UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS

"AUDITORIA INTERNA EN EL DEPARTAMENTO DE INFORMÁTICA DE UNA INSTITUCIÓN BANCARIA"

TESIS

PRESENTADA A LA JUNTA DIRECTIVA DE LA
FACULTAD DE CIENCIAS ECONÓMICAS

POR

EDWING ERNESTO RAMOS ROSALES

PREVIO A CONFERIRSELE EL TÍTULO DE
CONTADOR PÚBLICO Y AUDITOR
EN EL GRADO ACADÉMICO DE

LICENCIADO

GUATEMALA, NOVIEMBRE DE 2007

JUNTA DIRECTIVA DE LA FACULTAD DE CIENCIAS ECONÓMICAS

Decano	Lic. José Rolando Secaida Morales.
Secretario	Lic. Carlos Roberto Cabrera Morales.
Vocal I	Lic. Canton Lee Villela.
Vocal II	Lic. Mario Leonel Perdomo Salguero.
Vocal III	Lic. Juan Antonio Gómez Monterroso.
Vocal IV	S.B. Roselyn Janette Salgado Ico.
Vocal V	P.C. Deiby Boanerges Ramírez Valenzuela.

PROFESIONALES QUE REALIZARON

LOS EXÁMENES DE ÁREAS PRÁCTICAS

Auditoría	Lic. Rubén Eduardo Del Aguila Rafael
Matemática Estadística	Lic. José De Jesús Portillo
Contabilidad	Lic. Jorge Luis Reyna Pineda

PROFESIONALES QUE REALIZARON

EL EXAMEN PRIVADO DE TESIS

Presidente	Lic. Albaro Joel Girón Barahona
Examinador	Lic. Jorge Luis Reyna Pineda
Examinador	Lic. Erick Roberto Flores López

ORDEN DE IMPRESIÓN

DEDICATORIA

A Dios	Que me dio con su infinita bondad y amor, salud, fuerza y dedicación para alcanzar mi sueño.
A mis padres	**Marco Tulio Ramos y Maria Luisa Rosales** Quienes con su ejemplo de lucha y esfuerzo me apoyaron para alcanzar esta meta. Agradecimiento eterno.
A mis hermanos	**Maynor, Silvia y Marco,** con mucho aprecio y cariño.
A mis amigos	Con aprecio.
A mi asesora de tesis	**Licda. Cotty Mayary García Alburez** Por su asesoría y orientación en la elaboración del presente trabajo.
A la Universidad de San Carlos de Guatemala	Por hacer de mi un profesional capaz y útil a la sociedad.

CONTENIDO

CAPÍTULO V

CASO PRÁCTICO DE UNA AUDITORÍA EFECTUADA AL CENTRO DE PROCESAMIENTO DE INFORMACIÓN DEL DEPARTAMENTO DE INFORMÁTICA DE UNA INSTITUCIÓN BANCARIA

INDICE DE CUADROS

CONCLUSIONES Y RECOMENDACIONES

INTRODUCCIÓN

La Auditoría en Informática es la revisión y evaluación de los controles, sistemas y procedimientos establecidos en el departamento de Informática de una organización, para la utilización de tecnología de información. Esto con la finalidad de rendir informes oportunos a la administración de la institución si se detectan riesgos importantes y las medidas que el auditor de sistemas estime ayudarán a minimizarlos.

El presente trabajo fue enfocado a la Auditoría de Sistemas de Información de una institución bancaria privada guatemalteca, específicamente a la seguridad física del Centro de Procesamiento de Información.

La hipótesis de la investigación se enfocó en la dependencia que tienen las instituciones bancarias a la utilización de la tecnología de información, así como a la importancia de que la Auditoría Interna cuente con personal con conocimientos suficientes para realizar la labor de supervisión y asesoría de la forma de utilización de ésta para establecer que está siendo gestionada adecuadamente.

Derivado de las investigaciones y análisis efectuados se logró comprobar la hipótesis, derivado que las instituciones bancarias tienen una alta dependencia al proceso electrónico de datos, buscando siempre la optimización de sus procesos y el uso de los continuos avances tecnológicos. De la misma manera se estableció que el departamento de Auditoría Interna debe de contar con personal con conocimientos sólidos de los diferentes riesgos que afectan a un departamento de informática y las recomendaciones que permitan minimizarlos.

En el capítulo uno se presentan las generalidades del sistema financiero guatemalteco, formas de organización, las leyes que lo regulan, ente supervisor, los aspectos regulados en las leyes financieras, las principales ventas, fusiones, adquisiciones, compras y liquidaciones de bancos efectuados a partir de la aprobación de las leyes en el año 2002.

En el capítulo dos se expone la organización y funciones de un departamento de Informática. Los principales riesgos que afectan el uso de tecnología de información, además los conocimientos necesarios con los que debe de contar el personal del departamento de Informática, como parte importante del trabajo realizado se presentan la seguridad lógica y física con las que deberá contar un departamento de Informática para salvaguardar la información, los equipos y el personal asignado.

En el capítulo tres se analizan los conceptos de Auditoría de sistemas de información, el alcance, la importancia, las funciones, objetivos y los procedimientos a observar en las revisiones. Además se presenta el contenido de la norma internacional No. 401 “Auditoría en un ambiente de sistemas de información computarizado.

El capítulo cuatro trata de la metodología para realizar una Auditoría de sistemas de información. Para una adecuada exposición la metodología se divide en planeación, ejecución e informe del trabajo efectuado.

En este capítulo además se presentan las mejores prácticas internacionalmente recopiladas, contenidas en las metodologías internacionales para realizar Auditoría de sistemas de información.

En el capítulo cinco se expone un caso práctico de una Auditoría al Centro de Procesamiento de Información del departamento de Informática de una institución bancaria. El Centro de Procesamiento de Información de una entidad bancaria es el espacio físico dentro del departamento de Informática donde están asignados los equipos y sistemas computacionales más sensibles. Como se expone en este capítulo existen varios riesgos que les podrían afectar, así mismo se enumeran las conclusiones y recomendaciones del caso práctico.

Finalmente se presentan las conclusiones y recomendaciones obtenidas de la presente tesis.

CAPÍTULO I
LAS INSTITUCIONES BANCARIAS

1.1 Definición de institución bancaria

1.1.1 Banco

Es una institución financiera de intermediación que recibe fondos en forma de depósitos de las personas que poseen excedentes de liquidez, utilizándolos posteriormente para operaciones de préstamo a personas individuales o jurídicas con necesidades de financiamiento, o para realizar sus propias inversiones, principalmente en valores emitidos por el gobierno y/o entidades privadas.

Adicionalmente realiza actividades de compra y venta de moneda extranjera, cobros por cuenta ajena, venta de cheques de caja o gerencia, pago de impuestos y otros**. (11:1)**

1.1.2 Objeto de las instituciones bancarias

La función principal de los bancos es captar dinero de las personas con excedentes de liquidez para proporcionarlo a aquellas que necesitan financiamiento.

Esta actividad está regulada en el artículo No. 3 del decreto 19-2002 Ley de Bancos y Grupos Financieros donde se indica lo siguiente: Intermediación financiera bancaria. **"Los bancos autorizados conforme a esta Ley o leyes específicas podrán realizar intermediación financiera bancaria, consistente en la realización habitual, en forma pública o privada, de actividades que consistan en la captación de dinero, o cualquier instrumento representativo del mismo, del público, tales como la recepción de depósitos, colocación de bonos, títulos u otras obligaciones, destinándolo al financiamiento de cualquier naturaleza, sin importar la forma jurídica que adopten dichas captaciones y financiamientos". (5:19)**

1.1.3 Operaciones que realizan los bancos

Las operaciones y servicios que pueden realizar los bancos se indican en el artículo No. 41 del decreto 19-2002 Ley de Bancos y Grupos Financieros, son:

- **Operaciones pasivas**

  Son aquellas de las cuales nace mediata o inmediatamente una obligación para el banco, es una exigibilidad a la vista o a plazo y también se pueden operar en moneda nacional o extranjera, estas son:

  - Recibir depósitos monetarios;
  - Recibir depósitos a plazo;

- Recibir depósitos de ahorro;
- Crear y negociar bonos y/o pagarés, previa autorización de la Junta Monetaria;
- Obtener financiamiento del Banco de Guatemala, conforme la ley orgánica de éste;
- Obtener créditos de bancos nacionales y extranjeros;
- Crear y negociar obligaciones convertibles;
- Crear y negociar obligaciones subordinadas; y
- Realizar operaciones de reporto como reportado.

➢ **Operaciones activas**

Son aquellas operaciones de las cuales surge un derecho a ejercer por parte del banco contra terceros, las cuales se pueden efectuar en moneda nacional o extranjera, a continuación se indican:

- Otorgar créditos;
- Realizar descuento de documentos;
- Otorgar financiamiento en operaciones de cartas de crédito;
- Conceder anticipos para exportación;
- Emitir y operar tarjeta de crédito;
- Realizar arrendamiento financiero;
- Realizar factoraje;
- Invertir en títulos valores emitidos y/o garantizados por el Estado, por los bancos autorizados de conformidad con esta ley o por entidades privadas. En el caso de la inversión en títulos valores emitidos por entidades privadas, se requerirán aprobación previa de la Junta Monetaria;
- Adquirir y conservar la propiedad de bienes inmuebles o muebles, siempre que sean para su uso, sin perjuicio de lo previsto en la literal f anterior;
- Constituir depósitos en otros bancos del país y en bancos extranjeros; y
- Realizar operaciones de reporto como reportador.

➢ **Operaciones de confianza**

Son aquellas operaciones realizan mediante contratos firmados entre el banco y sus clientes, donde se estipulan las condiciones mediante las cuales se prestarán las operaciones. A continuación se describen:

- Cobrar y pagar por cuenta ajena;
- Recibir depósitos con opción de inversiones financieras;
- Comprar y vender títulos valores por cuenta ajena; y

- Servir de agente financiero, encargándose del servicio de la deuda, pago de intereses, comisiones y amortizaciones.

➢ **Pasivos contingentes**

Los pasivos contingentes son aquellos que podrían derivar en una obligación para el banco por la adopción de:

- Otorgar garantías;
- Prestar avales;
- Otorgar fianzas; y
- Emitir o confirmar cartas de crédito.

➢ **Servicios**

Adicionalmente a las operaciones indicadas anteriormente los bancos podrán prestar los siguientes servicios:

- Actuar como fiduciario;
- Comprar y vender moneda extranjera, tanto en efectivo como en documentos;
- Apertura de cartas de crédito;
- Efectuar operaciones de cobranza;
- Realizar transferencia de fondos; y
- Arrendar cajillas de seguridad.

La Junta Monetaria podrá, previa opinión de la Superintendencia de Bancos, autorizar a los bancos a realizar otras operaciones y prestar otros servicios que no estén contemplados en esta Ley siempre y cuando los mismos sean compatibles con su naturaleza. (5:29)

1.2 Clasificación de las instituciones bancarias

Por el tipo de operaciones los bancos pueden dividirse en:

1.2.1 Banco central

Banco de un país encargado de emitir la moneda nacional, regular el mercado monetario y de divisas así como ejecutar las políticas gubernamentales en lo referente a medidas monetarias y financieras.

En Guatemala el banco central se llama Banco de Guatemala y funciona bajo la dirección suprema de la Junta Monetaria.

Según el artículo No. 3 de Decreto No. 16-2002, Ley Orgánica del Banco de Guatemala, el objetivo fundamental del Banco de Guatemala es: **"contribuir a la creación y mantenimiento de las condiciones más favorables al desarrollo ordenado de la economía nacional, para lo cual, proporcionará las condiciones monetarias, cambiarias y crediticias que promuevan la estabilidad en el nivel general de los precios." (5:19)**

1.2.2 Banco comercial

Institución financiera que se dedica a recibir dinero en depósito y darlo a su vez en préstamo. Se consideran además todas las operaciones que natural y legalmente constituyen el giro bancario. **(11:12)**

1.2.3 Banco hipotecario

Institución financiera que se dedica al negocio de recibir dinero en depósito y darlo a su vez en préstamo, sea en forma de mutuo, de descuento de documentos o de cualquier otra forma. Se diferencia de los bancos comerciales porque sus principales operaciones pasivas están relacionadas con la concesión de préstamos hipotecarios. **(11:12)**

Así mismo por la propiedad del capital los bancos pueden dividirse de la siguiente manera:

1.2.4 Bancos estatales

Cuando el accionista mayoritario es el gobierno. **(11:16)**

1.2.5 Bancos privados

Cuando los accionistas mayoritarios corresponden a la iniciativa privada. **(11:16)**

1.2.6 Bancos mixtos

Cuando existe división de las acciones entre el gobierno y la iniciativa privada en partes proporcionalmente iguales. **(11:16)**

Adicionalmente, por el origen del capital los bancos pueden dividirse en:

1.2.7 Bancos nacionales

Cuando el capital proviene de inversionistas guatemaltecos. **(11:17)**

1.2.8 Bancos extranjeros

Cuando el capital proviene fuera de Guatemala. **(11:17)**

1.3 El sistema financiero guatemalteco

1.3.1 Objetivo

El objetivo principal de las instituciones financieras es la de obtener beneficios a través de la intermediación financiera.

El artículo No. 01 del decreto 19-2002 Ley de Bancos y Grupos Financieros indica lo siguiente:

"Los bancos autorizados conforme a esta Ley o leyes específicas podrán realizar intermediación financiera bancaria, consistente en la realización habitual, en forma pública o privada, de actividades que consistan en la captación de dinero, o cualquier instrumento representativo del mismo, del público, tales como la recepción de depósitos, colocación de bonos, títulos u otras obligaciones, destinándolo al financiamiento de cualquier naturaleza, sin importar la forma jurídica que adopten dichas captaciones y financiamientos". (5:18)

1.3.2 Legislación vigente

Para regular las actividades que realizan las entidades financieras, en el primer semestre del año dos mil dos se autorizaron las leyes financieras que sustituyeron la legislación bancaria vigente desde el año 1945.

La Ley de Bancos está basada en los principios emitidos por el Comité de Basilea sobre Supervisión Bancaria.

El Comité de Basilea sobre supervisión bancaria es un organismo que fue creado en el año de 1975 por los presidentes de los bancos centrales de Bélgica, Canadá, Francia, Italia, Japón, Luxemburgo, Holanda, Suecia, Suiza, Inglaterra y los Estados Unidos. Este comité tiene como objetivo principal el mejoramiento de la supervisión bancaria en sus países miembros.

La actualización total de la legislación financiera nacional por parte del Congreso de la República de Guatemala derivó en la aprobación de las siguientes leyes: Ley Orgánica del Banco de Guatemala, Decreto No. 16-2002; Ley Monetaria, Decreto Número 17-2002; Ley de Supervisión Financiera, Decreto 18-2002; y Ley de Bancos y Grupos Financieros, Decreto Número 19-2002, mismas que cobraron vigencia el 1 de junio de 2002, Ley para prevenir el Lavado de Dinero u Otros Activos Decreto 67-2001 y la Ley para prevenir y reprimir el financiamiento al Terrorismo Decreto 58-2005.

1.3.3 Principales aspectos regulados en la Ley de Bancos y Grupos Financieros

Para minimizar los riesgos a que se encuentran expuestas las instituciones bancarias, el decreto No. 19-2002 Ley de Bancos y Grupos Financieros contempla la implementación de varias regulaciones, las cuales incorporan muchas de las recomendaciones del Comité de Basilea. A continuación se indican las principales:

- **Adquisición de acciones (artículo No. 19)**

  Las personas que adquieran directa o indirectamente una participación igual o mayor al cinco por ciento (5%) del capital pagado de un banco, deberán contar con la autorización de la Superintendencia de Bancos, quien verificará el cumplimiento de los requisitos para accionistas de nuevas entidades bancarias. **(5:23)**

- **Consejo de administración y gerencia (artículo No. 20)**

  Los bancos deberán tener un consejo de administración integrado por tres o más administradores, quienes serán los responsables de la dirección general de los negocios de los mismos. **(5:24)**

- **Deberes y atribuciones del consejo de administración (artículo No. 21)**

  El consejo de administración, sin perjuicio de las demás disposiciones legales y contractuales que le sean aplicables, tendrá los deberes y atribuciones siguientes:

  - Ser responsable de la liquidez y solvencia del banco;
  - Definir la política financiera y crediticia del banco y controlar su ejecución;
  - Velar porque se implementen e instruir para que se mantengan en adecuado funcionamiento y ejecución, las políticas, sistemas y procesos que sean necesarios para una correcta administración, evaluación y control de riesgos;
  - Velar porque las operaciones activas y contingencias no excedan los límites establecidos en la ley;
  - Conocer y disponer lo que sea necesario para el cumplimiento y ejecución de las medidas de cualquier naturaleza que la Junta Monetaria o la Superintendencia de Bancos, en el marco de sus respectivas competencias, dispongan en relación con el banco;
  - Conocer los estados financieros mensuales y aprobar los estados financieros anuales de la entidad bancaria y del grupo financiero, en su caso, los cuales deben estar respaldados por Auditoría interna, y anualmente, por el informe de los auditores externos, con su correspondiente dictamen y notas a los estados financieros. Así como resolver sobre las recomendaciones derivadas de los mismos; y
  - En general cumplir y hacer cumplir las disposiciones y regulaciones que sean aplicables al banco. **(5:24)**

- **Grupos financieros (artículo No. 27)**

  Grupo financiero es la agrupación de dos o más personas jurídicas que realizan actividades de naturaleza financiera, de las cuales una de ellas deberá ser banco, entre las cuales existe control común por relaciones de propiedad, administración o uso de imagen corporativa, o bien sin existir estas relaciones, según acuerdo, deciden el control común por relaciones de propiedad, administración o uso de imagen corporativa, o bien sin existir estas relaciones, según acuerdo, deciden el control común. **(5:25)**

- **Empresa controladora o empresa responsable (artículo No. 32)**

  El objeto social exclusivo de la empresa controladora será la dirección, administración, control, y representación del grupo financiero. **(5:27)**

- **Empresas especializadas en servicios financieros y de apoyo al giro bancario. (artículo No. 36)**

  Las empresas de apoyo al giro bancario son aquellas que, sin asumir riesgo crediticio alguno, prestan a los bancos los servicios de cajeros automáticos, procesamiento electrónico de datos u otros servicios calificados por la Junta Monetaria, previo dictamen de la Superintendencia de Bancos. **(5:28)**

- **Concesión de financiamiento. (artículo No. 50)**

  Los bancos, antes de conceder financiamiento, deben cerciorarse razonablemente que los solicitantes tengan la capacidad de generar flujos de fondos suficientes para atender el pago oportuno de sus obligaciones dentro del plazo del contrato. Así mismo, deberán hacer un seguimiento adecuado a la evolución de la capacidad de pago del deudor o deudores durante la vigencia del financiamiento. **(5:33)**

- **Valuación de activos, contingencias y otros instrumentos financieros. (artículo No. 53)**

  Los bancos y las empresas del grupo financiero que otorguen financiamiento deben valuar sus activos, operaciones contingentes y otros instrumentos financieros que impliquen exposiciones a riesgos, de conformidad con la normativa correspondiente. Los bancos y en su caso, las empresas de grupo financiero, deben constituir, contra los resultados del ejercicio, las reservas o provisiones suficientes, conforme la valuación realizada. **(5:33)**

- **Riesgos (artículo No. 55)**

  Los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, según sea el caso, la administración, de riesgos de crédito, de mercado, de tasas de interés, de liquidez, cambiario, de transferencia, operacional y otros a que estén expuestos. **(5:34)**

- **Políticas administrativas (artículo No. 56)**

  Los bancos y las empresas que integran grupos financieros deben contar con políticas escritas actualizadas, relativas a la concesión de créditos, inversiones, evaluación de la calidad de activos, suficiencia de provisiones para pérdidas y en general, políticas para una adecuada administración de los diversos riesgos a que están expuestos. Asimismo, deben contar con políticas, prácticas y procedimientos que les permitan tener un conocimiento adecuado de sus

clientes, con el fin de que los bancos y grupos financieros no sean utilizados para efectuar operaciones ilícitas. **(5:35)**

- **Control interno (artículo No. 57)**

  Los bancos y las empresas que integran grupos financieros deben mantener un sistema de control interno adecuado a la naturaleza y escala de sus negocios, que incluya disposiciones claras y definidas para la delegación de autoridad y responsabilidad, separación de funciones, desembolso de sus fondos, la contabilización de sus operaciones, salvaguarda de sus activos, y una apropiada Auditoría interna y externa independiente, así como una unidad administrativa responsable de velar porque el personal cumpla estos controles y las leyes y disposiciones aplicables. **(5:35)**

- **Sistema de información de riesgos (artículo No. 58)**

  La Superintendencia de Bancos implementará un sistema de información de riesgos, para lo cual los entes a que se refiere la ley están obligados a proporcionar la información que para el efecto determine dicha Superintendencia. **(5:35)**

- **Régimen de contabilidad (artículo No. 59)**

  El registro contable de las operaciones que realicen las empresas reguladas por la ley de Bancos y Grupos Financieros, deberá efectuarse, en su orden con base en las normas emitidas por la Junta Monetaria a propuesta de la Superintendencia de Bancos y en lo aplicable en principios de contabilidad generalmente aceptados y en normas internacionales de contabilidad. **(5:35)**

- **Adecuación de capital (artículo No. 64)**

  Los bancos y las sociedades financieras deberán mantener permanentemente un monto mínimo de patrimonio en relación con su exposición a los riesgos de crédito, de mercado y otros riesgos, de acuerdo con las regulaciones de carácter general que para el efecto emita la Junta Monetaria. **(5:38)**

- **Capital de grupos financieros (artículo No. 68)**

  La empresa controladora o la empresa responsable deberá consolidar mensualmente los estados financieros de las empresas que integran el grupo financiero y hacer que se mantenga permanentemente por lo menos el monto legal mínimo de patrimonio, tanto en forma consolidada como individual para cada uno de los miembros. **(5:38)**

- **Deficiencias patrimoniales de grupos financieros (artículo No. 69)**

  La deficiencia patrimonial que resulte del proceso de consolidación de los estados financieros de las empresas que conforman el grupo financiero deberá ser subsanada por la entidad

controladora o la empresa responsable, para lo cual se aplicará la regularización patrimonial contenida en esta ley. **(5:38)**

- **Regularización, suspensión de operaciones y exclusión de activos y pasivos, procedimientos y plazos (artículo No. 70)**

  Cuando un banco o una sociedad financiera presente deficiencia patrimonial deberá informarlo inmediatamente a la Superintendencia de Bancos; de no hacerlo quedará sujeto a las sanciones previstas en esta ley sin perjuicio de aplicar otras disposiciones legales que correspondan. Asimismo, dentro del plazo de cinco días siguientes a la fecha de su informe, deberá presentar a dicha Superintendencia, para su aprobación, un plan de regularización. **(5:39)**

