

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONOMICAS

**"AUDITORIA DE INFORMATICA EN UN BANCO PRIVADO
GUATEMALTECO"**

TESIS

**Presentada a la Junta Directiva de la
Facultad de Ciencias Económicas
por**

HILDA DE MARIA BERGANZA GARZA

**Previo a conferírsele el Título de
CONTADOR PUBLICO Y AUDITOR
En el Grado Académico de:**

LICENCIADO

Guatemala, mayo del 2000



**MIEMBROS DE LA JUNTA DIRECTIVA DE LA
FACULTAD DE CIENCIAS ECONOMICAS**

Decano	Lic. Miguel Angel Lira Trujillo.
Secretario	Lic. Eduardo Antonio Velásquez Carrera.
Vocal I	Lic. Rolando de Jesús Oliva Alonzo.
Vocal II	Lic. Andrés Guillermo Castillo Nowell.
Vocal III	Lic. Gustavo Adolfo Vega.
Vocal IV	P.A.E Jairo Joaquín Flores Divas.
Vocal V	P.C. William Tomás Ramírez Raymundo.

EXAMINADORES DE AREAS PRACTICAS

Matemática-Estadística	Lic. Jorge Orlando Recinos Sandoval
Contabilidad	Lic. Gaspar Humberto López Jiménez
Auditoría	Licda. Esperanza Roldán de Morales.

**JURADO QUE PRACTICO
EL EXAMEN PRIVADO DE TESIS**

Presidente	Lic. Rolando Jiménez Godoy.
Examinador	Lic. Sergio Arturo Sosa Rivas.
Examinador	Lic. Rodolfo Payes Aguilar.

LIC. LUIS EDUARDO CHAVEZ YANCOS.
Contador Público y Auditor.
Colegiado No. 2339

Guatemala, 24 de noviembre de 1999.

Señor Decano
Miguel Angel Lira Trujillo
Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala
Ciudad Universitaria, Zona 12.

Señor Decano:

En atención al nombramiento emitido por esa Decanatura, procedí a asesorar y revisar el trabajo de tesis asignado a la señorita **HILDA DE MARÍA BERGANZA GARZA**, denominada "**AUDITORIA DE INFORMATICA EN UN BANCO PRIVADO GUATEMALTECO**".

El trabajo de tesis fue desarrollado con base en la experiencia personal de la autora, por lo que contiene material valioso en apoyo bibliográfico para los estudiantes de la carrera de auditoría, así como indudablemente constituye un gran aporte para los profesionales de la Contaduría Pública, en el sentido de servir como guía al realizar trabajos de Auditoría en función de la Informática.

En mi opinión, la tesis de mérito llena los requisitos técnicos necesarios, en tal virtud recomiendo que sea aceptada para su discusión en el Examen General Privado de la sustentante, para optar al título de Contador Público y Auditor en el grado de Licenciado.

Hago propicia la ocasión para quedar de Ud., atento servidor,

Atentamente,



DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA,
OCHO DE MAYO DOS MIL.

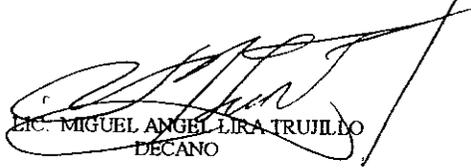
Con base en lo estipulado en el Artículo 23o del Reglamento de Evaluación Final de Exámenes de Areas Prácticas y Examen Privado de Tesis, el dictamen emitido por el Licenciado Luis Eduardo Chávez Yancos, quien fuera designado Asesor y el Acta AUD. 06-00, donde consta que la estudiante HILDA DE MARIA BERGANZA GARZA, ha aprobado su Examen Privado de Tesis, se le autoriza la impresión del Trabajo de Tesis, denominado: "AUDITORIA DE INFORMÁTICA EN UN BANCO PRIVADO GUATEMALTECO".

Atentamente,

"D Y ENSEÑAD A TODOS"



LIC. EDUARDO ANTONIO VELÁSQUEZ CARRERA
SECRETARIO



LIC. MIGUEL ÁNGEL LIRA TRUJILLO
DECANO

Smp.

27.



ACTO QUE DEDICO

A:

DIOS

Por permitirme culminar mi carrera.

MIS PADRES

Por el apoyo y el buen ejemplo.

MIS HERMANAS

Por el cariño y colaboración.

TODA MI FAMILIA Y AMIGOS

Con aprecio sincero.

USTED

Muy especialmente.

INDICE

<u>CONTENIDO</u>	<u>PAGINA No.</u>
INTRODUCCION	
CAPITULO I	
SISTEMA BANCARIO NACIONAL	
1.1 Legislación.	1
1.1.1 Ley de Bancos, Decreto 315 del Congreso de la República.	2
1.1.2 Ley Monetaria, Decreto 203 del Congreso de la República.	2
1.1.3 Ley Orgánica del Banco de Guatemala, Decreto 215 del Congreso de la República.	2
1.2 Clasificación de los Bancos.	3
1.2.1 Por el origen del capital.	3
1.2.1.1 Bancos Nacionales.	3
1.2.1.2 Bancos Extranjeros.	3
1.2.2 Por la conformación de Capital.	3
1.2.2.1 Bancos Estatales.	3
1.2.2.2 Bancos Privados.	4
1.2.2.3 Bancos Mixtos.	5
1.2.3 Por las operaciones que realizan.	5
1.2.3.1 Bancos Comerciales.	5
1.2.3.2 Bancos Hipotecarios.	5
1.2.3.3 Bancos de Capitalización.	6
1.2.3.4 Bancos Comerciales e Hipotecarios.	6
1.3 Operaciones que realizan.	6
1.3.1 Operaciones Activas.	6
1.3.2 Operaciones Pasivas.	8
1.3.3 Operaciones de Confianza.	9
CAPITULO II	
AUDITORIA INTERNA	
2.1 Naturaleza de la Auditoría Interna.	11
2.2 Estándares para la práctica profesional de la Auditoría Interna.	12
2.2.1 Independencia.	12
2.2.2 Formación técnica y capacidad profesional.	12
2.2.3 Alcance del trabajo.	13
2.2.4 Ejecución del trabajo de Auditoría.	14
2.2.5 Administración de Auditoría Interna.	14
2.3 Independencia.	15
2.3.1 Posición Organizacional.	15



2.3.2	Objetividad.	15
2.4	Administración de Auditoría Interna.	16
2.5	Normas Generales de Auditoría Interna.	17
2.6	Normas Específicas de Auditoría Interna.	20
2.6.1	Planeación y supervisión.	20
2.6.2	Procedimientos analíticos de revisión.	23
2.6.3	Estudio y evaluación del control interno.	24

CAPITULO III

AUDITORIA DE INFORMATICA

3.1	Terminología de la auditoría de informática.	31
3.1.1	Informática.	32
3.1.2	Auditoría.	38
3.1.3	Auditoría de Informática.	39
3.2	La auditoría de informática y su entorno.	41
3.3	Planeación.	43
3.3.1	Proceso de planeación.	43
3.3.2	Proceso de planeación en informática.	44
3.3.3	Proceso de planeación de la auditoría.	45
3.3.4	Proceso de planeación de la auditoría de informática.	47

CAPITULO IV

ASPECTOS QUE EL AUDITOR INTERNO DEBE EVALUAR Y RIESGOS ASOCIADOS DE LAS OPERACIONES.

4.1	Métodos utilizados por la entidad para procesar la información.	53
4.1.1	Sistema Manual.	53
4.1.2	Sistema Mecánico.	54
4.1.3	Sistema Electromecánico.	55
4.1.4	Sistema Computarizado.	55
4.2	Medida en que se utiliza el computador en cada aplicación dependiendo de la complejidad de las operaciones.	60
4.3	La estructura organizacional de las actividades de Procesamiento de Datos.	63
4.3.1	Organigrama.	63
4.3.2	Relaciones jerárquicas y funcionales entre órganos de la organización.	63
4.3.3	Flujos de información.	64
4.4	Riesgos a los que están expuestas las operaciones.	64
4.4.1	Los riesgos externos.	65
4.4.2	Los riesgos internos.	65
4.4.3	Identificación de Riesgos.	68
4.4.4	Evaluación de Riesgos.	69
4.5	Evaluación de Controles	72
4.5.1	Preventivo.	74

4.5.2	Detectivo.	75
4.5.3	Directivo.	75
4.5.4	Mitigantes o Compensatorios.	75
4.5.5	Generales.	75
4.5.6	En aplicaciones automatizadas.	81
CAPITULO V		
CASO PRACTICO		
5.1	Auditoría de Informática en el área de depósitos.	88
5.2	Plan de trabajo.	92
5.2.1	Conocimiento general.	95
5.2.2	Identificación de los riesgos.	98
5.2.3	Identificación de controles existentes.	98
5.2.4	Selección de riesgo crítico.	98
5.2.5	Evaluación y análisis de los controles en aplicaciones automatizadas en operaciones del área de depósitos.	101
5.2.5.1	Proceso de Entradas de Datos.	104
5.2.5.2	Procesos en Computador.	110
5.2.5.3	Proceso de Salida.	117
5.2.6	Informe de la auditoría.	123
CONCLUSIONES.		127
RECOMENDACIONES.		129
BIBLIOGRAFIA.		131

INTRODUCCION

El auditor debe contar con habilidades y conocimientos en el campo de la informática, ya que las operaciones de cualquier institución se están automatizando cada día, lo cual requiere contar con habilidades para asociar las transacciones a los procedimientos electrónicos, asimismo, se hace imprescindible que se mantenga informado de la evolución constante de la misma, ya que se ha extendido a todas las ramas de la sociedad, beneficiando en forma sorprendente el desarrollo de todas las actividades productivas y profesionales, en especial al Sector Bancario, convirtiéndose así, en una herramienta de uso indispensable y permanente en su diario accionar, derivado al alto volumen y a la complejidad de las operaciones que maneja, siendo a su vez, una ayuda para poder ofrecer a sus clientes, un servicio cada vez más rápido, confiable y eficiente.

En tal virtud, las instituciones bancarias deben de reconocer la necesidad de contar con un área independiente, que asegure y promueva el buen uso y aprovechamiento de la tecnología, como lo es la Auditoría Interna, de esta manera, al efectuar un diagnóstico desde el punto de vista de la función de informática, deberá de evaluar dicha función, para detectar las operaciones que están expuestas a mayores riesgos o debilidades, y planificar, a su vez, una auditoría de informática, considerando los controles y esquemas de seguridad requeridos para un óptimo aprovechamiento.

Como un apoyo que facilite el desarrollo de la función antes comentada, este trabajo de tesis se ha dividido en cinco capítulos, a efecto de que el tema sea interesante y de fácil comprensión. En ese contexto, el capítulo I trata del Sistema Bancario Nacional y su marco jurídico, el capítulo II, sobre los aspectos a considerar en una Auditoría Interna como: los estándares para la práctica profesional, normas generales y específicas de la auditoría; el capítulo III, enmarca lo



relacionado con la Terminología de la Auditoría de Informática y la planificación de la misma; para entrar al tema central el capítulo IV se refiere a los Aspectos que el Auditor Interno debe evaluar y los riesgos asociados de las operaciones; y para concluir el capítulo V, presenta un caso práctico acerca de una planificación de una Auditoría de Informática en el área de depósitos de un banco privado guatemalteco, en el cual se esquematiza lo analizado teóricamente en los capítulos precedentes

Por otra parte, no se pretende agotar el tema, sino más bien, hacer un aporte que proporcione los estándares mínimos para fortalecer el criterio del profesional, para planificar una auditoría de informática en una entidad bancaria; así como una fuente de consulta para los estudiantes de la Facultad de Ciencias Económicas, en virtud de carecer en la actualidad de información sobre el tema antes indicado.

CAPITULO I

SISTEMA BANCARIO NACIONAL

El sistema bancario está conformado por todos aquellos bancos que sirven de intermediarios financieros entre oferentes y demandantes de capital, y que contribuyen al desarrollo de la economía del país, realizan operaciones activas, pasivas y de confianza; las operaciones pasivas están constituidas por aquellas operaciones que implican la captación de recursos financieros en calidad de depósitos a la vista, depósitos de ahorros y depósitos a plazo, creando una obligación para la institución.

1.1 LEGISLACION

El sistema bancario guatemalteco está organizado bajo el sistema de Banca Central, y se basa en tres leyes fundamentales: Ley de Bancos, Ley Monetaria y la Ley Organica del Banco de Guatemala.

Según el artículo 133 de la Constitución Política de la República de Guatemala establece: La Junta Monetaria tendrá a su cargo la determinación de la política monetaria, cambiaria y crediticia del país y velará por la liquidez y solvencia del sistema bancario nacional, asegurando la estabilidad y el fortalecimiento del ahorro nacional.



1.1.1 LEY DE BANCOS, DECRETO 315 DEL CONGRESO DE LA REPUBLICA.

Del 5 de diciembre de 1946, reformado por los Decretos 1315, 23-95, 29-95, 26-99. Su objeto fundamental es dictar normas para las actividades de las instituciones de crédito, velando por la solvencia y liquidez de éstas, en resguardo de un sistema bancario sano, que coadyuve al crecimiento de la economía del país.

1.1.2 LEY MONETARIA, DECRETO 203 DEL CONGRESO DE LA REPUBLICA.

Del 10 de diciembre de 1945, reformando por los Decretos 1316, 22-72 y 1673, todos del Congreso de la República. Esta ley regula todo lo relativo a la moneda del país, como: su uso, emisión, circulación, especies, canje, desmonetización, paridad, etc.

1.1.3 LEY ORGANICA DEL BANCO DE GUATEMALA, DECRETO 215 DEL CONGRESO DE LA REPUBLICA.

Del 12 de febrero de 1947, reformado por los Decreto 331, 1315, 1704, 62-70, 12-95, 29-95 y 61-95, todos del Congreso de la República. Esta Ley creó un banco de Estado, descentralizado, con el nombre de "Banco de Guatemala", que administra el funcionamiento del sistema bancario nacional actuando como Banco Central, cuyo objeto principal es el de promover creación y el mantenimiento de las

condiciones monetarias, cambiarias y crediticias más favorables al desarrollo ordenado de la economía nacional.

1.2 CLASIFICACION DE LOS BANCOS.

De conformidad con el primer párrafo del artículo 1º. De la Ley de Bancos, Decreto 315 del Congreso de la República:

"Únicamente las entidades debidamente autorizadas podrán legalmente efectuar, dentro del territorio de la República, negocios que consistan en el préstamo de fondos obtenidos del público mediante el recibo de depósitos o la venta de bonos, títulos u obligaciones de cualquier otra naturaleza, y serán considerados para los efectos legales como instituciones bancarias".

Los bancos pueden clasificarse:

1.2.1 POR EL ORIGEN DEL CAPITAL

1.2.1.1 Banco Nacionales:

Son instituciones constituidas conforme a la legislación interna del país, en su mayoría están formadas como sociedades anónimas.

1.2.1.2 Bancos Extranjeros:

Son bancos organizados en otros países, que funcionan en Guatemala en forma de sucursales, legalmente autorizadas.

1.2.2 POR LA CONFORMACION DEL CAPITAL

1.2.2.1 Bancos Estatales:



Son las entidades cuyo capital es aportado exclusivamente por el Estado, constituidas mediante leyes específicas.

En Guatemala están establecidos los siguientes:

- Banco de Guatemala, Decreto Legislativo No. 215
- Crédito Hipotecario Nacional, Decreto Ley 25-79

1.2.2.2 Bancos Privados:

Son instituciones constituidas en forma de sociedades anónimas, cuyo capital es aportando por la iniciativa privada. Actualmente, están autorizados los siguientes:

Banco de Occidente, S. A.	Banco Industrial, S. A.
Banco Agrícola Mercantil, S.	Banco Internacional, S. A.
Banco del Agro, S. A.	Banco Metropolitano, S. A.
Banco Inmobiliario, S. A.	Banco del Café, S. A.
Banco Granai & Townson, S. A.	Banco de la Construcción, S. A.
Banco de Desarrollo Rural, S. A.	Banco de la República, S. A.
Banco del Quetzal, S. A.	Banco SCI, S. A.
Banco de Exportación, S. A.	Banco Americano, S. A.
Banco Uno, S. A.	Banco Privado para el Desarrollo, S. A.
Banco Promotor, S. A.	Banco de Antigua, S. A.
Banco Continental, S. A.	Banco de América Central, S. A.
Banco Reformador, S. A.	Banco Empresarial, S. A.
Banco Corporativo, S. A.	

Banco de Nor-oriente, S. A.	Lloyds Bank PLC, Sucursal
Banco de Comercio, S. A.	Guatemala.
Banco Vivibanco, S. A.	Citibank N. A, Sucursal
Banco Cuscatlán, S. A.	Guatemala.

1.2.2.3 Bancos Mixtos:

Son los bancos cuya participación en el capital es combinada entre el Estado y particulares. En nuestro medio figuran:

- Banco de los Trabajadores, Decreto Ley No. 383, en el cual participan, además del Estado, los trabajadores del país.
- Banco del Ejército, S.A., Decreto Ley 40-71, en el cual participa el IPM y el sector privado del país.

1.2.3 POR LAS OPERACIONES QUE REALIZAN

De conformidad con el artículo 34 del Decreto No. 315, Ley de Bancos, por las operaciones que realizan, se clasifican así:

1.2.3.1 Bancos Comerciales:

Constituyen las instituciones de crédito que reciben depósitos monetarios y depósitos a plazo menor, con objeto de invertir su producto, principalmente en operaciones activas de corto término.

1.2.3.2 Bancos Hipotecarios:

Son las instituciones de crédito que emiten bonos hipotecarios o prendarios, y reciben depósitos de ahorro y de plazo mayor, con objeto de



invertir su producto, principalmente, en operaciones activas de mediano y largo término.

1.2.3.3 Bancos de Capitalización:

Son instituciones de crédito que emiten títulos de capitalización y reciben primas de ahorro con objeto de invertir su producto en distintas operaciones activas, de plazos consistentes con los de las obligaciones que contraigan. En el país no existe este tipo de banca.

1.2.3.4 Bancos Comerciales e Hipotecarios:

Son todos los bancos habilitados a la vez como comerciales e hipotecarios pero se rigen como los bancos de categoría única. A excepción de Vivibanco y el Banco de Guatemala todos los bancos funcionan como bancos comerciales e hipotecarios.

1.3 OPERACIONES QUE REALIZAN

Según la Junta Monetaria en resolución JM-752-93 autorizó y definió las operaciones que pueden realizar las instituciones bancarias, así:

1.3.1 OPERACIONES ACTIVAS

Son las que realizan las instituciones intermediarias financieras, con el propósito de canalizar recursos financieros y otro tipo de bienes, o aquellas mediante las cuales asumen obligaciones por cuenta de terceros, independientemente de su forma jurídica de formalización e instrumentación o de su registro contable; es decir, son aquellas

operaciones que representan un derecho a ejercer por parte del banco contra terceros.

Entre las operaciones activas más comunes que realizan las instituciones bancarias figuran:

Préstamos: Representan los créditos concedidos por los bancos y pueden ser fiduciarios, prendarios, hipotecarios. Los préstamos están formalizados en pagarés o bien en escrituras públicas. Pueden estar garantizados en forma mixta; es decir, prendarios-fiduciarios, hipotecarios-prendarios, pueden ser también con bonos de prenda.

