego:

- Evitando artículos inflamables en el cuarto de máquinas?

()

- Prohibiendo fumar?

()

- Vigilando y manteniendo el sistema eléctrico?

()

- No se ha previsto.

()

79. ¿Se tienen identificadas y señaladas las salidas de emergencia?

SÍ NO

80. ¿Se encuentran las señalizaciones en la parte inferior y superior de los pasillos?

SÍ NO

81. ¿Se cuenta con máscaras contra gases o sistemas portátiles de oxígeno?

SÍ NO

82. ¿Se tiene bóveda contra incendio?

SÍ NO

SEGURIDAD EN GENERAL

83. ¿Se controla el préstamo de:

- Elementos magnéticos? ()
- Equipo? ()
- Software? ()

84. Explique la forma en que se ha clasificado la información: vital, esencial, no esencial, etcétera.

85. ¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?

SÍ NO

86. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad, etc.) para garantizar su integridad en caso de incendio, inundación, terremoto, etcétera.

87. ¿Se tienen establecidos procedimientos de actualización para estas copias?

SÍ NO

88. Indique el número de copias que se tienen, de acuerdo con la forma en que se clasifica la información.

89. ¿Existe departamento de auditoría interna en la institución?

SÍ NO

90. ¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?

SÍ NO

91. ¿Qué tipos de controles ha propuesto?

92. ¿Se cumplen?

SÍ NO

93. ¿Se auditan los sistemas en operación?

SÍ NO

94. ¿Con qué frecuencia?:

- Cada seis meses. ()
- Cada año. ()
- Otra (especifique). ()

95. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién?:

- Usuario. ()
- Director de informática. ()
- Jefe de análisis. ()
- Programador. ()
- Otras (especifique). ()

96. La solicitud de modificaciones a los programas se hacen en forma:

- Oral. ()
- Escrita. ()

(En caso de ser escrita solicite formatos.)

97. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?

SÍ NO

98. ¿Existe control estricto en las modificaciones?

SÍ NO

99. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?

SÍ NO

100. ¿Se verifica identificación:

- De la terminal? ()
- Del usuario? ()
- No se pide identificación. ()

101. ¿Se ha establecido el nivel de usuario de la información?

SÍ NO

102. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se dé aviso al responsable de ella?

SÍ NO

103. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?

SÍ NO

104. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

SÍ NO

¿Cuáles son?

- Recepción de documentos. ()
- Información confidencial. ()
- Captación de documentos. ()
- Cómputo electrónico. ()
- Programas. ()
- Discotecas y cintotecas. ()
- Documentos de salida. ()
- Archivos magnéticos. ()

- | | |
|--|-----|
| • Operación del equipo de computación. | () |
| • En cuanto al acceso de personal. | () |
| • Identificación del personal. | () |
| • Policía. | () |
| • Seguros contra robo e incendio. | () |
| • Cajas de seguridad. | () |
| • Otras (especifique). | () |

SEGURIDAD EN CONTRA DE VIRUS

Un virus de computadora es un programa o serie de instrucciones que al infectar otros programas provoca que se modifiquen sus instrucciones, o bien que al infectar los datos y la información provoque variaciones en los resultados inicialmente previstos. Su comportamiento y consecuencias pueden evolucionar mediante un número finito de instancias.

Los daños que puede provocar un virus son de muy diversa índole, pero uno de los principales es el psicológico, ya que muchos usuarios, cuando tienen cualquier tipo de problema, lo primero que piensan es que es un virus, sin examinar si se equivocaron o si el sistema tiene problemas (*bugs*), lo primero en que se piensa es en un virus.

Los daños más comunes son los siguientes:

Daños de virus

- Suplantación de datos.
- Eliminación aleatoria.
- Destrucción de la producción.
- Modificación de los códigos de protección.
- Bloqueo de redes.
- Cambios de información entre usuarios.
- Por medio de un canal encubierto, cambiar, acceder o difundir claves de seguridad.
- Modificación de información de salida o de pantallas.
- Saturación, reducción de disponibilidad o cambio de parámetros.
- Combinación de los anteriores.

En un principio los virus infectaban la parte protegida de la memoria o de los programas; después, se extendieron, en el sentido de que no sólo infectaban al usuario, sino a otros posibles usuarios de la información. Esto se presentaba principalmente en las redes y en las bases de datos, pero en la actualidad también se tiene el problema de persistencia, ya que el virus puede estar encapsulado, hasta que suceda un evento (fecha), o bien tenga posibilidades de infectar al sistema.

Para evitar que los virus se diseminen por todo el sistema computarizado o por las redes se debe:

- Utilizar paquetes y programas originales.
- Limitar la utilización en común. Sólo permitir el acceso a la parte del sistema o del programa autorizado para cada usuario.

- Limitar el tránsito. Evitar que todos los usuarios puedan navegar por todos los sistemas. Restringir el tránsito entre usuarios o entre sistemas (lo cual es difícil y va en muchos casos en contra de la filosofía de uso de la información y de comunicación).
- Limitar la programación y controlarla adecuadamente.

El problema de los virus en muchas ocasiones son los ciclos interminables; ya que se desinfeste una parte del sistema o algunos usuarios, el virus puede seguir latente e infectar nuevamente al sistema. Esto sucede sobre todo cuando el sistema se encuentra en operación. Para poder tener una cura parcial se debe dividir el sistema o los usuarios de tal forma que se pueda desinfectar una parte sin suspender totalmente la operación del sistema. Por lo anterior se recomienda que a la primera posibilidad de virus se apague el sistema y se evalúe hasta ser desinfectado, lo cual a su vez puede provocar también el problema psicológico de estar pensando que la primera falla que se tenga, se trate de un virus.

Se debe tener vacunas contra virus; el problema es que generalmente estas vacunas no cubren todos los virus, por lo que se requiere actualizarlas constantemente.

Otra forma de protegerse es a través de analizadores de virus. Estos programas detectan la existencia de un virus en el momento de la inicialización (*bootstrap*) de las computadoras personales. Estos analizadores presentan problemas, ya que son costosos y poco efectivos para todos los diferentes virus, aunque son actualmente muy populares en el mercado. Un analizador realmente efectivo debe detectar el virus antes de que ataque.

Entre los problemas en la utilización de analizadores y de vacunas contra virus están:

- Son efectivos solamente contra virus conocidos o patrones de ataques conocidos.
- Utilizan muchos recursos y tiempo para detectar virus en redes para analizar un sistema en busca de los patrones conocidos.
- En algunos de los casos, los ataques vienen del interior de la organización.
- Para que puedan seguir siendo efectivos se deben actualizar constantemente.
- Algunos no son efectivos para detectar virus evolutivos, los cuales cada día son más frecuentes.
- Algunos producen resultados positivos falsos, creando efectos psicológicos.
- Las personas no utilizan los programas analizadores de manera confiable.

PROTECCIONES CONTRA VIRUS Y ELEMENTOS A AUDITAR

Se debe evaluar y auditar que todos los paquetes que se utilicen sean originales; el problema está en descubrir qué elemento puede servir para determinar que el paquete es original.

**Analizadores
de virus**

Para ello se tiene la factura, el disquete original, el manual, la hoja de garantía, aunque en algunos casos se compra la autorización corporativa (licencia) para el uso de un número determinado de copias, lo cual dificulta evaluar que todas las copias que se tienen sean autorizadas.

En un principio, los virus se encontraban principalmente en los programas de juegos, por lo que se deben eliminar los juegos en todos los equipos de las oficinas, ya que éstos, en primer lugar, no tienen por qué estar en computadoras para trabajo y, en segundo, esto disminuye la posibilidad de infectar las computadoras.

Se debe verificar que todas las computadoras tengan analizadores y desinfectadores de virus instalados y actualizados.

Los sistemas deben estar debidamente aislados, de tal forma que un sistema sólo pueda acceder la información que requiera y no pueda entrar a otro sistema o base de datos.

Se debe prohibir la utilización de disquetes externos, a menos que sean debidamente probados y desinfectados.

Se debe vigilar como parte esencial y primaria que exista una defensa contra la introducción de algún virus, y en caso de que se infecten las computadoras, tener un adecuado procedimiento para desinfectarlas.

Deben de existir políticas y procedimientos de actuación en caso de que exista un virus, tanto para computadoras personales como para redes, y la forma de desinfectarlos y restaurar el sistema (política de encuéntralo, elimínalo y aléjate). En algunas partes se han creado los equipos conocidos como CERT (*Computer Emergency Response Team*: equipo de respuesta de emergencias de computadora), cuya función es preparar a la organización para dar respuesta a problemas relacionados con la computadora, los cuales tienen bajo su responsabilidad los planes de contingencia, emergencia y contra virus.

El equipo tiene la responsabilidad de detectar cualquier problema de virus, capacitar a los usuarios, determinar las precauciones técnicas necesarias, y asegurar que los sistemas técnicos y humanos funcionen adecuadamente en caso de una emergencia.

Desafortunadamente, las leyes contra los virus, principalmente los maliciosos, no han evolucionado al ritmo de la tecnología (se considera delito sólo cuando la persona actuó en forma maliciosa e intencional), y la detección del origen de los virus es cada día más complicada.

Internet

Internet es una asombrosa creación que ha reforzado nuestra economía; representa todavía un trabajo en marcha, capaz de ser derrumbado con sorprendente facilidad. Incluso los gigantes del cibercomercio no son más resistentes. Todo lo que se necesita es un bien dirigido ataque de degeneración de servicios (DOS, por sus siglas en inglés) para causar daños, al menos temporalmente.

La degeneración del servicio se hace por medio de plantar, primero, un software "esclavo" en computadoras de terceras partes o "zombies". En un momento, esos programas esclavos utilizan la capacidad de procesamiento de

sus an
que sor
En
Estados
siones
corto p
La
dores c
ataque
en los c
servicio
cias de
de info
que ab
Lo
hackers
perder
medio
La
ble al
millon
gro la
en los
tos no
Si
transm
rios es
vulner
Co
de cab
ras las
Lo
fin de
Se est
servic
dios d
legítim
Po
vulner

- Se
- pa
- N
- la

**La degeneración
del servicio DOS**

sus anfitriones para enviar una torre de mensajes destructivos a los servidores que son su verdadero blanco.

En 1998, el Equipo de Respuestas a Emergencias Informáticas (CERT) de Estados Unidos comenzó a prevenir a la comunidad cibernética sobre las incursiones de DOS, y admitió que: "No podrán prometer que esto desaparezca a corto plazo."

La solución es la protección de todo ciberespacio contra programas depredadores que reclutan a decenas y hasta cientos de máquinas inocentes para un ataque de DOS. Los proveedores de servicio de Internet deberán instalar filtros en los datos que transmiten, y los auditores deberán cuidar que sólo se utilicen servicios de Internet con proveedores que proporcionen este servicio. Las agencias de seguridad deberán introducir agentes zombies que husmeen en busca de información indeseada, o bien por medio de rompecabezas criptográficos que abrumen a las máquinas agresoras.

Los *hackers* malévolos, que intentan obtener ganancias financieras, o los *hackers* conocidos como de sombrero negro, que intentan divertirse al echarle a perder el día a un usuario de Internet, en la actualidad son combatidos por medio de *hackers* de sombrero blanco, que trabajan en firmas de seguridad.

La misma conexión que hace a la red tan robusta, también la deja vulnerable al efecto del eslabón débil de la cadena. La apertura y facilidad con que millones de personas pueden compartir la información, también pone en peligro la intimidad. La mayoría de los ataques no son diseñados para introducirse en los sistemas, sino simplemente para hacerlos más lentos. Pero los allanamientos no son difíciles y pueden venir más problemas.

Si los datos no se protegen apropiadamente, la información personal que se transmite en línea deja a la Web vulnerable al robo de identidad. Los funcionarios estadounidenses admiten que atrapan a 10 por ciento de quienes tratan de vulnerar o penetrar las computadoras del gobierno.*

Con un número creciente de conexiones permanentes, tales como módem de cable, los *hackers* malévolos podrían husmear digitalmente por las cerraduras las vidas de las personas y la privacidad de las empresas.

Los *hackers* usan herramientas de software para merodear por el sistema, a fin de encontrar debilidades que los operadores de redes no han enmendado. Se está a merced de los administradores de sitios web y de proveedores de servicios de Internet para mantenernos a resguardo contra los defectos y remedios de seguridad. Lo más peligroso es que los *hackers* podrían obtener empleos legítimos en cualquiera de las organizaciones que han sido afectadas por ellos.

Por lo anterior, para que el auditor se asegure que la información no sea tan vulnerable:

- Se debe utilizar siempre software antivirus y actualizarlo con frecuencia para alejar programas destructivos.
- No se debe permitir que comerciantes en línea almacenen información de la empresa o de las personas.

* *Newsweek*, 23 de febrero de 2000.

- Se debe utilizar contraseñas difíciles que combinen números y letras, y se deben cambiar con frecuencia.
- Se deben utilizar diferentes contraseñas para sitios en la red y aplicaciones, para despistar a posibles *hackers*.
- Se debe utilizar la versión más actualizada del navegador de red, software de E-mail y otros programas.
- Se deben enviar los números o información confidencial solamente a sitios seguros; se debe buscar el icono de candado o llave en el navegador.
- Se debe confirmar que se trata del sitio que se busca. Hay que tener cuidado al teclear.
- Se deben usar programas de seguridad para controlar los *cookies* que envían datos de vuelta a los sitios web.
- Se debe instalar software para inspeccionar el tráfico si se usa DSL o un módem de cable para conectarse a la red.
- No se deben abrir agregados de E-mail a menos que se conozca la fuente del mensaje recibido.

SEGUROS

Los seguros de los equipos en algunas ocasiones se dejan en segundo término, aunque son de gran importancia. Se tiene poco conocimiento de los riesgos que entraña la computación, ya que en ocasiones el riesgo no es claro para las compañías de seguros, debido a lo nuevo de la herramienta, a la poca experiencia existente sobre desastres y al rápido avance de la tecnología.

Como ejemplo de lo anterior tenemos las pólizas de seguros contra desastres, ya que algunos conceptos son cubiertos por el proveedor del servicio de mantenimiento, lo cual hace que se duplique el seguro, o bien que sobrevengan desastres que no son normales en cualquier otro tipo de ambiente.

Se deben verificar las fechas de vencimiento de las pólizas, pues puede suceder que se tenga la póliza adecuada pero vencida, y que se encuentre actualizada con los nuevos equipos.

El seguro debe cubrir todo el equipo y su instalación, por lo que es probable que una sola póliza no pueda cubrir todo el equipo con las diferentes características (existe equipo que puede ser transportado, como computadoras personales, y otras que no se pueden mover, como unidades de disco duro), por lo que tal vez convenga tener dos o más pólizas por separado, cada una con las especificaciones necesarias.

Se debe tomar en cuenta que existen riesgos que son difíciles de evaluar y de asegurar, como la negligencia.

El costo de los equipos puede variar, principalmente en aquellos países que tienen grandes tasas de inflación o de devaluación, por lo que los seguros deben estar a precio de compra (valor de adquisición de nuevo equipo con iguales características) y no a precio al momento de contratación del seguro.

El seguro debe cubrir tanto daños causados por factores externos (terremoto, inundación, etc.) como internos (daños ocasionados por negligencia de los operadores, daños debidos al aire acondicionado, etcétera).

También se debe asegurar contra la pérdida de los programas (software), de la información, de los equipos y el costo de recuperación de lo anterior.

En el caso de los programas se tendrá en cuenta en el momento de asegurarlos el costo de elaboración de determinado equipo, el costo de crearlos nuevamente y su valor comercial. En el caso del personal, se pueden tener fianzas contra robo, negligencia, daños causados por el personal, sabotaje, acciones deshonestas, etcétera.

Es importante que la dirección de informática esté preparada para evitar en lo posible el daño físico al personal, oficinas, equipo de cómputo, así como al sistema de operación. Además, deberá tener cuidado de que existan normas y prácticas eficaces.