- **Deficiencia patrimonial de grupos financieros (artículo No. 72)**

  Cuando un grupo financiero presente deficiencia patrimonial, conforme lo establecido en el artículo 69 de esta Ley la empresa controladora o la empresa responsable deberá informarlo inmediatamente a la Superintendencia de Bancos; de no hacerlo quedará sujeta a las sanciones previstas en esta Ley sin perjuicio de aplicar otras disposiciones legales que correspondan. Asimismo, deberá subsanar la deficiencia. **(5:40)**

- **Planes de Regularización (artículo No. 73)**

  Los bancos también estarán obligados a presentar planes de regularización con los plazos y características mencionados en los artículos 70 y 71 de la ley cuando la Superintendencia de Bancos detecte lo siguiente:

  - Incumplimiento de manera reiterada de las disposiciones legales y regulatorias aplicables, así como de las instrucciones de la Superintendencia de Bancos;
  - Deficiencias de encaje legal por dos meses consecutivos o bien por tres meses distintos durante un período de una año;
  - Existencia de prácticas de gestión que a juicio de la Superintendencia de Bancos pongan en grave peligro su situación de liquidez y solvencia; y
  - Presentación de información financiera que a juicio de la Superintendencia de Bancos no es verdadera o que la documentación sea falsa. **(5:40)**

- **Causales de suspensión y régimen especial (artículo No. 75)**

  La Junta Monetaria deberá suspender de inmediato las operaciones de un banco o de una sociedad financiera, en los casos siguientes:

  - Cuando haya suspendido el pago de sus obligaciones; y

- Cuando la deficiencia patrimonial sea superior al cincuenta por ciento del patrimonio requerido conforme esta Ley. **(5:41)**

➢ **Junta de exclusión de activos y pasivos (artículo No. 78)**

La Junta Monetaria a propuesta de la Superintendencia de Bancos, a más tardar al día siguiente dispuesta la suspensión de operaciones deberá nombrar una junta de exclusión de activos y pasivos, conformada por tres miembros, quienes estarán revelados, como cuerpo colegiado o individualmente considerados, a prestar fianza o garantía por su actuación. **(5:41)**

➢ **Fondo para la protección del ahorro (artículo No. 86)**

Se crea el fondo para la protección del ahorro, con el objeto de garantizar a los depositantes en el sistema bancario la recuperación de sus depósitos. **(5:43)**

➢ **Cobertura del fondo para la protección del ahorro (artículo No. 87)**

El fondo para la protección del ahorro cubrirá hasta un monto de veinte mil quetzales, o su equivalente en moneda extranjera, por persona individual o jurídica que tenga depósitos constituidos en un banco privado nacional o sucursal de banco extranjero. **(5:44)**

➢ **Infracciones (artículo No. 98)**

Las infracciones que cometan los bancos, sociedades financieras y las empresas integrantes de grupos financieros, a cualesquiera de las disposiciones de la Ley y otras que les sean aplicables, a las disposiciones que emita la Junta Monetaria, a su ley o estructura constitutiva, a reglamentos o estatutos, a órdenes administrativas o disposiciones de la Superintendencia de Bancos así como la presentación de informaciones, declaraciones o documentos falsos o fraudulentos, obstrucción o limitación a la supervisión de la Superintendencia de Bancos, y cuando realicen o registren operaciones para eludir el encaje bancario, o que conlleven el incumplimiento de los requerimientos patrimoniales, serán sancionados por el órgano supervisor, con observancia de los principios del debido proceso y del derecho de defensa, conforme lo dispuesto en la Ley. **(5:47)**

➢ **Entidades fuera de plaza (artículo No. 112)**

Son aquellas entidades dedicadas principalmente a la intermediación financiera, constituidas o registradas bajo leyes de un país extranjero, que realizan sus actividades principalmente fuera de dicho país.

1.3.4 Fusiones, absorciones, ventas, liquidaciones y autorizaciones de bancos después de la aprobación de la legislación vigente a partir del año 2002.

Uno de los principales efectos de la legislación vigente a partir de año 2002, fue la fusión, absorción y liquidación de bancos. A finales de 1999 se contaba con 34 Bancos. Al 31 de mayo de 2007 se cuenta con 24 bancos, de los cuales uno es estatal (El Crédito Hipotecario Nacional de Guatemala, CHN) y otro es sucursal de Banco extranjero (Citibank).

Las principales fusiones, absorciones, ventas de activos, liquidación y apertura de bancos observadas a partir de la Ley de Bancos y Grupos Financieros aprobadas en el año 2002 son:

- **Fusión de El Crédito Hipotecario Nacional de Guatemala con el Banco del Ejército, S.A.**

  Según autorización contenida en resolución JM-288-2002 del 27 de noviembre de 2002, la Junta Monetaria autorizó la fusión por absorción del Banco del Ejército, S.A. por parte de El Crédito Hipotecario Nacional de Guatemala.

- **Fusión de El Crédito Hipotecario Nacional de Guatemala con el Banco del Nor-Oriente, S.A.**

  Conforme resolución JM-34-2003 del 26 de febrero de 2003, la Junta Monetaria autorizó la fusión por absorción del Banco del Nor-Oriente, S.A. por parte de El Crédito Hipotecario Nacional de Guatemala.

- **Cesión de activos a favor de Banco Cuscatlán de Guatemala, S.A., por el Lloyds TSB Bank, PLC, Sucursal Guatemala.**

  En resolución JM-35-2004 del 21 de abril de 2004, la Junta Monetaria autorizó la cesión de una parte sustancial del balance de Lloyds TSB Bank PLC, Sucursal Guatemala, a favor del Banco Cuscatlán de Guatemala, S.A., que comprende la totalidad de los activos crediticios.

- **Fusión del Banco Industrial y el Banco de Occidente**

  En resolución JM-32-2006 del 9 de marzo de 2006, la Junta Monetaria resolvió autorizar al Banco Industrial, S.A. la adquisición de 2,151,114 acciones del Banco de Occidente, S.A.

- **Autorización de apertura de operaciones Banco de Crédito**

  Según resolución JM-677-2005 del 29 de noviembre de 2005, se autorizó el inicio de operaciones del Banco de Crédito, S.A.

- **Liquidación del Banco del Café, S.A.**
  Según resolución JM-120-2006 del 20 de octubre de 2006, la Junta Monetaria suspendió las operaciones del Banco del Café e inició el traslado de los activos y pasivos en tres bancos del Sistema. Estos bancos son: Reformador, De Desarrollo Rural y Agromercantil.

- **Liquidación de Banco de Comercio**
  Según resolución de la Junta Monetaria a partir del día 15 de enero de 2007 se suspendió las operaciones del Banco de Comercio, e inició los traslados de los activos y pasivos al Banco Industrial, S.A.

- **Apertura de operaciones Banco Azteca**
  El día 20 de mayo de 2007 inició sus operaciones el Banco Azteca.

- **Fusión Banco G&T Banco de Exportación**.

  En el primer trimestre del año 2007 se realizó la negociación por la cual el Banco G&T adquirió el Banco de Exportación Banex.

- **Compra de Banco Cuscatlán y operación de tarjetas de Banco Uno**
  Citigroup finalizó las negociaciones para la adquisición del Banco Cuscatlán y la operación de las tarjetas de crédito de Banco Uno.

- **Fusión Banco Agromercantil y Banco Corporativo**

  Los Bancos Agromercantil y Banco Corporativo concretaron la fusión por absorción, creando el Grupo Financiero Agromercantil.

- **Compra de Banco SCI por Banco Reformador**
  El Banco Reformador realizó la adquisición del 100 % de acciones del Banco SCI.

1.4 Legislación aplicable a las instituciones bancarias en Guatemala

1.4.1 Régimen legal

En el artículo No. 5 del Decreto 19-2002 Ley de Bancos y Grupos Financieros, se indica lo siguiente:

"Los bancos, las sociedades financieras, los bancos de ahorro y préstamo para la vivienda familiar, los grupos financieros, y las empresas que conforman a estos últimos, y las oficinas de representación de bancos extranjeros se regirán, en su orden, por sus leyes específicas, por la presente Ley por las disposiciones emitidas por la Junta Monetaria y en lo que fuere aplicable, por la Ley Orgánica del Banco de Guatemala, la Ley Monetaria y la Ley de Supervisión Financiera. En las materias no previstas en estas leyes, se sujetarán a la legislación general de la República en lo que les fuere aplicable. (5:1)

Los actos administrativos y resoluciones que dicten, tanto la Junta Monetaria como la Superintendencia de Bancos en aplicación de las leyes y reglamentos aquí indicados, observando el debido proceso, serán de acción ejecutiva y aplicación inmediata". (5:1)

A continuación se comentan las principales leyes aplicables a los Bancos:

1.4.2 Ley de Bancos y Grupos Financieros (decreto No. 19-2002)

Esta ley tiene por objeto regular lo relativo a la creación, organización, fusión, actividades, operaciones, funcionamiento, suspensión de operaciones y liquidación de bancos y grupos financieros, así como al establecimiento y clausura de sucursales y de oficinas de representación de bancos extranjeros. **(5:1)**

1.4.3 Ley Orgánica del Banco de Guatemala (decreto No. 16-2002)

Esta ley tiene como objeto normar el funcionamiento del Banco de Guatemala. El objetivo fundamental del Banco de Guatemala es contribuir a la creación y mantenimiento de las condiciones más favorables al desarrollo ordenado de la economía nacional. **(2:1)**

1.4.4 Ley Monetaria (decreto No. 17-2002)

Esta ley tiene por objeto regular lo relativo a la moneda nacional, indicando el nombre de la moneda nacional, la potestad de emisión, el canje, la forma de convertibilidad de la moneda, así como la descripción de las características de los billetes y monedas autorizados. **(3:1)**

1.4.5 Ley de Supervisión Financiera (decreto No. 18-2002)

Esta ley regula las actividades de la Superintendencia de Bancos, describiendo su naturaleza y objeto, las funciones, la organización y el presupuesto con el que deberá funcionar. **(4:1)**

1.4.6 Ley Contra el Lavado de Dinero u Otros Activos (decreto No. 67-2001)

Esta ley tiene por objeto prevenir, controlar, vigilar y sancionar el lavado de dinero u otros activos procedentes de la comisión de cualquier delito, y establece las normas que para este efecto deberán observar las personas obligadas. **(7:1)**

1.4.7 Ley Para Prevenir y Reprimir el Financiamiento del Terrorismo (decreto No. 58-2005)

Esta ley tiene por objeto adoptar medidas para la prevención y represión del financiamiento del terrorismo. **(6:1)**

1.4.8 Resoluciones de la Junta Monetaria

La Junta Monetaria ejerce la dirección suprema del Banco de Guatemala, tiene entre otras atribuciones las siguientes: determinar y evaluar la política monetaria, cambiaria y crediticia del país, velar por la liquidez y solvencia del sistema bancario nacional, reglamentar los aspectos relativos al encaje bancario y la cámara de compensación, aprobar las disposiciones, normas o instrumentos legales que someta a su consideración la Superintendencia de Bancos.

1.5 Supervisión de las instituciones bancarias

1.5.1 Superintendencia de Bancos

La supervisión de las instituciones bancarias es realizada por la Superintendencia de Bancos, a través de lo que establecen las siguientes regulaciones:

Constitución Política de la República artículo No. 133: "**La Superintendencia de Bancos organizada conforme a la ley es el órgano que ejercerá la vigilancia e inspección de bancos, instituciones de crédito, empresas financieras, entidades afianzadoras, de seguros y las demás que la ley disponga". (1:27)**

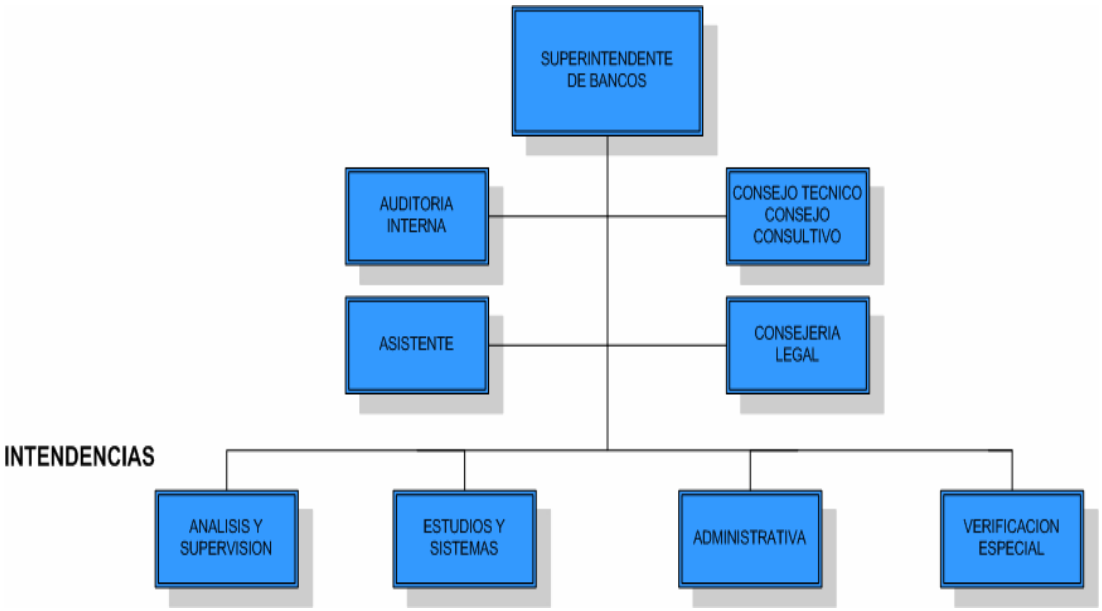
Congreso de la República Decreto No. 18-2002, Ley de Supervisión Financiera artículo No. 02 indica lo siguiente: **"Para los efectos de la Ley se entiende por supervisión la vigilancia e inspección de las entidades a que se refiere el artículo No. 01, realizada por la Superintendencia de Bancos, con el objeto de que las mismas adecuen sus actividades y funcionamiento a las normas legales, reglamentarias y a otras disposiciones que les sean aplicables, así como la evaluación del riesgo que asuman las entidades supervisadas…".**

1.5.2 Organización de la Superintendencia de Bancos

A continuación se presenta el organigrama de la Superintendencia de Bancos **(20:1)**

Cuadro No. 1

Organigrama de la Superintendencia de Bancos



Fuente: Página Web Superintendencia de Bancos Guatemala. www.sib.gob.gt

CAPÍTULO II
EL DEPARTAMENTO DE INFORMATICA DE UNA INSTITUCIÓN BANCARIA

El departamento de Informática de una institución bancaria tiene a su cargo administración de los recursos computacionales. Está integrado por personal con amplia experiencia en el uso de software y hardware y de los sistemas de comunicaciones necesarios para atender el procesamiento electrónico de datos.

A continuación se presenta los conceptos fundamentales para comprender la forma de administración y dirección de un departamento de Informática de una institución bancaria.

2.1 Comité de dirección del departamento de Informática

La alta dirección de la institución bancaria, deberá designar un comité de planeación, dirección y supervisión de las actividades del departamento de Informática. El comité de dirección es un factor importante para asegurar que la actividad informática esté encaminada a satisfacer la misión y los objetivos corporativos.

Este comité deberá estar presidido por el Gerente General, o un delegado gerencial y estará conformado por representantes de alto nivel de los departamentos usuarios de tecnología de información, y del departamento de Sistemas.

Los deberes y responsabilidades del comité deberán estar definidos en un documento formal.

Los miembros del comité deberán conocer las políticas, procedimientos utilizados por el departamento de Informática. Así mismo los miembros de este comité deberán tener autoridad para tomar decisiones, en las reuniones que se programen.

En este comité se deberá presentar periódicamente las actividades realizadas en el departamento de Informática. A continuación se presentan las actividades principales de este comité:

- Revisar los planes de largo y corto plazo del departamento de Informática de la institución bancaria.
- Aprobar las adquisiciones importantes de hardware y software.
- Autorizar y monitorear las actividades y proyectos de alta relevancia del departamento de Informática.
- Autorizar el presupuesto anual de tecnología de información.
- Reportar a la junta directiva las actividades realizadas por el departamento de Informática.

El comité de dirección, deberá recibir información gerencial apropiada del Departamento de Informática, los departamentos usuarios y de Auditoría Interna, para que en sus reuniones tenga la

visión completa y situación de la actividad informática. Las reuniones deberán programarse en forma periódica. Así mismo deberán realizarse actas formales en las cuales se documente las decisiones tomadas por el comité.

2.2 Definición del departamento de Informática

Es el departamento encargado de administrar los recursos tecnológicos de una institución bancaria, el proceso electrónico de datos, así como, el soporte y mantenimiento de la infraestructura tecnológica.

Un departamento de Informática comprende lo siguiente:

- El equipo físico o "hardware" utilizado para operar el sistema. Incluye monitores, unidades centrales de proceso, teclados, ratón, bocinas, audífonos, ups, impresoras, y otros.
- Los sistemas o "software" que incluyen el sistema principal y las aplicaciones específicas o paquetes computacionales, sistemas de comunicaciones y otros.
- Recurso humano capaz de administrar el hardware y el software.

2.3 Personal que integra un departamento de Informática

Para administrar adecuadamente un departamento de Informática de una institución bancaria es necesario realizar la división del personal de la siguiente forma:

- Gerencia del departamento.
- Mesa de ayuda a usuarios (help desk).
- Personal especializado encargado del análisis y programación del sistema.
- Personal para la administración del equipo (reparaciones, instalaciones de Sistemas, manejo de redes) y el soporte a la infraestructura tecnológica.

2.3.1 Gerente del departamento de Informática

El gerente del departamento de Informática de una institución bancaria es el enlace entre las necesidades informáticas de una institución bancaria y los usuarios de los servicios computacionales. Por lo anterior, deberá tener conocimientos sólidos de sistemas y equipos informáticos e infraestructura necesaria para su funcionamiento. Generalmente se recomienda que sea un ingeniero en sistemas, el encargado.

A continuación se listan los requerimientos, conocimientos y habilidades mínimas para desempeñar el puesto de jefe del departamento de Informática:

Graduado de la carrera de Ingeniería en Sistemas.

Experiencia de cinco años en lo siguiente:

- Manejo de presupuestos y negociaciones con proveedores.

- Análisis y desarrollo de sistemas cliente/servidor.
- Conocimientos en diseños y programaciones web.
- Manejo de bases de datos.
- Conocimientos de redes, comunicaciones.
- Manejo de equipo de computación, hardware y Software.
- Habilidad para el manejo de personal.
- Proactivo, investigador e innovador.
- Habilidad para redactar informes de avance de proyectos.
- Capacidad para el traslado de conocimientos.
- Buenas relaciones interpersonales.
- Valores morales y éticos.
- Conocimiento de normativa bancaria.

2.3.2 Mesa de ayuda (help desk)

La mesa de ayuda es una unidad especializada que tiene a su cargo el apoyo a usuarios finales de información. La atención a los usuarios puede ser derivado de consultas sobre la utilización de software o sobre problemas técnicos con los equipos. Las actividades de help desk se deben de documentar, para verificar la reincidencia en problemas de hardware o software, esto encaminado a la mejora del servicio.

Las actividades a cargo de help desk son:

- Apoyo a usuarios finales con dificultades en la utilización de hardware y software.
- Entrenamiento a usuarios finales en el uso de hardware y software.
- Responder a preguntas de los usuarios finales.
- Monitorear desarrollos técnicos e informar a los usuarios potenciales sobre la existencia de éstos.
- Identificar la fuente de problemas recurrentes e iniciar el proceso para la corrección.
- Informar a usuarios sobre problemas detectados que podrían efectuar sus actividades. **(12:372)**

2.3.3 Departamento de Sistemas

El departamento de Sistemas tiene a su cargo la administración del sistema principal, la implementación de mejoras, así como, el desarrollo y administración de los proyectos informáticos.

El departamento de Sistemas debe contar con personal con sólidos conocimientos informáticos, para poder realizar el análisis y la programación del sistema, así como, encargarse de los proyectos informáticos solicitados por los usuarios.

Los conocimientos y habilidades necesarias del personal son:

- Pensum cerrado de la carrera de Ingeniería en Sistemas.
- Experiencia en análisis y desarrollo de sistemas.
- Manejo de equipo de computación software y hardware.
- Conocimiento actualizado de software utilizado para desarrollo de sistemas.
- Habilidad en manejo de bases de datos.
- Proactivo.
- Capacidad para trabajo en equipo.
- Capacidad para elaborar informes.
- Buena actitud de servicio a cliente interno y externo.
- Valores morales y éticos.

El departamento de Sistemas puede dividirse en tres secciones:

- **Sección de Análisis de Sistemas**
  Se encarga de evaluar la funcionalidad y mejora de los sistemas, así como, recibir los proyectos informáticos, determinando los requerimientos necesarios de tiempo, recursos y horas hombre necesarios para su implementación.

- **Sección de Programación de Sistemas**
  Tiene a su cargo realizar la programación del sistema, o los nuevos programas, considerando el análisis realizado por los analistas del sistema.

- **Sección de Aseguramiento de Calidad**
  La labor de revisión y garantía de la calidad, la estandarización y seguimiento de la metodología del desarrollo de sistemas y atención a los usuarios está a cargo de la sección de Aseguramiento de Calidad.

2.3.4 Departamento de Soporte a la Infraestructura Tecnológica

Es el departamento encargado de administrar la información resultante del proceso electrónico de datos, las copias o back-up del sistema, realizar el mantenimiento preventivo y reparación de los equipos, el manejo de las comunicaciones entre otros. Tiene a su cargo también la instalación de los sistemas de aplicación a los equipos.

Adicionalmente, maneja el presupuesto anual designado para la adquisición del hardware y software, necesario para mantener el servicio y apoyar las áreas operativas y de negocios de una empresa.

El departamento de Soporte a la Infraestructura Tecnológica, puede dividirse en tres secciones:

- Sección de técnicos especializados en manejo del software y hardware.

- Sección de comunicaciones, que se ocupa de administrar lo siguiente: correo electrónico, redes, comunicaciones, internet, antivirus etc.
- Sección que administra la información y operaciones relacionadas con el proceso electrónico de datos, back-up del sistema e información, inventarios de equipos y las medidas de seguridad para protegerlo.