Descuentos: "Consiste en la entrega de una suma de dinero por parte del banco a su cliente, mediante la transferencia como contraprestación de un crédito no vencido a cargo de tercero. El monto de la entrega realizada por el banco está determinado por el valor del crédito transferido menos el interés equivalente al plazo pendiente entre la fecha del descuento y la del vencimiento del título". 10:361

Reporto: "Es un contrato por medio del cual el reportador, ordinariamente el banco, adquiere de un tercero (reportado) títulos valores mediante el pago de un precio con la obligación de transferirle los mismos u otros de idéntica especie, contra el reconocimiento de un precio aumentado o del mismo precio, más una prima, comisión o interés". 10:



Inversiones en Valores: Están constituidas por los títulos valores emitidos por entidades públicas y privadas que tienen un rendimiento garantizado y son negociables en el mercado financiero.

Créditos Documentarios: "Se entiende por crédito documentario el acuerdo mediante el cual, a petición y de conformidad con las instrucciones del cliente, el banco se compromete directamente o por intermedio de un banco corresponsal a pagar a un beneficiario hasta una suma determinada de dinero, o a pagar, aceptar o negociar letra del cambio giradas por el beneficiario, contra la presentación de los documentos estipulados y de conformidad con los términos y condiciones establecidos". 10:406

1.3.2 OPERACIONES PASIVAS:

Son aquellas operaciones que realizan las instituciones intermediarias financieras con el propósito de captar recursos financieros, sobre los cuales dichas instituciones ofrecen, explícita o implícitamente, cualquier tipo de seguridad o garantía, ya sea en cuanto a recuperabilidad, mantenimiento de valor, rendimiento, liquidez y otros compromisos que impliquen la restitución de fondos, independientemente de su forma jurídica de formalización e instrumentación o de su registro contable; es decir, nace una obligación para el banco a la vista o a plazo.

Entre las operaciones pasivas más comunes realizadas en las instituciones bancarias están:

Depósitos: Las operaciones de depósitos representan las obligaciones de la institución, siendo los medios de captación de recursos financieros en los diferentes tipos de depósitos: a la vista, ahorro y a plazo fijo.

Emisión de obligaciones y otros títulos: A través de la emisión de los títulos, es posible para las entidades bancarias movilizar parte de los créditos que integran parcialmente su activo. Es decir, que el título es un instrumento de captación de recursos sustentado de previas operaciones crediticias. En esta forma se integra un ciclo dinámico en donde la concesión de crédito sirve de base a la emisión de títulos que, al ser colocados en el mercado, permiten recuperar los recursos previamente comprometidos, garantizando nuevas captaciones con los mismos créditos que las originaron.

Reporto (como reportado): Es el contrato por el cual el reportado (demandante de dinero) transfiere en propiedad al reportador (inversionista) títulos-valores de una especie, por un determinado precio y este último asume la obligación al reportado al vencimiento del término establecido la propiedad de otros tantos títulos de la misma especie, contra reembolso de un precio que puede ser aumentado o disminuido en la medida convenida.

1.3.3 OPERACIONES DE CONFIANZA:

Son las que realizan las instituciones intermediarias financieras actuando como mandatarias o depositarias, con el propósito de prestar

servicios que no implican intermediación financiera ni compromisos financieros para las mismas. En otro sentido, son operaciones que ni dan origen a un derecho ni crean una obligación para los bancos, más bien se originan por cambio traslación de valores. Se distinguen porque en ellas no existe una intermediación crediticia, sino una mediación por parte del banco en los cobros, en los pagos, en el desempeño de ciertos servicios por cuenta de sus clientes o, en ellas, los bancos se limitan a recibir bienes en simple custodia o administración.

Entre estas operaciones tenemos:

Operaciones de cambio: Se refiere a las operaciones de compra-venta de moneda extranjera.

Cobros por cuenta ajena: Son operaciones de servicio que prestan las instituciones bancarias, tales como cobro de: energía eléctrica, agua, teléfono, tarjeta de crédito, etc.

Operaciones de fideicomiso: Es un contrato mediante el cual se transfieren los bienes en propiedad al fiduciario con cargo para este último de devolvérselos al fideicomiso o transferirlos a un tercero después de cierto tiempo.

CAPITULO II

AUDITORIA INTERNA

2.1 NATURALEZA DE LA AUDITORIA INTERNA

"La función principal de auditoría interna es dar un servicio a la entidad o corporación a la que pertenece, que logre un nivel aceptable de satisfacción en los usuarios del servicio o departamentos que cubre su función. Para el efecto es importante tener presente que el más importante usuario del servicio de auditoría interna son los Accionistas y en segundo lugar la Gerencia". 9:1

La auditoría interna mide y valoriza en forma posterior los controles que lleva a cabo la administración en forma previa o concurrente a la ejecución de las operaciones.

La auditoría interna ayuda a la administración a alcanzar sus metas y objetivos con mayor eficiencia, al proporcionarle, en forma oportuna, información, análisis, evaluaciones, comentarios y recomendaciones pertinentes sobre las operaciones que examina.

Más adelante se mencionan los estándares para la práctica profesional de auditoría interna, los cuales se consideran de suma importancia para que la función de auditoría interna alcance su cometido, siendo los siguientes:

- Independencia.
- Formación Técnica y Capacidad Profesional.

- Alcance del Trabajo.
- Ejecución del Trabajo de Auditoría.
- Administración del Departamento de Auditoría.

2.2 ESTANDARES PARA LA PRACTICA PROFESIONAL DE LA AUDITORIA INTERNA.

2.2.1 INDEPENDENCIA

Supone una actitud mental que permite al auditor interno actuar con libertad respecto a su juicio profesional, para lo cual debe encontrarse libre de cualquier predisposición que limite su imparcialidad. Los auditores internos deben ser independientes de las actividades que ellos auditan.

Es fundamental que el auditor interno posea autoridad funcional, (es decir actuar objetivamente y rendir sus juicios en forma imparcial y libre de prejuicios) para poder convencer a los usuarios del servicio de las razones de reportar deficiencias y de la intención que tiene la auditoría interna y la administración de apoyar y mejorar las debilidades de control, lo cual es beneficioso para la organización y para el departamento auditado.

2.2.2 FORMACION TECNICA Y CAPACIDAD PROFESIONAL

Las capacidades fundamentales que deben poseer los auditores internos son:

- Personalidad.
- Buenas relaciones interpersonales.
- Conocimientos básicos de la profesión.

- Experiencia en desarrollo e implantación de controles.
- Actitud positiva ante el trabajo.
- Creatividad.

El auditor interno a de llevar a cabo una actualización permanente de sus conocimientos. Hay que tener en cuenta que el entorno (económico y jurídico) en que se desenvuelve es cambiante, como son cambiantes las técnicas de información utilizadas por la misma.

Como parte del desarrollo personal y profesional, es necesario que la auditoría interna cuente con un instructivo para hacer evaluaciones periódicas del desempeño, con el fin de sugerir mejoras a los integrantes del equipo de auditoría y dar la capacitación que sea necesaria para desarrollar al personal que pueda dar un servicio de alta calidad.

2.2.3 ALCANCE DEL TRABAJO

Algo fundamental para definir un adecuado alcance de la auditoría interna es la preparación de un plan estratégico y detallado del trabajo a realizar.

El plan estratégico comprende el enfoque del trabajo y el análisis de las áreas de riesgo del negocio, así como la definición de los procedimientos de auditoría que se pueden seguir para cubrir dichos riesgos.

Además del plan estratégico debe existir metodología del trabajo, para que exista una estandarización de los procedimientos a efectuar.

El alcance de la auditoría interna deberá incluir el examen y evaluación de la propiedad y efectividad del sistema de control interno del banco y la calidad del cumplimiento en la ejecución de las responsabilidades asignadas.

El propósito de la revisión del sistema de control interno es asegurarse de que dicho sistema permite razonable seguridad de que los fines y objetivos de la organización se lleguen a cumplir en forma eficiente y económicamente.

2.2.4 EJECUCION DEL TRABAJO DE AUDITORIA

La ejecución del trabajo de auditoría interna debe comprender una mayor inversión de tiempo en planeación y análisis de las situaciones a evaluar para poder hacer trabajos bien hechos que puedan ser útiles a la administración para la toma de decisiones.

Para el alcance del trabajo de auditoría interna es necesario que los auditores tengan en mente el producto final del trabajo que es el informe, el cual debe ser trabajado desde el plan de auditoría, pasando por las pruebas a realizar y finalizando en la elaboración del informe de auditoría, el cual debe ser un documento que pueda ser leído sin dificultad.

2.2.5 ADMINISTRACION DE AUDITORIA INTERNA.

La administración de auditoría interna debe estar en una persona conocedora del negocio y que tenga un contacto con los Accionistas o Alta Dirección del negocio.

De la buena administración de auditoría interna dependen los resultados, obteniendo un buen ejemplo del jefe de la unidad y teniendo una estructura organizativa adecuada, que propicie el desarrollo.

2.3 INDEPENDENCIA.

2.3.1 POSICION ORGANIZACIONAL

En nuestro medio es común escuchar que auditoría interna depende del Gerente Financiero o del Contralor de la Corporación; sin embargo, no precisamente es ésta la mejor práctica.

La posición organizacional a nivel de Staff, dependiendo directamente del Consejo de Administración o de un Comité de Auditoría integrado por accionistas, es importante, puesto que de ello depende la libertad de acceso que tengan los auditores internos a la información y la cobertura de su trabajo, así como el nivel en que comunicarán sus hallazgos.

2.3.2 OBJETIVIDAD.

La objetividad de la auditoría interna es algo que puede mejorarse con una adecuada posición organizacional y, en segundo lugar, con una actitud libre de preferencias hacia alguna persona, departamento o sector de la organización, para lo cual no deben haber intereses de por medio que puedan afectar la objetividad.

2.4 ADMINISTRACION DE AUDITORIA INTERNA.

El auditor interno deberá administrar apropiadamente, él es responsable de la adecuada conducción, de modo:

- "Que auditoría interna cumpla con los propósitos generales y las responsabilidades aprobadas por la administración y aceptadas por el consejo de administración.
- Que los recursos asignados se utilicen en forma eficiente y efectiva.
- Que el trabajo efectuado cumpla con estándares para la práctica profesional de la auditoría interna ". 3:1

Asimismo la administración y organización de auditoría interna está afectada por los siguientes factores:

- La posición dentro de la estructura organizacional.
- La calidad de su personal (solvencia moral, intelectual y económica).
- La reputación en la organización.

La función administrativa y de organización de auditoría interna debe considerar que debe reunir características de imparcialidad, espíritu de servicio a la organización y capacidad en materia de control más que cualquier otra dependencia.

El nivel de crecimiento y credibilidad en auditoría interna hace que las responsabilidades asignadas se diversifiquen a tal grado que las funciones sólo pueden efectuarse a través de una unidad debidamente organizada y administrada.

La auditoría interna se desarrolla en función a normas, políticas, técnicas y procedimientos, definidas por institutos establecidos a nivel nacional e internacional; por lo tanto, a continuación se desarrollan:

- Normas Generales de Auditoría Interna
- Normas Específicas de Auditoría Interna.

2.5 NORMAS GENERALES DE AUDITORIA INTERNA.

Las normas generales se relacionan con el carácter y conducta del auditor, y la calidad de su trabajo. Se refieren a normas personales que se aplican a todo las fases del trabajo de campo del auditor, así como de la información.

La primera norma general de auditoría indica lo siguiente: El examen deberá ser realizado por una persona o personas que tenga o tengan entrenamiento y destreza técnicos como auditores.

El Contador Público y Auditor es un técnico en la materia contable y en Auditoría, lo que ello conlleva a que posea una preparación constante, ya que además de la instrucción académica adquirida durante su formación académica, debe estar al día en todos los conceptos relacionados con su campo, a efecto de poder sostener su calidad profesional.

Esta capacidad del auditor no sólo se determina por su educación y experiencia profesional, sino también por el cuidado, habilidad y eficiencia al realizar su trabajo. Por lo tanto, esta norma se refiere a:



- La educación necesaria para poder ingresar a la profesión.
- Experiencia y entrenamiento profesional en auditoría.
- Una educación profesional continua.

Asimismo, el profesional de la Contaduría Pública deberá ser diligente en la ejecución del trabajo y en la elaboración del informe, lo cual implica que debe estar atento siempre a su trabajo, ya que la disciplina y los procedimientos de contabilidad no siguen un patrón estrictamente rígido y, en consecuencia, los riesgos de cada trabajo deben evaluarse y ponderarse atinadamente.

Por otra parte, a de basarse en hechos objetivos para emitir una opinión sobre la información examinada, considerando que debe existir independencia no sólo de hecho sino también en apariencia.

La segunda norma se refiere: básicamente a que el Contador Público y Auditor debe considerar los suficientes elementos de juicio que evidencian en sus papeles de trabajo todas las situaciones encontradas en el examen realizado.

El auditor debe obtener el conocimiento suficiente de la estructura de control interno, para planificar la auditoría y determinar la naturaleza, oportunidad y alcance de la auditoría.

También en una auditoría debe hacerse una oportuna planeación del trabajo y ejercer una adecuada supervisión.

La tercera norma se refiere a: La elaboración del informe (reporte) de auditoría interna, el cual debe comprender como mínimo los siguientes aspectos:

Fecha del informe.

El informe deberá ser fechado, preferiblemente, con el momento de su entrega.

A quien va dirigido.

Como práctica adecuada debe ser dirigido al funcionario responsable directo de la actividad que estuvo sujeta a revisión.

Párrafo de introducción (alcance)

Se establece la naturaleza y alcance de la asignación de auditoría, el periodo cubierto u otro punto de referencia en fecha, el tiempo dedicado al trabajo de campo y el personal asignado en la auditoría.

Párrafo de Antecedentes

Se describe la naturaleza general de la actividad operacional cubierta en la revisión, tipo orientador para el lector del informe, y no es necesario que sea completo.

Resumen de aspectos principales

Incluir una relación de todos los aspectos principales, lo cual proporciona al lector un rápido informe acerca de la naturaleza y alcance del contenido del informe, sin entrar a un análisis detallado del mismo.

Presentación de aspectos individuales

El cuerpo del informe puede estar integrado por una serie de secciones que tratan individualmente situaciones especiales.

Párrafo final y firma

Debe haber una frase de "Respetuosamente", "Atentamente", etc, la firma y nombre del auditor que preparó el informe.

Distribución

La lista de distribución provee información acerca de los ejecutivos específicos que recibirán una copia del informe de auditoría.

Seguimiento

Deben programarse auditorías de seguimiento para cada informe emitido por auditoría interna con objeto de establecer las medidas correctivas adoptadas en relación con las observaciones y recomendaciones emitidas.

2.6 NORMAS ESPECIFICAS DE AUDITORIA INTERNA.

2.6.1 PLANEACION Y SUPERVISION

El auditor debe considerar, en la planeación de la auditoría, los métodos que la entidad usa para procesar información contable, porque tales métodos influyen en el diseño del sistema contable y en la naturaleza de los procedimientos del control interno contable. Por lo tanto, dichos métodos pueden también influir en la naturaleza oportunidad y extensión de los procedimientos de auditoría.

Por consiguiente, en el examen de estados financieros de una entidad, el auditor debe evaluar el efecto del procesamiento por computador, considerando lo siguiente:

- a. El grado en que se usa el computador en cada aplicación contable significativa. Entendiéndose por aplicaciones contables significativas las que incluyen movimientos o saldos que puedan afectar materialmente la información de los estados financieros que el auditor interno está examinando.
- b. La complejidad de las operaciones por computador de la entidad, incluyendo el uso de un centro de servicio externo, de conformidad con el SAS 44, Reportes de propósitos especiales en el Control Interno Contable de Organizaciones de Servicio, y la Guía de Auditoría del Instituto Americano de Contadores Certificados denominada "Auditorías de Registros Producidos por Centro de Servicio"
- c. La estructura organizacional de las actividades de procesamiento por computador.
- d. La disponibilidad de los datos. Los documentos fuente, ciertos archivos y otra evidencia, que pueden ser necesitados por el auditor, pueden existir solamente por un período corto o solamente en forma legible al computador.



En algunos sistemas por computador, los documentos de entrada pueden no existir, sobre todo porque la información es ingresada directamente al sistema.

La política de retención de datos de la entidad puede requerir que el auditor:

- Solicite la retención de alguna información para su revisión, o ejecute procedimientos de auditoría al mismo tiempo que la información esté disponible.
 - Además, cierta información generada por el computador para propósitos internos de la administración puede ser útil en la ejecución de pruebas sustantivas, particularmente en procedimientos analíticos de revisión que se describen en el SAS 23 y la Guía correspondiente.
- e. El uso de técnicas de auditoría con apoyo del computador puede incrementar la eficiencia en la ejecución de los procedimientos de auditoría y proporcionar la oportunidad para aplicar ciertos procedimientos a una población completa de cuentas o transacciones.

Además, en algunos sistemas contables, puede ser difícil o imposible para el auditor analizar ciertos datos o probar procedimientos de control específicos sin la ayuda del computador.

Previamente, el auditor debe considerar si necesita entrenamiento especializado para:

- Evaluar el efecto del procesamiento por computador sobre la auditoría.
- Entender el flujo de transacciones.
- Entender la naturaleza de los procedimientos de control interno contable.
- Diseñar y ejecutar los procedimientos de auditoría.

Si necesita entrenamiento especializado, el auditor interno debe buscar la asistencia de un profesional que posea tal entrenamiento, quien puede ser parte del personal del auditor o profesional externo.

Si se planea el uso de los servicios de un profesional, el auditor debe tener suficiente conocimiento relativo al computador para:

- Comunicar los objetivos del trabajo de otro profesional.
- Evaluar si los procedimientos especificados satisfacen los objetivos del auditor; y
- Para evaluar los resultados de los procedimientos aplicados cuando se relacionen con la naturaleza, oportunidad y extensión de otros procedimientos de auditoría planeados.

2.6.2 PROCEDIMIENTOS ANALITICOS DE REVISION.

Los sistemas por computador han incrementado la disponibilidad de datos preparados para uso de la administración por la capacidad

(inexistente en los sistemas manuales) para almacenar, recuperar y analizar datos.

Estos datos y análisis, aunque no parten necesariamente de los registros contables básicos, puede ser valiosa fuente de información para el auditor en la aplicación de procedimientos analíticos de revisión, pruebas sustantivas o de cumplimiento.

2.6.3 ESTUDIO Y EVALUACION DEL CONTROL INTERNO.

Los métodos que una entidad usa para procesar aplicaciones contables significativas, pueden influir en los procedimientos de control diseñados para lograr los objetivos de control interno contable. Aquellas características que distinguen el procesamiento por computador del procesamiento manual incluyen:

- a. **Pistas de las transacciones:** Las pistas de las transacciones son una cadena de evidencia proporcionada a través de códigos, referencias cruzadas y documentación relacionada a saldos de cuentas y otros resultados, resumidos con las transacciones y cálculos originales. Algunos sistemas por computador están diseñados de tal manera que una pista de la transacción completa, que es útil para propósitos de auditoría, podría existir sólo por un período corto de tiempo o sólo en forma legible al computador.
- b. **Procedimiento uniforme de las transacciones:** El procesamiento por computador trata uniformemente las

transacciones bajo las mismas condiciones. Por lo que, virtualmente elimina la ocurrencia de errores de oficina asociados con el procesamiento manual. Por lo contrario, los errores de programas y equipo de computación (software y hardware) resultarán en todas las transacciones cuando son procesadas bajo las mismas condiciones.