Como ejemplo y en forma genérica, por lo común un seguro de equipo de cómputo considera lo siguiente:

- Bienes que se pueden amparar. Cualquier tipo de equipo electrónico, como: de cómputo, de comunicación, de transmisión de radio y televisión, etc. Con excepción de los que formen parte de equipo especial en automóviles, camiones, buques, aviones.
- Riesgos cubiertos. La cobertura básica cubre contra todo riesgo de pérdida súbita, accidental e imprevista, con excepción de las exclusiones que se indican en las condiciones generales de la póliza. Esta cobertura ampara riesgos como: incendio, rayo, explosión, implosión, arcos voltaicos, cortocircuitos, sobretensiones, etcétera.
- Riesgos excluidos, pero que pueden ser cubiertos bajo convenio expreso, como son: terremoto y erupción volcánica; huracán, ciclón y tifón; equipos móviles o portátiles; huelgas y motín; hurto.
- Exclusiones. Las indicadas en las condiciones generales de cada seguro.
- Suma asegurada. En todos los casos se tiene que reportar como suma asegurada el valor de reposición de los equipos a asegurar (a valor nuevo sin descontar depreciación).
- Primas, cuotas y deducibles. Dependen del tipo de equipo.
- Indemnización en caso de siniestro. Las pérdidas parciales se indemnizan a valor de reposición (valor nuevo) y las pérdidas totales a valor real (valor nuevo menos depreciación).

CONDICIONES GENERALES DEL SEGURO DE EQUIPO ELECTRÓNICO

En la póliza de seguro se certifica que, a reserva de que el asegurado haya pagado a los aseguradores la prima mencionada en la parte descriptiva, y con sujeción a los demás términos, exclusiones, disposiciones y condiciones contenidas o endosadas, los aseguradores indemnizarán en la forma y hasta los límites estipulados en póliza.

Una vez que la instalación inicial y la puesta en marcha de los bienes asegurados haya finalizado satisfactoriamente, este seguro se aplica, ya sea que los bienes estén operando o en reposo, o hayan sido desmontados con el propósito de ser limpiados o reparados, o mientras sean trasladados dentro de los predios estipulados, o mientras se estén ejecutando las operaciones mencionadas, o durante el remontaje subsiguiente.

Exclusiones generales

Los aseguradores no indemnizarán al asegurado respecto a pérdidas o daños directa o indirectamente causados o agravados por:

- Guerra, invasión, actividades de enemigo extranjero, hostilidades (con o sin declaración de guerra, guerra civil, rebelión, revolución, insurrección, motín, tumulto, huelga, paro decretado por el patrón, conmoción civil, poder militar o usurpado, grupos de personas maliciosas o personas actuando a favor o en conexión con cualquier organización política, conspiración, confiscación, requisición, destrucción o daño por orden de cualquier gobierno *de jure* o *de facto*, o de cualquier autoridad pública.
- Reacción nuclear, radiación nuclear o contaminación radiactiva.
- Acto intencional o negligencia manifiesta del asegurado o de sus representantes.

La compañía aseguradora en ningún caso será responsable por: pérdidas, daños materiales, perjuicios o gastos causados, directa o indirectamente, por falta de funcionamiento o por fallas, errores o deficiencias de cualquier dispositivo, aparato, mecanismo, equipo, instalación o sistema, sea o no propiedad del asegurado o que esté bajo control o simple posesión, como consecuencia de la incapacidad de sus componentes físicos o lógicos.

Para efectos de esta cláusula, se entiende por componentes lógicos los sistemas operativos, programas, bases de datos, líneas de código, aplicaciones y demás elementos de computación electrónica, también denominados software, y por componentes físicos, los dispositivos electrónicos o electromecánicos, tales como procesadores, microprocesadores, tarjetas de circuitos impresos, discos, unidades lectoras, impresoras, reproductoras, conmutadores, equipos de control y demás elementos conocidos bajo la denominación genérica de hardware.

No obstante lo anterior, y únicamente aplicable para los riesgos de incendio, rayo y/o explosión, caída de aviones (u objetos caídos de ellos), vehículos y humo, granizo, terremoto, erupción volcánica e inundación, un daño directo ocurrido de forma accidental, súbita e imprevista, generado consecuentemente por las pérdidas o daños excluidos por la presente cláusula, gozará de cobertura, siempre y cuando se establezca como amparado en las condiciones del contrato de seguro.

En cualquier acción, litigio y otro procedimiento en el cual los aseguradores alegaran que, a causa de las disposiciones de las exclusiones anteriores, alguna

pérdida, destrucción o daño no estuviera cubierto por este seguro, entonces estará a cargo del asegurado el probar que tales pérdidas, destrucciones o daños sí están cubiertos por este seguro.

Condiciones generales

- La responsabilidad de los aseguradores sólo procederá si se observan y cumplen fielmente los términos de la póliza, en lo relativo a cualquier cosa que debe hacer o que deba cumplir el asegurado.
- El asegurado, por cuenta propia, tomará todas las precauciones razonables y cumplirá con todas las recomendaciones hechas por los aseguradores, con objeto de prevenir pérdidas o daños y cumplirá con los requerimientos legales y con las especificaciones técnicas del fabricante.
- Los representantes de los aseguradores podrán en cualquier fecha razonable inspeccionar y examinar el riesgo, y el asegurado suministrará a los representantes de los aseguradores todos los detalles e informaciones necesarias para la apreciación del riesgo.
- El asegurado notificará inmediatamente a los aseguradores, por telegrama y por carta, cualquier cambio material en el riesgo y tomará a su propio costo todas las precauciones adicionales que las circunstancias requieran para garantizar un funcionamiento confiable de la maquinaria asegurada. Si fuera necesario, se ajustarán el alcance de la cobertura y/o la prima, según las circunstancias. El asegurado no hará ni admitirá que se hagan cambios materiales que aumenten el riesgo, a menos que los aseguradores le confirmen por escrito la continuación del seguro.
- Al ocurrir cualquier siniestro que pudiera dar lugar a una reclamación, según esta póliza, el asegurado deberá:

- Notificar inmediatamente a los aseguradores, por teléfono o telégrafo, y confirmarlo por carta certificada indicando la naturaleza y la extensión de la pérdida o daños.
- Tomar todas las medidas dentro de sus posibilidades para minimizar la extensión de la pérdida o daño.
- Conservar las partes dañadas y ponerlas a disposición de un representante o experto de los aseguradores para su inspección.
- Suministrar toda aquella información y pruebas documentales que los aseguradores le requieran.
- Informar a las autoridades judiciales respectivas, en caso de pérdidas o daños debidos a robo con violencia, asalto y/o hurto.

Los aseguradores no serán responsables por pérdidas o daños, de los cuales no hayan recibido notificación dentro de un determinado número de días después de su ocurrencia.

Una vez notificado a los aseguradores, podrá el asegurado llevar a cabo las reparaciones o reemplazos de pérdidas de menor cuantía, debiendo en todos los demás casos dar a un representante de los aseguradores oportunidad de

inspeccionar la pérdida antes de que se efectúen las reparaciones o alteraciones. Si el representante de los aseguradores no llevara a cabo la inspección dentro de un lapso considerado como razonable bajo estas circunstancias, el asegurado estará autorizado a realizar las reparaciones o reemplazos respectivos.

La responsabilidad de los asegurados con respecto a cualquier bien asegurado bajo la póliza cesará; si dicho bien continúa operando después de una reclamación, sin haber sido reparado a satisfacción de los aseguradores o si se realizaran las reparaciones provisionales sin consentimiento de los aseguradores.

- El asegurado, por cuenta de los aseguradores, hará y permitirá realizar todos aquellos actos que puedan ser necesarios o requeridos por los aseguradores para defender derechos o interponer recursos o para obtener compensaciones o indemnizaciones de terceros (que no están asegurados en esta póliza), y respecto a los cuales los aseguradores tengan o tuvieran derecho a subrogación en virtud del pago de dichas compensaciones o indemnizaciones por cualquier pérdida o daño, ya sea que dichos actos o cosas fueran o llegasen a ser necesarias o requeridas antes o después de que los aseguradores indemnizaran al asegurado.
- Si en los términos de la póliza surgiera alguna diferencia respecto a la suma a pagar (habiéndose por otro lado admitido la responsabilidad), tales divergencias serán sometidas a la decisión de un árbitro designado por escrito por las partes en conflicto.
- Los beneficios derivados de la póliza se perderán:
 - Si la información proporcionada por el asegurado no corresponde a las realidades existentes, si la reclamación fuera en alguna forma fraudulenta, o si se hicieran o se emplearan declaraciones falsas para apoyar la reclamación.
 - Si al hacer una reclamación, ésta es rechazada por los aseguradores y si no se iniciara acción o demanda.

Daños materiales

Alcance de la cobertura. Los aseguradores, en caso de que esté pagada la póliza, se encuentre vigente y que la pérdida o daño no se encuentren específicamente excluidos, indemnizarán al asegurado por tales pérdidas o daños, en efectivo, o reparando o reemplazándolos (a elección de los aseguradores) hasta una suma que por cada anualidad de seguro no exceda de la suma asegurada asignada a cada bien asegurado en la parte descriptiva y de la cantidad total garantizada por la póliza.

Exclusiones especiales

Sin embargo, los aseguradores no serán responsables, a menos que se estipule lo contrario en las pólizas, de:

- El deducible estipulado.
- Pérdidas o daños causados directa o indirectamente por resultantes de terremoto, temblor, golpe de mar por maremoto y erupción volcánica, ciclón o huracán.
- Pérdidas o daños causados directa o indirectamente por hurto, robo con o sin violencia y/o asalto.
- Pérdidas o daños causados por cualquier fallo o defecto existente al inicio del seguro, que sean conocidos por el asegurado o por sus representantes responsables de los bienes asegurados, sin tomar en cuenta que dichos fallos o defectos fueran o no conocidos por los aseguradores.
- Pérdidas o daños causados directa o indirectamente por fallo o interrupción en el aprovisionamiento de corriente eléctrica de la red pública, de gas o agua.
- Pérdidas o daños que sean consecuencia directa del funcionamiento continuo (desgaste, cavilación, erosión, corrosión, incrustaciones) o deterioro gradual debido a condiciones atmosféricas.
- Cualquier gasto incurrido con objeto de eliminar fallos operacionales, a menos que dichos fallos fueren causados por pérdidas o daño indemnizable ocurrido a los bienes asegurados.
- Cualquier gasto erogado respecto al mantenimiento de los bienes asegurados; tal exclusión se aplica también a las partes recambiadas en el curso de dichas operaciones de mantenimiento.
- Pérdidas o daños cuya responsabilidad recaiga en el fabricante o el proveedor de los bienes asegurados, ya sea legal o contractualmente.
- Pérdidas o daños a equipos arrendados o alquilados, cuando la responsabilidad recaiga en el propietario, ya sea legalmente o según convenio de arrendamiento y/o mantenimiento.
- Pérdida o responsabilidades consecuenciales de cualquier tipo.
- Pérdidas o daños a partes desgastables, tales como bulbos, válvulas, tubos, bandas, fusibles, sellos, cintas, alambres, cadenas, neumáticos, herramientas recambiables, lentes, rodillos, grabados, objetos de vidrio, porcelana o cerámica a cualquier medio de operación (por ejemplo: lubricantes, combustibles, agentes químicos).
- Defectos estéticos, tales como raspaduras de superficies pintadas, pulidas o barnizadas.

Los aseguradores serán empero responsables respecto a pérdidas o daños mencionados anteriormente, cuando las partes especificadas hayan sido afectadas por una pérdida o daño indemnizable ocurrido a los bienes asegurados.

Entre las exclusiones que pueden contratarse mediante convenio expreso se encuentran:

- Terremoto y erupción volcánica.
- Huracán, ciclón y tifón.
- Huelgas y conmoción civil.
- Hurto y/o robo sin violencia.
- Robo con violencia y/o asalto.

Disposiciones aplicables

Es requisito indispensable del seguro que la suma asegurada sea igual al valor de reposición del bien asegurado por otro bien nuevo de la misma clase y capacidad, incluyendo fletes, impuestos y derechos aduaneros, si los hubiese, y gastos de montaje.

Si la suma asegurada es inferior al monto que debió asegurarse, los aseguradores indemnizarán solamente aquella proporción que la suma asegurada guarde con el monto que debió asegurarse. Cada uno de los bienes estará sujeto a esta condición separadamente.

Bases de la indemnización:

a) En aquellos casos en que pudieran repararse los daños ocurridos a los bienes asegurados, los aseguradores indemnizarán aquellos gastos que sean necesarios erogar para dejar la unidad dañada en las condiciones existentes inmediatamente antes de ocurrir el daño.

Esta compensación también incluirá los gastos de desmontaje y remontaje incurridos con el objeto de llevar a cabo las reparaciones, así como también fletes ordinarios al y del taller de reparación; impuestos y derechos aduaneros, si los hubiese, o siempre que tales gastos hubieran sido incluidos en la suma asegurada. Si las reparaciones se llevaran a cabo en un taller propiedad del asegurado, los aseguradores indemnizarán los costos de materiales y jornales.

No se hará reducción alguna en concepto de depreciación respecto a partes repuestas, pero sí se tomará en cuenta el valor de cualquier salvamento que se produzca.

Si el costo de reparación igualara o excediera el valor actual que tenían los bienes asegurados inmediatamente antes de ocurrir el daño, se hará el ajuste sobre la base de lo estipulado en el siguiente párrafo.

b) En caso de que el objeto asegurado fuera totalmente dañado, robado o destruido, los aseguradores indemnizarán hasta el monto del valor actual que tuviere el objeto inmediatamente antes de ocurrir el siniestro, incluyendo gastos por fletes ordinarios, montaje y derechos aduaneros, si los hubiera, y siempre que tales gastos estuvieran incluidos en la suma asegurada.

Se calculará el susodicho valor actual deduciendo del valor de reposición del objeto una cantidad adecuada por concepto de depreciación. Los aseguradores también indemnizarán los gastos que normalmente se erogan para desmontar el objeto destruido, pero tomando en consideración el valor de salvamento respectivo. El bien destruido ya no quedará cubierto por la póliza, debiéndose declarar todos los datos correspondientes al bien que los reemplace, con el fin de incluirlo en la parte descriptiva de la póliza.

A partir de la fecha en que ocurra un siniestro indemnizable, la suma asegurada quedará reducida, por el resto de la vigencia, en la cantidad indemnizada, a menos que fuera restituida la suma asegurada.

Cualquier gasto adicional erogado por concepto de tiempo extra, trabajo nocturno y trabajo en días festivos, fletes expreso, etc., sólo estará cubierto por el seguro si así se hubiera convenido por medio de un endoso.

Según la póliza no serán recuperables los gastos por modificaciones, adiciones, mejoramiento, mantenimiento y reacondicionamiento.

Los aseguradores responderán por el costo de cualquier reparación provisional, siempre que ésta forme parte de la reparación final, y que no aumente los gastos totales de reparación.

Los aseguradores sólo responderán por daños después de haber recibido a satisfacción las facturas y documentos comprobantes, de haberse realizado las reparaciones o efectuado los reemplazos, respectivamente.

SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO

En la actualidad los programas y equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

1. Se debe restringir el acceso a los programas y a los archivos.
2. Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
3. Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados. Como ejemplo de los problemas ocasionados por un mal uso de los respaldos está el de aquella instalación en que al mismo tiempo que se capturaba información para el archivo maestro, el programador hacía pruebas y cambios a los programas. El capturista capturaba el 15 de enero y en ese momento el programador deseaba que pusieran en el mismo usuario que el capturista la información del 13 de enero. El capturista continuaba capturando pero ya no en los archivos del 15 sino del día 13, y cuando volvían nuevamente a poner la información del día 15 descubrían que existía la información que habían capturado pero no la encontraba.
4. No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
5. En los casos de información confidencial, ésta debe usarse, de ser posible, en forma codificada o criptografiada.
6. Se debe realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.
7. Se debe monitorear periódicamente el uso que se les está dando a las terminales.
8. Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.
9. El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.