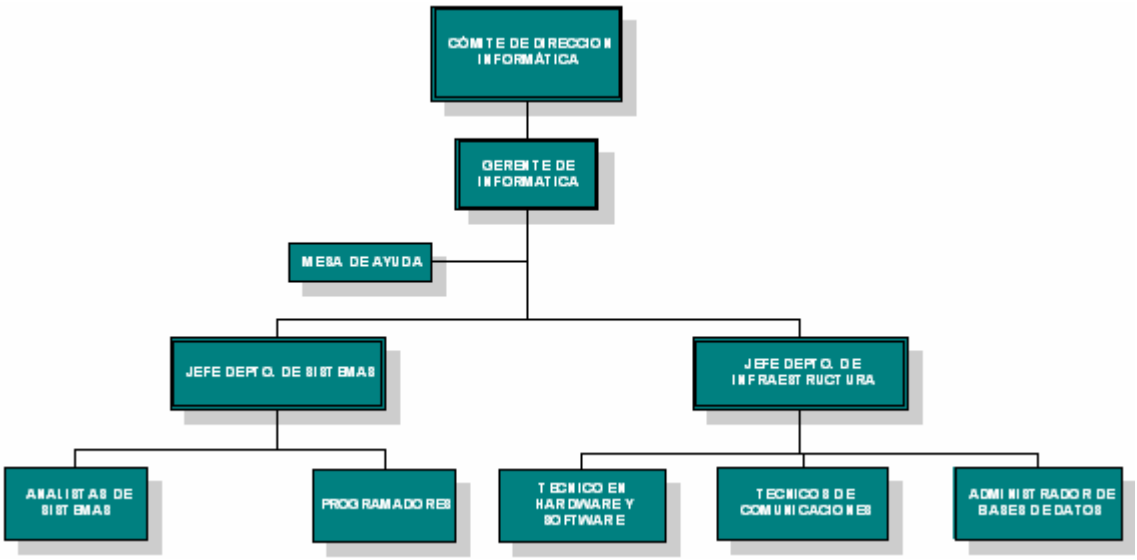
Por lo anterior, es importante que dicho personal cuente con los siguientes conocimientos y habilidades:

- Estudios de la carrera de Ingeniería en Sistemas.
- Experiencia en manejo de bases de datos, sistemas de redes y comunicaciones.
- Habilidad para la reparación, instalación y actualización de equipo de computación software y hardware.
- Conocimiento actualizado de software utilizado para desarrollo de Sistemas.
- Habilidad en manejo de bases de datos.
- Proactivo.
- Capacidad para trabajo en equipo.
- Capacidad para elaborar informes.
- Buena actitud de servicio a cliente interno y externo.
- Valores morales y éticos.

A continuación se presenta el organigrama del departamento de informática de una institución bancaria.

Cuadro No. 2

Organigrama del Departamento de Informática



Fuente: Muñoz Razo Carlos, Auditoría en Sistemas Computacionales

2.4 Administración del personal del departamento de Informática

La gerencia del departamento de Informática deberá establecer políticas y procedimientos para la contratación, promoción, capacitación, evaluación del desempeño de atribuciones, entrenamiento, goce de vacaciones y para cuando se decida la terminación del contrato de alguno de los colaboradores.

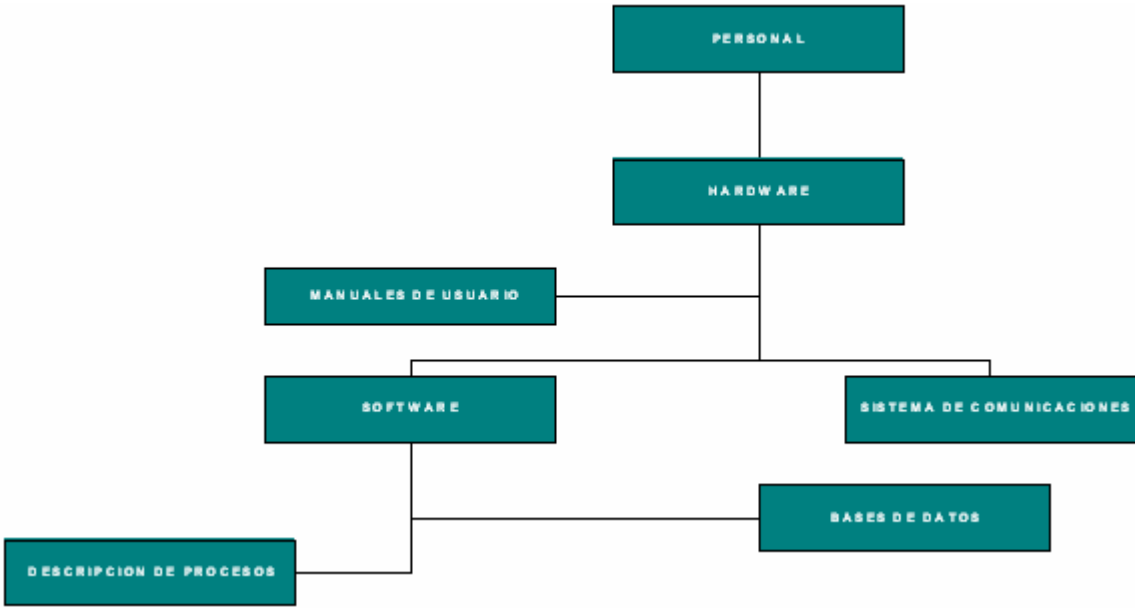
2.5 Infraestructura necesaria para que funcione un departamento de Informática

Adicional al personal técnico que administra el Departamento de informática, es necesario que se cuente con el hardware, software, sistemas de comunicaciones y manuales de uso de los sistemas y equipos.

Considerando los conceptos expuestos anteriormente y el análisis efectuado en un Departamento de Informática de una institución bancaria a continuación se presenta un cuadro descriptivo de la infraestructura necesaria para su funcionamiento:

Cuadro No. 3

Infraestructura del Departamento de Informática



Fuente: Investigación propia en el departamento de Informática de Banco Internacional, S.A.

2.5.1 Personal administrativo y operativo del departamento de Informática

Son las personas que realizan la programación del sistema y que dan soporte a la infraestructura tecnológica.

2.5.2 El hardware

Son todos los dispositivos y componentes físicos que realizan las tareas de entrada y salida, también se conoce al hardware como la parte dura o física del computador.

La mayoría de computadoras están organizadas de la siguiente forma:

Los dispositivos de entrada (teclados, lectores de tarjetas, lápices ópticos, lectores de códigos de barra, escáner, mouse, etc.) y salida (monitor, impresoras, bocinas, audífonos, etc.) que permiten la comunicación entre el computador y el usuario. **(12:377)**

2.5.3 Manuales de usuario

Son los documentos que contienen la información descriptiva que detalla o da instrucciones sobre el empleo y operación del software y el hardware a los usuarios.

Incluye también las guías de operación, los términos comúnmente utilizados y las operaciones básicas.

2.5.4 El software

El software es una colección de datos e instrucciones lógicas que permite la ejecución de tareas específicas previamente definidas, utilizando en el hardware de una computadora. **(12:242)**

El software tiene funciones específicas que son:

- Administrar los recursos de un sistema de cómputo.
- Proporcionar las herramientas necesarias para administrar adecuadamente los recursos de un sistema de cómputo.
- Actuar como intermediario entre el usuario, el hardware y la información almacenada internamente y en dispositivos externos.

El software deberá contar con documentación para tener un detalle comprensible por otro programador o usuario, de los elementos necesarios para que funcione el sistema principal o los programas.

A continuación se indica la siguiente definición de documentación del software:

"Es un documento especializado en el cual se indican todos los aspectos técnicos que se deben de considerar para el adecuado manejo del sistema; estos aspectos suelen ser muy sofisticados y con características especiales sobre el funcionamiento técnico de los sistemas computacionales, no sólo en cuanto a software y hardware, sino también en cuanto a sus instalaciones, equipos y manejo de información" **(12:156).**

Existes tres tipos de software que son:

- **Software de sistema**

  Es un conjunto de programas que administran los recursos de la computadora, ejemplos: unidad central de proceso, dispositivos de comunicaciones y dispositivos periféricos, el software del sistema administra y controla al acceso del hardware. **(12:222)**

- **Software de aplicaciones**

  Son programas que son escritos para o por los usuarios para realizar una tarea específica en la computadora, ejemplo: software para procesar un texto, para generar una hoja de cálculo, el software de aplicación debe estar sobre el software del sistema para poder operar. **(12:222)**

- **Software de usuario final**

  Es el software que permite el desarrollo de algunas aplicaciones directamente por los usuarios finales, el software del usuario final con frecuencia tiene que trabajar a través del software de aplicación y finalmente a través del software del sistema. **(12:222)**

2.5.5 Sistemas de comunicaciones

Para que se pueda comunicar el sistema principal con las terminales de los usuarios, así como entre ellas, es necesario contar con un sistema de comunicaciones que permita realizar esta actividad.

2.5.6 Descripción de procesos

Un departamento de Informática deberá contar con una documentación de sus procesos. En esta descripción se deberá indicar la secuencia de las operaciones y procesos, su importancia, horarios de ejecución, personal responsable, contingencias etc.

2.5.7 Bases de datos

Las bases de datos son una colección de información organizada y enlazada al sistema. Se accesa por medio del software.

Un sistema de bases es un conjunto de programas que permite realizar lo siguiente:

- Almacenar y organizar datos de manera secuencial, uniforme y consistente.
- Accesar en todo momento a la información ahí almacenada.
- Concentrar información para evitar su duplicidad y ahorro de espacio. **(12:654)**

Así mismo un departamento de Informática necesita contar con lo siguiente:

2.6 Políticas y procedimientos utilizados en un departamento de Informática

2.6.1 Políticas

Las políticas en una organización comunican los estándares definidos por la alta gerencia de una Organización. Definen las medidas y procedimientos que deben observar por los usuarios, al utilizar los activos y la información, con el objetivo de asegurar su salvaguarda. **(12:109)**

Deberán de actualizarse, por lo menos una vez al año o cuando existan cambios significativos, y deberán de darse a conocer a todo el personal.

Una política debe incluir los siguientes aspectos:

- Nombre del funcionario que la emite.
- Personal que debe de cumplir la política.
- Fecha de vigencia.
- Asunto que trata la política.
- Objetivo de la política.
- Descripción de la política.
- Normas a aplicar en la política.
- Sanciones por incumplimiento de la política.
- Disposiciones finales o aclaraciones.

Dentro de las políticas se pueden citar:

- Asignación y uso de claves de acceso al Sistema.
- Reglamento para el uso de correo electrónico e Internet.
- Ingreso al Departamento de Informática
- Pasos a producción.
- Manejo de servidores
- Back-up de información.

Las políticas de seguridad son importantes en una organización, por las siguientes razones:

- Proporcionan una base uniforme, estable y formal a seguir por parte del personal.
- Se crea conciencia de los riesgos.
- Contienen reglas y lineamientos a seguir en las actividades se evitan especulaciones, principalmente en el personal de nuevo ingreso. **(12:109)**

Estos aspectos permiten fortalecer el ambiente de control, por lo que en una organización es fundamental que se cuente con políticas de seguridad, que ayuden a minimizar los diferentes riesgos que le afectan.

2.6.2 Procedimientos

Los procedimientos son el detalle que contiene la documentación de los procesos y los controles integrados a los mismos.

Los procedimientos se derivan de las políticas y están creados para guiar a los usuarios, por lo que éstos deberán conocerlos a fondo. Así mismo, deberán actualizarse cuando existan cambios significativos. **(12:110)**

2.7 Administración de la seguridad informática

La Administración de la seguridad del departamento de Informática tiene como objetivos proteger la integridad, exactitud, disponibilidad, continuidad y confidencialidad de los sistemas de información. Así mismo el cumplimiento de las leyes y regulaciones internas y externas. **(8:191)**

Los desastres que pueden inhabilitar un centro de cómputo, pueden ser provocados por desastres naturales o provocados por el hombre, ya sea intencionalmente o por descuidos del personal encargado de realizar la operatoria del sistema, es por eso que es importante realizar una división necesaria para un departamento de Informática.

El éxito de la administración de la seguridad informática depende del compromiso y soporte de la alta Gerencia, que será monitoreado a través del Oficial de Seguridad Informática, quien será responsable de velar por el cumplimiento las políticas de seguridad de la organización.

La seguridad necesaria en un departamento de informática puede clasificarse en: seguridad lógica, física, del personal, de las bases de datos, y de los sistemas de comunicación. A continuación se describen.

2.7.1 Seguridad lógica

La seguridad lógica son los controles de acceso de datos a una computadora, para salvaguardar la información ahí almacenada. Así mismo controla las modificaciones realizadas a los códigos de programación del Sistema. **(8:192)**

La identificación y autorización es el proceso de establecer y probar la identidad de un usuario, en el caso del acceso al sistema, los permisos.

Para fortalecer la seguridad lógica existen los siguientes elementos:

- **Software de control de accesos**

  El software de control de acceso está diseñado para impedir el ingreso modificación o extracción de datos no autorizados, de un programa o sistema de información. **(8:199)**

  Los accesos deberán ser asignados por medio de códigos personalizados denominados "password". Para la asignación de estos es necesario que se cuente con perfiles de usuario, que deberán dar acceso a opciones del sistema de acuerdo a las funciones asignadas al personal de acuerdo a sus funciones dentro de la organización, tomando en consideración los manuales de puestos. **(8:199)**

  El historial de accesos de cada usuario deberá ser almacenado en una bitácora de operaciones, para futuras consultas.

  Se deberá monitorear las actividades realizadas por los usuarios. Este seguimiento se puede apoyar en software especializados disponible en el mercado, que puede dar las alarmas que se le parametricen, en tiempo real, para poder parar cualquier acceso no autorizado, sustracción o modificación de información.

  El software que se adquiera deberá poder monitorear como mínimo los accesos a: **(8:199)**

  - Librerías.
  - Archivos de datos.
  - Reportes.
  - La Red.
  - Programas de aplicación.
  - Diccionario de datos.
  - Sistema de Comunicaciones.
  - Intentos de acceso exteriores.

  Algunas de las vulnerabilidades más comunes observadas en el software de control de acceso son:

  - Métodos débiles de autenticación.
  - Usuarios con habilidades para evadir el mecanismo de autenticación.
  - Falta de confidencialidad e integridad en la información de los password almacenados.
  - Falta de encripción de los password.

- **Firewall**

  El firewall es un software que permite la administración centralizada de los accesos a la información, desde canales externos, principalmente, desde Internet o canales VPN (virtual protocol network).

Los Firewall funcionan programando o asignando los permisos que tendrán los usuarios, así como los privilegios para el uso de la información. Bloquean el acceso a sitios particulares de la Internet.

También impiden que determinados usuarios tengan acceso a servidores o servicios. Monitorean las comunicaciones entre una red interna y externa. Pueden encriptar o cifrar paquetes que son enviados entre diferentes ubicaciones físicas dentro de una organización creando una red virtual en Internet.

Los firewall son dispositivos que ejecutan políticas de seguridad para el tráfico de información que ingresa y se transmite desde diferentes segmentos de una red.

Un firewall proporciona un buen porcentaje de seguridad, sin embargo, es importante que se analice detalladamente los siguientes problemas o debilidades de éstos:

- El tráfico interno de comunicaciones en la red no es analizado por el firewall.
- Firewall mal configurados.
- Falta de monitoreo de las actividades de los usuarios.
- Falta de actualización de las políticas de los firewall. **(12:532)**

- **Software para prevención y detección de intrusos**

Este software funciona proporcionando alertas de la realización de ataques con éxito e incluso de ataques en progreso.

Estos sistemas deberán ser parametrizados con eficacia identificando plenamente las situaciones de riesgo, en el sentido de que no ofrezcan ni falsos positivos (calificar de ataque una actividad que no es tal) ni falsos negativos (no considerar como ataque una acción que en realidad sí lo era).

La efectividad de un sistema de prevención y detección de intrusos será mayor cuanto más corto sea el tiempo de respuesta a la alerta, para permitir actuar de forma consecuente y poder detener el ataque en curso.

Estas características deberán considerarse siempre para que software sea considerado de verdadera utilidad en la detección de intrusiones.

Prevención, detección y reacción constituyen tres conceptos clave en todo sistema de protección que pretenda ofrecer soluciones integrales de seguridad.

Hoy en día, la práctica totalidad de productos de seguridad del mercado se centran en exclusiva en la primera acción, la prevención del ataque, utilizando cortafuegos y criptografía. Aunque ningún sistema será nunca 100% seguro, lo cierto es que disminuirá la probabilidad de éxito en un ataque y de escapar impune.

El beneficio de un software para detección y prevención de intrusos, es proveer una solución proactiva, bloqueando amenazas antes de que ocurra el daño a través de inteligencia de seguridad en tiempo real, control de cambio, y administración de dispositivos.

El software para detección de intrusos tiene como finalidad permitir y controlar el acceso interno a los siguientes recursos:

- Programas de librerías.
- Archivos de datos.
- Programas de aplicación.
- Diccionarios de datos.
- Archivos.
- Sistemas de comunicación.

Los sistemas para detección de intrusos permiten detectar ataques que pasan inadvertidos a un cortafuegos (firewall) y avisa antes o justo después de que se produzcan estos ataques. **(12:537)**

- **Antivirus**

Un departamento de Informática deberá contar con un antivirus, que es un programa que detecta y elimina los virus. **(12:549)**

Los virus son programas computacionales avanzados que tienen como objetivo principal la destrucción de la información almacenada en las computadoras o la saturación de los sistemas, así como la obtención no autorizada de información.

2.7.2 Seguridad física

Para proteger adecuadamente el software, hardware y la información, es necesario que las instalaciones del departamento de Informática cuenten con medidas de seguridad.

A continuación se indican las principales: **(8:219)**

- **Accesos**

  Se deberá restringir los accesos para que únicamente personal autorizado ingrese a las instalaciones del departamento de Informática. El acceso puede ser controlado con el uso de un dispositivo electrónico activado por una tarjeta y códigos que se asignan al personal que tendrá libre acceso.

- **Cámaras de vigilancia**

  El departamento de Informática deberá contar con cámaras de vigilancia que monitoreen las actividades del personal que labora en un departamento de informática así como de los accesos.

- **Bitácoras de operación**

  Un departamento de Informática deberá contar con bitácoras (pistas de auditoría), en las cuales se consignen la fecha, nombre del usuario que realizó modificación y/o uso de la información, para verificar posteriormente y en tiempo real el acceso a ésta información.

- **Aire acondicionado**

  La concentración de equipos de cómputo generan calor, derivado de esta situación y para evitar sobrecalentamiento de las computadoras, es necesario que el departamento de Informática cuente con un equipo de aire acondicionado, generalmente la temperatura ideal que debe proporcionar el equipo de aire acondicionado es entre 14 y 17 grados centígrados.

- **Suministro de energía eléctrica**

  El servicio de energía eléctrica se considera uno de los servicios críticos, se debe de garantizar que en ausencia del servicio público una corriente alterna o servicio propio funcione.

  Esta corriente alterna puede ser provista mediante UPS (uninterruptible power supply), o plantas generadoras de electricidad. Así mismo es necesario contar con reguladores de voltaje, que protejan a los equipos de sobrecargas de electricidad.

- **Detección de humo e inundaciones**

  Se deberá contar con alarmas detectoras de humo e inundaciones para salvaguardar el equipo y el personal de los daños causados por fuego y el agua.

- **Seguros**

  Se deberá contar con seguros que contemple el resarcimiento de los daños provocados por incendios, terremotos, sabotaje, hurto, robo, daños al personal y otros que puedan afectar al software, hardware, información y al personal del departamento de Informática.

2.7.3 Seguridad del personal

La seguridad del personal debe de ser uno de los principales objetivos de la seguridad, en un departamento de Informática. Se deberá monitorear las actividades del personal.

Es importante contar con políticas de incentivos y reconocimientos, para garantizar que el personal esté motivado.

Se deberá contar con políticas de rotación de personal, para evitar tener personal insustituible y detectar posibles errores y/o fraudes e implementar estándares de calidad y de control interno en el desarrollo del software para evitar actos dolosos, realizados por los usuarios o los mismos programadores.

2.7.4 Seguridad de las bases de datos

Las bases de datos son la colección de información resultante del proceso electrónico de datos. La seguridad deberá orientarse a la prevención de la manipulación no autorizada de la información contenida en estas bases de datos.

2.7.5 Seguridad de los sistemas de comunicaciones

Los sistemas de comunicaciones permiten recibir, enviar y procesar la información entre computadoras en la empresa. Se deberá asegurar su utilización mediante niveles de acceso, controlando el envío y recepción de información mediante éstos sistemas.

2.7.6 Seguridad en la programación de los sistemas

El objetivo de esta seguridad es constatar que el sistema estará programado para satisfacer los requerimientos del usuario final. Por lo que previo a realizar ésta programación, es necesario seguir las siguientes etapas:

- **Análisis**

  En esta etapa se deberá recopilar toda la información que se considere necesaria, que deberá contemplar el programa a desarrollar. Esta etapa deberá incluir también el análisis de si no existe otro programa ya desarrollado que incluya los requerimientos actuales del usuario, esto para evitar hacer una nueva programación.

- **Informe de factibilidad del proyecto**

  Previo a iniciar la etapa de diseño, se deberá realizar un informe de la factibilidad para la realización del proyecto, éste análisis deberá incluir un informe sobre el costo-beneficio, para determinar que la inversión en recursos de programación, se justificarán con los beneficios para el usuario y la empresa.

2.8 Los presupuestos para adquisición y mantenimiento de tecnología de información

Un departamento de Informática deberá contar con un presupuesto que le permita realizar la adquisición oportuna de los diferentes recursos necesarios para el desarrollo de sus actividades. Generalmente este presupuesto es elaborado en forma anual.

Un presupuesto permite el pronóstico, monitoreo y análisis de la adquisición de recursos informáticos. Permiten la asignación adecuada de los recursos, tomando en consideración los planes a corto y largo plazo de tecnología de información.

Los presupuestos deberán ser elaborados por la gerencia del departamento, y autorizados en el comité de dirección informática, generalmente en forma anual, derivado de la fluctuación constante en los precios de los recursos a adquirir.

La aprobación de adquisición de software y hardware será conforme este presupuesto, sin embargo en caso de presentarse una compra fuera de presupuesto, se convocará a una reunión extraordinaria para evaluarla y autorizarla.

2.9 Riesgos a que está expuesto un departamento de Informática

Un departamento de Informática está expuesto a varios riesgos. Derivado de esta situación es necesario que se cuente con un proceso de administración de riesgos. Esto con el objetivo de identificar y clasificar adecuadamente los recursos de información.

Un proceso adecuado de administración de riesgos debe contar los siguientes pasos:

- **Identificación de los activos sujetos a riesgos**

  La identificación de los activos sujetos a riesgos se centraliza en un documento donde se indican los procesos que se realizan en el departamento de Informática, el equipo existente, su configuración, así como los servicios que se prestan y la descripción de las actividades que realiza el personal, denominado matriz de riesgo tecnológico.

  El objetivo de la matriz de riesgo tecnológico es servir de guía y apoyo al plan de continuidad del negocio.

  Así mismo, deberá contener la forma en que se realizan las comunicaciones, las condiciones ambientales que deberá protegerse el Centro de Procesamiento de Información, personal responsable de operaciones y procesos, nombres de proveedores, principales clientes, etc.

A continuación se presenta la identificación de los recursos típicos asociados a un departamento de Informática:

- Hardware
- Software
- Información
- Personal

➢ **Estudio de amenazas y vulnerabilidades que afectan los activos identificados**

Las amenazas en los activos descritos anteriormente ocurren por las vulnerabilidades o factores de riesgo asociadas al uso de estos recursos, a continuación se presentan los principales factores de riesgos de los recursos informáticos.