- c. **Concentración de funciones:** Muchos procedimientos de control interno contable (ejecutados en sistemas manuales por individuos separados), pueden ser concentrados en una persona en sistemas por computador. Por lo tanto, un individuo que tiene acceso al computador puede estar en posición para ejecutar funciones incompatibles. Consecuentemente, otros procedimientos de control pueden ser ordinariamente cumplidos por la separación de funciones en sistemas manuales. Otros controles pueden incluir adecuada separación de funciones incompatibles entre las actividades de procesamiento por computador, por ejemplo:
- Estableciendo un grupo de control para prevenir o detectar errores o irregularidades en el procesamiento, o
 - Uso de password para prevenir que funciones incompatibles sean ejecutados por individuos que tienen acceso a los activos y a los registros a través de una terminal en línea.

Estos serán efectivos, por supuesto en la medida que la administración vele porque se cumplan.

- d. **Posibilidad de errores e irregularidades:** La posibilidad que individuos (incluso los que ejecutan procedimientos de control) obtengan acceso no autorizado a los datos o alteren los datos sin dejar evidencia y además tengan acceso directo o indirecto a los activos, puede ser más grande en los sistemas contables computarizados que en los sistemas manuales. La disminución de la participación humana en el manejo de las transacciones por computador pueden reducir el potencial para observar errores o irregularidades. Los errores e irregularidades que ocurren en el diseño o cambio de programas de aplicación, pueden permanecer ocultos durante largos períodos de tiempo.
- e. **Incremento del potencial para supervisión de la administración:** El sistema por computador ofrece a la administración una amplia variedad de herramientas analíticas que pueden ser usadas para revisar y supervisar las operaciones de la compañía. La disponibilidad de estos controles adicionales, favorecen al control interno contable del sistema completo, en el cual el auditor puede desear depositar su confianza.
- Por ejemplo, las comparaciones tradicionales de razones de operación con las presupuestadas, así como la conciliación de

cuentas, son frecuentemente disponibles para la revisión de la administración sobre una base más oportuna si tal información es computarizada. Adicionalmente, algunas aplicaciones programadas proporcionan estadísticas respecto a las operaciones del computador que pueden ser usadas para controlar el procesamiento actual de transacciones.

- f. **Autorización de las transacciones:** Ciertas transacciones pueden ser iniciadas o ciertos procedimientos requeridos para ejecutar una transacción automáticamente por un sistema por computador. La autorización de estas transacciones o procedimientos puede no estar documentada en la misma forma que en un sistema contable manual, inclusive, esta autorización puede estar implícita en la aceptación del diseño del sistema por computador. En el grado que el computador se usa para iniciar transacciones o ejecutar procedimientos, el programa de aplicación generalmente incluye procedimientos diseñados para asegurar que los pasos son ejecutados de conformidad con autorizaciones generales o específicas emitidas por la administración actuando dentro del alcance de su autoridad. Aquellos procedimientos podrían incluir revisiones para reconocer los datos que caen fuera de los límites predeterminados y pruebas para la razonabilidad general.

- g. **Dependencia de otros controles en los controles sobre el procesamiento por computador:** El procesamiento por computador puede producir reportes y otras salidas que se usan en la ejecución de procedimientos de control manual, pueden depender de la efectividad de los controles sobre la integridad y exactitud del procesamiento por computador.

Por ejemplo, la efectividad de un procesamiento de control que incluya una revisión manual de un listado de excepción producido por computador, depende de los controles sobre la producción del listado.

Cuando existe procesamiento por computador en aplicaciones contables significativas, los procedimientos de control interno contable, pueden clasificarse en: controles generales y de aplicación. Los controles generales son aquellos que se relacionan con todas o muchas actividades contables computarizadas y, frecuentemente, incluyen controles sobre el desarrollo, modificación y mantenimiento de programas de computador, y control sobre el uso de datos mantenidos en archivos, y cambios a los mismos por computador. Los controles de aplicación se refieren a aplicaciones, programados para verificar números de cuenta de clientes y límites de crédito.

Los procedimientos de control antes descritos, apoyan al objetivo del sistema de control interno contable de proporcionar razonable, pero no absoluta seguridad, que los activos están protegidos de uso o disposición no autorizada y que los registros financieros son confiables para permitir la preparación de estados financieros.

Funciones incompatibles para propósitos de control contable, son aquellas que colocan a cualquier persona en una posición para perpetrar y conciliar errores o irregularidades en el curso normal de sus obligaciones. Cualquiera que registre transacciones o tiene acceso a los activos ordinariamente está en posición de cometer errores o irregularidades. En consecuencia, el control contable necesariamente depende grandemente de la eliminación de oportunidades para conciliación.

Por ejemplo, cualquiera que registre desembolsos podría omitir el registro de un cheque, sea intencionalmente o no. Si la misma persona también concilia la cuenta bancaria, la falta de registro del cheque podría ser cubierta a través de una conciliación incorrecta. En un sistema contable usando un computador para imprimir cheques y registrar desembolsos, el computador puede también generar información usada para conciliar el saldo de la cuenta. Si la misma persona que ingresa la información en el computador para ejecutar el proceso de pago, también recibe la salida para el

proceso de conciliación, una falta similar podría ser conciliada. Estos ejemplos ilustran el concepto que procedimientos diseñados para detectar errores e irregularidades deben ser ejecutados por personas diferentes de quienes están en posición de perpetrarlos, o sea, que estos procedimientos deben ser ejecutados por personas que no tengan funciones incompatibles.

- Los procedimientos de control que realizan o contribuyen a la realización de uno o más objetivos de control específico son frecuentemente independientes. Algunos procedimientos de control pueden ser esenciales para la operación de otros procedimientos de control que satisfacen objetivos de control específicos (o sea que necesitan estar funcionando adecuadamente para el logro de aquellos objetivos de control específicos).

CAPITULO III

AUDITORIA DE INFORMATICA

3.1 TERMINOLOGIA DE LA AUDITORIA DE INFORMATICA

Al practicar una auditoría de informática es necesario contemplar los siguientes aspectos:

- Conocimiento general de los lenguajes de programación, operaciones del computador, hardware y software, análisis y diseño de sistemas.

- Interpretación de las actividades de la institución al vocabulario computarizado, tal que, solucione los procesos que se encuentran a lo largo de la auditoría de informática con deficiencias en los controles.

- Determinación de los riesgos y problemas a través de evaluaciones y exámenes oportunos en el proceso de la información en las áreas que contemplan mayor complejidad de operaciones, ante la deficiencia de controles.

Asimismo, es necesario que el auditor conozca y maneje adecuadamente, los términos técnicos usados en Informática que le servirán para desarrollar la auditoría; una vez familiarizado con el entorno en el cual va a desarrollar su trabajo, puede evaluar y examinar apropiadamente las operaciones, de tal manera que dicha evaluación se realice por excepciones, con la finalidad de mostrar únicamente las debilidades de control en las áreas de mayor riesgo.



3.1.1 INFORMATICA

La información debe dividirse en varios niveles a saber:

Nivel técnico: Considera los aspectos de eficiencia y capacidad de los canales de transmisión.

Nivel pragmático: Considera al receptor en un contexto dado.

Nivel normativo: Considera cuándo, dónde y a quién se destina la información o la difusión que a ella se le dé.

Considerando lo anterior, se define a la informática como: Una disciplina apoyada por métodos y procedimientos que clasifica y ordena datos dado un hecho, por medios mecánicos, manuales, electromecánicos o electrónicos, generando información confiable, verificable, y oportuna, presentada en algún medio como papel, pantalla, medios magnéticos, que deberá contener el significado de los datos y/o símbolos una vez procesados por cualquier medio, para ser transmitida por canales eficientes para la toma de decisiones.

En otras palabras la informática es el campo que se encarga del estudio y aplicación práctica de la tecnología, métodos, técnicas y herramientas relacionadas con las computadoras y el manejo de la información orientadas al buen uso y aprovechamiento de los recursos computacionales para asegurar que la información de las organizaciones fluya de manera oportuna, veraz y confiable; además, es el proceso metodológico que se desarrolla de manera permanente en las

organizaciones para el análisis, evaluación, selección, implantación y actualización de los recursos humanos (conocimiento, habilidades normas, etc.) y financieros (inversiones) encaminados al manejo de la información, buscando que no se pierdan los propósitos de calidad, confiabilidad, oportunidad, integridad y veracidad, entre otros propósitos.

En el campo de informática se manejan algunos términos propios del mismo como lo son:

Hardware: Se refiere a los componentes físicos y tangibles de las computadoras, generalmente clasificados en cuatro grandes ramas:

- Microcomputadoras o computadoras personales.
- Redes (locales, abiertas, etc.)
- Minicomputadoras.
- Supercomputadoras (mainframes)

Software: Implica la parte no física de las computadoras. Esto significa que es la porción intangible de los equipos de cómputo, es decir, programas con orientaciones específicas para la administración de la información y el uso eficiente de los recursos de cómputo.

Sistemas de Información: Son el conjunto de módulos computacionales o manuales organizados e interrelacionados de una manera formal para la administración y uso eficiente de todos los recursos (humanos, materiales, financieros, tecnológicos, etc.) de un área específica de la organización (manufactura, administración, dirección, etc.)

con la finalidad de representar los procesos reales de la misma, y orientar los procedimientos, políticas y funciones inherentes para el logro de las metas y objetivos del negocio.

A continuación se listan algunos conceptos con sus respectivas definiciones, con las que el auditor debe familiarizarse para llevar a cabo una auditoría de informática:

Programación: Es el arte de escribir uno o varios programas en código fuente sin importar el lenguaje que se utilice; es decir, Foxbase, Foxpro, RPG, COBOL. etc. Todo esto es con la finalidad de crear aplicaciones financieras, comerciales o industriales que soluciones problemas dentro de las empresas.

Estándares de programación: Se le conoce así a la forma que adopta para nombrar programas, bases de datos y objetos. Logrando de esta manera, tener un mejor control, sobre los mismos, para su fácil manipulación.

Análisis de sistemas: Es la descomposición de un sistema en sus elementos para fines de estudio; es decir, que es un método deductivo de estudio, que va de lo general a lo particular.

Lenguaje de máquina: Cuando se escribe un programa, se le conoce como código lo que entiende un programador, pero para que una máquina pueda ejecutarlo se debe convertir en lenguaje de máquina, esto

significa que se debe compilar un programa para que se convierta en un código que la máquina entiende, por lo general es código binario.

Programa fuente: Es el código que se escribe en un lenguaje que entiende los programadores, pero no lo puede entender la máquina.

Programación estructurada: Se le conoce así al estudio de programar, en donde se evita que un programa se vuelva incomprensible mediante crear sub-programas que son llamados desde un programa principal, logrando así que dicho programa sea muy pequeño pero con bastantes llamadas a otros programas que deben ser lo más independientes entre sí.

Programación modular: Se le conoce así a las rutinas que son necesarias ejecutar de modo idéntico en diferentes puntos, éstos se escriben una sola vez para poder hacer referencia a ellos desde cualquier programa.

Compilar: Es la acción que ejecuta un lenguaje de programación para convertir un programa fuente en lenguaje de máquina o código binario.

Configuraciones de redes: Es la acción de conectar computadoras entre sí, logrando la transferencia de información entre cada una de ellas.

Degradación: Se conoce como degradación a la acción que toma una máquina, cuando se le recarga de trabajo; es decir, sus recursos tales como memoria RAM, espacio en disco o procesador son insuficientes para realizar el trabajo deseado.

Equipos abiertos: Se dice de toda computadora que acepta se le conecte diferentes dispositivos de diferentes marcas o tecnologías.

Equipos cerrados: Se le conoce también como equipos propietarios; es decir, únicamente se le pueden conectar dispositivos de su misma marca y tecnología.

Campos: Este término se utiliza desde el punto de vista de archivo o bases de datos; es decir, dentro de la máquina la unidad más pequeña se le conoce como bit, luego se encuentra el byte que es un conjunto de bits, por lo tanto un byte representa un carácter (a, b, c, 1, 2, etc.) Análogamente un campo es un conjunto de bytes o caracteres. Dentro de una base de datos representa una columna, es decir puede contener un nombre, un valor, un número de cédula, etc.

Registro: Si continuamos con la relación de la definición de campo, se puede decir que un registro es un conjunto de campos, a nivel de base de datos se conoce como una fila de campos.

Base de datos: Es un conjunto de datos no redundantes que son clasificados y ordenados con un objetivo en común y que se convierten en una fuente de información para que las personas la utilicen como una herramienta de apoyo.

Archivos planos: Es un conjunto de archivos en los cuales se tienen almacenados todos los datos de un sistema de información, también son conocidos con el nombre de archivos tradicionales los cuales interactúan

directamente con un sistema operativo convencional como DOS. Tienen la característica que para poder obtener información de ellos se requiere de la creación de uno o varios programas de aplicación.

Llaves: Se le conoce así a campos con valores únicos que identifican a los registros de un archivo. Pueden utilizarse para relacionar bases de datos o para efectuar ordenamientos.

Un sistema de información realiza cuatro actividades básicas, las cuales están identificadas a continuación:

Entrada de información: Es el proceso mediante el cual el sistema toma los datos que requiere para procesar la información.

Proceso de información: Es la capacidad del sistema para efectuar cálculos de acuerdo con una secuencia preestablecida de operaciones.

Almacenamiento de información: Es una de las actividades o capacidades más importantes, ya que a través de esta propiedad el sistema puede recobrar la información guardada en un proceso anterior.

Salida de información: Es la capacidad del sistema para editar la información procesada o bien los datos de entrada al exterior.

Los sistemas de procesamiento de datos computarizados liberan del tedio y la rutina a las tareas que se realizan manualmente, brindando velocidad y exactitud; sin embargo, el elemento humano sigue participando al llevar a cabo la captura de la información requerida, por lo

que existe la probabilidad de riesgos, tales como usos indebidos de la información.

3.1.2 AUDITORIA.

"Es un proceso sistemático para obtener y evaluar evidencia de una manera objetiva respecto de las afirmaciones concernientes a actos económicos y eventos para determinar el grado de correspondencia entre estas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados". 12:22

Asimismo, se puede definir que la auditoría es una actividad profesional, que implica el ejercicio de técnicas y procedimientos especializados, aplicables al tipo de revisión que deberá efectuarse, con el objeto de evaluar y mejorar lo existente, detectar y corregir errores, y proponer alternativas de solución en un informe que sirva como base para la toma de decisiones como resultado del trabajo realizado.

Tipos de Auditorías

Por quien la realiza puede ser de dos formas:

Auditoría Externa y Auditoría Interna.

Por los objetivos que se persiguen, la auditoría puede ser:

Auditoría Financiera, Auditoría Operacional, Auditoría Administrativa, Auditoría Fiscal y Auditoría de Informática.

De los tipos de auditoría antes mencionados, podemos efectuar una revisión que cumpla con la prestación de un servicio de asistencia

constructiva a la administración, con el propósito de mejorar la conducción de las operaciones y sistemas para obtener un mayor beneficio para la institución.

Objetivos principales de la auditoría:

- Estudiar y actualizar permanente las áreas susceptibles de revisión.
- Apegarse a las tareas que desempeñen las normas, políticas, procedimientos y técnicas de auditoría establecidas por los organismos generalmente aceptados a nivel nacional e internacional.
- Evaluación y verificación de las áreas requeridas por la alta dirección.
- Elaboración del informe de auditoría (debilidades y recomendaciones).

3.1.3 AUDITORIA DE INFORMATICA

Es una actividad profesional especializada apoyada en técnicas y procedimientos para revisar, evaluar y supervisar cada uno de los procesos que generan información, desde su inicio hasta su término, así como también establecer y evaluar los controles de acuerdo a los objetivos y políticas de la empresa, considerando al mismo tiempo los aspectos funcionales y organizacionales de quienes desarrollan la actividad informática, sin perder de vista la evaluación técnica de los recursos, para que al finalizar su actividad, emita un informe sobre las carencias detectadas que se presentan a la Dirección para proceder a la toma de decisiones.



"Se define también como el conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente." 1:21

La auditoría de informática comprende:

- a. Un proceso formal ejecutado por especialistas del área de auditoría y de informática; se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de informática en la organización se lleven a cabo de una manera oportuna y eficiente.
- b. Las actividades ejecutadas por los profesionales del área de informática y de auditoría, encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa.
- c. El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que todos los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos, la certeza de que la información

que pasa por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.

- d. Un proceso metodológico, que tiene el propósito principal de evaluar todos los recursos (humanos, materiales, financieros, tecnológicos, etc.) relacionados con la función de informática, para garantizar a la empresa, que dicho conjunto, opera con un criterio de integración y desempeño de niveles altamente satisfactorios para que apoyen la productividad y rentabilidad.

3.2 LA AUDITORIA DE INFORMÁTICA Y SU ENTORNO

Dado que la auditoría de informática es un proceso básico de evaluación y control en el uso de los recursos tecnológicos para el logro de las estrategias, debe contemplar el entendimiento del entorno del negocio como parte de sus actividades primarias.

En ocasiones, la función de auditoría de informática se ve relacionada de modo directo o indirecto con las acciones definidas por la alta dirección, ya sea porque será la responsable de llevarlas a cabo, o porque dará seguimiento formal a su cumplimiento.

Es importante señalar que la mayoría de las organizaciones carecen de la función de auditoría y tampoco contratan auditores externos, lo que causa un alto porcentaje de las irregularidades u omisiones que se presentan en relación con las estrategias y políticas definidas por la alta dirección para la función de informática o áreas usuarias.

Existen funciones como planeación, auditoría, contraloría y auditoría de informática que verifican y aseguran el cumplimiento formal de las estrategias definidas por el negocio.

No contar con estas áreas de aseguramiento y verificación expone a las empresas a vivir en una constante incertidumbre, ya que los problemas o deficiencias pueden aparecer en cualquier momento.

Son las características del mercado en cada unas de las ramas o criterios relacionados con la tecnología de informática, que definen el rumbo de la misma en gran parte de los negocios.

La función de informática debe estructurar sus servicios y proyectos sobre la base de los requerimientos específicos del negocio, apoyándose en la tecnología de vanguardia que domina el mercado, así como en las tendencias de la misma. El grado de apoyo que se buscará en el medio tecnológico depende en gran medida de la orientación y justificación que se le asigne al enfocarlo a cada estrategia del negocio.

No todo lo que ofrece el mercado, como estándares y soluciones tecnológicas, garantiza el desempeño eficiente de la función de informática en una organización; el auditor en informática deberá verificar la existencia de un análisis costo/beneficio en cada proyecto de inversión orientado a la adquisición de nueva tecnología o estándares (normas) para el uso y manejo de la misma. Además, la auditoría de informática mantendrá un proceso de seguimiento de los recursos de tecnología,

metodologías, técnicas, procedimientos y políticas de informática que aseguren calidad y productividad en esta área.