10. Debe existir una perfecta división de responsabilidades entre los capturistas de datos y los operadores de computadora, y entre los operadores y las personas responsables de las librerías.
11. Deben existir registros que reflejen la transferencia de información entre las diferentes funciones de un sistema.
12. Debe controlarse la distribución de las salidas (reportes, cintas, etcétera).
13. Se deben guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.
14. Se debe tener un estricto control sobre el transporte de discos y cintas de la sala de cómputo al local de almacenaje distante.
15. Se deben identificar y controlar perfectamente los archivos.
16. Se debe tener estricto control sobre el acceso físico a los archivos.
17. En el caso de programas, se debe asignar a cada uno de ellos una clave que identifique el sistema, subsistema, programa y versión. Esto nos servirá para identificar el número de veces que se ha compilado o corrido un programa, y permitirá costear en el momento que se encuentre un sistema en producción. También evitará que el programador ponga nombres que no signifiquen nada y que sean difíciles de identificar, y que el programador utilice la computadora para trabajos personales.

Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Por ejemplo, existe un gran robo de información confidencial por medio del fotocopiado. Se da el caso de compañías en que sus competidores han conocido los planes confidenciales por medio del desperdicio de papel, o bien el caso de una compañía que elaboró una serie de políticas de personal sumamente confidenciales y que los operadores y, consecuentemente, toda la compañía, conoció la información al momento de obtener los listados por medio de la computadora. Lo más drástico en este caso es que los listados que se obtuvieron eran planes que servirían como alternativas de solución, pero que no habían sido autorizados. Para controlar este tipo de información se debe:

- Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.
- Sólo el personal autorizado debe tener acceso a la información confidencial.
- Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.
- Controlar el número de copias, y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

El factor más importante para la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados, por lo cual se debe considerar la necesidad de tener un alto grado de seguridad desde el momento de hacer el diseño preliminar del sistema, siguiendo los pasos del diseño detallado y de la programación.

El siguiente factor en importancia es contar con los respaldos y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

En los
de datos y
cuanto a

- Equip
- Contr
- corre
- Defin
- Requ
- Estár
- Estár
- Audi
- punt

SEG

En un m
las comp
siniestro
el motiv
menor ti
futuro e
ción neg

En t
existe un
establec
que ocu
te posib

En u
conting

Ana
anudac
en caso
operati

- En
- pro

o

o

En los sistemas de cómputo en que se tiene sistemas en tiempo real, bases de datos y red de computadoras, se deben tomar medidas de alta seguridad en cuanto a:

- Equipo, programas y archivos.
- Control de aplicaciones por terminal (definir qué aplicaciones se pueden correr en una terminal específica).
- Definir una estrategia de seguridad de la red y de respaldos.
- Requerimientos físicos.
- Estándar de aplicaciones y de control.
- Estándar de archivos.
- Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

SEGURIDAD AL RESTAURAR EL EQUIPO

En un mundo que depende cada día más de los servicios proporcionados por las computadoras, es vital definir procedimientos en caso de una posible falla o siniestro. Cuando ocurre una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación existe un riesgo aceptable; es necesario analizar y entender estos factores para establecer los procedimientos que permitan eliminarlos al máximo, y en caso de que ocurran, poder reparar el daño y reanudar la operación lo más rápidamente posible.

En una situación ideal se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación, se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro. Las acciones de recuperación disponibles a nivel operativo pueden ser:

- En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.
 - Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.
 - El procesamiento anterior complementado con un registro de las transacciones que afectaron los archivos permitirá retroceder en los movimientos realizados a un archivo al punto de tener la seguridad del contenido del mismo y a partir de éste reanudar el proceso.

- Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alternativo de emergencia.
- Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones:
 - Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.

Este grupo de emergencia deberá tener un conocimiento de los procedimientos que puede utilizar, además de un conocimiento de las características de las aplicaciones, tanto desde el punto técnico como de su prioridad, nivel de servicio planeado e influjo en la operación de la organización.

Además de los procedimientos de recuperación y reinicio de la información, se deben considerar los procedimientos operativos de los recursos físicos, como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falla de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares. Éstas y otras medidas de recuperación y reinicio deben de ser planeadas y probadas previamente, como en el caso de la información.

Con frecuencia un problema en algún programa, un error en los datos, un error de operación o una falla del equipo hacen que una corrida en la máquina aborte antes de terminar el proceso.

Cuando esto sucede, generalmente no se puede iniciar el trabajo donde se produjo la interrupción.

El objetivo del siguiente cuestionario es evaluar los procedimientos de restauración y repetición de procesos en el sistema de cómputo:

1. ¿Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo? SÍ NO
2. Enuncie los procedimientos mencionados en el inciso anterior.

3. ¿Cuentan los operadores con alguna documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones? SÍ NO
4. En el momento en que se hacen cambios o correcciones a los programas y/o archivos se deben tener las siguientes precauciones:
 - Las correcciones de programas deben ser debidamente autorizadas y probadas. Con esto se busca evitar que se cambien por una nueva versión que antes no ha sido perfectamente probada y actualizada.
 - Los nuevos sistemas deben estar adecuadamente documentados y probados.
 - Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.
 - Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.
 - Los datos de entrada deben estar debidamente probados y verificados contra la entrada de datos durante el procesamiento.

PLAN DE CONTINGENCIA Y PROCEDIMIENTOS DE RESPALDO PARA CASOS DE DESASTRE

PLAN DE
CONTINGENCIA
Y PROCEDIMIENTOS
DE RESPALDO
PARA CASOS
DE DESASTRE

Los accidentes pueden surgir por un mal manejo de la administración, por negligencia o por ataques deliberados hechos por ladrones, por fraudes, sabotajes o bien por situaciones propias de la organización (huelgas). El trabajar con posibilidad de que ocurra un desastre es algo común, aunque se debe evitar en lo posible y planear de antemano las medidas en caso de que esto ocurra.

La organización debe tener todos los controles, las funciones y los dispositivos para evitar un desastre, pero en caso de que ocurra, debe contar con un plan de contingencia que permita restaurar el equipo en el menor tiempo posible y con las mínimas consecuencias.

En cada dirección de informática se debe establecer y aprobar un plan de emergencia, el cual debe contener tanto el procedimiento como la información necesarios para reanudar la operación del sistema de cómputo en caso de desastre.

Algunas compañías se resisten a tener un plan para casos de desastre o emergencia, pues consideran que es imposible que ocurra un accidente. En los sistemas en línea o en tiempo real, el plan difícilmente puede ser usado en otro equipo, por lo que la única alternativa es tener una alta seguridad en los equipos o bien computadoras en forma de tándem, sin embargo, es necesario que el plan de contingencia con el que se cuenta, permita restaurar el servicio en el menor tiempo posible, con la mejor afectación a la organización.

El sistema debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia se tenga la seguridad de que funcionará.

Según una de las ocho grandes firmas estadounidenses de contadores públicos, los planes de seguridad deben garantizar la integridad y exactitud de los datos; permitir identificar la información confidencial, de uso exclusivo o delicada en alguna otra forma; proteger los activos de desastres provocados por la mano del hombre y por actos abiertamente hostiles y conservarlos, asegurar la capacidad de la organización para sobrevivir a accidentes; proteger a los empleados contra tentaciones o sospechas innecesarias y la administración contra cargos por imprudencia.

La prueba del plan de contingencia o emergencia debe hacerse sobre la base de que un desastre es posible y que se han de utilizar respaldos (posiblemente en otras instituciones). Habrá que cambiar la configuración y posiblemente se tengan que usar algunos métodos manuales, no sólo simulando un ambiente ficticio cercano a la realidad sino considerando que la emergencia puede existir.

Se deben evitar suposiciones que, en un momento de emergencia, vuelvan inoperante el respaldo. En efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo, discos, etcétera.

Las revisiones al plan se deben realizar cuando se haya efectuado algún cambio en la configuración del equipo o bien cada seis meses. Una de las principales objeciones al plan de emergencia es su costo; pero, como en el caso de un seguro contra incendio, sólo podemos evaluar sus ventajas si desafortunadamente el desastre ocurre.

El plan de emergencia, una vez aprobado, se debe distribuir entre personal responsable de su operación. Por precaución, es conveniente tener una copia fuera de la dirección de informática.

Las organizaciones pueden ser afectadas en menor o mayor grado ante los diferentes tipos de desastres en informática y las repercusiones variarán según la dependencia que tenga la organización respecto a la tecnología.

Las organizaciones deben de identificar su procesos críticos, el tiempo y los recursos para restablecer el servicio ante una contingencia, por lo que el proyecto del plan debe tener una alta prioridad.

El plan de contingencias anteriormente sólo tomaba en cuenta los procesos basados en la computadora. Sin embargo, se debe considerar todo aquello que asegure la continuidad de la organización, incluyendo registros manuales y documentación fuente.

En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia. La estructura debe considerar facilitar su actualización.

PLAN DE CONTINGENCIAS

El plan de contingencias y el plan de seguridad tienen como finalidad proveer a la organización de requerimientos para su recuperación ante desastres.

Los desastres pueden clasificarse de la siguiente manera:

Tipos de desastres

- Destrucción completa del centro de cómputo.
- Destrucción parcial del centro de cómputo.
- Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire acondicionado, etcétera).
- Destrucción parcial o total de los equipos descentralizados.
- Pérdida total o parcial de información, manuales o documentación.
- Pérdida de personal clave.
- Huelga o problemas laborales.

La metodología tiene como finalidad conducir de la manera más efectiva un plan de recuperación ante una contingencia sufrida por la organización.

El plan de contingencia es definido como: la identificación y protección de los procesos críticos de la organización y los recursos requeridos para mantener un aceptable nivel de transacciones y de ejecución, protegiendo estos recursos y

preparando procedimientos para asegurar la sobrevivencia de la organización en caso de desastre.

En la elaboración del plan de contingencias deben intervenir los niveles ejecutivos de la organización y el personal usuario y técnico de los procesos.

Para la preparación del plan se seleccionará el personal que realice las actividades clave de éste. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática (por ejemplo, los jefes de operación, de análisis y programación, y de auditoría interna). Cada uno de ellos debe tener tareas específicas, como la operación del equipo de respaldo, la interfase administrativa y la de logística, por ejemplo, el proporcionar los archivos necesarios para el funcionamiento adecuado. Cada miembro del grupo debe tener asignada una tarea y contar con una persona de respaldo. Se deberá elaborar un directorio de emergencia con teléfonos particulares que contenga además los nombres y direcciones. Éste deberá estar almacenado en un lugar seguro y accesible.

Entre los objetivos del plan de contingencia se encuentran:

- Minimizar el impacto del desastre en la organización.
- Establecer tareas para evaluar los procesos indispensables de la organización.
- Evaluar los procesos de la organización, con el apoyo y autorización respectivos a través de una buena metodología.
- Determinar el costo del plan de recuperación, incluyendo la capacitación y la organización para restablecer los procesos críticos de la organización cuando ocurra una interrupción de las operaciones.

La metodología del plan de contingencias determina los procesos críticos de la organización para restablecer sus operaciones y debe tomar en cuenta ser eficaz y eficiente, los aspectos legales, el impacto de servicio al cliente y los riesgos para que sobreviva la organización.

El plan de contingencias debe contemplar lo siguiente:

- La naturaleza, la extensión y la complejidad de las actividades de la organización.
- El grado de riesgo al que la organización está expuesto.
- El tamaño de las instalaciones de la organización (centros de cómputo y número de usuarios).
- La evaluación de los procesos considerados como críticos.
- El número de procesos críticos.
- La formulación de las medidas de seguridad necesarias dependiendo del nivel de seguridad requerido.
- La justificación del costo de implantar las medidas de seguridad.

Entre las etapas del proyecto del plan de contingencias están:

- Análisis del impacto en la organización.
- Selección de la estrategia.
- Preparación del plan.
- Prueba.
- Mantenimiento.

Objetivos del plan de contingencia

Metodología del plan de contingencia

Etapas del plan de contingencias

**Impacto en la
organización**

El proyecto comienza con el análisis del impacto en la organización. Durante éste se identifican sus procesos críticos o esenciales y sus repercusiones en caso de no estar en funcionamiento:

- Clasificar la instalación en términos de riesgo (alto, mediano, pequeño) e identificar las aplicaciones que tengan un alto riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.

Algunas instalaciones y sus aplicaciones tienen un alto grado de riesgos, por lo que, si es que el servicio se interrumpe cierto periodo, la organización o la comunidad sufrirá un gran impacto; otras pueden fácilmente continuar sus operaciones sin afectar grandemente a la organización por medio de la utilización de métodos manuales.

Se debe evaluar el nivel de riesgo de la información para hacer un adecuado estudio costo/beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad.

Para clasificar el riesgo e identificar las aplicaciones de alto riesgo debemos preguntarnos qué sucedería si no se puede usar el sistema. Si la respuesta es que no se podría seguir trabajando, entonces estamos situados en un sistema de alto riesgo.

Ejemplo

El sistema de reservaciones de boletos de avión. Éste es un sistema de alto riesgo. De menor riesgo podría ser la nómina y por último el de la contabilidad (en periodos normales, no en periodos de entrega de información contable).

La siguiente pregunta es: ¿qué implicaciones tiene el que no se recupere el sistema y cuánto tiempo podríamos estar sin utilizarlos?

En el caso de reservaciones en línea y en tiempo real, no se puede trabajar si no se cuenta con el sistema, y no podemos estar sin él más que unos minutos. En el caso de la nómina depende de cuándo se debe entregar (semanal, quincenal, mensual), lo mismo que la contabilidad.

¿Existe un procedimiento alternativo y qué problemas nos ocasionaría? En las reservaciones, el procedimiento alternativo de utilizar otro sistema ajeno a la compañía no es posible debido a las redes y a los bancos de datos. El procedimiento alternativo consistiría en que sólo se reciban reservaciones en una oficina o bien que se estén comunicando por teléfono para que una oficina concentre las reservaciones. Sin embargo, esto provocaría una gran ineficiencia y un pésimo servicio. Al terminar la emergencia se deben dar de alta en el sistema las reservaciones captadas manualmente.

En el caso de la nómina se puede hacer de forma manual (lo cual puede resultar muy complicado) o bien pagar lo mismo que la nómina anterior (lo que provocaría reclamos por parte del personal al que se le pague menos) y después de la emergencia procesar la nómina nueva y sacar un programa que permita pagar la diferencia de más o de menos y ajustar los impuestos. En caso de contar con respaldos se puede tener como procedimiento alternativo procesarlo en otro sistema.

La contabilidad puede hacerse en forma manual o bien, en caso de tener respaldo, procesarse en otro sistema.

**Procedimientos
alternos**

¿Qué se ha hecho en un caso de emergencia? En el caso de sistemas como el de reservaciones, de bancos o casas de bolsa, el único procedimiento para evitar problemas es tener sistemas simultáneos (tándem o en paralelo) que permitan pasar de un equipo a otro en forma instantánea, disponer de sistemas duplicados en áreas críticas (aires acondicionados, discos, etc.) y contar con sistemas de energía no interrumpible (*no-break*), ya que debido a su alto riesgo son los que deben tener mayor seguridad.

Para evaluar la instalación en términos de riesgo se debe:

- Clasificar los datos, la información y los programas que contengan información confidencial de alto valor dentro del mercado de competencia de una organización, así como la información que sea de difícil recuperación.
- Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien que pueda provocar un gran impacto en la toma de decisiones.
- Determinar la información que pueda representar una gran pérdida en la organización y, consecuentemente, provocar incluso la posibilidad de que no se pueda sobrevivir sin esa información.

Un ejemplo de alto riesgo puede ser la información confidencial de tipo nacional o bien la información sobre el mercado y la publicidad de una compañía.

Para cuantificar el riesgo es necesario efectuar entrevistas con los altos niveles administrativos directamente afectados por la suspensión en el procesamiento para que cuantifiquen el impacto que les puede causar este tipo de situaciones.

Existe una importante etapa para identificar cada proceso de la organización, para determinar los procesos que son críticos en su continuidad y para definir los procesos que deberán estar incluidos en el plan de contingencias. Se trata de un paso vital en la implementación del plan de contingencias.