- **En el hardware**
  Falta de control y protección, condiciones inapropiadas de uso, falta de observancia de normas y procedimientos, obsolescencia, incompatibilidad, falta de soporte.

- **En el software**
  Por uso o acceso, copia no autorizados, modificación, destrucción, hurto, errores u omisiones, infección de virus y gusanos.

- **En la información**
  Usos o acceso, copia, modificación, destrucción, hurto.

- **En el recurso humano que administra el equipo y los sistemas**
  Personal deshonesto, incompetente, descontento, desactualizado.

➢ **Análisis del impacto de las amenazas y vulnerabilidades**

El impacto es la materialización de los factores de riesgo o vulnerabilidades y tiene como consecuencia una pérdida financiera, a continuación se indican las pérdidas que pueden generar las vulnerabilidades.

- Pérdida o daño significativo en los activos.
- Incumplimiento de normativa asociada.
- Pérdida de reputación.
- Peligro potencial en el uso de los activos y la tecnología.
- Pérdida de oportunidades de negocio.
- Reducción de la eficiencia.
- Cese temporal o definitivo de las actividades del negocio.
- Uso no autorizado de la información.

Cuando se han analizado los riesgos, se debe evaluar los controles existentes, para determinar si los mismos cubren satisfactoriamente o si es necesario fortalecerlos o crear nuevos.

- **Plan de continuidad de negocios**

Un plan de continuidad del negocio es un documento detallado, que establece todas las acciones que se tomarán antes, durante y después de que ocurra una catástrofe. **(12:625)**

- Antes de una catástrofe, se deberá tener un adecuado nivel de seguridad física.
- Durante una catástrofe, ejecutar el plan de contingencias.
- Después de una catástrofe, seguir con el plan de contingencia y evaluar los reclamos estipulados en los contratos de los seguros contratados.

El plan de continuidad del negocio deberá incluir los siguientes elementos:

- Realizar un análisis de riesgos de sistemas críticos, determinando la tolerancia máxima.
- Realizar un inventario de procesos críticos.
- Establecer el período máximo de recuperación por proceso crítico
- Identificar las pérdidas a que se puede incurrir al no cumplir los plazos.
- Establecer prioridades para inicio o fin de procesos de software o hardware.
- Determinar el orden correcto en que deberán de ser ejecutados de los procesos.
- Establecer objetivos de recuperación, indicando el período máximo tolerable.
- Designar un centro de procesamiento alternativo de información.
- Asegurar la capacidad de los servicios de back-up.
- Verificar con regularidad la vigencia de las pólizas de seguro.
- Asignar fecha de pruebas, para verificar la funcionalidad del plan. **(12:625)**

2.10 Crimen informático

El crimen informático es un delito especializado realizado mediante la utilización no autorizada de recursos informáticos, con el objetivo de robar dinero, equipos, software o manipular información.

Los crímenes informáticos son realizados por los “hackers” personas que tienen habilidad de explotar detalles de los sistemas programables y el conocimiento para explotar a su beneficio los recursos del sistema.

Los crímenes informáticos pueden ser realizados por las siguientes causas:

- Insatisfacción con la empresa.
- Beneficio personal o de terceros.
- Problemas financieros graves.
- Deseo de reconocimiento.
- Problemas psicológicos.
- Como diversión o pasatiempo.

CAPÍTULO III
LA AUDITORÍA INTERNA DE SISTEMAS DE INFORMACIÓN DE UNA INSTITUCIÓN BANCARIA

La Auditoría Interna de Sistemas de Información de una institución bancaria, depende del Departamento de Auditoría Interna. Tiene a su cargo la medición y evaluación de los principales riesgos que afectan el uso de sistemas computacionales. Así mismo brinda apoyo a la Auditoría de Operaciones a través del uso de software especializado de Auditoría, para realizar pruebas globales y revisiones a bases de datos voluminosas. La Auditoria de Sistemas de Información para efectuar sus evaluaciones, deberá contar con un plan de trabajo en el cual se incluyan los procesos efectuados en el departamento de Informática.

A continuación se presenta la definición de Auditoría de Sistemas de información y de los lineamientos internacionales y locales que se tienen para el desarrollo del trabajo.

3.1 Auditoría Interna de Sistemas de Información

3.1.1 Concepto

A continuación se presentan algunos conceptos de Auditoría de Sistemas de Información:

"Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos, y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes" (13:19).

"El examen y evaluación de los procesos del área de procesamiento automático de datos (PAD) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas" (18:01).

"La Auditoría en Informática es la revisión y la evaluación de los controles, sistemas, procedimientos de Informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones" (8:18).

Tomando en consideración estos conceptos se puede indicar que la Auditoría de Sistemas de Información es: la revisión y evaluación del uso del software y hardware, los controles y el nivel de seguridad en el uso de tecnología de información, así mismo en los aspectos técnicos especializados se apoyará en especialistas con amplia experiencia en sistemas de información y conocimientos de los riesgos que les afectan.

La Auditoria de Sistemas de Información es importante para evaluar el buen desempeño de los sistemas y equipos, notifica si los controles y lineamientos utilizados son confiables y con un nivel de seguridad aceptable, que garantice la protección de la información.

3.2 Antecedentes de la Auditoría Interna de Sistemas de Información

A continuación se presentan los antecedentes modernos de la regulación internacional y nacional para supervisar el trabajo de Auditoría en un ambiente computarizado de información. Es importante hacer constar que para el desarrollo ordenado de un trabajo de Auditoría se deberá tomar en consideración la norma internacional de Auditoría.

3.2.1 Nivel internacional

Norma internacional de Auditoría No. 401. "AUDITORÍA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN COMPUTARIZADO". **(15:135)**

- **Propósito**

  El propósito de la Norma Internacional de Auditoría (NIA) es establecer normas y proporcionar lineamientos sobre los procedimientos que deben seguirse cuando se conduce una Auditoría en un ambiente de sistemas de información computarizado (SIC).

  Para fines de las NIAS, un ambiente de sistemas de información computarizado existe cuando está involucrada una computadora de cualquier tipo o tamaño en el procesamiento de información financiera de importancia para la Auditoría, ya sea que dicha computadora sea operada por la entidad o por un tercero.

  El auditor deberá considerar como afecta a la Auditoría un ambiente SIC.

  El objetivo y alcance globales de una Auditoría no cambia en un ambiente SIC. Sin embargo, el uso de una computadora cambia el procesamiento, almacenamiento y comunicación de la información financiera y puede afectar los sistemas de contabilidad y de control interno empleados por la entidad. Por consiguiente, un ambiente SIC puede afectar lo siguiente:

  - Los procedimientos seguidos por un auditor para obtener una comprensión suficiente de los sistemas de contabilidad y de control interno.
  - La consideración del riesgo inherente y del riesgo de control a través del cual el auditor llega a la evaluación del riesgo.
  - El diseño y desarrollo por el auditor de pruebas de control y procedimientos sustantivos apropiados para cumplir con el objetivo de la Auditoría.

- **Habilidad y competencia**

  El auditor debería tener suficiente conocimiento del SIC para planear dirigir, supervisar y revisar el trabajo desarrollado. El auditor debería considerar si se necesitan habilidades especializadas en SIC en una Auditoría. Estas pueden necesitarse para:

- Obtener una suficiente comprensión de los sistemas de contabilidad y de control interno afectados por el ambiente SIC.
- Determinar el efecto del ambiente SIC sobre la evaluación del riesgo global y del riesgo al nivel de saldo de cuenta y de clase de transacciones.
- Diseñar y desempeñar pruebas de control y procedimientos sustantivos apropiados.

Si se necesitan habilidades especializadas, el auditor buscaría la ayuda de un profesional con dichas habilidades, quien puede pertenecer al personal del auditor o ser un profesional externo.

Si se planea el uso de dicho profesional, el auditor debería obtener suficiente evidencia apropiada de Auditoría de que dicho trabajo es adecuado para los fines de la Auditoría, de acuerdo con NIA "Uso del trabajo de un experto". **(15:135)**

- **Planeación**

De acuerdo con NIA " Evaluaciones del riesgo y control interno" el auditor debería obtener una comprensión de los sistemas de contabilidad y de control interno, suficiente para planear la Auditoría y desarrollar un enfoque de Auditoría efectivo.

Esta comprensión incluirá asuntos como:

- La importancia y complejidad del procesamiento por computadora en cada operación importante de contabilidad, por el volumen de transacciones, la generación automática de transacciones y su validación independiente, el intercambio de información con otras entidades.
- La estructura organizacional de las actividades SIC del cliente y el grado de concentración o distribución del procesamiento por computadora en toda la entidad, particularmente en cuanto puede afectar la segregación de deberes.
- La disponibilidad de datos. Los documentos fuente, ciertos archivos por computadora, y otro material de evidencia que pueden ser requeridos por el auditor, pueden estar disponibles por un corto período de tiempo o sólo en forma legible por computadora.

Al planear las porciones de la Auditoría que pueden ser afectadas por el ambiente SIC del cliente, el auditor debería obtener una comprensión de la importancia y complejidad de las actividades de SIC y la disponibilidad de datos para uso en la Auditoría.

Cuando el SIC es significativo, el auditor deberá también obtener una comprensión del ambiente SIC y de si puede influir en la evaluación de los riesgos inherentes y de control. La naturaleza de los riesgos y las características del control interno en ambientes SIC incluyen lo siguiente:

- Falta de rastros de las transacciones.

Derivado de la falta de recursos de almacenamiento y/o procesamiento, algunos SIC son diseñados de modo que un rastro completo de una transacción, que podría ser útil para fines de Auditoría podría existir sólo durante un corto período de tiempo o no estar disponible.

- Procesamiento uniforme de transacciones.

  El procesamiento por computadora generalmente es uniforme, cualquier cambio, debe de ser debidamente documentado y se deberá analizar su efecto y forma de comparación en el tiempo.

- Inadecuada segregación de funciones.

  Muchos procedimientos de control que ordinariamente serían desempeñados por individuos por separado en los sistemas manuales, pueden ser concentrados en SIC. De esta manera un empleado que tiene acceso a los programas de computadora, al procesamiento y a los datos, puede estar en posición de desempeñar funciones incompatibles.

- Potencial para errores e irregularidades.

  El potencial para error humano en el desarrollo, mantenimiento y ejecución de SIC puede ser mayor que en los sistemas manuales, parcialmente a causa del nivel de detalle inherente a estas actividades.

  También existe riesgo por la falta de supervisión a las actividades de los usuarios y programadores, pueden propiciar que algunos individuos gane acceso no autorizado a los datos o a la alteración de datos sin evidencia visible pude ser mayor en Sic que en sistemas manuales.

  Generalmente algunos errores o irregularidades que ocurren durante el diseño, análisis y/o modificación de programas de aplicación de software, pueden permanecer sin detectar por largos períodos de tiempo.

- Iniciación o ejecución de transacciones

  El SIC puede incluir la capacidad de iniciar o causar la ejecución de ciertos tipos de transacciones, automáticamente. La autorización de estas transacciones o procedimientos puede no estar documentada en la misma forma que en el sistema manual, y la autorización de la administración de estas transacciones puede estar implícita en su aceptación del SIC y modificaciones subsecuentes.

- Dependencia de otros controles

  El procesamiento por computadora puede producir reportes y otros controles que pueden ser utilizados para el monitoreo general de las actividades, la efectividad de estos controles está ligada a la oportunidad de controles preventivos y detectivos que la Administración pueda implementar.

- Potencial para mayor supervisión de la administración

  El SIC puede ofrecer a la administración una variedad de herramientas analíticas que pueden ser utilizadas para revisar y supervisar las operaciones de la entidad.

- Potencial para uso de técnicas de Auditoría con ayuda de la computadora

  En el caso de análisis de grandes cantidades de información y datos de un ambiente SIC, brinda la oportunidad al auditor de utilizar software de Auditoría y aplicar técnicas asistidas por la computadora. **(15:136)**

➢ **Evaluación del riesgo**

De acuerdo con NIA "Evaluación del riesgo y control interno", el auditor debería hacer una evaluación de los riesgos inherentes y de control para las aseveraciones importantes de los estados financieros.

Los riesgos pueden resultar de deficiencias en actividades generales de SIC como desarrollo y mantenimiento de programas, soporte al software de sistemas, operaciones, seguridad física y control general sobre acceso a programas.

Los riesgos incrementan el potencial de errores irregularidades así como actividades fraudulentas en aplicaciones específicas o en información ya procesada. **(15:138)**

➢ **Procedimientos de Auditoría**

De acuerdo con norma internacional de auditoría " Evaluaciones del riesgo y control interno" el auditor debería considerar el ambiente SIC al diseñar los procedimientos de Auditoría para reducir el riesgo a un nivel aceptablemente bajo.

Los objetivos específicos de Auditoría del auditor no cambian ya sea que los datos de contabilidad se procesen manualmente o por computadora. Sin embargo, los métodos de aplicación de procedimientos de Auditoría para reunir evidencia pueden ser influenciados por los métodos de procesamiento computarizado. El auditor puede usar procedimientos de Auditoría manuales, técnicas de Auditoría con ayuda de computadora, o una combinación de ambos para obtener suficiente material de evidencia. Sin embargo, en algunos sistemas de contabilidad que usan una computadora para procesar aplicaciones significativas, puede ser difícil o imposible para el auditor obtener ciertos datos para inspección, investigación, o confirmación sin la ayuda de la computadora. **(15:139)**

3.2.2 Nivel Nacional

El Instituto Guatemalteco de Contadores Públicos y Auditores publicó la norma de auditoría No. 26 “Auditoría en un Ambiente PED”. Los aspectos más importantes son los siguientes: **(14:42)**

➢ **Propósito**

Proporcionar los requerimientos adicionales necesarios que conlleva realizar una Auditoría en un ambiente de procesamiento electrónico de datos (PED). **(14:42)**

- **Objetivo y alcance**

El objetivo y alcance de una Auditoría en un ambiente PED. Sin embargo el uso de un computador cambia el procesamiento y conservación de la información financiera y puede afectar la organización y los procesamientos empleados por la entidad para alcanzar una adecuada estructura de control interno. En consecuencia los procedimientos utilizados por el auditor en sus evaluaciones pueden ser afectados por un ambiente PED. **(14:42)**

- **Capacidad y competencia**

Al realizar una auditoría en un ambiente PED, el auditor debe tener conocimientos suficientes sobre los equipos utilizados, (hardware y los programas utilizados (software), para planear su trabajo y entender como afecta el PED la evaluación de la estructura de control interno y la aplicación de los procedimientos de auditoría, incluyendo técnicas de auditoría con ayuda del computador. **(14:42)**

- **Trabajo efectuado por otros**

El Auditor no puede nunca delegar su responsabilidad para formarse conclusiones de auditoría importantes o para formarse y expresar su opinión sobre la información financiera. En consecuencia, cuando delega trabajo a asistentes o usa el trabajo de otros auditores o expertos, el auditor debe tener suficiente conocimiento PED para dirigir, supervisar y revisar el trabajo de asistentes con conocimientos PED o para obtener seguridad razonables de que el trabajo efectuado por otros auditores o expertos con conocimientos PED, es adecuado par su propósito aplicable. **(14:42)**

- **Planeación**

El auditor debe reunir información sobre el ambiente PED que sea relevante para el plan de auditoría, incluyendo información sobre:

- Como está organizada la función PED y el grado de concentración o distribución del procesamiento por computador a través de la entidad.
- El hardware y software de computación usados por la entidad.
- Las aplicaciones significativas procesadas por el computador, la naturaleza del procesamiento (por ejemplo lotes, en línea, etc.) y las políticas de conservación de datos.
- Implementación de proyectos de nuevas aplicaciones o modificaciones a las aplicaciones existentes. **(14:43)**

En la consideración de su plan general de auditoría debe tomarse en cuenta asuntos tales como:

- Determinar el grado de confianza, si es el caso, que espera depositar en los controles PED en su evaluación global de la estructura de control interno.
- Planear como, dónde y cuándo serán revisadas las funciones de PED, incluyendo la programación de expertos PED en donde sea aplicables.
- Planear procedimientos de Auditoría usando técnicas de Auditoría con ayuda del computador.

➢ **Sistema de contabilidad**

Durante la revisión y evaluación preliminar de la estructura de control interno, el auditor debe obtener conocimiento del sistema de contabilidad para comprender el ambiente general de control y del flujo de transacciones. Si el auditor planea apoyarse en controles internos para efectuar su auditoría, debe tomarse en cuenta los controles manuales y por computadora que afectan la función PED y los controles específicos sobre las aplicaciones contables relevantes. **(14:43)**

➢ **Evidencia de auditoría**

Un ambiente PED puede afectar la aplicación de procedimientos de cumplimiento y sustantivos en diversas formas:

- Puede requerirse el uso de técnicas de auditoría asistidas por computadora, debido a la ausencia de documentos de entrada y salida y soporte.

- La oportunidad de los procedimientos de auditoría puede verse afectada debido a que la información puede no ser conservada en los archivos del computador por un tiempo suficiente largo para uso de auditoría.

- La eficacia y eficiencia de los procedimientos de auditoría se incrementan con el uso de técnicas asistidas por computadora, así como la calidad y cobertura de cálculos y períodos de tiempo. **(14:43)**

3.2.3 Objetivos de la Auditoría Interna de Sistemas de Información

La Auditoría Interna de Sistemas de Información tiene como objetivo fundamental emitir informes sobre la situación del control interno así como identificar los principales riesgos que afectan el proceso electrónico de datos, para que la administración pueda realizar las correcciones que considere oportunas. **(13:36)**

Se identifican los siguientes objetivos:

- Verificar la existencia de controles sobre las operaciones y procesos.

- Verificar la existencia de políticas de seguridad.
- Verificar la existencia de planes de capacitación y carrera.
- Verificar la adecuada segregación de funciones.
- Evaluar la capacidad del recurso humano.
- Evaluar el uso y aprovechamiento de los recursos asignados.
- Evaluar el cumplimiento de las metas, planes y actividades.
- Evaluar la protección de personal y del equipo.
- Evaluar el soporte y atención de problemas.
- Verificar la confiabilidad de la información
- Verificar el uso eficiente de los recursos.

3.2.4 Funciones de la Auditoría de Sistemas de Información

Dentro de las funciones de la Auditoría de Sistemas de Información están la de comprobar la eficiencia y eficacia del sistema. Así mismo deberá detectar fisuras o vulnerabilidades en la seguridad del sistema, para evitar accesos, modificación o sustracción de información no autorizados.

Así mismo se deberá realizar el análisis de las operaciones y procesos contenidos en los manuales de procedimientos y políticas de seguridad informática, que una entidad ha adoptado, para garantizar la confidencialidad, integridad, seguridad y disponibilidad de la información que se procesa a través de medios electrónicos.

3.2.5 Conocimientos del personal que realiza Auditoría de Sistemas de Información

Es importante que el personal que realiza Auditoría de Sistemas de Información cuente con conocimientos generales de los procesos relacionados con Tecnología de Información, principales riesgos que afectan al departamento de Informática. También deberá contar con flexibilidad para adaptarse a cambios imprevistos, mismos que se derivan del continuo avance de la tecnología. Estos conocimientos serán utilizados en la planificación y realización de la auditoría, así como, cuando se emita el informe.

A continuación se indica la escolaridad y principales conocimientos que deberá acreditar el auditor de sistemas de información:

- Graduado de la carrera de Contador Público y Auditor.
- Conocimientos de la organización y principales operaciones del departamento de Informática.
- Conocimiento del sistema central, manejo de comunicaciones, bases de datos y redes.
- Conocimiento de riesgos que afectan la tecnología de información.
- Capacidad de redacción para emitir los informes.
- Flexibilidad para adaptarse a cambios.
- Actualización en los diversos sistemas de información, disponibles en el mercado.

3.3 Entorno legal que rige la Auditoría de Sistemas de Información en Guatemala.

En Guatemala actualmente no existe ninguna ley específica que regule la actividad de de la Auditoría de Sistemas de Información. No obstante lo comentado anteriormente si existen requerimientos a observar por las instituciones que utilicen tecnología de información tales como lo comentado en la Ley de Bancos y Grupos Financieros en su artículo número 55 indica lo siguiente: “Los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, según sea el caso, la administración, de riesgos de crédito, de mercado, de tasas de interés, de liquidez, cambiario, de transferencia, operacional y otros a que estén expuestos”.

CAPÍTULO IV

AUDITORÍA INTERNA EN EL DEPARTAMENTO DE INFORMÁTICA DE UNA INSTITUCIÓN BANCARIA

4.1 Estándares y metodologías internacionales

Para la realización de la Auditoría de Sistemas de Información existen metodologías y estudios realizados por instituciones interesadas en la mejora de estos procesos.

En la presente tesis se logró identificar que derivado del soporte y grado de madurez la metodología de ISACA (Asociación de auditoría y control de sistemas de información), como la más adecuada para realizar las revisiones de auditoría de sistemas de información, en un departamento de Informática de una institución bancaria.

A continuación se presentan los principales estudios y recopilaciones internacionales efectuadas referentes a la Auditoría de Sistemas de Información.

4.1.1 Metodología de ISACA

ISACA (Asociación de auditoría y control de sistemas de información). Fue fundada en 1969, con el objetivo de proporcionar bases a los profesionales que se dedican a realizar Auditoría a los Sistemas de Información. Derivado de este trabajo ISACA ha implementado estándares, directrices y procedimientos para el desarrollo del trabajo de Auditoría a los Sistemas de Información **(12:2).**

- **Estándares**

  Los estándares elaborados ISACA son los siguientes: **(12:38**)

  - **Independencia profesional**

    En todos los asuntos relacionados con la realización de la auditoría, el auditor de sistemas de información deberá ser independiente del auditado.

  - **Independencia organizacional**

    La ejecución de la Auditoría de Sistemas de Información deberá ser independiente del área o actividad auditada.

  - **Ética y estándares profesionales**

    Se deberá acatar el código de ética. Este código proporciona una guía para que los auditores miembros de ISACA, observen una conducta profesional adecuada. Deberá además ejercer el debido cuidado profesional, incluyendo la observancia de los estándares profesionales de Auditoría aplicables.

- **Competencia profesional**

  El auditor deberá ser profesionalmente competente, poseyendo las habilidades y los conocimientos para realizar el trabajo de auditoría asignado. Deberá mantener la actualización profesional, a través de apropiada educación y capacitación profesional continua.

- **Planeación**

  Para la planeación y el alcance de la auditoría se deberá tomar en consideración los objetivos que se persiguen, así como el cumplimiento de las leyes y los estándares profesionales de auditoría aplicables.

- **Ejecución**

  Se deberá supervisar el trabajo realizado por el Auditor, para proveer certeza razonable de que los objetivos de la auditoría han sido alcanzados. Se deberá obtener evidencia competente y suficiente para documentar el trabajo realizado. Así mismo es conveniente considerar en el análisis del trabajo realizado la evaluación de riesgos, irregularidades y actos ilícitos.

- **Actividades de seguimiento**

  Después de presentar el informe de auditoría y en un plazo prudencial se deberá requerir información del avance de la implementación de las recomendaciones y corrección de errores.