El medio informático sufre cambios continuos en algunos de sus elementos, ya sea en hardware, software, telecomunicaciones, etc., debido a la búsqueda constante de soluciones más eficientes en aspectos relativos a desempeño y costos, entre otros. En consecuencia cualquier área que tenga como objetivo operar o evaluar que es el entendimiento y aprovechamiento para brindar a la organización resultados de alta calidad y la confianza de que la información seguirá cumpliendo los requisitos de control esperados: exactitud, totalidad, autorización, actualización, etc.

La finalidad del auditor es evaluar y dar seguimiento oportuno, al conjunto de proyectos de auditoría de informática, que serán ejecutados en un plazo determinado, con el fin de apoyar directa o indirectamente las estrategias del negocio, considerando los diversos factores internos y externos que se relacionan con la organización. Es conveniente señalar que, cada uno de estos proyectos, deberá estar enmarcado en los límites definidos para la función, esto es, debe enfocarse al control, seguridad y auditoría de los diferentes elementos que tengan contacto directo o indirecto con la tecnología de informática.

3.3 PLANEACION

3.3.1 PROCESO DE PLANEACION

La planeación es un proceso intelectualmente exigente, que requiere la determinación de los recursos de acción y la fundamentación

de las decisiones en los fines, conocimientos y estimaciones razonadas. La planeación significa, decir por adelantado, qué hacer, cómo y cuándo hacerlo y quién ha de hacerlo, además cubre la brecha que va desde dónde estamos hasta dónde queremos ir. La naturaleza esencial de la planeación puede ponerse de manifiesto mediante sus cuatro aspectos principales: contribución a los objetivos y propósitos, primacía de la planeación, extensión de ésta, y eficacia de los planes, siendo el propósito de cada plan, y de todos los derivados, el de facilitar el logro de los objetivos y propósitos de la empresa.

La función de planeación tiene cuatro importantes metas: reducir la incertidumbre y el cambio, dirigir la atención hacia los objetivos, propiciar una operación económica, y facilitar el control.

3.3.2 PROCESO DE PLANEACION EN INFORMATICA

De manera general una planeación consiste en una serie de actividades predeterminadas y estructuradas para el logro de metas específicas, por lo que en informática cabe mencionar que donde se observa mayor énfasis en lo relativo a planeación es en la fase de desarrollo de sistemas, la que conlleva la formulación de planes a largo plazo asegurando que el enfoque de los sistemas haya sido definido y sirva como guía para futuros diseños e implantaciones de sistemas, el cual debe considerar como elementos más importantes los siguientes:

- Las guías de orientación del proyecto se documentan en mayor detalle.
- Se preparan divisiones del trabajo para cada actividad y tarea de desarrollo.
- Se establecen fechas de inicio y de terminación para cada unidad de trabajo. Estos calendarios se basan en el nivel de experiencia y en las instalaciones asignadas al proyecto.
- Se revisan y aprueban los planes y calendarios y se obtienen compromisos formales respecto a su cumplimiento. En este punto, la documentación de la planeación de los proyectos se convierte en una medida contra la cual se vigilan y miden todas las actividades posteriores dentro de un proyecto de desarrollo de sistemas, a fin de que puedan reportarse las variaciones.

3.3.3 PROCESO DE PLANEACION DE LA AUDITORIA

En esencia consiste en definir un conjunto de proyectos de evaluación y verificación de políticas, controles y procedimientos inherentes a las áreas administrativas, financieras, operativas, etc., de la organización, con el objeto de asegurar el buen manejo y administración de los recursos de la organización.

Un punto de partida esencial en el proceso de una auditoría consiste en llegar a comprender perfectamente bien el negocio del cliente, lo cual requiere un esfuerzo para adquirir esos conocimientos.



El segundo paso en esta fase del proceso de auditoría consiste en diseñar programas detallados para los trabajos específicos, los cuales comprenden pruebas o los procedimientos de auditoría que se deberán realizar durante el examen.

Para poder planear adecuadamente un trabajo de auditoría, el auditor deberá considerar:

Planeación de la auditoría

- Obtener información acerca del negocio del cliente, industria y políticas contables.
- Preparar programas de auditoría.
- Programa de trabajo.
- Asignar personal profesional al trabajo a realizar.

Realización del trabajo de campo.

- Estudio y evaluación del Control interno
- Verificación de los saldos de las cuentas.
- Evaluar evidencia obtenida

Información acerca de los hallazgos.

- Determinar si son razonables las cifras de los estados financieros.
- Formarse una opinión, redactar y expedir el dictamen e informe de auditoría.

Es importante considerar que los negocios deben tener un conjunto de políticas emanadas de la alta dirección que manifiesten la necesidad de

contar con una función externa o interna de la organización que asegure la congruencia de todos los estados financieros y contables con las operaciones y transacciones que se realizan en la empresa.

Esta función ha de ser un área de control y aseguramiento; es decir, una entidad en la organización independiente y profesional, capacitada para ejercer las tareas de evaluación y seguimiento sobre todas las actividades u operaciones que afecten de manera directa o indirecta los estados financieros, contables y administrativos.

La función de auditoría se responsabiliza tanto de la planeación y ejecución de cada proyecto al cumplimiento formal y oportuno de las políticas, controles y procedimientos establecidos por la alta dirección, así como del seguimiento permanente de los mismos.

El período de elaboración o actualización del plan de auditoría depende de las prioridades o necesidades externas que tenga dicho proceso en cada organización.

3.3.4 PROCESO DE PLANEACION DE LA AUDITORIA DE INFORMATICA.

Consta de la definición y formalización de proyectos, abarca las actividades desarrolladas por el auditor de informática que tienen como objetivo principal elaborar y presentar un conjunto de proyectos inherentes a la función de auditoría de informática a la alta dirección, y que estarán orientados primordialmente al aseguramiento de la calidad y

control de los diferentes elementos que se encuentran relacionados de manera directa o indirecta con los recursos de informática.

La configuración de criterios para orientar las decisiones fundamentales y la identificación de las formas o maneras de llevar adelante las actividades necesarias para alcanzar los objetivos, hace necesario, como en cualquier actividad, preparar un plan de trabajo, el cual debe ser flexible, considerándose en el mismo un margen de tolerancia, en función de que las circunstancias son cambiantes.

El proceso de planeación depende en gran medida del diagnóstico previo que haga el auditor en informática de la situación que prevalece en cada una de las áreas de la función de informática. También debe considerar las necesidades o prioridades que tenga la alta dirección de auditar o evaluar un área específica.

El diagnóstico de la situación de informática previo a la planeación de ésta, deberá ser breve y muy objetivo; de ninguna manera debe descuidarse el objetivo principal de esta tarea, que es determinar las áreas de mayor riesgo de la función de informática con base en criterios económicos, grado de satisfacción, seguridad, calidad, tecnología, etcétera.

El auditor deberá utilizar todos los parámetros de medición y evaluación posibles, sin caer en un análisis detallado, para detectar la problemática principal de cada área. El auditor tendrá que basarse en su

experiencia y dominio de la auditoría en informática para efectuar un diagnóstico objetivo y contundente; además, se apoyará en la visión de los principales usuarios y del responsable de informática.

Tareas básicas del proceso de planeación de auditoría de informática.

En el proceso de planeación de una auditoría de informática se deben de considerar los siguientes puntos a saber:

1. Establecer objetivos

Los objetivos se definen como lo que se desea lograr, los mismos se establecerán de acuerdo a las necesidades de cada trabajo a desarrollar.

2. Conocimiento general del negocio.

El auditor de informática debe obtener una idea global del tipo de organización, los procesos básicos del negocio, así como las entidades externas al negocio que se relacionan con cada área del negocio.

3. Conocimiento de la función de informática

El auditor de informática debe conocer el nivel jerárquico de la función de informática. Asimismo, un aspecto clave que se tiene que considerar en la etapa preliminar es la evaluación general de los servicios que presta informática a las diferentes áreas la organización.

El auditor en informática ya puede formarse un juicio inicial de la congruencia entre las áreas usuarias y el responsable de informática; aquí



se detecta por lo general qué servicios ya son aceptados en la organización como estratégicos y cuáles sólo son operativos o necesarios para llevar a cabo tareas que no producen valor agregado.

El auditor en informática tiene responsabilidad moral de dar un sentido crítico y práctico a todas las áreas de la organización para encontrar un mejor modo de hacer las cosas desde el punto de vista profesional en el campo de informática y, de ser posible en las áreas del negocio involucradas en este tipo de proyectos.

4. Identificación de los riesgos.

Para identificar riesgos es necesario que se formulen entre otras las preguntas enunciadas en el punto 4.4.3 Identificación de Riesgos, del presente capítulo.

Para lo cual se deben de considerar las posibles situaciones que, de llegarse a cristalizar, pueden afectar la consecución de los objetivos previstos para la obtención de información.

5. Identificación de controles existentes.

En un proceso de evaluación de riesgos se deben de identificar los controles existentes, que minimicen los riesgos en caso de activarse alguno de éstos. Por lo tanto los controles deben de evaluarse y calificarse como adecuados o inadecuados.

6. Selección del área de riesgo crítico.

La selección del área de riesgo crítico se realiza con base en la que resulta con más riesgos altos en la matriz de análisis de riesgo.

7. Matriz de análisis de riesgo.

El objetivo principal de elaborar una matriz de riesgos es detectar las áreas de mayor riesgo en relación con la función de informática y que requieren una revisión formal y oportuna.

8. Recursos.

Esta fase es muy importante considerarla en un plan de trabajo, comprende la necesidad de la utilización de recursos humanos, físicos y financieros, sin los que no sería posible la realización del trabajo de auditoría.

9. Tiempo requerido.

En este punto debe determinarse la secuencia de las actividades que se van a realizar y el tiempo probable que consumirá su ejecución.

10. Técnicas y Métodos.

- ✓ Indagación.
- ✓ Observación.
- ✓ Cuestionarios.
- ✓ Programas de auditoría.
- ✓ Procedimientos de verificación.
- ✓ Determinación de deficiencias.

11. Informe de resultados.

La función del informe por parte del auditor se refiere exclusivamente a la expresión de su opinión acerca del resultado de la identificación de los riesgos a que están expuestas las operaciones analizadas y el grado o nivel en el que los controles existentes lo minimizan.

El informe deberá ser fechado, preferiblemente, en el momento de su entrega, se debe dirigir a la administración de la organización, se incluye un párrafo que indique el período que comprendió la auditoría, así como los objetivos, alcances, resultados, conclusiones y recomendaciones, como anexos de las observaciones y sugerencias resultantes de la evaluación y por último, el nombre y la firma del auditor de informática.

CAPITULO IV

ASPECTOS QUE EL AUDITOR INTERNO DEBE EVALUAR Y RIESGOS ASOCIADOS DE LAS OPERACIONES

El trabajo del auditor al realizar una auditoría de informática, debe en primera instancia contemplar un estudio inicial de la situación general, aunque la auditoría a realizar sea solamente a un área específica.

Para realizar dicho estudio han de examinarse las funciones, actividades, riesgos y controles, los cuales se desarrollan de manera general en los puntos siguientes:

- Métodos utilizados por la entidad para el procesamiento de datos.
- Medida en que se utiliza el computador en cada aplicación dependiendo de la complejidad de las operaciones.
- La estructura organizacional de las actividades de procesamiento de datos.
- Riesgos a los que están expuestas las operaciones.
- Evaluación de Controles.

4.1 METODOS UTILIZADOS POR LA ENTIDAD PARA PROCESAR LA INFORMACIÓN

Los métodos utilizados por las diferentes entidades para procesar la información pueden ser por medio de:

4.1.1 SISTEMA MANUAL

En este sistema todas las tareas se ejecutan en forma manual, usualmente con la ayuda de uno o más dispositivos mecánicos.



Los medios utilizados en este sistema son: la tinta y el papel para las anotaciones respectivas y para efectuar las operaciones aritméticas.

Este sistema, fue el primero que se utilizó para el registro de las operaciones de compra-venta y otras transacciones efectuadas por los comerciantes, por medio del cual se conocen los resultados favorables o desfavorables durante un período de tiempo determinado.

Actualmente este sistema es utilizado por comerciantes individuales, empresas pequeñas y en algunas empresas medianas debido al bajo costo que éste puede representar para ellos.

4.1.2 SISTEMA MECÁNICO

En un sistema mecánico se utilizan máquinas mecánicas para auxiliar la labor contable, esto ha dado lugar a la denominada mecanización del trabajo manuscrito, siendo esta mecanización variable según la empresa y el volumen de operaciones.

Cuando se utiliza el sistema mecánico se adoptan ciertas normas con el objeto de suprimir en lo posible todo trabajo manuscrito y los cálculos mentales, reemplazándolos por las escrituras mecanográficas y cálculo automático.

Con la mecanización no se anula la capacidad intelectual del individuo sino su racionalización. En todo trabajo hay una parte de cantidad y otra de calidad; la primera viene simplificada por la máquina, en tanto que la segunda queda sujeta al elemento humano que la maneja.

Para aplicar con éxito la mecanización es necesaria la formación especializada de la persona, para que esté en condiciones de dar el máximo rendimiento. Para ello hay que proceder a la selección del personal, colocándolo en aquellas labores más en consonancia con su forma de ser y su grado de formación profesional.

4.1.3 SISTEMA ELECTROMECAÁNICO

Este sistema consiste en utilizar máquinas eléctricas para el registro de las operaciones mercantiles que se realizan en una empresa.

Existen diferentes grados de mecanización, de los que se destacan tres:

- Mecanización de la labor de cálculo y formulación de comprobantes (máquinas de escribir, sumadoras y calculadoras)
- Mecanización de la labor de formulación de asientos y para auxiliares (máquinas de escribir plana, máquinas convencionales de contabilidad).
- Mecanización integral (programadas, ordenadores electrónicos).

4.1.4 SISTEMA COMPUTARIZADO

Este sistema es el basado en computadoras, que va desde usar la computadora para clasificar y resumir transacciones, hasta los sistemas que ejecutan todas las tareas de procesamiento mediante una o más computadoras y el equipo conexo.

El proceso electrónico asociado con las telecomunicaciones, es el de mayor desarrollo tecnológico, y proporciona ventajas competitivas a los negocios; en los últimos años ha evolucionado rápidamente, por lo que los empresarios están modificando continuamente sus procedimientos para obtener provecho de las crecientes capacidades de las computadoras y de las telecomunicaciones.

Ventajas del sistema computarizado

- Proporciona una gran velocidad en las operaciones.
- Proporciona seguridad y versatilidad, cualidades inalcanzables a través de los otros medios que existen actualmente.
- Incrementa ampliamente la capacidad de una empresa de procesar grandes cantidades de datos con eficiencia y economía.
- Proporciona una gran ayuda para generar información oportuna en la toma de decisiones.

El sistema acepta datos, los procesa según las instrucciones proporcionadas por los programadores y operadores, almacena e imprime o expone los resultados.

Las medidas de control interno que se pueden adoptar dentro de un sistema de procesamiento electrónico de datos son de gran variedad y dependerán del sistema en particular; sin embargo, se utilizarán aquellas que cumplan de manera óptima las funciones deseadas. Dentro de estas medidas de control interno están los controles administrativos, que

abarcaban la mayoría de las aplicaciones contables procesadas por un sistema electrónico de datos. Este medio de control incluye los siguientes procedimientos: protección contra interrupciones de energía eléctrica y contra magnetismo, controles de diseño y programación, procedimientos de depuración de los programas, control de cambios, protección de registros y archivos, etiquetas externas, retención de los documentos fuente, respaldo de archivo en cinta magnética o disquetes, reconstrucción de archivos.

Clasificación de los sistemas basados en computadora

- Proceso por lotes
- Proceso en línea
- Sistemas de procesamiento distribuido.

Proceso por lotes

Este consiste en que el proceso de las transacciones se lleva a cabo en grupos de ellas; es decir, que la actualización a los archivos maestros o principales, se da únicamente cuando todas las operaciones han sido previamente validadas y agrupadas.

El proceso en lotes puede realizarse fuera de línea (off line) o en línea (on line). La primera se refiere a que la captura se hace en un dispositivo que no está directamente conectado al computador, y la segunda es cuando el dispositivo está conectado directamente al



computador mediante elementos físicos y lógicos, los cuales pueden ser: cableado, líneas telefónicas, transmisiones vía radio, vía satélite, etc.

Proceso en línea

Permite que las transacciones se procesen de manera individual a medida que se van introduciendo al sistema, o bien en la modalidad por lotes.

Asimismo, el proceso en línea permite:

Consulta en tiempo real:

Es aquel en el que las respuestas a solicitudes de información de una terminal son inmediatas.

Actualización en tiempo real:

Es aquel que permite que los archivos maestros sean alterados mediante transacciones de entrada, de actualización de mantenimiento de archivos o de corrección de errores.

Procesamiento distribuido

Es una combinación de los dos anteriores, para la información se concentra en un procesador central (host del sistema), el cual a su vez cuenta con varios puestos de salida que comunican a otros computadores remotos, los cuales descargan de manera sustancial la tarea de procesamiento requerida por las aplicaciones.

Lo que se hace es distribuir la tarea entre varias computadoras efectuando un cargo de información desde el computador central y procesándolos en otro de la red.

Configuraciones del Centro de Procesamiento Electrónico de Datos.

Centralizado

Es aquel en el cual todas las tareas son administradas por un computador central y toda la información de los sistemas se concentra en él, información que se maneja por programas en medios magnéticos conectados al Host (computador central)

Se encarga, asimismo de atender las consultas, modificaciones o simplemente, la captura de los datos.

Descentralizado

Cada aplicación o grupo de ellos reside en dos o más computadores, no existiendo jerarquía entre ellos para la administración del sistema; es decir, que un computador puede estar atendiendo a un grupo de usuarios, mientras que otro, atiende a un distinto grupo de ellos.

La integración de los datos se realiza mediante procesos en lotes (batch), los cuales se ejecutan, por lo general, en horario inhábil, para evitar la sobrecarga de operaciones físicas de cableado o dispositivos para lograr este intercambio.

4.2 MEDIDA EN QUE SE UTILIZA EL COMPUTADOR EN CADA APLICACION DEPENDIENDO DE LA COMPLEJIDAD DE LAS OPERACIONES.

Entre algunas de las principales causas que pueden hacer que una empresa considere la conveniencia del uso del proceso electrónico de datos, están:

- Cuando la gerencia no logra obtener información adecuada;
- Dificultades en operaciones de trabajo manual;
- Necesidad de mejorar el servicio en ciertas áreas de operación
- Volúmenes de la información.
- Complejidad del procesamiento o de cálculos.

Lo anterior es en virtud de que, un porcentaje típico para los errores manuales es de aproximadamente el 5%, la automatización puede eliminar esta inconsistencia y, en efecto, es una de sus mayores ventajas.

Los factores inherentes al uso de las computadoras en las organizaciones son:

Velocidad: La velocidad de una computadora se relaciona íntimamente con la cantidad de datos que debe procesar. Además, se utilizan los términos volumen y frecuencia para describir la cantidad de datos manejados por una computadora. El volumen puede representar la cantidad total de datos que se han de procesar, y la frecuencia señala qué tan seguido se usa un dato específico en el procesamiento.