Existen diferentes métodos para determinar los procesos críticos de una organización:

- Todos los procesos críticos. Con este método, la decisión es tomada por todos los departamentos y se parte de que todas las funciones de cada departamento son críticas. Por lo general, se eliminan uno o dos departamentos, pero casi todo es clasificado como crítico.

Si se elige este método, se deben enlistar todas las funciones de cada departamento. Este método no es recomendable porque elaborar el plan de contingencias requerirá de mucho tiempo. Sería costoso y llevaría tiempo respaldar todas las funciones en todos los departamentos.

- Mandatos de los gerentes. Este método asume que los gerentes conocen los elementos críticos para mantener un aceptable nivel en la organización. La identificación de funciones críticas es hecha en base a la intuición de los gerentes. El beneficio de este método es el tiempo que se ahorra durante la fase inicial. Lo peligroso es que está basado en una intuición y éste no es un análisis riguroso.

**Métodos para
determinar los
procesos críticos**

**Objetivos de la
técnica de análisis
del impacto**

- **Análisis de riesgos financieros.** Consiste en la determinación de pérdidas financieras por cada función y proceso de la organización. Esto se obtiene por la determinación de la probabilidad de un desastre y la pérdida anual. Es comparado con el nivel de pérdida financiera aceptable para la organización. Son críticos aquellos procesos de los que se esperan grandes pérdidas. Sin embargo, no se puede determinar exactamente el riesgo.
- **Análisis del impacto en la organización.** La metodología del plan de contingencias se basa en la técnica de análisis de impacto en la organización. Para ello se distribuyen cuestionarios para todos los departamentos de la organización. Los cuestionarios completos y la información obtenida durante las entrevistas definen los criterios para determinar los procesos críticos. Este método tal vez tome más tiempo inicialmente que el de "todos los procesos son críticos". Sin embargo, disminuye considerablemente el tiempo y el dinero cuando se desarrolla el plan de recuperación.

Los cuestionarios y entrevistas persiguen los siguientes objetivos:

- Identificar los procesos críticos y necesarios de la organización, así como las dependencias críticas de los sistemas.
- Identificar los procesos críticos en cuanto a la imagen y operacionalidad de la organización, así como sus repercusiones en caso de suspenderse su utilización.
- Determinar los procesos con probabilidad de ser destruidos, tomando en cuenta periodos de pérdida específicos (tres horas, un día o una semana).
- Definir recursos alternativos de información y servicio.
- Determinar el costo financiero de un desastre y el probable tiempo de recuperación.
- Identificar amenazas específicas de cada proceso crítico (instalación de luz, localización geográfica, etcétera).
- Especificar los sistemas que ponen en riesgo la continuidad de las operaciones de la organización.

Después de que la información esté reunida gracias a las entrevistas y los cuestionarios, se analizará para determinar cada proceso crítico. La clasificación de los procesos será el resultado del análisis, discutido con la gerencia o dirección, para asegurar que todos los procesos son apropiados, se incluyan en el plan de contingencias. Los procesos que son identificados como críticos en esta fase, deberán ser considerados en el plan de contingencias.

**Información
preliminar**

El objetivo de la información preliminar es crear una muestra de cuestionarios y conducir las entrevistas preliminares con el fin de identificar procesos críticos para la continuidad de las operaciones fundamentales de la organización.

Esta tarea comienza con el diseño, la creación y la prueba de los cuestionarios:

- Los cuestionarios en el análisis del impacto de la organización son usados para dirigir las entrevistas.
- Los cuestionarios deberán servir para analizar a detalle las funciones críticas de la organización.

Un
ción, es
mente e
de decis
El p

- Las
- Los
- Los
- Dep
- Dep
- Pér
- seg
- Cos
- Res
- Des
- Nú
- Mé
- Pro
- Pri

Las
asistir e
cluyen
ternativ
Co
cados e
mencio
proces
tadora
ticas.

De
una rev
Estas e

- An
- tra
- Á
- Inf
- Seg
- org
- Al
- la
- Co
- du
- cia
- Al

**Propósitos
de las entrevistas**

Un beneficio adicional al de analizar los procesos críticos de la organización, es conocer la documentación e integración de la información que usualmente está en propiedad de diversos individuos, lo que ayuda a la mejor toma de decisiones.

El propósito de las entrevistas preliminares es para identificar lo siguiente:

- Las áreas vitales de la organización para que la corporación sobreviva.
- Los componentes críticos entre cada área de la organización.
- Los sistemas esenciales para cada área de la organización.
- Dependencia y facilidades de soporte.
- Dependencia e impacto en otras áreas de la organización.
- Pérdidas financieras directas y costos de recuperación involucrados en el seguimiento de las pérdidas.
- Costos de un probable desastre como repercusión en las ventas.
- Responsabilidad de los entrevistados.
- Descripción del trabajo realizado y procesos involucrados.
- Número de personas y habilidad requerida para realizar el proceso.
- Métodos alternativos de posibles procedimientos.
- Procedimientos sugeridos de recuperación.
- Prioridades de recuperación.

Las guías de análisis de las áreas de la organización deben ser usadas para asistir en la generación de discusiones en diferentes procesos críticos. Éstos incluyen componentes esenciales sugeridos, dependencias críticas, recursos alternativos y probabilidad del impacto de destrucción para diferentes áreas.

Como la mayoría de los planes de contingencias en el pasado estaban enfocados en las operaciones basadas en los sistemas automáticos, es necesario mencionar en las entrevistas que el plan de contingencias debe cubrir todos los procesos de la organización. Algunos de los que no están basados en la computadora deben ser discutidos y debe llenarse el cuestionario de las funciones críticas.

Deben realizarse entrevistas con los jefes de departamento para obtener una revisión inicial de la organización y confirmar la naturaleza y sus procesos. Estas entrevistas deben incluir lo siguiente:

- Antecedentes de la organización, como su naturaleza, líneas de productos, transacciones anuales (compras y ventas), mercado y competidores.
- Áreas de la organización y jefes de departamento.
- Información estratégica y decisiones de operación.
- Seguridad en el centro de cómputo y en las áreas más importantes de la organización.
- Algunos riesgos específicos que pongan en peligro los procesos críticos de la organización.
- Conocimiento de los requerimientos legales (multas, estándares de la industria, requerimientos de auditoría en relación con el plan de contingencias).
- Algún plan de contingencias emprendido.

**Elementos
de las entrevistas**

**Recolección
de datos**

Los directivos deben conocer la información general para el mantenimiento de la organización, pero tal vez no tengan el conocimiento específico de la información.

La información requerida para el proyecto del plan de contingencias puede existir en varias formas en la organización.

Se deberá obtener la documentación existente que contenga antecedentes de la organización. Éstos deben incluir:

- Organigramas.
- Descripción de procesos operativos.
- Medidas de seguridad existentes contra desastre.
- Seguros.
- Procedimientos de desastres existentes.

Además de las entrevistas generales, se requiere información más detallada sobre los sistemas automáticos. Durante las entrevistas con el jefe de informática y con especialistas se deberán revisar los sistemas y sus componentes esenciales, como son:

**Componentes
de los sistemas
automáticos**

- Términos de información, estrategias tecnológicas y propósitos de desarrollo de sistemas.
- Personas de informática y detalles de escritorio.
- Instalaciones de informática y funciones específicas.
- Hardware requerido, modelo y configuración.
- Comunicaciones, redes, LAN, WAN (incluyendo microcomputadoras).
- Periféricos, como terminales, impresoras y capacidad de disco.
- Facilidades esenciales de soporte.
- Tiempos de proceso.
- Procesos en línea y *batch*.
- Lista de las aplicaciones mayores.
- Plan de contingencias existente.
- Localización y frecuencia de respaldos de programas y datos.
- Historia de fallas en el sistema.

Los cuestionarios deben distribuirse en todos los niveles de la organización, principalmente entre los empleados que usan y manejan sistemas diariamente, para asegurar que toda la información relevante sea revisada.

Los cuestionarios de las funciones críticas deben ser distribuidos al mismo tiempo que los cuestionarios del impacto en la organización y junto con información concerniente a los propósitos de las entrevistas, procedimientos, duraciones y tiempos.

Cuestionarios para análisis del impacto en la organización

Las entrevistas y cuestionarios sobre el análisis del impacto de la organización deberán basarse en las discusiones con los jefes de departamento.

Estos cuestionarios sobre el análisis del impacto de la organización deberán basarse en las discusiones con los jefes de departamento.

Estos cuestionarios no deben plantear preguntas específicas, sino de las áreas en general. Las entrevistas deberán ser consistentes.

También tendrán que ser incluidas otras áreas no automatizadas que pueden tener información crítica y recursos físicos (maquinaria) para la continuidad del funcionamiento de la organización.

A continuación ofrecemos un ejemplo de cuestionario para guiar la entrevista sobre el análisis del impacto en la organización:

CUESTIONARIO SOBRE EL IMPACTO

1. ¿Cuáles áreas del negocio son de mayor responsabilidad?

De éstas, identifique los componentes que en su opinión son:

- Lo esencial para que la organización sobreviva.
- Lo esencial para mantener las funciones más importantes de la organización.
- Funciones no críticas para la organización y que pueden ser suspendidas temporalmente en un evento de emergencia.

2. ¿Cuáles son las consecuencias financieras de la pérdida de un componente clave de la organización?

- ¿Cuáles son las consecuencias del deterioro de la imagen ante la pérdida de un componente clave de la organización?
(Ejemplo: problemas laborales).
- Provea la información básica de cada componente de tu responsabilidad. Esto puede ser en forma de diagrama de flujo, el cual deberá identificar entradas y salidas en las áreas de la organización. Debe incluir funciones sistematizadas, funciones manuales y sus interdependencias.

3. ¿Con qué información y facilidades cuenta en cada área de la organización?

Se deben identificar todos los recursos internos y externos de datos, aplicaciones por computadora y las facilidades con las que se cuenta, incluyendo personal clave y comunicaciones.

Los cuestionarios de funciones críticas son diseñados para recolectar información que refleje la importancia de cada proceso en la organización, y poder evaluar qué tan crítica puede ser una función, o si es posible que ésta se detenga durante un periodo determinado. Deberá ser aplicado un cuestionario para cada proceso.

Para determinar lo que es "crítico", se debe usar la medida de "tolerancia", que es definida como la capacidad de continuar con los procesos durante una interrupción de las actividades normales de la organización. Si la tolerancia de un proceso particular es pequeña, el proceso es probablemente crítico. La tolerancia puede y debe ser cuantificada en términos monetarios, de impacto a la organización y de impacto a la imagen de la organización.

Los usuarios deben conocer el valor de los sistemas críticos, porque ellos son los responsables. La experiencia muestra que son normalmente imparciales para evaluar lo crítico de sus sistemas.

Las preguntas deben ser directas para determinar procesos críticos y se deben buscar métodos alternativos.

CUESTIONARIO DE FUNCIONES CRÍTICAS

Departamento _____
 División _____
 Teléfono _____
 Oficina _____
 Nombre de la función _____
 Descripción de la función _____

COMENTARIO

¿Con qué frecuencia es realizada la función?

Anual Semestral Mensual Semanal Diario

Otra explicación: _____

1. ¿Cuál sería el costo para la organización si esta función no fuera realizada:

Por día? \$ _____
 Por semana? \$ _____
 Por mes? \$ _____

2. Estimar cuál sería el costo adicional (multas, pérdidas de arrendamiento, contratos cancelados) en qué organización puede incurrir si esta función no es realizada:

Por día \$ _____
 Por semana \$ _____
 Por mes \$ _____

3. ¿La vida humana es puesta en riesgo si esta función no se realiza?

SÍ NO
4. ¿La organización tendrá conflictos si esta función no es realizada?

SÍ NO
5. ¿Esto impactaría a la operación eficiente dentro de la organización?

SÍ NO
6. ¿El servicio a los clientes es afectado por la no realización de esta función?

SÍ NO
7. ¿Los requerimientos legales pueden no ser cumplidos sin esta función?

SÍ NO

CUESTIONARIO DE OPERACIÓN

1. Impacto de una hora de interrupción en el centro de cómputo:

- La mayor interrupción operacional en el servicio al cliente es tener grupos de personal totalmente parado. ()
- Inconveniente, pero el centro de las actividades del negocio continúa intacto. ()
- Esencialmente insignificante. ()

2. Impacto de una interrupción total en el centro de cómputo, durante dos o tres semanas:

- Casi fatal, no hay fuentes de respaldo. ()
- Facilidades de respaldo externas, menores ingresos y mayores costos. ()
- Caro. Algunos procesos pueden ser preservados. ()

3. Aptitud del personal observado en caso de emergencia:

- En el centro de cómputo la fuerza de trabajo es organizada. ()
- Son inexpertos (medios organizados). ()
- Son desorganizados. ()

4. Número de operaciones críticas en sistemas en línea o en sistema en batch:

- 10 o más. ()
- 6-9. ()
- 3-5. ()
- 0-2. ()

5. Localización de los sistemas:

- En un área específica. ()
- En dos o tres áreas. ()
- Corre por múltiples departamentos. ()

6. De fácil recuperación después de la interrupción:

- 3 o 4 días en sistemas críticos. ()
- 12 o 24 horas en sistemas críticos. ()
- Sin problemas (recuperación inmediata). ()

7. Control de recuperación después de la interrupción:

- Mucho tiempo consumido y costoso por los sistemas interrelacionados. ()
- Alguna interrupción. ()
- Relativamente rápido, daño controlado. ()
- Parcialidad de copias manuales. ()
- Imposible. ()
- Algo posible. ()
- Relativamente fácil. ()

SELECCIÓN DE LA ESTRATEGIA

Una vez que hemos definido el grado de riesgo, hay que elaborar una lista de los sistemas con las medidas preventivas que se deben tomar, así como las correctivas en caso de desastre, señalándole a cada función su prioridad.

El siguiente paso es identificar y comentar procesos alternativos para procesos identificados como críticos en la organización. Si existen otros procedimientos con recursos similares aprovechables, éstos podrán ser considerados como posibles procedimientos alternos.

En caso de desastre se procurará trabajar los sistemas de acuerdo con sus prioridades, ya que no se podrá hacer en otra instalación en la misma forma como se venían trabajando en la instalación original.

Cada uno de los riesgos y su probabilidad de ocurrencia deben ser identificados.

Las medidas de prevención de desastre deben estar respaldadas en un lugar seguro. Se debe considerar y evaluar rangos de estrategias de recuperación posibles, para que al final de esta etapa de selección una sea elegida.

El plan de recuperación de la organización es proyectado y probado. Su preparación requiere de la participación del personal de la organización para asegurar que éstos sean miembros del plan y que estén disponibles cuando éste se lleve a la práctica.

Es importante contar con la documentación completa del plan de contingencia para ser usada en caso de desastre. Ésta debe ser evaluada y aprobada y periódicamente revisada para actualizarla. Toda la documentación asociada con el plan de contingencias y el control de procedimientos juega un importante papel dentro de la organización.

Después de que el plan de contingencias sea desarrollado, los documentos deberán archivar en un lugar que esté protegido de desastre, deterioro o pér-

dida, pero accesible en caso de contingencias. A cada director se le dará una copia, la cual deberá incluir la versión, la fecha y el lugar donde estará el documento.

Los datos que contendrá para su identificación son:

- Título del documento.
- Identificación o número de referencia.
- Número de la versión y fecha.
- Autor.
- Número de versión. La vida del documento tendrá varios cambios. Los lineamientos a seguir para controlar las versiones son:
 - Historia.
 - Número de páginas.
 - Aprobación del documento.
 - Control de cambios.
 - Distribución del documento.

Los departamentos deben tener implantada su propia estrategia de respaldo. Se debe asegurar que el personal asignado a la tarea de recolección de datos esté correctamente instruido.