➢ **Directrices**

ISACA ha emitido varias directrices que tienen como objetivo proveer información adicional sobre como cumplir con los estándares emitidos por ésta. **(12:731)**

➢ **Procedimientos**

Los procedimientos emitidos por ISACA proveen ejemplos de procesos que un auditor de sistemas de información deba seguir como guía en el desarrollo de su trabajo. **(12:731)**

4.1.2 Metodología COBIT

COBIT es una iniciativa llevada a cabo por el Instituto de Gobierno de Tecnología de Información. Este instituto fue creado en el año de 1998 en los Estados Unidos de América, y su objetivo fundamental es establecer normas y lineamientos para la utilización de tecnología de información.

COBIT ha sido desarrollado como una norma generalmente aplicable y marco aceptado para las buenas prácticas de seguridad y control de la tecnología de información que proveen una referencia para la administración, los usuarios, y los que ejercen la Auditoría de Sistemas de Información, el control y la Seguridad de TI. **(17:1)**

COBIT es una herramienta innovadora que toma en consideración las mejores prácticas para la evaluación del manejo, administración y evaluación de la tecnología de Información, vinculando los distintos procesos del negocio con los recursos informáticos que los sustentan.

COBIT también trata sobre los procesos de aseguramiento de la auditoría de TI, los cuales pueden resumirse como:

- Obtener una comprensión de los requerimientos del negocio, riesgos relacionados y medidas de control relevantes.
- Evaluar lo adecuado de los controles establecidos.
- Evaluar el cumplimiento a través de pruebas, sobre los controles establecidos, verificando si éstos están trabajando para lo que fueron diseñados y en forma consistente y continua.
- Substanciar el riesgo de los objetivos de control de riesgo que no han sido cumplidos, utilizando técnicas y/o consultando fuentes alternativas.

COBIT Comprende la evaluación de la Tecnología de Información desde cuatro áreas y treinta y cuatro procesos. Los dominios son: Planeación y Organización (11 objetivos), Adquisición e Implementación (6 objetivos), Entrega Servicios y Soporte (13 objetivos) y Monitoreo (4 objetivos).

Al tomar en consideración los 34 objetivos de control de alto nivel, las organizaciones pueden asegurar que cuentan con una estructura adecuada de gobierno y control para su entorno de TI, según el Instituto de Gobierno de Tecnología de Información. **(17:22)**

Respaldando estos procesos de TI existen más de 200 objetivos detallados de control necesarios para una implementación efectiva

COBIT, está dirigido a la dirección y al personal que provee servicios de información, departamentos de control y que realiza funciones de Auditoría.

4.1.3 Metodología ISO 17799

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de seguridad informática.

Esta norma es emitida por el British Standard Institute y la adaptación española de la norma se denomina UNE-ISO/IEC 17799.

La Norma ISO 17799 se divide en 10 áreas y 36 objetivos de control, a continuación se indican:

- Políticas de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de continuidad del negocio.
- Conformidad con la legislación.

4.1.4 Metodología ITIL

Las ITIL (Information Technology Infraestructura Library), fueron emitidas por la Agencia Central de Equipos y Telecomunicaciones (CCTA) del Reino Unido. Es una recopilación de las mejores prácticas para la gestión de servicios de Tecnología de Información, incluye cinco disciplinas que proporcionan las empresas flexibilidad y estabilidad para manejarlas, éstas son:

- Gestión de incidencias.
- Gestión de problemas.
- Gestión de cambios.
- Gestión de versiones.
- Gestión de configuración.

Incluye también cinco disciplinas que soportan los servicios TI de calidad y bajo costo de las empresas estas son:

- Gestión del nivel de servicio,
- Gestión de la disponibilidad,
- Gestión de la capacidad,
- Gestión financiera para servicios TI, y
- Gestión de la continuidad de los servicios TI.

El objetivo de ITIL en todas sus disciplinas es la definición de las mejores prácticas para los procesos y responsabilidades que hay que establecer para gestionar de forma eficaz los servicios de TI de la organización, y cumplir así los objetivos empresariales en cuanto a la distribución de servicios y la generación de beneficios.

Muchas organizaciones han adoptado el concepto de ITIL derivado que ofrece un enfoque sistemático y profesional de la administración de los servicios informáticos. Con la adopción de las guías proporcionadas por las ITIL, las organizaciones obtienen muchas ventajas, entre ellas se incluyen:

- Aumento de la satisfacción de los clientes.
- Reducción del costo de desarrollo de prácticas y procedimientos.

- Mejora en los flujos de comunicación entre el personal de informática y los clientes.
- Aumento de la productividad y del uso de capacidades y experiencia.

4.1.5 Metodología MOF

Las MOF (Microsoft Operation Framework), es una colección de recomendaciones, principios y modelos. Proporciona una guía técnica completa para lograr confiabilidad, disponibilidad, y capacidad de soporte técnico y de administración del sistema de producción crítico con productos y tecnologías de Microsoft.

Las MOF se basan en un conjunto de principios que subyacen a los dos modelos que componen los elementos centrales de la estructura, el modelo de equipo y el modelo de proceso para operaciones. Los modelos dividen las guías de operaciones en tres categorías fundamentales, personas, procesos y tecnología.

Las MOF abordan la naturaleza dinámica en constante evolución de los entornos informáticos distribuidos actuales. Esta estructura consta de seis principios que son básicos en el diseño y fundamentales para la aplicación con éxito:

- Proceso de Operación.
- Modelo de procesos.
- El rol de las personas.
- Modelo de Equipo.
- Manejo del Riesgo.
- Disciplina de Gestión del Riesgo

4.2 Metodología para realizar una auditoría de Sistemas de Información

La metodología a seguir por parte del auditor es la descripción secuencial del trabajo que realizará. Considerando las mejores prácticas para realizar auditoría de sistemas de información, a continuación se presenta de forma secuencial la forma de realizar un trabajo de auditoría de sistemas, dividido en tres fases que son: planeación, ejecución y dictamen. **(13:179)**

4.2.1 Primera fase, planeación de una Auditoría de Sistemas de Información

En la planeación se debe obtener información general sobre la organización, políticas así como tener claro el alcance que se quiere dar a la auditoría.

Se deberá realizar una visita preliminar para identificar los controles establecidos, comentarios de usuarios y aspectos generales del departamento.

En esta etapa se deberán identificar y asignar los métodos, herramientas, técnicas y procedimientos a utilizar por parte del personal que realizará la auditoría.

En la planeación se deberán asignar los recursos con que se cuenta, (humanos, físicos y económicos) y los documentos, manuales de operación, contratos de servicio que se deberán requerir.

Cuando el auditor tiene claros los objetivos, los métodos y las técnicas a utilizar, así como los recursos con que podrá contar, deberá elaborar un plan de trabajo, en el cual deberá integrar los recursos descritos anteriormente.

Es importante que para realizar cada actividad se cuente con un programa de trabajo, derivado que en éste se indican los objetivos de la revisión a realizar, el alcance, la documentación a requerir, la forma de revisarla, el personal a contactar y los procedimientos a seguir por parte del Auditor. **(13:186)**

La planeación se divide en:

- **Identificación del trabajo a realizar**

  Para realizar una adecuada revisión, así como maximizar los recursos, es necesario que se identifiquen los siguientes aspectos:

  - Área, operación, proceso o personal a evaluar.
  - Alcance.
  - Dependencia.
  - Personal participante.
  - A quien se informará sobre los resultados del trabajo realizado.

- **Investigación preliminar**

  Previo a iniciar el trabajo se deberá tener una visión general del departamento de Informática.

  En esta fase preliminar se deben utilizar los siguientes medios de recolección de información: observación, entrevistas, cuestionarios, etc.

  Así mismo deberá solicitarse la siguiente documentación: organigramas, manuales de puestos, descripción de sistemas, contratos de servicio, flujogramas de procesos etc.

  La investigación preliminar podrá apoyarse en el trabajo efectuado en informes posteriores de otros auditores.

  En la investigación preliminar se debe de incorporar la evaluación del control interno de la administración y del control de los equipos y el recurso humano. Durante la revisión del control interno el auditor debe estar en capacidad de entender la organización y las políticas y prácticas utilizadas.

Esta visita permite al auditor, conocer de manera preliminar los siguientes aspectos del departamento de Informática:

- Antecedentes del departamento.
- Forma de organización.
- Servicios prestados.
- Políticas y procedimientos generales.
- Objetivos a corto y largo plazo.
- Medidas de seguridad.
- Configuración de los equipos, capacidad instalada, recursos ociosos.
- Distribución del personal, equipos y sistemas.
- Conocimientos y habilidades del personal.
- Fortalezas y debilidades.
- Riesgos actuales y futuros.
- Opiniones de los usuarios.
- Posibles limitaciones en el trabajo a realizar.

➢ **Determinación de los alcances y objetivos**

Se deberán definir cuáles serán los alcances de la auditoría, indicando el período a auditar, las áreas que se abordará y el personal que participará en las entrevistas y cuestionarios. Así mismo deberá indicarse cuáles son los objetivos que persigue la Auditoría, identificando los generales y específicos.

- **Objetivo general**
  El objetivo general será el fundamento principal que el auditor tiene para realizar el trabajo.

  En una Auditoría al Departamento de Informática el objetivo general será evaluar los riesgos inherentes al uso de tecnología de información, así como, la emisión de recomendaciones para minimizar estos riesgos.

- **Objetivo específico**
  Son los fines particulares o individuales que se pretende alcanzar, tales como:

  - Evaluar la segregación de funciones.
  - Evaluar la existencia de una metodología de costeo de software.
  - Evaluar la dependencia a ciertos equipos y terceros. Etc.

➢ **Elaboración y planteamiento del programa de trabajo**

Para realizar adecuadamente una auditoría en Informática es necesario que después de haber realizado la planificación de la auditoría, se plasme en un documento denominado “plan de trabajo”. En este plan se distribuirán los recursos humanos, económicos y físicos con que se cuente, así como el alcance que se le dará a la revisión.

En el programa de trabajo de auditoría se identifican las actividades a realizar, asignando al personal que la realizará, así como el tiempo y recursos necesarios.

A continuación se presentan las siguientes definiciones de plan de trabajo:

"El programa de auditoría establece la naturaleza, oportunidad y alcance de los procedimientos del auditor, contribuye a informar al personal que lo ejecuta, sobre el trabajo que se ha de realizar, ayuda a organizar y distribuir el trabajo y sirve de protección contra posibles omisiones o duplicaciones". (9:321)

Los programas de trabajo de auditoría consisten de un listado de los procedimientos que se realizarán durante el trabajo de campo.

Estos procedimientos proporcionan:

- Una descripción del trabajo a realizar, dando instrucciones respecto a la forma de cómo se realizará.
- Una base para coordinar, supervisar y controlar la Auditoría.
- Como un registro del trabajo realizado". **(10:75)**

Con base a lo anterior un programa de trabajo deberá incluir lo siguiente:

- Objetivo de la revisión.
- Alcances de la revisión.
- Descripción del trabajo a efectuar
- Cronograma de trabajo.
- Informe a presentar.
- Bibliografía y normativa interna y externa a considerar.

➢ **Medios para la recopilación de información**

La recopilación de información es una parte importante del trabajo a realizar en una auditoría.

Esta recopilación de información se apoya no sólo de documentos sino que también a través de entrevistas con el personal auditado.

A continuación se describen los medios utilizados para recopilar la información.

- **Entrevista**
  La entrevista es la recopilación de información en forma directa con el personal auditado, constatando de esta forma sus conocimientos, experiencia y comentarios del trabajo que realiza.

Las entrevistas se utilizan para confirmar si en la práctica se utilizan los procesos plasmados en los diferentes manuales y políticas de procedimientos. **(8:134)**

Para realizar adecuadamente una entrevista es necesario conocer plenamente los manuales, políticas y procedimientos de la empresa evaluada. La entrevista deberá ser elaborada de acuerdo a una guía de preguntas necesarias para documentarla. Esta guía podrá sufrir modificaciones de manera que se pueda adaptar en el desarrollo de la entrevista.

- **Cuestionario**

Los cuestionarios son documentos impresos que contienen preguntas relacionadas al trabajo a realizarse. Las preguntas las responde el auditado de acuerdo a su criterio y experiencia. El cuestionario deberá contener preguntas sencillas, claras evitando confundir al auditado. **(8:134)**

- **Encuesta**

La encuesta es otra técnica utilizada para conocer la opinión de los usuarios del departamento de Informática. Se utilizan para conocer la calidad del servicio, oportunidad de resolución de problemas y comentarios generales. Tienen la ventaja de que los usuarios tienen libertad de expresar su opinión, ya que regularmente no se debe consignar el nombre del encuestado.

- **Observación**

La observación permite conocer como se realizan las actividades en el departamento de Informática. En la etapa de la observación el Auditor tiene la oportunidad de comparar la teoría con la práctica, es decir, lo establecido en manuales y políticas contra lo que realmente se hace.

- **Técnicas tradicionales para realizar Auditoría de Sistemas de Información**

Las técnicas son los métodos mediante los cuales el Auditor de Sistemas de Información obtiene evidencia para fundamentar su opinión.

La Auditoría de Sistemas de Información debe de apoyarse en las técnicas tradicionales, para comprobar la eficiencia y eficacia en la utilización de éstas.

Dentro de las técnicas tradicionales se encuentran: el examen, la inspección, la confirmación, la comparación, la revisión documental, las matrices de riesgos, etc. A continuación se definen:

- **El examen**

  Es la evaluación del conocimiento y cumplimiento de las funciones, procesos, actividades y operaciones por parte del personal auditado.

- **La inspección**

  Es análisis del cumplimiento de las funciones, procesos, actividades y operaciones por parte del personal auditado.

- **La confirmación**

  La confirmación es una técnica mediante la cual se solicita se nos informe o certifique si los datos que estamos reportando están conforme a sus registros. Generalmente se utiliza para las cuentas por cobrar, proveedores, cuentas corrientes, etc.

- **La comparación**

  La comparación se refiere a utilizar datos de otros meses o de otras empresas con características similares para medir la razonabilidad de los resultados obtenidos.

- **La revisión documental**

  La revisión documental es el examen a los documentos que respaldan las operaciones, manuales de puestos, procedimientos operativos, etc.

- **Lista de chequeo (check list)**

  Una lista de chequeo es un documento de inventario de actividades a evaluar o procedimientos que conforman una actividad, brindan la certeza al auditor de que se considerarán todos los temas y actividades en una auditoría.

- **Matriz de evaluación**

  Es un documento en el cual se asigna calificación de acuerdo a criterios a las diferentes operaciones realizadas en la empresa. Los criterios utilizados generalmente son a mayor cantidad de errores, se obtendrá una calificación de riesgo superior.

- **Técnicas asistidas por computadora (TAACs)**

Las técnicas especiales para Auditoría Asistidas por computadora, **(TAACs),** son herramientas utilizadas por el auditor de sistemas de información para recopilar datos del entorno de éstos ambientes.

El uso de las TAACs, está contemplado en la norma internacional de auditoría No. 1009 **(16:526)**

Generalmente se le denomina TAACs a cualquier técnica automatizada de auditoría, que utiliza un software especializado.

Las TAACs pueden efectuar diversos procedimientos de auditoría que incluyen:

- Pruebas de detalles de transacciones y saldos.
- Procedimientos de revisión analítica.
- Pruebas de cumplimiento de controles generales de sistemas de información.
- Pruebas de cumplimiento de controles de aplicación de sistemas de información.
- Pruebas de penetración y evaluación de vulnerabilidades de sistemas operativos.

El auditor de sistemas de Información deberá tener un entendimiento profundo de las TAACs y saber dónde y cuándo aplicarlas.

Las TAACs ofrecen las siguientes ventajas.

- Nivel reducido de riesgo de Auditoría, por cálculos manuales.
- Mayor independencia respecto al personal auditado.
- Cobertura de Auditoría más amplia y consistente.
- Disponibilidad de la información con mayor rapidez.
- Identificación oportuna de excepciones.
- Flexibilidad en tiempos para ejecución de programas.
- Incremento de la posibilidad para identificar desviaciones y debilidades de control interno.
- Mejora en el muestreo.
- Ahorro de tiempos y costos.

- **Software para realizar auditoría de sistemas de información**

El software de auditoría se refiere a los programas computacionales sofisticados que tienen la capacidad realizar cálculos a una gran velocidad, tomando como base archivos de información de diferentes plataformas y formatos.

Estos software proveen un medio independiente para obtener acceso a datos para su análisis y escrutinio por parte del auditor.

Sus principales características incluyen la habilidad para realizar cálculos matemáticos, estratificación, análisis estadístico, verificación de la secuencia, recálculos a bases de datos de tamaño considerable, en un tiempo menor y con mayor exactitud.

La utilización de estos programas permite el manejo de una gran cantidad de información, adicionalmente permite implementar procesos automáticos rutinarios que ahorran tiempo y permiten tener documentados los procesos a realizar.

A continuación se describen algunos Software para realizar Auditoría de Sistemas de Información:

- **ACL (Audit command lenguaje)**

  Es un software de auditoría, que analiza datos y genera informes, permite profundizar en el alcance del análisis transaccional de las operaciones. Aumenta la productividad del personal proporciona fiabilidad en los resultados obtenidos. Así mismo no se necesita ser un especialista para usarlo.

  ACL identifica tendencias, señala excepciones y áreas que requieren atención, localiza errores y posibles irregularidades, comparando y analizando los archivos según los criterios especificados por los usuarios, recalcula y verifica saldos.

  Analiza y determina la antigüedad de las cuentas por cobrar, cuentas por pagar u otras transacciones a las que afecta el tiempo transcurrido.

  ACL es capaz de recuperar ingresos perdidos o gastos, detectando pagos duplicados, secuencias numéricas incompletas en la facturación o servicios no facturados.

  Por otra parte ACL determina la aplicación de los controles y el cumplimiento de las normas.

- **IDEA (Interactive data extraction and analysis)**

  IDEA es un software que permite visualizar, analizar, manipular, muestrear o extraer datos de virtualmente cualquier tipo de archivo, sin importar su tamaño.

  IDEA es un software que presenta facilidad de uso, por esta razón se convirtió en una herramienta de un gran número de profesionales en auditoría, Contadores y Gerentes Financieros quienes lo utilizan para resolver problemas complejos de negocios.

El software de análisis general requiere bastante codificación o generación de reportes para satisfacer los objetivos de auditoría. IDEA está funcionalmente precodificado para hacer esto como una solución más segura y eficiente que las hojas electrónicas o que el software de base de datos utilizado para análisis general.

- **SQL**

  SQL es una herramienta para organizar, gestionar y recuperar datos almacenados en una base de datos informática. El nombre "SQL" es una abreviatura de structured query lenguaje (lenguaje de consultas estructurado). Como su nombre indica, SQL es un lenguaje informático que se puede utilizar para interaccionar con una base de datos.

  SQL es a la vez un lenguaje fácil de aprender y una herramienta completa para gestionar datos. Las peticiones sobre los datos se expresan mediante sentencias, que deben escribirse de acuerdo con reglas sintácticas y semánticas de este lenguaje.

➢ **Software para apoyo en la realización de Auditoría de Sistemas de Información**

- **Software para monitoreo de transacciones en tiempo real Monitor-Byte**

  Este software apoya la labor de auditoría, estableciendo una monitoreo permanente y en tiempo real sobre los sistemas informáticos utilizados por una institución, monitorea la ocurrencia de ciertos eventos definidos como críticos por las personas encargadas de la administración del mismo.

  Monitor-Byte mantiene una permanente vigilancia sobre el sistema, se activa cuando un evento crítico previamente parametrizado ocurre, generando un mensaje de “alerta” a la persona designada para su seguimiento y control, utilizando como medio de envío el servicio de correo electrónico, telefónico, fax u otro que se establezca. En este mensaje se envían las especificaciones de la “alerta” para que el usuario receptor la analice y determine las acciones que procedan.

  Este software ha sido diseñado para identificar las siguientes operaciones de clientes:

  - Retiros y pagos de cheques mayores a cierto monto.
  - Consultas repetitivas de saldos de cuentas.
  - Reversiones realizadas en “n” minutos.
  - Pagos de cheques por montos bajos en diferentes agencias.
  - Errores repetitivos.
  - Intentos de pagos de cheques.
  - Autorizaciones de sobregiros.

- Depósitos superiores al sueldo mensual en cuentas de empleados.
- Aperturas y cancelaciones de cuentas en un lapso corto de tiempo.
- Depósitos y/o retiros en cuentas superiores al saldo promedio y/o al perfil del cliente.

4.2.2 Segunda fase, ejecución de la Auditoría de Sistemas de Información

En esta etapa se aplican las técnicas y procedimientos de auditoría, así como los medios de recopilación de información. Se deja constancia a través de los papeles de trabajo.

Así mismo se identifican las desviaciones observadas en el trabajo realizado y deberán de presentarse al personal auditado para que realice la validación de las mismas.

En la ejecución de la auditoría se desarrollará el plan de trabajo, a través de los programas de trabajo específicos que se tengan para cada actividad.

El auditor de sistemas deberá evaluar los resultados de la evidencia obtenida, en donde verificará el cumplimiento de los controles, la normativa interna y externa.

Por otra parte en la evaluación de los controles el auditor deberá indicar si los controles satisfacen los requerimientos del negocio.

Como parte del trabajo a realizar se deberá juzgar la materialidad de los hallazgos, analizando la conveniencia de su inclusión en el informe.

Después de desarrollar el programa de trabajo y de recolectar la evidencia de auditoría, se debe evaluar la información que se recopiló para tener que el auditor forme su opinión.

Las desviaciones o situaciones especiales obtenidas en el trabajo realizado, deberán ser comentadas al gerente del departamento de Informática, así como las recomendaciones que se considere subsanarán las deficiencias observadas.

El desarrollo del trabajo se realiza de la siguiente manera:

- Empleo de las técnicas, procedimientos y herramientas seleccionadas.
- Asignación de los recursos, el personal conforme el plan de trabajo.
- Recopilación de documentación y evidencias.
- Examen de la documentación.
- Evaluación del cumplimiento de las políticas y procedimientos internos, así como la normaiva externa aplicable.
- Evaluación de procesos.
- Elaboración e integración de los papeles de trabajo.

- Identificación de problemas y desviaciones.
- Discusión de las desviaciones y situaciones especiales observas, así como de las recomendaciones propuestas que se considera podrían subsanarlas. **(13:235)**

Los puntos de revisión a evaluar en el departamento de Informática son los siguientes:

- **Evaluación de la administración del departamento de Informática**

  Se deberá obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos. A continuación se indican los requerimientos de información necesarios:

  - **Forma de organización del departamento**

    Para conocer las secciones del departamento de Informática de una institución bancaria, se deberá solicitar el organigrama.

  - **Plan estratégico**

    El plan estratégico es la planificación que contiene los objetivos a corto y largo plazo, así como las estrategias que ayudarán a cumplir y satisfacer la misión y metas de la organización.