Precisión: La precisión es una consideración de primera importancia en el uso de las computadoras (cualquier dispositivo de cálculo que no sea confiable será inútil). La probabilidad de que la computadora cometa un error es bastante pequeña y en general puede decirse que su origen se debe a datos erróneos

Confiabilidad: A diferencia de la mayoría de los humanos, las computadoras pueden operar por grandes periodos de tiempo bajo las más adversas circunstancias, sin mostrar signos de fatiga. Cuando son usadas correctamente, pueden mejorar la eficiencia de una organización, proporcionan un medio rápido, preciso y confiable para procesar información.

Por otra parte, el papel del área de procesamiento de datos es muy simple, satisfacer al usuario. Conviene entonces que los usuarios entiendan del proceso de datos para poder definir y comunicar sus necesidades con claridad; sin embargo, en ocasiones no se logra por la actitud de los usuarios y los técnicos, debido a la brecha que existe de conocimientos del área de informática, por lo que los usuarios no logran entender la terminología utilizada por los técnicos.

El procesamiento de datos con computadora consiste en una metódica y bien planeada secuencia de actividades. Cada actividad va encaminada a proporcionar un dato que será empleado en la preparación del resultado final. Todo este proceso no es un agrupamiento al azar de



varias ideas, sino uno cuidadosamente planeado, en el cual la computadora juega un importante papel.

La computadora, a través de un programa, toma los datos en su estado original, sin procesamiento, y los convierte en información, directamente disponible para el usuario; este concepto es uno de los aspectos principales del procesamiento de datos. Puede almacenar grandes cantidades de datos y convertirlos en información de uso inmediato.

Cada aplicación de proceso de datos se compone de una serie de tareas bien definidas, por lo que de manera general se puede citar así:

- La captura de datos; representa la obtención de la información que ha de procesarse.
- La entrada; es la alimentación de datos a la computadora.
- Procesamiento; es el manejo de datos, e incluye la actualización de archivos de datos.
- Un archivo; es un conjunto organizado de registros.
- La salida; se define como la recuperación de la información de la computadora.
- Los controles; se aplican al procesamiento de datos para revisar la precisión de cualquier sistema.

4.3 LA ESTRUCTURA ORGANIZACIONAL DE LAS ACTIVIDADES DE PROCESAMIENTO DE DATOS.

Para el auditor, el conocimiento de quién ordena, quién diseña, quién ejecuta, quién autoriza y quién verifica es fundamental, ya que sin conocer con bastante aproximación la estructura de la informática sujeta a auditoría no podrá realizar su misión.

Por lo que al menos, deberá considerar los conceptos siguientes:

4.3.1 ORGANIGRAMA

El organigrama expresa inicialmente la estructura oficial de la organización a auditar, el cual debe estar con todo detalle, sin omitir las casillas que realicen funciones auxiliares o complementarias no informáticas.

4.3.2 RELACIONES JERÁRQUICAS Y FUNCIONALES ENTRE ÓRGANOS DE LA ORGANIZACIÓN.

Además del organigrama y de las funciones principales de cada área, el auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas, o por el contrario, detectará por ejemplo, si algún empleado tiene dos jefes.

Las relaciones de jerarquía implican la correspondiente subordinación. Las funcionales, por su parte, indican relaciones de naturaleza complementaria y no estrictamente subordinables. Estas relaciones deben estar bien definidas por el nivel inmediato superior, el



cual deberá informar a sus propios grupos horizontales de la existencia de tales relaciones, así como de cualquier variación en ellas.

4.3.3 FLUJOS DE INFORMACIÓN

Los flujos de información entre los grupos de una organización son necesarios y aún imprescindibles para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.

En ocasiones, las organizaciones crean espontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales de información alternativos se producen porque hay pequeñas o grandes fallas en la estructura y en el organigrama que los representa.

Se ha dicho con verdad que no existe el organigrama perfecto, por lo que puede resultar inevitable la existencia de flujos de información no deseados, pero esta realidad no debe excusar la proliferación de dichos flujos.

Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización.

4.4 RIESGOS A LOS QUE ESTAN EXPUESTAS LAS OPERACIONES.

Riesgo se puede definir de manera general como:

- La probabilidad de sufrir un daño, una pérdida o disminución en el valor, a que están expuestos los bienes.
- Cualquier cosa que pueda impedir el logro de un objetivo.

Los riesgos desde el punto de vista de su origen pueden clasificarse en externos e internos.

4.4.1 LOS RIESGOS EXTERNOS

Se identifican como todos aquellos que se presentan en el ambiente físico y social que rodea a una instalación de procesamiento de datos.

Estos pueden clasificarse en naturales, humanos y materiales; los naturales se refieren a los riesgos que se relacionan con siniestros ocasionados por terremotos, incendios, inundaciones, tormentas, etc.; los humanos se refieren a los que son causados por personas y pueden ser, principalmente, intencionales, por ejemplo sabotaje; o accidentales, por ejemplo disturbios externos; por su parte, los materiales se refieren a descomposturas de equipo, fallas de energía eléctrica, etc.

4.4.2 LOS RIESGOS INTERNOS

Son los que se generan desde la misma institución, para el caso que nos ocupa cabe mencionar los riesgos de aplicación siguientes, a saber:

Acceso no autorizado a las funciones de procesamiento de transacciones.

Los datos permanentes y/o de transacciones pueden ser:



- Leídos
- Modificados
- Eliminados
- Ingresados
- Recuperados

Datos ingresados incorrectamente

Los datos permanentes y/o de transacciones ingresados para su procesamiento pueden ser:

- Inexactos
- Incompletos
- Ingresados en el período contable incorrecto
- Ingresados más de una vez
- Omitidos.

Las partidas rechazadas en suspenso pueden no ser resueltas en forma adecuada.

- Las transacciones pueden ser omitidas
- Los items en suspenso pueden ser resueltos sin la debida autorización.

Las transacciones pueden ser procesadas o informadas incorrectamente.

Las transacciones ingresadas pueden:

- Ser procesadas en forma incompleta.
- Ser procesadas en forma inexacta
- No ser procesadas

Las transacciones generadas pueden:

- Perderse
- Ser procesadas en forma incompleta
- Ser procesadas en forma inexacta.

Las transacciones pueden:

- Ser informadas en forma inexacta
- No ser informadas

La información gerencial (análisis, resúmenes, informes de excepción, totales) puede:

- Ser generada o informada en forma incompleta
- Ser generada o informada en forma inexacta.

La estructura organizativa y los procedimientos operativos pueden no ser adecuados.

Fraudes pueden ser perpetrados por:

- Personal del Centro de Cómputo.
- Usuarios.

Los programas o los archivos de datos pueden ser:

- Copiados o robados
- Destruídos intencionalmente

Los recursos del centro de cómputo pueden ser:

- Utilizados sin la debida autorización.
- Destruídos intencionalmente

Procedimientos inadecuados de desarrollo de sistemas pueden originar:

- Sistemas de aplicación deficientes (desarrollados a medida o paquetes)
- Errores durante la implantación.

La integridad interna de las bases de datos puede ser dañada.

Pueden producirse errores de operación del computador.

Pueden producirse errores de hardware

Los programadores pueden realizar cambios incorrectos o no autorizados a los programas.

- Los programadores de aplicaciones o de sistemas pueden perpetrar fraudes a través de cambios a los programas de aplicación.



- Pueden surgir errores inadvertidos a partir de cambios no autorizados y/o no probados a los programas de aplicación.

Acceso no autorizado a los programas o a los datos.

El personal del Centro de Cómputo o terceros ajenos a la empresa pueden:

- Tener acceso no autorizado a datos confidenciales.
- Perpretar fraudes o provocar errores realizando cambios no autorizados a los archivos de transacciones o de datos permanentes.
- Sabotear los recursos del Centro de Cómputo.
- Utilizar los recursos sin autorización.

4.4.3 IDENTIFICACIÓN DE RIESGOS.

El proceso ideado de identificación de riesgos comienza con objetivos claramente definidos. La esencia y la forma de estos objetivos variará, dependiendo de la naturaleza del proceso.

Para identificar riesgos, es necesario que se formulen preguntas como las siguientes:

- Qué podría salir mal?
- Cómo podríamos fallar?
- Qué debemos hacer bien para tener éxito?
- Dónde somos vulnerables?

- Qué recursos necesitamos proteger (físicos, de información, humanos)?
- Cómo podría alguien desorganizar nuestras operaciones?
- Cómo sabemos si estamos logrando nuestros objetivos?
- En qué información confiamos más?
- Qué decisiones requieren de mayor criterio?
- Qué actividades son muy compleja?

4.4.3 EVALUACIÓN DE RIESGOS.

Una vez que hemos identificado claramente los riesgos en un proceso, necesitamos evaluarlos; es decir, necesitamos evaluar tanto la magnitud como la probabilidad de cada riesgo. Esto nos permitirá dedicar la mayor parte de nuestros esfuerzos a los riesgos más importantes y determinar que controles son necesarios, para minimizarlos.

En el criterio que a continuación se presenta para evaluar riesgos debe comprender los siguientes aspectos para llenar la matriz correspondiente de evaluación de riesgos:

- Identificar el riesgo: Lo que puede resultar mal para evitar que se alcancen los objetivos.
- Determinar la magnitud y la probabilidad.
- Diseñar el Control: Lo que puede hacer para minimizar los riesgos.

Criterios de Evaluación:

CATEGORÍA	PROBABILIDAD	MAGNITUD
BAJA	Es improbable que suceda un riesgo.	Si el riesgo se produce, probablemente no impactará materialmente en el logro del objetivo.
MEDIANA	Puede suceder algún riesgo.	Si el riesgo se produce, puede afectar el logro del objetivo.
ALTA	Es muy posible que se produzca el riesgo.	Si el riesgo se produce, puede significativamente afectar el logro del objetivo.

Matriz de Evaluación

PROBABILIDADES	Alta			
	Mediana			
	Baja			
		Baja	Mediana	Alta
	MAGNITUD			

Más adelante se presenta una matriz de análisis de riesgos, por medio de la cual se selecciona el área de mayor exposición al riesgo, resultante de la aplicación de los criterios de evaluación antes mencionados.

Matriz de Evaluación

RIESGOS	Áreas de Evaluación			
	I	II	III	IV
<p>Riesgos generales de informática</p> <ul style="list-style-type: none"> ✓ El acceso físico del Hardware no está restringido, lo cual ocasiona que se utilicen los recursos de informática sin autorización. ✓ No existe confidencialidad y seguridad de los datos. ✓ La metodología en el desarrollo del sistema, es inadecuada, por lo cual se incurre en errores y pérdida de tiempo en la implantación, lo que impide que se brinde un servicio de calidad a los clientes. ✓ El personal de informática incurre en incumplimiento a políticas y procedimientos de backup y recuperación de la información. ✓ No existen manuales de usuario adecuados que sirvan de apoyo en el conocimiento de los sistemas. <p>Riesgos en el proceso de ingreso de datos.</p> <ul style="list-style-type: none"> ✓ Datos ingresados incorrectamente. ✓ Datos ingresados más de una vez. ✓ Datos Omítidos. ✓ No se utiliza dígito verificador. ✓ No existe verificación de integridad de la información. <p>Riesgos en el proceso de procesamiento de datos.</p> <ul style="list-style-type: none"> ✓ Uso inadecuado de claves de acceso al sistema. ✓ No se realizan pruebas de edición. ✓ Los totales de control no se reflejan adecuadamente. ✓ Los programas no son flexibles para hacer modificaciones, lo cual ocasiona errores frecuentes. <p>Riesgos en el proceso de salida de datos.</p> <ul style="list-style-type: none"> ✓ Las operaciones rechazadas quedan en suspenso sin ser resueltas de manera adecuada. ✓ Las cifras de control son registradas inadecuadamente en los reportes. ✓ Los reportes emitidos a diario no son entregados de manera formal a los usuarios responsables, lo que puede ocasionar usos indebidos de la información. 				
Total A				
Total M				
Total B				

A= Alto
M= Mediano
B= Bajo

4.5 EVALUACION DE CONTROLES

Los controles son mecanismos situados en puntos de riesgo para detectar fallas o errores y advertir sobre ellos.

Los elementos creados para la detección de alguna falla o error, pueden ser de tres tipos:

Aparatos (Máquina): Avisan por medio de una alarma u otro medio.

Ejemplo: detector de humo, incendio, ventana quebrada, sistema de seguridad violado, autos robados.

Humanos: Trabaja por medio de rastreo de procedimientos y avisa mediante un informe. Ejemplo: El auditor.

Automatizados: El computador detecta por ejemplo un uso inadecuado de una clave de acceso y éste avisa mediante la generación de una llamada telefónica a la persona usando voz digitalizada.

Como ya se indicó los controles son mecanismos situados en los puntos de riesgo, siendo éstos a su vez, los lugares o momentos donde existe la posibilidad de falla o error.

Para una mayor comprensión de un punto de riesgo se puede enfocar en dos esquemas:

Lugares: Son puntos físicos; lugar físico del punto de riesgo. Ejemplo: habitación, archivo, expediente, disco de computadora, etc.

Momentos: Es un paso de proceso donde existe el riesgo (proceso simple) Ejemplo: Asentar una partida de kardex, pasar datos de un expediente a un libro, actualizar saldos, archivar.

En el entendido que los controles son establecidos para minimizar la posibilidad de riesgo y permitir averiguar que falla o error se dio, se define entonces que:

Falla: Se refiere a mecanismos. Descompostura de mecanismos (no funcionó). Falta de precisión; puede ser física: cuando se quiebra una pieza. De mantenimiento: mal funcionamiento de un dispositivo.

Error: Se refiere a proceso. No hace lo que el procedimiento establece. Se debe a: negligencia (por falta de capacitación) y desconocimiento (equivocación en los pasos de un procedimiento).

En algún caso, puede suceder que la falla y el error se mezcle. Ejemplo: el extinguidor de incendios, falla en el momento de accionar por falta de carga.

En virtud de lo antes descrito, se concluye que un mecanismo de control detecta una falla o error y avisa por medios prediseñados, ya sean éstos mecánicos o automatizados, lo que está sucediendo.

Por lo consiguiente, no tiene objeto el establecimiento de controles si no existe un procedimiento de solución.

Los controles en los sistemas incluyen: controles administrativos, de recuperación ante desastres, de entrada, de procesamiento, de bases

de datos, de salida, de documentación, de hardware (equipo), del sistema operativo, los programas de utilería y de las operaciones de la computadora.

Asimismo, es importante mencionar la categoría de controles que son utilizados para evitar o prevenir que ocurra una causa de riesgo, para detectar un hecho ya ocurrido, los directivos, los mitigantes o compensatorios, generales y de aplicaciones automatizadas.

4.5.1 PREVENTIVO

Son aquellos que reducen la frecuencia con que ocurren las causas de riesgo. Los controles detectivos no evitan que ocurran las causas de riesgo sino que más bien, las detectan después de que han ocurrido. No es suficiente la simple detección de una causa de riesgo. Cuando se detectan tales situaciones, debe tomarse una decisión respecto a cuál es la acción correctiva apropiada, y posteriormente debe llevarse a cabo dicha acción. Un control preventivo actúa como una guía para ayudar a que las cosas sucedan como deben ser. Con frecuencia son pasivos y no implican ninguna actividad física directa. Los controles preventivos se encuentran a menudo tan sutilmente intercalados dentro de un proceso, que las personas involucradas en la operación pueden no estar siquiera conscientes de su existencia.

4.5.2 DETECTIVO

Puede poner fin al procesamiento posterior o simplemente registrar la ocurrencia. Los controles detectivos alertaran a las personas involucradas en el proceso, a fin de que estén conscientes de la existencia de un problema. Tal conocimiento es imprescindible si ha de seguirse la acción correspondiente para corregir los efectos de la causa detectada.

4.5.3 DIRECTIVO

Son los que provocan o estimulan un hecho deseable.

4.5.4 MITIGANTES O COMPENSATORIOS

Son los que compensan por lo menos parcialmente, un control que no existe o que es excesivamente costoso.

Ahora bien, la evaluación que hace un auditor respecto al entorno de control dentro de un sistema computarizado, normalmente comprenderá dos categorías: generales y de aplicación; por consiguiente, éstos se amplían a continuación:

4.5.5 GENERALES

Se refieren a los controles que deben existir en un sistema computarizado y en todas las actividades del mismo. Estos controles contribuyen significativamente a la efectividad de los controles de aplicación, los cuales son diseñados para evitar, detectar errores e irregularidades que afecten los resultados finales o la información directamente relacionada con éstos.



Los controles generales abarcan la segregación de funciones, los controles para el desarrollo y documentación de sistemas, controles de equipo y programas, controles de acceso y controles de los datos y procedimientos.

Segregación de funciones.

Las responsabilidades deben ser distribuidas de forma tal que el acceso de los empleados a las funciones de procesamiento computarizados no los habilite para llevar a cabo funciones incompatibles.

La segregación de funciones es un control general. No obstante, en un ambiente computarizado los controles basados en software que normalmente son utilizados para restringir el acceso a las funciones de procesamiento de transacciones o a los registros de datos resultantes, pueden constituir un medio efectivo para asegurar dicha segregación.

Debido al amplio rango de datos y programas que son potencialmente accesibles para una persona que tiene acceso a un sistema computarizado moderno, la segregación de funciones por sí sola raramente constituirá un control efectivo.

Por ejemplo, el acceso a funciones de procesamiento, este riesgo se refiere a que personas no autorizadas pueden tener acceso a las funciones de procesamiento de transacciones de los programas de aplicación, permitiéndoles leer, modificar, agregar o eliminar datos, o ingresar transacciones no autorizadas para su procesamiento.

Por lo que este riesgo puede reducirse sí:

- Existe una adecuada segregación de funciones tanto en la organización como en el centro de cómputo.
- Se controlan los accesos no autorizados.

Controles para desarrollo y documentación de sistemas.

Estos controles generales se refieren a tres áreas:

- Revisión, prueba y aprobación de nuevos sistemas;
- Control de cambios a los programas; y
- Procedimientos de documentación.

Los controles para el desarrollo y documentación de sistemas deben asegurar que en todos los sistemas nuevos se han incorporado controles de aplicación antes de que se implanten. Cuando los controles para el desarrollo y documentación de sistemas se han diseñado adecuadamente, pueden prevenir o detectar los siguientes tipos de errores:

- Implantación de sistemas que no tienen controles de aplicación adecuados;
- Desarrollo de sistemas que no cumplen los objetivos de la gerencia, o que no funcionan de acuerdo con las especificaciones originales;
- Implantación de sistemas que pueden ser modificados sin autorización.

Los controles de documentación corresponden a los documentos y registros llevados por una compañía para describir actividades de procesamiento de la computadora. Una adecuada documentación se considera importante tanto para la administración como para el auditor. Para la administración, la documentación proporciona una base para: revisar el sistema, entrenar nuevo personal y mantener y revisar los actuales sistemas y programas. Para el auditor, la documentación proporciona la fuente principal de información respecto al flujo de transacciones a través del sistema y controles contables relativos. La documentación incluye:

- Descripciones y gráficas de flujos de los sistemas y programas.
- Instrucciones de operaciones para el operador de la computadora.
- Procedimientos de control que deban de seguirse por operadores y usuarios.
- Descripciones y muestras de datos de entrada y salida requeridos.