El personal de procesamiento de datos frecuentemente no está enterado de la importancia funcional de los sistemas que soporta. Es más apropiado en las aplicaciones críticas automatizadas consultar a los usuarios o a los jefes de departamento. De cualquier manera, el departamento de procesamiento de datos conoce el procesamiento a detalle de estas aplicaciones.

Al finalizar el plan de contingencia, éste debe contener:

- El señalamiento de los procesos críticos.
- Su impacto.
- Prioridad.
- Tiempo en que puede estar fuera de servicio.
- Información existente de cada proceso (procedimientos y políticas).
- Documentación para la recuperación.
- Por cada proceso, se requiere del usuario de:
 - Software.
 - Hardware.
 - Recursos materiales.
 - Personal.
 - Consumibles.
 - Utillerías.
 - Sistemas de comunicación.
 - Redes.
 - Transporte.
 - Bases de datos.
 - Archivos (respaldos).

Elementos de la documentación

Elementos del plan de contingencias

Para evaluar las medidas de seguridad, se debe especificar:

- La aplicación, los programas y archivos.
- Las medidas en caso de desastre, pérdida total, abuso y los planes necesarios.
- Las prioridades que se deben tomar en cuanto a las acciones a corto y largo plazos.

El plan en caso de desastre debe incluir:

- La documentación de programación y de operación.
- Los equipos.
- El equipo completo.
- El ambiente de los equipos.
- Datos, archivos, papelería, equipo y accesorios.
- Sistemas (sistemas operativos, bases de datos, programas de utilería, programas).

Al final de esta etapa, el plan de recuperación entra en una fase de prueba, para asegurar que se trabaja en forma eficiente.

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se actualizan las últimas modificaciones, lo que provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá:

- Asegurar que todos los miembros sean notificados.
- Informar al director de informática.
- Cuantificar el daño o pérdida del equipo, archivos y documentos para definir qué parte del plan debe ser activada.
- Determinar el estado de todos los sistemas en proceso.
- Notificar a los proveedores del equipo cuál fue el daño.
- Establecer la estrategia para llevar a cabo las operaciones de emergencia tomando en cuenta:
 - Elaboración de una lista con los métodos disponibles para realizar la recuperación.
 - Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustitución de procesos en línea por procesos en lote).
 - Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieran.
 - Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deberá reducir la carga de procesos, analizando alternativas como:

Pruebas del plan de recuperación

- Posponer las aplicaciones de prioridad más baja.
- Cambiar la frecuencia del proceso de trabajos.
- Suspender las aplicaciones en desarrollo.

Por otro lado, se debe establecer una coordinación estrecha con el personal de seguridad a fin de proteger la información.

Hay que tener mucho cuidado con la información que sale de la oficina, y la forma en que es utilizada así como prever que sea borrada al momento de dejar la instalación que está dándole respaldo.

Respecto a la configuración del equipo, hay que tener toda la información correspondiente al hardware y software del equipo propio y del respaldo.

Deberán tenerse todas las especificaciones de los servicios auxiliares, tales como energía eléctrica, aire acondicionado, etc. A fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de proceso, se deberán tomar en cuenta las siguientes consideraciones:

- Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.
- Se debe tener documentados los cambios de software.
- En caso de respaldo en otras instituciones, previamente se deberá conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

- Configuración de equipos.
- Configuración de equipo de captación de datos.
- Sistemas operativos.
- Configuración de equipos periféricos.

Finalmente, se deberá tener una lista de los requerimientos mínimos para un efectivo plan de recuperación en caso de desastre.

Lo más importante es identificar el número y tipo de componentes esenciales que puedan ser críticos en caso de emergencia o de desastre, para lo cual ofrecemos el siguiente cuestionario:

A) Equipo principal (equipo, canales de comunicación, memoria, etcétera).

Equipo fabricante	Proyecto en el equipo	¿Es esencial para procesar?
----------------------	--------------------------	--------------------------------

B) Unidades de disco (incluyendo controladores, número de unidades, paquetes de discos, número de discos por paquete).

Fabricante	Número de unidades	Capacidad	Proyectos	¿Es esencial para procesar?
------------	-----------------------	-----------	-----------	--------------------------------

C) Unidades de cinta.

D) Unidades de almacenamiento (en línea o fuera de línea).

E) Equipo periférico (lectoras, impresoras, etcétera).

F) Unidades de comunicación, controladores.

Número de equipos	Proyecto en equipo	¿Es esencial para procesar?
----------------------	-----------------------	--------------------------------

G) Sistemas operativos.

H) Terminales.

I) Equipo adicional.

- Electricidad KVA.
- Aire acondicionado BTU.
- Temperatura requerida.
- Humedad requerida.

RED DE COMUNICACIÓN

1. Descripción de la red de comunicación.

2. En caso de emergencia, ¿es esencial el uso de la red de comunicación?
Describe el porqué de su respuesta. SÍ NO

3. Programas necesarios para la comunicación.

4. Se debe contar con:

- Copia de programas de producción. ()
- Copia de archivos maestros de las aplicaciones clave y sistemas operativos. ()
- Copia de la documentación de los sistemas e instructivos de operación. ()
- Copia de los archivos necesarios para procesar las transacciones. ()
- Inventario de formas especiales utilizadas en la operación normal (se deben incluir también papelería normal, cintas magnéticas). ()
- Un local con las instalaciones necesarias (energía, aire acondicionado, piso adecuado, etcétera). ()
- Convenios para el uso de computadoras compatibles. ()

Es importante que en la prueba del plan exista disciplina en la ejecución. La disciplina es importante no sólo para facilitar la recuperación, sino para detectar problemas (en el momento del desastre), con el fin de minimizar la pérdida de vidas y costos.

Deberá existir un coordinador de la recuperación, quien debe ser el encargado de las pruebas.

El plan de contingencias debe ser elaborado asegurándose de que sea mantenido y revisado regularmente para que refleje los cambios en la organización o modificado adaptando los procedimientos.

Después de la creación inicial, el plan debe ser formalmente revisado, por varios meses se debe asegurar que los procedimientos de recuperación hayan sido mantenidos y probados apropiadamente.

**Mantenimiento
del plan de
contingencias**

OBJETIVOS

El plan de contingencias debe ser elaborado asegurándose de que sea mantenido y revisado regularmente para que refleje los cambios en la organización o modificado adaptando los procedimientos.

Después de la creación inicial, el plan debe ser formalmente revisado, por varios meses se debe asegurar que los procedimientos de recuperación hayan sido mantenidos y probados apropiadamente.

7

CAPÍTULO

Interpretación de la información

OBJETIVOS

Al finalizar este capítulo, usted:

1. Conocerá las técnicas para la interpretación de la información del sistema.
2. Comprenderá cómo se evalúa el grado de madurez del sistema.
3. Definirá los diferentes tipos de evaluación de los sistemas de información.
4. Describirá la importancia de los controles en la auditoría.
5. Conocerá cómo realizar la presentación de las conclusiones de la auditoría.

TÉCNICAS PARA LA INTERPRETACIÓN DE LA INFORMACIÓN

Para interpretar la información se puede utilizar desde técnicas muy sencillas hasta técnicas complejas de auditoría.

ANÁLISIS CRÍTICO DE LOS HECHOS

Una de las primeras técnicas es el análisis crítico de los hechos. Esta técnica sirve para discriminar y evaluar la información; es una herramienta muy valiosa para la evaluación y se basa en la aplicación de las siguientes preguntas.

Pregunta	Finalidad que determina
Qué	El propósito
Dónde	El lugar
Cuándo	El orden y el momento, sucesión
Quién	La persona
Cómo	Los medios
Cuánto	La cantidad

La pregunta más importante es qué, pues la respuesta permitirá saber si puede ser:

- Eliminada.
- Modificada o cambiada.
- Simplificada.

Las respuestas que se obtengan deben ser sometidas a una nueva pregunta: "Por qué", la cual planteará un nuevo examen que habrá de justificar la información obtenida. Cada interrogante se debe descomponer de la siguiente manera:

1. Propósito:
 - Qué se hace.
 - Por qué se hace.
 - Qué otra cosa podría hacerse.
 - Qué debería hacerse.
2. Lugar:
 - Dónde se hace.
 - Por qué se hace ahí.

- En qué otro lugar podría hacerse.
- Dónde debería hacerse.

3. Sucesión:

- Cuándo se hace.
- Por qué se hace entonces.
- Cuándo podría hacerse.
- Cuándo debería hacerse.

4. Persona:

- Quién lo hace.
- Por qué lo hace esa persona.
- Qué otra persona podría hacerlo.
- Quién debería hacerlo.

5. Medios:

- Cómo se hace.
- Por qué se hace de ese modo.
- De qué otro modo podría hacerse.
- Cómo debería hacerse.

6. Cantidad:

- Cuánto se hace.
- Por qué se hace esa cantidad (volumen).
- Cuánto podría hacerse.
- Cuánto debería hacerse.

METODOLOGÍA PARA OBTENER EL GRADO DE MADUREZ DEL SISTEMA

Para poder interpretar la información de los sistemas se debe evaluar el grado de madurez de los mismos:

- Verificar si el sistema está definido.
- Verificar si el sistema está estructurado.
- Verificar si el sistema es relativamente estable.
- Verificar si los resultados son utilizados o no.

Características	Maduro	Inmaduro
Definido	Completamente	Incompleto
Estructurado	Alta	Baja
Estable	No cambia	Muchos cambios
Resultados	Utilizados	No utilizado

Dependiendo del grado de madurez y de su grado de estructuración, se determina si debe estar automatizado y la posible madurez que repercutirá en una mejor utilización y en disminución de cambios.

Si el sistema está estructurado y maduro se debió usar la técnica de sistema de información; si está estructurado pero no está maduro se debió seguir haciendo manualmente; si está semiestructurado y maduro se podrá usar la técnica de soporte en la toma de las decisiones (DSS = *Decision System Support*).

Si el sistema está semiestructurado pero no está maduro debió seguirse haciendo en forma manual; si no está estructurado y maduro, es un sistema guiado por la intuición y deberá seguirse haciendo en forma manual. Si no está estructurado ni maduro el sistema no tiene razón de existir.

Nivel madurez	Maduro	Inmaduro
Nivel estructura	Estructurado	Sistema de información general
	Sistema de soporte	Manual de decisiones
Semiestructurado	Intuitivo	Sin razón
No estructurado		

Uso de diagramas

Otra forma de analizar los hechos es seguir la ruta de la información desde su origen hasta su destino, y disponer de este camino en una secuencia cronológica, con el fin de clarificar dónde aparece, cómo avanza a lo largo del sistema y cómo llega a su destino. Esta técnica ayuda a hacer un estudio objetivo de todos los pasos por los cuales deberá pasar la información.

Se considera necesario agregar algunas características que definan aún más este estudio como frecuencia, tiempo, costo y distancia física de cada paso coadyuvando a una evaluación más objetiva del sistema.

EVALUACIÓN DE LOS SISTEMAS

Se debe evaluar el desarrollo que ha tenido el sistema mediante el análisis de los pasos que comprendió el desarrollo del sistema, y comparar lo que se planeó contra lo que realmente se está obteniendo.

ANÁLISIS

Se debe evaluar la información obtenida en los sistemas para poder:

- Determinar el objeto y compararlo con lo obtenido.
- Buscar la interrelación con otros sistemas.

- Evaluar la secuencia y flujo de las interacciones.
- Evaluar la satisfacción del usuario.

Entre las etapas del análisis están:

1. Análisis conceptual:

- Evaluar el sistema funcional.
- Evaluar la modularidad del sistema.
- Evaluar la segmentación del sistema.
- Evaluar la fragmentación del sistema.
- Evaluar la madurez del sistema.
- Evaluar los objetivos particulares del sistema.
- Evaluar el flujo actual de información.
- Definir el contenido de los reportes y compararlo con el objetivo.

2. Evaluar los modelos de reportes:

- Evaluar los controles de operación.
- Cuantificar el volumen de información.
- Evaluar la presentación y ajustes.

Se debe conocer en términos generales el nivel del sistema funcional para obtener los elementos suficientes que permitan evaluar el nivel de interacción, su grado de estructuración y la madurez del sistema con el fin de determinar si se justifica su automatización.

Entre las evaluaciones que deben hacerse están:

Evalúe el objetivo. Evalúe que el objetivo general y el alcance del sistema funcional estén definidos en forma clara y precisa. Esta actividad se encarga de delimitar el sistema obteniendo todo lo relacionado con él, mediante las entrevistas a los usuarios involucrados con el fin de evaluar si se cumplió con el objetivo. Las versiones que ofrezcan los usuarios deberán ser confrontadas para verificar su compatibilidad.

Evalúe la interacción con otros sistemas. Se debió analizar la información del sistema con el propósito de localizar sus interacciones y sus contactos con otros sistemas, a fin de determinar si existe un sistema integral de información, sistemas aislados o simplemente programas, o si existe redundancia y ruido, así como cuáles son los controles con que cuenta el sistema. Para evaluar todas las entradas y salidas que tienen lugar en el sistema, esta parte de la auditoría determina el flujo de operación y también todas las entradas y salidas que ocurren internamente. La manera de desarrollar esta actividad es usar aquellos documentos de información que maneja el sistema, rastreando las fuentes y destinos, elaborando o reservando la matriz de recepción/distribución de los documentos, y la matriz de entradas/salidas.

Evalúe si se obtiene la secuencia y flujo de las interacciones. Para llevar a cabo esta actividad es necesario establecer el flujo de información a través del

sistema, tomas de la matriz de entradas/salidas y agregar el orden de ocurrencia, así como la periodicidad. Grafíquela en un plano horizontal para tratar de encontrar duplicidad de información. Este plano debe hacerse de tal manera que refleje un periodo, así como el orden de ocurrencia.

Evalúe el sistema funcional. Dado que ya se evaluó el objetivo, las interacciones y su flujo, lo que sigue es analizarlos para tener una idea más clara de su función. Tomando como base los elementos de los primeros tres pasos, se debe verificar si es congruente con su objetivo, es decir, si la descripción define sus propósitos. En esta etapa se evalúa "qué hace" el sistema.

Evalúe la modularidad del sistema. Esta actividad subdivide el sistema en partes que pueden ser procesadas en forma independiente, pero cuyo objetivo particular es buscar el objetivo general del sistema funcional, correspondiendo a cada módulo una función general del sistema. Asimismo, una función general del sistema consiste en identificar aquellas partes de éste donde ocurre una entrada, un proceso, y se obtiene un resultado parcial.

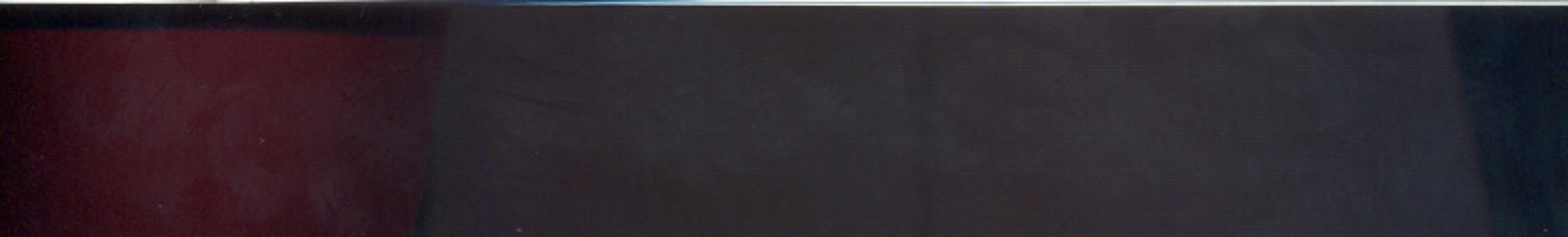
Evalúe la segmentación del sistema. Este paso tiene por objeto subdividir los módulos en funciones particulares, de tal manera que el conjunto de funciones defina al módulo en cuestión. En esta parte deben evaluarse aquellas funciones que son realizadas para distintos módulos (interconexión modular); cada función extraída del módulo debió ser consistente y validada con el usuario.