  - **Objetivos a corto y largo plazo**

    Los objetivos a corto plazo deberán ser asignados de acuerdo a las necesidades inmediatas de la institución bancaria de tecnología de información. Los objetivos a largo plazo, contienen las expectativas de crecimiento de la institución bancaria, atención de nuevos segmentos de clientes.

    Los aspectos vitales para asignar objetivos a corto y largo plazo, son los siguientes:

    - Costos a asumir.
    - Costo-beneficio.
    - Requerimientos legales o regulatorios.
    - Expectativas de crecimiento.
    - Reingeniería de procesos.
    - Asignación de personal.
    - Evaluación de servicios Outsourcing.
    - Capacidad y tolerancia máxima al cambio de la tecnología actual.

- **Funciones y servicios prestados.**

  Se deberá solicitar el listado de funciones y servicios prestados por parte del departamento de Informática, que generalmente son:

  Area de Sistemas
  - Programación, mantenimiento del sistema principal y programas conectados a través de Interfases.
  - Análisis, programación e implementación de proyectos informáticos.
  - Asesoría en el uso de sistemas al personal operativo.

  Area de TI
  - Soporte técnico al hardware.
  - Asesoría en el uso y mantenimiento del hardware.
  - Mantenimiento de archivos ejecutables, antivirus, redes y sistemas de comunicación.
  - Instalación de software y hardware.
  - Reparación de hardware.
  - Impresión de listados.
  - Operatoria del sistema, procesos de cierre y mantenimiento a reportes en línea.

- **Antecedentes del departamento de sistemas**

  Los antecedentes del departamento de Sistemas permiten conocer la evolución del mismo y los cambios que ha sufrido en el tiempo, por lo que es conveniente solicitar la siguiente información, preferente de los últimos cinco años:

  - Cambios en la administración del departamento.
  - Cambios en el sistema central y mainframe.
  - Cambios de metodologías y estándares de programación.
  - Cambios de procedimientos en la selección de personal, equipo, proveedores, etc.

- **Políticas del departamento**

  Las políticas en un sentido amplio determinan lo que es permitido y lo que no. Las principales políticas de un departamento de Informática son:

  - Política de contratación de personal.
  - Política de ascensos.
  - Determinación de la confidencialidad para la información.

- Políticas de contratación de servicios y elección e proveedores.
- Atención de requerimientos y soporte.

- **Planes de carrera**

  Un plan de carrera es la expectativa de superación que puede tener un colaborador dentro de la institución. Deberá contener los requisitos de promoción, las escalas salariales y nombres de los puestos que podrá optar un colaborador si cumple los requerimientos previos para optar a uno.

- **Plan de capacitación**

  Derivado del constante avance de la Tecnología de Información y Sistemas es conveniente la inversión en actualización del personal del Departamento de Informática. Un plan de capacitación deberá contener el listado de requerimientos de actualización por año, asignando el personal que recibirá la capacitación y actualización correspondiente.

- **Formas de medición del desempeño y cumplimiento de metas**

  El desempeño del personal debe de ser evaluado. Por ser el departamento de Informática un departamento netamente de servicio, es conveniente que cuente con personal calificado, por lo que se deberá establecer un formato de medición el desempeño y cumplimiento de metas, fortalecido con los comentarios de los usuarios de tecnología de información, como parte integra de la evaluación.

- **Presupuestos y costos del área**

  Es conveniente que el departamento de Informática cuente con un presupuesto y costos por área, para poder estar en capacidad de indicar a la gerencia, las necesidades de equipo y software oportunamente. Así mismo partiendo de la determinación de los costos por hora hombre incurridos indicar cuál es el valor del desarrollo de sistemas, previo a iniciar un proyecto. Este costeo es sumamente importante derivado que permite determinar previamente al inicio el costo-beneficio de iniciar cualquier desarrollo de sistemas.

➢ **Evaluación de los sistemas**

Para dimensionar y conocer la funcionalidad del sistema, procedimientos y la forma de realizar el mantenimiento del mismo se deberá requerir los manuales de administración siguientes:

- Manuales e instructivos técnicos del software del sistema.
- Manuales e Instructivos de operación del sistema de cómputo.

- Manuales e instructivos de los usuarios del sistema.
- Manuales para la estandarización y garantía de calidad en el desarrollo de Sistemas.
- Manuales, instructivos y procedimientos para el procesamiento de información.
- Manuales e instructivos de mantenimiento lógico del sistema (software).
- Manuales e instructivos didácticos de apoyo.
- Otros manuales e instructivos para el desarrollo del sistema.
- Descripción de los sistemas de comunicación.
- Vulnerabilidades detectadas.
- Procesos críticos.
- Descripción genérica.
- Flujogramas que contengan procesos de entrada, proceso, back-up, y salida de la información.
- Fecha de instalación
- Condiciones de actualización, mantenimiento y utilización.
- Informes externos realizados con relación al Software.
- Vida útil y obsolescencia.

➢ **Evaluación de los equipos**

En esta evaluación el auditor deberá conocer las principales características, componentes y funcionamiento de la parte física de los sistemas, a fin de poder evaluar su aplicación uso y aprovechamiento, así como su función específica.
Los puntos principales de evaluación son los siguientes:

- No. de inventario del equipo, marca, fabricante, tipo, No. de serie.
- Descripción del sistema central.
- Listado de periféricos, (teclado, monitor, bocinas, unidades de cd, disket, usb).
- Manuales e instructivos técnicos del hardware, referentes a condiciones de uso, vida útil, mantenimiento preventivo, corriente eléctrica, protección contra agentes ambientales.
- Capacidad máxima, mínima de los discos duros, procesador y memorias.
- Descripción del sistema operativo necesario para administrarlo.
- Garantías y soportes del fabricante.
- Contratos de seguros.
- Vida útil estimada.
- Evaluaciones externas realizadas.

➢ **Evaluación del recurso humano**

Esta evaluación está dirigida a conocer la capacidad del personal del departamento de Informática. Se deberá obtener información referente a la forma de evaluar el desempeño y

comportamiento, condiciones de ambiente y trabajo, horarios, organización del desempeño, capacitación y supervisión, manuales de puestos.

- **Evaluación de procesos**

Un proceso es un conjunto de actividades o eventos que se realizan de acuerdo a un fin determinado.

Para tener idea de todos los procesos que se realizan dentro de un Departamento de Informática, se deberá solicitar un listado de procesos que se ejecutan, la descripción de los mismos, periodicidad de ejecución, responsables, problemas observados en su ejecución, así como las soluciones implementadas para corregirlos.

- **Evaluación del control interno**

El control interno Informático tiene como objetivo establecer las bases para la protección de la información, sistemas equipos y recurso humano, así como incrementar la seguridad de los recursos informáticos de una empresa, ante los diversos riesgos que le afectan. **(13:95)**

Por lo anterior se deberá evaluar la existencia de normas, políticas y procedimientos establecidos, para verificar su oportunidad, alcance, funcionalidad y actualización.

El control interno informático, deberá cubrir los diferentes procesos del área Informática.

Los puntos de control necesarios en un departamento de Informática son: **(13:95)**

- **Control sobre la organización del departamento de Informática.**
  - Estandarización de metodologías para el desarrollo de proyectos.
  - Asegurar que el beneficio de los sistemas sea el óptimo.
  - Elaborar estudios de factibilidad del Sistema.
  - Garantizar la eficiencia y eficacia en el análisis y diseño de Sistemas.
  - Vigilar la efectividad y eficiencia en la implementación y mantenimiento del Sistema.
  - Optimizar el uso del Sistema por medio de su documentación.

- **Control sobre el análisis, desarrollo e implementación de sistemas.**
  - Prevenir y corregir los errores de operación.
  - Prevenir y evitar la manipulación fraudulenta de la información.
  - Implementar y mantener la seguridad en la operación.

- Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información de la Institución.
- Verificar la estandarización y documentación de la programación.

- **Control para el ingreso, procesamiento, egreso y back-up de información.**
  - Verificar la existencia y funcionamiento de los procedimientos de captura de datos.
  - Comprobar que todos los datos sean debidamente procesados.
  - Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.
  - Comprobar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procesamiento de información.

- **Control sobre la seguridad de los equipos, sistemas y el personal.**
  - Controles para prevenir y evitar las amenazas, riesgos y contingencias que inciden en las áreas de sistematización.
  - Controles sobre la seguridad física del área de sistemas.
  - Controles sobre la seguridad lógica de los Sistemas.
  - Controles sobre la seguridad de las bases de datos.
  - Controles sobre la operación de los Sistemas.
  - Controles sobre la seguridad del personal del Departamento de Informática.
  - Controles sobre la seguridad de la telecomunicación de datos.
  - Controles sobre la seguridad de redes y sistemas multiusuarios.

➢ **Evaluación de los manuales de puestos del departamento de Informática**

Los manuales de puestos son los documentos formales donde se describen los requerimientos mínimos establecidos para poder desempeñar cada uno de lo puestos de un área de trabajo, en el departamento de Informática, así como para valorar las características, aptitudes y otros aspectos necesarios para cada puesto de trabajo.

La revisión de estos documentos permitirá conocer si se está cumpliendo con lo establecido en los manuales, así como para verificar la actualización correspondiente.

Como se indicó anteriormente los manuales de puestos deberán contener como mínimo la siguiente información:

- Nombre del puesto
- Nivel del puesto
- División del organigrama a la que pertenece el puesto
- Objetivo del puesto de trabajo
- Funciones del puesto.
- Escolaridad.
- Conocimientos necesarios.
- Atribuciones.
- Horarios.

- Aspectos generales del trabajo realizado.
- Flujogramas de procesos.
- Fecha de última actualización.

➢ **Evaluación de la seguridad**

La seguridad en un departamento de Informática puede dividirse en seguridad lógica y física.

- **Seguridad lógica**

  Los objetivos de la seguridad lógica deben de asegurar ser la prevención o minimización del riesgo a que está expuesto el software y la información, que proviene principalmente de los virus informáticos, copias o uso no autorizado del software o la información. **(12:480)**

  Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues solicitan al usuario una contraseña antes de permitirle el acceso a información confidencial.

  Un esquema adecuado de seguridad debe abarcar los siguientes puntos:

  - Definición de las políticas de seguridad
  - Organización y división de responsabilidades
  - Seguridad física y contra catástrofes (incendio, terremotos, inundaciones, etc.)
  - Prácticas de seguridad del personal
  - Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
  - Aplicación de los sistemas de seguridad, incluyendo datos y archivos
  - El papel de los auditores, tanto internos como externos, para la medición del cumplimiento de las políticas establecidas.
  - Planeación de programas de desastre y su prueba.

  Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo-beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

  Clasificar las aplicaciones en términos de riesgo (alto, mediano, pequeño) de la siguiente manera:

  - Identificar las aplicaciones que tengan un alto riesgo.
  - Cuantificar el impacto en el caso de suspensión del servicio de las aplicaciones con un alto riesgo.
  - Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.

La justificación del costo de implantar las medidas de seguridad para poder clasificar el riesgo e identificar las aplicaciones de alto riesgo, se debe preguntar lo siguiente:

¿Qué sucedería si no se puede usar el sistema? ¿Qué implicaciones tiene el que no se obtenga el sistema y cuánto tiempo podríamos estar sin utilizarlo? ¿Existe un procedimiento alterno y qué implicaciones tendría utilizarlo? ¿Qué se ha hecho para un caso de emergencia?

Una vez que se ha definido, el grado de riesgo, hay que elaborar una lista de los sistemas con las medias preventivas que se deben tomar, así como las correctivas en caso de desastre señalándole a cada uno su prioridad.

Es importante contemplar que al implementar sistemas de seguridad puede reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

- **Seguridad física del personal y equipos**

El objetivo de la seguridad física es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo. **(12:483)**

Entre las precauciones que se deben revisar están:

- Equipos de aire acondicionado para mantener temperaturas adecuadas para el funcionamiento de las computadoras.
- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
- En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan.
- También se debe verificar si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
- Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.

Por lo anterior, a continuación se presenta un listado de las medidas de seguridad a verificar en el departamento de Informática para la protección de los equipos.

  - Sistema para el control en el ingreso y egreso de los equipos y personal.
  - Personal de seguridad para el ingreso a las instalaciones.

- Segregación de funciones.
- Controles para el personal fuera del horario.
- Vigilancia y monitoreo a través de video.
- Existencia de alarmas detectoras de humo, inundaciones y de accesos no autorizados.
- Puerta de emergencia.
- Prohibición para ingerir alimentos en los escritorios de trabajo.
- Inventario actualizado de equipos.

➢ **Seguimiento a los proyectos informáticos**

Para atender adecuadamente los requerimientos de la gerencia y/o de los clientes, es necesario que el departamento de Informática modifique sustancialmente el sistema o lo cambie completamente. Así mismo los cambios o modificaciones al Sistema pueden provenir de requerimientos de las entidades reguladoras. **(12:186)**

Para evaluar los cambios y/o mejorar al Sistema, es conveniente que el auditor de sistemas participe activamente, para garantizar que los proyectos cumplan con las expectativas de la gerencia y los usuarios finales.

A continuación se comentan los puntos principales que deberá contar un adecuado seguimiento de los proyectos informáticos:

- **Plan maestro del proyecto**

  Es un programa previamente establecido a la iniciación del proyecto que deberá incluir los objetivos que se persiguen con el cambio del Sistema, los recursos a utilizar, responsabilidades de la Institución y de los Proveedores, plan de aseguramiento de calidad, aceptación de riesgos y se deberá mantener la retroalimentación permanente a la Gerencia de los avances del proyecto. **(12:192)**

- **Líder del proyecto**

  Se deberá nombrar un encargado que tendrá a su cargo la administración del proyecto, sus atribuciones serán las siguientes:
  - Será el enlace entre la gerencia-proveedores del software-usuarios.
  - Será el encargado de que se cumpla el plan maestro del proyecto.
  - Deberá retroalimentar a la gerencia en forma continua los avances y retrasos en el proyecto.
  - Será el responsable directo del éxito o fracaso del proyecto. **(12:192)**

- **Determinación de los recursos a utilizar**

  Se deberá determinar los recursos a utilizar, considerando que para poner en marcha un proyecto informático es necesario como mínimo lo siguiente:

  - Recurso humano (programadores y personal operativo que validará la programación.
  - Costo de adquisición del nuevo software y equipo (hardware).
  - Costo de mantenimiento y licencias. **(12:192)**

- **Cronograma de trabajo**

  El cronograma de trabajo es la asignación de tiempos a las actividades que se considera serán necesarias para culminar el proyecto. **(12:192)**

- **Participación del departamento usuario en el desarrollo de proyectos**

  Para garantizar el éxito de los proyectos informáticos es necesario que se fomente la participación de los usuarios como pilar fundamental del proyecto, ya que son ellos quienes autorizarán la programación realizada por el departamento de Informática. **(12:192)**

- **Miembros y responsabilidades del equipo del proyecto**

  Se deberá asignar establecer y especificar las bases para asignar a los miembros del equipo del proyecto, así como definir las responsabilidades y autoridades que estarán investidos. El criterio para la asignación deberá estar basado en el conocimiento que posean estas personas de las operaciones realizadas por la empresa. **(12:192)**

- **Plan de pruebas**

  Para validar la funcionalidad del nuevo Sistema, es necesario crear un set de pruebas, estas pruebas deberán evidenciar la capacidad y calidad de respuesta, confiabilidad de la información presentada, así como el tiempo de respuesta. **(12:192)**

- **Aprobación de las fases del proyecto**

  Previo a dar por finalizada cada fase del proyecto es necesario que los miembros responsables del desarrollo del proyecto autoricen en su conjunto pasar a la siguiente fase del proyecto. **(12:192)**

- **Plan de aseguramiento de la calidad de sistemas**

  Para asegurar el cumplimiento de los estándares de servicio requeridos para el nuevo Sistema, es necesario crear un plan de aseguramiento de calidad, al que deberá darse seguimiento, en la vida del proyecto. **(12:192)**

- **Administración formal de riesgos de proyectos**

  Se deberá establecer un programa formal de riesgos para eliminar o minimizar los riesgos asociados a la administración de proyectos, así mismo es oportuno identificar la tolerancia máxima del riesgo razonable a asumir en cada fase del proyecto. Este plan deberá contemplar cuando será necesario parar el proyecto como medida extrema. **(12:192)**

- **Plan de entrenamiento**

  El plan de entrenamiento deberá estar orientado a capacitar a los analistas programadores del Departamento de Informática, y de los usuarios finales del Sistema. **(12:192)**

- **Documentación del Sistema**

  Se deberá solicitar al proveedor del sistema la documentación del nuevo Sistema. Esta documentación deberá contener como mínimo lo siguiente:

  - Especificaciones detalladas.
  - Configuraciones de los equipos.
  - Interfases.
  - Secuencia u orden lógico de los procesos.
  - Material de consulta para apoyo a usuarios.

- **Plan de revisión post-implementación**

  Como parte integral de las actividades del proyecto, se desarrollará un plan de revisión post-implementación, con la finalidad de determinar si el proyecto ha generado los beneficios planeados. **(12:192)**

➢ **Proceso de back-up de información**

Se deberá verificar los procedimientos utilizados para realizar los back-up de información. En este análisis se deberá constatar que se realicen oportunamente prueba a las copias de respaldo y que periódicamente se verifique la funcionalidad de éstas.

- **Pronóstico de carga de trabajo de los equipos y sistemas**

  Los pronósticos de carga de trabajo son utilizados como base para determinar oportunamente la adquisición de nuevos equipos y sistemas. A través de la comparación de los recursos utilizados en un período determinado y comparándolo contra las especificaciones del fabricante se pude determinar cuando será necesario realizar el reemplazo.

- **Manejo de incidentes operacionales y de usuarios (helpdesk)**

  La labor de atención de incidentes operacionales y la atención de los usuarios está a cargo de la mesa de ayuda a usuarios. Se deberá verificar que se documente adecuadamente el origen del problema y la solución adoptada. Esto con el objetivo de verificar reincidencia de problemas en los sistemas y equipos.

  Las funciones de helpdesk son:

  - Determinar el origen de los problemas y canalizar las acciones correctivas.
  - Documentar adecuadamente los reportes de problemas, y asegurar que sean resueltos en un tiempo razonable.
  - Atención a usuarios de sistemas computacionales resolviendo dudas y brindarles soporte.

- **Plan de contingencia**

  Se deberá verificar la existencia de un plan de contingencia, así mismo se deberá analizar si las medidas adoptadas en éste plan podrán recuperar en un tiempo razonable las operaciones del negocio. Los puntos a verificar son los siguientes:

  - Obtener una copia del manual.
  - Se deberán verificar las copias distribuidas del manual observando su actualización.
  - Revisar que se hayan identificado todas las actividades y procesos y que se hayan asignado prioridades a las actividades.
  - Verificar la existencia de copias despaldo y existencia de equipo capaz de restaurar las operaciones en una plazo prudencial (sitio alterno de operaciones).
  - Evaluar la actualización de teléfonos del personal involucrado y de los proveedores.
  - Constatar que el plan haya sido dado a conocer al personal responsable.
  - Analizar la forma utilizada para realizar la actualización del plan.
  - Requerir las pruebas efectuadas al plan de continuidad para verificar su funcionalidad.

- **Revisión de la base de datos**

  La revisión a la base de datos deberá orientarse a conocer el diseño, el acceso, la administración, las interfases y la portabilidad de ésta.

- **Diseño**

  La base de datos deberá contener nombres de campos que tengan nombres coherentes o que posean una descripción de los mismos. En los casos de bases de datos relacionales (bases de datos que se relacionan por un campo específico), se deberá verificar esta relación.

- **Acceso**

  Se deberá analizar los accesos permitidos, analizando quienes tienen acceso a realizar actualizaciones y quienes sólo de sólo lectura.

- **Administración**

  La administración deberá ser centralizada en un usuario con privilegios para realizar actualizaciones al diseño y a los datos contenidos en ésta. Así mismo deberá contemplarse las bitácoras de seguimiento a las operaciones de este usuario administrador.

- **Interfases**

  Para garantizar integridad y confidencialidad de la información, es conveniente verificar las interfases, para analizar los procedimientos de actualización, importación y exportación de información.

- **Portabilidad**

  La portabilidad se refiere al medio de consulta de los datos contenidos en ésta. Generalmente un buen medio de consulta es el Lenguaje Estructurado de consulta (SQL, Structured Query Language).

➢ **Auditoría a la red**

La red deberá contar con las siguientes medidas de seguridad: **(12:398)**

- Los usuarios deberán contar con contraseñas únicas y se deberá obligar a cambiarlas periódicamente. Las contraseñas deberán guardarse y presentarse en la pantalla encriptadas.

- La autorización a los usuarios deberá realizarse por escrito y deberán otorgarse de acuerdo al criterio de necesidad de saber y mínimo privilegio y separación de funciones.

- La estación de trabajo deberá deshabilitarse o bloquearse después de un período breve de inactividad, generalmente de cinco minutos.

- Deberá contarse con un único administrador, debiendo controlar los accesos o intentos de ingreso con la clave de éste.

- Deberá entrevistarse con los usuarios y con el administrador para conocer si tienen conocimiento de las medidas de seguridad y riesgos asociados al uso de la red.

- Para conocer si existen usuarios no autorizados deberá compararse contra las autorizaciones de ingresos y la nómina de la Entidad.

- Una buena práctica es tratar de ingresar con alguna clave no autorizada, para validar los controles existentes.

➢ **Cambios a programas**

Los cambios o mejoras a programas deberán ser autorizados por la gerencia del departamento de Informática, deberán ser probados en un ambiente de pruebas, para previo realizarlos en producción. Los objetivos de control son:

- Se deberá verificar que el acceso a bibliotecas y librerías de programas esté restringido.
- Todo cambio deberá ser probado y sus efectos deberán ser documentados y supervisados.

- El impacto de los cambios deberá ser analizado.

- El formulario de autorización del paso a producción deberá ser firmado de conformidad por el usuario, el programador y la Jefatura del Departamento de Informática.

➢ **Pista de Auditoría**

Las pistas de Auditoría son útiles al auditor de sistemas de Información para determinar los accesos a las diferentes opciones del sistema, por lo que se deberá verificar lo siguiente:

- Que se contemplen todos los programas y la red.
- Determinar el personal responsable de realizar la carga de la información, los privilegios con que cuentan.
- Pruebas para verificar que se tengan totales de control tendientes a asegurar que se estén cargados en el sistema de bitácoras todos los días y todos los sistemas.
- Determinar que personal tiene acceso a consulta de las bitácoras.
- Verificar si se está dando seguimiento a las bitácoras.
- Analizar la tendencia de consulta de los usuarios de los diferentes sistemas de información.

4.2.3 Tercera fase, informe de la Auditoría de Sistemas de Información

En esta fase se elabora el informe final.