Control de equipo y programas

La mayoría de los equipos de computador pueden detectar y registrar fallas del equipo, en virtud de que la tecnología de las computadoras modernas ha alcanzado un alto grado de confiabilidad en equipo de cómputo. Algunos factores que han contribuido a lo anterior se refiere a ciertos controles de sistemas incorporados a la máquina, para

detectar un funcionamiento inapropiado del equipo, esta categoría de controles incluye:

Doble lectura: Los datos de entrada son leídos dos veces y las dos lecturas se comparan.

Leer después de escribir: La computadora lee nuevamente los datos después de que se hayan registrado, ya sea en la memoria o en listados, y verifica los datos mediante comparación con su fuente original.

Controles de acceso

Los controles de acceso dan la protección necesaria que garantiza que los recursos de informática se utilizan en forma adecuada. Una debilidad o falla de controles de acceso puede afectar la integridad del sistema y, desde luego, el grado de confianza del auditor en los resultados del proceso.

Los controles de acceso adecuados sirven para prevenir o detectar errores accidentales o deliberados causados por uso inadecuado o manipulación de los archivos de datos, uso incorrecto o no autorizado de los programas del computador, y uso incorrecto de los recursos del mismo.

Cuando los datos son ingresados o están a disposición de los usuarios en forma interactiva, el control del acceso resulta más complicado. La efectividad del control dependerá, por lo general, del uso



de software que permita el acceso del usuario a ciertas funciones de procesamiento computarizadas, pero no a otras.

Se utilizan varios mecanismos para lograr este control, incluyendo:

- Menús
- Normas/perfiles de acceso.
- Acceso a los datos por programa.
- Dispositivos de acceso a los datos/programas a través de restricciones lógicas de las terminales.
- Dispositivos de seguridad de terminales, incluyendo dispositivos de acceso personalizado o tarjetas de banda magnética.

Controles de los datos y procedimientos

Una vez que una nueva aplicación entra en operación, deberá estar sujeta a los controles que aseguren un proceso oportuno y exacto. Los controles de los datos y los procedimientos proveen un marco para controlar las operaciones diarias y establecer medidas de seguridad contra errores en el proceso. Los siguientes controles pueden establecerse en el área de procesamiento de datos:

- Control de la función de cuadro.
- Manuales que contemplen los procedimientos y los sistemas.
- Capacidad para restaurar o reemplazar archivos perdidos, dañados o incorrectos.

4.5.6 EN APLICACIONES AUTOMATIZADAS.

Se relacionan con tareas específicas que deben ser realizadas por la computadora. Estos controles están diseñados para proporcionar una seguridad razonable que el registro, procesamiento e información de datos se realizan de manera apropiada.

Para fines del presente trabajo se mencionan los controles de aplicación en el orden acostumbrado (entrada, proceso, salida); no obstante, cabe indicar que lo importante es el objetivo que satisfacen, independientemente de donde lo hace, siendo entre otros: preventivos, detectivos, directivos, mitigantes o compensatorios, las diferentes causas de riesgo relativas a las aplicaciones.

Derivado de lo antes descrito, es factible resumir los objetivos de los controles de aplicación en cinco aseveraciones:

- Asegurar que todas las transacciones autorizadas se procesen completamente una vez, y sólo una vez.
- Asegurar que los datos de las transacciones estén completos y sean exactos.
- Asegurar que el procesamiento de las transacciones sea correcto y apropiado en las circunstancias.
- Asegurar que los resultados del procesamiento se utilicen para los fines previstos.
- Asegurar que la aplicación pueda seguir funcionando.

El procesamiento de datos en computador deberá producir información confiable, completa y válida en forma oportuna. Se puede definir como un "ciclo de procesamiento", la producción de esta información durante una unidad de tiempo dada, tal como un día. Normalmente el ciclo de procesamiento, se asocia con un período de tiempo específico, el cual debe ser predeterminado para fines de la programación de producción de trabajo.

El ciclo completo de procesamiento, incluye procedimientos tanto en los departamentos de origen y usuario, como en el centro de cómputo. Estos procedimientos se pueden agrupar en las fases siguientes: entrada, procesamiento en computador y salida, cada una de éstas cuenta con procedimientos específicos, los que se detallan más adelante.

En una auditoría de informática el auditor debe considerar específicamente, las técnicas básicas de verificación que debieran ser empleadas para determinar si existe en vigor una técnica de control, que contribuya a lograr un estándar mínimo de control.

Controles de datos de entrada

Los controles de datos de entrada son un tipo de controles de aplicación, su importancia se debe fundamentalmente a que la mayor parte de los errores ocurren en este punto. Su diseño debe estar encaminado a proporcionar una seguridad razonable; es decir, que los

datos recibidos para procesamiento hayan sido: debidamente autorizados, convertidos a lenguaje de máquina y controlados posteriormente.

Entre los controles de entrada figuran:

Controles de edición y validación

Los controles de edición y validación están diseñados para permitir la identificación de errores en los datos ingresados, ingresos duplicados, o datos que no satisfacen ciertos criterios preestablecidos de aceptación.

Los controles de edición y validación normalmente son aplicados cuando se ingresan los datos; si el ingreso de datos es interactivo, el usuario recibirá inmediatamente la indicación de corregir los datos que contienen los errores o que no fueron ingresados correctamente.

Controles de formato

Aseguran que cada campo tenga el formato de datos apropiado (numérico, alfabético o alfanumérico) y la cantidad adecuada de caracteres.

Control de campos faltantes

Son diseñados para asegurar que todos los campos de datos importantes hayan sido completados. Los controles de combinación se utilizan en forma similar para requerir que se ingresen datos en un determinado campo cuando se ingresan datos en campos conexos o dependientes.

Dígito verificador

Son utilizados para verificar la integridad de un campo. Cuando la transcripción de datos es necesaria, siempre existe la posibilidad de error. Si bien no es posible prevenir estos errores, es necesario hacer cuanto se pueda para detectarlos. Con campos numéricos claves como números de cuentas y códigos de productos, es común agregar un dígito extra al código. Este dígito verificador se calcula a partir de los otros dígitos del campo usando un simple algoritmo para detectar toda transcripción, transposición, omisión, repetición y combinaciones sucesivas de estos errores.

Contraseña

Este control comprende las autorizaciones para permitir el acceso a información o proceso, por medio de una señal o "clave" conocida únicamente por los individuos autorizados.

Acceso dual

Antes de permitirse el procesamiento se requieren dos acciones o condiciones independientes, pero simultáneas, por ejemplo, un cajero para realizar una reversión deberá requerir clave de autorización para realizar la operación.

Verificación de Integridad

Una prueba de que se hayan anotado los datos en aquellos campos que no pueden procesarse si se dejan en blanco, por ejemplo: el

computador no imprimirá un cheque si el nombre del beneficiario se encuentra en blanco.

Controles de procesamiento

Estos proporcionan una seguridad de que el procesamiento electrónico de datos es razonable, o bien se puede confiar en que una aplicación específica, se realizó tal como se pensaba; es decir, todas las transacciones procesadas fueron autorizadas, las transacciones no autorizadas se omiten y las no desautorizadas se incluyen.

Los controles de procesamiento pueden variar dependiendo la complejidad de cada aplicación, entre las más importantes están:

Controles de Lote

La agrupación de documentos fuente en lotes impide que eventualmente se pierda alguno, o bien que se agreguen en el ingreso de los mismos.

También permite:

- Establecer totales de control,
- Verificar la exactitud de los datos preparados para el ingreso,
- Minimizar la cantidad de registros/transacciones rechazados en caso de presentarse errores,
- Facilitar y acelerar el seguimiento de los errores, ya que la agrupación en lotes limita el número de registros a inspeccionar.



Controles de validación

Se utilizan para asegurar que los datos ingresados sean compatibles con los datos permanentes o del archivo maestro, una vez que se ha controlado el formato de los datos, el control de validación compara los datos ingresados con registros de los archivos maestros para determinar su validez.

Controles de procesamiento duplicado

Identifican los números de documentos o lotes que son ingresados para su procesamiento más de una vez.

Controles de totales

Se incluye dentro del programa de la computadora medios para acumular controles de totales para así facilitar cotejar los totales de los datos de entrada con los totales de procesamiento para cada corrida.

Marcas identificadoras de archivo

Las marcas externas permiten una identificación visual de un archivo. Las marcas internas de archivo se cotejan contra las instrucciones específicas de operadores incorporados dentro del programa de la computadora antes de poder iniciar el procesamiento o antes de que pueda terminarse con éxito.

Controles de salida

El objetivo de estos controles es básicamente corregir los resultados de inconsistencias de datos de entrada y de procesamiento. Este objetivo se satisface de la siguiente manera:

Conciliación de totales

Los totales de datos de salida son generados por los programas de la computadora, y se concilian con los totales de datos de entrada y de procesamiento, por el grupo de control de datos, así como por los departamentos usuarios.

Comparación con los documentos fuente

Por los datos de salida se generan listados los cuales se comparan contra los documentos fuente.

La información que se genera deberá manejarse de manera confidencial, por lo que la distribución de la misma incluirá una noja que permita llevar un control adecuado.

Cifras Control de Cantidades

Este control comprende, totales de valores homogéneos para un grupo de transacciones o registros, generalmente en valores monetarios o cantidades.

Cifras de Control de Número de Documentos

Este consiste en un conteo del número de documentos individuales.

CAPITULO V

CASO PRACTICO

5.1 AUDITORIA DE INFORMATICA EN EL AREA DE DEPOSITOS.

Según se indica en el Capítulo I. numeral 1.3 en relación con las operaciones que realizan las instituciones bancarias, se pueden clasificar en operaciones activas, pasivas y de confianza, y dentro de las segundas toma relevancia la correspondiente a la captación de recursos financieros a través de operaciones de depósitos, con lo cual nace una obligación para la institución a la vista o a plazo, subdividiéndose, a su vez, en depósitos monetarios, de ahorro y a plazo.

Con la finalidad de enfocar la auditoría de informática, de manera tal, que le dé valor agregado a nuestro trabajo, asegurando con ello que responda más eficientemente a las necesidades de la institución, con respecto a controles y asesoria, se propone un plan de trabajo para llevar a cabo una auditoría de informática mediante la utilización de un sistema de evaluación de riesgos.

Como en cualquier actividad, para desarrollar con efectividad las diferentes labores de auditoría se desea que exista, una adecuada planeación de las actividades a desarrollar; por lo tanto, una planeación deberá incluir la determinación del área de la entidad, que requiere la revisión de los diferentes aspectos, para nuestro caso, del sistema computarizado, la elección del camino adecuado para analizar el sistema y



los datos resultantes, e identificar las pruebas de cumplimiento de los procedimientos establecidos, para luego planificar y establecer las comprobaciones sustantivas que podrán llevarse a cabo con mayor efectividad, mediante la aplicación de técnicas de auditoría.

Según lo muestra la matriz de riesgos que se presenta más adelante, en el punto de Selección de Riesgos Críticos, el área de depósitos del Banco XYZ, muestra un número más alto de riesgos con relación con las demás áreas evaluadas. Esta área está constituida por los fondos entregados por clientes, que la entidad se obliga a devolver a la vista, o dentro de un plazo determinado, según se indica al inicio de este apartado.

BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

INDICE

	REFERENCIA
Nombramiento.	A
Plan de trabajo.	B
Conocimiento General.	C
Identificación de los riesgos.	D-1
Identificación de controles existentes.	D-1
Selección de riesgos críticos.	D-1
Matriz de análisis de riesgos	D-2
Evaluación y análisis de los controles en aplicaciones automatizadas en operaciones del área de depósitos	E
Proceso de entrada de datos	F
Cuestionario de Control Interno	F-1
Programa de Auditoría	F-2
Cédula de procedimientos de verificación	F-3
Cédula de deficiencias encontradas	F-4
Proceso en computador	G
Cuestionario de Control Interno	G-1
Programa de Auditoría	G-2
Cédula de procedimientos de verificación	G-3
Cédula de verificación de niveles de acceso	G-3-1
Cédula de cambio de tasa de interés en el sistema	G-3-2
Cédula de deficiencias encontradas	G-4
Proceso de salida	H
Cuestionario de Control Interno	H-1
Programa de Auditoría	H-2
Cédula de procedimientos de verificación	H-3
Cédula de verificación del uso de cifras de Control.	H-3-1
Cédula de deficiencias encontradas	H-4
Informe de la auditoría.	I

BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. A
Hecho por: HB
Fecha: 30.9.99

NOMBRAMIENTO NAI-01-99

Guatemala, 1 de julio de 1999.

A:
Hilda de María Berganza Garza
Auditor de Informática.
Presente.

El presente nombramiento la acredita para que efectúe:

- Evaluación desde el punto de vista de informática en el área de Depósitos, para lo cual debe realizar una investigación de las actividades que intervienen en los procesos de información, comprendiendo el periodo del 1 de julio al 30 de septiembre de 1999.
- De los resultados que se obtengan sirvase rendir informe detallado.

Atentamente,

JOSE DOMINGO SANTIZO CRUZ
AUDITOR INTERNO.

Colaboradores:

Silvia Marieny Sánchez López, auditor auxiliar I.
Mario Roberto Aguilar Pineda, auditor auxiliar II.

5.2 PLAN DE TRABAJO

Objetivo General

Definir el plan de trabajo tomando como base un Sistema de Evaluación de Riesgos, con el propósito de asignar los recursos de auditoría a las áreas de mayor riesgo en la organización.

Objetivos Específicos

1. Identificar de una forma técnica y sistemática las áreas de mayor riesgo en la organización.
2. Evaluar las distintas áreas de la Organización sobre una base común.
3. Identificar las áreas de mayor exposición al riesgo.
4. Asignar los recursos de Auditoría Interna a las áreas de mayor riesgo.
5. Evaluar la adecuación de los controles existentes para asegurarse de la justificación de su dependencia.
6. Proponer la implementación de controles adecuados o mejoras a los ya establecidos que coadyuven a minimizar los riesgos asociados a las operaciones examinadas.

Estimación de Recursos

Para efectos de la realización del presente trabajo, se hace necesario la utilización de los recursos siguientes: humanos, físicos y financieros.



Recursos Humanos

Auditor coordinador: Supervisará las actividades a efectuar.

Auditor Auxiliar I: Realizará las actividades delegadas por el auditor coordinador.

Auditor Auxiliar II: Realizará las actividades delegadas por el auditor coordinador.

Recursos Físicos

Centro de cómputo: Lugar para realizar las pruebas y verificaciones de auditoría; es decir, el trabajo de campo.

Oficina: Lugar asignado para realizar el informe de la auditoría.

Papelería y útiles.

Equipo de Computación.

Mobiliario y Equipo de Oficina.

Recursos Financieros

Papelería y útiles de oficina	Q. 500.00
Depreciación Equipo de Computación	Q. 1,500.00
Sueldos	Q. 15,000.00
Otros	<u>Q. 2,000.00</u>
Total	<u>Q.19,000.00</u> =====

Tiempo requerido

El tiempo requerido para ejecutar el presente plan se estima del período comprendido del 1 de julio al 30 de septiembre de 1999.

Se considera para la preparación del plan de trabajo que previamente se realice un diagnóstico, efectuándose a su vez, una evaluación de riesgos, para lo cual se cubrirán los aspectos siguientes:

- ✓ Conocimiento General
- ✓ Identificación de Riesgos.
- ✓ Identificación de los Controles Existentes.
- ✓ Selección de Riesgos Críticos.
- ✓ Evaluación y Análisis de los Controles.

Técnicas y Métodos.

La revisión de informática se realizará en tres fases: entrada de datos, proceso de datos y salida de datos; para lo cual se incluirá las siguientes técnicas y métodos, a saber:

- ✓ Indagación.
- ✓ Observación.
- ✓ Cuestionarios.
- ✓ Programas de auditoría.
- ✓ Procedimientos de verificación.
- ✓ Determinación de deficiencias.

Informe de resultados.

- ✓ Observaciones
- ✓ Recomendaciones.

5.2.1 CONOCIMIENTO GENERAL

Conocimiento general del medio ambiente de la entidad.

Generalidades.

Denominación Social " BANCO XYZ, SOCIEDAD ANONIMA", localizado en la 6ª calle 8-55, Zona 10, ciudad de Guatemala; fecha de apertura, 10 de junio de 1991, actividad a la que se dedica: PRESTACION DE SERVICIOS BANCARIOS: depósitos monetarios, depósitos de ahorro especial, depósito de ahorro corriente, depósito de ahorro a plazo, compra y venta de cheques de viajero, cobros por cuenta ajena, compra y venta de giros, cobranzas locales y del exterior, cartas de crédito, transferencia de créditos, préstamos, descuentos de documentos, etc.

Conocimiento general del Centro de Cómputo.

Generalidades.

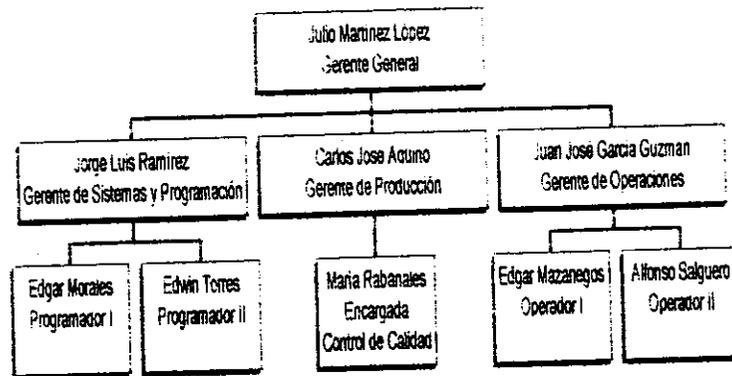
Denominación Social "DATACENTRO, SOCIEDAD ANONIMA", localizado en la 8ª calle 5-10, Zona 10, ciudad de Guatemala; fecha de Apertura, 10 de septiembre de 1992; actividad a la que se dedica: PRESTACION DE SERVICIOS DE PROCESAMIENTO ELECTRONICO DE DATOS, A LA ENTIDAD BANCARIA, BANCO XYZ, S.A., tales como proceso de datos electrónicos en aplicaciones automatizadas para las áreas comprendidas del banco: Caja, Inversiones, Préstamos, Depósitos, Cuentas por pagar, Capital, Productos y Gastos.

Estructura Organizacional

La función de la empresa DATACENTRO, S.A. es externa con relación a la institución bancaria BANCO XYZ, S.A., a quien reporta las actividades de procesamiento de datos; es decir, el servicio que le presta.

La estructura organizativa de DATACENTRO, S.A. se muestra en el organigrama que se grafica más adelante, siendo los responsables de la gestión las personas indicadas en el mismo.

ORGANIGRAMA
DATACENTRO, S.A.



El entorno operacional en el cual se desenvuelve el centro de cómputo, comprende lo siguiente:



El sistema que se utiliza para el procesamiento de datos, es denominado IBM AS-400.

La interconectividad entre el equipo, está sobre la base de configuraciones de redes, que facilitan la comunicación a través de terminales remotas, usando fibra óptica, por lo que la transmisión de datos puede ser inmediata y el procesamiento en tiempo real.