Evalúe la fragmentación del sistema. Se subdivide el segmento en funciones específicas o procedimientos, pues cada función particular o segmento puede contener uno o más procedimientos. A su vez, cada procedimiento puede estar formado por distintos niveles (jerarquía de procedimientos); dependiendo de su complejidad en esta parte se debe evaluar haciendo énfasis en "qué hace" y no en el "cómo lo hace", ya que esto se evalúa en el análisis detallado.

Evalúe el flujo de información del sistema funcional. Identifique en cada documento su origen y su seguimiento a través de las diferentes entidades o departamentos por donde transita; a la vez vaya identificando sus adiciones y supresiones de información. Por último, identifique cómo y dónde llega a su destino. Se recomienda el uso del diagrama de flujo de información.

Una forma de analizar los hechos es seguir la ruta de la información desde su origen hasta su destino y disponer de este camino en una secuencia cronológica con el fin de clarificar dónde aparece, cómo avanza a lo largo del sistema y cómo llega a su destino. Esta técnica ayuda a hacer un estudio objetivo de todos los pasos por los cuales deberá pasar la información. Se considera necesario agregar algunas características que definan aún más este estudio, como frecuencia, volumen, tiempo, costo y distancia física de cada paso, lo cual ayudará a un mejor análisis y a una evaluación más objetiva del sistema.

Evalúe los documentos de entrada y el contenido de los reportes. Se deben evaluar las formas de entrada, su contenido, claridad, controles, copias solicitadas y autorizaciones, verificar que los reportes o pantallas de salida contengan



- Usuario.
- Contenido.

Pruebas y revisiones. El objetivo es asegurarse que el sistema funcione de acuerdo con las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación (utilice la información obtenida en las opiniones de los usuarios). Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detecta. Las pruebas del sistema buscan asegurar que se cumplan los requisitos de las especificaciones funcionales, verificando datos estadísticos, transacciones, reportes, archivos, anotando las fallas que pudieran ocurrir y realizando los ajustes necesarios. Los niveles de prueba pueden ser agrupados en módulos, programas y en el sistema total.

EVALUACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Esta función tiene una gran importancia en el ciclo de evaluación de las aplicaciones de sistemas de información por computadora. Busca comprobar que la aplicación cumpla las especificaciones requeridas por el usuario, que se haya desarrollado dentro de lo presupuestado y que efectivamente cumpla con los objetivos y beneficios esperados.

Un cambio a un sistema existente, como la creación de uno nuevo, introduce necesariamente cambios en la forma de obtener la información y un costo adicional. Ambos deberán ser evaluados antes y después del desarrollo.

Se debe evaluar el cambio (si lo hay) de la forma en que las operaciones son ejecutadas, comprobar si mejora la exactitud de la información generada, si la obtención de los reportes efectivamente reduce el tiempo de entrega, si es más completa, en qué tanto afecta las actividades del personal usuario, si aumenta o disminuye el personal de la organización, y los cambios de las interacciones entre los miembros de la organización. De ese modo se sabrá si aumenta o disminuye el esfuerzo por generar la información para la toma de decisiones, con el objeto de estar en condiciones de determinar la productividad y calidad del sistema.

El análisis deberá proporcionar: la descripción del funcionamiento del sistema desde el punto de vista del usuario, indicando todas las interacciones del sistema, la descripción lógica de cada dato, las estructuras que forman éstos y el flujo de información que tiene lugar en el sistema; lo que el sistema tomará como entradas, los procesos que serán realizados, así como las salidas que deberá proporcionar, los controles que se efectuarán para cada variable y los procedimientos.

De este modo se agruparán en cuatro grandes temas:

- Evaluación en la ejecución.
- Evaluación en el impacto.

- Evaluación económica.
- Evaluación subjetiva.

EVALUACIÓN EN LA EJECUCIÓN

Se refiere al uso de cuestionarios para recabar datos acerca de la actuación de la aplicación en la computadora, con objeto de conocer qué tan bien o qué tan mal está siendo usada y si opera eficientemente.

Los cuestionarios son medios para recopilar datos acerca del uso de los recursos de la computadora y pueden ser cuestionarios manuales, encuestas de opiniones, evaluación de documentación, obtención de información electrónica integrada al equipo (hardware) y de programas ejecutándose (software), obteniéndose en ambas las estadísticas acerca de su uso.

Los dispositivos de hardware son dispositivos electrónicos que pueden ser conectados a varios puntos del equipo, como lo son en la unidad de control, los canales de comunicación, etc., que durante la ejecución de una aplicación registran cantidad, frecuencia y dirección de los componentes del equipo. Los datos son almacenados normalmente sobre cinta magnética o disco, para que puedan ser analizados después; por ejemplo, algunos de éstos contabilizan la frecuencia de uso de la unidad central de proceso en relación con la espera para operaciones de entrada-salida. Analizando estos datos quizá se detecte la necesidad de agregar procesadores de entrada-salida con objeto de acortar la espera del procesador central, eliminando los cuellos de botella que por esta causa se generan.

Las estadísticas de software son juegos de instrucciones ejecutables conectadas al sistema operativo con el fin de coleccionar datos acerca de la operación del sistema y acerca de los programas de aplicación. Este tipo de monitor requiere memoria y proceso adicional, lo que disminuye la rapidez del procesador. Los datos también son almacenados en cinta magnética o cualquier otro dispositivo de almacenamiento secundario con el fin de analizarlos después. Este monitor ayuda a detectar qué recursos adicionales se necesitan o qué recursos existentes deben ser ejecutados para lograr más eficiencia.

Una estadística de hardware puede ser utilizada para medir la cantidad de tiempo de la unidad de procesamiento central, pero también podrá ser concentrada en los canales de comunicación y dispositivos de almacenamiento secundario para determinar la frecuencia y cantidad utilizada. Su importancia se puede evaluar con el siguiente ejemplo.

Si estamos considerando agregar una nueva aplicación al sistema, el análisis del monitoreo ayuda a determinar si la computadora podrá soportarla, si puede ayudar al administrador a decidir si se agregan nuevas unidades de almacenamiento, líneas de comunicación, terminales, etc. Asimismo, puede usarse para determinar si todo el equipo es necesario, si se deben rediseñar los archivos, etcétera.

Uso
de cuestionarios

Las estadísticas del software nos pueden ayudar a identificar cuáles son los lenguajes más usados, qué tipo de proceso es más común (alto volumen de actualizaciones contra secuencia de cálculos, complejos procesos en lotes contra procesos en línea, frecuencia de corridas, frecuencia de pruebas, programas terminados anormalmente, etcétera).

Estas evaluaciones son generadas automáticamente mostrando a qué horas del día los trabajos son corridos y también qué recursos del sistema fueron utilizados y qué tan grandes son las aplicaciones en relación con el equipo.

Basándose en estos datos, el auditor contará con la información necesaria para hacer las evaluaciones tendientes a mejorar el servicio e incrementar la eficiencia.

Estos dos tipos de monitores normalmente son proporcionados por el fabricante de computadoras, pero algunos monitores de software pueden ser desarrollados por la propia organización.

EVALUACIÓN EN EL IMPACTO

Es la evaluación que se hace sobre la manera en que afecta a la gente que interviene en la aplicación (usuarios) con el objeto de determinar cómo la implantación y el uso del sistema de información afecta a la organización distinguiendo qué factores son directamente atribuibles al sistema. Las principales áreas que deben interesar son las que intervienen en la toma de decisiones y en las actividades de operación.

Esta evaluación se hace con el fin de detectar a la gente involucrada; las actividades que son necesarias realizar, la calidad de la información, y el costo de operación resultante.

Algunas expectativas deben ser elaboradas y jerarquizadas antes de empezar a diseñar el sistema con el fin de que, cuando se instale, se compruebe si los resultados satisfacen plenamente lo planeado. Estos datos también son importantes para guiar futuros proyectos.

Asimismo se debe evaluar el efecto que tiene sobre el ambiente del sistema (personas, leyes, etc.). Para ello contamos con varias técnicas que nos ayudan en este propósito, las cuales son: bitácora de eventos, registro de actitudes, contribución, peso y análisis de sistemas.

Bitácora de eventos

Esta información se obtuvo en la sección de la opinión del usuario donde se registraron los eventos relacionados con la introducción de una aplicación. Cualquier evento que influya en el sistema y cualquier nuevo evento introducido por él, es registrado en forma de notas, y al final se agrupan. Para un estudio sistemático no se requiere equipo adicional, y debe usarse cuando la medición tiene lugar en periodos largos o cuando se desean medir varios tipos de impac-



**Técnicas
de la evaluación**

económico del sistema dentro de la organización en relación con los beneficios obtenidos por éste.

En el impacto se mide cómo una aplicación de sistemas de información ha contribuido o mejorado la eficiencia en el área donde se usa. Asimismo la evaluación después de su implementación es crítica para conocer cómo el sistema opera y dónde pueden necesitarse cambios.

La evaluación económica es importante puesto que el capital de la organización no es gratuito, debiéndose cuantificar los beneficios y los costos del sistema en términos monetarios para estar en condiciones de justificar o no su desarrollo e implantación.

Cuando la aplicación ha sido realizada, se busca obtener el costo real contra el beneficio real para comprobar o determinar el porqué de la diferencia con lo presupuestado y/o la calidad de la aplicación.

Estas técnicas nos ayudan a obtener los elementos necesarios para evaluar por medio de un análisis de costo/beneficio de la aplicación. Nos permite además evaluar si fue desarrollado en las condiciones económicas esperadas, por lo que este análisis deberá efectuarse antes y después del desarrollo de la aplicación. La justificación la encontramos en el hecho de que cualquier tipo de organización busca alcanzar sus objetivos con recursos económicos limitados.

El administrador de sistemas de información deberá verificar y cuidar que estas actividades se realicen en forma sistemática y completa para evitar crear sistemas que perjudiquen a la organización y minen su economía. Este punto es de suma importancia dado el momento actual en donde los recursos computacionales se ven afectados constantemente por las devaluaciones y el costo del capital. Hay que tratar de obtener el mayor beneficio con el equipo disponible e invertir en equipos adicionales sólo cuando esté plenamente justificada la inversión por los beneficios que se obtendrán.

EVALUACIÓN SUBJETIVA

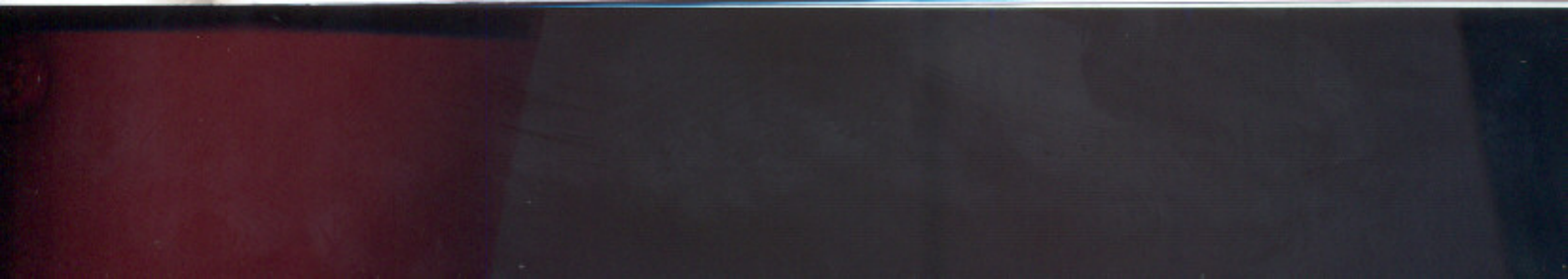
Partiendo de la premisa de que los usuarios son los principales afectados directamente por el sistema, sus puntos de vista y necesidades deberán ser considerados para la evaluación.

Los que procesan los datos, el personal de sistemas y el personal de alta dirección deberán también participar en la determinación de los beneficios económicos de la actividad particular a ser desarrollada.

Un enfoque experimental propone un mecanismo para obtener los factores, además del ahorro de costos, que habrán de ser considerados en la evaluación del sistema de información.

Necesitamos incorporar a nuestra contribución de beneficios los puntos de vista y opiniones de la gente que usará o será afectada por la aplicación del sistema de información.

La justificación de evaluación subjetiva se centra en que la opinión del grupo usuario proporciona un punto de vista más completo de la aplicación, ayudando a obtener aquellos factores que hubiéramos pasado por alto.



Los controles operativos comprenden cada uno de los sistemas en forma individual y constan de:

- Control de flujo de la información.
- Control de proyectos.
- Organización del proyecto.
- Reporte de avance.
- Revisiones del diseño del sistema.
- Técnicas:
 - De usuario.
 - De control.
- Control de cambios a programa:
 - Requisición de cambio.
 - Razón del cambio.
 - Naturaleza del cambio.
 - Persona que lo solicita.
 - Persona que revisa y autoriza.
 - Frecuencia de cambios.
 - Persona asignada al mantenimiento.
 - Bitácora de cambios.
- Mantenimiento y documentación.
- Producción.
- Controles de documentación.
- Documentación:
 - Del sistema.
 - Del programa.
- Mantenimiento y acceso a la documentación.
- Control de sistemas y programas.
- Sistemas en lote (*batch*):
 - De entrada.
 - Autorización de entrada.
 - Armado de lotes.
 - Verificación de lotes.
- Control de programas.
- Reporte de control:
 - Balanceo de lotes.
 - Reporte de errores.
 - Reporte de excepción.

- Reporte de transacciones.
- Reporte de cambios en el archivo maestro.
- Validación de entradas:
 - Verificación de secuencia.
 - Campos omitidos.
 - Totales de control.
 - Transacciones válidas.
 - Caracteres válidos.
 - Campos válidos.
 - Códigos válidos.
 - Pruebas de razonabilidad.
 - Dígito verificador.
 - Etiquetado de archivos.
- Controles de programas misceláneos:
 - Control de programa a programa.
 - Verificación de etiquetas de archivo.
 - Intervención del operador.
 - Punto de verificación y reinicio.
 - Control de salida.
 - Formato de salida.
 - Control de formas de salida.
 - Corrección de errores.
 - Controles corrida a corrida.
 - Sistemas en línea.
- Controles de entrada:
 - Acceso a terminales.
 - Acceso a programas, archivos, datos y a la computadora.
 - Comunicaciones.
 - Información confidencial.
- Control de programa:
 - Reportes de control.
 - Validación de entrada.
- Corrección de errores.
- Puntos de verificación y reinicio.
- Controles de salida:
 - Formatos de reporte.
 - Formas de control de salida.
 - Información confidencial.

Los controles técnicos que se deben evaluar son:

- Controles de operación y uso de la computadora.
- Supervisor.
- Capturistas.
- Bibliotecario.
- Operadores.
- Controles de entrada y salida.
- Recepción de información.
- Detección y corrección de errores.
- Distribución de la información.
- Calendarización.
- Reporte de fallas y mantenimiento preventivo.
- Controles sobre archivos.
- Recuperación de desastres.
- Controles de usuarios.
- De origen de datos.
- Origen de documentación fuente.
- Autorización de documentación fuente.
- Recolección y preparación de entrada y documentación fuente.
- Manejo de errores de documentación fuente:
 - Tipos de errores que pueden aparecer.
 - Pasos a seguir para su corrección.

Los métodos a utilizar para recuperar documentos fuente corregidos son:

- Retención de documentos fuente.
- Controles de entrada de datos.
- Conversión de datos y captura.
- Validación de datos.
- Manejo de errores en datos y captura.
- Controles de salida de datos.
- Balanceo y conciliación de salidas.
- Distribución de salidas.
- Procedimientos documentados que describen los métodos de distribución.
- Calendarización, revisión y distribución de salida por parte de los usuarios.
- Bitácoras de reportes.
- Manejo y retención de registros de salida y documentos contables.
- Formatos de salida:
 - Frecuencia.
 - Número de copias.

Controles técnicos:

- Programática.
- Aplicaciones.
- Sistemas.

Recursos de los programas por aplicación:

- Calendario de programas.
- Errores y recuperación.

Registro contable:

- Equipos.
- Unidad control de procesos.
- Memoria secundaria.
- Dispositivos periféricos.