- **Informe**

  El informe final es el documento donde se plasman los hallazgos realizados en la auditoría, se incluyen los procedimientos utilizados, las evaluaciones realizadas, entrevistas cuestionarios y las conclusiones y recomendaciones. **(13:271)**

  Un informe deberá contener las siguientes características: claridad, confiabilidad, sencillez en el vocabulario utilizado, oportunidad, efectividad, veracidad, congruencia, imparcialidad, exactitud, etc.
  Para realizar un informe se deberán observar los siguientes pasos:

  - Aplicar los instrumentos de recopilación de la información.
  - Registro de los hallazgos y desviaciones.
  - Discusión de hallazgos y desviaciones y soluciones propuestas para solventarlos.
  - Elaborar el informe.

  El informe deberá contener como marco referencial lo siguiente: introducción, objetivos, marco de revisión o alcance, limitaciones, resumen del trabajo, trabajo efectuado, conclusiones, recomendaciones, anexos.

- **Presentación del Informe Final**

  Los resultados obtenidos en las evaluaciones contenidas en el informe final deberán presentarse al gerente del departamento de Informática. Se deberá requerir un plan para la implementación de las recomendaciones.

- **Seguimiento de recomendaciones**

  En la presentación del informe final se deberá requerir un plan para la implementación de las recomendaciones. El papel del auditor es de seguimiento a los plazos que se establezcan para lograr la subsanación de estas deficiencias.

CAPÍTULO V

CASO PRÁCTICO DE UNA AUDITORÍA EFECTUADA AL CENTRO DE PROCESAMIENTO DE INFORMACIÓN DEL DEPARTAMENTO DE INFORMÁTICA DE UNA INSTITUCIÓN BANCARIA

Para dar a conocer la forma de efectuar una Auditoría Interna al Centro de Procesamiento de Información del departamento de Informática de una institución bancaria, a continuación se presentan los aspectos fundamentales que el auditor de sistemas debe contemplar.

5.1 Antecedentes del caso práctico

El análisis efectuado se realizó en el Banco Guatemalteco de Finanzas, S.A. A continuación se presentan los datos del banco:

- **Datos del banco Guatemalteco de Finanzas, S.A.**

  El banco Guatemalteco de Finanzas, S.A. es un banco privado que inició sus operaciones en el año de 1975. Las oficinas centrales están ubicadas en la zona 10 de la ciudad de Guatemala. La dirección del banco está a cargo del Consejo de Administración.

- **Estructura organizativa del banco**

  La estructura organizativa es de la siguiente forma: Gerencia General, Gerencia Financiera y de Riesgos, Asesoría Jurídica, Auditoría Interna, Oficialía de Cumplimiento, Gerencia de Recursos Humanos, Gerencia Administrativa, Gerencia de Negocios, Gerencia de Medios informáticos y Operaciones, que es de donde depende el Departamento de Informática.

- **Estructura organizativa del departamento de Informática**

  El departamento de Informática se conforma de la siguiente forma:

  Gerente, jefe del departamento de Sistemas, jefe de sección de Desarrollo de Sistemas, jefe de sección de Análisis de Sistemas. jefe del departamento de Infraestructura Tecnológica, jefe de sección de Soporte a la infraestructura tecnológica y operaciones, jefe de sección de Soporte técnico, y Mesa de ayuda (Help desk).

5.2 Aplicación del caso práctico

El caso práctico presentará la evaluación de los principales riesgos que afectan el Centro de Procesamiento de Información (CPI), que es el espacio físico dentro del departamento de Informática, que contiene la computadora central (mainframe) y el sistema principal de la entidad bancaria (software). Así mismo en el (CPI) se encuentran las impresoras de alto volumen, cableado de comunicaciones, las cintas de uso diario y demás equipos y documentación que por sus características debe de estar custodiadas para evitar accesos no autorizados.

Los objetivos de control interno a observar tienen la finalidad de asegurar que el Centro de Procesamiento de Información cuente con un ambiente que resguarde los equipos y el personal que los administra.

La recopilación de información se realizará con entrevistas y observación. Las técnicas a utilizar serán el examen, la inspección, la comparación, la revisión documental y lista de chequeo (check list).

A continuación se presenta la guía a utilizar para realizar el caso práctico:

5.2.1 Guía del caso práctico

INDICE DEL CASO PRÁCTICO

Cédula	A
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	04-01-2007
FECHA FIN:	05-01-2007

5.2.2 Papeles de trabajo del caso práctico

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

CARTA DE NOTIFICACION DE LA REALIZACION DE REVISIÓN DEL CONTROL INTERNO Y OPERACIONES EN EL CENTRO DE PROCESAMIENTO DE INFORMACIÓN

Sr. Jacobo Juárez
Gerente del Departamento de informática
Presente.

Sr. Juárez:

Se le comunica que conforme a plan de trabajo, se iniciará la revisión del control interno y operaciones en el Centro de Procesamiento de Información. Para realizar esta actividad se ha asignado al Sr. Marco Tulio Ramos.

Del resultado de la evaluación se enviará informe, con los hallazgos y recomendaciones.

Agradecemos su acostumbrada colaboración.

Atentamente:

EDWING RAMOS
Auditor Interno

CC. Archivo

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A1
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	04-01-2007
FECHA FIN:	05-01-2007

NOMBRAMIENTO PARA REALIZAR REVISIÓN DEL CONTROL INTERNO Y OPERACIONES EN EL CENTRO DE PROCESAMIENTO DE INFORMACIÓN

Sr. Marco Tulio Ramos
Asistente de Auditoría
Presente.

Sr. Ramos:
Se le comunica que ha sido nombrado para realizar revisión del control interno y operaciones en el Centro de Procesamiento de Información. Para llevar a cabo esta actividad se deberá apoyar en plan de trabajo elaborado para esta actividad.

Se asignan 5 días para el desarrollo de esta actividad. Deberá presentarse al departamento de Informática el día 4 de enero del presente año.

Atentamente:

EDWING RAMOS
Auditor Interno

Banco Guatemalteco de Finanzas, S.A.
Auditoria Interna.

Cédula	A2
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	04-01-2007
FECHA FIN:	05-01-2007

PROGRAMA AUDITORÍA INTERNA PARA REALIZAR REVISIÓN DEL CONTROL INTERNO Y OPERACIONES EN EL CENTRO DE PROCESAMIENTO DE INFORMACIÓN

I. INTRODUCCIÓN

El departamento de Informática deberá contar con un espacio dentro de sus instalaciones, dedicado al Centro de Procesamiento de Información que reúna las condiciones mínimas de seguridad que protejan los equipos y al personal asignado a éste.

II. OBJETIVO

Verificar el cumplimiento de los controles internos y políticas establecidas, para salvaguardar los equipos asignados al Centro de Procesamiento de Información.

III. ALCANCE

Los resultados serán referidos al 05 de enero de 2007 e incluirán los siguientes procedimientos:

- Entrevista con personal del departamento de Informática.
- Revisión de la documentación, para evaluar el cumplimiento de controles internos y políticas establecidas.
- Revisión de las instalaciones para verificar la adecuada salvaguarda de los activos.

IV. PROCEDIMIENTO

Para la revisión del control interno y operaciones se revisará lo siguiente:

CONTROL INTERNO

- **Revisión de control utilizado para el ingreso y egreso de equipos y personal**

  Se revisará la actualización de los formularios, con la siguiente información:

  - Fecha y hora de ingreso y egreso.
  - Nombre de la persona que ingresa y persona que la acompaña.
  - Motivo del Ingreso.
  - Constancia de Autorización para el ingreso de personal o egreso de equipos.

- **Claves de acceso**

  Para el control del ingreso del personal se utilizan claves de acceso y una tarjeta electrónica, se deberá verificar lo siguiente:

  - Listado de usuarios habilitados para el ingreso al Centro de Procesamiento de Información.

- Fecha de habilitación.
- Nombre del usuario.
- Fecha que expira la clave.
- Fecha de último acceso.
- Funcionario que autorizó la clave.
- Estatus de la clave.
- Verificar que la clave administrador esté siendo custodiada en sobre lacrado en bóveda de seguridad del banco.

➢ **Inventario de equipos**

Se deberá solicitar el registro del inventario de equipos, verificando su existencia física en el centro de cómputo, así como si se está efectuando la amortización del valor de los mismos.

➢ **Control de egreso de equipos**

Se deberá verificar la existencia de un control para el egreso de equipos, que deberá contener como mínimo los siguientes aspectos:

- Fecha del egreso.
- Nombre del equipo.
- Motivo del egreso.
- Nombre de la persona que recibe el equipo.
- No. de inventario.

➢ **Inventario de cintas de respaldo**

Para verificar la existencia física de las cintas de respaldo de información se solicitará el inventario de cintas de respaldo. Así mismo se deberá verificar la periodicidad con que se realizan los back- up de información, así como si se está efectuando las pruebas para comprobar su funcionalidad.

OPERACIONES Y PROCESOS

➢ **Seguridad para la protección de los equipos**

Para verificar que la adecuada protección de los equipos se deberá verificar la existencia de los siguientes equipos:

- Cámara de vigilancia. Verificar el medio de almacenamiento de las imágenes.
- Extintores de incendios. Comprobar que la carga no esté vencida.
- Aire acondicionado. Revisar cuando fue realizado el mantenimiento preventivo.
- Dispositivo para evitar inundaciones.
- Alarmas detectoras de `humo y temperatura. Verificar que se realicen las pruebas periódicamente.
- Reguladores de voltaje y UPS.

- Software y hardware para el control de accesos al Centro de Procesamiento de Información.

➢ **Contratos de mantenimiento**

El mantenimiento periódico a los equipos es necesario para mantenerlos en óptimas condiciones, se deberá verificar el cumplimiento y actualización de estos contratos. Así mismo verificar la suficiencia de los mismos.

➢ **Pólizas de seguro**

Para proteger los equipos se deben de contratar seguros que cubran el equipo y su instalación, así mismo se deberá verificar la actualización de los nuevos equipos y la fecha de vencimiento.

➢ **Plan de contingencia**

Un plan de contingencia deberá contemplar todo los procesos críticos de la organización, para reestablecer sus operaciones y deberá ser eficaz y eficiente, los aspectos legales, el impacto en el servicio del cliente.

Deberá verificarse la actualización de los procesos, misma que se deberá realizar por lo menos una vez al año, las pruebas para verificar su funcionalidad y la distribución al personal responsable.

V. INFORME

➢ **Elaboración de informe**

Se deberá preparar el informe de los hallazgos, indicando las recomendaciones que se considere subsanarán las debilidades de control interno.

➢ **Normativa**

Circular normativa No. 75-2006 “Control de accesos al Centro de Procesamiento de Información”.

➢ **Bibliografía**

Para apoyar la presente revisión se recomienda la lectura del libro “Auditoría en Informática” del autor José Antonio Echenique García.

➢ **Cronograma**

Para realizar esta revisión se asignan 5 días para la recolección de información, entrevistas y elaboración del informe. La revisión deberá iniciarse el 4 de enero de 2007 y se deberá entregar informe el 31 de enero, con el resultado del trabajo realizado.

➢ **Presentación de los resultados**

Se deberá presentar los resultados del trabajo realizado al Auditor Interno. Previo a presentar este informe se deberá de exponer los resultados al jefe del departamento de Informática, indicando las

observaciones y recomendaciones que se considere ayudarán a fortalecer el entorno de control interno, así mismo se deberá obtener el compromiso para la implementación de las recomendaciones.

- **Envío de informe**

  Luego de que se presenten los resultados se deberá enviar el informe dirigido al Jefe del Departamento de Informática. Se deberá copiar el informe a los siguientes puestos: Consejo de Administración, gerente general, gerente de la división de Medios Informáticos y jefe del departamento de Infraestructura Tecnológica.

Atentamente,

Edwing Ernesto Ramos Rosales
Auditor Interno

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A3
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	04-01-2007
FECHA FIN:	06-01-2007

ÍNDICE DE LAS MARCAS DE AUDITORÍA

Marca de Auditoría	Descripción de la Marca
☑	Verificado contra documento original.
✓	Revisado.
≠	Se observó el cumplimiento del procedimiento.
¥	Existe procedimiento formal.
£	Confirmado con el usuario final.
®	Revisado y confirmado con el usuario.
©	Revisado y cuadrado contra informe original.
µ	Confirmado con el proveedor del servicio.
Φ	Se revisó la copia física de la copia de respaldo.
β	Se revisó el funcionamiento del equipo en presencia del encargado.

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A4
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	04-01-2007
FECHA FIN:	08-01-2007

REVISIÓN DEL CONTROL UTILIZADO PARA EL INGRESO DE PERSONAL EXTERNO AL CENTRO DE PROCESAMIENTO DE INFORMACIÓN.

Conforme plan de trabajo se procedió a verificar el control utilizado para el ingreso de personal externo a las instalaciones del Centro de Procesamiento de Información. La utilización de este control está establecida en circular normativa No. Informática-75-2006. Los resultados se presentan a continuación.

Fecha	Nombre de la Persona que Ingresa	Motivo del Ingreso	Nombre de la persona que acompaña	Hora Ingreso	Hora Egreso	Marca de Auditoría
07-11-06	Vinicio Paz 1/	Revisión problemas en equipo AS-400				☑
10-11-06	Jorge Brolo 1/	Revisión en servidor de Reportes				✓
23-12-06	Marco Tulio Ramos	Revisión Servidor Ag. 25	Victor Pérez	9:55	10:56	☑
27-12-06	María Luisa Rosales	Revisión Impresora Multifuncional	Victor Pérez	14:25	17:05	☑
28-12-06	Hugo Suchini 1/	Revisión problemas en servidor de Contabilidad				✓
02-01-07	Edwing Ramos	Auditoría	Victor Pérez	08:30	12:30	☑
03-01-07	Mattew Pineda	Revisión Problemas Servidor Banca por Internet	Victor Pérez	15:35	16:45	☑
04-01-07	Ana Lorena Medina	Revisión problemas en servidor de Contabilidad	Victor Pérez	08:30	11:45	☑
06-01-07	Hugo Suchini 1/	Revisión servidor de reportes				✓

Índice de referencias

1/ Personal del departamento de Sistemas que no presentaron autorización para el ingreso al Centro de Procesamiento de Información.

Conclusión y recomendación.

Los resultados obtenidos en la presente revisión se consideran aceptables, sin embargo como se comentó en la referencia No. 1, el personal del departamento de sistemas debe de presentar autorización para el ingreso al Centro de Procesamiento de Información. Así mismo es importante que se documenten las soluciones implementadas, para la corrección de los problemas en los equipos, para tener estadísticas sobre la recurrencia de problemas.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A5
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	23-01-2007
FECHA FIN:	23-01-2007

REVISIÓN DE LAS CLAVES UTILIZADAS PARA EL ACCESO AL CENTRO DE PROCESAMIENTO DE INFORMACIÓN.

Conforme plan de trabajo se procedió a verificar las claves de acceso utilizadas por personal para el ingreso a las instalaciones del Centro de Procesamiento de Información. La asignación y custodia de claves de acceso está establecida en circular normativa No. Informática-80-2006. Los resultados se presentan a continuación.

Fecha de habilitación	Nombre de la Persona que tiene clave	Fecha que expira la clave	Fecha de último acceso	Funcionario que autorizó	Estatus de la clave	Marca de Auditoría
01-01-05	Administrador 1/	**Indefinida**	**01-01-06**	N/A	Activa	☑
01-01-06	Victor Pérez	**31-12-07**	**23-01-07**	Maynor Ramos	Activa	☑
06-02-06	Wendy Rivera	**30-06-07**	**23-01-07**	Maynor Ramos	Activa	☑
07-06-06	María Luisa Rosales	**30-06-07**	**23-01-07**	Maynor Ramos	Activa	
01-01-06	Juan Carlos Gómez 2/	**31-12-07**	**02-02-06**	Maynor Ramos	Activa	☑

Nota:

1/ Se observó que el password administrador no está siendo custodiado en un sobre lacrado en bóveda de seguridad del banco.

2 / La clave corresponde a ex-empleado, misma que no se ha dado de baja del sistema.

Conclusión y recomendación.

Se considera importante que la clave de administrador, que es la clave con mayores privilegios, sea custodiada en un sobre lacrado en la bóveda del banco, actualmente únicamente el Sr. Pérez tiene acceso a la misma. Así mismo al momento de que un colaborador termine su relación laboral con el banco, deberá de darse de baja al sistema, minimizando de esta forma la posibilidad de accesos no autorizados.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A6
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	04-01-2007
FECHA FIN:	08-01-2007

REVISIÓN DEL CONTROL DE EGRESO DE EQUIPOS DEL CENTRO DE PROCESAMIENTO DE INFORMACIÓN

Conforme plan de trabajo se procedió a verificar el control utilizado para el egreso de personal externo, a las instalaciones del Centro de Procesamiento de Información. El control para el egreso de equipos está establecido en circular normativa No. Informática-85-2006. Los resultados se presentan a continuación.

Fecha	Nombre del Equipo	Motivo del Egreso	Nombre de la persona que recibe	No. De Inventario	Marca de Auditoría
15-06-2006	Cámara de vigilancia	Reparación del monitor	Juan Zepeda	CPI-20	®
02-01-2006	Servidor de Compensación	Cambio de memoria	Hugo López	CPI-254	®
06-10-2006	Servidor de Compensación	Cambio de memoria y disco duro	Manuel Poz	CPI-254	®
05-12-2006	Servidor de Bitácoras	Cambio de fuente de poder	Juan Zepeda	CPI-258	®
07-12-2006	Servidor de Internet y Correo Electrónico	Cambio de disco duro	Manuel Poz	CPI-261	®

Nota:
En todos los casos no se observó la fecha de reingreso del equipo, ni el diagnóstico final de la reparación.

Conclusión y recomendación.

Se recomienda que se agregue una casilla al control de egreso de equipos, para que se lleve el registro de cuando ingresan los equipos, así mismo que se adjunte la boleta que indica cuál fue el motivo que originó el envió a reparación.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A7
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	04-01-2007
FECHA FIN:	08-01-2007

INVENTARIO DE EQUIPOS DE COMPUTACIÓN
UBICADOS EN EL CENTRO DE PROCESAMIENTO DE INFORMACIÓN

Conforme plan de trabajo se procedió a verificar el inventario de equipos ubicados en el Centro de Procesamiento de Información. Este inventario fue realizado comparando los registros en libros según la conciliación de saldos de la cuenta 110101.02 mobiliario y equipo. Los resultados se presentan a continuación.

Fecha Ingreso	Nombre del Equipo	Encargado del Equipo	Observaciones	Marca de Auditoría
01-01-2003	Computador central AS-400 1/	Victor Pérez	No. Inventario CPI-1	©
01-01-2005	Computador central AS-400	Victor Pérez	No. Inventario CPI-250	©
01-01-2005	Firewall	Victor Pérez	No. Inventario CPI -251	©
01-01-2005	IPS (equipo de prevención de intrusos)	Victor Pérez	No. Inventario CPI -252	©
01-01-2005	Servidor de Red	Victor Pérez	No. Inventario CPI -253	©
01-01-2005	Servidor de Compensación	Victor Pérez	No. Inventario CPI -254	©
01-01-2005	Servidor de Contabilidad	Victor Pérez	No. Inventario CPI -255	©
01-01-2005	Cintoteca	Victor Pérez	No. Inventario CPI -256	©
01-01-2005	Servidor de Respaldo	Victor Pérez	No. Inventario CPI -257	©
01-02-2005	Servidor de Bitácoras	Victor Pérez	No. Inventario CPI -258	©
01-04-2005	Servidor de Reportes e Históricos	Victor Pérez	No. Inventario CPI -259	©
01-04-2005	Servidor de Cajeros Automáticos	Victor Pérez	No. Inventario CPI -260	©
01-05-2005	Servidor de Internet y Correo Electrónico	Victor Pérez	No. Inventario CPI -261	©
06-06-2005	Impresora multifuncional Canon	Victor Pérez	No. Inventario CPI-500	©
31-12-2006	Servidor de Banca por Internet	Victor Pérez	No. Inventario CPI -262	©
S/F	Servidor Marca IBM Serie 52-32251500 2/			©

ÍNDICE DE REFERENCIA

1/ Este computador central fue sustituido el 01-01-2005, ya fue dado de baja en libros, sin embargo no se ha trasladado del CPI.

2/ Este servidor corresponde a equipo de prueba perteneciente a la empresa GBM de Guatemala. Este equipo está descontinuado, esta empresa no lo ha reclamado.

Conclusión y recomendación.

Se determinó que no se realizan inventarios, para verificar la existencia física de los equipos en el CPI. Se recomienda trasladar los equipos descritos en la referencia 1 y 2 para dar más espacio en el Centro de Procesamiento de Información.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A8
HECHO POR:	M.T.R.G.
REVISADO POR:	E.E.R.R.
FECHA INICIO:	08-01-2007
FECHA FIN:	12-01-2007

VERIFICACIÓN DEL INVENTARIO
DE CINTAS DE RESPALDO (REVISIÓN SELECTIVA)

Conforme plan de trabajo se procedió a verificar el inventario de cintas de respaldo de información ubicadas en las instalaciones del Centro de Procesamiento de Información. El control de las cintas de respaldo está establecido en circular normativa No. Informática-95-2006. Los resultados se presentan a continuación.

Fecha Proceso de cinta	Información Almacenada	Nombre de la persona que realizó la copia	Fecha de verificación de la funcionalidad	Nombre de quien revisó	Marca de auditoría
01-10-06	Archivo maestro de operaciones realizadas en agencia No. 5	Sebastián Pérez	No se ha realizado	Wendy Guzmán	✓
07-01-07	Archivo maestro de Clientes al 30-11-06	Martin Foster Gómez	08-01-2007	Marvin Poz	Φ
23-12-06	Archivo maestro de tarjetas de crédito al 22-12-2006	Sebastián Pérez	24-12-2007	Wendy Guzmán	Φ
07-01-07	Archivo maestro de saldos al 06-01-07	Martin Foster Gómez	08-01-2007	Marvin Poz	Φ
10-01-07	Archivo maestro de operaciones realizadas en agencia No. 5	Axel Rivera	14-01-2007	Wendy Guzmán	Φ

Conclusión y recomendación.

Según revisión a la circular normativa No. Informática-95-2006, se comprobó que en el mismo no se incluye la periodicidad con la que se deberá comprobar la utilidad de las cintas de respaldo. Únicamente se comprueban cuando se necesita restaurar un proceso. Por lo anterior es necesario que se incluya esta verificación en el proceso de back-up de información.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoria Interna.

Cédula	A9
HECHO POR:	M.T.R.G
REVISADO POR:	E.E.R.R.
FECHA INICIO:	04-01-2007
FECHA FIN:	08-01-2007

REVISIÓN DE LA SEGURIDAD FISICA DE LAS INSTALACIONES DEL CENTRO DE PROCESAMIENTO DE INFORMACIÓN

Conforme plan de trabajo se procedió a verificar los equipos utilizados para proporcionar la seguridad física, a las instalaciones del Centro de Procesamiento de Información, los resultados se presentan a continuación.