El lenguaje de programación utilizado es el denominado RPG, los programas se nombran de manera estándar para cada aplicación (depósitos, créditos, inversiones, contabilidad, etc.), logrando de esta manera tener un mejor control sobre las mismas.

El software cuenta con niveles de acceso dependiendo de la jerarquía, así como a las labores que tiene asignadas cada empleado, de manera tal que las desarrolle con el menú de información con el que cuenta.

5.2.2 IDENTIFICACION DE LOS RIESGOS

En esta parte, dentro de la comprensión del sistema asociado a las operaciones automatizadas se deben determinar las posibles situaciones que, de llegarse a cristalizar, pueden afectar la consecución de los objetivos previstos por el Banco para la obtención de información relativa a tales operaciones.

El resultado de dicha labor se detalla en la matriz de riesgos que se presenta en el punto de Selección de Riesgos Críticos, en la cual se aprecia, para cada área definida en donde se concentra la mayor exposición de los riesgos identificados como : alto, mediano y bajo.

5.2.3 IDENTIFICACION DE CONTROLES EXISTENTES.

En la matriz de riesgos que se presenta más adelante, se contempló un análisis de los controles, mismos que fueron detallados en el numeral 4.5 Evaluación de Controles del capítulo IV; en especial, a los asociados con los riesgos que se consideran estar expuestas las operaciones que son procesadas en el centro de cómputo: es decir los controles existentes que minimizan el riesgo en caso que este se activara.

5.2.4 SELECCION DE RIESGOS CRITICOS.

Para fines del presente trabajo, ha sido seleccionada para evaluación el área que más número de riesgos altos presenta (es muy

posible que se produzca el riesgo y que afecte significativamente), según se muestra en la matriz respectiva.

Como ya se indicó, el tema principal del presente trabajo se enmarca, precisamente, en una Auditoría de Informática en un Banco Privado Guatemalteco; por consiguiente las áreas consideradas de objeto de evaluación corresponden a las operaciones del Banco XYZ, S. A., como: Caja, Inversiones, Préstamos, Depósitos, mismas que en cierto grado se encuentran automatizadas; en consecuencia, tienen relación con el Centro de Cómputo DATACENTRO, S.A.

Los riesgos de las áreas indicadas, fueron examinadas tanto en magnitud como en probabilidad, bajo la categoría de: alto, mediano y bajo, lo que permite dedicar la mayor parte de nuestros esfuerzos a los riesgos más importantes o bien más altos (muy posible que se produzcan y afecten significativamente) y determinar que controles son necesarios, para minimizarlos.

Como puede apreciarse en la matriz de análisis de riesgo el área de operaciones de depósitos es la que refleja un mayor número de riesgos altos con respecto del resto de áreas evaluadas; en consecuencia, es la que se selecciona para un examen más detallado.

Matriz de Evaluación

RIESGOS	Areas de Evaluación			
	Caja	Inv.	Pmos.	Dep
Riesgos generales de informática				
✓ El acceso físico del Hardware no está restringido, lo cual ocasiona que se utilicen los recursos de informática sin autorización.	B	B	B	B
✓ No existe confidencialidad y seguridad de los datos.	B	B	B	B
✓ La metodología en el desarrollo del sistema, es inadecuada, por lo cual se incurre en errores y pérdida de tiempo en la implantación, lo que impide que se brinde un servicio de calidad a los clientes.	B	B	B	B
✓ El personal de informática incurre en incumplimiento a políticas y procedimientos de backup y recuperación de la información.	B	B	B	B
✓ No existen manuales de usuario adecuados que sirvan de apoyo en el conocimiento de los sistemas.	B	B	B	B
Riesgos en el proceso de ingreso de datos.	B	M	M	M
✓ Datos ingresados incorrectamente.	B	B	B	B
✓ Datos ingresados más de una vez.	B	B	B	B
✓ Datos Omitidos.	B	B	B	A
✓ No se utiliza dígito verificador.	B	A	B	B
✓ No existe verificación de integridad de la información.				
Riesgos en el proceso de procesamiento de datos.				
✓ Uso inadecuado de claves de acceso al sistema.	A	A	A	A
✓ No se realizan pruebas de edición.	B	B	B	B
✓ Los totales de control no se reflejan adecuadamente.	A	B	M	A
✓ Los programas no son flexibles para hacer modificaciones, lo cual ocasiona errores frecuentes.	M	B	M	A
Riesgos en el proceso de salida de datos.				
✓ Las operaciones rechazadas quedan en suspenso sin ser resueltas de manera adecuada.	B	A	A	B
✓ Las cifras de control son registradas inadecuadamente en los reportes.	B	M	B	A
✓ Los reportes emitidos a diario no son entregados de manera formal a los usuarios responsables, lo que puede ocasionar usos indebidos de la información.	B	M	M	A
Total A	2	3	2	6
Total M	1	3	4	1
Total B	14	11	11	10

A= Alto
M= Mediano
B= Bajo

5.2.5 EVALUACION Y ANALISIS DE LOS CONTROLES EN APLICACIONES AUTOMATIZADAS EN OPERACIONES DEL AREA DE DEPOSITOS.

Actividades	Explicación de las actividades
Entrada	
Iniciación	Depósito o retiro en cualquier cuenta de depósitos.
Registro	Se crea el registro de la transacción en las terminales remotas, cuyo procesamiento es en tiempo real.
Transmisión	La transmisión de la información es por medio de fibra óptica
Procesamiento	
Comparación	Verifica la información ingresada utilizando pruebas de lógica, condiciones para determinar o identificar similitudes o diferencias, por ejemplo: dígito verificador.
Cálculo	Efectúa distintas operaciones matemáticas para producir un resultado numérico.
Actualización	La actualización de los archivos se realiza mediante la verificación de la información, cuando se ingresa por segunda vez, quedando así confirmada para afectar los archivos maestros.
Archivo	Almacena la información o los registros a fin de que puedan extraerse cuando se requieran.
Salida	
Reportes	En el área de depósitos se reciben los reportes producidos por el centro de cómputo, los cuales contienen información resumida o por excepciones.
Consulta pantalla	Son solicitudes que se hacen desde pantallas remotas, para obtener información, sin alterarla.

Lo antes descrito esquematiza las actividades sujetas a control en el área de depósitos, principalmente en los procesos de depósitos y retiros en cuentas, abarcando las fases de entrada, proceso y salida de la información.

A continuación, para cada fase del proceso de datos (entrada, proceso y salida), se detallan los objetivos de control, cuestionarios de control interno, programas de auditoría, procedimientos de verificación y cédula de deficiencias encontradas; aspectos mínimos considerados al formularse el plan de Auditoría de Informática en el área de depósitos de un Banco Privado Guatemalteco.

La guía que más adelante se presenta no es inflexible; es decir, que se podrá ampliar o reducir, dependiendo de las circunstancias a medida que se ejecute o desarrolle, y su objetivo además, de la obtención de información acerca del procesamiento de datos de las operaciones del área de depósitos, abarca el que se utilice como una herramienta de análisis para arribar a conclusiones objetivas, que sirvan de base para la formulación de recomendaciones, que tiendan a mejorar los controles aplicables y, consecuentemente, a minimizar los riesgos asociados a las operaciones de depósitos.



BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. E
Hecho por: HB
Fecha: 30.9.99

La metodología para obtener y resumir información relacionada con los subsistemas o aplicaciones del área de depósitos, podrá incluir desde una anotación en forma descriptiva y la respuesta a cuestionarios, hasta la elaboración de gráficas, para ello se juzga preferible, como ya se indicó al inicio, dividir la revisión del sistema en tres partes o fases: entrada de datos, proceso de datos y salida de datos.

La información relativa a la fase de entrada y a la de salida será obtenida a través de conversaciones directas con los empleados relacionados con el sistema y poner atención especial a las modificaciones de las características claves de registro de los totales de control, las modificaciones a los archivos maestros, reportes de errores y conversiones de datos.

La información referente a la fase de proceso de datos provendrá en forma documentada del centro de cómputo, en caso contrario, el auditor preparará los resúmenes convenientes para alcanzar un adecuado conocimiento general del área indicada de depósitos.

5.2.5.1 PROCESO DE ENTRADA DE DATOS.

Esta fase incluye el flujo de los datos desde el punto de vista de origen de la operación hasta el último trámite visible antes de su alimentación al computador.

Objetivos de Control

- Asegurar que la totalidad de los datos sean ingresados al computador.
- Asegurar la exactitud de los datos ingresados al computador.
- Asegurar que todos los datos ingresados al computador estén debidamente autorizados.

CUESTIONARIO DE CONTROL INTERNO

PROCESO DE ENTRADA DE DATOS.

PREGUNTAS	SI	NO	N/A
1. Existe algún método que asegure que inicialmente son registrados e identificados la totalidad de los datos?	✓		
2. Se establece el control acerca del origen de la transacción?	✓		
3. Existe algún método que asegure que las correcciones de todos los errores identificados sean realimentadas al sistema?	✓		
4. Existen procedimientos para prevenir errores en la preparación de los datos de entrada o datos fuente, para detectar y corregir cualquier error significativo que pudiera presentarse?	✓		
5. Existen procedimientos para prevenir errores originados en la conversión y captura de los datos, para detectar y corregir cualquier error significativo que ocurra?	✓		
6. Existen procedimientos que aseguren que los datos sean transmitidos correctamente al centro de cómputo?	✓		
7. Se asegura que sólo se procesan datos autorizados, los documentos de entrada deberán mostrar evidencia de autorización y ser revisados respecto a la misma por el grupo de control?	✓		

PROGRAMA DE AUDITORIA

PROCESO DE ENTRADA DE DATOS

No.	PROCEDIMIENTOS	REF.
1.	Determinar mediante comentarios e inspección de documentos, que se utilizan formas especialmente diseñadas.	F-3.
2.	Examinar las formas para ver que el diseño coadyuva a evitar la omisión de datos o el uso equivocado de formas y propicia la adecuada autorización.	F-3.
3.	Examinar los métodos de transmisión de los datos de entrada, mediante dispositivos de alimentación, para determinar la existencia de salvaguardas, diseñadas para prevenir la pérdida de datos e inexactitudes, debidas a errores de transmisión.	F-3.
4.	Determinar que existe evidencia adecuada de la autorización para operaciones accedidas mediante terminales de acceso directo, en línea o no en línea, ya sea en los medios originales en los que hizo el acceso o mediante listados de las operaciones que fueron autorizadas después del acceso, para antes del procesamiento definitivo.	F-3.
5.	Determinar, mediante comentarios y observación, que el personal del área de depósitos, involucrados en la función de procesamiento de datos poseen ejemplares de los manuales y que los supervisores vigilan su aplicación	F-3.
6.	Determinar mediante comentarios y observación, que existen capacitación y supervisión.	F-3.
7.	Determinar, mediante observación que los dígitos de verificación están siendo utilizados en los códigos clave que no se controlan en otra forma.	F-3.

PROCEDIMIENTOS DE VERIFICACION

PROCESO DE ENTRADA DE DATOS

No.	VERIFICACIONES	HECHO
1.	<p>Se evaluó mediante la observación y revisión física el diseño de formas, registro inicial en documentos, llenado y prenumerado, obteniendo el siguiente resultado:</p> <ul style="list-style-type: none"> ✓ Están diseñadas especialmente. ✓ Son identificadas eficientemente. ✓ Son llenadas adecuadamente. <p>Lo antes expuesto asegura razonablemente que las operaciones sean registradas completamente; es decir, desde el registro inicial, hasta su conversión a una forma sensible para la máquina, por el adecuado diseño de las mismas.</p>	HB
2.	<p>Mediante la indagación y observación se determinó que no existen manuales de usuario adecuados que sirvan de apoyo en el conocimiento de los sistemas en el área de depósitos. Lo que consecuentemente ocasiona que los usuarios no estén lo suficientemente familiarizados con el contenido de los mismos</p>	HB
3.	<p>Se indagó sobre los métodos de transmisión de los datos de entrada, siendo éstos transmitidos a través de la fibra óptica, por lo cual ofrece, la transmisión de datos a alta velocidad, en tiempo real, entre un número de estaciones separadas en distancias considerables.</p>	HB
4.	<p>Se determinó que existe una capacitación formal, completa y adecuada para los empleados, en virtud a establecerse que los mismos, tienen una comprensión general de las etapas previas o subsecuentes del procesamiento de datos, o de qué datos deben ser sometidos a autorización.</p>	HB

BANCO XYZ S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. F-3
Hecho por: HB
Fecha: 30.9.99

5. Se determinó que no se usan dígitos verificadores, para las cuentas de depósitos de ahorros y para las cuentas de depósitos a plazos, por lo que consecuentemente ocurren inconsistencias en las transacciones de las mismas.

HB

BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. F-4
Hecho por: HB
Fecha: 30.9.99

CEDULA DE DEFICIENCIAS ENCONTRADAS

- ✓ No existen manuales de usuario adecuados que sirvan de apoyo en el conocimiento de los sistemas utilizados en el área de depósitos.

- ✓ No se usan dígitos verificadores, para las cuentas de depósitos de ahorros y para las cuentas de depósitos a plazos, por lo que consecuentemente ocurren inconsistencias en las transacciones.

5.2.5.2 PROCESO EN COMPUTADOR

Esta fase consiste en el flujo invisible de los datos a través del computador y controles de:

- a. La lógica de la programación de cada proceso individual del computador, y
- b. Las interrelaciones en el computador, de los diferentes procesos relacionados con una misma aplicación.

Para su evaluación debe adquirirse una comprensión de dicha fase.

Objetivos de Control

- Asegurar que la totalidad de los datos sean procesados por el computador.
- Asegurar la exactitud de los datos procesados por el computador.
- Asegurar que todos los datos procesados por el computador estén debidamente autorizados.



BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. G-1
Hecho por: HB
Fecha: 30-9-99

CUESTIONARIO DE CONTROL INTERNO

PROCESO EN COMPUTADOR

PREGUNTAS	SI	NO	N/A
1. Se ponen en práctica procedimientos que aseguren que el equipo de computación esté funcionando correctamente y que las fallas de funcionamiento y los errores resultantes en los datos, sean detectados?	✓		
2. Hay procedimientos que garanticen que únicamente se utilizan los archivos correctos?	✓		
3. Se aplican procedimientos para asegurar que los cálculos del programa se realicen en forma correcta?	✓		
4. Existe un sistema de control sobre la operación física del sistema del computador?	✓		

PROGRAMA DE AUDITORIA

PROCESO EN COMPUTADOR.

No.	PROCEDIMIENTOS	REF.
1.	Determinar, mediante comentarios y revisión del programa formal de conversión y de los archivos maestros convertidos, que se ejercen adecuados controles sobre los archivos maestros importantes durante y después de su conversión.	G-3
2.	Examinar la documentación de la conciliación del grupo de control por un número apropiado de ciclos de procesamiento, inmediatamente después de la conversión, para determinar la evidencia de errores resultantes de una compilación defectuosa de los archivos maestros, su subsecuente corrección y posterior realimentación al sistema.	G-3
3.	Asegurarse, mediante un examen de la documentación de los programas, revisión de conciliaciones y uso de datos de prueba, que se han seguido los estándares de programación establecidos y que las características de control de programación disponibles han sido utilizadas.	G-3
4.	Asegurarse mediante observación y procedimientos documentados, de la existencia de controles para prevenir o detectar: acceso no autorizado a la documentación de los programas, modificación no autorizada de programas operativos, acceso no autorizado al computador e introducción de datos de entrada no autorizados.	G-3
5.	Asegurarse de la existencia de medidas para protección de los datos, relativas al acceso a los sistemas desde terminales remotas.	G-3
6.	Determinar por medio de pruebas, que solamente se pueden acceder datos e iniciar programas desde terminales remotas, sobre la base de una autorización previa.	G-3

BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. G-3
Hecho por: HB
Fecha: 30.9.99

PROCEDIMIENTOS DE VERIFICACION

PROCESO EN COMPUTADOR

No.	VERIFICACIONES	HECHO POR:	REF.
1.	Se estableció que los controles sobre los archivos maestros son adecuados, además las bibliotecas se nombran de manera estándar, logrando de esta manera tener un mejor control sobre las mismas.	HB	
2.	Derivado del análisis y comprobación de los menús de acceso a información del sistema que tiene asignado el personal del área de Depósitos, se observó que existen opciones que no corresponden a las funciones en las que cada empleado se desempeña; asimismo, se observó que el uso de terminales remotas en línea en el área de depósitos no está restringido por el uso apropiado de claves o contraseñas; es decir, que las claves o contraseñas son compartidas entre los empleados, lo cual puede ocasionar el ingreso de operaciones ficticias o inexactas, debido al acceso no autorizado. El acceso a la información debe estar restringido, de tal manera que cada persona cuente únicamente con la información necesaria para desempeñar las labores que tiene a su cargo.	HB	G-3-1
3.	El sistema calcula en las cuentas de depósitos de ahorro los intereses a pagar mensualmente. En los cambios de tasas de interés se determinó que el sistema aplica la tasa modificada para el mes completo; es decir, que no efectúa el cambio en la fecha de la modificación. En esa virtud el área de depósitos procede a efectuar los ajustes realizando el cálculo de manera manual por los días que el sistema no tomó en cuenta; dicho procedimiento por ser manual es sujeto de errores. Los programas de computación tienen que ser flexibles de manera que puedan soportar o permitir cambios, con el fin de disminuir el número de errores que puedan cometer.	HB	G-3-2

BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. G-3-1
Hecho por: HB
Fecha: 30.9.99

CEDULA DE VERIFICACION DE LOS NIVELES DE ACCESO

No.	DESCRIPCION	Enc. DM			Enc. AH			Enc. PF		
		DM	AH	PF	DM	AH	PF	DM	AH	PF
1.	Cambio de característica	✓	✓	✓	✓	✓	•	✓	✓	✓
2.	Datos personales.	✓	✓	✓	✓	✓	•	✓	✓	✓
3.	Cambia estado de inactiva.	✓	✓	✓	✓	✓	•	✓	✓	✓
4.	Cambia marca de embargo.	✓	✓	•	✓	✓	•	✓	✓	•
5.	Cambia forma de cálculo de intereses	✓	✓	•	✓	✓	•	✓	✓	•
6.	Cambia cálculo de intereses	✓	✓	✓	✓	✓	•	✓	✓	•
7.	Notas de cargo pendientes de anotar	✓	✓	•	•	•	•	✓	✓	•
8.	Notas de abono pendientes de anotar	✓	✓	•	•	•	•	•	•	•
9.	Intereses pendientes de anotar	✓	✓	•	•	•	•	•	•	•

Enc. DM = Encargado de la cartera de Cuentas de depósitos monetarios.
 Enc. AH = Encargado de la cartera de Cuentas de depósitos de ahorro.
 Enc. PF = Encargado de la cartera de Cuentas de depósitos a plazo.
 DM = Cartera de Cuentas de depósitos monetarios.
 AH = Cartera de Cuentas de depósitos e ahorros.
 PF = Cartera de Cuentas de Plazo Fijo.
 ✓ = Con acceso.
 • = Sin acceso.