Controles lógicos del sistema:

- Sistemas operativos.
- Sistemas de utilería.
- Sistemas de bibliotecas.
- Sistemas de mantenimiento de archivo.
- Sistemas de seguridad.

Control de acceso al sistema.

Control de cambios al sistema:

- Redundancia en la información.
- Inconsistencia de datos.
- Seguridad.

Controles de seguridad, respaldo y confidencialidad.

Sobre las bases de los objetivos de la auditoría en informática se deben presentar, de acuerdo con la información obtenida, los controles existentes, las conclusiones, opiniones y alternativas de solución debidamente fundamentadas en cuanto a:

- Evaluación de los sistemas.
- Evaluación de los equipos.

PRESENTACIÓN

La presentación de las conclusiones de la auditoría podrá hacerse en la siguiente forma:

1. Una breve descripción de la situación actual en la cual se reflejen los puntos más importantes. (Esta presentación es para el nivel más alto de la organización.)

2. Una descripción detallada que comprende:

- Los problemas detectados.
- Posibles causas, problemas y fallas que originaron la situación presentada.
- Repercusiones que pueden tener los problemas detectados.
- Alternativas de solución.
- Comentarios y observaciones de la dirección de informática y de los usuarios sobre las soluciones propuestas.

Si se opta por alguna alternativa de solución, cuáles son sus repercusiones, ventajas y desventajas, y tiempo estimado para efectuar el cambio.

1. Se debe hacer hincapié en cómo se corregirá el problema o se mejorará una determinada situación, se obtendrán los beneficios, en cuánto tiempo y cuáles son los puntos débiles.
2. Se debe romper la resistencia a la lectura que tienen algunos ejecutivos por medio de conclusiones concretas que sean sencillas (se procurará que se entiendan los términos técnicos y, si es posible, usar técnicas audiovisuales).

Como ejemplo de formato de presentación de las conclusiones de la auditoría en informática, véase la figura 7.1, y como ejemplo del seguimiento de la auditoría en informática, véase la figura 7.2.

Figura 7.1. Conclusiones de la auditoría en informática

DIRECCIÓN _____ HOJA NÚM. _____ DE _____ AUDITORÍA A _____ FECHA DE TÉRMINO DE LA AUDITORÍA _____							
NÚM.	PROBLEMÁTICA	CAUSAS	REPERCUSIONES	ALTERNATIVAS DE SOLUCIÓN	OBSERVACIONES	FECHA PROBABLE DE IMPLAN.	RESPONS. DE LA RECOMEN.

PERIODO QUE SE REPORTA _____

DIRECCIÓN _____ HOJA NÚM. _____ DE _____
AUDITORÍA A _____ FECHA DE TÉRMINO DE LA AUDITORÍA _____

[illegible]

Conclusiones

El avance tecnológico que se ha logrado en los últimos años ha sido impresionante. El avance se ha reflejado más posiblemente en el área de informática, lo cual ha provocado que se tenga microcomputadoras con un bajo costo y con una gran capacidad de procesamiento y que se cuente con computadoras que permitan desde el control del proceso de ensamble de automóviles en forma completamente automática, hasta que en la década de los sesenta se haya podido llegar a la Luna. En el área educativa este avance ha influido en todas las carreras, desde las subtécnicas y subprofesionales hasta las técnicas y profesionales. Nos encontramos así con que los niños de primaria ya están usando las computadoras y no hay profesión que no necesite en forma directa o indirecta su utilización.

Si analizamos que aproximadamente 80 por ciento de las computadoras digitales son utilizadas en las organizaciones con fines de información, de toma de decisiones, contables y administrativos, y si evaluamos el costo que representa la utilización de estas computadoras, podremos ver la importancia que tiene para la alta dirección poder evaluar la adecuada utilización de esta herramienta. Esto trae como consecuencia que el profesionista deba actualizarse en el uso adecuado de la nueva tecnología, así como en la evaluación que se haga de este recurso tan costoso. También deben adecuarse las normas de auditoría y del control interno para que sean congruentes con el desarrollo tecnológico. La auditoría en informática es una nueva materia que es consecuencia directa del desarrollo en el área y de la necesidad de evaluar la adecuada utilización, respaldo y confidencialidad de la información de la organización.

Esta nueva área evalúa la información desde su generación (dato) hasta su utilización (información), y debe considerar la herramienta que se utiliza, su optimización, el respaldo de la información, la seguridad y confidencialidad de la misma, y conseguir el mejor uso de la información al menor costo, evitando duplicidad.

Para lograr esta evaluación se requiere que el auditor conozca no sólo sobre las materias que le son propias, sino que tenga una capacitación técnica en el área de sistemas computacionales e informática.

La auditoría no debe terminar con la presentación, sino ser el inicio de una serie de auditorías y revisiones periódicas, con un adecuado seguimiento de las observaciones, para lograr las correcciones a los problemas y las mejoras a los sistemas que lo ameriten.

Bibliografía

- Apuntes de auditoría administrativa*, Lic. y C.P. Jorge Álvarez Anguiano. Facultad de Contaduría y Administración, Universidad Nacional Autónoma de México.
- La auditoría administrativa*, Lic. José Antonio Fernández Arena, editorial Diana.
- Administración*, Koontz, O'Doneel y Weihrich, editorial McGraw-Hill.
- Auditoría de estados financieros, un caso práctico*, Gabriel Sánchez Curiel, editorial McGraw-Hill, 1997.
- Auditoría de sistemas electrónicos*, Porter Jr., W. Thomas, editorial Herrero Hermanos, sucesores, 2a. edición, México, D.F.
- Auditoría en informática, un enfoque práctico*, Mario G. Piattini, Emilio del Peso, editorial Ra-Ma, 1998.
- Auditoría en informática, un enfoque metodológico y práctico*, Enrique Hernández Hernández, editorial Continental, 1996.
- Control y auditoría del computador*, Instituto Mexicano de Contadores Públicos, A. C., México, D. F.
- Control Objectives*, EDP Auditors Foundation for Education and Research, U.S.A.
- La computación en México, diagnóstico, perspectiva y estrategias de desarrollo*, Fundación Arturo Rosembleuth, A.C., 1982.
- Computer Audit Guidelines*, Canadian Institute of Chartered Accounts, Toronto, Canadá.
- Derecho intelectual*, David Rangel Medina, 1a. edición, editorial McGraw-Hill, 1998.
- EDP Auditing Conceptual Foundations and Practice*, Ron Weber, editorial McGraw-Hill.
- EDP Auditing*, Kenneth W. Clowews, Holt, Rinehart y Winston, Canada Limited.
- Foundations of Information Systems*, V Ladimir Zwass, editorial McGraw-Hill, 1997.
- La gestión de los nombres y direcciones de Internet: cuestiones de propiedad intelectual*, 30 de abril de 1999, Organización Mundial de la Propiedad Intelectual (OMPI).
- Guía 11*, International Federation of Accountants (IFAC), Revisado, 1998.
- Information System Management*, James A. Senn, State University of New York Bringhamton, editorial Wadsworth Publishing Company, Inc., Belmont, California, 1978.
- Information System in Management*, editorial Reston Publishing Company, Inc., 1a. edición, Reston Virginia.
- Ingeniería computacional, diseño de hardware*, M. Morris Mano, editorial Prentice Hall, 1991.

- Management An Experimental Approach*, Knudson, Harry R., Woodworth, Robert, Bell, Cecil H., editorial McGraw-Hill, 1a. edición, Nueva York.
- Management Information System, The Management View*, Robert Schulthers, Mary Sumner, editorial McGraw-Hill, 1998.
- Management Information and Control System*, R.I. Trickner, Oxford Center for Management Studies, editorial Willer-Interscience Publication, 1976.
- Management Information Systems*, Stephen Haag, Maeve Cummings, James Dawkans, editorial McGraw-Hill, 2a. edición, 2000.
- Management Standards for Data Processing*, Brandon, Dick H., editorial Van Nostrand Reinhoold Company, 1a. edición, Nueva York, USA.
- Manual de informe del auditor*, Instituto Mexicano de Contadores Públicos.
- Metodología y técnicas de investigación en ciencias sociales*, Felipe Pardinas, editorial Siglo XXI, 1981.
- Modern Control Systems*, Richard C. Dorf, Robert H. Bishop, editorial Addison-Wesley, 1995.
- Normas y procedimientos de auditoría*, Instituto Mexicano de Contadores Públicos.
- Procedimientos de control en computación*, Canadian Institute of Chartered Accounts, Instituto Mexicano de Contadores Públicos, A.C.
- Protección informática*, Pierre Gratton, editorial Trillas, 1998.
- La protección jurídica de los programas de computación*, Universidad Nacional Autónoma de México, 1998.
- Redes de computación*, Andrew S. Tanenbaun, 3a. edición, editorial Prentice Hall, 1997.
- Secretos industriales, comentarios sobre aspectos relevantes de su reglamentación en México*, Mauricio Jalife Daher.
- Seguridad en centros de cómputo*, Leonard H. Fine, editorial Trillas, 1988.
- Seguridad en computación*, William P. Martin, Interface Age, febrero, 1984.
- Seguridad en informática*, Jao Marcos Fantinatti, editorial McGraw-Hill.
- Sistemas operativos, conceptos fundamentales*, A. Silberschatz, J. Peterson, P. Galvin, 3a. edición, editorial Addison-Wesley Iberoamericana, 1994.
- Sistemas de información administrativa*, Robert G. Murdic, 2a. edición, editorial Prentice Hall.
- The System Development Audit*, Horeld Werss, PTH International Conference of EDP, Auditor Association.
- Técnicas de la auditoría en informática*, Yan Derrien, editorial Alfaomega Marcombo, 1995.

ÍNDICE ANALÍTICO

-A-

Acceso

- claves de, 198-199
- controles de, 225
- llaves de, 198-199
- rutras de, 197-198

Actividades

- calendario de, 121
- control de, 122
- hoja de planeación de, 126

Administración de la investigación

- preliminar, 39

Agua, desastres por, 224

Aire

- acondicionado, 221
- ductos de, 228
- movimiento de (CFM), 227

Alarma contra incendio, 226

Alcance de la cobertura, 244

Almacenamiento

- de documentos de entrada, proceso y salida, 15
- dispositivos de, 173-177

Alta gerencia, 37

Análisis

- crítico de los hechos, 270-271
- de informes, 107, 113
- de la situación, 56
- de organizaciones, 75-76
- de sistemas, 279
- del impacto de la organización, 259
- del sistema, 93
- evaluación del, 95-97
- manuales de, 96
- y diseño estructurado, 97

Analizadores de virus, 237

Aplicación(es)

- ciclo de evaluación de las, 276
- planeación de las, 95
- situación de una, 95-96

Aseguradores, 244

Asegurados, 243

- responsabilidad de los, 244

Asignación de trabajo, control de, 171-172

Auditor(es), 16, 32, 239

- independencia del, 37
- número de, 32
- participación, 92
- responsabilidades de los, 29-30, 187-188

Auditor interno, 8-9, 26, 34

- conocimiento y experiencia del, 27-29
- habilidades del, 16-17, 28
- objetividad del, 27

Auditoría

- asistida por computadora, 10
- conclusiones de la, 287
- definición, 2
- de programas, 22-23
- personal de la, 43
- planeación de, 16, 30-31, 41-42
- presentación de la, 285-286
- procedimientos de, 34
- programa(s) de, 11, 43-44
- programas de trabajo de, 32
- reportes especiales, 215
- requerimientos de una, 40-42
- seguimiento de la, 288
- técnicas avanzadas de, 12-16

Auditoría administrativa, 9-10

Auditoría con informática, 10

Auditoría en informática, 17-18

- campo de acción de la, 20
- concepto, 17-18, 26
- director de, 35
- elementos que debe evaluar la, 96-97
- la, y los tipos de auditoría, 22
- objetivos de la, 21-22
- pasos de una, 37
- planeación de la, 30-32
- Auditoría interna, 26
- normas de, 26
- responsabilidades del departamento de, 27

- Autenticación
 - del usuario, 212
 - en sentido digital, 216
- Autorización de accesos, seguridad de, 225

-B-

- Bases
 - de indemnización, 246-247
 - jurídicas del departamento de informática, 64-67
- Bases de datos, 99-100, 249
 - administrador de, 100-101
 - componentes a evaluar en una, 100
 - modelos de, 101
 - sistema de administración de, 99
 - software manejador de (DBMS), 202-203
- Batch, véase Sistemas en lote
- Bitácora(s), 158
 - de auditoría, 200-201, 205, 206
 - de eventos, 278-279
- Boletín C, 2
- Boletín E-02, 5
- Bootstrap, 237
- BTU, véase Disipación térmica
- Bugs, 236

-C-

- CAD/CAM, véase Diseño de manufactura por medio de asistencia computarizada
- Calendario de actividades, 121
- Calor, pérdidas por transferencia de, 227
- Cambios y mejoras al sistema, 93
- CASE, véase Software de ingeniería de asistencia computarizada
- Categorización del software, 90
- Centralización, 188-189
- Centro de cómputo, 182-183
 - seguridad de acceso, 225
 - ubicación y construcción del, 220, 228-230
- CERT, véase Equipo de respuesta de emergencias de computadora
- CFM, véase Movimiento de aire
- Ciclo de evaluación de las aplicaciones, 276
- Clasificación
 - de desastres, 252
 - de transacciones, 6
 - del riesgo, 254
- Cobertura, alcance de la, 244
- Componentes
 - de un sistema de comunicación, 102
 - lógicos, 242
- Computadora
 - crímenes por, 193-194
 - delitos por, 192, 193
 - virus de, 193
- Comunicación, 102-103, 113
 - sistema de, 102
- Conclusiones, 289
- Confidencialidad, 197
- Configuración del equipo, 265
- Consideraciones al auditar, 208-215
 - autenticación del usuario, 212
 - instalación y mantenimiento, 209-210
 - operación, 210
 - recursos para controlar el acceso, 212
 - software de control de acceso, 196, 199-205, 212-215
- Consulta a los usuarios, 92
- Contingencia(s)
 - etapas del proyecto del plan de, 253
 - metodología del plan de, 253
 - plan de, 251, 252, 257, 263
- Contratación de empleados, planes de, 32
- Contribución y peso, 279
- Control(es)
 - a auditar, 205-208
 - de acceso, 225
 - de asignación de trabajo, 171-172
 - de avance, 129
 - de avance de programación, 128
 - de calidad, programa de, 35
 - de datos fuente, 161-162
 - de diseño de sistemas, 119, 130-132
 - de mantenimiento, 177-179
 - de medios de almacenamiento masivo, 173-177
 - de proyectos, 117-119
 - de seguridad, 285
 - generales, 281
 - mesa de, 164, 165
 - operativos, 282-283
 - salida, 170-171
 - técnicos, 284-285
- Control interno, 5
 - objetivo(s)
 - autorización, 6
 - básicos, 5
 - de salvaguarda física, 7

de verificación y evaluación, 7
 generales, 5-6
 procesamiento, 6
 utilidad de los objetivos elementales
 del, 29
 Cookie, 143
 Copias "piratas", 193
 Costo
 de la operación, 164, 166
 de un sistema, 94
 del equipo de cómputo, *xi*, 240
 Credenciales con banda magnética, 199
 Criptoanálisis, 217
 Criptografía, 217-218, 247
 Cuestionario(s), 134-138, 256
 de funciones críticas, 260
 de operación, 261-262
 de seguridad física, 228-236
 para guiar la entrevista, 259
 sobre el impacto de la organización,
 259
 y entrevistas, 256
 Cumplimiento de los documentos
 administrativos, 57

-D-

Datos, 156
 DBMS, *véase* Sistema de administración de
 bases de datos
 Decisiones, soporte en la toma de, 272
 Degradación del equipo, 182
 Delitos por computadora, 192
 motivos, 192-193
 Departamento (o área) de informática
 bases jurídicas, 64-67
 evaluación administrativa del, 20
 funciones en el, 67-72
 objetivos, 72-75
 seguridad del, 192-193
 tipos de dependencias del, 62-63
 Derechos de autor, 138-142
 protección de los, 144-145
 Desarrollo
 del sistema, evaluación, 115
 estrategia de, 91-92
 implementación y, físico, 93
 programas de, 98-99
 Desastre(s)
 clasificación de, 252-253
 plan en caso de, 264
 por agua, 224