Fecha de revisión por parte del proveedor	Nombre del equipo	Observaciones	Marca de auditoría
30-09-2006	Cámara de vigilancia	Existen 3 cámaras distribuidas de la siguiente manera: al ingreso del CPI, monitoreando al operador de turno y el ingreso a la Cintoteca.	β
30-09-2006	Software y hardware de cámara de vigilancia	Este software tiene almacenado el monitoreo diario, realizado por las cámaras de vigilancia	β
25-10-2005	Extintores de Incendios 1/	Se observó la existencia de 4 extintores distribuidos adecuadamente.	β
31-12-2006	Aire Acondicionado	El aire acondicionado funciona adecuadamente.	β
02-01-2007	Dispositivo para evitar inundaciones	Los equipos están instalados a 25 centímetros del suelo y se cuenta con un dispositivo que absorbe a su interior el agua proveniente de inundaciones.	β
03-01-2005	Alarmas detectoras de humo. 1/	Se cuenta con 2 alarmas detectoras de humo distribuidas adecuadamente.	β
10-01-2007	Alarmas detectoras de temperatura y humedad	Para mantener la temperatura en 17 grados centígrados y prevenir daños ocasionados por humedad se cuenta con 2 alarmas detectoras.	β
20-01-2007	Reguladores de voltaje y UPS	Los equipos están protegidos con un regulador de voltaje así como un UPS capaz de mantener el servicio por 5 horas.	β
18-01-2007	Software y hardware control ingreso al CPI	Se comprobó que para el ingreso al CPI, es necesario utilizar tarjeta y un código personalizado, el registro de estos ingresos es registrado automáticamente y se puede consultar de manera cronológica.	β

INDICE DE REFERENCIA

1/ Según especificaciones del fabricante la carga de los extintores de incendios y las alarmas detectoras de humo, deberán de ser revisados una vez al año.

Conclusión y recomendación.

Se recomienda establecer un procedimiento escrito, en el cual se contemple la periodicidad necesaria para el mantenimiento de los equipos, según las especificaciones de los proveedores y/o lo establecido en los contratos de mantenimiento.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A10
HECHO POR:	M.T.R.G.
REVISADO POR:	E.E.R.R.
FECHA INICIO:	22-01-2007
FECHA FIN:	22-01-2007

VERIFICACIÓN DE LOS CONTRATOS DE MANTENIMIENTO DE EQUIPOS DEL CENTRO DE PROCESAMIENTO DE INFORMACIÓN

Conforme plan de trabajo se procedió a verificar los contratos de mantenimiento de equipos, del Centro de Procesamiento de Información, los resultados se presentan a continuación.

Fecha Vencimiento	Contrato	Empresa	Observaciones	Marca de Auditoría
01-12-2006	Mantenimiento de aire acondicionado.	AIRETEC, S.A.	A la fecha aún no se ha renovado contrato.	µ
01-12-2007	Mantenimiento a equipo de cómputo.	GBM, S.A.	El contrato está vigente y cubre adecuadamente el mantenimiento preventivo y correctivo a los equipos. Las cuotas están al día.	µ
31-10-2008	Mantenimiento a equipo de telecomunicaciones.	TELGUA, S.A.	Se observó que se realiza trimestralmente. Las cuotas están al día.	µ
02-01-2009	Mantenimiento a equipo UPS.	TELGUA, S.A.	Se determinó que el contrato fue utilizado en dos ocasiones por desperfectos en el equipo. Las cuotas están al día.	µ
31-12-2007	Mantenimiento a cableado.	TELGUA, S.A.	Se observaron boletas de servicio mensuales. Las cuotas están al día.	µ

Conclusión y recomendación.

Se estableció que no existe un procedimiento escrito para la negociación y control de los contratos de mantenimiento. Es importante que se lleve un control de los contratos de mantenimiento firmados, la fecha de vencimiento, los derechos y obligaciones adquiridos.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A11
HECHO POR:	M.T.R.G.
REVISADO POR:	E.E.R.R.
FECHA INICIO:	22-01-2007
FECHA FIN:	22-01-2007

VERIFICACIÓN DE LOS CONTRATOS DE SEGURO

Conforme plan de trabajo se procedió a verificar los contratos de seguros de equipos, del Centro de Procesamiento de Información, los resultados se presentan a continuación.

Fecha Vencimiento	Seguro	Empresa	Observaciones	Marca de Auditoría
1-05-2006	Responsabilidad civil.	LA SEGURIDAD DE CENTRO AMERICA, S.A.	Este contrato cubre accidentes en el área del departamento de Informática, a la fecha aún no se ha renovado contrato.	µ
31-12-2007	Equipo de cómputo.	LA SEGURIDAD DE CENTRO AMERICA, S.A.	Este contrato cubre el equipo de cómputo, en caso de incendios, inundaciones y robo. Se observó el pago de las cuotas por el año 2007.	µ

Conclusión y recomendación.

Se estableció que no existe un procedimiento escrito para la negociación y control de los seguros. Es importante que se lleve un control de los seguros, la fecha de vencimiento, los derechos y obligaciones adquiridos.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A12
HECHO POR:	M.T.R.G.
REVISADO POR:	E.E.R.R.
FECHA INICIO:	22-01-2007
FECHA FIN:	22-01-2007

VERIFICACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)

Conforme plan de trabajo se procedió a verificar el plan de continuidad del negocio, los resultados se presentan a continuación.

No.	Proceso	Observaciones	Marca de Auditoría
1	Copia del vigente plan de continuidad del negocio.	La copia obtenida fue actualizada el 20-12-2006	☑
2	Muestra de copias distribuidas del PCN.	Se obtuvieron 2 copias que fueron distribuidas al personal involucrado en el PCN y se observó que no fueron copiadas del original actualizado el 20-12-2006.	≠
3	Inventario de actividades y procesos críticos.	Se determinó que se identificaron los procesos críticos y fueron incluidos en matriz diseñada para el efecto, misma que está adjunta al PCN	¥
4	Listado de Proveedores y Clientes a informar con relación a la contingencia.	Actualizado.	≠
5	Determinación de prioridades en cuanto a la restauración de operaciones.	Se observó que se ordenaron las actividades y se asignó prioridad.	≠
6	Sitio alterno para el procesamiento de información	Existe sitio alterno, por una interfase se realiza automáticamente la réplica de todas las operaciones del sistema principal.	≠
7	Personal encargado de ejecutar el PCN	Según listado, se constataron los números telefónicos del personal encargado de ejecutar el plan.	£
8	Conocimientos del personal del PCN	Selectivamente se seleccionó al personal observando que cuentan con conocimientos suficientes para ejecutar el PCN.	≠
9	Actualización del PCN	En la revisión del PCN se comprobó que debe de ser actualizado por lo menos dos veces al año y deberá consignarse las fechas de actualización, se observaron estas actualizaciones los últimos dos años.	≠
10	Pruebas al PCN	Para verificar la funcionalidad del PCN está establecido que se realice una prueba al año, anotando la fecha y resultados de ésta. En la presente revisión se observó que el año 2006 no se realizó esta actividad.	✓

Conclusión y Recomendación.

Para garantizar la funcionalidad del plan de continuidad del negocio, es importante que cuando se actualice el plan, deberán de distribuirse las copias al personal involucrado. Así mismo deberá de realizarse pruebas para verificar la oportunidad de los procesos contenidos en este plan y documentar los resultados.

Marco Tulio Ramos
AUDITOR ASISTENTE

Vo. Bo. Edwing Ramos
AUDITOR INTERNO

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A13
HECHO POR:	M.T.R.G.
REVISADO POR:	E.E.R.R.
FECHA INICIO:	22-01-2007
FECHA FIN:	22-01-2007

MATRIZ DE RIESGO OPERACIONAL

Para representar el nivel de riesgo de cada aspecto evaluado en la presente auditoría e impacto en las operaciones del banco, a continuación se presenta una matriz de impacto en la cual se utilizaron colores para representar niveles de riesgo de la siguiente forma: verde (sin riesgo), amarillo (riesgo medio) y rojo (alto riesgo).

Area de control	Controles	Activos de información	Dependencia de activos	Dependencia de personal interno	Fiabilidad de Sistemas
Continuidad de sistemas	Control de acceso físico	**Amarillo**	**Verde**	**Amarillo**	**Verde**
	Back-up de información	**Amarillo**	**Amarillo**	**Verde**	**Amarillo**
	Inventario de equipos	**Amarillo**	**Amarillo**	**Verde**	**Verde**
	Contratos de mantenimiento y seguros	**Amarillo**	**Rojo**	**Verde**	**Verde**
	Plan de continuidad de negocios	**Verde**	**Rojo**	**Verde**	**Amarillo**
	Resultado de la evaluación	**Riesgo medio**	**Riesgo alto**	**Riesgo leve**	**Riesgo Medio**

La combinación de un riesgo alto con un riesgo medio incrementa la posibilidad de la materialización de una contingencia de importancia. Derivado de esta premisa se considera la siguiente categorización de riesgo:

Categorización de Riesgo

1 Aspecto calificado con color amarillo y ningún aspecto ponderado en color rojo = riesgo leve.
2 Aspectos calificados con color amarillo y ningún aspecto ponderado en color rojo = riesgo medio.
3 Aspectos calificados con color amarillo y un aspecto ponderado en color rojo = riesgo alto.

Conclusión

Los resultados obtenidos indican que el riego de continuidad de sistemas está siendo afectado por la falta de pruebas al plan de continuidad del negocio y la falta de renovación al contrato de mantenimiento del aire acondicionado y al seguro de responsabilidad civil.

5.2.3 Informe de la revisión del control interno y operaciones

Banco Guatemalteco de Finanzas, S.A.
Auditoría Interna.

Cédula	A14
HECHO POR:	M.T.R.G.
REVISADO POR:	E.E.R.R.
FECHA INICIO:	29-01-2007
FECHA FIN:	31-01-2007

Para: Jefe del departamento de Informática
De: Auditoría Interna
Asunto Revisión de la seguridad física de las instalaciones del Centro de Procesamiento de Información.
Fecha: 31 de enero de 2007

Como parte del programa de trabajo anual del departamento de Auditoría Interna, adjunto encontrará informe de la revisión efectuada al los controles existentes para salvaguardar la seguridad física del Centro de Procesamiento de Información.

Trabajo desarrollado

REVISIÓN DEL CONTROL INTERNO

- **Revisión del control de accesos al Centro de Procesamiento de Información.**

  Se estableció que según circular normativa No. Informática-75-2006 que indica que el personal del departamento de Sistemas deberá presentar autorización para el ingreso al Centro de Procesamiento de Información. Por lo anterior se considera conveniente que el personal asignado al Centro de Procesamiento de Información cumpla su función de solicitar la autorización para el ingreso.

- **Claves de acceso autorizadas para el ingreso al Centro de Procesamiento de Información.**

  En la revisión efectuada se identificaron 5 claves de acceso habilitadas para el ingreso al Centro de Procesamiento de Información. Se compararon los usuarios contra la nómina de empleados activos, estableciendo que la clave asignada al a clave del Sr. Juan Carlos Gómez, no se ha dado de baja, derivado que es un exempleado del Banco.

  Así mismo la clave de Administrador del Software de acceso al Centro de Procesamiento de Información no está siendo custodiada en un sobre lacrado en la Bóveda del Banco.

  Estos procedimientos están establecidos en Circular Normativa No. Informática-80-2006.

- **Inventario de equipos de computación ubicados en el Centro de Procesamiento de Información.**

Tomando el como base conciliación de saldos de la cuenta 110101.02 Mobiliario y Equipo, se realizó inventario de los equipos asignados al Centro de Procesamiento de Información. Derivado de esta revisión se obtuvieron resultados satisfactorios únicamente se observaron dos equipos que no están registrados en los libros del banco, de la siguiente manera:

- Computador central sin número de inventario ya fue dado de baja en libros.
- Servidor correspondiente a equipo de prueba perteneciente a la empresa GBM de Guatemala.

- **Control de egreso de equipos del Centro de Procesamiento de Información.**

El control para el egreso de equipos está establecido en circular normativa No. Informática-85-2006. En esta circular se establece que en el control auxiliar deberá consignarse la fecha de reingreso de los equipos, así mismo que se deberá adjuntar la boleta que indica cuál fue el motivo que originó el envió a reparación.

- **Inventario de cintas de respaldo.**

El control de las cintas de respaldo está establecido en circular normativa No. Informática-95-2006. Según revisión a esta circular normativa, se comprobó que en el mismo no se incluye la periodicidad con la que se deberá comprobar la utilidad de las cintas de respaldo. Únicamente se comprueban cuando se necesita restaurar un proceso. Por lo anterior es necesario que se incluya este aspecto en la circular normativa.

REVISIÓN DE OPERACIONES Y PROCESOS

- **Revisión de la seguridad física de las instalaciones del Centro de Procesamiento de Información.**

Como parte importante del trabajo efectuado analizamos la seguridad física de las instalaciones del Centro de Procesamiento de Información. Derivado de este trabajo se determinó que no existe un procedimiento escrito para el mantenimiento de los equipos. Un procedimiento para el mantenimiento a los equipos asigna la periodicidad necesaria de mantenimiento a los equipos. Actualmente no se ha dado mantenimiento preventivo a los extintores de incendios, ni a las alarmas detectoras de humo.

- **Contratos de mantenimiento y seguros.**

Se estableció que no existe un procedimiento escrito para la negociación y control de los contratos de mantenimiento ni de seguro. Es importante que se lleve un control de los contratos de mantenimiento firmados, la fecha de vencimiento, los derechos y obligaciones adquiridos. A la fecha se encuentran vencidos los contratos de mantenimiento de aire acondicionado y el seguro de responsabilidad civil.

- **Plan de continuidad del negocio.**

  El Banco cuenta con un Plan de Continuidad del Negocio, sin embargo se observó que el 20 de diciembre de 2006 se realizó la actualización anual, sin embargo no se distribuyeron las copias al personal involucrado, así mismo no se han realizado pruebas para verificar la oportunidad de los procesos contenidos en este plan y documentar los resultados.

- **Plan de acción para mejora de los riesgos detectados**

Riesgo	Responsable	Fecha para la corrección
Control de acceso físico	Victor Pérez	31-06-2007
Back-up de información	Victor Pérez	31-06-2007
Inventario de equipos	Victor Pérez	31-06-2007
Contratos de mantenimiento y seguros	Victor Pérez	31-06-2007
Plan de continuidad de negocios	Victor Pérez	31-06-2007

5.3 Resultados del caso práctico

CONCLUSIONES DEL CASO PRÁCTICO

Derivado de la revisión de los procedimientos y normativa interna y tomando en consideración la matriz de impacto de riesgos detectados, se obtuvieron las siguientes conclusiones:

1. **Riesgo leve**
   - Se observaron dos equipos obsoletos ubicados en el Centro de Procesamiento de Información, que ocupan espacio físico.

   - No se cuenta con un control de las reparaciones efectuadas a equipos, así como de la fecha en que fueron devueltos al Centro de Procesamiento de Información.

2. **Riesgo medio**
   - Se establecieron accesos no autorizados de analistas programadores del sistema al Centro de Procesamiento de Información, por incumplimiento de normativa interna.

   - Se observó una clave de acceso al Centro de Procesamiento de Información habilitada perteneciente a exempleado del Banco.

   - Se determinó falta de custodia de clave Administrador de software de control de acceso al Centro de Procesamiento de Información.

- Se comprobó falta de pruebas para verificar la funcionalidad de las cintas de respaldo de información.

3. Riesgo alto

- Se observó que el contrato se mantenimiento del aire acondicionado y el de seguro de responsabilidad civil están vencidos, por ausencia de un control en la fecha de vencimiento.

- Se determinó que las copias del Plan de Continuidad del Negocio vigentes no fueron distribuidas al personal responsable de implementarlo así como ausencia de pruebas para verificar la funcionalidad del Plan.

RECOMENDACIONES DEL CASO PRÁCTICO

1. Es conveniente realizar inventarios periódicos a efecto de verificar la existencia física de los equipos en el Centro de Procesamiento de Información. Así mismo trasladar los equipos que no figuran en libros del Banco a donde corresponda.

2. Se sugiere implementar un control para dejar constancia la fecha de ingreso de los equipos en caso de reparaciones, así como el diagnóstico por el cual se originó el egreso del Centro de Procesamiento de Información.

3. Se recomienda fortalecer los controles a efecto de cumplir lo establecido en la normativa interna, referente a los ingresos de personal externo, depuración de claves de acceso de excolaboradores y custodia de clave Administrador del Software para el control de acceso al Centro de Procesamiento de Información.

4. Se recomienda establecer por escrito la periodicidad con la que se deberán realizar las pruebas a las cintas de respaldo de información, para verificar su funcionalidad.

5. Es oportuno contar con un control de la fecha de vencimiento de los contratos de mantenimiento, las cuotas y los derechos y obligaciones contraídos.

6. Se considera necesario que al realizar la actualización del Plan de Continuidad del Negocio, se asegure distribuir las copias del Plan actualizado al personal involucrado, así como dejar por escrito la periodicidad de las pruebas a este Plan y documentar los resultados para analizar los resultados y medir la funcionalidad de éste.

EDWING ERNESTO RAMOS ROSALES

Auditor Interno

EERR/nmdg

cc Gerente General
Gerente de la División de Medios Informáticos
Jefe del Departamento de Infraestructura Tecnológica

CONCLUSIONES

1. Para el buen funcionamiento de un departamento de Informática será necesario que éste actúe bajo la dirección de un comité de dirección informática. Este comité le proporcionará las directrices de actuación. Las instalaciones del departamento de Informática deberán contar con condiciones de seguridad que permitan proteger adecuadamente los equipos y sistemas sensibles de la organización.

2. La Auditoría de Sistemas de Información es necesaria en una institución bancaria derivado que identifica a través de sus evaluaciones, procedimientos e informes, los principales riesgos inherentes al uso de tecnología de información y las sugerencias para minimizar estos riesgos.

3. Por el continuo avance en la tecnología de información y su consiguiente utilización en las diferentes organizaciones financieras y ante el incremento de los diferentes riesgos inherentes al uso de ésta, así como para apoyar la actividad de Auditoría de Sistemas de Información, es necesario que se cree una regulación específica en el tema de riesgo de información, que proporcione los lineamientos a cumplir por parte de las organizaciones que la utilizan.

4. El Auditor de Sistemas de Información con el apoyo de la alta gerencia de la institución, deberá contemplar en el desarrollo de su trabajo los lineamientos contenidos en la norma internacional de Auditoría de Sistemas de Información y las metodologías internacionales emitidas por ISACA, COBIT, ITIL, MOF, ISO 17799. Así mismo es importante que se identifiquen los procesos clave de el departamento de Informática en la matriz de riesgo tecnológico para su monitoreo y evaluación, contemplando la actualización necesaria cuando se realicen cambios de importancia.

5. En la presente investigación se comprobó la hipótesis planteada referente a la dependencia que tienen las instituciones bancarias a la utilización de la tecnología de información, así como a la importancia de que la Auditoría Interna cuente con personal que pueda identificar oportunamente los riesgos que afectan el uso de tecnología de información.

RECOMENDACIONES

1. Que el departamento de Informática de una institución bancaria funcione bajo la dirección de un comité de dirección informática, para asegurar que cumpla su misión y visión así como monitorear su adecuado funcionamiento. Así mismo para evitar accesos no autorizados o sustracción de información y equipos es necesario que el departamento de Informática cuente con un espacio físico restringido y protegido. Deberá contar con procesos escritos y normativa interna.

2. Que el departamento de Auditoría Interna de una institución bancaria realice evaluaciones al departamento de Informática, para identificar oportunamente riesgos y debilidades de control interno, comunicando a través de sus informes las recomendaciones que se consideren ayudarán a solventar los problemas detectados.

3. Que la Superintendencia de Bancos, eleve a consideración del Congreso de la República, la conveniencia de autorizar una normativa específica que establezca los lineamientos a cumplir por parte de las instituciones bancarias para la utilización de tecnología de información.

4. Que la utilización de estándares internacionales recopilados en las mejores prácticas de gestión de tecnología de información proporcionan al auditor de sistemas de información una guía clara y ordenada para realizar las evaluaciones en un departamento de Informática.

5. Que derivado de la dependencia que tienen las instituciones bancarias a la utilización de la tecnología de información, se considera oportuno que la administración de estos departamentos y la Auditoría Interna, se capacite constantemente en las mejores prácticas para la gestión y administración de ésta, para analizar oportunamente los cambios y minimizar los riesgos inherentes a su uso.

BIBLIOGRAFIA

1. Congreso de la República de Guatemala
   Constitución Política de la República de Guatemala.

2. Congreso de la República de Guatemala
   Decreto No. 16-2002 Ley Orgánica del Banco de Guatemala.

3. Congreso de la República de Guatemala
   Decreto No. 17-2002 Ley Monetaria.

4. Congreso de la República de Guatemala
   Decreto No. 18-2002 Ley de Supervisión Financiera.

5. Congreso de la República de Guatemala
   Decreto No. 19-2002 Ley de Bancos y Grupos Financieros.

6. Congreso de la República de Guatemala
   Decreto No. 58-2005 Ley para Prevenir y Reprimir el Financiamiento al Terrorismo.

7. Congreso de la República de Guatemala
   Decreto No. 67-2001 Ley Contra el Lavado de Dinero u Otros Activos.

8. Echenique García, José Antonio
   Auditoría en Informática
   Editorial McGraw Hill.
   México. 2001.

9. Enciclopedia de la Auditoría
   Editorial Océano
   España. 1996.

10. Kell Ziegler, Walter William
    Auditoría Moderna
    Compañía Editorial Continental
    México. 1987.

11. Luis Emilio Barrios Pèrez
    Leyes Bancarias
    Editorial Ediciones Legales Comercio e Industria,
    Guatemala. Año 2000.

12. Manual para la preparación para el Examen CISA,
Asociación de Auditoría y Control de Sistemas de Información
Estados Unidos de América. 2006.

13. Muñoz Razo, Carlos, Auditoría de Sistemas Computacionales
Editorial Pearson Educación
México. 2002.

14. Norma de Auditoría No. 26 Auditoría en un ambiente PED
Instituto Guatemalteco de Contadores Públicos y Auditores
Guatemala. 2001.

15. Norma Internacional de Auditoría No. 401 Auditoría en un Ambiente de Sistemas de Información.
Federación Internacional de Auditores
Estados Unidos de América. 2000.

16. Norma Internacional de Auditoría No. 1009 Técnicas de Auditoría con ayuda de la Computadora.
Federación Internacional de Auditores
Estados Unidos de América. 2000

17. Objetivos de Control para la Información y Tecnologías Afines COBIT
Instituto de Gobierno de Tecnología de Información
Estados Unidos de América. 2002.

18. Página Web, Conceptos de Auditoría de Sistemas. www.monografias.com

19. Página Web, Manual de Auditoría de Sistemas. www.monografias.com

20. Página Web. Superintendencia de Bancos de Guatemala. www.sib.gob.gt

21. Principios de Auditoría,
Editorial Whittington – Pany
México. 2004.

22. Sobrinoz Sanchez, Roberto.
Planificación y Gestión de Sistemas de Información
Escuela Superior de Informática de Ciudad Real Universidad de Castilla
España. 1997.