Observación:

Derivado del análisis y comprobación de los menús de acceso a la información del sistema que tiene asignado el personal del área de Depósitos, se observó que existen opciones que no corresponden a las funciones en las que se desempeñan; asimismo, se observó que el uso de terminales remotas en línea en el área de depósitos no está restringido por el uso apropiado de claves, o contraseñas; es decir, que las claves o contraseñas son compartidas entre los empleados, lo cual puede ocasionar el ingreso de operaciones ficticias o inexactas, debido al acceso no autorizado.



BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. G-3-2
Hecho por: HB
Fecha: 30.9.99

CEDULA DE CAMBIO DE TASA DE INTERES EN EL SISTEMA

BANCO XYZ, S. A. Cuentas de Ahorro	
MANTENIMIENTO DE TASAS AUTORIZADAS.	
Número de cuenta:.....	
Tasa de interés:.....	
Fecha de cambio:.....	
INTRO=GRABA	F03=SALIR

Observación:

El sistema calcula en las cuentas de depósitos de ahorro los intereses a pagar mensualmente. En los cambios de tasas de interés se determinó que el sistema aplica la tasa modificada para el mes completo; es decir, que no efectúa el cambio en la fecha de la modificación. En esa virtud el área de Depósitos procede a efectuar los ajustes realizando el cálculo de manera manual por los días que el sistema no tomó en cuenta; dicho procedimiento por ser manual es sujeto de errores.

CEDULA DE DEFICIENCIAS ENCONTRADAS

- ✓ Derivado del análisis y comprobación de los menús de acceso a la información del sistema que tiene asignado el personal del área de Depósitos, se observó que existen opciones que no corresponden a las funciones en las que se desempeñan; asimismo, se observó que el uso de terminales remotas en línea en el área de depósitos no está restringido por el uso apropiado de claves, o contraseñas; es decir, que las claves o contraseñas son compartidas entre los empleados, lo cual puede ocasionar el ingreso de operaciones ficticias o inexactas, debido al acceso no autorizado.

- ✓ El sistema calcula en las cuentas de depósitos de ahorro los intereses a pagar mensualmente. En los cambios de tasas de interés se determinó que el sistema aplica la tasa modificada para el mes completo; es decir, que no efectúa el cambio en la fecha de la modificación. En esa virtud el área de depósitos procede a efectuar los ajustes realizando el cálculo de manera manual por los días que el sistema no tomó en cuenta; dicho procedimiento por ser manual es sujeto de errores.



5.2.5.3 PROCESO DE SALIDA

Esta fase representa el flujo de datos a partir del primer reporte producido o editado por el computador ya sea mediante pantalla, impresoras o cualquier otro dispositivo de salida de datos, e incluye asimismo la distribución y acceso de la información de los usuarios de la misma. Para su evaluación debe considerarse, y no limitarse a, lo siguiente:

Objetivos de Control

- Asegurarse de la exactitud de los resultados entregados a través de reportes.
- Asegurarse que los reportes de salida se están distribuyendo oportunamente, y a los usuarios indicados.

CUESTIONARIO DE CONTROL INTERNO**PROCESO DE SALIDA**

PREGUNTAS	SI	NO	N/A
1. Hay procedimientos para asegurar que todos los errores significativos que fueron identificados en diferentes etapas del sistema, han sido corregidos y realimentados, y adecuadamente reflejados en los datos de salida?	✓		
2. Existen procedimientos que aseguren que todos los datos de salida requeridos, se entreguen a los usuarios autorizados?		✓	

BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. H-2
Hecho por: HB
Fecha: 30.9.99

PROGRAMA DE AUDITORIA

PROCESO DE SALIDA.

No.	PROCEDIMIENTOS	REF.
1.	Examinar los procedimientos relativos a las partidas rechazadas (errores), para determinar que son adecuadamente registradas y que se toman provisiones para asegurar su reentrada, una vez que se les han hecho las correcciones necesarias.	H-3
2.	Determinar mediante comentarios y examen de los documentos de la conciliación, que las cifras de control se están conciliando debidamente.	H-3
3.	Hacer pruebas de cálculo de las cifras de control generadas por computador, mediante el uso de datos de prueba y/o programas generalizados de auditoria.	H-3
4.	Determinar a través de comentarios con los usuarios e inspección de la documentación de sus conciliaciones, que éstas son adecuadas y toman en consideración la recepción de todos los reportes importantes.	H-3
5.	Determinar mediante comentarios e inspección de la documentación de los sistemas y bitácoras del grupo de control, que los reportes de salida se están distribuyendo oportunamente a los usuarios indicados.	H-3

PROCEDIMIENTOS DE VERIFICACION
PROCESO DE SALIDA

No.	VERIFICACIONES	HECHO POR:	REF.
1.	Se determinó que los listados generados a diario por el centro de cómputo no son entregados de manera formal al área de depósitos. El no mantener controles adecuados sobre la distribución de reportes puede tener resultados radicalmente impredecibles, pueden omitirse asientos contables importantes, las excepciones serias pueden continuar sin resolverse, o puede hacerse uso indebidos de los documentos.	HB	
2.	Se determinó que se usan cifras de control, para la salida de información a través de reportes; sin embargo, aparecen registradas inadecuadamente, según lo observado en los reportes de la cartera de depósitos monetarios, donde no coincide el total del número de depósitos con el valor en conjunto de los mismos, consecuentemente puede ocurrir que no estén completos los datos procesados o que hayan inexactitudes en los mismos.	HB	H-3-1

BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. H-3-1
Hecho por: HB
Fecha: 30.9.99

CEDULA DE VERIFICACION DEL USO DE CIFRAS DE CONTROL

LISTADO POR LEGAJOS.
CARTERA DE DEPOSITOS MONETARIOS.

No	Cuenta No.	Nombre	Depósitos
1.	02-220525-3	Sandra Pérez López	Q. 15,000.00
2.	01-752852-6	Maria Isabel Morales	Q. 2,000.00
3.	01-325322-8	Rodolfo López Corzo	Q. 4,000.00
4.	51-471455-5	Maria José Morales Sosa	Q. 300.00
	Total		Q. 21,300.00

Total de documentos: 8 por valor de Q. 21,000.00

Observación:

El listado antes indicado tiene registrados 4 documentos, para un total de Q. 21,300.00; sin embargo, el listado en su resumen tiene consignado 8 registros, como cifra de control.

Se determinó que se usan cifras de control, para la salida de información a través de reportes; sin embargo, aparecen registradas inadecuadamente, según lo observado en los reportes de la cartera de depósitos monetarios, donde no coincide el total del número de depósitos con el valor en conjunto de los mismos, consecuentemente puede ocurrir que no estén completos los datos procesados o que hayan inexactitudes en los mismos.

CEDULA DE DEFICIENCIAS ENCONTRADAS

- ✓ Se determinó que los listados generados a diario por el centro de cómputo no son entregados de manera formal al área de depósitos. El no mantener controles adecuados sobre la distribución de reportes puede tener resultados radicalmente impredecibles, pueden omitirse asientos contables importantes, las excepciones serias pueden continuar sin resolverse, o puede hacerse uso indebidos de los documentos.

- ✓ Se usan cifras de control, para la salida de información a través de reportes; sin embargo, aparecen registradas inadecuadamente, según se observe en la cartera de depósitos monetarios, donde no coincide el total del número de depósitos con el valor en conjunto de los mismos, consecuentemente puede ocurrir que no estén completos los datos procesados o que hayan inexactitudes.

BANCO XYZ, S. A.
AUDITORIA DE INFORMATICA
AREA DE DEPOSITOS

P. T. I
Hecho por: HB
Fecha: 30.9.99

5.2.6 INFORME DE LA AUDITORIA

Guatemala, 2 de octubre de 1999.

Ref.: Auditoría de Informática, en el Area de Depósitos.

*Señor
Gerente General
Banco XYZ, S.A.
Ciudad de Guatemala.*

De nuestra consideración:

Como parte de nuestra revisión en las áreas de la institución, se realizó la evaluación de la función de informática correspondiente al área de depósitos, comprendida por el periodo del 1 de julio al 30 de septiembre de 1999, efectuamos un diagnóstico desde el punto de vista de informática, con el alcance que consideramos necesario de la información que genera el centro de procesamiento de datos, denominado Datacentro, S. A. Nuestra evaluación no debe considerarse como un estudio detallado de los sistemas y, por lo tanto, no revela todas las posibles deficiencias de los mismos; sin embargo, observamos las situaciones que se detallan en el apartado de resultados, las cuales deben ser analizadas con la finalidad de adoptar las medidas correctivas necesarias.

I. ALCANCE

Se realizó una evaluación de la función de informática, para detectar las operaciones que están expuestas a mayores riesgos o debilidades, enmarcada específicamente en el área de depósitos, del Banco XYZ, S. A., comprendiendo el periodo del 1 de julio al 30 de septiembre de 1999.

II. RESULTADOS

De conformidad con el trabajo de Auditoria realizado, se obtuvo el siguiente resultado:

Observación

- No existen manuales de usuario adecuados que sirvan de apoyo en el conocimiento de los sistemas utilizados en el área de depósitos.

Recomendación

Solicitar al proveedor de sistemas la documentación necesaria que facilite la labor de los usuarios.

Observación

- No se usan dígitos verificadores, para las cuentas de depósitos de ahorros y para las cuentas de depósitos a plazos, por lo que consecuentemente ocurren inconsistencias en las transacciones de las mismas.

Recomendación

Se sugiere implementar controles preventivos a través del dígito verificador, en las cuentas de depósitos de ahorros y en las de depósitos a plazos, con el propósito de minimizar el riesgo de errores e irregularidades en la captura de la información.

Observación

- Derivado del análisis y comprobación de los menús de acceso a la información del sistema que tiene asignado el personal del área de Depósitos, se observó que existen opciones que no corresponden a las funciones en las que se desempeñan; asimismo, se observó que el uso de terminales remotas en línea en el área de depósitos no está restringido por el uso apropiado de claves, o contraseñas; es decir, que las claves o contraseñas son compartidas entre los empleados, lo cual puede ocasionar el ingreso de operaciones ficticias o inexactas, debido al acceso no autorizado.



Recomendación

Se sugiere que el acceso a la información o a procesos en el área de depósitos, esté debidamente controlada a través del uso adecuado de las claves o contraseñas; las cuales deben ser conocidas únicamente por la persona autorizada; por lo cual, su uso debe ser personal e intransmisible.

Observación

- *El sistema calcula en las cuentas de depósitos de ahorro los intereses a pagar mensualmente. En los cambios de tasas de interés se determinó que el sistema aplica la tasa modificada para el mes completo; es decir, que no efectúa el cambio en la fecha de la modificación. En esa virtud el área de depósitos procede a efectuar los ajustes realizando el cálculo de manera manual por los días que el sistema no tomó en cuenta; dicho procedimiento por ser manual es sujeto de errores.*

Recomendación

Los programas de computación tienen que ser flexibles de manera que puedan soportar o permitir cambios, con el fin de disminuir el número de errores que puedan cometer, por lo que se sugiere que el referido procedimiento se automatice.

Observación

- *Se usan cifras de control, para la salida de información a través de reportes; sin embargo, aparecen registradas inadecuadamente, según lo observado en los reportes de la cartera de depósitos monetarios, donde no coincide el total del número de depósitos con el valor en conjunto de los mismos, consecuentemente puede ocurrir que no estén completos los datos procesados o que hayan inexactitudes en los mismos.*

Recomendación

Se estima conveniente evaluar la inconsistencia reflejada en los reportes correspondientes a la cartera de depósitos monetarios, con la finalidad de minimizar el riesgo antes indicado, optimizando de esta manera los controles detectivos implementados.

Observación

- Se determinó que los listados generados a diario por el centro de cómputo no son entregados de manera formal al área de depósitos. El no mantener controles adecuados en la distribución de reportes puede tener resultados radicalmente impredecibles, pueden omitirse asientos contables importantes, las excepciones serias pueden continuar sin resolverse, o puede hacerse uso indebidos de los documentos.

Recomendación

Se sugiere mantener un control adecuado en la distribución de reportes, debido a que muchos reportes tienen un propósito especial y son de naturaleza confidencial, la seguridad en su distribución es un aspecto delicado, intensificando esta preocupación, se encuentra el hecho de que algunos reportes, pueden ser de gran valor para personas ajenas a la institución, particularmente para la competencia.

III. CONCLUSION

Derivado de la evaluación realizada desde el punto de vista de informática en el área de Depósitos, se concluye que en conjunto la misma se presenta razonablemente; a excepción, de las objeciones manifestadas anteriormente.

IV. RECOMENDACION

Se estima conveniente que las observaciones antes indicadas se analicen con el propósito de mejorar los controles existentes en el área de Depósitos, adoptando a su vez, medidas correctivas para cada caso específico; en tal virtud, se trasladan para su conocimiento y seguimiento oportuno.

Atentamente,



Hilda de María Berganza Garza.
Auditor de Informática.

c. c. archivo

CONCLUSIONES

1. El sistema bancario está conformado por todas aquellas instituciones que sirven de intermediarios financieros entre oferentes y demandantes de capital, y que contribuyen al desarrollo de la economía del país, realizan operaciones activas, pasivas y de confianza; las operaciones pasivas están constituidas por aquellas operaciones que implican la captación de recursos financieros en calidad de depósitos a la vista, depósitos de ahorros y depósitos a plazo, creando una obligación para la institución.
2. La auditoría interna ayuda a la administración a alcanzar sus metas y objetivos con mayor eficacia, al proporcionarle en forma oportuna, información, análisis, evaluaciones, comentarios y recomendaciones pertinentes sobre las operaciones que examina.
3. El proceso de planeación de la auditoría de informática comprende la configuración de criterios para orientar las decisiones fundamentales y la identificación de las formas o maneras de llevar adelante las actividades necesarias para alcanzar los objetivos, hace necesario como en cualquier actividad, preparar un plan de trabajo, el cual debe ser flexible, considerando en el mismo un margen de tolerancia, en función de que las circunstancias son cambiantes.

4. El trabajo del auditor al realizar una auditoría de informática, en primera instancia contempla un estudio inicial de la situación general, aunque la auditoría a realizar sea solamente a un área específica. Para realizar dicho estudio, toma en cuenta, lo siguiente:

- ✓ Métodos utilizados por la entidad para el procesamiento de datos.
- ✓ Medida en que se utiliza el computador en cada aplicación dependiendo de la complejidad de las operaciones.
- ✓ La estructura organizacional de las actividades de procesamiento de datos.
- ✓ Riesgos a los que están expuestas las operaciones.
- ✓ Evaluación de Controles.

5. El plan de trabajo, tomando como base un Sistema de Evaluación de Riesgos, tiene como propósito asignar los recursos de auditoría a las áreas de mayor riesgo en la organización.

6. La hipótesis planteada en el plan de investigación, con relación a que en el terreno de los sistemas de información y tecnología, un alto porcentaje de las instituciones financieras tienen problemas en el manejo y control de la información que almacenan, procesan y distribuyen, así como los aspectos que el Auditor Interno tiene que evaluar al efectuar un diagnóstico desde el punto de vista de la función de informática, para detectar las operaciones que están expuestas a mayores riesgos o debilidades, y planificar, en la actualidad, una auditoría de informática en un banco privado guatemalteco, se concluye que la misma es confirmada, según los resultados obtenidos en el trabajo de Auditoría de Informática, realizado en el área de depósitos, y los cuales se detallan en el informe de auditoría expuesto en el caso práctico.

RECOMENDACIONES

1. Se sugiere que la auditoría interna evalúe si está cumpliendo con su función de ayudar a la administración a alcanzar sus metas y objetivos con mayor eficacia, al proporcionarle en forma oportuna, información, análisis, evaluaciones, comentarios y recomendaciones pertinentes sobre las operaciones que examina.
2. Con la finalidad de enfocar el trabajo de auditoría interna, al efectuar un diagnóstico desde el punto de vista de la función de informática, para detectar las operaciones que están expuestas a mayores riesgos o debilidades en una institución bancaria, se sugiere que el proceso de planeación de la auditoría de informática, comprenda la configuración de criterios para orientar las decisiones fundamentales y la identificación de las formas o maneras de llevar adelante las actividades necesarias para alcanzar los objetivos, preparar un plan de trabajo, el cual debe ser flexible, considerando en el mismo un margen de tolerancia, en función de que las circunstancias son cambiantes.
3. Se sugiere que el trabajo del auditor al realizar una auditoría de informática, contemple un estudio inicial de la situación general, aunque la auditoría a realizar sea solamente a un área específica. Para realizar dicho estudio debe tomarse en cuenta lo siguiente:
 - ✓ Métodos utilizados por la entidad para el procesamiento de datos.
 - ✓ Medida en que se utiliza el computador en cada aplicación dependiendo de la complejidad de las operaciones.
 - ✓ La estructura organizacional de las actividades de procesamiento de datos.
 - ✓ Riesgos a los que están expuestas las operaciones.
 - ✓ Evaluación de Controles.

4. El plan de trabajo, tomando como base un Sistema de Evaluación de Riesgos, tiene como propósito asignar los recursos de auditoría a las áreas de mayor riesgo en la organización, por lo que se recomienda que se consideren objetivos específicos como:

- ✓ Identificar de una forma técnica y sistemática las áreas de mayor riesgo en la organización.
- ✓ Evaluar las distintas áreas de la Organización sobre una base común.
- ✓ Identificar las áreas de mayor exposición al riesgo.
- ✓ Asignar los recursos de Auditoría Interna a las áreas de mayor riesgo.
- ✓ Evaluar la adecuación de los controles existentes para asegurarse de la justificación de su dependencia.
- ✓ Proponer la implementación de controles adecuados o mejoras a los ya establecidos, que coadyuven a minimizar los riesgos asociados a las operaciones examinadas.

BIBLIOGRAFIA

1. Achata Iturmendi, Jose. Auditoria Informática en la Empresa, Editorial Paraninfo, S. A. Magallanes, Madrid, España 1994.
2. Careño, Manuel. Seminario de Auditoría y Control de Sistemas de Información, Guatemala, noviembre 1997.
3. Comisión de Auditoría Interna, Guía de Auditoría Interna, No. 14, Instituto Guatemalteco de Contadores Públicos y Auditores. Guatemala, mayo 1999.
4. Instituto de Auditores Internos, Seminario Controles que Agregan Valor al Negocio: La Manera Correcta de Manejar los Riesgos. Guatemala, septiembre 1999.
5. Ley de Bancos, Decreto 315 del Congreso de la República.
6. Ley Monetaria, Decreto 203 del Congreso de la República.
7. Ley Orgánica del Banco de Guatemala, Decreto 215 del Congreso de la República.
3. Li, David H. Auditoría de Centros de Cómputos, México, enero 1990.
9. Méndez, Byron. Seminarios de Auditoría Interna; Instituto Guatemalteco de Contadores Públicos y Auditores. Guatemala, mayo 1998.
10. Rodríguez Azuero, Sergio. Contratos Bancarios; 2da. Edición, Bogotá, Felaban, 1979.
11. Turk Mejía, Luis Alfredo. Tesis: Evaluación y clasificación de activos en los Bancos del Sistema. Facultad de Ciencias Económicas, Universidad de San Carlos de Guatemala, noviembre 1992.
12. Ziegler, Kell. Auditoria Moderna, Compañía Editorial Continental, México, 1995.