Descripción
 de formas, 111
 de formas de papelería, 112
 de informes, 106
 Detección de humo y fuego, 226, 232-234
 Diagrama(s)
 de flujo, 97
 uso de, 272
 Diseño
 de formas, 104-113
 de manufactura por medio de
 asistencia computarizada
 (CAD/CAM), *xii*
 del sistema, 93
 detallado, 93
 estructurado, análisis y, 97
 evaluación del, 130-131
 formas de, 104
 general, 93
 lógico del sistema, evaluación del,
 98-103
 Disipación térmica (BTU), 227
 Dirección del autor en Internet, *xiv*
 Disponibilidad, 197
 División de tareas entre los empleados, 15
 Dominio, nombres de, 149-154
 DSS, *véase* Soporte en la toma de decisiones

-E-

EDI, *véase* Intercambio electrónico de datos
 Eficiencia de la operación, 164, 166
 EFTS, *véase* Sistema de transferencia
 electrónica de fondos
 EIS, *véase* Sistemas de información para
 ejecutivos
 Elementos de las entrevistas, 257
 EMS, *véase* Sistemas de reuniones en
 forma electrónica
 Encriptamiento, 216-218
 Entrevista(s)
 a usuarios, 133-134
 con el jefe de informática y con
 especialistas, 258
 con el personal de informática,
 82-83
 cuestionario para guiar la, 259
 elementos de las, 257
 propósito de las, 257
 y cuestionarios, 256, 259
 Entropía, 115
 Equipo(s)

configuración del, 265
 de cómputo, seguridad de, 241
 de respuesta de emergencias de computadora, 238
 seguridad al restaurar el, 249
 seguridad en la utilización del, 247
 seguros de los, 240
 Estrategia
 de desarrollo, 91-92
 de respaldo, 263
 Estudio
 de factibilidad, 92, 94, 119
 de viabilidad, 58-59
 Etapas del proyecto del plan de contingencias, 253-254
 Evaluación
 administrativa del departamento de informática, 21
 ciclo de, de las aplicaciones, 276
 de formas, 108-110
 de la configuración del sistema de cómputo, 183-189
 de la estructura orgánica, 61-63
 de la gerencia de informática, 58
 de la instalación en términos de riesgo, 255-256
 de los recursos humanos, 76-82
 de los sistemas de información, 276-277
 de sistemas, 90-95, 272-276
 de acuerdo con el riesgo, 38
 distribuidos, 116
 y procedimientos, 21
 de software, 99
 de un sistema con datos de prueba, 12
 del desarrollo del sistema, 115
 del diseño, 130
 del diseño lógico del sistema, 98, 103
 del mantenimiento, 179-182
 del proceso de datos, 21
 detallada, 33
 económica, 279-280
 en el impacto, 278-279
 en la ejecución, 277-278
 subjetiva, 280-281
 Examen y evaluación de la información
 pruebas de consentimiento, 35-36
 pruebas de controles del usuario, 36
 pruebas sustantivas, 36-37
 Extintores (o extinguidores), 226-227, 232-234
 Extranet, xi

-F-

Factibilidad, estudio de, 92, 94
 Firma digital, 216-217
 Formas
 de diseño, 104
 descripción de, 111, 112
 evaluación de, 108, 109, 110
 Formas tradicionales de evidencia
 almacenamiento de documentos de entrada, proceso y salida, 15
 división de tareas entre los empleados, 15
 listado de los resultados del proceso, 14-15
 mantenimiento en manuales de información, 14
 manuales de procedimientos con información relativa, 15
 procesamiento manual, 14
 proceso de grandes cantidades de datos, 15-16
 proceso simplificado, 14
 registro manual de la información, 13-14
 revisión de procesos, 15
 revisión de transacciones por el personal, 14
 transacciones originadas por personas, 13
 transporte de documentos, 14
 uso de documentos impresos, 15
 Fraude, 194, 195
 Fuego y humo, 226-227
 detección de, 226, 232-234
 Funciones
 críticas, cuestionarios de, 260
 en informática, 67-72

-G-

Grado de madurez del sistema, 271
 Gráfica de flujo de la información, 104
 Grupo de recuperación, 253

-H-

Hackers, 239
 Hardware, 277
 Hechos, análisis crítico de los, 270

Humedad, temperatura y, 227-228

Humo, fuego y, 226-227

detección de, 226, 232-234

-I-

Implantación, 133

Implementación y desarrollo físico, 93

Incendios, 224

Indemnización, bases de, 246

Información, 4

confiabilidad e integridad de la, 29

de niveles, 4

entrada de la, 162-164

examen y evaluación de la, 34-37

gráfica de flujo de la, 104

manejo de la, 248

pérdida de, 19-20

planeación y control de la, 4

sistema de, 29

utilidad de la, 57-58

Informática, 3, 8

departamento de, 20, 62-63

entrevistas con el personal de, 82-83

funciones en, 67-72

gerencia de, 58

Informes, 103-113

análisis de, 107, 113

descripción de, 106

Inicialización, 237

Instalación eléctrica, 222-224

Instructivo(s) de operación, 132, 170

Integridad, 197

Intercambio electrónico de datos (EDI), *xii*

Internet, *xi*, 142-144, 238

dirección del autor en, *xiv*

Investigación preliminar, 39-42

-L-

Lenguajes de programación, 98

Listado de los resultados del proceso,
14-15

Llaves de acceso, 198-199

-M-

Mainframe, *xi*, 227

Manejo de información, 248

Mantenimiento

en manuales de información, 14

evaluación del, 179-182

excesivo, 131-132

instalación y, 209-210

tipos de contratos de, 177-179

Manual(es)

de análisis, 96

de organización, 26, 61

de procedimientos con información
relativa, 15

Memorias RAM y ROM, *xi*

Metas, 31-32

Metodología del plan de contingencias, 253

Movimiento de aire (CFM), 227

-N-

Nombres de dominio, 149-154

-O-

Objetivo(s)

de la auditoría en informática,
21-22

de la seguridad en el área de
informática, 192

del departamento de informática,
72-75

del libro, *xiii*

del plan de contingencias, 253

Operación(es)

consideraciones a auditar, 210

de los sistemas en lote, 166-170

en paralelo, 12

instructivos de, 132, 170

Organización(es)

análisis de, 75-76

análisis del impacto de la, 259

antecedentes de la, 258

manual de, 26

plan de recuperación de la, 262

procesos críticos de una, 255-256

-P-

Password, 198

Pérdida de la información, 19-20

Pérdidas por transferencia de calor, 227

- Personal
 - de cargas de máquina, 171
 - de procesos electrónicos, 56
 - participante, 42-54
 - Piso elevado, 221
 - Plan(es)
 - de contingencias, 251-263
 - de proyectos, 60-61
 - de recuperación de la organización, 262, 264
 - de seguridad, 61, 252
 - estratégico, 91-92
 - maestro, 60
 - Planeación
 - de actividades, hoja de, 126, 129
 - de auditoría, 16
 - de cambios, 59
 - de la auditoría en informática, 30-32
 - de programación, 125
 - de sistemas, 92
 - documentada, 31
 - estratégica, 95
 - proceso de, 31
 - Política(s)
 - de respaldos, 156-157
 - de revisión de bitácora, 158
 - de seguridad física del *site*, 159-161
 - y procedimientos, 157
 - Póliza de seguro, 241
 - Presupuestos, 84-85
 - Problemas de los sistemas de
 - administración de bases de datos, 101
 - Procedimientos de restauración, 250
 - Procesamiento manual, 14
 - Proceso(s)
 - críticos de una organización, 255-256
 - de grandes cantidades de datos, 15-16
 - repetición de, 250
 - simplificado, 14
 - Productividad, 184-186
 - Programación
 - control de avance de, 128
 - facilidades de, 133
 - informe de avance de, 127
 - planeación de, 125
 - riesgos en la, 248
 - Programador(es)
 - control de, 124
 - control de actividades del, 122
 - Programas
 - copias de, 193, 194
 - de desarrollo, 98-99
 - de trabajo, 172
 - Propósito de las entrevistas, 257
 - Protección contra virus, 237
 - Proyecto(s)
 - control de, 117-119, 120
 - del plan de contingencias, 252-254
 - Pruebas de consentimiento, 35-36
 - Pruebas integrales, 12
- R-
- RAM, *xi*
 - Recuperación
 - grupo de, 253
 - plan de, 265
 - Recopilación de la información, 56-58
 - Recursos financieros, 85-86
 - Recursos humanos, 56-57
 - Recursos materiales, 86-87
 - Red(es)
 - de computadoras, 249
 - puntos a revisar en las, 103
 - tipos y topología, 102
 - Redundancia, 114-115
 - Registro(s)
 - de actitudes, 279
 - extendidos, 12
 - Reguladores, 222-223
 - Relación precio/memoria, *xi*
 - Renta, 187-188
 - Repetición de procesos, 250
 - Reportes, 212-213
 - especiales de auditoría, 215
 - Respaldo(s)
 - de información, 156-157
 - estrategia de, 263
 - Responsabilidad de los asegurados, 244
 - Restauración, procedimientos de, 250
 - Resultados de cálculos para
 - comparaciones, 13
 - Revisión(es)
 - de acceso, 12
 - de procesos, 15
 - detallada, 33
 - preliminar, 32-33
 - Riesgo(s)
 - clasificación del, 254
 - en la programación, 248
 - evaluación de la instalación en
 - términos de, 255-256
 - ROM, *xi*
 - Ruido, 113
 - Rutas de acceso, 198

-S-

- Salida, control de, 170-171
- Secretos industriales, 145-149
- Seguridad, 21
 - al restaurar el equipo, 249-250
 - contra desastres por agua, 224, 231
 - de autorización de accesos, 225, 231-232
 - en contra de virus, 236
 - en el personal, 218-219
 - en la utilización del equipo, 247-249
 - física, 219, 228-236
 - lógica, 194-197
 - objetivos de la, en el área de informática, 192
 - plan de, 252
 - sistema integral de, 196
- Seguro(s)
 - condiciones generales, 243-244
 - de los equipos, 240, 241
 - exclusiones especiales, 244-245
 - exclusiones generales, 242-243
 - póliza de, 241-242
- Selección
 - de determinado tipo de transacciones, 13
 - de la estrategia, 262-267
- Simulación, 12
- Sistema(s)
 - cambios y mejoras al, 93
 - ciclo de vida de los, 92-93
 - componentes esenciales, 258
 - confidencialidad de los, de información, 197
 - críticos, 260
 - de administración de bases de datos (DBMS), 99
 - problemas de los, 101
 - de bases de datos, 100
 - ventajas de los, 101
 - de cómputo, evaluación de la configuración del, 183-189
 - de comunicación, 102
 - de energía no interrumpido (UPS), 223
 - de información, 29
 - evaluación de los, 276-277
 - de información para ejecutivos (EIS), xii
 - de reuniones en forma electrónica (EMS), xii
 - de transferencia electrónica de fondos (EFTS), xii
 - disponibilidad de los, de información, 197
 - distribuidos, 116
 - en línea o en tiempo real, 249, 251
 - en lote (*batch*), 166-170
 - estudio de los, 96
 - evaluación de, 90-95, 272-276
 - evaluación del desarrollo del, 115
 - evaluación del diseño lógico del, 98, 103
 - grado de madurez del, 271
 - integral de seguridad, 196
 - integridad de los, de información, 197
 - operativos, 201-202
 - planeación de, 92
 - problemas más comunes de los, 94-95
 - procedimiento en el, 104
 - pruebas del, 93
 - reporte semanal de los responsables del, 123
- Site
 - características del, 160
 - instalaciones del, 159-160
- Situación de los recursos humanos, 56
- Software
 - a la medida de la oficina, 91-95
 - categorización del, 90
 - comercial, 90
 - compartido o regalado, 90
 - control de las licencias del, 158-159
 - de ingeniería de asistencia computarizada (CASE), xii, 98
 - de seguridad, 200
 - de seguridad general, 205
 - elaborado por el usuario, 90
 - esclavo, 238
 - específico, 206
 - evaluación de, 99, 209
 - transportable, 90
 - un solo usuario o multiusuario, 90
- Software de control de acceso, 196, 199-205
 - consideraciones a auditar, 210-211
 - reportes y vigilancia, 212-213
 - sistemas operativos, 201-202, 206-207, 213
 - software de consolas o terminales maestras, 203, 207
 - software de librerías, 203-204, 207, 214
 - software de telecomunicaciones, 205, 208, 215
 - software de utilerías, 204-205, 208, 214-215

software manejador de bases de datos, 202-203, 207, 213-214

Soporte

cotidiano, 93

en la toma de decisiones (DSS), 272

Subplanes del plan maestro, 60

-T-

Técnicas de auditoría

análisis crítico de los hechos, 270-271

evaluación de un sistema con datos de prueba, 12

grado de madurez, 271-272

operaciones en paralelo, 12

pruebas integrales, 12

registros extendidos, 12

resultados de ciertos cálculos para comparaciones posteriores, 13

revisiones de acceso, 12

selección de determinado tipo de transacciones, 13

simulación, 12

totales aleatorios de ciertos programas, 12

Tecnología

de flujos (WORKFLOW), xii

neutral, 20

Telecomunicaciones, software, 205, 208

Temperatura y humedad, 227

Tierra física, 222

Tipos y topología de redes, 102

Tolerancia, 260

Toma de decisiones incorrectas, 18

Totales aleatorios de ciertos programas, 12

Transacción(es)

clasificación de, 6

originadas por personas, 13

registro manual de la información para originar una, 13-14

revisión de, por el personal, 14

-U-

UPS, *véase* Sistema de energía no interrumpido, 223

Uso de documentos impresos para construir el proceso, 15

Usuario(s)

aceptación por parte del, 93

autenticación de, 212

consulta a los, 92

cuestionario para los, 211-212

entrevistas a, 133-134

requerimientos del, 92, 135

tipos de, 196-197

Utilerías, 204

Utilización del equipo, seguridad en la, 247

-V-

Vacunas contra virus, 237

Validación por características, 199

Virus

analizadores de, 237

daños por, 236

de computadora, 193, 236

protección contra, 237-240

seguridad en contra de, 236-237

vacunas contra, 237

-W-

WORKFLOW, *véase* Tecnología de flujos

-Z-

Zombies, 238-239

AUDITORÍA EN INFORMÁTICA

AUDITORÍA EN INFORMÁTICA

JOSE ANTONIO ECHENIQUE GARCÍA

Universidad Nacional Autónoma de México
Universidad Autónoma Metropolitana

McGraw-Hill

MÉXICO - BUENOS AIRES - CARACAS - GUATEMALA - LIMA - MADRID
NUEVA YORK - SAN JUAN - SANTAFÉ DE BOGOTÁ - SANTIAGO - SÃO PAULO
AUCKLAND - LONDRES - MILÁN - MONTREAL - NUEVA DELHI - SAN FRANCISCO
SINGAPUR - ST. LOUIS - SIDNEY - TORONTO

La auditoría en informática es una práctica administrativa por demás sana en empresas y organizaciones, sobre todo en esta época donde las características del software y del hardware varían con el fin de satisfacer necesidades muy diversas.

Presentamos la esperada segunda edición de *Auditoría en informática*, obra que se ha actualizado para responder a los cambios más actuales que la industria informática ha generado en sus múltiples áreas.

De manera indudable, quien tenga necesidad de saber cómo realizar la tarea de la auditoría informática, encontrará aquí todos los elementos para cumplir su cometido.

ISBN 970-10-3356-6



9 789701 033562

**McGraw-Hill Interamericana
Editores, S.A. de C.V.**

A Subsidiary of The McGraw-Hill Companies
www.mcgraw-hill.com.mx

